Die resiliente Organisation

Eine Analyse der Internationalen Politischen Ökonomie zur Sicherheitsproduktion in Unternehmen

Carsten Baran

Dissertation zur Erlangung des Grads eines Doktors der Sozialwissenschaften (Dr. rer. pol.) der Universität Erfurt,

Staatswissenschaftliche Fakultät

2023

Gutachter: Prof. Dr. Oliver Kessler

Gutachter: PD. Dr. Martin Koch

Datum der Disputation: 07.06.2023

Persistent Identifier URN: nbn:de:gbv:547-202300619

Inhalt

I) Einleitung 7
1. Problemkontext 7
1.1. Sicherheitsrelevante Implikationen für die Internationale Politische Ökonomie durch die Corona-Pandemie 7
1.2. Die Pandemie als Digitalisierungsschub 10
1.3. Disziplinäre Positionierung der Erforschung von Unternehmen 13
1.4. Multi-Nationale Unternehmen (MNU) 16
1.5. Kritische Infrastruktur und Sicherheitsproduktion im privaten Sektor 17
1.6. Ziel, Vorgehen und Kapitelstruktur 21
2. Verortung und Relevanz des Forschungsthemas 24
2.1. Die Rolle privater Autoritäten 24
2.2. Unternehmen als Akteure der Sicherheitsproduktion 26
2.3. Einordung in die Sicherheitsforschung 29
2.3.1. Versicherheitlichung und Kopenhagener Schule 30
2.3.2. Pariser Schule und die Bedeutung sozialer Praktiken 31
2.4. Methodische Grundlagen und Vorgehen 33
2.4.1. Ethnographische Untersuchung 33
2.4.2. Datenerhebung 36
2.4.2.1. Kapazität, Zeitrahmen und Rolle 37
2.4.2.2. Dokumentation der Beobachtungen 39
2.4.2.3. Inklusion und Reflexion 41
2.5. Digitalisierung, Risiko und Resilienz als Forschungsobjekte 44
2.5.1. Forschungsstand 45
2.6. Zusammenfassung – Sicherheitsproduktion in Unternehmen 51
II) Digitalisierung, Risiko und Organisation 53
3. Digitalisierung als Zäsur 54
3.1. Zeitalter der Informationen 55
3.1.1. Schlüsselbegriffe der Digitalisierung 56
3.1.2. Informationen und Informationserzeugung 64
3.2. Facetten der Digitalisierung 66
3.2.1. Informationen und Räumlichkeit 68
3.2.2. Von Informationsbruchteilen zu Big Data 72
3.2.3. Künstliche Intelligenz und Algorithmen 77
3.2.4. Virtualisierung in der Cloud 79
3.2.5. Nutzer 85

3.3. IT Kompetenz in Unternehmen 89
3.4. Neue Dienstleistungsangebote, alte Probleme 91
3.5. Zusammenfassung - Zäsur des digitalen Zeitalters 96
4. Organisations- und Risikobegriff in der soziologischen Organisationstheorie 97
4.1. Organisationssystematik und Selbstreflexion von Unternehmen 100
4.1.1. Autopoiesis von Organisationen 100
4.1.2. Abgrenzung von Systemen 104
4.1.3. Technologie, Informationen und Kommunikationsabbruch 108
4.2. Unsicherheitsabsorption 113
4.2.1. Umgang mit Unsicherheit 115
4.2.2. Risiko, Gefahr und Sicherheit 119
4.2.3. Risikokontrollsysteme 125
4.2.3.1. Risikoidentifikation und –Kategorien 128
4.2.3.2. Risikobewertung 135
4.3. Zusammenfassung – Risikokontrolle und Organisation im Wandel 140
III) Unternehmensinterne Sicherheitsproduktion im Wandel 142
5. Risikomitigation im analogen Zeitalter 144
5.1. Risikokontrolle und Sicherheit nach traditionellem Muster 145
5.1.1. Traditionellen Risikokontrollsysteme in Unternehmen 147
5.1.2. Schnittmenge zwischen Betriebskontinuität und Risikomanagement 150
5.1.3. Risikomatrix 153
5.1.4. Business Continuity Management und Krisenmanagement 156
5.2. Verantwortungsdelegation 164
5.2.1. Public-Private Partnership 165
5.2.2. Sicherheitsdiskurs und kritische Infrastruktur 168
5.2.3. Risikoträger und Verantwortung 171
5.3. Fallbeispiel 1 - Ausfall von Gebäuden – New York 11.09.2001 174
5.3.1. Bedeutung von RIA und BIA 177
5.3.2. Nicht-Verfügbarkeit von Gebäude 180
5.4. Fallbeispiel 2 - Ausfall von Dienstleistern – Fukushima 11.03.2011 184
5.4.1. Unerwartete Vermengung der Risikokategorien 187
5.4.2. Globale Produktionsprozesse und Abhängigkeiten 189
5.4.3. Risikokontrollsysteme und Verantwortungsdelegation 193
5.5. Fallbeispiel 3 - Ausfall von Personal – Pandemie 2003 – 2022 197
5.5.1. Adaptionsfähigkeit der Vorsorgeplanung 200
5.5.2. Die Angemessenheit von Maßnahmen 204

5.5.3. Krisen- und Risikokommunikation 207
5.5.4. Aktivierung von Krisenplänen 211
5.6. Zusammenfassung - Entwicklungsstand der Risikomitigation im analogen Zeitalter 212
6. Digitalisierung als Chance und Gefahr - Risikokontrolle im Cyberzeitalter 214
6.1. Die Orientierung an Prozessen und Systemen – der Resilienzbegriff 215
6.1.1. Veränderung des Risikoverständnis 217
6.1.1.1. Kritische Infrastruktur und rechtlicher Rahmen im Informationszeitalter 218
6.1.1.2. Verfügbarkeitsrisiken im Informationszeitalter 221
6.1.1.3. Bedeutung von Informationsschutz 222
6.1.2. Risikoexposition im digitalen Raum 225
6.1.3. Der Resilienzbegriff im Cyberzeitalter 227
6.2. Informationen und Daten als Schutzziel 233
6.2.1. Der sicherheitsrelevante Wert von Daten 233
6.2.2. Das Risiko der Daten 235
6.3. Fallbeispiel 1 - Identitätsdiebstahl und Social Engineering 239
6.3.1. Digitale Maskerade - Identitätsdiebstahl 240
6.3.2. Der menschliche Faktor - Social Engineering 244
6.4. Fallbeispiel 2 – Malware 248
6.4.1. Schadsoftwaretypen im Überblick 249
6.4.2. Malware als komplexe Bedrohung 253
6.5. Fallbeispiel 3 – Ransomware 256
6.5.1. Analyse einer modernen Lösegelderpressung 257
6.5.2. Strategische und praktische Krisenvorsorge 262
6.6. Fallbeispiel 4 – ITSCM zwischen Anspruch und Wirklichkeit 268
6.6.1. ITSCM - Rückkehr zum Ursprung 268
6.6.2. ITSCM - Theorie in der Praxis 271
6.7. Zusammenfassung- Risikomitigation im analogen und digitalen Zeitalter 274
IV) Implementierung der resilienten Organisation 276
7. Handlungsfelder und Umsetzung 277
7.1. Fortschritt und Schutz im Widerspruch? 278
7.2. Integrativer Risikokontrollansatz 282
7.2.1. Kritikalitäts- und Risikoanalyse 287
7.2.2. Ressourcenerfassung 293
7.2.3. Strategieformulierung 298
7.2.4. Plandefinition und Testen 305
7.2.5. Planaktivierung und Krisenmanagement 309

7.3. Herausforderungen einer erfolgreichen Implementierung 311
7.4. Zusammenfassung- Handlungsfelder und Prioritäten 314
8. Abschlussbetrachtung 317
8.1. Ergebnisreflektion 317
8.1.1. Exposition und Einordung in die Forschung 318
8.1.2. Methodisches Vorgehen und Erkenntniseinbindung 318
8.1.3. Folgen der Digitalisierung für Unternehmen und Organisationstheorie 320
8.1.4. Erkenntnisse der ethnographischen Untersuchung 322
8.2. Ausblick 326
9. Anhang 330
9.1. Abbildungsverzeichnis 330
9.2. Verzeichnis der Hintergrundgespräche 332
9.3. Bibliografie 334
A-F 334
G-M 344
N-Q 353
R-Z 355
Onlinequellen: 360
Zeitschriften: 364

I) Einleitung

1. Problemkontext

1.1. Sicherheitsrelevante Implikationen für die Internationale Politische Ökonomie durch die Corona-Pandemie

Die Corona-Pandemie, auch SARS-CoV-2 oder COVID-19-Pandemie genannt, zeigte neben den epidemiologischen und medizinischen Folgen, vielfältige Veränderungen im politischen, ökonomischen, technologischen und weiteren Bereichen auf[1]. Auch wenn die Corona-Pandemie zum Zeitpunkt des Verfassens dieser Arbeit noch nicht überwunden ist, lassen sich bereits einschlägige Auswirkungen beobachten. Neben makroperspektivischen Aspekten wie unterbrochenen Lieferketten[2] und Verschiebungen innerhalb der globalen Wirtschaftsstrukturen[3], sind auch signifikante Veränderungen auf der Mikroebene von Unternehmen zu verzeichnen. Auf den Führungsebenen von Unternehmen wurden in Folge der staatlich verordneten Lockdown-Maßnahmen nicht-ökonomische Entscheidungen diskutiert, die nicht einer ökonomischen Rationalität, sondern exogen vorgegebenen Sicherheitsdispositiven zuzuordnen waren.[4] Die Übersetzung dieser exogenen Problemsituationen in unternehmensinterne Entscheidungen war mit der Fortsetzung der unternehmenseigenen Prozesse und damit auch der Produktion von Sicherheit verbunden. Dadurch stellt sich die Frage, wie diese Übersetzung von Sicherheit in Unternehmen stattfindet und welche Folgen sie für die gesamtgesellschaftliche Sicherheitsproduktion nachzeichnen lassen? Diese Frage ist sowohl auf der Ebene der Unternehmen interessant, da von einer weiteren Einbeziehung nicht-ökonomischer Fakten und Prozesse in die Entscheidungen der Unternehmensführung auszugehen ist.[5] Darüber hinaus ist die Frage auch für die

[1] Die Bekämpfung der Pandemie verursachte hohe Kosten für die betroffenen Volkswirtschaften (Brzoska, Neuneck und Scheffran 2021: 4), vertiefte soziale Spannungen und Unterschiede, zeigte aber auch die gestiegene Dependenz von technologischen Strukturen auf, durch deren Einsatz Prozesse trotz Abstandsgebot in vielen Fällen fortgesetzt werden konnten (Bellmann et. al. 2021).

[2] Die pandemiebedingten Einschränkungen globaler Liefer- und Produktionsketten wurde durch die plötzliche Nachfrage nach medizinischer Schutzausrüstung, aber auch anderer Handelsgüter wie im Bereich der Automobilproduktion deutlich (Brzoska, Neuneck und Scheffran 2021: 3).

[3] Bisherige Modelle der Globalisierung von Arbeitsprozessen stoßen während der Pandemie, aber auch der Vrosrgeplanung von Staaten an ihre Grenzen. Dies zeigt auch die Abhängigkeiten zwischen Wirtschafts- und Produktionsräumen auf (Menzel 2021: 5), was zuletzt durch den Risikodiskurs um russische Gaslieferungen im Kontext des Angriffs auf die Ukraine extrapoliert wurde.

[4] Viele Staaten verhängten Ausgangssperren und Distanzregelungen zur Eindämmung der Pandemie. Als deren Folge waren viele Unternehmen mit der Herausforderung konfrontiert ihren Betrieb unter den Bedingungen des Infektionsschutzes und der einhergehenden Kontaktbeschränkungen fortzusetzen (Bellmann et. al. 2021: 713).

[5] An dieser Stelle sei auf das vierte Kapitel verwiesen, in dem die Risikokategorien im Unternehmenskontext diskutiert werden. Kategorien wie politische Risiken beziehen nicht-ökonomische Aspekte ein, waren aber selten von einem vergleichbaren globalen und zeitgleichen Umfang wie die Problematik durch die Lockdown-Maßnahmen im Zuge der Corona-Pandemie geprägt.

Sicherheitsforschung innerhalb der internationalen Beziehungen von Interesse, da die Rolle und Einbindung von Unternehmen in die Sicherheitsproduktion ein bereits längerfristig beobachtbarer Prozess ist. Insbesondere ist aber diese Frage für die Internationale Politische Ökonomie und die soziologische Organisationsforschung interessant, da hier zwei Systemrationalitäten zusammentreffen und neue Rückschlüsse ermöglichen, wie diese in Unternehmen ausgehandelt werden. Wie in dieser Arbeit zu zeigen sein wird, fällt vor allem die zunehmende Thematisierung und Bedeutung unternehmerischer Resilienz[6] auf, deren offensichtlichste Erscheinung in Form der Kontinuität von Arbeitsprozessen und (gesellschaftlich-)relevanten Dienstleistungen anzutreffen ist (Wentland und Klimburg-Witjes 2021: 185) und hier den Risikodiskurs im Unternehmen verändert.

Dieser neue Diskurs konnte während der Pandemie beobachtet werden. Die Fortführung der unternehmerischen Handlungsfähigkeit wurde vor allem durch die Lockdowns vor Herausforderungen gestellt. Die von den meisten Regierungen erlassenen Einschnitte in die Bewegungs- und Handlungsfreiheit ihrer Bürger zum Schutz vor einer unkontrollierten Ausbreitung der Krankheit führten zu einer weiteren Beschleunigung der Nutzung neuer Technologien (Engels 2020: 2). Zwar waren Arbeitsflächen und Büros im Lockdown funktional nutzbar und einsatzbereit[7], aber aufgrund des Abstandsgebots im Sinne des Infektionsschutzes dennoch nicht geeignet, die Mitarbeiter von dort arbeiten zu lassen. Dies hatte weitreichende Folgen für die volkswirtschaftliche Entwicklung und Produktionsleistung (Kocher und Weyerstraß 2020: 4). Die darauffolgende Verlagerung von Arbeitsschritten, zumindest in den dafür geeigneten Berufen[8], in eine virtuelle Arbeitsumgebung hatte neben organisatorischen, psychologischen oder monetären Auswirkungen auch signifikante Implikationen für die Hard- und Softwareanforderungen zur Folge (Boland et. al. 2020). Der Trend zur Virtualisierung von Prozessen und Vernetzung von Informationen erlebte mit der Pandemie eine rasante

[6] Resilienz bezeichnet die Risikovorsorge von Organisationen, um unter den Umständen von Unsicherheit Risiken durch ex ante geplante Maßnahmen zu steuern (Rose 2004: 308). Unter dem Eindruck des durch die Digitalisierung induzieren Wandels von Wertschöpfungsketten, Organisationsabläufen und Strukturen innerhalb von Unternehmen gewinnt Resilienz nicht nur an Bedeutung in der operativen Risikosteuerung (Choras et. al. 2015: 689), sondern bedeutet auch, dass „resilience policies act on the assumption that a disruption will take place“ (Kaufmann 2013: 55). Daher kann Resilienz als ein Werkzeug zur organisationsinternen Sicherheitsproduktion verstanden werden, deren Vorsorgeplanung einen besseren Umgang mit Unsicherheit bieten soll.

[7] Eine Studie aus dem Juni 2020 zeigte, dass ein Großteil der Beschäftigten in Nordamerika und Europa zu diesem Zeitpunkt bereits aus dem Home Office oder wie es im korrekten arbeitsrechtlichen Terminus heißt, aus dem mobilen Büro heraus arbeiteten (Boland et. al. 2020). Die Abstands- und Hygieneregeln (darunter insbesondere „social distancing“) und die Investition in technologische Alternativen zum physikalischen Arbeitsplatz im Büro bildeten den Imperativ für alternative Strategien, um die Fortsetzung von Geschäftsprozesse sicherzustellen.

[8] Es sind allerdings große Unterschiede zwischen den einzelnen Branchen zu verzeichnen. Während Unternehmen und Organisationen in den Bereichen Information und Kommunikation sowie Dienstleistungen stark in neue Technologien während der Pandemie investierten, fanden sich für Sektoren wie Verkehr oder Baugewerbe kaum substituierende Lösungen durch digitale Strukturen (Bellmann et. al. 2021: 714).

Beschleunigung.[9] Innerhalb von kurzer Zeit investierten Organisationen im erheblichem Umfang (Anant, Caso und Schwarz 2020: 2) in Hardware, Software und die zugrundeliegende IT-Infrastruktur (Bellmann et. al. 2021: 713), um dadurch die Existenz von Unternehmen während der Corona-bedingten Ausnahmesituation zu sichern (Hessel und Rebman 2021: 263).

Die Digitalisierung von Unternehmensprozessen und die Sicherstellung von deren Kontinuität waren als neuer Risikodiskurs bereits vor der Pandemie zu beobachten. Die Kehrseite dieser Entwicklung wird durch die gestiegene Notwendigkeit zur Sicherheitsproduktion in Unternehmen[10] mit Blick auf die kritischen Prozessen, Informationen und Mitarbeitern widergespiegelt (Bitaab et. al. 2021). Die Anzahl an registrierten Sicherheitsvorfällen und Angriffen mit Schadsoftware (Malware) nahm bereits zum Beginn der Pandemie mit einer Steigerung von über 600 Prozent zu (Lallie et. al. 2020: 3). Der weltweit gestiegene Datenverkehr (Engels 2020: 3) und die mithilfe virtueller Zugangskanäle kurzfristig umgesetzte Verlagerung an den heimischen Arbeitsplatz erhöhte die Risikoexposition vieler Unternehmen deutlich (Hessel und Rebman 2021: 263). Das Bewusstsein für die Bedrohung durch Cyberkriminalität, das bedeutet die Durchführung unautorisierter, computergestützter Maßnahmen gegen die Informationssouveränität von Individuen oder Unternehmen (Chigada und Madzinga 2021: 3), wurde zudem spätestens seit Beginn des Krieges in der Ukraine im Frühjahr 2022 und den öffentlichen Diskurs um die Versorgungssicherheit und dem zugrundeliegenden Schutz informationsverarbeitender Systeme weiter verschärft.[11]

Als Beispiel für die gesamtgesellschaftliche Relevanz von exogenen Sicherheitsdispositiven seien hier die gestiegenen IT-basierten Angriffe auf Krankenhausinfrastrukturen erwähnt, deren Zahl und Intensität mit dem Beginn der Pandemie signifikant anstiegen und Krankenhausbetreiber vor ungewohnt drängende Entscheidungen nicht-ökonomischer Natur zur Sicherstellung ihrer Funktionsfähigkeit stellten (Dochow 2022: 100). Deshalb ist es wichtig zu verstehen, welche bedeutende Rolle der digitalen Infrastruktur bereits vor der Pandemie zufiel und wie die pandemiebedingte Schließung von Arbeits- und Büroflächen zu einer

[9] Die Strukturen und Hintergründe dieser seit mehreren Jahrzehnten voranschreitenden Transition wird im Folgenden von mehreren Blickwinkeln aus beleuchtet werden. Die Bedeutung digitaler Strukturen für die Erbringung von Leistungen in Unternehmen war durch die erzwungene vollständige oder teilweise Abwesenheit von physikalischen Arbeitsflächen in Büros und Betrieben noch deutlicher zu Tage getreten und implizieren weitreichende Folgen für das organisationale Design der Wertschöpfung (Foss 2020).

[10] Die Unterscheidung zwischen der Sicherheitsproduktion in Unternehmen gegenüber der Sicherheitsbereitstellung durch Unternehmen wird weiter unten in einem eigenen Abschnitt dargelegt. Während Unternehmen in der Sicherheitsforschung als Erzeuger von Sicherheit an der Seite staatlicher Autorität bekannt sind, beispielsweise durch private Sicherheitsdienste (Olaniyan 2011: 7), wird hier das Konzept der Sicherheitsproduktion in Unternehmen betont, welches die Prozesskontinuität von Unternehmen adressiert.

[11] Die Sorge um gezielte Angriffe mit Schadsoftware im Rahmen der russischen Invasion in der Ukraine durch von Russland beauftragte oder gelenkte Hackergruppen trat im Frühjahr 2022 verstärkt in den Fokus (BSI: 2022).

exponentiellen Steigerung der virtuellen Arbeitsumgebung und ihrer kontinuierlichen Verfügbarkeit und Sicherheit führte.

1.2. Die Pandemie als Digitalisierungsschub

Die Folgen der Pandemie für viele Bereiche der nationalen und internationalen Politik können nach zweieinhalb Jahren sicherlich als einschneidend bezeichnet werden und werfen weiterführende Fragen für die Forschung auf. In dieser Arbeit wird die Pandemie vor allem als Digitalisierungsschub verstanden, der sich bereits im vorpandemischen Trend als langfristiger Prozess der Veränderung von Infrastrukturen und Prozessen zeigte. In Deutschland zeichnete sich beispielsweise bereits in den Jahren vor der Pandemie eine strukturelle Verschiebung hin zu virtuellen Erweiterung des physisch-räumlichen Verständnisses von Arbeitsplätzen ab. So stieg die Anzahl der Unternehmen, die zumindest einzelnen Mitarbeiter die Arbeit vom heimischen Arbeitsplatz ermöglichten, zwischen 2014 von 22 Prozent auf 39 Prozent im Vorpandemiejahr an (Engels 2020: 2). Der wesentliche Unterschied während der durch die Corona-Pandemie beschlossenen Lockdowns lag darin, den bestehenden "Trend zur Flexibilisierung von Arbeitsumgebungen“ (Wentland und Klimburg-Witjes 2021: 185) innerhalb kürzester Zeit und unter den erschwerten Bedingungen verknappter Ressourcenverfügbarkeit für einen Großteil der Belegschaft bereitzustellen und als Nebeneffekt dem Grad der Digitalisierung innerhalb der Unternehmen wesentlichen Vorschub zu leisten (Bellmann et. al. 2021: 718).

Die paradoxe Gestalt der digitalen Vernetzung im Informationszeitalter[12] mithilfe des Internets über Länder- und Kulturgrenzen hinweg auf der einen Seite fiel auf der anderen Seite mit einer temporären Isolation von Individuen als Folge des Lockdowns, der Einschränkungen von Grundfreiheiten und Abgrenzung von Nationalstaaten zusammen (Menzel 2021: 4). Der Wettbewerb um medizinisch relevante Ausstattung und Vorprodukte bis hin zur Verteilung von Impfstoffen zwischen Staaten zeigte die Schwierigkeiten der meisten Gesundheitssysteme auf, in Zeiten gestiegener globaler Nachfrage, bei gleichzeitig eingeschränkter

[12] Der Begriff des Informationszeitalters, ebenso wie das hier synonym verwendete digitale oder Cyberzeitalter, bezieht sich auf die technologischen, sozialen und wirtschaftlichen Veränderungen dieser Epoche. Ihre Charakteristiken sind nach Manuel Castells, dass “information generation, processing, and transmission become the fundamental sources of productivity and power because of new technological conditions emerging in this historical period” (Castells 2010: 21). Auf deren Grundlage entstanden Systeme, deren Elemente sich auf die (1) Bedeutung von Informationen, sowie (2) Anwendungsmöglichkeiten der informationsbasierten und –verarbeitenden Technologien sowie deren disruptive Gestaltungskraft beziehen. Drittens ist die (3) Rolle der Netzwerke als Verbindung von Informationen und Technologien zu nennen, deren Zusammenwirken erhebliche Implikationen für die ökonomische Rationalität von Unternehmen nach sich ziehen (ebd.: 70), aber auch deren Sicherheitsproduktion tangieren.

Lieferkettenkapazitäten, die Abhängigkeiten von den internationalen Wertschöpfungsketten[13] zu überwinden (Brzoska, Neuneck und Scheffran 2021: 3). Dadurch zeigten sich einerseits die Chancen der Digitalisierung zur Aufrechterhaltung der Geschäftsprozesse und Produktion in einigen Branchen, aber auch anderseits die signifikante Interdependenz globaler Versorgungs- und Transportrouten, sowie die massiven Beschränkungen in Branchen, deren Arbeitsschritte hauptsächlich auf den analogen Raum[14] beschränkt sind (Bellmann et. al. 2021: 714).

Durch diese Entwicklung spitzt sich allerdings auch eine sich seit mehreren Jahren anschwellende Konstellation zu, in der die Produktion von Gütern und Dienstleistungen, darunter auch gesellschaftsrelevante Grundleistungen, auf der Basis der Informationstechnologie entwickelt und betrieben werden, aber nicht ausreichend auf die exogene Sicherheitsproblematik vorbereitet waren, welche im Rahmen der Corona-Pandemie auftraten. Durch die Entscheidungen zur flächendeckenden und seit der Corona-Pandemie intensivierten Nutzung neuer Technologien erhöhte sich das Risiko von Zwischenfällen erheblich. Zwischen Ende 2019 und März 2020, dem Beginn der Lockdown-Maßnahmen in Europa, versechsfachte sich die Anzahl an dokumentierten Angriffen mit Schadsoftware (Lallie et. al. 2020: 3), beziehungsweise verfünffachte sich die Zahl der Ransomware-Attacken (Schulze 2021:2). In konkreten Schadenswerten ausgedrückt bedeutet dies, dass sich der geschätzte weltweite Schaden durch Angriffe auf digitale Infrastruktur im Jahr 2021 auf etwa 6 Billionen US-Dollar[15] beläuft, was eine Verdoppelung gegenüber der Annahmen für das Jahr 2015 darstellt (Chigada und Madzinga 2021: 8). Wie eine Studie von Bernand und Nicholson im Auftrag von Deloitte darlegt, belaufen sich die Kosten zur Durchführung eines Angriffs mit Schadsoftware nur auf den Bruchteil der Aufwendungen für Schutzmaßnahmen (Bernard und Nicholson 2020). Die Aussicht der Angreifer auf wertvolle Beute, welche Behörden und insbesondere Unternehmen im digitalen Raum zu schützen versuchen, folgt dabei ökonomischer Rationalität, welche mit Blick auf die verursachten Kosten durch Cyberkriminalität im digitalen Alltag nach Corona noch weiter zunehmen könnte.

[13] Allein die europäische Arzneimittelproduktion war zum Stand 2021 auf über 300 Vorprodukte angewiesen, die ausschließlich aus China bezogen werden konnten. Dies zeigt ein Beispiel der Abhängigkeit von globalen Produktions- und Lieferketten (Menzel 2021: 26).

[14] Dazu können Unternehmen aus den Sektoren Tourismus oder Baugewerbe gezählt werden, deren hauptsächlich auf physischen Interaktionen beruhenden Prozesse nicht durch digitale Prozesse substituierbar sind.

[15] Die Komplexität und Vertraulichkeit des Themas erschweren exakte Berechnungen des globalen Schadenwertes. Allerdings nehmen auch neben der seit Jahren zunehmenden Wertsteigerung digitaler Prozesse auch die kurzfristige und exponentielle Verlagerung von Wertschöpfungsketten in den virtuellen Raum während der Pandemie einzurechnen, welche den potentiellen Gewinn von Cyberangriffen erhöhen.

In den letzten Jahren illustrieren verschiedene Beispiele den globalen Wirkungskreis und das vielfältige Bedrohungsspektrum von kriminellen Gruppen. Unter den relevanten Erscheinungsbildern lassen sich ein Großteil der Bedrohungen in den drei Kategorien Phishing[16] (Dreißigacker, von Skarczinski und Wollinger 2020: 946), spezialisierte Malsoftware wie etwa Emotet[17] (Hessel und Rebman 2021: 263) oder Lösegelderpressung durch Ransomware[18] (Dochow 2022: 100) zusammenfassen. Diese Angriffe zielen nicht nur auf staatliche Organisationen wie Behörden oder andere Träger von sensiblen Daten ab, sondern auch im zunehmenden Maße auf den privaten Sektor. Ein Großteil der digitalen Infrastruktur, Software und virtuellen Produktionsprozesse befinden sich in der Eigentümerschaft von privaten Unternehmen (Carr 2016: 52), welche aufgrund ihrer Marktmacht, ihres spezialisierten Wissens um prozedurale Abläufe und der Technologiemonopole eine zentrale Rolle in der Entwicklung und Umsetzung von IT-Sicherheit spielen (Huang et. al. 2021: 627). Die bereits existierende Komplexität und Tragweite der Bedrohungslage interdependenter Technologien (Kaufmann und Blum 2011: 235) wurden durch die rasante Ausweitung der Digitalisierung im Rahmen der Corona-Pandemie signifikant erhöht und stellen die Beziehung zwischen staatlichen und privaten Sektor hinsichtlich der Sicherheitsproduktion vor neue Herausforderungen.

Somit stellt sich die Frage, welche Rolle Unternehmen bei der Sicherstellung von relevanten Dienstleistungen und Infrastrukturen spielen, von deren ununterbrochenen Bereitstellung die Fortführung der wirtschaftlichen, gesellschaftlichen, aber auch überlebenswichtigen Grundversorgung der Bevölkerung abhängt (vgl. Huang et. al. 2021; Kianpour, Kowalski und Øverby 2022; Schulze 2021). Diese zentrale Frage unserer Arbeit bezieht sich dabei sowohl auf Forschungsbereiche der Sicherheitstheorie in den Internationalen Beziehungen, aber auch auf Untersuchungsobjekte auf der Mikroebene handelnder Akteure im Wirtschaftsraum. Dadurch ist diese Arbeit anschlussfähig an die Literatur der Internationalen Politischen Ökonomie (IPÖ) einerseits und der Sicherheitsforschung innerhalb der Internationalen Politischen Soziologie (IPS) anderseits (vgl. Graz, Kessler und Kunz 2020), da die Einbeziehung nicht-ökonomischer Themen und Probleme in Entscheidungsfindungsprozesse von Unternehmen und deren

[16] Phishing beschreibt den unautorisierten Zugang zu vertraulichen Informationen wie Passörtern oder Zugangsdaten (Hejase et. al. 2021: 20) um im nächsten Schritt Systeme zu infiltrieren (Hong 2012: 75).
[17] Spezialisierte Malsoftware erfüllt einen dezidierten Aufgabenbereich, zumeist im Rahmen einer arbeitsteiligen Strategie zur Erbeutung wertvoller Datensätze aus fremden Systemen. Emotet ist eine Software, die als Eintrittsplattform für andere Schadsoftware dient und diese je nach Aufgabenbeschreibung auf ein System nachladen kann (Hessel und Rebman 2021: 263).
[18] Ransomware dient im Allgemeinen der Verschlüsselung von Daten auf fremden Systemen, deren Dekodierung nur gegen die Zahlung eines Lösegeldes ermöglicht wird (Bhardwaj et. al. 2016: 2).

Teilhabe an der Sicherheitsproduktion im Grenzbereich zwischen IPÖ und IPS anzutreffen ist. Die sich durch die Corona-Pandemie beschleunigenden Veränderungen der Sicherheitsherausforderungen erfordern daher im Kontext dieser Arbeit eine Einbeziehung von sowohl wirtschaftlicher, als auch sicherheitspolitischer Perspektiven, an deren Schnittstellen diese Arbeit einen Beitrag zur Grenzauslotung leisten kann. Dies soll durch die Anwendung des sicherheitstheoretischen Diskurses und deren methodischen Werkzeuge auf die politisch-ökonomischen Beobachtungsobjekte auf der Ebene von Unternehmen erreicht werden.

Das Angebot dieser Arbeit richtet sich trotz der Untersuchung einer wirtschaftlichen Akteursebene in Form von Unternehmen also nicht vorrangig an die klassische ökonomische Forschung oder Managementliteratur, als vielmehr an die Autoren der Sicherheitsforschung. Nichtsdestotrotz öffnet diese Arbeit Möglichkeiten zur allgemeinen Anschlussfähigkeit in andere Bereiche wie beispielsweise der IPÖ oder IPS. Wie im nächsten Kapitel gezeigt werden wird, werden insbesondere Vertreter der Pariser Schule[19] angesprochen, deren Anwendung ethnographischer Methoden auf relevante sicherheitstheoretische Fragestellungen in dieser Arbeit auf die Rolle unternehmensinterner Sicherheitsproduktion im Kontext der Risiken der Digitalisierung erweitert werden soll. Dieser Anschluss an die Sicherheitsliteratur wird durch unsere Fragestellung als Möglichkeit vorgestellt, die aktuellen Forschungspraktiken der IPÖ und IPS zusammenzubringen und ein bisher unterrepräsentiertes Feld zu beleuchten. Denn vor dem Hintergrund der fortschreitenden digitalen Vernetzung der Gesellschaft, nimmt der private Sektor eine essentielle Rolle durch die Eigentümerschaft und das Wissen zur Nutzung der technologische Grundlagen ein (Christensen und Petersen 2017: 1442f.; Bryce et. al. 2020: 883). Auf der Basis dieser Einordnung soll im Folgenden der disziplinäre Hintergrund unserer Fragestellung und die Rolle von Unternehmen im bisherigen Sicherheitsdiskurs vertieft werden.

1.3. Disziplinäre Positionierung der Erforschung von Unternehmen

Blickt man innerhalb der Literatur der Internationalen Beziehungen auf die Bedeutung des privaten Sektors für die Produktion von Sicherheit, erscheint die Rolle von Unternehmen im Vergleich zu ihrer tragenden Rolle im Bereich der Digitalisierung unterbewertet, insbesondere mit Blick auf die Rolle technologischer Risiken (Davidshofer, Jeandesboz und Ragazzi 2016: 220). Aus der Perspektive klassischer Ökonomieliteratur werden Unternehmen als rational handelnde Akteure beschrieben, deren Interaktionen und Handlungsmuster vom Ziel der Nutzenmaximierung bestimmt werden, beispielsweise zur Vermeidung von Produktionskosten

[19] Die Pariser Schule wird im zweiten Kapitel vorgestellt. Vertreter dieses Ansatzes betrachten die transformativen Praktiken von Akteuren und Abläufe innerhalb von Organisationen, um sicherheitstheoretische Fragestellung zu thematisieren (Bigo und McCluskey 2018: 123).

oder Steuerbelastungen durch globale Diversifizierung (Zschoche 2015: 3). Diese Ziele verstehen sich im disziplinären Verständnis der Ökonomie im Interessenskonflikt, wenn nicht Widerspruch zu den Zielen des wohlfahrt-orientierten Gemeinwesens, repräsentiert durch staatliche Akteure[20] (Eden 1991: 198; Carr 2016: 56).

Auch im Fall der oben skizzierten Partnerschaft zwischen privaten und staatlichen Sektor zur Sicherheitsproduktion verzeichnen sich in dieser Hinsicht nur geringfügige Unterschiede in der Literatur (Cavelty und Suter 2009: 7; Huang et. al. 2021: 262). Doch es stellt sich die Frage, warum und nach welcher Methodik Unternehmen zur Sicherheitsproduktion beitragen? Diese Frage beschränkt sich jedoch nicht nur auf die Erzeugung von Sicherheit durch Unternehmen, sondern vor allem auf Maßnahmen und Strukturen zur Risikomitigation innerhalb von Unternehmen selbst, wie im unten nachfolgenden Abschnitt detaillierter erklärt werden soll. Um nun die Handlungsmotive und Innenperspektive von Unternehmen stärker beleuchten zu können, bietet es sich entgegen der auf die inhärente Eigenlogik gewinnorientierter Unternehmen fokussierte klassisch-ökonomische Sichtweise an, eine organisationssoziologische Perspektive einzubeziehen.

In diesem Kontext erscheinen Forschungsimpulse aus der Organisationssoziologie, allen voran Luhmanns einflussreiche Organisationssystematik, sowie Differenzierung von Risiko, Gefahr und Entscheidung (Luhmann 1991; 2000), sowie der Sicherheitsforschung in den Internationalen Beziehungen (IB) als interessante Anknüpfungspunkte.[21] Die später einzuführende Rolle von Entscheidungsprogrammen zum Umgang mit Risiken bei Luhmann (Luhmann 2000: 271) wird hier aber weniger im Mittelpunkt stehen, als vielmehr die Unterbindung einer möglichen Unterbrechung der Anschlusskommunikation, welche wir im vierten Kapitel vertiefen werden. Mit Blick auf die disziplinären Überschneidungen kann - ohne den Anspruch auf eine Neuerzählung der gemeinsamen Geschichte zwischen IPÖ und IPS zu erheben - beiden Disziplinen die Tendenz attestiert werden, sich hinsichtlich neuer Strömungen und Spezialisierungen zu öffnen (Graz, Kessler und Kunz 2020). Über die Zeit stellte sich jedoch eine jeweilige Fokussierung im Kontext der Sicherheitsforschung heraus, die sich im Fall der IPS auf Identitäten richtete und für die IPÖ auf die finanziellen Aspekte des Begriffs

[20] Ein Beispiel hierfür ist der Ein- und wieder Austritt des US-Unternehmens Walmart auf den deutschen Markt, das neben anderen ökonomischen Gründen, in Konflikt mit nationalen Standards der Betriebsverfassung und einen Widerspruch zwischen unternehmensinternen, globalen Verhaltensstandards auf der einen Seite gegenüber nationalen Grundlagen auf der anderen hervorbrachte (Talaulicar 2009: 52).

[21] Wie bereits zuvor eingeleitet, ergeben sich mit Blick auf die Internationale Politische Soziologie (IPS) und die Internationale Politische Ökonomie (IPÖ) nicht nur spannende Überschneidungen, sondern auch Klärungsbedarf hinsichtlich unserer Forschungsfrage. Dies betrifft die disziplinäre Verortung einerseits und die empirischen Grundlagen andererseits, welche im zweiten Kapitel vertieft werden.

Sicherheit abzielte, beispielsweise über die Bekämpfung der Finanzierung organisierter Kriminalität oder des Terrorismus (Kahler 2018).

Die disziplinäre Verortung dieser Forschungsarbeit richtet sich an die Gemeinsamkeiten von IPS und IPÖ. Ein Dialog zwischen beiden Disziplinen und ihren jeweiligen Perspektiven auf das Feld der Sicherheitsforschung erscheint durch die zunehmenden Risiken der Digitalisierung, nicht zuletzt durch den Digitalisierungsschub als Folge der Corona-Pandemie vielversprechend, wenn nicht sogar eine zwingende Konsequenz (Graz, Kessler und Kunz 2020: 590). Zudem sind wie eingangs erwähnt organisationssoziologische Aspekte relevant, um die Handlungsmotive und Entscheidungsgrundlagen von Unternehmen zu beleuchten, deren Einsatz und kontinuierlicher Betrieb von Technologien den Ausgangspunkt unserer Frage bildet. Bereits vor drei Dekaden thematisierte Niklas Luhmann die Ambivalenz[22] von Hochtechnologie: Denn wenn der gezielte Einsatz von Technologie zur Sicherheitssteigerung dennoch „unvorhergesehene Wirkungen von unter Umständen katastrophalen Ausmaßen auslöst, wird die Anwendung von Technik auf Technik zu einem andersartigen Problem“ (Luhmann 1991: 102). Übertragen auf die Erfahrungen der Corona-Pandemie bedeutet dies, dass die Kontinuität von Geschäftsprozessen durch eben solche *neuen* technologischen Lösungen sichergestellt werden sollte (Bellmann et. al. 2021: 713), aber auch Sicherheitsrisiken durch die Entscheidung zum Einsatz dieser Technologien beinhaltet (Lallie et. al. 2020: 15).

Die relevante Neuerung in der technologischen Risikobetrachtung der Digitalisierung liegt in ihrer globalen Reichweite und interdependenten Struktur begründet. Vereinfacht gesprochen kann zumeist die Fehlfunktion oder Manipulation eines einzelnen, autonom operierenden Elements durch eine Isolation des Bereichs kompensiert werden. Doch dies gilt nicht für eine Komponente mit multiplen Verknüpfungen zu anderen vitalen Systemen, welche durch ihren Ausfall eine gravierende Problematik entfalten könnte (Kaufmann und Blum 2011: 235). Dies gilt sowohl für biologische Organismen, Wirtschaftskreisläufe oder eben auch für die zunehmend vernetzte, digitalisierte Systeminfrastruktur, von deren Integrität und Verfügbarkeit elementare Leistungen der Grundsicherung in modernen Gesellschaften abhängen. Vor dem Hintergrund der gestiegenen und weiter zu vertiefenden Cyberbedrohungen[23] bietet eine

[22] Solange das Risiko auf das Nicht-Funktionieren begrenzt ist, also das Ausmaß des Schadenspotentials auf die Nichtverfügbarkeit einzelner Komponenten limitiert und durch abgegrenzte Kontrollmaßnahmen eingedämmt ist, können Vereinfachung und Isolation geeignete technische Absorptionsmaßnahmen sein (Luhmann 2000: 252).
[23] Der Industrieversicherer AGCS verzeichnete in einer Umfrage unter mehr als 2.000 Risikoexperten für das Jahr 2022 das größte Risiko aufgrund der zugenommenen Bedrohungslage in der Kategorie Cyberzwischenfälle für Unternehmen, worunter Cyberangriffe, Systemausfälle und Verletzungen der Datensicherheit subsumiert wurden (vgl. AGCS 2022).

Betrachtung der diese Infrastruktur verantwortenden Unternehmen einen aufschlussreichen Beitrag zur Sicherheitsforschung an. Dies soll zudem unter Berücksichtigung der benannten disziplinären Perspektiven aus IPÖ, IPS mithilfe der Organisationssoziologie zusammengeführt werden, um die Betrachtung von Sicherheit innerhalb politisch-ökonomischer Prozesse zu ermöglichen. Der nächste Abschnitt wird sich daher zunächst der Einordnung und Relevanz von Unternehmen für die IPÖ widmen.

1.4. Multi-Nationale Unternehmen (MNU)

In der Internationalen Politischen Ökonomie werden Multinationale Unternehmen (MNU) über ihren Beitrag zur globalen Produktion und Wertschöpfung beschrieben, deren Produktionsprozesse in mindestens zwei verschiedenen Staaten angesiedelt sind (Caves 2000: 145), beziehungsweise aus makroökonomischer Sicht „global systems of production, exchange and distribution" darstellen (Eden 1991: 197). MNU sind strukturprägend für die Internationale Politische Ökonomie und waren Gegenstand von Debatten zur richtungsgebenden Rolle von Unternehmen in den Internationalen Beziehungen. Hierbei war die Bedeutung von MNU relevant, welche aufgrund ihrer wirtschaftlichen Einflussmöglichkeiten für die Analyse von internationaler Politik und der Rolle einer globalen wirtschaftsbasierten Serviceindustrie auf Aspekte staatlicher oder regionaler Entscheidungsprozesse referenzierten (Babic, Fichtner und Heemsker 2017: 20f.). Insbesondere die Einflussmöglichkeiten von MNU als strategische Akteure im globalen Kontext durch ihren Zugang zu Märkten oder der in manchen Bereichen exklusive Einsatz von Technologie waren nach Ansicht von Autoren wie Susan Strange wesentliche Gründe die MNU stärker in die Perspektive der IB zu rücken (Strange 2000: 64).

Mit Blick auf die kapitalgestützten Einflussmöglichkeiten von MNU gibt folgendes Bild Aufschluss: Die weltweit größten MNU[24] verantworten einen erheblichen Teil der globalen Wertschöpfung (Babic, Fichtner und Heemsker 2017: 21) und tragen wesentlich zur Definition von Gestaltungspraktiken in der internationalen Ökonomie bei (Isolauri, Zettinig und Nummela 2021: 16). Ein Beispiel dafür entlehnt sich der Rolle multinationaler Unternehmen in der Bereitstellung und Bewegung von Ressourcen und Geldmitteln, durch deren komplexe Interdependenzen sich grenzüberschreitende Finanzaktivitäten der absoluten Kontrolle (einzel-)staatlicher Institutionen entziehen können (Hart und Ortiz 2014: 488). Auch andere Bereiche, in denen MNU gesellschaftsrelevante Dienstleistungen erbringen, können als Beispiele dafür dienen, wie die Umsetzung von Vorgaben verschiedener nationaler Anforderungen im Rahmen

[24] Im Jahr 2017 verwaltete eine Gruppe von 147 MNU etwa 40% der weltweiten Wertschöpfung (Babic, Fichtner und Heemsker 2017: 21). Zu Beginn der 1990er Jahre teilten sich noch mehr als 600 Unternehmen, einen wesentlich kleineren Anteil der globalen Wirtschaftsleistung untereinander auf (Eden 1991: 197).

des eigenen Normenkontrollsystems geschieht. Die Kontrolle der Umsetzung staatlicher Vorgaben stellt insbesondere eine Herausforderung im Fall von MNU dar, wenn sie im definitorischen Sinne auf multinationaler Ebene agieren und daher mehr als nur eine rechtsgebende Institution zu berücksichtigen haben (Cutler, Haufler und Porter 1999: 7).

Die grenzüberschreitende Struktur und Aktivitäten von MNU begründen somit die Herausforderung, verbindliche Anforderungen an Unternehmen für die verlässliche Erbringung kritischer Dienstleistungen durch einen einzelnen Staat oder Wirtschafts- und Rechtsraum zu benennen, festzuschreiben und durchzusetzen. Die IPÖ-Literatur verfolgte dieses Problem zumeist aus der Sicht des grundsätzlichen Interessenskonfliktes zwischen Staaten und Märkten (Eden 1991) beziehungsweise der Rolle von Unternehmen in der Wahrnehmung gesellschaftlicher Verantwortung aus Sicht der IPS (Dolan, Garsten und Rajak 2011: 4). Der Trend der letzten Dekaden zur Privatisierung (Carr 2016: 48) und die Verschiebung der Machtbasis im Fall von Unternehmen von Kapital auf Technologie beziehungsweise Wissen (*Know-how*) (Fieldhouse 2000: 174) lassen MNU zum Beginn der 2020er Jahre in einem neuen Kontext erscheinen (Huang et. al. 2021: 626). Denn die zunehmende Bedeutung von MNU zur Sicherheitsproduktion im digitalen Raum wirft neue Fragen an das Verhältnis von staatlicher Verantwortung, Ökonomie und Sicherheit auf. Dies zeigt sich insbesondere am Spannungsverhältnis der Verantwortung und Umsetzung von Sicherheitsstandards für gesellschaftsrelevante Güter und Dienstleistungen, welches im Folgenden erörtert werden wird.

1.5. Kritische Infrastruktur und Sicherheitsproduktion im privaten Sektor

Mit Blick auf die Fragestellung dieser Arbeit sind MNU als zentrale Elemente innerhalb der Bereitstellung von Sicherheit besonders interessant, um Anknüpfungspunkte für die Sicherheitsforschung ableiten zu können. Die ursprüngliche Vorstellung einer exklusiven Zentrierung der Kompetenzen zur Bereitstellung von Sicherheit in der alleinigen Verantwortung staatlicher Institutionen (Goldstein 2010: 492) erlebte in der jüngsten Vergangenheit eine signifikante Veränderung (Davidshofer, Jeandesboz und Ragazzi 2016: 217). Die Betrachtung der Privatisierung von Sicherheit in Form von privaten militärischen Unternehmen belegte den problematischen Fall der Aufhebung staatlicher Monopole und Kapazitäten, wie es beispielsweise Anna Leander für den afrikanischen Kontinent zeigte (Leander 2005: 609). Auch jenseits der militärischen Dimension von Erscheinungsformen privater Teilhabe an sicherheitspolitischen Domänen entwickelten sich Handlungsfelder und Geschäftsmodelle für private Anbieter von spezialisierten Dienstleistungen im

Sicherheitsumfeld (Krahmann 2007: 15). Der Markt für Sicherheit[25], also die Produktion von Sicherheit durch Unternehmen eröffnete dem privaten Sektor Möglichkeiten gewinn-orientierte Angebote für Dienstleistungen zu unterbreiten (Christensen und Petersen 2017: 1439) und originäre Aufgaben des Staates in diesem Feld zu übernehmen (Olaniyan 2011: 7). Durch die Digitalisierung beschleunigte sich dieser Prozess insbesondere für den exponentiell wachsenden Wirkungskreis der Cybersicherheit, durch welche sich die Rolle des Staates zunehmend auf die Normenvorgabe und Garantie für die Einhaltung für Sicherheit konzentrierte (Carr 2016: 48).

Die Bereitstellung von Sicherheit durch MNU entwickelte sich zu einem essentiellen Bestandteil der gesamtgesellschaftlichen Sicherheitsproduktion durch die geteilte Verantwortung zwischen staatlichem Schutzanspruch und privatwirtschaftlicher Eigentümerschaft[26] über die für relevante Güter und Leistungen benötigten Ressourcen (Christensen und Petersen 2017: 1439). Für Organisationen aus diesem Bereich findet sich in der Literatur der Begriff der kritischen Infrastruktur (Alcaraz und Zeadally 2015: 5370). Dieser Terminus umfasst die Strukturen und Ressourcen für die Erbringung von gesellschaftlich relevanten, unverzichtbaren Leistungen, deren kontinuierliche Bereitstellung für die Funktionsfähigkeit der Gesellschaft als notwendig erachtet wird. Unter kritischer Infrastruktur im Kontext dieser Arbeit sind zum überwiegenden Teil MNU zu verstehen (vgl. Schintler et. al. 2007: 291), durch „deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (Dochow 2022: 103).

Jedoch stehen sich die Interessen von MNU, welche im klassischen ökonomischen Verständnis profit-orientierte Interessen verfolgen (Carr 2016: 56) und denjenigen der Öffentlichkeit mit Blick auf die gemeinsame Verantwortung für den Schutz der Bevölkerung unter Umständen entgegen. Für den Fall der Cybersicherheit ist in dieser Hinsicht keine Ausnahme zu erwarten (Huang et. al. 2021: 262). Unternehmen befinden sich als Teilhaber der öffentlichen Sicherheit und bei gleichzeitiger Verortung in einem System ökonomischer Profitorientierung in einem interessanten Spannungsfeld, das später in dieser Arbeit wieder aufgegriffen werden wird. Im

[25] Private Sicherheitsunternehmen übernehmen beispielsweise Schutzaufgaben bei der Bewachung von Liegenschaften (im In- und Ausland) oder Personen (Personenschutz, aber auch in privat-geführten Gefängnissen) und auch eine zunehmende militärische Unterstützung für Staaten in Krisengebieten (Olaniyan 2011: 7).

[26] Die Corona-Pandemie verdeutlichte diese Ambivalenz besonders anschaulich im Fall der pharmazeutischen Produzenten von Impfstoffen sowie der Organisation und Beschaffung von Schutzkleidung (Ghanchi 2020: 806). Dies reicht von der Kompetenz privater Unternehmen zur Entwicklung und Produktion von Pharmaprodukten, oder medizinischen Gütern bis hin zu Infrastrukturbetreibern mit hohem gesellschaftlichem Interesse, welche in der Pandemie zu einer Frage der nationalen Sicherheit generierten (Marom und Lussier 2020: 255).

Folgenden wird kritische Infrastruktur[27] als die Verbindung zwischen den eingangs besprochenen sicherheitsbezogenen Entscheidungen von Unternehmen und ihrem elementaren Beitrag zum Gemeinwohl verstanden. Eine Prozessunterbrechung innerhalb von Unternehmen in der kritischen Infrastruktur würde demnach die Grundversorgung der Bevölkerung gefährden.

Daher ist es notwendig Unternehmen auf eine komplexe und Schadensereignisse antizipierende Perspektive des Schutzes der für die öffentliche Grundversorgung relevanten Prozesse und Leistungen vorzubereiten (Fekete, Grinda und Norf 2016: 222). Dazu ist es notwendig zwei Begriffe und Handlungsräume klar zu unterscheiden. Einerseits leisten private Unternehmen weiterhin einen Beitrag zur Bereitstellung von Sicherheit durch Dienstleistungen, welche im Rahmen erweiterter staatlicher Kompetenz oder an deren Stelle in Erscheinung treten (Kuerbis und Badiei 2017: 472). Dieses Forschungsfeld ist in der IB repräsentiert und betrachtet beispielsweise die geteilte Teilhabe des Gewaltmonopols zwischen staatlicher und privater Ebene oder die Übertragung von Autorität auf ausführende Organisationen in privater Trägerschaft unter Legitimierung durch staatliche Auftraggeber (Carr 2016; Cavelty und Suter 2009; Kaufmann 2015). Die Beteiligung von Unternehmen an sicherheitsrelevanten Aufgaben des Staates wurde in der Vergangenheit etwa im Sinne der Insolvenzverhinderung systemkritischer Finanzinstitute diskutiert (BCBS 2012: 11; Best 2010: 42) oder zeigten etwa die Komplexität durch private Akteure im globalen Sicherheitsdialog auf (Kessler 2011:197).

Der zweite Begriff ist von signifikanter Bedeutung für unsere Fragestellung, indem die zuvor gezeichnete Betrachtung von privaten Unternehmen als Bereitsteller von Sicherheit für die Gesellschaft durch die Perspektive auf die interne Produktion von Sicherheit in Unternehmen erweitert wird. Insbesondere mit Blick auf die technologische und zentrale Rolle von Unternehmen im Cyberraum wird die Sicherheitsproduktion in Unternehmen relevant (Huang et. al. 2021: 626). Der in Betracht zu ziehende Geltungsumfang von sicherheitsrelevanten Akteuren in Gestalt von Unternehmen wird dadurch wesentlich erweitert, da nun nicht nur jene Unternehmen mit klarem sicherheitsorientiertem Leistungskatalog in Frage kommen, sondern alle privaten Träger von Infrastruktur, Technologie und Wissen[28], die für die Aufrechterhaltung

[27] Kritische Infrastruktur liegt zu über 85 Prozent in der Eigentümerschaft von privaten Unternehmen und wird durch deren Betrieb aufrechterhalten. Eine mögliche Prozessunterbrechung auf Seiten dieser Unternehmen würde die Versorgung mit den jeweiligen Gütern und Dienstleistungen für die Bevölkerung gefährden (Carr 2016: 52).

[28] Die Einführung und Nutzung von Technologien zur Verbesserung der Sicherheitsproduktion basiert im Kern neben der technischen Implementierung wesentlich vom Kenntnisstand und Vertrautheit im Einsatz dieser Technologien. Dazu sind spezialisierte Experten notwendig, welche sich vorrangig in den Unternehmen finden, welche die Technologien herstellen oder zum Einsatz bringen (Davidshofer, Jeandesboz und Ragazzi 2016: 212).

gesellschaftskritischer Strukturen notwendig sind. In dieser Rolle unterscheiden sich nicht nur der bisherige Umfang und die Natur gegenüber der Bereitstellung von Sicherheit durch Unternehmen, sondern auch das methodische Konzept sicherheitspolitischer Analyse.

Neben dieser essentiellen Unterscheidung zwischen Sicherheitsproduktion *durch* gegenüber *in* Unternehmen, wird im Kontext unserer Fragestellung auch die Differenzierung der semantischen Interpretation von Sicherheit relevant werden. Die Literatur der IB verzeichnet die Sicherheitsbereitstellung innerhalb des Vokabulars des klassischen staatszentrierten Verständnisses (Goldstein 2010: 492), demgegenüber sich für die Sicherheitsproduktion in Unternehmen der Begriff der Resilienz herausgebildet hat. Dieser Terminus unterscheidet sich im Bedeutungssinn privater Anwender wie Unternehmen von dem vorherrschenden Bild in den Internationalen Beziehungen durch die begriffsinhärente Ablehnung des Sicherheitsbildes als erreichbaren Zustand (Blum et. al. 2016: 155). Resilienz als Bezeichnung für unternehmensinterne Sicherheitsproduktion meint vielmehr eine Richtungsorientierung und agile, fortschreitende Methodik zum Schutz relevanter Schutzziele (Fekete, Grinda und Norf 2016: 220). Gegenüber anderen Deutungen von Resilienz, wie beispielsweise als Möglichkeit zur politischen Steuerung (vgl. Chandler 2014) verstehen wir im Folgenden Resilienz im Kontext der unternehmensinternen Sicherheitsbereitstellung. Somit thematisiert Resilienz in dieser Arbeit als Überbegriff der internen Vorsorgeplanungen die Fähigkeit auf unvorhergesehene, auch plötzliche Schadensereignisse zu reagieren und die eigene Geschäftstätigkeit fortführen zu können. Wir werden diesen Begriff und die dahinterliegende Logik der systemischen, prozess-orientierten Risikokontrolle im sechsten und siebten Kapitel im Detail als Schlussfolgerung aus der ethnographischen Untersuchung diskutieren.

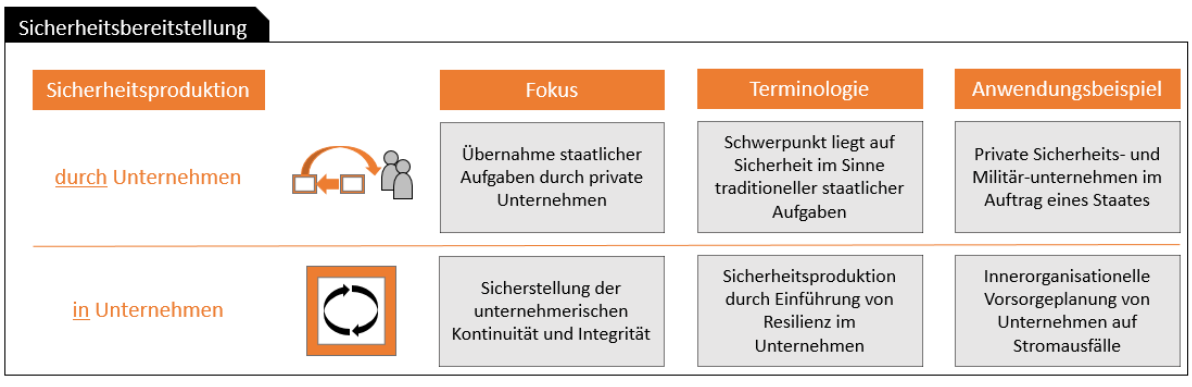

Abb. 1.1. Differenzierung von Sicherheitsproduktion durch und in Unternehmen. Eigene Darstellung.

Der Blick in die Organisation, Strukturen und Strategien von MNU zur Sicherstellung ihrer eigenen Sicherheit sind nicht zuletzt durch die Corona-Pandemie zu einem Novum des gesamtgesellschaftlichen Risiko- und Sicherheitsdiskurses avanciert. Die interne

Vorsorgeplanung von MNU ermöglichte es diesen in erster Instanz die Herausforderungen der Pandemie größtenteils erfolgreich zu bestehen, doch beschleunigte sich mit der Intensivierung technologischer Lösungen auch die eigene Risikoexposition.[29] Betrachtet man nun zusammenfassend erstens die essentielle Rolle von MNU für die kritische Infrastruktur, zweitens die geteilte Verantwortung für Sicherheitsproduktion zwischen staatlichen und privatem Sektor, sowie drittens die zunehmende Komplexität und folglich Vulnerabilität digitaler Systeme, stellen sich spannende Fragen über die Umsetzung von Sicherheit innerhalb von Unternehmen. Diese Fragen repräsentieren schließlich das Kernthema dieser Arbeit und sollen im Folgenden vertieft werden.

1.6. Ziel, Vorgehen und Kapitelstruktur

Die Verortung dieser Arbeit in der Schnittmenge zwischen IPÖ und IPS eröffnet neben der eingangs erwähnten Öffnung der disziplinären Zusammenarbeit auch die Möglichkeit, die Betrachtung auf ein bisher unterrepräsentiertes Feld der Sicherheitsforschung zu lenken, was sowohl die Rolle der Unternehmen, als auch der eingesetzten Technologien betrifft (Davidshofer, Jeandesboz und Ragazzi 2016: 220). Die Implikationen der Corona-Pandemie auf den Bedarf und die Abhängigkeit im Verhältnis zur digitalen Infrastruktur bietet ein spannendes Metanarrativ für die Sicherheitsforschung. Die Sicherstellung der eigenen (Fort-)Existenz von Unternehmen und Integrität ihrer Schutzwerte, differenziert sich auch vom staatsorientierten Ansatz sicherheitspolitischer Steuerung, indem Unternehmen auf der Grundlage intrinsischer und extrinsischer Motivation[30] in Maßnahmen zur Verringerung von Risiken investieren und somit einen Beitrag zur gesamtgesellschaftlichen Sicherheit leisten. Der Unterschied ist allerdings, dass dies nicht als ausführende Instanz staatlicher Autorität geschieht, sondern als eigengesteuerter Prozess intraperspektivischer Interessen von MNU als Akteuren der Sicherheitsarchitektur. Dies setzt die Betrachtung von Unternehmen voraus und damit die Einbeziehung von Analyseobjekten der IPÖ, aber aus dem Blickwinkel der sicherheitstheoretischen Domäne und Methodologie der IPS.

Als Antwort auf die Frage nach der Bereitstellung von Sicherheit in Unternehmen müssen folglich die Strukturen, Entscheidungsprozesse und Prozeduren innerhalb der Organisationen berücksichtigt werden. Die dafür notwendigen Informationen sollen mit Hilfe ethnographischer

[29] Das Risiko der Entscheidung ist für Luhmann durch eben diese Ambivalenz gekennzeichnet, in der die Entscheidung für oder gegen eine Handlung das eigentliche Risiko darstellt (Luhmann 1991: 24f.).
[30] Die Gründe zur Etablierung von Resilienz in Unternehmen wird Gegenstand der nächsten Kapitel sein. Prinzipiell sei hier auf den Gegensatz zwischen intrinsischen Nutzen der Investitionen (Christensen und Petersen 2017: 1443) und der Ausrichtung an gewinnorientierten Zielen im privaten Sektor hingewiesen, welcher zu einem Interessenskonflikt führen könnte Carr 2016: 56).

Methoden gewonnen werden (Hanson 2018: 136), deren Anwendung neue Erkenntnisse aus dem Inneren von Unternehmen zum Sicherheitsdiskurs beisteuern kann.[31] Die Auswertung der Prozesse zur Risikomitigation auf Mikroebene, der zugrundeliegende Wandel der Anforderungen an Unternehmen durch die Chancen und Risiken der Digitalisierung, insbesondere die Bedrohungslage der fortschreitenden Vernetzung, sowie der Einfluss der Pandemiemaßnahmen auf die Vulnerabilität von Systemen[32] sind dabei relevante Bezugsquellen. Gemeinsam mit einer Betrachtung der internen Sicherheitsproduktion von MNU soll diese Arbeit daher eine bisher unterrepräsentierte Perspektive zur Sicherheitsforschung in der IB beitragen. Daraus ergibt sich die nachfolgende Kapitelstruktur und Vorgehensweise, welche in vier Themenblöcke gegliedert ist.

Der (1) erste Themenblock erläutert gemeinsam mit dieser Einleitung die disziplinäre Einordnung und theoretischen Hintergründe der Verortung unseres Themas. Die gewählte Vorgehensweise dieser Arbeit und Betrachtung von Praktiken innerhalb der Organisation durch ethnographische Methodik werden anschließend ausgeführt. Ferner wird ein Überblick über den Forschungsstand gegeben. Der (2) zweite Themenblock ist mit Digitalisierung, Risiko und Organisation überschrieben und behandelt im dritten Kapitel zunächst die elementaren Veränderungen durch die Digitalisierung und verdeutlicht die Chancen, aber auch Risiken dieser neuen Technologien für Unternehmen. Dadurch sollen die sicherheitsrelevanten Herausforderungen herausgearbeitet werden, um auf dieser Grundlage im vierten Kapitel auf die Logik des unternehmerischen Risikomanagements einzugehen. Auch diese unterliegt durch die Digitalisierung einer Veränderung (Petersen 2017: 119) und bedarf einer genaueren Einordnung zur Bewältigung von Sicherheitsherausforderungen im unternehmerischen Kontext. Gleiches gilt für die Strukturen und den Aufbau von Unternehmen und ihrer Beschaffenheit als Organisationen, welche ebenfalls in diesem Kapitel in der theoretischen Betrachtung der Risikosoziologie und einem Rückgriff auf Niklas Luhmanns Organisationsanalyse den konzeptionellen Rahmen des Beobachtungsobjekts in dieser Arbeit beschreiben (Luhmann 1984; 1991; 2000).

[31] Die detaillierte Schilderung der ethnographischen Betrachtung sowie der Datenanalyse finden sich im zweiten Kapitel und beleuchten die Möglichkeiten, Vorgehensweise und Herausforderungen dieser Methode.

[32] Die Vernetzung von Systemen, Anwendungen, Datenbanken und Drittsystemen in Zusammenarbeit mit selbstlernenden Programmen erschaffen eine Komplexität und Eigendynamik von IT-Netzwerken, welche von Schadprogrammen ausgenutzt werden können, um versteckte Aktivitäten durchzuführen (Huber et. al. 2009: 122). Zusätzlich schafft die Vernetzung zwischen Systemkomponenten die Möglichkeit den Umfang eines Angriffes zu skalieren und Grenzen zwischen Systemen zu überwinden (Gaycken und Karger 2011). Dies wird im sechsten Kapitel im Detail erläutert werden.

Das Spannungsverhältnis zwischen Risikoexposition und Risikokontrolle für Unternehmen im Informationszeitalter wird im (3) dritten Themenblock adressiert. Dazu wird im fünften Kapitel die Methodik des Business Continuity Managements vorgestellt, welches einem Teilaspekt der unternehmensspezifischen Risikokontrolle entspricht.[33] Dieser traditionelle Ansatz der Sicherheitssteuerung entstammt dem analogen Zeitalter und berücksichtigt noch im unzureichenden Umfang die Herausforderungen der Cyberbedrohungen, welche im sechsten Kapitel behandelt werden. Hier liegt der Schwerpunkt auf der Risikoanalyse von Unternehmen unter den Bedingungen der Unsicherheit als Folge der Digitalisierung und in deren Folge auftretenden Bedrohungen. Diese wird im Wesentlichen auf die Bedeutung und den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen bezogen werden. Der (4) vierte und letzte Themenblock thematisiert die Herausforderungen der Implementierung einer resilienten Organisation und zeigt das Zielbild durch den Aufbau eines angemessenen Risikokontrollsystems und den Umgang mit Informationen im Cyberzeitalter auf. Beginnen wir die Untersuchung zunächst mit einer detaillierten Einordnung unserer Fragestellung in die bestehende Terminologie und Literatur.

[33] Gerade in der Methodik des Business Continuity Managements spiegelt sich der Antagonismus aus analoger und digitaler Welt wieder, denn hier werden die Anforderungen der digitalen Zeit deutlich. Die durch die Digitalisierung initiierten Veränderungen der Unternehmensorganisation machen eine grundsätzliche Überarbeitung der Schutzkonzepte notwendig. Darunter steht insbesondere die Fähigkeit von Unternehmen im Mittelpunkt, Prozesse auch trotz der gesteigerten Komplexität und Vernetzung im Fall einer Unterbrechung fortzuführen und kritische Informationen effektiv schützen zu können (Anant, Caso und Schwarz 2020: 2).

2. Verortung und Relevanz des Forschungsthemas

Die Einleitung hat einen ersten Zugang zu den zentralen Fragestellungen und Themen dieser Arbeit eröffnet. In diesem Kapitel soll nun das Vorgehen sowie die Relevanz des Forschungsthemas erläutert werden. Dazu werden im Folgenden zunächst MNU als die im Fokus stehenden Akteure der Sicherheitsproduktion näher betrachtet. Dies umfasst die bisherige Rolle von MNU als private Autoritäten in der IPÖ, sowie die Einordnung von MNU als handelnde Akteure im Feld der Sicherheitsforschung. Dazu wird insbesondere die Unterscheidung der Bereitstellung von Sicherheit durch Unternehmen gegenüber der Maßnahmen von MNU zum Schutz ihrer Organisation, also Sicherheitsproduktion in Unternehmen wichtig sein. Dieses Spannungsfeld wurde während der Corona-Pandemie deutlich und zeigt, dass zwischen den Chancen der Digitalisierung für Unternehmen einerseits und den Risiken durch die intensivierte Vernetzung im Informationszeitalter anderseits spannende Fragestellungen für weitere Forschungsarbeiten entstehen (Lallie et. al. 2020: 15).

Nach dieser Verortung sollen im zweiten Teil dieses Kapitels die angewendeten Methoden und Grundlagen erklärt werden. Wie bereits angedeutet, bietet sich für die Untersuchung der Vorsorgeplanung von Unternehmen eine Einbeziehung von organisationsinternen Praktiken und Entscheidungsprozessen an. Aus diesem Grund werden die theoretischen und methodischen Grundlagen der angewandten Sicherheitsforschung vorgestellt und die Anleihen beziehungsweise Anknüpfungspunkte an vorausgegangen Forschungsinitiativen verdeutlicht werden. Dies nimmt Bezug auf den Bereich der Sicherheitsforschung durch die Kopenhagener Schule (vgl. Buzan, Waever und de Wilde 1998; Wæver 1995) und die Beschreibung diskursiver Praktiken innerhalb von Organisationen durch die Pariser Schule (vgl. Bigo 2000; Bigo und McCluskey 2018; Browning und McDonald 2011). Beide Bezugspunkte und theoretischen Hintergründe werden weiter unten genauer beleuchtet. Den Abschluss dieses Kapitels bildet der Überblick über den Stand der Forschung und wird die verschiedenen, für unsere Fragestellung relevanten Aspekte gruppieren und einordnen. Beginnen wir nun mit dem Blick auf MNU und ihre Reflexion als Akteure in der IB-Literatur.

2.1. Die Rolle privater Autoritäten

Das Interesse an MNU für die Untersuchung in den Internationalen Beziehungen bildete sich ausgehend von ihrer grenzüberschreitenden Aktivitäten und Strukturen heraus, welche auch als Transnationalität bezeichnet werden (Babic, Fichtner und Heemsker 2017: 21). Für die Literatur der IPÖ war im Speziellen der Interessenskonflikt zwischen staatlicher Regulation und privatwirtschaftlicher Gewinnausrichtung relevant (Eden 1991: 199). Dieser Fokus

thematisiert den Gegensatz von Markt und Staat, zwischen Gewinnmaximierung und Kontrolle. Doch neue Impulse, wie beispielsweise von Susan Strange, hinterfragten die etablierten Betrachtungsmodelle und stellten die Einbeziehung von privaten Akteuren in den erweiterten Forschungsrahmen zur Diskussion (Stange 2000). Auch in anderen Bereichen veränderte sich der Blick auf MNU. Die Herausbildung globaler Konglomerate und Marktkonzentration von Unternehmen (Sheth, Uslay und Sisodia 2021: 12) trugen zudem in den vergangenen Dekaden zu Verschiebungen der Machtverhältnisse innerhalb der politischen Ökonomie bei (Babic, Fichtner und Heemsker 2017: 20f.). Der Einzug neuer Technologien, darunter insbesondere der Informationstechnologie, verdrängte das Kapital als originäre und primäre Machtbasis von MNU (Fieldhouse 2000: 174). Ferner waren MNU aufgrund ihrer grenzüberschreitenden Strukturen und Globalisierung der Märkte zunehmend in der Lage, sich der effektiven Kontrolle von Staaten zu entziehen und Möglichkeiten der Finanzierung jenseits des Heimatlandes zu etablieren. Dennoch erschienen MNU in der Literatur der IB unterrepräsentiert, insbesondere mit Blick auf die zunehmende Teilhabe von privaten Akteuren an staatlichen Aufgabenfeldern (Strange 2000: 64).

Susan Stranges Forderung, welche mittlerweile mehr als 20 Jahre zurückliegt, traf auf gemischte Resonanz, aber es zeigte sich seitdem immer mehr die Notwendigkeit zur Einbeziehung des privaten Sektors in die Fragestellungen der IB, um Machtstrukturen und Interdependenzen im globalen Kontext besser verstehen zu können (Babic, Fichtner und Heemsker 2017: 20). Die Delegation von vormals staatlichen Aufgaben in die Verantwortung durch private Unternehmen wurde seitdem in einigen Feldern untersucht. Die Einbeziehung privater Kompetenzen und Ressourcen ist beispielsweise in der Bekämpfung von Geldwäsche und Terrorismusfinanzierung thematisiert worden. Autoren haben die Rolle von MNU bei der Überwachung des grenzüberscheitenden Zahlungsverkehrs und Unterbindung illegaler Finanzbewegungen untersucht, in deren Kontext organisierte Kriminalität (Isolauri, Zettinig und Nummela 2021) oder terroristische Gruppen von Dienstleistungen der MNU ausgeschlossen werden sollten (Kahler 2018). Auch die Forschung zur globalen Korruptionsbekämpfung nahm nun verstärkt private Akteure in den Mittelpunkt der Betrachtung, wie etwa der Umsetzung von Antikorruptionsnormen, bei deren Kontrolle sich das aktive Handeln von MNU als unabdingbar erwies (Heineman und Heimann 2006: 80f.). Als drittes Beispiel kann die Stärkung von Menschenrechten genannt werden, für deren Umsetzung MNU gewichtigen Einfluss, insbesondere in Entwicklungsländern zugesprochen wurde (Majinge 2020: 9).

Das Bild von MNU veränderte sich ebenfalls durch die Arbeitsteilung zwischen staatlicher und privater Sphäre, in dessen Folge der Begriff der privaten Autoritäten entstand (Cutler, Haufler und Porter 1999). Wenn private Akteure staatliche Funktionen übernehmen, entsteht eine Delegation von Autorität, als deren Konsequenz nicht-staatliche Organisationen ihre Befugnisse und Funktionen auf die vorausgegangene Kompetenzübertragung durch staatliche Stellen zurückführen. Dadurch werden diese selbst zu ausführenden Akteuren originär staatlich legitimierter Macht.[34] Dennoch wird die Vorstellung von MNU in den Internationalen Beziehungen den staatlichen Machtstrukturen untergeordnet (vgl. Babic, Fichtner und Heemsker 2017: 21; Goldstein 2010: 492) und eher als ausführender, denn als gestaltender Partner innerhalb der öffentlich-privaten Partnerschaft („public-private partnership“) adressiert (Cavelty und Suter 2009: 2). Dabei zeigte vor allem die ungleiche Verteilung von Eigentümerschaft, Zugriff und Wissen im Zuge der an Bedeutung gewinnenden Informationstechnologie die Problematik dieser Sichtweise (Christensen und Petersen 2017). Diese Konstellation tritt insbesondere im Bereich der Sicherheitsproduktion in Erscheinung, in der MNU eine aktive und gestaltende Rolle in der Kontrolle von Risiken der Digitalisierung wahrnehmen (Huang et. al. 2021: 262), welches im Folgenden aufgezeigt werden soll.

2.2. Unternehmen als Akteure der Sicherheitsproduktion

Zwar waren Unternehmen in der klassischen IB-Forschung bereits als Akteure des internationalen Systems anerkannt, doch erreichte die Rolle von MNU als Akteure der globalen Sicherheitsproduktion erst in den letzten beiden Dekaden größere Aufmerksamkeit. Neben den zahlreichen Faktoren, welche die Entstehung weltumspannender Netzwerke von MNU ermöglichten[35], führte die Privatisierung von sicherheitsrelevanten Aufgabenfeldern, wie beispielsweise in der Telekommunikations- und Finanzbranche zu einer Differenzierung zwischen zwei Verantwortungssphären (Axworthy, 2001: 22). Auf der einen Seite bleibt das staatliche Selbstverständnis zum Schutz der Bevölkerung bestehen, doch ist auf die Kooperation mit Unternehmen aufgrund deren praktischer Verantwortung durch Eigentum und Betrieb der dafür notwendigen Ressourcen angewiesen (Davidshofer, Jeandesboz und Ragazzi 2016: 217).

[34] Diese Entwicklung kann auch als “general trend of globalisation towards privatisation and outsourcing of government functions” bezeichnet werden (Olaniyan 2011: 7).

[35] Die Veränderungen in den Kontrollmöglichkeiten von Handels- und Finanzierungsregeln nationaler Ökonomien durch Staaten in der Nachkriegszeit erlaubten es Unternehmen nach dem Ende des Systems von Bretton Woods ihren Einfluss und Handlungsspielraum im internationalen System aufzuwerten (Babic, Fichtner und Heemsker 2017: 23). Ferner nahm die Bedeutung von MNU als Akteure unter Einbeziehung technologischer Neuerung zur besseren Koordination von Prozessen im globalen Kontext (Strange 2000: 61) und Entbürokratisierung beziehungsweise Privatisierung nach neoliberalem Verständnis (Cavelty und Suter 2009: 2) weiter zu.

Die konkrete Abwehr sicherheitsrelevanter Bedrohungen blieb bis zu den Anschlägen vom 11. September 2001 eine vornehmlich staaten-zentrierte Perspektive (Fekete, Grinda und Norf 2016: 221), doch kamen nun Forschungsbereiche in der IPÖ und IPS hinzu, welche beispielsweise die Rolle von MNU bei der Terrorfinanzierung oder Geldwäsche thematisierten. Auf diesem Feld wurden auf Seiten der staatlichen Autoritäten Regulationsbestimmungen und insbesondere Sanktionsmechanismen gegenüber unerlaubten Finanzaktivitäten erlassen, durch welche vorrangig Finanz- und Versicherungsunternehmen zur Einführung effektiver Kontrollmechanismen verpflichtet wurden (Kahler 2018: 4). Da MNU den Großteil der Finanzströme zwischen ökonomischen Zonen, Organisationen und Privatpersonen durchführen, wäre ohne die Einbindung privater Unternehmen keine flächendeckende Überwachung illegaler Transaktionen möglich gewesen (Babic, Fichtner und Heemsker 2017: 20f.). Auch wenn MNU in diesem Beispiel zur Durchsetzung der neuen Kontrollmaßnahmen durch staatliche Institutionen veranlasst wurden, also auf Anweisung von Staaten handelten, zeigt dies doch die notwendige Einbeziehung der privaten Akteure zur Gestaltung globaler Schutzziele (Hanson 2018: 136). Unter der Voraussetzung geteilter Verantwortung erschien es zunehmend relevant ein neues Rahmenwerk für die staatlich-private Kooperation zum Zweck der Realisierung einer effektiven Sicherheitsdurchsetzung zu entwickeln.

Durch die Digitalisierung wurde die Rolle privatwirtschaftlicher Verantwortung schließlich noch stärker in den Risikodiskurs aufgenommen (Eriksson und Giacomello 2006: 225), da die Perzeption von zunehmenden Bedrohungen und Vulnerabilität der systemrelevanten Technologie im Informationszeitalter die verantwortlichen Akteure im privaten Sektor als sicherheitsrelevant einstufte (Kuerbis und Badiei 2017: 469). Spannende Beispiele dafür sind die Einführung von IT-Sicherheitsstandards für (private) Krankenhausbetreiber (Chigada und Madzinga 2021: 4), welche bereits vor der Corona-Pandemie häufig Ziele von Cyberangriffen wurden. Während der Corona-Pandemie wurde die Vorsorgeplanung von Pharmakonzernen und Impfstofffabrikanten debattiert, deren Risikoexposition gegenüber Cyberangriffen stark angestiegen war (Dochow 2022: 100). Auch Hersteller und Betreiber kritischer Infrastruktur im eher traditionellen Verständnis (vgl. Braubach 2011: 34), wie Stromerzeuger, Telekommunikationsunternehmen oder die Finanzbranche werden vermehrt Ziele dieser Angriffe, deren Erfolg beträchtlichen Schaden für die Versorgungssicherheit der Bevölkerung (Schulze 2021: 2) oder zumindest des Schutzes ihrer vertraulichen Daten haben kann (Lallie et. al. 2020: 3).

Daraus leiten sich neue Fragen für die Sicherheitsforschung ab, unter anderem welche Rolle der Staat im Kampf gegen Cyberbedrohungen übernimmt und ob Unternehmen noch stärker als Akteure und Verantwortliche der Sicherheitsproduktion berücksichtigt werden sollten. Letzteres wird voraussichtlich an Relevanz zunehmen, da im Informationszeitalter nicht nur ein Großteil der benötigten Ressourcen von MNU kontrolliert wird, sie dominieren in binnenlogischer Folge der Plattformökonomie auch ihren jeweiligen Markt und gewinnen signifikanten Einfluss auf das jeweilige Dienstleistungs- und Produktsegment.[36] Zwei Beispiele sollen dies verdeutlichen: Das Unternehmen Google, die vielleicht auffälligste Version des modernen lateralen Konzerns, bedient etwa 90 Prozent aller Internetanfragen und kann mit großer Zuversicht als Monopolist für Suchanfragen gehandelt werden. Auch Facebook, als bekanntestes Unternehmen innerhalb der Meta-Gruppe, kann zwei Drittel des globalen Social-Media-Marktes für sich beanspruchen (Huang et. al. 2021: 627). Ein Ausfall oder Datenabfluss aus einem solchen Unternehmen würde gravierenden Schaden mit globaler Wirkung bedeuten, da MNU wie diese beiden Beispiele im Informationszeitalter nicht nur weitverzweigte Netzwerke unterhalten, sondern auch aufgrund ihrer Marktmacht einen enormen Wirkungskreis für einen großen Teil der Bevölkerung und ihrer sensiblen Daten entfalten.

Insbesondere Technologieunternehmen im Informationszeitalter verfügen aufgrund einiger branchenspezifischer Faktoren über mehr Handlungsspielraum im Spektrum staatlich-privater Partnerschaft. Die Entscheidungen für oder gegen den Einsatz bestimmter Kontrollmechanismen, Technologien oder Schutzmaßnahmen in MNU obliegen dem Risikobewusstsein der Unternehmensführung (Carr 2016: 52). Gleichzeitig erschwert das Wissensmonopol um die verwendeten Systeme und Applikationen einerseits und die multinationale Struktur der Unternehmen über Jurisdiktionsgrenzen hinweg den effektiven Zugriff von Regulationsbehörden (Huang et. al. 2021: 626). Dadurch schließt sich die Frage an, was das für den Schutz kritischer Infrastruktur in Zeiten der Digitalisierung und Abhängigkeit von privaten Betreibern beziehungsweise technologischer Monopolisten bedeutet? Mit Blick auf die Risikodimensionen und Wahrnehmung der Problematik betonen Autoren wie Carr den Interessenskonflikt zwischen privatem und öffentlichen Schutzbedürfnissen: „The language is deliberately cooperative and implies a shared purpose and shared interests (…). It implies that the challenge and the threats are the same for the public and the private sector, when in fact

[36] Das Angebot eines virtuellen Marktplatzes über Plattformen hat Unternehmen wie Amazon, Alibaba oder Facebook zu bedeutenden Akteuren werden lassen. Die Grundidee der Plattformökonomie ist es möglichst viele Nutzer auf der Plattform eines Anbieters mit immer mehr Angeboten zu akkumulieren und somit ein Maximum an Daten generieren zu können. Zudem ist die Ausspielung der dadurch entstehenden Marktmacht ein Problem für den freien Wettbewerb (Haucap 2020: 23).

they are not. The private sector regards cyber-security challenges as financial and reputational - not as a common public good, which is how governments regard national cyber security" (Carr 2016: 55). Diesen Konflikt werden wir weiter unten im fünften Kapitel aufgreifen und detailliert besprechen.

Mit Blick auf die aktuellen Diskurs im Jahr 2022 um eine verteidigungspolitische Strategiewende vor dem Hintergrund hybrider Bedrohungsszenarien im Konflikt mit Staaten wie Russland (Demary 2022: 2) zeigt sich gerade eine weitere Verschiebung in der Bedeutung von privaten Trägern kritischer Infrastruktur.[37] Dies ist insbesondere interessant, als dass Bedrohungen durch Cyberangriffe für die staatliche Souveränität und territoriale Integrität bisher von untergeordneter Rolle für die Debatten in den Internationalen Beziehungen waren (Eriksson und Giacomello 2006; Gomez und Whyte 2021). Daher sollten mit Blick auf MNU als relevante Akteure der Sicherheitsforschung nicht nur den Beitrag zum allgemeinen Schutz kritischer Infrastruktur analysiert werden, sondern auch wie Unternehmen ihre eigene Sicherheit organisieren, dies bedeutet in unserem Kontext vor allem die Strukturen und Maßnahmen innerhalb von Unternehmen. Diese Perspektive wird im folgenden Abschnitt über die Einordnung von MNU in die Sicherheitsforschung Berücksichtigung finden und das methodische Verständnis des weiteren Vorgehens erläutern.

2.3. Einordung in die Sicherheitsforschung

Innerhalb der Sicherheitsliteratur der Internationalen Beziehungen existieren verschiedene Denkrichtungen und Theorien, welche sicherheitsrelevante Fragestellung mit einem jeweils anderen Schwerpunkt analysieren. Unter diesen bietet der Ansatz der „Securization" (Waever 1995) oder zu Deutsch Versicherheitlichung interessante Referenzen für unser Thema. Dieser durch die sogenannte Kopenhagener Schule entwickelte Ansatz bietet verschiedene Anknüpfungspunkte bei dem verwandten Forschungsfeld der Pariser Schule (Bigo 2000), welche mithilfe ethnographischer Methoden die Praktiken und Strukturen von Akteuren der Sicherheitsproduktion untersucht und somit unserer Unterscheidung zwischen Sicherheit durch Unternehmen gegenüber der Bereitstellung von Sicherheit in Unternehmen zuträgt. Aufbauend auf dieser Einordnung werden wir im Folgenden die ethnographische Methodologie weiter

[37] Die Rolle von (privaten) Trägern zur Sicherstellung der Gas- und Energieversorgung ist neben der allgemeinen Abwehr von Cyberangriffen auf Unternehmen in Deutschland durch den Krieg in der Ukraine und der internationalen Sanktionen gegen Russland zum sicherheitsrelevanten Fokus der öffentlichen Diskussion geworden, in dessen Folge der private Sektor in die Planungen staatlicher Akteure einbezogen wird. Die Abwehr von Cyberangriffen zur Sicherstellung der eigenen Funktionsfähigkeit im Fall kritischer Infrastruktur zeigt zudem auch in diesem Konflikt die Bedeutung der Sicherheitsproduktion in Unternehmen (BSI 2022).

erläutern und die Vorgehensweise und Datenerhebung dieser Arbeit vertiefen. Im Folgenden werden beide Schulen vorgestellt und die relevanten Aspekte für unser Thema hervorgehoben.

2.3.1. Versicherheitlichung und Kopenhagener Schule

Die Kopenhagener Schule beziehungsweise die Securization-Theorie ist maßgeblich mit Ole Waever, Barry Buzan und Jaap de Wilde verbunden (Buzan, Waever und de Wilde 1998; Wæver 1995), deren prinzipielles Interesse der Versicherheitlichung durch Sprechakte gilt. Die Publikationen der Kopenhagener Schule wurden als „europäische" Interpretation und Debattenbeitrag zum sozialkonstruktivistischen Diskurs über Sicherheit verstanden (Williams 2003: 511), welcher einen Schwerpunkt auf die Entwicklung nationaler Leitlinien zur Bereitstellung (nationaler) Sicherheit als Folge politischer Kommunikation begreift (Kirk und McDonald 2021: 3). Dazu ist eine legitimierende Formulierung von Sicherheitsimperativen gemeint, welche außerordentliche politische Maßnahmen aufgrund der besonderen Notwendigkeit einer Bedrohung begründen (Eriksson und Giacomello 2006: 234). Die konstruktivistische Leseart[38] politischer Risikokommunikation ermöglicht somit eine kollektive Zustimmung zu exzeptionellen Maßnahmen, die der Eindämmung oder Bekämpfung der Bedrohung dienen sollen (Goldstein 2010: 492).

Die empirische Anwendung der Theorie der Versicherheitlichung kann im Fall des Krieges gegen den Terror beobachtet werden, in denen terroristische Anschläge mit dem semantischen Repertoire der zwischenstaatlichen Kriegsrhetorik beantwortet werden. Einige Autoren sehen hier sogar die inhaltliche Nähe zu strukturellen Regierungspraktiken[39] und strategischen Einflussnahme durch die Artikulation von Bedrohungen wie Terrorismus (Browning und McDonald 2011: 240; Kirk und McDonald 2021: 4), durch welche die Ausnahme zur Normalität wird. Auch hebt der Risikodiskurs in der Deutung der Versicherheitlichungstheorie die Unsicherheit anstelle statistischer Abwägungen in den Mittelpunkt der Folgenabschätzung (Aradau und van Munster 2007: 5). In deren Konsequenz werden die Anwendung von Gewalt, die Einschränkung von Freiheitsrechten oder andere Maßnahmen mit dem Ausnahmezustand begründet, wie beispielsweise nach den Anschlägen vom 11. September 20221 (Blum et. al.

[38] Kritische Einwände thematisierten die zum Teil simplistische Unterscheidung zwischen der politischen Ebene auf der einen Seite und dem öffentlichen Publikum des Sprechakts, beziehungsweise der Einführung von „Sicherheit" als artikulierte Normvorstellung (Browning und McDonald 2011: 242). Ein weiterer Kritikpunkt betrifft die Ausrichtung an theoretischen Beiträgen gegenüber empirischer Arbeit: eine Untersuchung von 171 Publikationen aus dem erweiterten Feld der Securization-Theorie ergab, dass nur 10 Arbeiten empirischer Natur waren (Baele und Jalea 2022: 5).

[39] Die Steuerung von politischen Entscheidungen durch Praktiken der Einflussnahme orientiert sich an Foucaults Theorie der „Governmentality" (Lemke 2000: 4). Risiko wird daher aus post-strukturalistischer Sicht als eine Technik zur gesellschaftlichen Beeinflussung interpretiert (Clapton 2011: 283).

2016: 157). Auch Krankheiten können in den Rang von staatenähnlichen Feindbildern erhoben werden, wie dies im Fall von HIV/Aids oder der Corona-Pandemie zu beobachten war. Mit Bezug auf das Corona-Virus rief der französische Präsident Emanuel Macron 2020 aufgrund der grassierenden Infektionen sogar den Kriegszustand aus (Kirk und McDonald 2021: 8).

Zu beobachten ist, dass der Ansatz der Kopenhagener Schule den Risikodiskurs selbst in den Mittelpunkt stellt und damit Debatten um Risiken nicht anhand ihrer objektiven Messbarkeit, sondern vielmehr im Licht ihrer jeweiligen Wahrnehmung hervorhebt (Clapton 2011: 284). Dadurch können (neue) Themen in den Fokus der Sicherheitsproduktion gelangen oder auch von diesem ausgeschlossen werden.[40] Dieser Akt der Sicherheits- beziehungsweise Unsicherheitskonstruktion erlaubt es somit auch Prozesse zu beschreiben, in denen Akteure als Gegenstand oder Lösung eines Problems in Erscheinung treten (Wentland und Klimburg-Witjes 2021: 182). Als solche können MNU als Akteure der Sicherheitsproduktion aus sicherheitstheoretischer Sicht wahrgenommen und deskriptiv verortet werden. Ebenfalls können Unternehmen als Akteure an der Umsetzung von Maßnahmen beteiligt werden, ihre eigenen Ansprüche und Strategien artikulieren, aber auch Anforderungen seitens der Gesellschaft entgegennehmen und diese zufriedenstellen. Daraus leitet sich die Folgefrage ab, wie MNU diese Einbeziehung als Organisation verstehen, abwägen und in Entscheidungen übersetzen können? Dazu ist eine weitere theoretische Perspektive notwendig, welche mit der Innenperspektive auf Unternehmen und deren praktische, organisationsinterne Umsetzung von Sicherheitsproduktion interessante Einblicke erlaubt. Das soll im folgenden Abschnitt über die Einbeziehung der Pariser Schule in das theoretische Konzept geschehen.

2.3.2. Pariser Schule und die Bedeutung sozialer Praktiken

Wenn man die Frage stellt, wie Unternehmen mit den gestiegenen Erwartungen der Gesellschaft[41] und regulatorischer Anforderungen im Speziellen umgehen, können die Innenperspektiven der internen Entscheidungspraktiken interessante Antworten liefern. Der Blick in die Organisation und Beobachtung ihrer Praktiken kann dazu beitragen relevante Fragen über das Verhalten und die Motivation von MNU bezüglich ihrer Teilhabe in der Sicherheitsproduktion zu beantworten. Dazu zählt beispielsweise, ob MNU die staatlichen Vorgaben als Widerspruch zu ihren eigenen Profitzielen sehen (Carr 2016: 56), oder die

[40] Problematisch ist dies insbesondere, wenn aus der Versicherheitlichung von Themen, zumindest gefühlte Unsicherheit wird: „On the contrary, noticing […] many policemen in the street, people may become aware that something goes wrong and may feel even more insecure“ (Langwald 2021: 4).
[41] Man denke an die gestiegene Bedeutung unternehmerischer gesellschaftlicher Verantwortung (Corporate Social Responsibility) oder der Nachhaltigkeit, deren Einführung im Unternehmenskontext mit den Erwartungen seitens der Öffentlichkeit zusammenhängt (Dolan, Garsten und Rajak 2011: 5).

Risikodiskussion als Option für neue Geschäftsfelder auffassen (Krahmann 2007: 9), oder wiederum unternehmerische Risikovorsorge zur Erhaltung der eigenen Geschäftstätigkeit aus intrinsischer Motivation heraus wahrnehmen (Christensen und Petersen 2017: 1443). Die Pariser Schule beschäftigt sich mit diesen Fragestellungen, deren prominentester Fürsprecher Didier Bigo die enge Beziehung zwischen Kopenhagener und Pariser Schule hervorhebt (Bigo und McCluskey 2018: 117). Allerdings beziehen sich Vertreter des Pariser Ansatzes mehr auf die transformativen Praktiken der Akteure und Abläufe innerhalb von Organisationen, als auf die reine Reaktion der Sicherheitsakteure in Folge artikulierter Bedrohungen (ebd.: 123).

Die Pariser Schule bietet der Sicherheitsforschung ein interessantes Konzept zur Analyse von Mechaniken und Verhaltensmustern von Experten und Praktikern innerhalb der betroffenen Organisationen an und dies mit dem Ziel, vielfältige Anknüpfungspunkte zu anderen Disziplinen der Internationalen Beziehungen zu ermöglichen (Langwald 2021: 1). Ein Problem der Beobachtung von MNU in der IPÖ ist die Ausrichtung auf Kennziffern aus dem unternehmerischen Umfeld. Informationen über Unternehmen werden bevorzugt den jeweiligen Jahresberichten und Beiträgen der Unternehmenskommunikation entnommen (Fieldhouse 2000:174) oder durch externe Beobachtungen von Handlungen gewonnen. Die Motivation, Entscheidungsgrundlage oder potentielle Konflikte zwischen Machtstrukturen innerhalb von MNU werden dabei kaum berücksichtigt. Die Pariser Schule bietet daher eine erweiterte Perspektive durch ethnographische Methoden zur Beobachtung von handelnden Akteuren innerhalb der Organisation an.

In unserem Fall kann die ethnographische Dokumentation dabei helfen zugrundliegende Muster und Entscheidungsprozesse zu erforschen und Auffassungen von Sicherheit sowie deren Auswirkungen auf lokaler und globaler Ebene zu verstehen (Goldstein 2010: 499). Die Aufdeckung von Beziehungen und sozialen Praktiken innerhalb von Organisationen dient daher dem Zweck, die internen Logiken mit Blick auf den Umgang mit Unsicherheit zu erkunden (Handson 2018: 136). Insbesondere die Untersuchung der Umwandlung von sozialen Praktiken in alltägliche Routine oder die Überführung von Entscheidungen in strukturelle Normen (Langwald 2021: 5) können der Untersuchung von Sicherheitsproduktion innerhalb von Unternehmen zuträglich sein. Ethnographie als wissenschaftliche Methode versucht dabei die „black box“ der auf Vertraulichkeit und Außenwirkung bedachten privaten Unternehmen zu öffnen und das „intimate knowledge of situated actors and objects“ hervorzubringen, sowie Mechanismen zu identifizieren, welche das Verhalten der Organisation bestimmen (Ciuk, Koning und Kostera 2018: 271).

2.4. Methodische Grundlagen und Vorgehen

Die Ursprünge der Pariser Schule und die angewendeten Organisationsethnographie erkennen zwar die Bedeutung und Interkonnektivität von internen und externen Akteuren der Sicherheitsproduktion an (Langwald 2021: 3), allerdings versteht sich der Schwerpunkt von Bigos Betrachtung als Analyse staatlicher Institutionen wie Polizei oder Militär. Dadurch entsteht eine Forschungslücke mit Blick auf die intraorganisationale Verantwortung des privaten Sektors für die interne Sicherheitsproduktion und dessen Beitrag zur gesamtgesellschaftlichen Daseinserhaltung. Der Beitrag dieser Arbeit richtet sich folglich an die Untersuchung eben jenes weißen Flecks in der Sicherheitsliteratur und wendet die Methodik der beobachtenden Teilnahme[42] am Entstehungsprozess der Sicherheitsproduktion innerhalb von MNU an. Dadurch soll ein Anschluss an die bestehenden Erkenntnisse der Sicherheitsforschung in den internationalen Beziehungen geknüpft werden und die Zusammenhänge, Praktiken und Auswirkungen im Rahmen des unternehmerischen Sicherheitsbeitrages aufgezeigt werden.

2.4.1. Ethnographische Untersuchung

Die Beobachtung mittels ethnografischer Methoden setzt einige Grundannahmen voraus. Dazu zählt der Zugang zu Informationen und Akteuren, in diesem Fall Experten aus sicherheitsrelevanten Bereichen der Privatwirtschaft. Dies macht gegenseitiges Vertrauen zur Vorbedingung, sowie einen längeren Beobachtungszeitraum notwendig, um strukturelle Entwicklungen von Momentaufnahmen differenzieren zu können (Ciuk, Koning und Kostera 2018: 271). Des Weiteren sind Fragen der Einmischung und Inklusion in den Beobachtungsgegenstand nicht zu vernachlässigen, durch welche die Beobachtung bereits einem Prozess der bewussten und unbewussten Selektion unterworfen ist (Knoblauch 2001: 130). Die Methoden der ethnographischen Datenerhebung setzen im Fall unserer Fragestellung die Einbindung des Beobachters in die Lebens-, oder in diesem Fall besser gesagt, Arbeitswelt von Akteuren der unternehmerischen Sicherheitsproduktion voraus. Diese Beobachtung ersten Grades betrifft mit den Worten Luhmanns die „reale Welt“ von Sicherheitsexperten, welche in Konkurrenz und Ermangelung vollständiger Informationen Entscheidungen zu treffen haben und in Abgrenzung zur zweiten Beobachtungsebene, durch die Interpretation der direkt beteiligten Personen sowie ohne deren zwingende Kenntnisnahme seinen Deutungsgehalt modifizieren können (Luhmann 1991: 30f.).

[42] Dieser Begriff wird im nächsten Abschnitt weiter ausgeführt und beschreibt die aktive Teilhabe an internen sozialen Praktiken zur ethnographischen Erforschung von Organisationen (Hitzler und Gothe 2015).

Übertragen auf unsere Kernfrage bezieht sich die ethnographische Untersuchung daher auf die Rezeption von Ereignissen und den Umgang mit Unsicherheit aus der Perspektive von Entscheidungsträgern und Experten im Unternehmensumfeld. Beide Gruppen müssen nicht zwangsläufig identisch sein, da die Genese und Weiterentwicklung von operativen Sicherheitsangelegenheiten hin zu einer holistischen Sicherheitsarchitektur oder einem strategischen Rahmenwerk für die Sicherheitsproduktion den Kreis der Betroffenen und Entscheidungsträger verändert hat, dennoch aber das Zusammenwirken von Expertise und Mandat erforderlich macht (Liebermann 2015).[43] Als Werkzeug zur Analyse der Risikomitigation bietet sich daher im Anschluss an die Sicherheitsliteratur der Pariser Schule die Ethnographie an, um den Handlungsrahmen von Akteuren und Sinnzusammenhänge (deskriptiv) zu erfahren und geeignete Schlussfolgerungen durch Hintergrundgespräche, Beobachtung und deren Auswertung zu ziehen.

Die Perspektive auf die internen Prozeduren und Praktiken setzt eine integrierte, das bedeutet in das Geschehen involvierte Beobachtung voraus (Hitzler 2000: 17), deren übergeordnetes Forschungskonzept die Interdependenzen und Herausforderungen der Organisation im Umgang mit Risiken und insbesondere, wie in unserem Fall den Veränderungen der Sicherheitsanforderungen durch den Einsatz von Technologien reflektiert. Die Methoden und Datenquellen der ethnographischen Arbeit beziehen sich im Allgemeinen auf die Auswertung von Dokumenten und Gesprächen, um den bestmöglichen Überblick sowie Vollständigkeit des beobachtenden Geschehens erarbeiten zu können (vgl. Deppermann 2000: 103). Beachtet man zudem die dem privaten Sektor im Allgemeinen inhärente Relevanz von Vertraulichkeit und Exklusivität von Erfahrungen und Wissen, bietet ein Ansatz der beobachtenden Teilnahme Vorteile für das geplante Vorgehen (Hitzler und Gothe 2015: 9).[44]

An dieser Stelle sollen zwei Beispiele für die beobachtende Teilnahme vorgestellt werden, die für unsere Vorgehensweise als Vorlage dienten, um die Sicherheitsproduktion in Unternehmen aus der Perspektive von Praktikern zu beobachten. Ein bekanntes Beispiel in dieser Hinsicht ist die Forschungsarbeit von Horacio Ortiz, der sich zum Investmentmanager ausbilden ließ, um

[43] Budgetrelevante Entscheidungskompetenz und operative Erfahrung im Umgang mit sicherheitsspezifischen Risiken sind zumeist auf unterschiedlichen Ebenen der Organisation angesiedelt. Die ideale Rolle eines Sicherheitsexperten in Organisationen hängt von mehreren Faktoren ab, unter anderem der (disziplinarischen) Entfernung zum oberen Führungskreis (Shaw 2004), aber auch von der Interaktion und interner Akzeptanz durch andere Akteure im Unternehmen, deren Fokus auf der operativen Steuerung des Geschäfts liegen kann.

[44] Eine relevante Unterscheidung betrifft die Begriffe der teilnehmenden Beobachtung und der beobachtenden Teilnahme. Ersteres beschreibt eine Untersuchungsmethode mit Schwerpunkt auf die Beobachtung als inkludierter Teil der zu analysierenden Organisation. Die zweite Form thematisiert hingegen die Beobachtung als Bestandteil der Teilnahme und damit eine intensivere Variante der Organisationsinklusion (Hitzler und Gothe 2015: 11).

als Mitarbeiter in einem Vermögensveraltungsunternehmen die Entscheidungsprozesse und Praktiken eines von außen schwer zugänglichen Forschungsobjekts nachzuzeichnen. Ortiz absolvierte unter anderem zwischen 2002 und 2004 drei Praktika in Paris und New York und beobachte die für Außenstehende kaum einsehbaren Abläufe und Routinen der dort angestellten Börsenmakler und Vermögensverwalter bei ihrer Arbeit, unterstützt durch begleitende Interviews (Ortiz 2013: 66). In der sprachlich und verhaltensangepassten Rolle eines informierten Beobachters konnte er sich den sozialen Praktiken des Finanzsektors von Innen annähern und durch die Einbindung in Tagesabläufe die Hintergründe und Rationalitäten erforschen. Durch die beobachtende Teilnahme an den internen Prozessen der Vermögensverwaltung war es dem Beobachter möglich, die Übersetzung und Anwendung von theoretischen Modellen, wie beispielsweise den Annahmen zur effizienten Marktstruktur aus der Finanzökonomie, mit den Praktiken der Experten in dieser Branche in Verbindung zu setzen (Ortiz 2009: 34). In den folgenden Jahren konnte Ortiz seine Feldarbeit zudem dazu nutzen, um weitere aufschlussreiche Erkenntnisse wie zum Beispiel über die Rolle von Moral und finanzieller Wertschöpfung (Ortiz 2013) oder der anthropologischen Beschreibung von Verhaltensweisen und Entscheidungsstrukturen innerhalb der Finanzindustrie aufzuzeigen (Ortiz 2021).

Als zweites Beispiel kann hier Douglas Holmes angeführt werden, der sich mit Bezug auf die ethnographische Betrachtung von geschlossen Gruppen mit der Problematik auseinandersetzte, Zugang zu geschlossenen Gemeinschaften zu finden und wertstiftende Schlussfolgerungen aus der Beobachtung zu ziehen (Holmes und Marcus 2012: 127). Douglas untersuchte beispielsweise mithilfe ethnographischer Methoden die Sprache und Suggestion neofaschistischer Bewegungen in Europa und die Rezeption in milieuspezifischen Gruppen der Wählerschaft, um die Aufnahme von Informationen und Umsetzung in Praktiken innerhalb dieser Gruppen aufzuzeigen (Douglas 2009: 52). Mit Blick auf die Nutzung von (experimenteller) Sprache, zeigte Douglas die diskursiven Kommunikationstechniken von Zentralbanken, welche sich aus Mitschriften und veröffentlichten Kommunikationsbausteinen zusammensetzen (Douglas 2019: 9). Durch eine ethnographische Beobachtung der Praktiken innerhalb der Europäischen Zentralbank in Frankfurt konnte Douglas zudem die Kommunikation von Zentralbankmitarbeitern untersuchen und aufzeigen, wie deren Sprachgebrauch im Rahmen der Währungspolitik die europäische Integrität beeinflusste (Douglas 2009: 63). Ferner war es möglich durch die Beobachtungen aufzuschlüsseln, wie bürokratische Traditionen und Praktiken die Gestaltung von Regeln und Regulation der Zentralbank beeinflussen (ebd.: 66).

Durch diese Beispiele zeigen sich die Möglichkeiten, als Praktiker mithilfe der beobachtenden Teilnahme Einsicht in Rationalitäten und Praktiken in nach außen geschlossen Gruppen zu nehmen. Die Teilnahme und Einbindung durch die von den Gruppenmitgliedern als Praktiker wahrgenommen Funktion unterstützen dabei den Zugang zu Informationen und ungefilterten Einsichten in die Routinen und Rationalitäten der Experten in Unternehmen. Allerdings setzt dies auch Reflektionen und kritische Auseinandersetzung mit dem zu Beobachtenden einerseits und der eigenen Teilnahme beziehungsweise Einflussnahme andererseits voraus. Die Rolle als teilnehmender, also inkludierter Beobachter ermöglicht tiefergehende Einblicke und beruht neben regelmäßiger Interaktionen auf beständiger Reflektion des zu Beobachteten (Hitzler 2000: 23f.). Ein weiterer Aspekt betrifft auch die Möglichkeit konkrete Handlungsempfehlungen auf der Grundlage der vorausgegangenen problemfeld-nahen Beobachtung zu entwickeln (Ciuk, Koning und Kostera 2018: 275).

Im Kontext unseres Themas bezieht dies neben der inhaltlichen Einarbeitung in die Anforderungen unternehmensinterner Sicherheitsproduktion auch die aktive (teilnehmende) Einbindung in die ausführenden Einheiten sicherheitsrelevanter Praktiken mit ein. Die Vertraulichkeit in diesem Kreis und die inhärente Skepsis gegenüber öffentlicher Zitierung stellen allerdings Herausforderungen an die notwendigerweise vorausgehende Vertrauensbildung. Zu diesem Zweck wurden auch solche informellen Gespräche und Erkenntnisse aus Dokumentenquellen in die Beobachtung mit einbezogen, welche nicht freigegeben wurden, das heißt nur in abstrakter, anonymisierter Form rezitiert werden können, aber dennoch aufschlussreichen Einblick geben. Die konkreten Rahmenbedingungen der Datenerhebung sollen im folgenden Abschnitt thematisiert und eingeordnet werden, bevor auf den Forschungsstand und die Literaturgrundlage eingegangen werden wird.

2.4.2. Datenerhebung

Dieser Abschnitt wird die zugrundeliegende Datenerhebung mittels ethnographischer Methoden, vor allem der teilnehmenden Beobachtung darlegen und dabei die zeitliche Abfolge, den Umfang der untersuchten Objekte, den Aufbau von Vertraulichkeit sowie die eigene Reflektion über Positionalität und Herausforderungen umfassen. Generell stellte sich die Frage, wie es gelingen kann Unternehmen als Untersuchungsobjekte zu betrachten, vor allem aber zugänglich zu machen. Wie sich im Rahmen dieser Arbeit herausstellte, kann die zuvor skizzierte Bedeutung von Vertraulichkeit auf Unternehmensseite dabei kaum überschätzt werden. Auch von „Außen“ erscheinen MNU als verschlossene Gebilde mit starker Abgrenzung ihrer Kommunikation und Mitgliedschaft gegenüber ihrer Umwelt (vgl. Luhmann

2000: 86ff.), wie wir es auch im vierten Kapitel über die Risiko- und Organisationssoziologie besprechen werden. Die unternehmensinternen Vorgänge und Prozesse treten dem externen Betrachter zumeist nur als Endprodukt der Entscheidung und in Form der nach außen gerichteten Kommunikation in Erscheinung („black box“) und fanden bisher nur in unterrepräsentierter Form Beachtung (Ouma: 2012: 201). Daher sollen hier der gewählte Zugang, die Länge und Art der Teilhabe im Folgenden dargestellt werden.

2.4.2.1. Kapazität, Zeitrahmen und Rolle

Im Rückblick erzählen der Entwicklungsprozess und die Datenerhebung dieser Arbeit eine solche Geschichte der Vertrauensbildung und Zugangsfindung in ein nach Außen abgegrenztes System. Während der beginnenden Konkretisierung des Forschungsthemas blieben viele Anfragen und Ansprachen an MNU unbeantwortet oder nicht zielführend. Die eigene Beobachtung der initialen Korrespondenz war vom tendenziellen Desinteresse der Adressaten an wissenschaftlicher Beschäftigung mit dem Thema der unternehmerischen Vorsorgeplanung gezeichnet. Auf Seiten der Unternehmen, so die Vermutung, erzeugten eingehende Anfragen zu sensiblen Unternehmensinformationen durch einen der Organisation Außenstehenden Skepsis. Um relevante Informationen über die Prozesse innerhalb von Unternehmen in Erfahrung zu bringen, waren eine dauerhafte Teilnahme an den alltäglichen Praktiken notwendig, welche eine ethnographische Beobachtung anbieten würde (Genz und Tschoepe 2021: 230). Dazu war der Zugang zu Unternehmen als Mitglied der Organisation eine entscheidende Voraussetzung, um Glaubwürdigkeit, Inklusion und nicht zuletzt Vertraulichkeit[45] aufzubauen. Das Erlernen der Praktiken, Teilnahme (und auch spätere Teilhabe) an Entscheidungsprozessen sowie ein generelles Verständnis der Fachterminologie über eine Unternehmenszugehörigkeit eröffneten schließlich Einsicht in die inneren Prozesse der Sicherheitsproduktion im Unternehmen.

Der Zugangspunkt zur unternehmensinternen Perspektive erfolgte über einen Doktorandenvertrag über drei Jahre, der zwischen 2012 und 2015 die Möglichkeit eröffnete, zu siebzig Prozent als Teil der mit der Kontinuitätsplanung beauftragten Abteilung eines im DAX-30 gelisteten Unternehmens zu arbeiten. Die verbleibende Zeit war für Literaturrecherche, Hintergrundgespräche und weitere wissenschaftliche Aspekte wie der Dokumentation und Ablage von Informationen reserviert. Während dieser Zeit ermöglichte der Zugang zu regelmäßigen Terminen der Abteilung (Jour-Fixes) und aufgabenbezogenen Interaktionen mit

[45] Vertrauen und Vertraulichkeit werden wir in einem gesonderten Abschnitt innerhalb der Sektion Datenerhebung genauer beleuchten.

den 14 Mitarbeitern den Zugang zu alltäglichen Problem- und Lösungsdiskursen, deren Inhalt verschiedene Aspekte der Herausforderungen bezüglich Resilienz thematisierte. Über die Mitarbeit an Schriftstücken, Leitlinien und Audits anderer Unternehmensbereiche entstand dadurch nicht nur ein wichtiger Einstieg in die Materie, sondern auch ein wachsendes Bewusstsein auf beobachtender Seite für die Komplexität, Dynamik und vor allem Vielseitigkeit der Herausforderungen eines MNU im Wandel durch die Digitalisierung und globalen Interdependenzen.

Im Anschluss an die Doktorandenstelle ermöglichte ein Stellenangebot als „Business Continuity Manager“[46] in der Unternehmenszentrale die Beobachtung aus der Rolle aktiver Teilnahme heraus fortzusetzen. Im Unterschied zur teilnehmenden Beobachtung, war diese Vollzeitstelle vorrangig auf die aktive Gestaltung der Vorsorgeplanung in Form der Implementierung von Business Continuity Management ausgerichtet, bot jedoch vielfältige Einblicke in die strategische Verortung und Implementierung des Themas. In dieser Position war es möglich die tägliche Arbeit in der globalen Steuerung von BCM-Konzepten in einer Gruppe aus vier BCM-Verantwortlichen für das Unternehmen zu verfolgen. Die Position verschaffte zudem stärker Einblicke in die Alltagswelt von Suborganisationseinheiten in der Peripherie der Unternehmensgruppe, die durch ihre eher dezentrale Struktur diesen Landesgesellschaften Freiraum zur Risikomitigation erlaubte und damit die Frage nach Sicherheitsproduktion in Unternehmen um eine Vielzahl an alternativen Herangehensweise an (lokale) Herausforderungen auf dem Feld der Anwendungspraktiken wie BCM ermöglichte.

Im Rahmen dieser Kooperation wurde der Kontakt zu mehr als sechzig Verantwortlichen in Landesgesellschaften ermöglicht, welche einen wesentlichen Beitrag zur Erkenntnisfindung und Differenzierung der Problematiken und individuellen Lösungen für lokale Herausforderungen in rechtlicher, (unternehmens-)kultureller und operationeller Hinsicht. Auch wurde der Zugang zu anderen DAX-30 gelisteten MNU durch die Funktion und Autorität als Mitglied einer vergleichbaren Organisation im Rahmen von Konferenzen, direkten Interaktionen auf Expertenebene und Hintergrundgesprächen erleichtert. Dadurch konnten Einblicke in die informellen Abläufe und Entscheidungsprozesse dieser Unternehmen gewonnen werden. Ab 2017 wurde dieser Zugang durch eine neue Funktion als „Inhouse Consultant“ auf der Grundlage einer Berater-Kunden Beziehung um weitere Aspekte erweitert. Als projektbezogener (temporärer) Teil der lokalen Organisation entstanden neue

[46] Business Continuity Management wird im folgenden fünften Kapitel vertieft und bildete gemeinsam mit der Domäne des Krisenmanagements den Nukleus Risikokontrolle im analogen Zeitalter.

Opportunitäten, um Vertrauensaufbau zu betreiben und statt der Unternehmenszentrale nun die Perspektive der ausführenden Entitäten einzunehmen.

Gegenüber der zuvor ausgefüllten Funktion als Koordinator im Stammsitz teilten in der neuen Rolle Praktiker aus den Landesgesellschaften merklich andere Informationen, da man sich als Teil der gemeinsamen Unternehmung empfand und Vertrauen im Erreichen desselben Ziels aufbaute. In diese Zeit fielen vor allem neue Herausforderungen wie die Bewältigung der Corona-Pandemie seit Ende 2019 und das Krisenmanagement im Rahmen des Krieges in der Ukraine mit Blick auf die Gas- und Energieversorgung in der EU. Zu diesem Zweck wurden etwa 30 vertrauliche Hintergrundgespräche mit Verantwortlichen aus den Bereichen BCM und Krisenmanagement beziehungsweise IT-Infrastruktur durchgeführt. Zeitgleich veränderte sich während dieses Beobachtungszeitraums der Schwerpunkt der Forschungsfrage vom allgemeinen risikosoziologischen Blick auf die Rolle von Informationstechnologie und ihrer Verwundbarkeit im Kontext unternehmensinterner Sicherheitsproduktion, deren Auswirkungen auf die gesellschaftlichen Strukturen. Dieses Motiv wurde auch immer mehr als Tenor in internen Diskussionen während der Beobachtung wahrgenommen. In beiden Funktionen war seit 2015 die Kapazität für dezidierte Forschung den Aufgabenanforderungen der Stellenbeschreibung als Unternehmensmitarbeiter untergeordnet, wurde aber regelmäßig strukturiert durchgeführt. Die Beobachtung erstreckte sich schließlich über die Verschriftlichung der Doktorarbeit hinaus bis zum August 2022, aus dem die letzten Beobachtungen für diese Arbeit stammen.

2.4.2.2. Dokumentation der Beobachtungen

Die Art, Frequenz und Niederschrift der Beobachtungen sind über den Beobachtungszeitraum hinweg durch ihre unterschiedliche Natur und jeweiligen Schwerpunktsetzung gekennzeichnet. Die erste Phase im Rahmen des Doktorandenstatus umfasste Annäherungs- und Strukturierungsaktivitäten. Der Fokus galt hier dem grundsätzlichen Verständnis der Unternehmensstrukturen und der (zu diesem Zeitpunkt) vorherrschenden Vorgaben für unternehmensinterne Risikovorsorge. Diese Informationen wurden in Form von Strategiepapieren, branchentypischen „Best Practises“ und Hintergrundgesprächen, sowie vor allem durch die Beobachtung und Teilnahme an internen Arbeitsgruppen, Fachgesprächen und Abstimmungsrunden gesammelt. Mithilfe von standardisierten Fragebögen zur personellen und technischen Ausstattung der Ländergesellschaften und lokal unterschiedliche Relevanz von Krisenszenarien wurden die Grundlagen für das Verständnis der internen Ressourcenverteilung und Risikovorsorge dokumentiert. Die daraus folgende initiale Beschreibung der

unternehmensinternen Organisationsstruktur von MNU und die Einordnung der Handlungsfelder des Risikomanagement, Business Continuity Management und Krisenmanagement in einen übergreifenden Rahmenwerk ermöglichten einen Zugang zur praktischen Gestaltung und Ausformung von Risikokontrolle in Unternehmen.

Der Zugang und selbstmotivierte Beitrag zur Gestaltung dieser strategischen Einordnung in das Unternehmen wurden in der zweiten Phase durch die Rolle als BCM Manager und die damit einhergehende Aufwertung im unternehmensinternen Hierarchiemodell ausgeweitet. Ferner ermöglichte die während der ersten Phase gewonnene Akzeptanz, insbesondere über die Grenzen der eigenen Funktionseinheit hinaus, einen anderen Zugang zu beteiligten Personengruppen aus Fachabteilungen wie beispielsweise Risikomanagement, Compliance, Regulatory Affairs oder IT Governance. Unter den beobachteten und dokumentierten Erfahrungen sind Memos über alltägliche und kontinuierliche Muster und Handlungsroutinen zu verzeichnen. Ferner wurden Projektumgebungen und Richtungsentscheidungen mit Relevanz zur Forschungsfrage als Tagesnotiz festgehalten, auf deren Grundlagen neben den sich wiederholenden Mustern des Alltäglichen auch die strategischen Entwicklungen und Entscheidungen des Unternehmens beobachtet wurden. Neben den regelmäßigen Interaktionen wurden gezielte, vertrauliche Hintergrundgespräche mit Experten aus den Bereichen Business Continuity Management, Krisenmanagement und Information Security geführt.

Die dritte Phase war von einer Positionsverschiebung gekennzeichnet, da nun vermehrt andere Organisationsbereiche in den Fokus der Beobachtung und alltäglichen Interaktion traten. Neben dem Austausch über virtuelle Interaktionsmedien, waren vor allem Reisen und persönliche Begegnungen ausschlaggebend für eine vertrauensvolle Zusammenarbeit und Einblick in informelle Prozesse und Entscheidungsgrundlagen vor Ort. In dieser Zeit wurden mit mehr als vierzig Standorten zahlreiche physische Orte der internen Sicherheitsproduktion des Unternehmens und seiner Landesgesellschaften besucht und manche Entitäten darüber hinaus regelmäßig frequentiert. Wie die Darlegung im fünften und sechsten Kapitel zeigen wird, ergaben sich daraus aufschlussreiche Beobachtungen über die Unterschiedlichkeit von lokalen und regionalen Herausforderungen beziehungsweise kulturelle Besonderheiten innerhalb der globalen Organisation in der Bereitstellung von Sicherheit durch Maßnahmen in den jeweiligen Entitäten. Ebenfalls fiel in diese Phase die fortschreitende Schwerpunktverschiebung auf die Rolle der Informationstechnologie und die Beobachtung der unternehmensweiten Chancen und Herausforderungen durch die Einführung neuer Technologien. Im Rahmen der dritten Phase wurden zudem strukturierte Fragebögen zur lokalen Mitigation der Corona-Pandemie im Jahr

2020 und der Risikoeinschätzung einer möglichen Energiekrise in Folge des Ukrainekrieges im Jahr 2022 durchgeführt. Die Ergebnisse wurden als Studien aggregiert und durch Experteninterviews im Rahmen der projektbezogenen Tätigkeit validiert beziehungsweise ergänzt.

Übergreifend für das hier gewählte Vorgehen kann festgehalten werden, dass die Grundlage des Verständnisses über sowohl die Unternehmensstruktur und Prozesse einerseits, als auch über die technischen Aspekte und Praktiken andererseits durch eine Literaturrecherche und Auswertung interner Dokumente gelegt wurde. Darauf aufbauend wurden branchenspezifische Industriestandards und detaillierte Fachliteratur einbezogen, über deren Stand im später folgenden allgemeinen Überblick über die Literatur ausgiebig gesprochen werden wird. Mit Bezug auf die durchgeführte Datenerhebung im Rahmen der ethnographischen Beobachtung sind darüber hinaus die Bedeutung von informellen Expertengesprächen hervorzuheben, durch deren Konkretisierung der sich verändernden Herausforderungen über die Länge des Analysezeitraums klare Ableitungen für die Thesenentwicklung und Bearbeitung unserer Fragestellung ermittelt werden konnten.

Es ist wichtig mit Blick auf die strukturierte Datenerhebung hervorzuheben, dass die Beobachtung der Sicherheitsproduktion im Unternehmen aus der Rolle eines Praktikers ähnlich zum zuvor beschriebenen Fall von Horacio Ortiz durchgeführt wurde und über einen mehrjährigen Zeitraum aus unterschiedlichen Positionen und Blickwinkeln erfolgte. Dadurch ergaben sich einzigartige Einblicke in die inneren Entscheidungsmuster und Rationalitäten, welche in den folgenden Kapiteln dargestellt werden und auch zur normativen Schlussfolgerung in der Umsetzung einer resilienten Organisation führte. Daher wurde diese Arbeit im Bewusstsein einer beobachtenden Teilnahme als Praktiker verfasst und reflektiert diesen Umstand in der Ergebnisfindung. Mit Blick auf die erhobenen Daten und deren strukturierte Dokumentation ergibt sich aus dem beschriebenen Entstehungsprozess dieser Arbeit allerding die Einschränkung, dass die Möglichkeit zur Einsichtnahme und Teilnahme an Gesprächen durchgehend an Vertraulichkeit gebunden war und daher eine wörtliche Wiedergabe oder konkrete Referenz zu einzelnen Individuen oder Gesprächen ausschließt. Dieser Aspekt wird im nachfolgenden Abschnitt zur Inklusion und Reflexion detaillierter angesprochen werden.

2.4.2.3. Inklusion und Reflexion

Ein besonderer Aspekt der Involvierung in geschlossene Gruppen zur Durchführung ethnographischer Untersuchungen ist, dass insbesondere im Kontext von MNU eine Phase der

Vertrauensbildung unerlässlich ist, um als Teil der Gruppe und letztlich der Organisation akzeptiert zu werden. Das betrifft sowohl Aufwände an die Vertrauensbildung durch langfristige Interaktion, professioneller Distanz bei zeitgleicher Teilhabe an alltäglichen Routinen, als auch die Zusicherung von Vertraulichkeit. Dabei ist Zeit ein relevanter Faktor, über den in diesem Fall Vertrauen aufgebaut wurde, während Vertraulichkeit die Kontinuität der Kollaboration absicherte. In diesem Kontext sind regelmäßige Interaktionen, die Verwendung der gleichen Terminologie, aber auch das Erleben gemeinsam bestandener Herausforderungen wesentliche Elemente der Inklusion in die Organisation gewesen. Die Beobachtung von Praktiken und Verhaltensmuster folgte dabei einer schrittweisen Assimilation in die zugeordnete Fachabteilung. Dies hatte auch Auswirkungen auf die Perspektive des Beobachters auf Kommentare, Handlungen oder Eskalationen seitens anderer Unternehmensfunktionen, deren Handlungsmotivation tendenziell und mit fortschreitender Zeit vermehrt aus Sicht der eigenen Mitglieder und Arbeitsumgebung interpretiert wurde.

Diese nicht unübliche Herausforderungen ist Teil der Involvierung von Beobachtern in ihre Forschungsumgebung, da Interaktionen und geteilte Erfahrungen nicht nur eine Verbindung zwischen Beobachter und Beobachtetem erzeugen, sondern auch Fragen mit Blick auf die Selbstreflektion aufwerfen (Genz und Tschoepe 2021: 231). Auch Luhmann sprach mit Blick auf die Beobachtung von Sicherheitsexperten von verschiedenen Ebenen und Interdependenzen, welche beide durch die Handlung oder durch die Beobachtung den Prozess beeinflussen und Auswirkungen auf die zu ziehenden Schlussfolgerungen haben können (Luhmann 1991: 29), wodurch eine kritische Reflexion über Interpretationen geboten ist. Dieser Eindruck wurde im Fall dieser Arbeit noch vermehrt, als dass die Beobachtung nicht immer als solche in Erscheinung trat, schließlich sind Sicherheitsexperten – zumindest nach der Erfahrung der zurückliegenden Beobachtung - nur ungern wissentlich Gegenstand einer Kontemplation. Daher stellt sich einerseits die Frage nach der eigenen Positionalität als Teilnehmender und Beobachter zugleich, aber auch andererseits nach der Reflexion über die Beobachtung als langfristig intervenierende Handlung.

Mit Blick auf die Positionalität der Beobachtung ergeben sich aus einem längeren Betrachtungszeitraum wie in unserem Fall auf der einen Seite eine langfristige Möglichkeit die Zusammenhänge und Perspektiven auf das zu Beobachtende strukturiert und durch intensive Einbindung detailliert zu studieren. Auf der anderen Seite bringt es auch Herausforderungen mit sich, durch die zeitliche Ausdehnung die Grenzziehung zwischen Beobachtung und eigener Handlung zu ziehen (Ouma: 2012: 26). Mit Blick auf diese Besonderheit wirkten die sich

verändernden und beobachteten Herausforderungen durch die Digitalisierung an das Unternehmen und die Wirtschaft im Allgemeinen ausgleichend aus. Denn durch die drei Phasen der Beobachtung ermöglichten sich unterschiedliche Blickwinkel, die einhergehend mit der Schwerpunktverlagerung in der unternehmerischen und fachlichen Identifikation von geschäftsgefährdenden Risiken durch die Abhängigkeit zur Informationstechnologie neue Anreize, Perspektiven und Routinen ergaben.

Dennoch birgt die Teilnahme an internen Prozessen und Praktiken auch eine arbeitsethische Komponente, die durch Selbstreflektion und Abwägung adressiert, um somit der normativen Notwendigkeit wissenschaftlicher Standards zu entsprechen (Genz und Tschoepe 2021: 231). Die genannte Uneindeutigkeit der stattfindenden Beobachtung für die Beteiligten, vorrangig der Beobachteten, aber auch der fließende Übergang von alltäglicher Routine zu dokumentierter Beobachtung, machen diese Reflexion notwendig. In solchen Momenten klarer Abgrenzung, beispielsweise in einem Hintergrundgespräch mit explizitem Hinweis auf das Forschungsvorhaben, waren alle Gesprächspartner über die Agenda und weitere Verwendung des Besprochenen im Bilde.[47] Der Vertraulichkeit über den Gesprächsrahmen, sowie die Teilnehmer und Inhalte wurde dadurch entsprochen, dass die Mitschriften nur als Gedächtnisprotokolle angefertigt wurden. Diese Voraussetzung[48] für die Einsicht in die Hintergründe und Rationalitäten der Experten galt für alle zum Zweck der Forschungsarbeit im Unternehmen geführten Untersuchungen. Die Ergebnisprotokolle aus den Gesprächen und Beobachtungen wurden jedoch systematisch ausgewertet, um die Veränderungen und Konturen der Sicherheitsproduktion und seiner zugrundeliegenden Verschiebung der Risikokontrolle nachzuzeichnen.

Zusammenfassend bot die Methode der ethnographischen Beobachtung ein starkes Analysewerkzeug an, mit dem die informellen Hintergründe und Abläufe der unternehmensinternen Sicherheitsproduktion auf verschiedenen Ebenen der komplexen Struktur von MNU und unter dem Vorbehalt der Vertraulichkeit untersucht werden konnten. Ferner lassen sich darüber hinaus zwei Aspekte durch die ethnografische Beobachtung für die Fragestellung dieser Arbeit festhalten: Die sich wandelnde und während der Corona-Pandemie

[47] Allerdings wurde im Laufe der (informellen) Unterhaltungen auch die Erfahrung gemacht, dass der Hinweis auf diese Verwertung, vielmehr noch der Verweis auf eine Aufzeichnung des Gesprächs, den Verlauf und den Tiefgang des Gesagten tangierte. Daraus ergab sich die Herausforderungen die Formalität der Beobachtung in Abhängigkeit vom Thema und Gesprächsrahmen ex ante zu reflektieren und falls notwendig anzupassen.

[48] Analog zu Gesprächen in diplomatischen Kreisen ist die Zitierung des Gesprächspartners und –Inhalts unüblich, jedoch die Auswertung der Gedächtnisprotokolle etabliert, um Einsicht in die vertrauensvolle Arbeitsroutine von Diplomaten überhaupt zu ermöglichen.

beschleunigte technologische Infrastrukturproblematik basiert simplifiziert dargestellt auf der Abhängigkeit von Hard- und Software-gestützten Prozessen zur Erbringung von Leistungen an Kunden, welche ohne die digitalen Strukturen kaum oder nur unter erheblichen Anstrengungen aufrechtzuerhalten wären. Diese vulnerable Grundlage wurde in einem Lern- und Entwicklungsprozess innerhalb des Unternehmens durch die befragten Mitglieder als maßgebliche Verschiebung von Ressourcen und Umdeutung von Schutzzielen konnotiert. Daraus ergibt sich die Notwendigkeit die Bedingungen und Herausforderungen der digitalen Veränderung genauer zu untersuchen, beziehungsweise deren Folgen für die Organisationsstruktur und Entscheidungsprozesse zu beleuchten. Das zweite Problemfeld thematisiert einen internen Diskurs über die notwendige Entsprechung gegenüber nationalen und supranationalen Normen, welche die Veränderungen von Risikokontrollsystemen in MNU beeinflussen können (beispielsweise in Gestalt der Europäischen Datenschutzgrundverordnung) und geeignete Schutzmaßnahmen umzusetzen, deren Ursprung und stärkster Treiber die potentiellen Sanktionen durch staatliche Autoritäten darstellen. Diesen Befunden aus der ethnographischen Beobachtungen wird durch die weitere Untersuchung der Folgen der Digitalisierung sowie der Analyse der Risikoexposition und Mitigationsstrategien im zweiten und dritten Themenblock zusätzlich Rechnung getragen.

2.5. Digitalisierung, Risiko und Resilienz als Forschungsobjekte

Aufbauend auf den angewendeten ethnographischen Methoden und deren Einbettung in die sicherheitstheoretische Literatur wird somit eine Anschlussmöglichkeit für Autoren der Pariser Schule angeboten. Zur genauen Einordnung unserer Fragestellung und Feststellungen ist daher zunächst der Blick in die bestehende Literatur und die Themenfelder Digitalisierung, Risiko und Resilienz im Kontext der sicherheitsrelevanten Forschung notwendig. Obgleich die Digitalisierung ein allgemeines und weitreichendes Phänomen darstellt, ist sie dennoch ein relativ junges Forschungsthema. Ihre Herausforderungen werden in unterschiedlichen Disziplinen und Wissenschaftszweigen thematisiert, doch nur sehr selten in Bezug auf den Resilienzbegriff oder die Kontinuitätsplanung von Unternehmen. Dahingegen ist der Risikobegriff kein unbeschriebenes Blatt in der Literatur. Die Fülle der Publikationen zum erweiterten Themenfeld bezüglich Risiken ist groß und vor allem stark differenziert.[49] Dem schießt sich die Spartenbildung entlang von unterschiedlichen Disziplinen und Subthemen an. Innerhalb der Wirtschaftswissenschaften, Psychologie, Sicherheitsliteratur oder Soziologie

[49] Die Diversität des Themas zeigt sich zum einem in der Unterscheidung zwischen Texten, die sich mit der detaillierten Erörterungen seiner Bedeutung befassen und solchen, denen vor allem die Pointierung eines Themenfeldes unter Nutzung einer pauschalen Gleichstellung von Risiko und Gefahr zu Grunde liegt.

finden sich diverse Unterkategorien der Vorsorgeplanung und Risikoliteratur (Flüter-Hoffmann, Hammermann und Stettes 2018: 9; Scherrer 2018: 98; Stowasser und Peschl 2019: 7f.). Man erfährt hier detaillierte Informationen über die Akzeptanz, Vermeidung, Bewertung, Kultur, Konsequenzen, Berechnung, Prävention oder finanzielle Mitigation von Risiken. Die Herausforderung liegt demnach in dem Alleinstellungsmerkmal, das man zu erbringen gedenkt. Ähnlich verhält es sich mit der Titelauswahl zur Digitalisierung. Daher wollen wir im Folgenden einen Überblick über die für diese Arbeit relevante Literatur geben und den Beitrag dieser Arbeit vor diesem Hintergrund spezifizieren.

2.5.1. Forschungsstand

Beginnen wir unsere Einordnung des Forschungsstandes mit der Sicherheitsliteratur in den Internationalen Beziehungen (IB), welche für diese Arbeit insbesondere mit Blick auf den Transfer von Verantwortlichkeit zwischen staatlicher und privater Ebene für die Sicherheitsproduktion und Risikobewertung von Relevanz ist. Darunter fällt zunächst die Verantwortungswahrnehmung und Kooperation zwischen staatlichen und privaten Akteuren im Bereich sicherheitsspezifischer Leistungen (Carr 2016, Cavelty und Suter 2009; Christensen und Petersen 2017; Hanson 2018). Das sind zum einen Diskurse über die Sphären von Sicherheitskulturen (Kaldor 2018) und zum anderen der Übergang von nationalen Sicherheitsperspektiven auf den digitalen Raum (Huang et. al. 2021; Kuerbis und Badiei 2017; Kaufmann 2015). Darunter ist vor allem die Delegation von Aufgaben zwischen staatlichen und nicht-staatlichen Einrichtungen relevant, da hieraus die Transformation und Einbindung von Unternehmen als Akteuren innerhalb der Bereitstellung von Sicherheit hervortreten (Eriksson und Giacomello 2006; Liebetrau und Kristoffer 2020).

Ferner stellt sich die Frage nach der Zuweisung beziehungsweise Abgrenzung von Verantwortlichkeit der Führungsebene von privaten Unternehmen im globalen Sicherheitskontext (Grant 2018). Mit der zunehmenden Relevanz der Digitalisierung finden sich zudem Beiträge über die Verbindung zwischen klassischen Forschungsfeldern der Sicherheitsliteratur und der Bedeutung von Normen und Strukturen im digitalen Raum (vgl. Erskine und Carr 2016). Dennoch fehlen fokussierte Fragestellungen nach den spezifischen Risiken im Informationszeitalter einerseits und dem Gefahrenpotential anderseits, welches sich durch die Fortführung von traditionellen Risikokontrollsystemen für die neue Dimension technologischer Risiken ergeben kann (Babic, Fichtner und Heemsker 2017). Ansätze dazu finden sich eher im Bereich der Literatur zur Digitalisierung und bieten einen interessanten Perspektivenwechsel auf die gewählte Fragestellung.

Die Auswahl an relevanten Titeln zur Digitalisierung kann für diese Arbeit in vier Kategorien eingeteilt werden. Die erste Gruppe überschreibt die allgemeinen Darstellungen zur Rolle der Digitalisierung für das Wirtschaftsleben, ihrer Facetten und differenziert die Konsequenzen des technologischen Wandels für die unterschiedlichsten Anwendungsfelder. Dieser Bereich umfasst einige gute Beschreibungen des Umbruchs und der Durchdringungskraft einiger aktuell diskutierter, technologischer Innovationen. Darunter sind beispielsweise Werke zu unterschiedlichen Bereichen der Digitalisierung und deren Veränderungen der analogen Gesellschaft zu nennen (vgl. Krüger 2016; Nasiri et. al. 2020; Wittpahl: 2016) oder auf themenspezifische Untersuchungen von Folgeerscheinungen der Veränderungen wie beispielsweise der Veränderung der Arbeitswelt (vgl. Buhr 2015; Eichhorst et. al. 2016, Hammermann und Klös 2016) oder der Produktionsbedingungen (Haucap et. al. 2015) zu zählen. Ein allgemein lesenswerter Beitrag zum Informationszeitalter stammt von Manuel Castells, dessen Überlegungen zur Netzwerkgesellschaft und den generellen Implikationen einer globalen und vernetzten Welt die weitläufigen Dimensionen der Digitalisierung erfassen (Castells 2010).

Auch technologische Aspekte sind für diese Arbeit relevant, etwa im Fall des ökonomischen Potentials technischer Lösungen wie dem Cloud Computing (vgl. Armbrust et. al. 2016; Heinrich 2016). Die weitverzweigte Ausgestaltung der Digitalisierung, ihrer unterschiedlichen Trends und innovativen Dynamik werden diesem Forschungsfeld sicherlich noch lange Zeit Bedeutung sichern. So baut Benjamin Bratton seine Darstellung auf der Idee eines systematischen Verständnisses des Cloud Computing auf, deren säulenartiger Struktur über unterschiedliche Ebenen mit dem Begriff „stack“ überschrieben wurde (Bratton 2015). Die Zielsetzung seiner Überlegung ist es die Vorstellungen von politischer Geografie unter den Bedingungen der globalen Informationsverarbeitung und Vernetzung in der Cloud zu betrachten (ebd.: 3), ein Ansatz der den umfassenden Einfluss des Cloud Computing zur Grundlage des Informationszeitalters erhebt. Seine Überlegung, dass Technologie die Formen und Entscheidungen von staatlichen Akteuren steuern können, wird in die Diskussion dieser Arbeit einfließen, wenn im sechsten Kapitel von dem Beziehungskonstrukt zwischen Staat und privaten Unternehmen im Informationszeitalter zu sprechen sein wird.[50] Im dritten Kapitel wird uns diese Überlegung ebenfalls begegnen und helfen, die Dimensionen der Digitalisierung zu strukturieren. Für die weitere Diskussion in dieser Arbeit wird allerdings die

[50] Die Disruption dieses Verhältnisses werde schließlich weitreichende Veränderungen nach sich ziehen: “At stake is more than a new way for states to operate or a new set of technologies requiring governance; rather, it is a scale of technology that comes to absorb functions of the state and the work of governance” (Bratton 2016: 7).

Sicherheitsproduktion von Unternehmen weiterhin im Vordergrund stehen und nach erfolgter Spezifizierung der Facetten der Digitalisierung wieder verstärkt auf die sicherheitsrelevante Entwicklung der dadurch hervorgetretenen technologischen Risiken eingehen.

Einige Publikationen formulieren Marketingstrategien und allgemeine Beiträge unter dem Schlagwort der Digitalisierung. Diese eher allgemeine Literaturkategorie beinhaltet kaum Relevantes für die vorliegende Arbeit. Wortgenaue Verwendungen des Themas finden sich in der Literatur zur Übertragung von Wissensbeständen der analogen Welt, so zum Beispiel von Bibliotheksbeständen in die digitale Sphäre[51] und fragen nach der Bedeutung von Wissensgemeinschaften oder Konzepten der Räumlichkeit beziehungsweise Wissenszugänglichkeit (vgl. Boas und Dunning 2000, Conway 2010, Rieger 2008). Ferner kommt die Rolle der Digitalisierung als intervenierende Variabel des Geschäftsumfelds ins Blickfeld (vgl. Bonsel und Le Blanc 2004, Kulatilaka 2001, Langheinrich und Mattern 2003, Xue et. al. 2013). Andere Beiträge beinhalten interessante Einsichten in die Arbeitswelt der (nahen) Zukunft und deren soziale Konsequenzen (vgl. Harty 2012, Krabel 2016, Weber 2016).

Die zweite Kategorie thematisiert die Risiken der digitalen Epoche, allen voran für die Exklusivität von Informationen. Darunter zählen Betrachtungen der Cyberrisiken in allgemeinen Beiträgen (vgl. Cavelty 2013, Choras et. al. 2015) und konkrete Gefahrenbeschreibungen, welche in den Fallbeispielen dieser Arbeit Beachtung finden, wie beispielsweise zum Datenverlust (Greitzer 2014), Social Engineering (Huber et. al. 2009; Vassilaki 2015) oder Ransomware-Angriffen (Felt et. al. 2011). Auch Studien über die spezifischen Folgen der Nutzung von digitalen Technologien zur Sicherheitsproduktion (Aradau und Blanke 2017) oder die Nutzung von Informationstechnologie und deren Risiken im Zuge der Corona-Pandemie sind interessant (vgl. Mishna et. al. 2021). Hervorzuheben ist hierbei die lesenswerte Übersicht von Borges et. al. über die Vorrausetzungen und Variationen des Identitätsdiebstahls (Borges et. al. 2011). Die dritte Kategorie umfasst die praktischen Möglichkeiten von Gegenmaßnahmen, worunter zumeist technische Abhandlungen der Etablierung von präventiven Schutzvorkehrungen zu nennen sind (vgl. Brand, Valli und Woodward 2011; Khan und Sepúlveda 2015, Linkov et. al. 2013), sowie die konzeptionelle Arbeit von Claudia Eckert über IT-Sicherheit (Eckert 2008; Eckert 2014). Zusammenfassend kann festgestellt werden, dass die Breite an Publikationen die zahlreichen Schadprogrammen

[51] Hierbei handelt es sich um Fragestellungen nach der Verfügbarmachung von Wissen (Conway 2010).

und Variationen krimineller Innovation widerspiegelt, welche in der Konsequenz eine sehr heterogene Ansammlung an Bedrohungsbildern für Unternehmen darstellen.

Für den traditionellen Risikobegriff ist das ideengeschichtliche Vorfeld der anzutreffenden Literatur bereits abgesteckt und die Masse an möglichen Quellen groß. Doch was zunächst unübersichtlich erscheint, lässt sich durch die konkrete Fragestellung reduzieren. Es findet sich hier zum Beispiel die Fragestellung nach einer Gesellschaft im Zeitalter globaler, nicht mehr versicherbarer Risiken und deren Folgen, aber auch einen Begriff des technischen Risikos, welche jedoch nicht den Schwerpunkt dieser Arbeit bilden. Die Verbindung zwischen Risiko und Gefahr tritt hingegen in den Vordergrund dieser Betrachtung, denn für diese Arbeit ist die von Niklas Luhmann vorgeschlagene Unterscheidung zwischen Risiko und Gefahr (Luhmann 1991) ein interessanter Pfad, um sich der vorausgegangenen Fragestellung zu nähern. Was Luhmann als allzu selten getroffene Unterscheidung kritisiert, ist hier mit der Pauschalisierung des Risikobegriffs gemeint. Dieser wird aber in Beiträgen zur Unternehmenssteuerung in der Regel nicht angewendet.[52]

Die Soziologie des Risikos qualifiziert sich als geeignete Möglichkeit, die Fragestellung dieser Arbeit in den Kontext der sozialwissenschaftlichen Betrachtungsweise einzuordnen. Die Überlegungen von Niklas Luhmann (Luhmann 1984; 1986; 1991, 1996, 2000) nehmen eine prominente Stellung ein, da sie nicht nur einen wesentlichen Beitrag zur Debatte geliefert haben, sondern auch eine gewichtige Grundlage für die Agenda dieser Arbeit ermöglichen. Weitere risikosoziologische Arbeiten dienen als Referenzen einer Einbettung der aufzuzeigenden Risikoterminologie und nehmen unterschiedliche Perspektiven ein (vgl. Jarvis 2000; Jarvis 2011; Kasperson 1998; Lupton 2006; Mingers 1989; Rasmussen 1997; Sjörberg 1998; Vanderstraeten 2000). Dennoch bleibt ein Mangel an empirischer Fundierung zu vermerken: “Grand theorizing of writers like Beck, Giddens and Douglas to lack a firm grounding in empirical research which is able to support their propositions” (Lupton 2006: 21).[53]

Das Gros der Werke über *Risiko* bezieht sich auf die diversifizierten Ausgestaltungen des Risikomanagements. Trotz einer großen Anzahl an Publikationen zur Umsetzung des Risikomanagements in der betriebswirtschaftlichen Realität und – wenn auch zahlenmäßig geringfügiger – in der theoretischen Betrachtung, mangelt es häufig an einer Unterscheidung in

[52] Luhmann selbst nennt als möglichen Grund eine gewisse Sorglosigkeit um die terminologische Bedeutung (Luhmann 1991: 37)

[53] Vergleiche hierzu auch die Arbeit von Beck zur Weltrisikogesellschaft (Beck 1991, 2002, 2006), welche allerdings in dieser Arbeit eine untergeordnete Rolle spielt.

Luhmanns Sinn zwischen Risiko und Gefahr. Ein häufig wiederkehrendes Unterscheidungsmerkmal ist die Einbettung des klassischen Risikomanagements als Teil der Organisationsstruktur und operationellen Risikomitigation. Innerhalb der disziplinbedingten Kernkompetenz der Bewertung von Risiken gilt es zudem auf die Unterscheidung zwischen der subjektiven und objektiven Bemessung von Risiken einzugehen.[54] Diese Literatur ist hilfreich um das hier verwendete Verständnis von unternehmenseigener Risikobewertung nachzuvollziehen (vgl. Best 2010; Bradbury 1989; Clapton 2009; Eliott et. al. 2000; Kasperson 1998; Klinke und Renn 2002; Klinke und Renn 2004; Jonen und Lingnau 2004; Miller 1992; Pfeiffer 2006; Ward 2003).

Dem schließt sich eine reichhaltige Literatur zur Bearbeitung einzelner Risikokategorien[55] an, die sich allerdings in wechselnder Trennschärfe zwischen Risiko und Gefahr mit dem Thema beschäftigt. Hieraus sind insbesondere die Schlussfolgerungen für die vorherrschenden Denkmuster von Unternehmen in Bezug auf bestimmte Risikogruppen hilfreich. Jede Risikokategorie kann auf eine eigne, umfangreiche Bandbreite an Publikationen verweisen. Zum einem sind Autoren anzutreffen, die sich mit politischen Risiken auseinandersetzen (vgl. Busse und Hefeker 2005; Delios und Heinz 2003; Goldstone et. al. 2010; Heinsz und Zelner 2003; Hood und Nawez 2004; Jakobsen 2012; Jarvis 2008). Zum anderen finden sich Publikationen zum medizinischen Risiko (Ferguson 2006; Günther et. al. 2011; Horst 2012; Merith et. al. 2008) oder zum technologischen Risiko und seiner Perzeption in der Gesellschaft (vgl. Aradau 2008; Krahmann 2007), welche in dieser Arbeit an späterer Stelle referenziert werden, um die Umsetzung von Analysemechaniken in spezifischen Risikofeldern zu untersuchen.

Schließlich gibt es noch die kleinste Gruppe, welche sich mit den Risiken der Geschäftsunterbrechung als Risikokontrolle beziehungsweise mit einer Spezialisierung auf BCM und allgemein auch Resilienz beschäftigt. Diese Arbeiten sind häufig als Arbeitsanleitung für Experten konzipiert (vgl. Brunsdon und Dalziell 2005; Pike, Dawley und Tomaney 2010; Rose 2011; Utz, Schultz und Glocka 2012). Andere beschreiben Teilaspekte der Materie (Kahan, Allen und George 2009; Murray und Gubesic 2007; Torabi et. al. 2014) oder behandeln die Evolution von BCM (Rose 2004; Sahebjamnia et. al. 2015) beziehungsweise des Resilienzbegriffs (Blum et. al. 2016; Bryce et. al. 2020; Christensen und Petersen 2017; Lam 2002; Moamani 2010; Zsidisn, Melnyk und Ragatz 2005). Dem überwiegenden Großteil der

[54] Ein großer Teil der der Literatur beschäftigt sich mit Analyse von Katastrophen natürlichen und technischen Ursprungs (vgl. für einen Überblick Power 2010: 304ff.).
[55] Die Bedeutung von Risikokategorien wird im dritten Kapitel verdeutlicht.

Beiträge aus dieser Gruppe ermangelt es an empirischen Anwendungsbeispielen und konkreten Handlungsempfehlungen. Eine ertragreiche Quelle in dieser Hinsicht bietet die Literatur des Lieferkettenmanagements (*supply chain management*), welche die Ausfälle und Mitigation von Warenlieferungen und Prozessen thematisieren und damit eine Untergruppe der Risikokontrolle (vgl. Behnezhad, Connett und Nair 2016; Fekete, Grinda und Norf 2016; Jüttner 2005; Roitsch und Meyr 2008; Todo, Nakajima und Matous 2014). Interessante Einblicke bietet die Literatur zur Rolle der kritischer Infrastruktur[56] für die Gesellschaft (Braubach 2011; Fischer 2007; Hindmarsh 2013; Kaufmann 2013; Ng und Lean 2012; Norio et. al. 2011; Perrow 2011). Ähnliches gilt für die Methoden des BCMs und deren Anwendbarkeit und überaus hilfereich für das Verständnis der Business Impact Analysis und der Risikobewertung im Sinne der Ausfallwahrscheinlichkeit sein können (Cavelty 2013; Church et. al. 2004; Church und Scaparra 2007; Holmgren 2007; Rodriguez und Palomares 2014; Schintler et. al. 2007; Shaw 2004; Smit 2005). Dem schließen sich Trendstudien und Umfragen im Auftrag der Wirtschaft an, welche interessante Stimmungsbilder und Entwicklungsprofile aus Sicht von Unternehmen widerspiegeln (vgl. AGCS 2012, AGCS 2013, AGCS 2018; AGCS 2020; AT&T 2013, BCM Academy 2016, Continuity Insights und KPMG 2008).

Zusammenfassend stellt sich die Frage was die zuvor skizzierte Übersicht über die Literaturgrundlage für die vorliegende Arbeit bedeutet? Insbesondere mit Blick auf die Risikoliteratur und sowohl die Forschung zur technologischen als auch operationellen Schutzkomponente im Informationszeitalters bieten umfassende Grundlagen für die weitere Analyse der Fragestellung. Die Lücke in der bisherigen Forschung ist in zwei Bereichen anzutreffen: Erstens ist der Blick auf Unternehmen als Akteure der Sicherheitsproduktion durch Bereitstellung und Kontinuität ihrer internen Prozesse ein unterrepräsentiertes Forschungsobjekt. Die Unterscheidung zwischen Sicherheitsbereitstellung *in* Unternehmen gegenüber dem Beitrag zur gesamtgesellschaftlichen Unsicherheitsabsorption *durch* private Akteure verspricht aufschlussreiche und anschlussfähige Erkenntnisse in einem bisher unterbeleuchteten Bereich. Dies bezieht sich sowohl auf die Rolle von Unternehmen, welche bisher nur unterrepräsentiert in die Sicherheitsforschung einbezogen wurden, als auch für die Internationale Politische Ökonomie, die bisher nur in Grundzügen auf die Veränderungen der Sicherheitsrelevanten Entwicklungen reagiert hatte. Als nennenswerte Ausnahmen sind hier

[56] Wir werden auf die Perspektive der Literatur in den internationalen Beziehungen auf die kritische Infrastruktur im vierten und sechsten Kapitel zu sprechen kommen. Hier wird insbesondere die Rolle von staatlichen und privaten Akteuren zur Sicherstellung der Verfügbarkeit der kritischen Infrastruktur diskutiert werden, deren primäre Ausrichtung in der Literatur jedoch private Akteure und deren Mitigationsstrategien vernachlässigt (vgl. Aradau 2008; Clapton 2011).

Horacio Ortiz (Ortiz 2009; Ortiz 2013; Ortiz 2021) und Douglas Holmes (Holmes 2009; Holmes 2019) zu nennen, die mithilfe von ethnographischen Methoden Organisationen von innen beobachtet haben, um Praktiken und Rationalitäten der Mitglieder in den Organisationen zu erforschen.

Zweitens sind die unternehmensinternen Praktiken der Sicherheitsproduktion mit dem Übergang von traditionellen, objektbezogen Risikomodellen hin zu prozessorientierten Ansätzen zur Steuerung und Kontrolle von Risiken verbunden. Diese Neuerung betrifft vor allem den in Unternehmen geführten Risikodiskurs und die damit verbunden Anwendung von Risikokontrollen zur Sicherstellung der Prozess- und Kommunikationskontinuität. Diese neue Methodik zum Umgang mit den exogenen Herausforderungen im Zeitalter der Digitalisierung wurde bisher kaum als Beitrag zur allgemeinen Sicherheitsarchitektur konnotiert und wird in dieser Arbeit als Erkenntnis aus der ethnographischen Beobachtung eingeführt werden. Der Beitrag der vorliegenden Arbeit soll daher Lücke in der Literatur durch die Zusammenführung der unterschiedlichen Disziplinen und Strömungen aus IPÖ, IPS und Sicherheitsforschung, aber auch Digitalisierungsliteratur schließen

2.6. Zusammenfassung – Sicherheitsproduktion in Unternehmen

Wie durch die Einleitung und das nachfolgende Kapitel zur Verortung dieser Arbeit in der Sicherheitsliteratur aufgezeigt wurde, eröffneten sich durch die Corona-Pandemie neue Ansatzpunkte für die Sicherheitsforschung in den Internationalen Beziehungen. Neue Technologien[57], beziehungsweise deren beschleunigte Nutzung als Resultat der Lockdowns sicherte zwar einerseits den Fortbestand von vielen Unternehmen, erzeugte aber gleichzeitig eine gesteigerte Bedrohungslage durch Cyberrisiken. In diesem Kontext gewinnt die Rolle der Sicherheitsproduktion innerhalb von Unternehmen an Bedeutung für die Sicherheitsforschung, da die Abhängigkeit der Gesellschaft von der ununterbrochenen Bereitstellung von Gütern und Dienstleistungen durch die fortschreitende Digitalisierung in der Verantwortung privater Träger

[57] Im Informationszeitalter ermöglichen neue Technologien die Erstellung globaler Wissensnetzwerke, welche Nutzer und Wissensbestände unabhängig von ihrer physischen Verortung verbinden. Die Relevanz von Entfernungen und dem Aufenthaltsort tritt somit in den Hintergrund (vgl. Serres 1995). Die Transzendenz örtlicher Gebundenheit im Informationszeitalter wird nur noch durch die Schnittstellen der digitalen Sphäre gekennzeichnet, wie der Hardware in Rechenzentren oder Endgeräten. Die Übersetzung zwischen beiden Sphären war und ist Gegenstand der Digitalisierung, die im Laufe ihres Fortschreitens ein beständiges Kommunikationsnetzwerk erschaffen hat, für dessen Betrieb nicht mehr nur der Mensch Sorge zu tragen hat, sondern auch die Komponenten des Informationsnetzwerkes. Diese haben gelernt eigenständig zu kommunizieren (vgl. „Internet of Things“): „Things inform one another in specific ways, and this specificity is how Michel Serres defines communication as the work of Hermes. Adjacent to this, I see addressability not just as an absolute logistics but as a transalphabetic compositional platform” (Bratton 2015: 210).

deutlich wird. Dies trifft im besonderen Umfang auf die sogenannte kritische Infrastruktur zu, deren interne Sicherheitsproduktion bisher in der Sicherheitsliteratur vernachlässigt wurde.

In Anlehnung an die Pariser Schule kann daher ein anschlussfähiger Beitrag zur Sicherheitsforschung durch die Anwendung der ethnographischen Methodik zur Untersuchung der Sicherheitsbereitstellung innerhalb von MNU geleistet werden. Diese Arbeit richtet sich daher mit der Innenperspektive von privaten Akteuren der Sicherheitsstrukturen an eine Lücke der bisherigen Literatur innerhalb der Schnittmenge aus IPÖ, IPS und Organisations- beziehungsweise Risikosoziologie. Ferner können Empfehlungen für die Gestaltung der Sicherheitspolitik und Risikomitigation artikuliert werden, welche die Rolle von MNU als Akteure der Gestaltung einer neuen Sicherheitsarchitektur berücksichtigen. Daher werden wir im folgenden dritten Kapitel zunächst die Folgen der Digitalisierung für MNU untersuchen, bevor wir die Risiko- und Organisationssoziologie von Unternehmen im Informationszeitalter im vierten Kapitel beleuchten werden.

II) Digitalisierung, Risiko und Organisation

Dieser Themenblock dient der Einordnung der elementaren Begriffe für unsere Forschungsfrage und adressiert drei wesentliche Aspekte, die als Grundlage für die weitere Untersuchung der Sicherheitsproduktion in Unternehmen dienen werden. Der erste Aspekt fasst im nachfolgenden dritten Kapitel eine Auswahl der für unsere Fragestellung relevanten Facetten[58] der Digitalisierung zusammen, welche einem Überblick über die wesentlichen Veränderungen durch die neuen Technologien bieten. Daher wird hier die Digitalisierung als Zäsur betrachtet und unter dem Gesichtspunkt der disruptiven Wirkung für Unternehmen thematisiert. Dadurch werden wir in der Lage sein, auf den zweiten Abschnitt dieses Themenblocks überzuleiten. Dieser hat die Implikationen der Digitalisierung auf Risikomanagementsysteme in Unternehmen zum Inhalt. Dies wird im vierten Kapitel besprochen und soll die Implikationen der Digitalisierung für die internen Risikokontrollen aufzeigen. Dies soll auch die unternehmensinterne Perspektive auf traditionelle Kontrollsysteme zur Bereitstellung von Sicherheit innerhalb der Organisation erläutern.[59]

Der Aufbau, Methodik und Bewertungsschemata des unternehmerischen Risikomanagements werden daher hier thematisiert. Die zentrale Frage an dieser Stelle wird sein, wie traditionelle, in diesem Sinne analoge, Strategien zur Risikovorsorge auf die potentiellen Sicherheitsrisiken der neuen technologischen Strukturen in unternehmerische Kernprozesse Sicherheit erzeugen können. Dieser Betrachtung werden sich die Auswirkungen der Digitalisierung auf den Organisationsbegriff im Kontext der Struktur, Verantwortungszuweisung und Kommunikation von Entscheidungen in MNU anschließen. Dieser dritte Aspekt untersucht die Ursachen für die Revision von Strategien und Strukturen von Unternehmen im Informationszeitalter, welche unter dem Gesichtspunkt unserer Fragestellung wesentlichen Anteil an der Veränderung des Risikobegriffs und der Bereitstellung von Sicherheit in der Organisation haben.

[58] Die Auswahl der Facetten der Digitalisierung wird im Abschnitt 3.2 näher erläutert. Der Aufbau und die Auswahl orientieren sich an Brattons Darstellung des „Stack“ (Bratton 2015), sollen aber nur der grundlegenden Annäherung an das Informationszeitalter und seiner technologischen Komponenten dienen. Die fortschreitende Betrachtung der nächsten Kapitel wird wieder den Fokus auf die Sicherheitsproduktion in Unternehmen legen.

[59] Dies betrifft vor allem den im vierten Kapitel zu zeigenden Aufbau von Risikokontrollsystemen, deren Kontrollkatalog über die zu prüfenden Risiken nach einem thematisch-gegliederten Ansatz folgen (Luburić 2017). Dadurch werden übergreifende Aspekte der operationellen Resilienz nicht in einem einheitlichen Rahmenwerk zusammengeführt und Schutzwerte, wie die Verfügbarkeit, werden isoliert von der Integrität oder Vertraulichkeit von Daten verstanden. Die dadurch entstehenden Risiken sind Gegenstand der späteren Entwicklung eines umfassenden, integrierten Risikokontrollsystems, wie es im siebten Kapitel gezeigt werden wird.

3. Digitalisierung als Zäsur

Bevor wir die Sicherheitsproduktion in Unternehmen und die erhöhte Bedrohungssituation in Folge der Corona-Pandemie in den nachfolgenden Kapiteln analysieren, wollen wir zunächst die Grundlagen des technologischen Wandels betrachten. Dazu wollen wir in diesem Kapitel die fundamentalen Begriffe und Strukturen des Informationszeitalters klären. Der bereits längerfristige Prozess des digitalen Wandels[60] (Buhr 2015) zeigt unter anderem die Bedeutung informationsbasierter Wertschöpfungsketten und der Automatisierung beziehungsweise Virtualisierung von Geschäftsprozessen hervor (Hettich, Schimmer und Müller-Stewens 2015) und betrifft damit auch die ökonomische Rationalität und Entscheidungsprozesse von Unternehmen. Die zentrale Bedeutung von Informationstechnologie und ihrer Prozesse für die unterbrechungsfreie Bereitstellung von gesellschaftlich relevanten Leistungen zeigt aber auch, dass die Digitalisierung zum sicherheitsrelevanten Faktor geworden ist. Ferner haben sich Unternehmen als Entwickler und Nutzer der damit verbunden Technologien im Sinne unserer Fragestellung zu aufschlussriechen Untersuchungsobjekten der Sicherheitsforschung entwickelt.

Bevor wir uns dieser Konstellation im Detail widmen wollen wir zunächst die Vielfältigkeit, aber allen voran die strukturellen Grundlagen und den Einfluss der Digitalisierung auf die Abläufe, Schutzziele[61] und Organisation von Unternehmen in diesem Kapitel betrachten. Um später die Folgen der durch die Corona-Pandemie beschleunigten Digitalisierung und veränderten Bedrohungslage mit Blick auf die Sicherheitsproduktion von Unternehmen zu verstehen, ist daher eine strukturierte Analyse der Digitalisierung und eine Einordnung der in diesem Kontext verwendeten Schlüsselbegriffe notwendig. Darunter fallen die (1) Rolle von Informationen und die Relevanz von Räumlichkeit in der virtuellen Sphäre, (2) Zusammenfassung großer Datenmengen unter dem Überbegriff von Big Data und die (3) Nutzungsmöglichkeiten von Algorithmen und selbstlernenden Programmen. Die Betrachtung von (4) Cloud-Computings soll die Vernetzung von Systemkomponenten, Informationen und Anwendungen verdeutlichen, welche die zuvor genannten Elemente mit der (5) Ebene der Nutzer verbindet. Abschließend werden die (6) Anwendungspraktiken behandelt, durch welche

[60] Der Prozess der Digitalisierung erstreckt sich über fast alle Branchen, Wirtschaftsbereiche (Buhr 2015), Märkte und große Teile des gesellschaftlichen Lebens (Arnold et. al. 2016). Die Digitalisierung ist ein Phänomen, das Veränderungen in vielfältiger Weise bewirkt, vom Aufstieg der Internetkonzerne wie Google und Amazon und deren Expansion in andere Märkte Google etwa versucht die vorhandenen Daten in neue Geschäftsmodelle und Märkte zu übersetzen, wie etwa der Einführung eines eigenen Versicherungsangebots (Hettich, Schimmer und Müller-Stewens 2015: 60).

[61] Schutzziele sind besonders schützenswerte Bereiche, Informationen, oder Abläufe in Organisationen, deren Definition die Grundlage für den Rahmen der internen Sicherheitsproduktion ermöglicht.

exemplarische Veränderungen von Märkten und Geschäftsmodellen aufgezeigt werden können. Die Betrachtung dieser spezifischen Facetten der Digitalisierung ist als spezifische Auswahl zu verstehen, deren Zusammenwirken den Anpassungsdruck auf Unternehmen begründet und somit der ökonomischen Rationalität im Informationszeitalter Ausdruck verleiht.[62]

3.1. Zeitalter der Informationen

Die Digitalisierung kann als kontroverser Diskussionsgegenstand angesehen werden. Ökonomisches Wachstumspotential und schöpferische Zerstörung[63] sind zwei Annahmen über die Natur der Digitalisierung. Aus Sicht der optimistischen Betrachter ermöglicht die Vernetzung von Informationen und Systemen ungeahnte Chancen. Skeptische Stimmen verweisen aber auf die Risiken der Technologie und beide haben ihre Berechtigung. "[W]e are witnessing a point of historical discontinuity", wie es Manuel Castells in seiner lesenswerten Abhandlung zum Informationszeitalter unterstreicht (Castells 2010: 78). Denn Chancen und Risiken der Digitalisierung beginnen sich erst langsam zu offenbaren und ein Einblick in die Geschichte aus etwa einem Vierteljahrhundert digitaler Präsenz erlaubt erst eine vorläufige Bewertung der Möglichkeiten und Herausforderungen zum gegenwärtigen Zeitpunkt. Der Cyberraum ist dabei eine Sphäre, die es zu besetzen gilt. Was im Zeitalter der Industrialisierung mithilfe von Dampfschiffen, Eisenbahnen und der Kolonialverwaltung umgesetzt wurde[64], wird in der digitalen Epoche durch Informationen, Infrastrukturkomponenten und Software erreicht. Die digitale Zeit verfügt über ihre eigenen Regeln und Instrumente, welche auch ihre spezifische Wertedimension inkludieren (Weber 2016: 33). Dies hat weitreichende Folgen und zeigt sich in unterschiedlichen Facetten. Diese Ausprägungen des Cyberzeitalters wollen wir im Folgenden adressieren und exemplarisch auch im Detail betrachten. Zunächst sollen einige Schlüsselbegriffe definiert und eingeordnet werden, um anschließend die Facetten der Digitalisierung mit einer klaren Terminologie zu beleuchten.

---

[62] Die Auswahl geht wie zuvor erwähnt auf Benjamin Bratton zurück (Bratton 2015) und wird hier nur zur Einordnung der Begriffe verwendet, um danach wieder zur Sicherheitsproduktion zurückzukehren.

[63] Der Ausdruck der schöpferischen Zerstörung wird auf das Werk von Josef Schumpter zurückgeführt, das den begleitenden Effekt von Neuerungen in der ökonomischen Theorie beschreibt, nach dem neue Wirtschaftszweige oder Technologien Gewinne erwirtschaften, während traditionelle Geschäftsmodelle aufgrund der veränderten Wettbewerbssituation Nachteile erzielen (Schumpter 1942). Dieser Effekt zeigte sich etwa in Form der Gewinnverschiebungen zu Gunsten der Industrie im 18 Jahrhundert auf Kosten der Agrarwirtschaft (vgl. Acemoğlu und Robinson 2015: 118f.) oder beispielsweise in jüngerer Vergangenheit in Gestalt von Kurznachrichtendiensten. Das für Telekommunikationsunternehmen einträgliche Geschäft mit Kurznachrichten wurde durch die Verbreitung von kostenlosen Messenger-Diensten wie Whatsapp in kurzer Zeit annihiliert.

[64] Vgl. die Frontiermigrationsprozesse des 18. und 19. Jahrhunderts, in deren kultureller Konnotation des Zeitgeistes entsprechend, der Aufbruch in eine neue Welt als Zäsur verstanden wurde. Die Besetzung der zu entdeckenden Territorien entsprach einer mentalen Grenzziehung zwischen dem Alten und dem Neuen (Osterhammel 2010: 466ff.). Hier ergibt sich eine Parallele zur Unterscheidung zwischen dem analogen und dem digitalen Raum.

3.1.1. Schlüsselbegriffe der Digitalisierung

Einige Begriffe sind in unserem Kontext zu unterscheiden und im späteren Gebrauch zudem weiter zu konkretisieren. Dazu zählen die (1) Digitalisierung, (2) Automatisierung und (3) Robotisierung. Neben diesen allgemeinen Sammelbegriffen schließen sich drei weitere an, die unmittelbar mit der Entwicklung des virtuellen Wissensbestandes verbunden sind, (4) Big Data, das (5) „Internet of Things" (IoT), sowie deren Verbindung über (6) Cloud Computing. Hinzu kommen weitere Termini, welche im Verlauf dieses Kapitels eingeführt werden. Diese sechs Begriffe sollen zuallererst das Grundverständnis der im Folgenden zu erörternden Untersuchung ermöglichen. Die (1) *Digitalisierung* wird als ein anhaltender Prozess verstanden, der die Umwandlung von Informationen der analogen Welt in eine virtuelle Sphäre beschreibt (Boas und Dunning 2000: 3). Dieser Prozess der Transition hat unmittelbare Auswirkungen auf die Lebens- und Erfahrungswelten der Menschen, welche mit diesen Daten arbeiten, aber auch für jene, deren Daten prozessiert werden.[65] Der technologische Kern des Phänomens beschreibt somit die Erschließung des digitalen Raums zur effizienten Verwaltung und Nutzung von Informationen auf einem hohen und komplexen Niveau. Dieser beruht auf der Weiterentwicklung von Hardware, also technischer Infrastruktur- und Gerätekomponenten, welche den Aufbau der virtuellen Speicherung von Daten erst ermöglicht hat (Heinrich et. al. 2016: 53). Diese Entwicklung befindet sich in einen sich selbst bestärkenden Kreislauf der fortwährenden Eigenoptimierung. „Mit erstaunlicher Präzision gilt das bereits Mitte der sechziger Jahre beschriebene *‚mooresche Gesetz'*, welches besagt, dass sich die Rechenleistung von Computern etwa alle 18 Monate verdoppelt" (Langheinrich und Mattern 2003: 4).

Eingeleitet durch den Prozess der Digitalisierung erhält die digitale Epoche ihre Bezeichnung, welche hier auch als Informationszeitalter tituliert wird. Der Name leitet sich von der Bedeutung der Informationen für die Produktivität und deren Stellenwert innerhalb einer vernetzten Gesellschaft ab (Castells 2010: 21f.). Durch die umfangreiche technologische Innovation, deren Grundlage auf der Bereitstellung von virtuell verfügbaren Informationen beruht (Digitalisierung als Prozess), gelangten Informationen zum eigentlichen Mehrwert und Schlüsselelement der Epoche (Fisher 2013: 217). Auch in vergangenen Jahrhunderten sicherten Informationen Einfluss und Gewinnmöglichkeiten. Die Kenntnis über Technologien, Präferenzen und Zusammenhängen versprachen finanzielle, politische oder soziale Vorteile.

[65] Castells beschreibt die Tragweite der technologischen Innovation in Verbindung mit der Aufhebung lokaler Handlungs- und Wahrnehmungsparadigmen als Metamorphose zur Netzwerkgesellschaft: "A technological revolution, centered around information technologies, began to reshape, at accelerated pace, the material basis of society. Economies throughout the world have become globally interdependent, introducing a new form of relationship between economy, state, and society, in a system of variable geometry" (Castells 2010: 1).

Dennoch kennzeichnet sich das Informationszeitalter in Abgrenzung zu vorausgegangenen Epochen durch seine spezifische Wertdisposition, Dynamik und Konstellation ab, durch welches „(…) information generation, processing, and transmission become the fundamental sources of productivity and power because of new technological conditions emerging in this historical period" (Castells 2010: 21). In der Folge werden die Begriffe zur zeitlichen Einordnung des durch die Digitalisierung eingeleiteten Phänomens als digitales, Informations- oder Cyberzeitalter bezeichnet. Demgegenüber steht die analoge Epoche, welche hier als Umschreibung der Zeitspanne vor dem Durchbruch der informationsbasierten Gesellschaft verstanden wird.[66]

Die Informationsverbreitung durch die Digitalisierung bedarf darüber hinaus einer weiteren Unterscheidung zwischen Informationen und Daten. Informationen werden in unserem Kontext wie zuvor gezeigt als Inhalte verstanden, welche einen Wert repräsentieren. Dieses Wissen kann in Form von Daten gespeichert werden. Informationen sind folglich Gegenstand von Daten und bestimmen dadurch auch den Wertstatus von Daten. Die Digitalisierung eröffnete indes neue Möglichkeiten für den Umgang mit Daten. Dazu waren zwei wesentlichen technischen Komponenten notwendig: (a) die virtuelle Verfügbarkeit der Daten über das Internet und (b) der Fortschritt der Hardware im Sinne der gesteigerten Leistungsfähigkeit von Computern und mobilen Endgeräten (Lepping und Palzkil 2016: 19). Ein immenses Informationsangebot steht heute für jede Person theoretisch zur Verfügung, die über ein Endgerät mit Internetzugang verfügt. Die Anfänge des Internets waren jedoch noch von relativer Exklusivität gekennzeichnet. Kommerzielle Pioniere des privaten Netzzuganges wie AOL oder YAHOO boten über browsergestützte Applikationen Zugriff auf die verfügbaren Datenmengen und zugleich die Möglichkeit, Wissen zu transferieren (vgl. Bomsel und Le Blanc 2004: 196). Die Schnelligkeit und Erschwinglichkeit der Übermittlung war nicht weniger relevant. Große Mengen an Daten konnten nun in einer Email versendet werden. Eine E-Mail mit 100 Kilobyte Textdaten war ungleich günstiger zu verschicken, als ein Buch mit gleicher Textmenge auf dem Postweg zuzustellen, vom zeitlichen Aspekt ganz zu schweigen. Das Internet wurde zum Beschleuniger einer Informationsgesellschaft und zum Wegbereiter neuer Industrien (Boas und Dunning 2000: 3).

[66] Die technologischen Optionen, welche sich dank der Digitalisierung bieten, übertreffen das bisher bekannte Potential zur Informationsauswertung. In dieser Hinsicht grenzt sich das digitale Zeitalter vom analogen durch den Einsatz neuer Technologien wie beispielsweise dem Cloud Computing und die umfassende Vernetzung von Komponenten der Informationskonglomerate ab (Amoore 2016: 2).

Denn die technologische Innovation ermöglichte es neuen Marktteilnehmern[67], und Wirtschaftszweigen in kurzer Zeit an Bedeutung zu gewinnen und mit zunehmender technologischer Durchdringung die Wertschöpfung verschiedenster Industieren zu verändern (Welzbacher et. al. 2015: 16). Es ergeben sich neue Konstellationen in den Wertschöpfungsketten und Beziehungen zwischen Kunden, Anbietern und Zulieferern[68], in deren Konsequenz der Anpassungsdruck auf Unternehmen zunimmt (Buchholz und Wangler 2016: 179). Im Kern dreht es sich zumeist um die Vernetzung zuvor isoliert erscheinender Akteure, wie es zum Beispiel im analogen Zeitalter der Fall war. Hier traten individuelle Kunden, verschiedene Produzenten oder ein Katalogversandhaus in direkte Geschäftsbeziehungen miteinander. Ein Onlinevertrieb von Waren wie beispielsweise Amazon kann hingegen auf ein komplexes Netzwerk aus Informationen zurückgreifen, so zum Beispiel auf die Präferenzen der Kunden, basierend auf der Verlaufshistorie zurückliegender Einkäufe. Anders als das (analoge) Warenhaus, welches bestenfalls auf eine persönliche Bindung der Kunden zum Haus und deren Verkaufspersonal angewiesen ist, kann der Online-Händler anonymisierte Daten des Suchverlaufs verwenden um passende und individualisierte Angebote zu unterbreiten.[69] Wie dieses Beispiel aus dem Einzelhandel zeigt, ergeben sich auch Auswirkungen auf die Beziehungen von Unternehmen zueinander, insbesondere was die Verknüpfung von Informationen in Gestalt der Cloud-basierten Dienstleistungen[70] in noch größerem Umfang betrifft, wie wir es im Abschnitt über die Cloud näher adressieren werden.

Das Zusammenspiel der einzelnen digitalen Informationen und deren Kontextualisierung wird durch die (2) *Automatisierung* der Geschäfts- und vor allem Produktionsprozesse fortgesetzt. Ein zuvor von Menschen erbrachter Arbeitsschritt kann durch die Zusammenführung der benötigten Informationen potentiell durch ein Computerprogramm ersetzt werden, sofern die

[67] Die Treiber dieser Entwicklung sind jedoch nicht paritätisch verteilt. Unternehmen aus den USA dominieren den Markt der Internetwirtschaft, auch wenn sich weltweit eine dynamische Verteilung der Hard- und Softwareentwicklung attestieren lässt. Mit Blick auf quantifizierbare Kriterien, lässt sich beispielsweise die Marktkapitalisierung im Bereich der Internetwirtschaft in den USA für das Jahr 2015 auf 4.551 Milliarden Euro beziffern. Dem stehen zum Vergleich 331 Milliarden Euro in Deutschland gegenüber (Buchholz und Wangler 2016: 180). Für das Jahr 2022 erreichten in Folge der Beschleunigung der Digitalisierung alleine Apple, Microsoft, Amazon, Alphabet und Meta eine gemeinsame Marktkapitalisierung von 8.711 Milliarden Euro (Statista 2022).

[68] Mit den neuen Ansätzen und Möglichkeiten entstehen auch neue Bedürfnisse auf Seiten der Kunden, welchen die gleiche Technologie zur Verfügung steht. Der digitale Direktverkauf von Waren und Dienstleistungen ermöglicht neue Absatzmöglichkeiten, doch erlaubt es auch Kunden, Produkte online zu vergleichen und möglicherweise auf Substitute der Konkurrenz zurückzugreifen.

[69] Zudem drängt sich das digitale Warenhaus zwischen Produzenten und Absatzmarkt, ohne allerdings alle Produkte physikalisch ausstellen zu müssen. Durch die hohe Präsenz gegenüber dem Kunden, kann sich das Online-Warenhaus als Marke etablieren und diese Marktmacht gegenüber den Zulieferern im Rahmen der Einkaufverhandlungen ausspielen (Hettich, Schimmer und Müller-Stewens 2015: 16f.).

[70] Software und Plattformen können als Dienstleistungen auf der Cloud hinterlegt werden, die durch ein paar wenige Anbieter wie Amazon Web Services (AWS) oder Microsoft Azure Marktführer (Armbrust et. al. 2010: 52) und konzentrieren auf ihren Cloud-Universen die Daten und Anwendungen von anderen Unternehmen.

Tätigkeitsanforderung es zulässt. In Verbindung mit leistungsfähigen Endgeräten kann ein digitaler Prozess in die analoge Welt übersetzt werden. Die Automatisierung beziffert in diesem Sinne eine Fortsetzung der Industrialisierung, etwa durch die zentrale Steuerung von Produktionsschritten in einer Fabrik oder des von einem Computer durchgeführten Betriebs eines Zuges. Automatisierung basiert auf Repetition, also auf der Wiederholung eines exakt vordefinierten Prozesses (Eichhorst et. al. 2016: 5). Die Maschine unterstützt den Menschen durch die Übernahme eines konkret beschriebenen Auftrages und dessen effektiven, in vielen Fällen sogar weniger fehleranfälligen Ablaufs, wie es Produktionsstrecken von Fahrzeugwerken oder Computerchipfabriken seit etwa 40 Jahren zeigen (Krüger 2016: 7). Die Automatisierung im Informationszeitalter geht über diese Eigenschaft hinaus, indem sie durch die Sammlung von Daten aus den vernetzten Endgeräten und Maschinen Handlungsrichtlinien ableitet, deren Einsatz für einfache und mittlere Formen der Interaktion mit Nutzern und für Dienstleistungen verwendet werden können (Buhr 2015: 3). Automatisierung betrifft auch die Zuordnung von Daten und deren Verknüpfung auf Plattformen und Cloud-Systemen, auf deren Grundlagen Entscheidungen getroffen werden (Amoore und Raley 2016: 6).

Die Automatisierung lässt sich anhand von mehreren Punkten nachzeichnen. Dazu zählt die weitreichende Optimierung der Produktionsabläufe durch automatische Vernetzung von Informationen. Ein häufig zitierter Begriff für die informationsbasierte Automatisierung der Produktion ist die „Industrie 4.0“, dessen Merkmal ist, dass „(…) Werkstoffe und Maschinen (…) Wissen und Kenntnisse über ihre Identität und den Sinn und Zweck ihres Daseins“ erhalten (Krüger 2016: 6). Gemeint ist damit die vollständige Erfassung aller in der Produktion involvierten Elemente, von der vernetzten Produktionsstrecke bis zum Computerchip im Produkt zur Lokalisierung im Post-Produktionsstadium. Durch die Digitalisierung wurde die Verbindung der drei Kernelemente der Industrie 4.0 ermöglichte: automatisierte Prozesse, virtualisierte Umgebungen und eine globale Vernetzung (Hammermann und Klös 2016: 3). In einem historischen Kontext kann sie als vierte Revolution der Industrie, als eine von wenigen großen Zäsuren der Produktionsbedingungen in der Neuzeit verstanden werden. Damit steht sie in einer Linie mit der vorindustrialisierten Mechanisierung, der tatsächlichen Industrialisierung durch die Dampfmaschine und die spätere Elektrifizierung (Castells 2010: 33), sowie die Automatisierung der Produktion durch Fließbänder und elektronische Steuerungselemente (Krüger 2016: 7). Die informationsgestützte Automatisierung erlaubt weitgehend selbstständig

arbeitende Produktionseinrichtungen, deren Abläufe vorgegebenen Parametern folgen und von Menschen lediglich als Überwachungsinstanz begleitet werden.[71]

Die (3) *Robotisierung* hingegen hat das Potential den Menschen in seiner Fähigkeit, besser gesagt in seinem bisherigen Monopol, zur Definition und Überwachung von Prozessen zu ersetzen.[72] Ein selbstlernendes Programm beispielsweise überprüft seine eigene Performanz und entwickelt eigenständig, das heißt die vorgegebenen Rahmenparameter des automatisierten Prozesses verlassende Lösungen zu einem Problem. Mithilfe einer derart gestalteten künstlichen Intelligenz (KI) gelingt es dem Menschen als erste Spezies ein artifizielles, selbst-referenzielles und -verbesserndes Werkzeug zu erschaffen. Eine eigenständig handelnde Maschine, die Rechenleistungen erbringen kann, welche die Fähigkeiten ihres Erschaffers übersteigen können (Lepping und Palzkil 2016: 20). Ein Werkzeug, das den Menschen auch in bisher ungeahnten Lebensbereichen unterstützen, aber auch substituieren kann. Denn jede Freisetzung einer Ressource durch technologische Innovation beherbergt auch das Potential die Einkommensquelle eines Individuums zu ersetzen (Eichhorst et. al. 2016: 6).

Die Grundlage der Robotisierung und im Besonderen die Leistungsfähigkeit einer KI basieren auf der Allokation von Informationen sowie deren selbstständiger Auswertung. Beispielsweise können Chat-Bots – das sind künstliche, humanoide Verhaltens- und Kommunikationsmuster nachahmende Programme - bereits heute den Erstkontakt mit Websitebesuchern oder an Informationsständen beispielsweise an Flughäfen übernehmen. Sie folgen entweder einem automatisierten Prozess probabilistischer Interaktionsmuster oder erschließen selbstständig den Gesprächsinhalt auf einer kognitiven Ebene (Abdul-Kader und Woods 2015: 72). Die KI kann trainiert werden, im richtigen Zeitpunkt Emotionalität in den Gesprächsverlauf einzubauen oder

[71] Die quantitativen Vorteile eines dergestalt konzipierten Produktionsprozesses liegen in der langfristigen Senkung der Betriebskosten und qualitativen Aspekten wie der Erhöhung der Planungs- und Kontrollstrukturen (Krüger 2016: 8). Rohstofflager, Transportsteuerung oder Lagerbestandorganisation können durch die flächendeckende Einführung von Nanochips und deren Erfassung in einem zentralen System optimiert werden und den Wettbewerbsvorteil eines Unternehmens durch gesteigerte Effizienz begründen und zu Wachstumspotentialen beitragen (Hettich, Schimmer und Müller-Stewens 2015: 55).

[72] Die Robotisierung grenzt sich vom ursprünglichen Begriffssinn des Automaten oder einer mechanischen Maschinenkonstruktion ab und umfasst die selbstlernende, künstliche Intelligenz. Diese benötigt allerdings keinen maschinellen Körper, wie der Terminus „Roboter“ suggeriert. Die Geschichte des „Automaten“, eines gedanklichen und technischen Vorläufers, reicht mehr als 200 Jahre zurück. Auch in kultureller Hinsicht fand die Faszination am künstlichen Menschen, einem Roboter der zumindest im Erscheinungsbild einen Menschen imitieren konnte großen Anklang, beispielsweise in den Werken der Romantik wie in E.T.A Hoffmans Geschichte „Der Sandmann“ (Hoffmann 1819). In unserem Kontext beziffert die Robotisierung den Übergang von unterstützenden Leistungen künstlicher Intelligenz hin zu selbst-lernenden und -verantwortlichen Maschinen, deren Einsatz auch Einfluss auf die Beschaffenheit des Arbeitsumfeldes hat (Arnold et. al. 2016: 5). Der mittelfristig von Computerprogrammen und Maschinen bedrohte Anteil an Arbeitsplätzen ist signifikant. Von manchen wird dieser Anteil auf bis zu 42 Prozent geschätzt (Eichhorst et. al. 2016: 6), auch wenn Arbeitsplätze – und das ist die andere Seite der Entwicklung – neu entstehen und die Verluste kompensieren (Krabel 2016: 104).

die Gefühlswelt und *natürlichen* Reaktionen einer realen Person zu simulieren (Hill, Ford und Farreras 2015: 249). Zum Einsatz können solche Chatbots auch in Partnerbörsen oder als Ansprechpartner für Kundenfrage kommen, doch ihr ökonomisches Potential ist noch lange nicht ausgereizt[73], ebenso wie der potentiale Abbau von Arbeitsplätzen in Call Centern, Hotelrezeptionen oder den meisten skalierbaren Dienstleistungsberufen, deren Arbeit auf Informationsaustausch beruht (Krabel 2016: 101). Ein Bot muss nach initialer Entwicklung nur auf die spezifische Umgebung konfiguriert werden. Er wird nicht krank, unterliegt keiner personellen Fluktuation und kennt kein Arbeitszeitschutzgesetz.

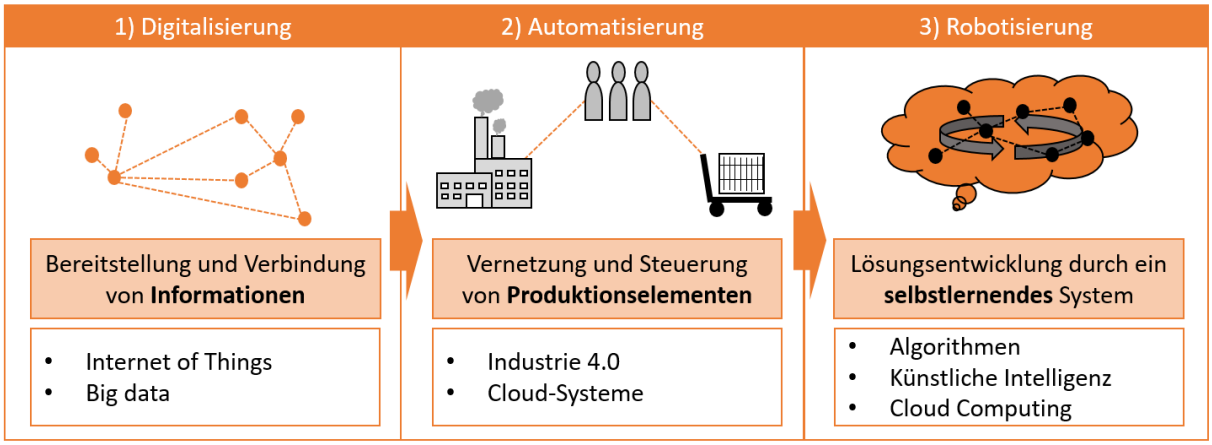

Abb. 3.1. Digitalisierung, Automatisierung und Robotisierung. Eigene Darstellung.

Mithilfe der Digitalisierung als Vorbedingung, sowie der Automatisierung und Robotisierung als Anwendungswerkzeuge in den analogen Raum hinein, basiert das Phänomen des Cyberzeitalters auf der Verknüpfung von Informationen. Ein Leitbegriff der Mehrwertschaffung aus einzelnen Datensätzen ist (4) *Big Data*, das allokierte und konzeptualisierte Wissenskollektiv, das mithilfe von Referenzen Verhaltensprädiktionen schafft.[74] Big Data bedeutet komplexe Nutzerinformationen, die auf einer umfassenden Akquise und Verbindung von Datensätzen beruhen, zu analysieren und einem konkreten Anwendungsbereich zuzuführen (Hettich, Schimmer und Müller-Stewens 2015: 56). Die Erkenntnisse können etwa für das strategische und operative Marketing verwendet werden, bei der Entwicklung von Produkten oder bei der Bewertung der Zahlungsverlässlichkeit von Kunden zum Einsatz kommen. Stimmungsbilder und Tendenzen in der Bevölkerung können ebenso online ausgelesen werden, als auch Rezeptionen von Ideen und Ereignissen (Amoore

[73] Diese Fähigkeit kann ebenso für kriminelle Zwecke missbraucht werden, beispielswiese können Chatbots oder automatisierte Anfragen genutzt werden um Systeme zu infiltrieren (Huber et. al. 2009: 121) oder für betrügerische Zwecke in sozialen Medien oder Partnerbörsen eingesetzt werden, um sensible Daten in Erfahrung zu bringen (Riekmann und Kraus 2015: 299).

[74] Big Data wird als ein zentrales Element der Digitalisierung mit einem großen Wachstumspotential (McKinsey 2011: 8). Wir werden diesen Aspekt weiter unten im Abschnitt 3.2.2 im Detail betrachtet.

2016: 15). Dieses Anwendungsfeld erstreckt sich über traditionelle, produktionsbasierte Branchen wie der Automobilbranche, tangiert aber auch vermehrt dienstleistungsorientierte Wirtschaftszweige. In der Medizin etwa beginnt Big Data ebenso Einzug zu nehmen und erlaubt den Einstieg in ein IT-zentriertes Behandlungssystem, dessen Hoffnungen auf der Steigerung von Anamnese- und Therapieerfolgen sowie der Kosteneffizienz beruht (Gigerenzer, Schlegel-Matthies und Wagner, 2016: 24). Allerdings gilt dazu die Voraussetzung, dass es gelingt, „die großen, heterogenen und sich schnell ändernden Datenmengen im richtigen Kontext und mit der passenden Methodik zur Datenanalyse einzusetzen“ (Dwertmann und Schürholz 2016: 168). Denn Daten sind nicht sofort gleichbedeutend mit Wissen und Informationsbausteine ergeben isoliert betrachtet noch keine gesicherte Erkenntnis über Kundenverhalten oder den Behandlungserfolg.

Big Data ist hingegen vielmehr ein Anwendungs- und Experimentierfeld der Wissensallokation. Erst die Masse und Kontextualisierung der singulären Informationen erschafft den komplementären Nutzen. Dies kann aber auch eine große Gefahr für den Individualismus und den Schutz der Privatsphäre bedeuten. Die Überwachung einer Person durch die Sicherheitsorgane des Staates sollte daher auch für die digitale Sphäre stets den Anforderungskriterien des Rechtsstaats unterliegen (Amoore und Raley 2016: 4). Ebenso eröffnet sich ein Potential für betrügerische Handlungen (vgl. Borges et. al. 2011; Willems 2012), wie wir im sechsten Kapitel aufzeigen werden. Die Informationsallokation im Internet basiert jedoch zumeist auf freiwilliger Preisgabe der Informationen, schließlich stimmen Nutzer den Geschäftsbedingungen zumeist implizit oder explizit beim Gebrauch zu. Die einzelne Information vermag – so die Logik - kaum Nutzen zu versprechen und ihre Freigabe erscheint unbedenklich. Doch die Bündelung vieler einzelner Daten bedeutet mehr als nur die Summe vieler Einzelteile. Big Data ermöglicht eben diesen Einblick in ein zusammenhängendes Bild über Nutzer und erlaubt die Vorhersage von Handlungen oder sogar deren potentielle Initiierung (Amoore und Raley 2016: 2). Die Freiheit und (scheinbare) Anonymität des Wissenszugangs im Internet geht ebenso mit einer Protokollierung des Nutzungsverhaltens einher. Diesem Spannungsverhältnis werden wir uns ebenfalls später im Detail widmen.[75]

Im Informationszeitalter werden selbst Daten außerhalb des Monitorbildschirms erfasst. Der Begriff des (5) *Internet of Things* (IoT) beschreibt diese umfassende Vernetzung von Gegenständen des alltäglichen Gebrauchs, vom intelligenten Auto bis zum inventarführenden

[75] Die Diskrepanz zwischen Vorteilen der Informationsspeicherung im digitalen Zeitalter und den individuellen Persönlichkeitsrechten und der Hoheit über Informationen im Berufs- und Privatleben werden wir im Abschnitt 3.2.5 genauer beleuchten.

Kühlschrank, vom Lichtschalter bis zur digitalen Körperwaage. Das IoT sammelt diese Daten und erstellt ein Profil des Benutzers. „Smart metering“[76] beispielsweise sammelt und sendet Angaben des häuslichen Stromzählers an den Energieanbieter (Neumann, Moorfeld und Reulke 2016: 143). So kann die Deutsche Telekom heute beispielsweise auf das größte Repertoire[77] an Energienutzungsdaten in Deutschland zurückgreifen (Hettich, Schimmer und Müller-Stewens 2015: 58). Gleichzeitig eröffnet der intelligente Zähler Gefahren für die Privatsphäre des Nutzers, so können die gesammelten Daten auch unerlaubt Aufschluss über das Nutzungsverhalten in Haushalten geben (Neumann, Moorfeld und Reulke 2016: 148). Anwesenheitszeiten und Routinen der Hausbewohner lassen sich durch deren Stromkonsum nachzeichnen. Ein Hackerangriff auf die vernetzten Stromzähler könnte zudem die Energieversorgung unterbrechen, da diese Geräte einfache Angriffsplattformen darstellen (Müller 2011: 547). Dieses Beispiel ist nur eines von vielen Anwendungsfeldern des „Internet of Things“, dessen Schnittstellenportfolio beständig wächst, allerdings die Sicherheitseinstellungen der eingesetzten Geräte oder Software mit dieser Entwicklung häufig nicht Schritt halten können.[78]

Aufbauend auf den gesammelten und vernetzten Daten erlaubt das (6) *Cloud Computing* eine Kontextualisierung, Auswertung und Steuerung der Informationen im Sinne computergestützter Analyse- und Entscheidungsprozesse. Die Cloud bezeichnet eine konturschwache, weil weitreichende und interaktive Plattform, auf der Rohdaten gespeichert und ausgewertet werden (Armbrust et. al. 2010: 50). Ihren Informationsgehalt erfährt das Cloud-System durch die hier stattfindenden Verarbeitungs- und Veredelungsprozesse durch Algorithmen und selbstlernende Programme, welche aus den Rohdaten verwertbare und aufschlussfähige Informationen formen (Bratton 2015: 116ff.). Als solche offeriert Cloud Computing neben anderen Angeboten drei wesentliche Dienstleistungen, deren Services von Konzernen oder Privatpersonen gegen Gebühr genutzt werden können ohne sich die investitionsreiche Infrastruktur der Cloud leisten zu müssen.[79] Die drei zentralen

[76] Die grundlegende Motivation zur Einführung von vernetzten Stromzählern, den „Smart Meters“, war es die Manipulation des analogen Stromzählers zu verhindern und das Nutzungsverhalten der Stromabnehmer zu analysieren (Müller 2011: 548).

[77] Die Dateneinspeisungen erfolgen zwar durch die intelligenten Stromzähler oder Regulierungssysteme auf dem Smartphones zur Fernsteuerung des heimischen Energieverbrauchs, verlaufen über die Leitungen und Server der Telekom (Neumann, Moorfeld und Reulke 2016: 147f.).

[78] Die Betrachtung der Schattenseiten wird im Abschnitt 3.3 sowie im Detail im sechsten Kapitel näher diskutiert. Das Beispiel der Überwachung und unerlaubten Einsicht in vertrauliche Informationen oder Konversationen zählt dabei ebenso zu den problematischen Aspekten der eingesetzten Technologie, wie die potentiellen Sicherheitslücken durch vernetzte Systeme ohne ein einheitliches Schutzkonzept.

[79] Die Cloud-Infrastruktur besteht aus Servern, Datenbanken und Applikationen, deren Zusammensetzung aufwendig und kostspielig ist (Armbrust et. al. 2010: 51). Diese Konstellation wird im Abschnitt 3.2.4 analysiert.

Dienstleistungen der Cloud sind die Nutzung der bereitgestellten Infrastruktur wie etwa der virtualisierten Server („Infrastructure as a Service“ – IaaS), der Plattformen zur Speicherung von Daten („Plattform as a Service“ – PaaS) oder die Nutzung von Applikationen in der Cloud („Software as a Servie“ - SaaS). Diese Dienstleistungen werden vorzugsweise in Kombination aller drei Elemente in Anspruch genommen, um den maximalen Nutzen aus der Datenanalyse generieren zu können (Amoore 2016: 5).

Als virtuelle Umgebung bietet die Cloud umfangreiche Möglichkeiten zur Skalierung und Flexibilität der Datennutzung. Ihre globale Verfügbarkeit macht sie für ihre Nutzer ebenso allgegenwärtig wie wenig greifbar[80], denn sie scheint nur durch die lokal gebundenen Elemente ihrer Infrastruktur in einem physikalisch-materiellen Sinn auf einer Karte zu verzeichnen sein (Velte, Velte und Elsenpeter 2010: 17). Die Plattformen der Clouds speichern die dezentral eingegebenen Daten ihrer Schnittstellen in einem höheren Aggregationszustand ab, welcher die Mehrwertschöpfung der Algorithmen und Applikationen möglich macht. Bratton beschreibt ihre Funktionsweise wiefolgt: „Platforms centralize and decentralize at once, drawing many actors into a common infrastructure. They distribute some forms of autonomy to the edges of its networks while also standardizing conditions of communications between them” (Bratton 2015: 46). In diesem Sinne ist Cloud-Computing das strukturierende Element der Informationsverwaltung im digitalen Zeitalter, das verbindende Glied vormals inhaltlich und räumlich separierter Wissensräume.

3.1.2. Informationen und Informationserzeugung

Die Auflösung räumlicher Beschränkungen und lokaler Wissensräume findet sich in den virtuellen Bibliotheken des Internets. Es bietet einerseits Zugang zu bestehenden Informationen oder von Nutzern kreierten Inhalten, wie beispielsweise auf selbst-erstellten HTML-Seiten, Foren, professionellen Web-Auftritten von Unternehmen oder in Enzyklopädien wie Wikipedia sowie anspruchsvoller Recherchedatenbanken. Eine elementare Notwendigkeit war und ist es, die Masse an verfügbaren Daten zu filtern und den Zugang in angemessener Zeit zu ermöglichen (Amoore und Piotukh 2015: 345). Ein bekanntes Beispiel der Steuerung von Wissensräumen im Informationszeitalter sind Suchmaschinen, welche auf der Grundlage von Suchbegriffen arbeiten. Das sind Parameter, welche dem gesuchten Datensatz eine bestimmte Eigenschaft zur Identifizierung von Dokumenten zuweisen. Intelligentere Suchmaschinen arbeiten auf der Grundlage vergangener Suchverläufe, entweder eigener oder der von anderen

[80] Der Aspekt der Räumlichkeit des Cloud Computing wird weiter unten diskutiert. Generell stellen Rechenzentren, Leitungen, Endgeräte oder Kühleinheiten für solche Hardware die analogen, lokalisierbaren Aspekte der Digitalisierung, ungeachtet der Anwendungsfelder in der analogen Welt dar (vgl. Bratton 2015: 23f.).

Nutzern, im Idealfall im Vergleich mit anderen Nutzern deren Verhalten im Internet dem des Suchenden entspricht (Lepping und Palzkil 2016: 19).

Suchmaschinen etablieren dabei eine nicht zu unterschätzende Machtposition[81] als zentraler Zugangspunkt neben sozialen Medien zur Steuerung von Informationsflüssen und Verbindung von Anfragen und verfügbaren Informationen (Buchholz und Wangler 2016: 179). Denn kaum jemand erinnert sich an die URL-Codes, also die Übersetzung der Internetadressen aus Zahlenreihen in semantisch mehr oder weniger verständliche Direktionen, sondern bedient sich der praktischen Dienste von Suchmaschinen, um sein Ziel im Netz zu finden (Bratton 2015: 198). Die problematische Situation für Unternehmen ergibt sich dadurch, dass sie einerseits auf die Selektion und Verknüpfung von Suchmaschinen angewiesen sind, um sich gegenüber anderen Unternehmen vorteilhaft zu platzieren. Andererseits bedeutet diese Abhängigkeit auch eine Erweiterung des Schutzbegriffes unternehmerischer Kontinuitätsplanung. Denn falls es eine Unterbrechung auf der Seite des Suchmaschinenbetreibers oder des Netzwerkes ergeben sollte, wäre der Schaden unmittelbar auch für das Unternehmen spürbar.

Der sichere Verbindungsaufbau zwischen Kunden und Unternehmen, ebenso zwischen anderen Interaktionspartnern wie Zulieferer, stellt eine Grundvoraussetzung der unternehmerischen Sicherheitsbereitstellung dar. Doch in diesem Fall sind Entscheidungsträger und Infrastrukturen außerhalb der eigenen systemischen Grenzen notwendig, um die Reproduktion von Prozessen sicherzustellen (vgl. Luhmann 1991: 202). Dadurch erweitern sich der Organisationsbegriff und auch die sicherheitsrelevante Betrachtung von Unternehmen und den benötigten Ressourcen, einschließlich anderer Unternehmen und ihrer technologischen Infrastruktur. Diesen Aspekt der Digitalisierung von Wissenserzeugung und Konnektivität werden wir aus organisationssoziologischer Sicht im vierten Kapitel im Detail besprechen.

Darüber hinaus erstreckt sich die Herausforderung für Unternehmen auch darüber, die Verknüpfung und Steuerung von verfügbaren Informationen sowohl effizient, als auch sicher zu gestalten. Eine unzureichende Definition und Implementierung von Systemprotokollen beziehungsweise die Einhaltung von Standards zur Datenablage können erhebliche Schwachstellen für die Sicherheit der internen Daten und damit für das Unternehmen selbst darstellen (Chigada und Madzinga 2021: 5). Im Informationszeitalter versprechen die Nutzung

[81] Unternehmen wie Google verfügen über das Potential mithilfe ihrer Algorithmen erheblichen Einfluss auf die Gesellschaft und deren Meinungsbildung, Konsumverhalten und Entscheidungen zu nehmen (Bratton 2015: 3). Die EU-Kommission verurteilte Google am 27. Juni 2017 zu einer Rekordstrafe von 2,43 Milliarden Euro, da das Unternehmen bei der Selektion seiner Suchtrefferliste allzu drastisch einzelne Anbieter bevorzugte und andere benachteiligte. Der Umfang der Benachteiligung sei so gravierend, dass diese in ihren Möglichkeiten der freien Angebotsplatzierung bei den Kunden eingeschränkt worden seien (Vgl. Spiegel Online 2017).

von Big Data und großflächige Vernetzung von Systemen einerseits Chancen für gewinnorientierte Unternehmen, doch bedeuten sie anderseits auch eine große Verantwortung. Denn die komplexe Herausforderung die akkumulierten Daten vor einer zunehmend professionalisierten und organisierten Cyberbedrohung zu schützen nimmt mit fortschreitender Vernetzung zu (Schulze 2021: 2). Um die Interaktionen und Interdependenzen der informationsbasierten Technologien besser zu verstehen und schließlich auch ihr Risikopotential für die unternehmensinterne Sicherheit darzulegen, werden im Folgenden einige der für unser Thema relevanten Aspekte der digitalen Strukturen erläutert.

3.2. Facetten der Digitalisierung

Aufbauend auf den zuvor eingeführten Schlüsselbegriffen, gilt es ein umfassendes Spektrum an Zusammenhängen zu benennen, um die Auswirkungen der Digitalisierung auf unternehmerische Entscheidungen, Strukturen und schließlich auch Sicherheitsproduktion verstehen zu können. Für unsere Fragestellung sind vorrangig jene Facetten der Digitalisierung von Interesse, welche die Funktions-, Produktions- und Autoreflexion von Unternehmen betreffen, um die Gründe für die Veränderungsprozesse zu verstehen, aber eben auch die potentiellen Risiken beleuchten zu können. Digitalisierung in diesem Kontext bedeutet vor allem die treibenden Elemente der Veränderung für Unternehmen zu beleuchten, welche sich unter den folgenden sechs Facetten der Digitalisierung analog zu Benjamin Brattons Beschreibung des „Stack“ subsumieren lassen.[82] Darunter zählt die Frage der Bedeutung von (1) Räumlichkeit im Informationszeitalter, welche durch die Virtualisierung von Informations- und Produktionskontexten einer lokalen Positionierung entzieht, gleichzeitig aber durch ihre technische Infrastruktur, der Hardware, an physikalischen Interaktionspunkten mit der analogen Welt zusammentrifft (Bratton 2015: 66). Diesen Zusammenhang, zwischen der räumlichen Entkoppelung des Informationstransfers und der fortwährenden Bindung an lokale Fixpunkte

[82] In seinem Werk “The Stack” präsentiert Benjamin Bratton ein Modell zur Beschreibung des tiefgreifenden Wandels des Informationszeitalters, das maßgeblich an der Cloud ausgerichtet ist. In seinem Modell finden sich sechs Ebenen, welche im gegenseitigen Austausch stehen. Diese umfassen „six interdependent layers: Earth, Cloud, City, Address, Interface, User.” (…) “Each is considered on its own terms and as a dependent layer within a larger architecture, and each is drafted from the superimposed image of the geographic and computational machines we now inhabit and the ones we might yet make” (Bratton 2015: 11). In dieser Arbeit wird auf Aspekte des “Stack” referenziert, insbesondere auf die lesenswerten Erörterungen über die Rolle von Räumlichkeit („Earth“), die Beschaffenheit der Cloud im Allgemeinen („Cloud“) oder der Nutzer („User“). Das Modell des „Stack“ als holistische Entität eignet sich jedoch nur bedingt zur Einordnung der Digitalisierung im Blickfeld unserer Untersuchung der Rollen und Bedeutungsverschiebung des erweiterten Risiko- und Resilienzbegriffs im Cyberzeitalter, da die hier vorliegende Untersuchung einen anderen Schwerpunkt setzt.

gilt es zu beleuchten, da es essentielle Bedeutung für die Betrachtung der unternehmensspezifischen Auffassung im Sinne seiner Schutzziele hat.[83]

Der zweite Aspekt soll die Rolle von Informationen, insbesondere von (2) Big Data für die Entwicklung und den Vertrieb von Produkten und Dienstleistungen thematisieren. Als wesentliche Voraussetzung für die nachfolgenden Elemente der digitalen Wertschöpfungskette ist das Verständnis der Akquise und Archivierung von großen Datenmengen wichtig, um die Analyse und Auswertung der Daten durch (3) Algorithmen und selbstlernender Programme (KI) zu ermöglichen. Die technische Infrastruktur für deren Betrieb wird schließlich durch die Cloud bereitgestellt, deren virtualisierte Plattformen den Rahmen für die effiziente Einbindung der Datensammlung und deren Auswertung bieten. Der Betrieb der (4) Cloud, in der Summe ihrer Möglichkeiten als Cloud Computing zu verstehen, ermöglicht Unternehmen eine ungeahnte Hebelwirkung für die Effizienz und Profitabilitätssteigerung ihrer Prozesse zu erzielen (Armbrust et. al. 2010: 50), insbesondere unter Ausnutzung der Serviceangebote spezialisierter Anbieter (IaaS, PaaS oder SaaS). Doch gerade diese Innovation in der Cloud-verarbeitenden Auswertung von Informationen steht für die Ambivalenz der Digitalisierung, in welcher wertschöpferisches Potential auf der einen Seite signifikanten Sicherheitsrisiken auf der anderen Seite gegenüberstehen, wie in den nächsten Kapiteln zu konkretisieren sein wird.

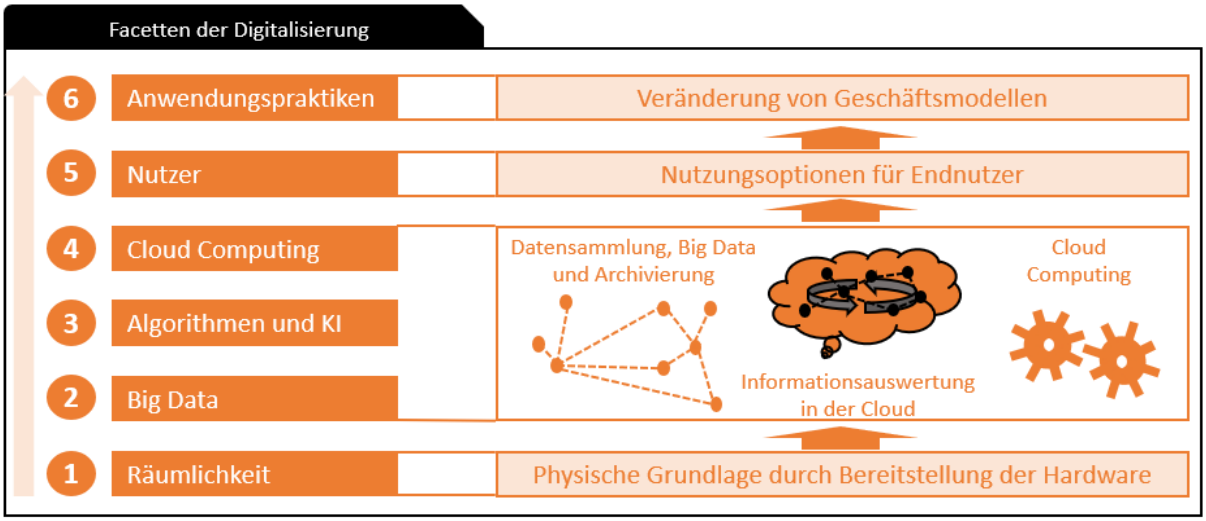

Abb. 3.2. Facetten der Digitalisierung und Einordnung der nachfolgenden Abschnitte. Eigene Darstellung, aufbauend auf dem Modell von Benjamin Bratton (Bratton 2015).

[83] Der räumliche Aspekt einer für vitale Ressourcen wie der Cloud-Infrastruktur ist für die Definition einer Wiederherstellungsstrategie von großer Bedeutung, da diese unter Berücksichtigung einer lokalen Risikoanalyse erarbeitet werden. Beispielsweise ist das Risiko eines Schadens für ein Rechenzentrum lokal zu betrachten, wenn man an Schadensursachen wie Naturkatastrophen oder Feuer denkt. Eine Einordnung der Cyberrisiken, wie Malwareattacken ist hingegen im globalen Kontext zu sehen, insbesondere im Fall des Cloud Computing.

Ebenfalls ist die Ebene der (5) Nutzer durch den Zugriff auf Dienstleistungen und Produkte von der Digitalisierung betroffen. In diesem Abschnitt wird die individuelle IT-Kompetenz – das heißt die Fähigkeit den Umgang mit den neuen Technologien zu erlernen und die Rolle der Nutzer als Konsumenten und Inhaltsschaffende beleuchtet werden. Schließlich wird am Beispiel des Gesundheitswesens eine konkrete (6) Anwendungspraktik vorgestellt werden, welche die Folgen der digitalen Veränderung für das Verhältnis zwischen Informationen und Dienstleistung aufzeigen und in den Kontext sicherheitsrelevanter Überlegungen setzen wird. Dieses Beispiel wurde gewählt, da insbesondere Unternehmen im Gesundheitswesen sich im Zuge der Corona-Pandemie mit signifikanten Sicherheitsrisiken konfrontiert sahen, aber zeitgleich ihre sensiblen Daten im Branchendurchschnitt nur im unzureichenden Maße durch Schutzmaßnahmen abgesichert waren (Dochow 2022: 105). Dieses Beispiel soll auch zeigen, wie die digitalen und analogen Sphären ineinandergreifen und mithilfe von Big Data, Algorithmen, Cloud Computing beziehungsweise der Interaktionen mit der Nutzerebene durch neue Anwendungspraktiken zusammenwirken. Beginnen wir mit der Rolle von Informationen im Kontext von Räumlichkeit.

3.2.1. Informationen und Räumlichkeit

Die Geschichte der weltweiten Verknüpfung von Warenströmen, Kommunikation und Migration reicht weit in die Vergangenheit zurück. Geographische Gegebenheiten wie Berge, Flüsse, Wüsten oder Ozeane definierten Kultur-, Handels- und Sprachräume, verhalfen Staaten zu ihren Grenzen und dominierten die Grundzüge politischer Strategien (Marshall 2017). Die Industrialisierung und die durch sie bereitgestellten Möglichkeiten der technologischen Innovation verringerten die Entfernungen und Hindernisse der Geographie, wenn sie auch stets wahrnehmbar blieben. Der Dampfantrieb revolutionierte den Personen- und Warenverkehr auf den Meeren und zu Lande und die Fortschritte in der Kommunikationstechnologie ermöglichten den Austausch von (begrenzten) Informationen über Kontinente hinweg.[84]

[84] Der Übergang in das Industriezeitalter veränderte zudem die Sozialstrukturen der Gesellschaften und schuf auch eine neuartige soziale Globalität. Diese zeigte sich in der Verbindung von Personen, welche nicht über eine gemeinsame Sprache oder Religion begründet wurde, sondern über die Klassenzugehörigkeit, ein soziales Produkt der industrialisierten Arbeitsbedingungen. Die Erfahrung vergleichbarer Lebensbedingungen, die nun unabhängig von anderen sozialen Differenzierungsmerkmalen, wie sie beispielsweise in Form der Religion über Jahrhunderte fortwährte, ein Gefühl der Verbundenheit erzeugte, verhalf in vielen wenngleich nicht allen Fällen zur Solidarität. Es zeichnen sich jedoch erneute Veränderungen der Sozialbeziehungen im Informationszeitalter ab: “But, if work, workers, and working classes exist and even expand around the world. The social relationships between capital and labor are profoundly transformed” (Castells 2010: 505). Die bisher gängigen Beziehungskonstellationen aus besitzender und arbeitender Sozialklasse, die Abhängigkeit der Beschäftigung und darüber hinaus die Perzeption der Solidaritätsgemeinschaft klassischer Prägung unterliegt einem Wandel durch die technologische Innovation, welche dem Individuum arbeitsbezogene Alternativen und Artikulationsmöglichkeiten bietet.

Wie wir gesehen haben, verändert die Digitalisierung die Verfügbarkeit und die Bereitstellung von Informationen. Dies gelingt vorrangig über die Überwindung der Ortsgebundenheit analoger Wissensträger wie Bücher oder Personen durch die Übertragung des analogen Wissens in die digitale Sphäre. Die räumliche Dimension zwischen beiden Sphären wird als Cyberspace beschrieben, eine nicht-materialisierte Ebene zwischen Hardwarekomponenten und visualisierter Darstellung auf dem Endgerät (Cavelty 2013: 107). Durch den Übergang zwischen beiden Bereichen verändert sich die Verfügbarkeit der Informationen schlagartig. Die Entkoppelung des lokalen Bezugspunkts ist ein entscheidendes Kriterium der Digitalisierung von Informationen und virtualisiert Informationen, deren Ursprung lokal verhaftet ist. Eine Information kann an einem Ort in das digitale Netz eingespeist werden und an anderen Orten der Welt ausgelesen werden. Dadurch verliert der Begriff von Räumlichkeit an Bedeutung, allerdings mit drei Einschränkungen: Beginnend mit der semantischen Unterscheidung, dass unser (1) Sprachgebrauch weiterhin das Internet als digitalen Raum interpretiert und somit das Konzept der Räumlichkeit auf den originär raumlosen Bereich der Virtualität überträgt. Dies scheint die logische Konsequenz der subjektiven Wahrnehmung zu sein, so wird doch die jeweils verwendete Information an einem *Ort* abgelegt (Velte, Velte und Elsenpeter 2010: 17). Dieser Ort, ob nun eine Festplatte, ein mobiles Endgerät oder eine Partitionszuweisung in einer virtualisierten Umgebung sind Orte der Zuschreibung, wenn auch fallabhängig mehr oder weniger mit einer physikalischen Adresse. Dennoch ist der Speicherort die Navigationshilfe zur Orientierung im digitalen Netzwerk und relevant zum Auffinden der relevanten Information.

Eine zweite Einschränkung betrifft die essentielle Rolle der zum Einsatz kommenden (2) Hardware. Benjamin Brattons Feststellung, dass „[t]he Cloud is not virtual; it is physical even if it is not always 'on the ground', even when it is deep underground" (Bratton 2015: 29), pointiert die Ambivalenz der digitalen Sphäre in ihrer Abgrenzung zum analogen Bereich. Die Grundlage der Digitalisierung ist eine physikalische Infrastruktur, die Raum, Energie und Rohstoffe beansprucht. Die wichtigsten Elemente der weltumspannenden Netzwerke sind die – physikalischen oder virtuellen – Server, welche in Rechenzentren unterschiedlichster Größe und Konstruktionsweise[85] den Kreislauf der Informationszirkulation ermöglichen und am Leben erhalten. Die lokale, natürliche Beschaffenheit ist für die Einrichtung von energieabhängigen Rechenzentren ebenso von Bedeutung wie die jeweiligen ökonomischen

[85] Wir werden im Abschnitt 2.2.4 erneut darauf zurückkommen. Rechenzentren können unterschiedliche Gestalt, Ausmaße und Verwendungszwecke haben. Von transportablen Einheiten, deren Aufbau in einen einzuschiffenden Standardcontainer passt (Amoore 2016: 6), bis hin zu kreativen Lösungsansätzen natürliche Umgebungen für den Bedarf der Hardware einzusetzen, wie etwa ausgediente Raketensilos oder Bergwerksstollen (Bratton 2015: 71f.).

Rahmenfaktoren der jeweiligen Jurisdiktion, Steuersätze und Verfügbarkeit von Mitarbeitern (Amoore 2016: 6). Ferner erstrecken sich die Datenkabel und Knotenpunkte der drahtlosen Kommunikation, die Arterien und Venen dieser Netzwerke durch Meere, Wüsten und Ballungsräume.[86] Die globale Konnektivität des Informationszeitalters kennt in Form von Kupfer- oder Glasfaserkabeln, sowie den seltenen Erden zur Herstellung der mobilen Endgeräte auch die Notwendigkeit zur Förderung von Rohstoffen (Bratton 2015: 28), zusätzlich zu den benötigten Energiequellen. Diese Materialien finden sich im Boden der analogen Welt und haben ihrerseits Auswirkungen auf die geopolitische Perspektive auf die Landkarten der globalen Prospektion.[87]

Das Netzwerk selbst steht in enger Verbindung mit der räumlichen Disposition, seit die Ausbreitung von interagierenden Systemen in den 1990er Jahren die dezentralen Microcomputer in ein vernetztes System aus einer steigenden Zahl an Betriebsplattformen in Rechenzentren einleitete (Castells 2010: 51). Gleichzeitig vermehrte die Marktdurchdringung von Personal Computers (PC) und später der vielzähligen mobilen Endgerättypen die Rezipienten der Netzwerkinhalte, beziehungsweise ermöglichte die dezentrale Einspielung eigener Informationen in dieses System. Die Masse an Informationen mit räumlichen Zusatzinformationen, beispielsweise die der eingewählten Funkzelle oder die Lokation eines Digitalfotos zum Zeitpunkt der Aufnahme in Form von Georeferenzen etablieren eine neue digitale Geografie, die Amoore als „geography of the cloud“ bezeichnet und die dazu beiträgt „to map and to make perceptible the geography of our world in particular ways” (Amoore 2016: 3). Was mit der Erdung der Hardware der Cloud seinen Anfang nimmt, trifft in Form des Nutzers auf einen physikalischen, geografisch bestimmbaren Abnehmer der Information, welcher eventuell auch selbst Inhaltsschaffender über die Tastatur seines Endgerätes ist. Der diffuse, kaum in sichtbare Konturen zu materialisierende Raum zwischen den analogen Fixpunkten ist die digitale Sphäre in der die Cloud operiert. Dieser Bereich ist allerdings in vielerlei Hinsicht durch keine starre Membran abgegrenzt, sondern erlaubt den fließenden Austausch in einem zunehmenden Prozess der Verschmelzung. [88]

[86] Etwa 95% der weltweiten Kommunikation verläuft durch etwa 1 Million Kilometer Kabel auf dem Grund der Meere (Bratton 2015: 94). Eine erstaunliche Zentrierung des vitalen Datenaustausches im Informationszeitalter, gemessen an der elementaren Bedeutung des ununterbrochenen Flusses von Informationen.

[87] Die weltweite Verfügbarkeit von bestimmten Materialen wie Kobalt oder seltenen Erden ist limitiert und bestimmt die politischen Geschicke der diese beheimateten Regionen, einschließlich kriegerischer Auseinandersetzungen wie in Zentralafrika, in der die involvierten Akteure großes Interesse an der Ausbeutung dieser Ressourcen haben (Marshall 2017: 140).

[88] Bereits im 19. Jahrhundert attestierten Beobachter die Aufhebung der Räumlichkeit, als die Eisenbahn und die Dampfschifffahrt Distanzen relativierten und damit Lebenswelten massiv veränderten. Die entstehende Eisenbahnindustrie etwa hatte große Auswirkung auf die Produktion von Stahl und Maschinen und verhalf

Denn das Zusammenwachsen der analogen und der digitalen Welt bedeutet an ihren Schnittstellen auch einen Wirkungszusammenhang zwischen beiden Sphären. Ereignisse im Cyberraum können Konsequenzen in der analogen Umwelt haben und umgekehrt. Diese Wirkungsweisen können sich weltweit ereignen und sollten Bestandteil einer Risikoanalyse im unternehmerischen Kontext sein. Denn Daten und Befehle können um den Globus zirkulieren und Endgeräte an beinahe jedem beliebigen Ort adressieren. Die Lokalisierung eines Rechenzentrums an einem bestimmten Ort limitiert dessen Risikoexposition, beispielsweise für Hackerangriffe nicht nur auf dessen unmittelbare räumliche Umgebung, sondern artikuliert vielmehr eine dynamische Interdependenz seiner Schnittstellen (Cerullo und Cerullo 2004: 75f.). Der virtuelle Raum des Cyberspace ist daher kein abgesteckter, lokal definierter Ort, sondern eine Artikulationshilfe der Interaktions- und Kommunikationssphären, welche sich durch das Internet und die technologische Weiterentwicklung der Schnittstellen zur analogen Welt geöffnet haben.[89]

Eine dritte Einschränkung gilt der generellen Möglichkeit im digitalen Wirtschaftsraum andere (3) Märkte zu erschließen ohne eine tatsächliche Präsenz vor Ort aufbauen zu müssen.[90] Lokale Regulationen, Steuervor- oder Nachteile und die Möglichkeiten zur Datenspeicherung im Besonderen können standortspezifische Ausschlusskriterien darstellen, für deren Umsetzung Akteure aus dem analogen Raum, namentlich staatliche Behörden, verantwortlich sind (Castells 2010: 280). Somit sind Dienstleistungsangebote in lokal geschützten Räumen zwar möglich,

---

Regionen wie dem Ruhrgebiet zum rasanten Wachstum. Die meisten Mitglieder des sich entwickelten Industrieproletariats hingegen profitierten kaum von dieser Entwicklung und konkurrierten um unzureichend bezahlte Arbeitsplätze (Osterhammel 2010: 235f.). Allerdings boten die althergebrachten Erwerbstätigkeiten im ländlichen Raum aufgrund des Bevölkerungswachstums im 19. Jahrhundert nicht mehr ausreichend Möglichkeiten für alle Kinder einer Familie und die legalen Veränderungen wie beispielsweise die „Bauernbefreiung" begünstigten die innerstaatliche Migration weiter. Die Folge war eine fortgesetzte Migrationsbewegung in die industrialisierten Ballungsgebiete. Im Unterschied dazu sind im digitalen Zeitalter weniger nationalstaatliche Organe oder Unternehmen an der Umgestaltung der Welt beteiligt (Walter: 2008: 8). Da die maßgeblichen Internetkonzerne eigenständig agieren, entwickelt sich ein dynamischer, dezentralisierter und vor allem entnationalisierter Prozess der Veränderung. Die ist auch ein Grund für die äußerst geringen Transaktionskosten der Digitalisierung.

[89] Über das globale Kommunikationsnetzwerk können Informationen und Arbeitsanweisungen verteilt und empfangen werden und selbst der Arbeitsplatz im wachsenden digitalen Arbeitsmarkt muss nicht mehr aufgesucht werden. Dadurch verlieren Distanzen und auch Zeit an der besonderen Bedeutung, welche sie über Jahrhunderte hatten. Barrieren und Entfernungen werden durch die digitale Kommunikation annihiliert. Auch andere Kommunikationshürden wie Sprachbarrieren könnten in Zukunft durch leistungsfähige Übersetzungstools abgebaut werden. Dennoch bleibt eine „digital Spaltung" relevant, welche in eine Welt unterscheidet, in der die zuvor genannten Freiheiten und Möglichkeiten für deren Bewohner gelten und eine andere Sphäre, in der die Verlierer und Unbeteiligten der digitalen Revolution beheimatet sind. „Das Internet ist also nicht global (…), [e]s ist allerdings fast vollständig globalisiert, denn es kennt keine nationalstaatlichen Grenzen" (Walter: 2008: 7f.).

[90] Eine Einschränkung könnte hierbei die jeweils unterschiedlichen Datenschutzregelungen der politisch definierten Wirtschaftsräume sein. Datentransfer in und aus den USA heraus gestalten sich durch den Patriot Act als schwierig (Velte, Velte und Elsenpeter 2010: 26) und auch andere Märkte wie beispielsweise China setzen bestimmte Spielregeln auf, wie beispielsweise den Zugang zu sozialen Medien, die Eröffnung von (analogen oder digitalen) Vertriebsstrukturen oder dem Verbot des Handels von Kryptowährungen, wie zum Beispiel Bitcoin..

aber stellenweise Anpassungsdruck aufgrund der jeweiligen Jurisdiktion ausgesetzt, wie beispielsweise die Versuche des Personentransportwesens in Deutschland das Geschäftsmodell von Uber mit rechtlichen Schritten zu unterbinden (Krabel 2016: 101).

Ein weiterer Aspekt von Räumlichkeit ist die Lokalisierung von IT-Kompetenz und Kapazitätsnutzung. Ein Ort der sinnbildlich für den digitalen Wandel steht ist Palo Alto in Kalifornien[91], um den sich die Internetkonzerne wie Facebook und Google, aber auch Start-ups und jene ansiedeln, die gerne zu den Großen der Branche aufschließen würden. Dieser Standort symbolisiert die unternehmerische Seite des Informationszeitalters und materialisiert in gewisser Hinsicht eine überraschende, ausnehmende Ortsungebundenheit des Internets. Ähnlich, aber deutlich schneller als im Fall der Industrialisierung verbreitet sich das Wissen um die Reproduktion und sogar Innovation der neuen Technologien um den Globus. Interessanteweise überschneiden sich viele metropolitane Standorte der Industrialisierung mit den Schaffenszentren des digitalen Wandels (Castells 2010: 66). Widmen wir uns nun einer der elementaren Grundlagen des Informationszeitalters selbst, den kontextualisierten Daten und ihrer Bedeutung für die neue digitale Wirtschaft.

3.2.2. Von Informationsbruchteilen zu Big Data

Informationen sind zunächst Rohdaten und waren schon lange vor dem Anbruch des Informationszeitalters von großer Bedeutung (Dwertmann und Schürholz 2016: 169). Der Unterschied entsteht durch die systematisierte Erfassung, Kategorisierung und Auswertung der Daten, in dessen Folge entwickelten sich Informationen zu den elementaren Wertobjekten der Digitalisierung (Castells 2010: 21). Vor diesem Hintergrund nimmt der Begriff Big Data eine herausgehobene Bedeutung ein, welche auf seiner deskriptiven Aussagekraft für das außerordentliche Potential der Verknüpfung und Kontextualisierung von singulären Datensätzen zu einem großen Bild beruht. Dieses lässt sich mithilfe von Sortierungs- und Auswertungsanwendungen, den Algorithmen, in wirtschaftliches Kapital umwandeln und ist eine der derzeit signifikantesten Erscheinungsformen der Digitalisierung (Amoore und Piotukh 2015: 344).

Big Data bezeichnet die konsequente Erhebung und Auswertung von Informationen oder besser gesagt Verhaltensmustern und potentiellen Präferenzen (Hettich, Schimmer und Müller-

[91] Die Entwicklung des Standortes wurde durch mehrere Faktoren begünstigt, darunter die Förderung durch die US-Regierung in Form von Subventionen, die Nähe zur Stanford Universität und der San Francisco Bay Area als wohlhabender Metropolregion. Diese Bedingungen schufen eines der bedeutendsten Zentren der Digitalisierung, was Manuel Castells zu der Aussage bewegte: „“If the first industrial revolution was British, the first information technology revolution was American, with a Californian inclination” (Castells 2010: 61f.).

Stewens 2015: 58). Die Verfügbarkeit einzelner Datensätze verspricht allerdings noch keinen Erfolg, sondern die systematische Erfassung von einer signifikanten Anzahl an Daten, welche Rückschlüsse auf einzelne und kollektive Interessen und Präferenzen zulassen (Amoore und Raley 2016: 2). Daten werden in den meisten Fällen durch Interaktionshandlungen der Nutzer mit einem an das Internet angeschlossenes Endgerät erhoben, also mit jeder Suchanfrage, Bewertung von Filmen oder dem wiederholten Abspielen einer Playlist.[92] Auch andere Endgeräte, wie beispielsweise die Fernsteuerung von Waschmaschine und Heizung über das Smartphone oder das vernetzte Fahrzeug liefern eben jenen Input, welcher die Datenspeicher von Big Data füllen. Informationen sind allerdings in erster Instanz Rohmaterialien (Castells 2010: 70), deren Quantität zwar mehr als ausreichend vorhanden ist, doch qualitative und mehrwertschaffende Schlussfolgerungen damit nicht automatisch gewonnen sind (Heinrich et. al. 2016: 51).

In der zweiten Dekade des 21. Jahrhunderts existieren vielfältige Schnittstellen zwischen der analogen Lebenswelt und der digitalen Sphäre (Gigerenzer, Schlegel-Matthies und Wagner, 2016: 12). Im Jahr 2015 wurde die Zahl der internetfähigen Geräte auf 15 Milliarden Einheiten weltweit geschätzt (Heinrich et. al. 2016: 53). Fünf Jahre später wurde diese Schätzung bereits auf ungefähr 30 Milliarden Geräte im weltweiten Einsatz angehoben und könnte sich innerhalb von fünf weiteren Jahren erneut verdoppeln[93] Schätzungen des deutschen Bundeswirtschaftsministeriums gehen bis 2030 sogar von bis zu 500 Milliarden Geräten mit einer Schnittstellenfunktion zum Internet aus.[94] Ein beindruckendes Potential der globalen Vernetzung und eine deutliche Tendenz hinsichtlich der zunehmenden Verfügbarkeit von Datensätzen (Bratton 2015: 112). Diese Vielzahl an Schnittstellen und Systemkomponenten wird uns im fünften Kapitel erneut begegnen, wenn wir über die Sicherheitslücken und potentiellen Krisenszenarien zu sprechen kommen, welche als Schattenseite der verknüpften und automatisiert erfassten Daten in Erscheinung tritt.

[92] Ein Beispiel für das Potential von Big Data bietet der amerikanische Streaming-Dienst Netflix. Das Unternehmen begann als regulärer Videoverleih, doch sicherte er sich ein damals profitables Nischensegment durch die Verfügbarkeitsstellung von Filmen und Serien über das Internet (Streaming). Die Kunden konnten im Rahmen eines Abonnements bequem von zuhause cineastische Unterhaltung auswählen. Seinen rasanten Aufstieg verdankt Netflix aber der konsequenten Analyse der Erwartungen und Präferenzen seiner Kunden. Teurere und damit riskante Eigenproduktionen, die sonst als Alleinstellungsmerkmale den großen Studios und Privatsendern vorbehalten waren, konnte der Konzern produzieren, weil ihm die Erwartungen der Kunden an Serien und Filme aus dem Streaming eingängig bekannt waren (Hettich, Schimmer und Müller-Stewens 2015: 56). Dank Big Data konnte das Unternehmen in vergleichsweise kurzer Zeit in einen Markt einsteigen, welcher für Dekaden von etablierten Akteuren dominiert wurde.

[93] Vgl. Bundesministerium für Bildung und Forschung 2021.

[94] Vgl. Bundesministerium für Wirtschaft 2016.

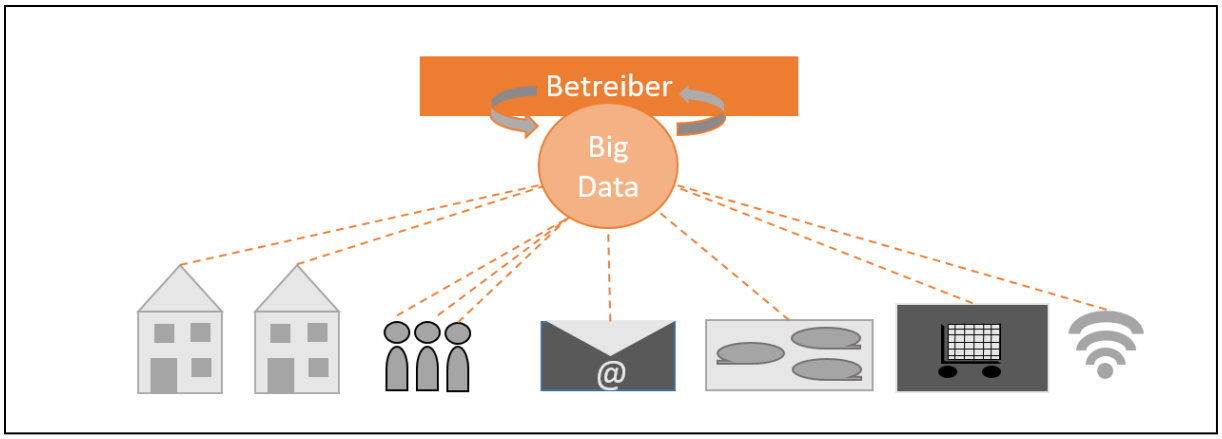

Abb. 3.3. Bezugsquellen von Informationen durch Big Data, welche über das heimische oder Gast-Wlan, Nachrichten, Social Media, Postings oder Einkäufe im Internet Daten sammelt. Eigene Darstellung.

Für Unternehmen bedeutet Big Data vorrangig ein strategisches Element für ihre Produktplatzierung, Marketing, Produktionsoptimierung, Kundenservice und als Grundlage für Unternehmensentscheidungen.[95] Im englischen Sprachraum wird die Kombination aus gesteigertem „volume, variety, velocity, [und] veracity" verwendet, um die Skalierung und Bedeutung von Big Data als umfassende Datenallokation zu beschreiben (Amoore und Piotukh 2015: 344). Während beispielsweise im Jahr 2012 mehr als 900 Millionen Personen ein Profil auf Facebook unterhielten und etwa 100 Millionen Nachrichten täglich über soziale Medien versendeten (Utz, Schultz und Glocka 2012: 40), stieg die Zahl der Facebook-Accounts Im Jahr 2017 auf mehr als 2 Milliarden an (Statista 2018). Die über diese Accounts und Schnittstellen erhobenen Daten sind von großem Wert, denn sie sind bereits personalisiert, das heißt einem digitalen Profil zugeordnet und dadurch für Werbe- oder Analysezwecke der potentiellen Kunden einsetzbar.[96] Big Data repräsentiert dabei den rasant wachsenden Bedarf, sowie die Verfügbarkeit von Informationen im digitalen Zeitalter.

Im Jahr 2018 werden etwa sechseinhalb Zettabytes an Daten auf den privaten und öffentlichen Datenbanken des Planeten abgespeichert sein, das sind 10^{21} Byte (Bratton 2015: 117). Andere Quellen gehen von bis zu 16 Zettabytes aus, manche Schätzungen sagen bis 2025 sogar 160 Zettabytes voraus (Statista 2018b). Zur Verdeutlichung: Ein Byte beschreibt die notwendigen Informationen zur Darstellung eines Schriftzeichens. Ein Film in HD-Qualität schlägt mit

[95] Bratton merkt zu Endgeräten an: "Just as your mobile is not really so much a 'phone' anymore (…), the Google mobile apparatus should be understood less as a car than, as said, as a car-shaped end device within a larger Cloud platform. It is a robotic device that a person gets inside and which carries her around" (Bratton 2015: 281).

[96] Das Geschäftsmodell von Unternehmen wie Facebook basiert auf einer direkten Verbindung zum Privatleben seiner Nutzer und deren Interesse an dem (digitalen) Leben von anderen. „Its reserve currency is what the theory of symbolic interactionism in sociology calls the 'presentation of self-identity'" (Bratton 2015: 125). Das Interesse von Facebook gilt der massenhaften Erzeugung von Inhalten und Bewertungen, welche Rückschlüsse auf die Vorlieben ihrer Nutzer zulässt.

mindestens 1 Gigabyte zu Buche, folglich 10^6 Bytes. Das gesamte Angebot an Spielfilm das der Streaming-Dienst Netflix im Jahr 2016 in den USA anbot nahm zum Vergleich etwa $4{,}1^{12}$ Byte an Speicherplatz ein (Statista 2018c). Diese digitalen Datenberge sind das Herz von Big Data (Conway 2010: 62). Mehr Daten sind aber nicht zwangsläufig immer besser, vielmehr ist es die sinnvolle Auswertung der gesammelten Datensätze notwendig, welche einen Vorteil durch Selektion, Abstraktion und Kontextualisieurng versprechen (Dwertmann und Schürholz 2016: 172). Auch gibt es technische Einschränkungen in der unkontrollierten Skalierung der Datenflut. Die Bandbreiten der Verbindungen sind in technischer und ökonomischer Hinsicht endlich. Dies bedeutet zuvorderst, dass Informationen selektiert werden müssen, bevor sie übermittelt werden (Hettich, Schimmer und Müller-Stewens 2015: 58). Denn das Ziel von Big Data ist es nicht Daten als Selbstzweck zu sammeln, sondern in profitable Anwendungsmodelle zu überführen.[97]

Im Jahr 2016 wurden zum Beispiel alleine in Deutschland 1,4 Milliarden Euro Umsatz nur mit Big Data als Wirtschaftsgut erwirtschaftet, das bedeutet mit der Erfassung, Reduktion und Weitergabe von Daten (BMWi 2016), allerdings exklusive indirekte Absätze und Vorteile durch gezieltes Marketing. Somit bleibt festzuhalten, dass „[w]hat characterizes the current technological revolution is not the centrality of knowledge and information, but the application of such knowledge and information to knowledge generation and information processing/communication devices, in a cumulative feedback loop between innovation and the uses of innovation" (Castells 2010: 31). Dies verdeutlicht das ökonomische Potential von Big Data, allerdings ebenso die Gefahr mittelfristig in Abhängigkeit von Technologiekonzernen zu geraten, beziehungsweise langfristig die Marktposition zu verlieren, falls Unternehmen wie Google. Facebook oder Amazon Big Data einsetzen um neue Wirtschaftszweige zu erschließen.

Dennoch folgt die Erhebung von Daten, insbesondere über das „Internet of Things"[98] einer beindruckenden und zugleich besorgniserregenden Geschwindigkeit, da Informationen zunächst gesammelt werden – stellenweise bevor ihr möglicher Einsatz geklärt ist. Die

[97] Die Überlastung der Kommunikationsverbindung zwischen Milliarden von Endgeräten und deren Servern kann beispielsweise verhindert werden und die Unmengen an Speicherplatz auf Clouds für potentialreiche Daten gewahrt bleiben. Viele Geräte mit Sprachsteuerung werden beispielsweise mithilfe eines Druckknopfs aktiviert, um nicht permanent die Umwelt aufzuzeichnen, was zu einen permanenten Datenstrom führen würde, welcher zumindest gegenwärtig nicht zu verarbeiten wäre (Heinrich et. al. 2016: 54).

[98] Das Internet of Things bezeichnet den Zusammenschluss von Endgeräten, welche Rohdaten in ihrer Umgebung oder einem zugewiesenen Operationsrahmen erfassen, beispielsweise Smart Meter oder Internet-fähige Lichtschalter. Big Data umfasst hingegen alle im digitalen oder analogen Umfeld erhobenen Daten, welche in einen Kontext und personalisierbaren oder zumindest spezifizierbaren Rahmen kategorisiert wurden. Das Problem beider Arten der Datenerfassung und Katalogisierung ist die Zunahme und aus Sicherheitssicht unzureichende Einbindung neuer Schnittstellen von Hard- und Software in Sicherheitskonzepte (McGuire 2015: 46f.).

Innovationszyklen drehen sich im Hypertempo und die Frage ist zu stellen, ob die vorherrschenden Sicherheitsstandards dieser Entwicklung gerecht werden können. Für das Internet of Things gilt, dass ‚innovation in this area is happening very quickly, but the security is a step behind. (…) [T]o be effective, security must be built into products as they are being developed, not 'bolted on' later" (McGuire 2015: 47). Tatsächlich finden viele Sicherheitspakete erst nachträglich ihren Eingang in Hard- und Softwareprodukte. Diesem Aspekt werden wir uns im fünften Kapitel daher im Detail zuwenden.

Hier ist hervorzuheben, dass Big Data die größte Ansammlung an Daten in der Geschichte darstellt (Bratton 2015: 117). Denn Informationen selbst entwickelten sich im Informationszeitalter zu einem Wirtschaftsgut, dessen Attraktivität sowohl für legale Geschäftsinteressen als auch für kriminelle Absichten in der jüngsten Vergangenheit stark angewachsen ist (Fisher 2013: 217). Daneben kann der Schutz der digitalen Persönlichkeit auch Gegenstand von Dienstleistungen werden und ein gewinnbringendes Element von Geschäftsmodellinnovationen sein (Walter 2008: 19). Die „(…) Ende-zu-Ende-Verschlüsselung des Kommunikationsdienstes WhatsApp zeigt, dass Datenschutz auch Bestandteil einer Marketingstrategie sein kann" (Buchholz und Wangler 2016: 181). Ähnlich verhält es sich mit neuen Kommunikationsnetzwerken und Identifikationstechnologien wie der Blockchain, welche in Zukunft eine Alternative für sensible Transaktionskommunikation wie den klassischen Geldtransfer darstellen könnte.[99]

Zusammenfassend betrachtet, stehen Unternehmen mit Big Data ein enormer Wissensschatz zur Disposition, dessen Absicherung gegen Missbrauch (in diesem Kontext insbesondere durch Dritte) aber ebenfalls ein vitales Interesse darstellt, um am Markt Bestand haben zu können, denn der Wesensgehalt dieser Informationsansammlungen ist bedeutender als jemals zuvor.

[99] Anstelle eines einzelnen, zentralen Programms, welche den Vorgang steuert, reguliert lediglich ein auf mehrere, um genau zu sein zwingend allen teilnehmenden Einzelkomponenten verteiltes Regelwerk die Rahmenbedingungen für die Transaktionen und dazu notwendigen Kommunikationsstandards. Dadurch erlangt das System seine Sicherheit und zugleich einen Vertrauensnachweis über die Lauterkeit des zumeist anonymen Interaktionspartners (Barmert et. al. 2013). Denn wenn die Sicherheitsprotokolle an einem Element geändert werden, verlässt dieses automatisch die Transaktionsgemeinschaft, da die Blockchain nicht mehr mit der mehrheitlich geteilten Referenzquelle kompatibel ist. Daher müsste das gesamte Netzwerk simultan angegriffen werden, welches sich aber per Definition als dezentrales System einerseits zu schützen versteht und andererseits eine enorme Rechenleistung für einen solchen Angriff voraussetzen würde, der gegenwärtig nicht vorstellbar ist. Vgl. Caspar Dohmen: Bezahlsystem Bitcoin. Wie die digitale Währung funktioniert. Deutschlandfunk. Zuletzt aufgerufen am 27.06.2017 unter: http://www.deutschlandfunk.de/bezahlsystem-bitcoin-wie-die-digitale-waehrung-funktioniert.724.de.html?dram:article_id=389484. Daher spricht man von einem Netz von Einzelrechnern, dass sich auf eine gemeinsame Kommunikationsbasis einigt, indem einzelne Nutzer das gemeinschaftliche, dauerhaft fixierte Regelgrundbuch akzeptieren (Kharraz et. al. 2015: 17). Das Novum ist, dass diese Aufgabe nun auch von einem nicht-staatlichen Netzwerk bestehend aus singulären Akteuren in ihrem Alleinstellungsmerkmal herausgefordert wird (Bornholdt und Sneppen 2014: 1).

Wir wollen den Gedanken an dieser Stelle verlassen und später in fünften Kapitel erneut aufgreifen. Zunächst gilt es die Auswertungsmechaniken der gesammelten Daten durch Algorithmen und selbstlernende Programme genauer zu betrachten, durch deren Einsatz der Wert der gesammelten Informationen zu erklären ist.

3.2.3. Künstliche Intelligenz und Algorithmen

Wenn man Informationen mit Vokabeln vergleicht, dann entsprechen die Algorithmen der Grammatik. Erst durch die Klassifizierung, Einordnung und Zusammenstellung der steigenden Masse an Informationen wird ein Mehrwert in Form einer anwendbaren Datenanalyse ermöglicht. "[W]here an image of interest is extracted from a whole, data analytics are instruments of perception: they carve out images, reduce heterogeneous objects to a homogeneous space, and stitch together qualitatively different things such that attributes can be rendered quantifiable" (Amoore und Piotukh 2015: 346). Die von Milliarden von Endgeräten gelieferten Billionen von Datensätzen können auf einer Plattform wie beispielsweise der Cloud effizient ausgewertet werden, denn erst die Verbilligung des Cloud Computing ermöglichte die profitable Konzeption dieser Datenfabriken (Bratton 2015: 116). Bevor wir auf die Cloud im nächsten Abschnitt im Detail eingehen, wollen wir zunächst auf die Rolle von Algorithmen und selbstlernenden Programmen zur Auswertung der Informationen zu sprechen kommen. Denn sie sind die Anwendungen zur effizienten Datenanalyse und ermöglichen erst einen Erkenntnisgewinn aus den Zettabyte an Informationen, welche die Leistungsfähigkeit des Menschen bei Weitem überfordern würden.[100]

Die großen Allokationen von Datenmassen, welche als Resultat der Vernetzung zur Verfügung stehen, verhelfen (selbstlernenden) Algorithmen zum Erfolg, welche insbesondere in Form der künstlichen Intelligenz in vielen Lebensbereichen zum Einsatz kommen können (Amoore und Raley 2016: 4). Künstliche Intelligenz kann mithilfe der zur Verfügung stehenden Datensätzen Regeln und Abweichungen erkennen, welche es Programmen wiederum erlauben sollen aus den Informationen der Vergangenheit auf zukünftige Ereignisse schließen zu können. Diese Prognose auf der Grundlage von gesammelten Daten erlaubt es dem Algorithmus eigenständige Entscheidungen zu treffen (Lepping und Palzkil 2016: 20). Beide Systeme, der Algorithmus und auch die höher entwickelte selbstlernende KI benötigen zunächst ein klares Verständnis der verwendeten Daten, schließlich muss das Programm zu verstehen lernen, zwischen

[100] Amoore und Piotukh halten diesbezüglich zwei Aspekte der Innovation fest, welche die Bedeutung von Big Data einordnen: "First, big data pushes at the limits of traditional relational databases as tables of rows and columns, and requires new ways of querying and leveraging data for analysis, in addition to the structured query language (SQL) built for relational databases in the 1970s. (…) Second, big data is big to the extent that it exceeds and changes human capacities to read and make sense of it" (Amoore und Piotukh 2015: 345).

unterschiedlichen Inhalten differenzieren zu können. Eine simple Textsuche kann beispielsweise herausfinden wie oft ein Unternehmensname in Presseveröffentlichungen innerhalb eines Monats genannt wurde und durchsucht Texte nach dem vorgegebenen Suchnamen (Roark, Saraclar und Collins 2007: 372). Wesentlich interessanter wäre jedoch die Frage in welchem Kontext das Unternehmen in Fachartikeln, Kommentarspalten und Referenzen erwähnt wurde. Zu diesem Zweck muss der Algorithmus die Semantik und den Zusammenhang der Nennung betrachten und eine positive oder negative Konnotation feststellen können. Dies wäre ein Beispiel für ein lernendes Programm, welches mit jedem interpretierten Textpassus lernt die Aussagen der Nutzer einzuordnen.[101]

Das Onlinewarenhaus Amazon stand beispielsweise vor der Aufgabe die mittlerweile hunderte Millionen von Artikeln in seinem Sortiment zu identifizieren und treffende Lieferzeiten zu prognostizieren. Daher entwickelte das Unternehmen seine eigene Anwendung zur Objektidentifizierung und Katalogisierung, den „Amazon Standard Identifier" (Bratton 2015: 131). Mit dessen Hilfe gelingt es dem Onlineshop Angebot, Käuferanfragen, Lieferzeit und Anweisungen an das nächste Logistikzentrum zu koordinieren.[102] Anwendungen wie diese erlaubten den Zusammenschluss von einzelnen Datensätzen zu komplexen Netzwerken, deren Informationen effizient verwaltet und prozessiert werden konnten (Castells 2010: 51). Als deren Konsequenz ermöglichten erst die Algorithmen wie die Mustererkennung („pattern recognition"), Wahrscheinlichkeitsmodellierungen („n-gram modelling") und Querabfragen innerhalb von Plattformen eine sinnvolle, anwendungsorientierte Sichtung der digitalen Informationen (Amoore und Raley 2016: 2). Die richtige Klassifizierung der Information in einem bestimmten Kontext basiert zudem auf der korrekten Adresszuordnung. Diese dient der eindeutigen Identifizierung, gewissermaßen die Identität einer Information, denn je eindeutiger ein Datensatz[103] einem Nutzerprofil oder einer Bezugsquelle wie einem Kommentar über ein Unternehmen zugewiesen werden kann, desto größer fällt die Aussagekraft des Ergebnisses ins

[101] Wahrscheinlichkeitsmodellierungen wie die sogenannte n-gram-Modellierung basieren auf der Aufteilung eines Textes in Fragmente, beispielsweise Silben und der anschließenden Auswertung der Wahrscheinlichkeit, welche Silbe (Fragment) als nächstes folgen wird. Somit können Algorithmen für die Aufgabe trainiert werden Texte von menschlichen Nutzern zu sichten und innerhalb eines probabilistischen Modells auszuwerten (Roark, Saraclar und Collins 2007: 373).

[102] Ihre Analysefähigkeiten steigen dabei dramatisch: „Algorithms increasingly have the capacity to analyse across different forms of data (images, text, video, audio) and across cloud-based spatial locations of data. (…) [T]he historical significance of the increased use of generative machine learning algorithms cannot be overstated" (Amoore und Raley 2016: 4).

[103] Eine CMDB-Datenbank (Configuration Management Data Base) hat beispielsweise den Namen einer Applikation als „Libary_1" abgespeichert, basierend auf dem Routinekonfigurationsimport. Gleichzeitig findet sich die von einem Nutzer manuell eingetragene Anwendung „Libary_01". Auch wenn der Nutzer die gleiche Anwendung meinte, referenziert nun jede weitere Verknüpfung von Datensätzen auf unterschiedliche Ziele, weil beide Anwendungen verschiedene, aber für das System jeweils eindeutige Identifikationstitel tragen.

Gewicht (Bratton 2015: 193). Problematisch erscheint es indes, wenn die künstlichen Algorithmen auch Entscheidungen automatisch treffen und kommunizieren,[104] wie dies beispielsweise im Hochfrequenz-Trading (Amoore und Piotukh 2015: 22) oder im Fall von Krediteinschätzungen durch Algorithmen geschieht (Mühlbauer 2018). Gleiches gilt für Unternehmen, die sensible Daten an Algorithmen freigeben und potentielle Sicherheitsrisiken unterschätzen, beispielweise dass die Zugriffsrechte des Programms eigentlich abgeschottete Datenbereiche tangieren können. Diese unbemerkten Nebeneffekte einer Vernetzung und Ausweitung der Zugänglichkeit von Daten durch den Einsatz von Algorithmen können zu unerwarteten Sicherheitslücken und damit Risiken evolvieren. Diese werden wir insbesondere im fünften Kapitel aufgreifen. Zunächst widmen wir uns der Virtualisierung von Informationen, Plattformen und Programmen, deren Kombination in der Cloud die Skalierung der neuen Technologien ermöglicht.

3.2.4. Virtualisierung in der Cloud

Beim Cloud Computing handelt es sich wie eingangs eingeleitet um die Bereitstellung von Speicherplatz auf einer virtuellen Umgebung, sowie der Nutzung von Anwendungen, die im virtuellen Raum anstatt auf einem physischen Endgerät laufen. Die Vorteile liegen vor allem in der globalen Verfügbarkeit der Daten, der Geschwindigkeit der Datenverarbeitung und der Verknüpfung von Informationen auf einer gemeinsamen Plattform (Velte, Velte und Elsenpeter 2010: 6). In der Cloud verweben sich Hardware und Software miteinander und ermöglichen bemerkenswerte Leistungsangebote mit Blick auf Performanz und Datenanreicherung. “Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services” (Armbrust et. al. 2010: 50). Die Cloud ist eine der wichtigsten technologischen Anwendungen, derer sich Unternehmen aktuell bedienen können, um die Vielzahl an Informationen und komplexen Softwarelösungen in ihren Organisationen zu steuern (Bratton 2015: 94). Wir werden uns im Folgenden ansehen, welche Chancen sich in ökonomischer Hinsicht durch die Cloud-

[104] Dies betrifft etwa sensible Lebensbereiche wie im Pflegedienst oder in der Strafverfolgung. Denn die zugrundeliegenden Datensätze bilden die maßgeblichen Quellen für Entscheidungen der Maschine. Informationen können Fehler enthalten, welche selbst den Programmieren des Systems unbekannt sind, könnten statistische Fehler enthalten oder diskriminierende Aspekte reproduzieren. Zwar können Algorithmen über eine entsprechende Sensorik und Rückkoppelungsfunktion die Auswirkungen ihrer Entscheidung überprüfen, aber gerade in Situationen, welche ein hohes Maß an sozialer Kompetenz erfordern, kann sich dies als eine unzureichende Qualitätssicherung herausstellen. Deshalb ist eine sorgfältige Auswahl der Datengrundlage für selbstlernende Algorithmen unverzichtbar und eine kritische Auseinandersetzung mit den Folgen des Kompetenztransfers zu Gunsten von Maschinen beständig zu erinnern. Denn die Abhängigkeit von diesen Informationen birgt die Gefahr, soziale Diskriminierungen oder Fehler zu reproduzieren.

Technologie eröffnen, aber auch potentiellen Risiken betrachten,[105] welche durch den Einsatz der Cloud entstehen können.

Zwei Veränderungen verhalfen dem Cloud Computing zum Durchbruch. Zum Einem bewirkte der Transfer von Informationen in eine primär digitale Aggregationsform einen entscheidenden Anreiz Daten effizienter zu verwalten und für virtuelle Wertschöpfungsketten zu verwenden (Castells 2010: 31f.). Die dadurch gestiegenen Initial- und Betriebskosten ließen ein eigenes Rechenzentrum jedoch mit der Zeit unrentabel erscheinen, während gleichzeitig das Preisleistungsverhältnis von professionellen Cloud-Anbietern interessanter wurden (Armbrust et. al. 2010: 52). Zum Zweiten entsteht durch die allgegenwärtige Datenerhebung (Internet of Things) eine zuvor kaum vorstellbare Menge an Informationen und damit Anforderungen an Speicherplatz und geeignete Auslese- beziehungsweise Verarbeitungsprozesse (Heinrich et. al. 2016: 51). Im Allgemeinen besteht eine Cloud-Lösung aus mindestens drei Elementen: einem oder mehreren Rechenzentren, diversen virtualisierten Servern und den Kunden, letztere in Form von Lieferanten und Nutzern der Daten (Velte, Velte und Elsenpeter 2010: 6). Dieser Liste sind noch die Plattformen („system layer“), sowie Datenbanken und Applikationen („business layer“) hinzuzufügen, über welche die eingespeisten Daten verwaltet und ausgewertet werden (Doelitzscher et. al. 2011: 26).

Die Cloud ermöglicht es die Daten in einen systemübergreifenden Kontext zu setzen, was eine Fähigkeit beschreibt zu der vorherige IT-Systeme in separierten Konfigurationsnetzwerken nicht in der Lage gewesen wären.[106] Man stelle sich ein international agierendes Unternehmen vor, dass Informationen aus seinen Landesgesellschaften auszuwerten gedenkt. Die singulären Systemkonfigurationen in den jeweiligen Subentitäten können sich mitunter stark unterscheiden und eine zentrale Auswertung der Daten erheblich erschweren, wenn nicht gar ausschließen. Die Cloud hingegen kann die jeweiligen Rechenzentren und

[105] Datenwiederherstellung („data recovery“) war in den 1990er und beginnenden 2000er Jahren fast ausschließlich durch die Spiegelung von Datenbankinhalten in einem zweiten Rechenzentrum möglich. Gegenwärtige Konzepte basieren zwar ebenfalls auf einem Ausweichkonzept, reduzieren aber die Kosten und vor allem Wiederherstellungszeit von Daten durch den Einsatz virtueller Server und Datenbanken, welche simultan in beiden Rechenzentren betrieben werden und nicht erst von einem physikalischen Server auf einen anderen umgeschaltet werden müssen (Jadeja und Modi 2012: 880). Wir werden uns mit dieser Materie im Detail im fünften und sechsten Kapitel auseinandersetzen.

[106] Es können drei Formen von Clouds unterschieden werden: Die (1) Private Cloud ist eine Plattform die ausschließlich von einem Nutzer betrieben wird, beispielsweise eine Eigenentwicklung eines Unternehmens oder einer Behörde zur Aufbewahrung sensibler Daten. Die (2) Public oder Community Cloud wird von einem Anbieter für mehrere Nutzer geöffnet, auf der Daten in unterschiedliche Datenbanken segmentiert werden können, aber zum Einem auf den Servern des Drittanbieters laufen und zum anderen im Falle einer Fehlkonfiguration oder Sicherheitslücke auch von anderen Nutzern eingesehen werden könnten. Die dritte Option ist eine (3) Hybrid Cloud, in der eine private Cloud in eine öffentliche eingebunden ist und bei Bedarf auf Rechenleistung des Drittanbieters in Anspruch nehmen kann (vgl. Jadeja und Modi 2012: 879).

Plattformadministration ersetzen und zusätzlich ein einheitliches Klassifikationssystem einführen, durch welches die Informationen nach standardisierten Berichten zur Verfügung gestellt werden können. Die Cloud unterstützt folglich die Zusammenführung von Datenmodellen und Plattformen und speist seine Attraktivität für Unternehmen aus seiner „ability to generate synergy on the basis of knowledge and information, directly related to industrial production and commercial applications" (Castells 2010: 67).

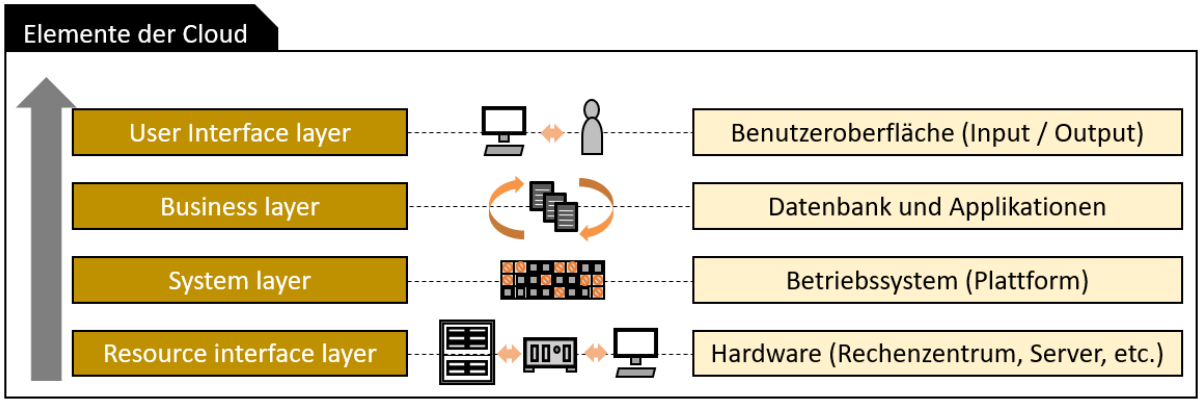

Abb. 3.4. Elemente der Cloud. Eigene Darstellung nach Doelitzscher et. al. 2011.

Durch ihren Aufbau bieten Cloud-Lösungen ihren Kunden zwei wesentliche Vorteile mit Bezug auf die Administration ihrer Daten an: erstens Speicherplatz in großen Mengen und zweitens anspruchsvolle Applikationen zur Filterung, Bearbeitung und der intelligenten Auswertung der gesammelten Daten. Anbieter von Clouds sind zudem in der Lage ihren Kunden Modelle zur Auswahl zu stellen, nach denen die Verrechnung der Dienstleistung variabel gestaltet werden kann, um Leistungsspitzen abzudecken, aber gleichzeitig auch im Fall einer geringeren Auslastung nur die in Anspruch genommene Kapazität zu bezahlen.[107] Die Skalierbarkeit der Cloud bietet dadurch den Vorteil der technischen Flexibilität, abhängig vom benötigten Leistungsumfang und den vertraglichen Spezifikationen.[108] Die „Echtzeitfähigkeit der

[107] Armbrust et. al. beschreiben die Variationsmöglichkeiten einer Cloud-Lösung: „Cloud computing lets an organization pay by the hour for computing resources, potentially leading to cost savings even if the hourly rate to rent a machine from a cloud provider is higher than the rate to own one. A second case is when demand is unknown in advance. For example, a Web startup will need to support a spike in demand when it becomes popular, followed potentially by a reduction once some visitors turn away" (Armbrust et. al. 2010: 52).

[108] Die inverse Logik, sprich diese Dienste bei Bedarf graduell abzubestellen, erscheint in unsichereren Zeiten eine besonders lohnenswerte Risikomitigation. Marktanteile und Datenmengen können innerhalb eines Jahres variieren, gravierender noch die technologische Weiterentwicklung, welche den Eigenbetrieb von Rechenzentren und Speicherplattformen teuer macht und gegebenenfalls dem Risiko der technischen Überholung aussetzt. Ein Beispiel für extreme Skalierbarkeit ist die „Google AppEngine", eine von Google zentral verwaltete Anwendungsplattform auf der Kunden Webbrowser-basierte Applikationen nutzen können, allerdings ohne größere Konfigurationen vornehmen zu können. Dieses Modell erlaubt es Google eine einmal entwickelte Software als Service über seine Cloud massenhaft zur Verfügung zu stellen, ohne spezifische Parameter der Kundenhardware in der Entwicklung berücksichtigen zu müssen (Armbrust et. al. 2010: 52). Für Unternehmen bietet sich hingegen die Möglichkeit nicht genutztes Potential wie beispielsweise nachts, in der Urlaubszeit, Semesterferien oder Spät-Saison – je nach Branche unterschiedlich - im Vertrag auszuschließen, und nur die

Datenreduktion“, welche an eine hohe Rechenleistung gebunden ist, stellt somit ein Anforderungskriterium und Leistungsmerkmal der Cloud dar (Heinrich et. al. 2016: 56). Denn im Gegensatz zu anderen Lösungen verfügen die virtuellen Server der Cloud über eine hohe Rechenleistung und Flexibilität dank skalierter Performanz. In der Cloud-Ökonomie trägt der Betreiber der Cloud das unternehmerische Risiko ungenutzter Kapazitäten und unternimmt die Vorkehrungen sowohl hinsichtlich der Leistungsfähigkeit der Cloud, ihrer Sicherheit als auch der technischen Innovation des Systems. Vor diesem Hintergrund erscheint die Cloud für Unternehmen aus wirtschaftlichen Gesichtspunkten lohnend, vergleicht man sie gegen die Entwicklungs-, Betriebs- und Innovationskosten einer eigenen technischen Lösung.

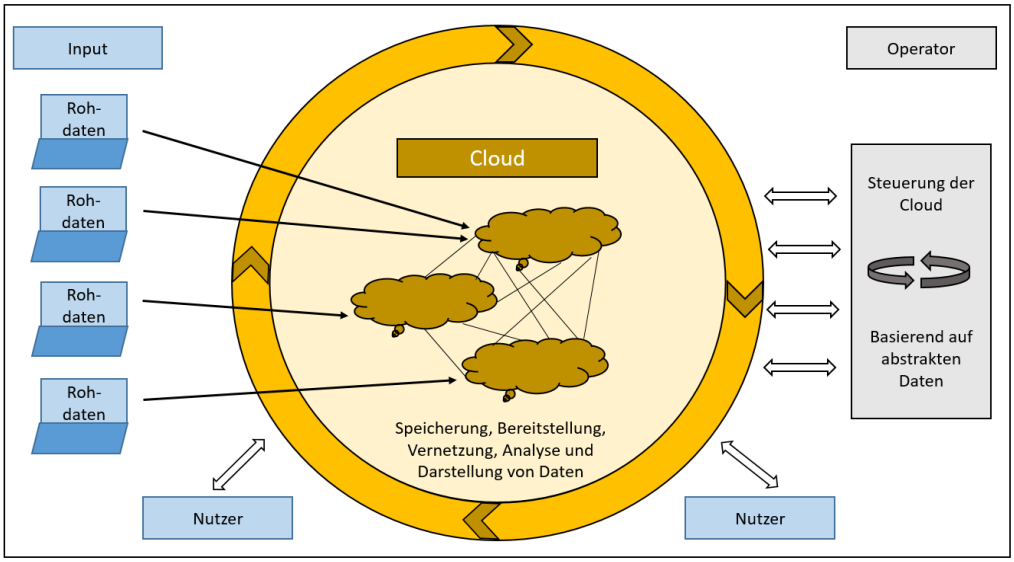

Abb. 3.5. Die Funktionsweise der Cloud. Eigene Darstellung basierend auf Heinrich et. al. 2016: 53.

Konzerne wie Google, Microsoft oder Amazon bieten mittlerweile eine Vielzahl an Dienstleistungen innerhalb der Cloud-Ökonomie an, welche mit dem ursprünglichen Geschäftsmodell auf den ersten Blick wenig gemeinsam haben.[109] Die Strategie der Cloud-Anbieter ist es möglichst viele Schnittstellen zu seinen Kunden und generell gesehen Daten zu konsolidieren.[110] Denn über möglichst viele Interaktionsschnittstellen zwischen Kunden und

tatsächlich genutzte Datenmenge oder Anwendungsleistung zu bezahlen, ohne jedoch den teuren Betrieb der Hardware tragen zu müssen (Doelitzscher et. al. 2011: 24).

[109]Amazon ergänzte nach erfolgreichen Erweiterungen seines ursprüngliches Warenangebots sein Angebot mit dem Abonnementdienst Prime in Form von exklusiven Lieferungskonditionen, einschließlich dem Zugriff auf das Musikstreaming und die Videodatenbank. Ferner zählen dazu eigene Hardwareproduktreihen, Serien und Filme. Ferner drängt der Konzern in die Paket- und Warenzustellung mit eigenen Lieferdiensten im Experimentalstadium (Drohnentransport) und plant die Eröffnung einer dezidierten Niederlassung zur Abholung von Produkten und versucht sich sogar im Lebensmittelhandel (Hettich, Schimmer und Müller-Stewens 2015: 55). Das große Geschäft macht Amazon hingegen als Anbieter von digitalen Dienstleistungen wie seinem Cloud-Service. Das Unternehmen ist heute mit Amazon EC2 neben Microsoft einer der größten Anbieter für Cloud-Infrastruktur (IaaS), Datenbankspeicherplatz (PaaS) und plattformbasierte Applikationen (SaaS) (Armbrust et. al. 2010: 52).

[110] Google verfolgt eine vergleichbare Strategie wie Amazon, indem es den Zugang zu Informationen mithilfe seiner Suchmaschine dirigiert. Zusätzliche Leistungen wie die Digitalisierung von Büchern - im wörtlichen Sinne

Anbieter entstehen wertvolle Informationsströme, die es den Dienstleistern ermöglichen ein Datenportfolio anzulegen und Verhaltensmuster von Kundengruppen zu erstellen. Denn „(…) [c]loud services costs no money for Users to use, but they are not exactly free; the company generates far more money in aggregate by optimizing attention and information that it costs them to provide those services" (Bratton 2015: 137). Die Cloud ist daher das geeignete Mittel für Unternehmen um möglichst viele Daten zu sammeln und eine entscheidende Position im Zugang zum globalen Wissen im Informationszeitalter einzunehmen.[111] Dies zeigt die enormen Erwartungen von Analysten, Investoren und privaten Aktienkäufern in das Geschäftsmodell der Internetkonzerne und Cloud-Anbieter (Castells 2010: 158). Der kalkulierte Wert der Marktkapitalisierung in dieser Branche beruht maßgeblich auf der Annahme, dass die vielen gesammelten Daten der Nutzer in ein geeignetes Anwendungsmodell überführt (oder verkauft) werden können (Velte, Velte und Elsenpeter 2010: 8). Allein der Wert der Aktien von Microsoft, Apple, Google, Amazon, dem chinesischen Onlinewarenhaus Alibaba und Facebook gemeinsam erreichten 2019 einen kulminierten Börsenwert von 4,4 Billionen US-Dollar[112] (Statista 2019)

Die Cloud fällt zudem durch zwei weitere Aspekte hinsichtlich ihrer Bedeutung für das Informationszeitalter und die ihr spezifische Risikoexposition auf. Erstens beruht die Cloud-Architektur auf einer umfangreichen Hardware-Infrastruktur, deren physikalische Präsenz neben dem Ursprungsort der erhobenen Daten, sowie dem Sitz des Cloud-Anbieters eine geografisch-räumliche Dimension verleiht.[113] Ebenso betrifft dies die lokale juristische

- füllen die Datenbanken von Google Books, welche als eine Art Onlinebibliothek mit Volltextsuchfunktion eine bemerkenswerte Literatursammlung darstellt. Diese Initiative beruht auf dem Unternehmensziel die Internetnutzer weiterhin über die Suchmaschinen zum gesuchten Ziel zu führen und als Mittler zwischen Information und Nutzer dessen Präferenzen zu erlernen. "Google's business model is based on attracting as many users as possible to its site by offering a far-reaching search engine" (Rieger 2008: 7). Auch Google expandiert in andere Bereiche und bietet neben Hardwareprodukten auch Internetbrowser („Google Chrome"), Cloud-gestützte Applikationen („Google Docs") und Betriebssoftware für Mobilfunkgeräte („Android") an. Hinter den einzelnen Angeboten steht die Cloud, das verbindende Element zwischen Infrastruktur, Plattform, Datenbank, Anwendungen und Nutzer. (Hettich, Schimmer und Müller-Stewens 2015: 60).

[111] Diese Strategie wird von den Beobachtern an den Aktienmärkten geteilt. Bereits 1999 wurde der Aktienwert von Amazon trotz eines wenig euphorisierenden Quartalsgewinns von nur 45 Millionen US-Dollar auf erstaunliche 25 Milliarden US-Dollar geschätzt. Zum Vergleich, der Gesamtwert der gehandelten Aktien in der Russischen Föderation wurden im gleichen Jahr auf 12 Milliarden US-Dollar beziffert. Einer der Gründe für den im historischen Rückblick Russlands niedrigen Wert, liegt in der Auslagerung von Kapital in zweistelliger Milliardenhöhe ins Ausland. "This is precisely the point of the observation: in the new financial world whatever makes market value only lasts as long as this value remains in the market" (Castells 2010: 158f.).

[112] Dieser Wert wurde allerdings durch die Probleme der Technologiekonzerne 2022 wieder drastisch reduziert. Die Entlassungswellen im Silicon Valley markieren daher eventuell eine Zäsur des bisher steilen Wachstums.

[113] Ein weiteres Beispiel wären schwimmende Rechenzentren, deren Aufenthalt in internationalen Gewässern die Frage der Jurisdiktion weiter verschärfen könnte: "Oceanic data centers theoretically would help solve this by using both tidal and wind energy to power the stations, as well as the abundant supply of water to assist in the cooling process, but in doing so, the literal offshoring of such critical infrastructure also raises issues about the jurisdiction and legal control of data and the governance of the emergent Cloud Polis" (Bratton 2015: 112).

Verantwortung, wenn beispielsweise die Daten französischer Kunden in einem Rechenzentrum in Sibirien gehostet werden, doch der Sitz des Unternehmens in Kalifornien liegt (Bratton 2015: 112). Ein weiterer Aspekt der Cloud-Infrastruktur ist ihr enormer Energiebedarf, welcher Anforderungen an die Standortauswahl der benötigten Hardware definiert.[114] Diese räumlichen Schnittstellen sind relevante Elemente welche in einer Risikobewertung vor Eingabe von Daten in eine Cloud geprüft werden sollten. Denn wie wir später im Abschnitt über Prozessauslagerungen und Outsourcing zu sprechen werden kommen, liegt die Verantwortung für die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen beim auslagernden Unternehmen (Schwering 2010: 231).

Zweitens ist eine der Stärken auch eine der größten Schwächen des Cloud Computing. Diese janusköpfige Ambivalenz liegt in der Verbindung von Ebenen und Komponenten in der Cloud, welche einerseits die Geschwindigkeit und Qualität der Datenverwaltung ermöglicht, aber andererseits ein Risiko für die Verfügbarkeit und Sicherheit der dort betriebenen Datenbanken und Anwendungen bedeutet. Diese Thematik werden wir ausführlich im fünften Kapitel diskutieren, aber es sei vorgemerkt, dass die grundsätzliche Problematik mit dem Konzept der Auslagerung von IT Operationen und Informationen an Dritte zusammenhängt, sowie der Durchlässigkeit von Segmenten innerhalb der Cloud. In beiden Fällen „sind die Sicherheitsvorkehrungen der jeweiligen Anbieter sowie die Sicherheit der Netzverbindungen zu diesen Anbietern zu hinterfragen“ (Gaycken und Krager 2011: 8). Die Vulnerabilität der Daten wird durch die Auslagerung signifikant erhöht, denn die Herausgabe, Übermittlung und Schnittstellenbedienung zwischen Unternehmen und Cloud bieten potentielle Einfallstore für (automatisierte) Angriffe (Borges et. al. 2011: 152).

Die Cloud selbst entzieht sich den Sicherheitsstandards des Unternehmens und kann nur mittels eines Outsourcing-Kontrollrahmens überwacht werden, also in Form von schriftlichen Zusicherungen des Sicherheitsniveaus und Zertifizierungen durch spezialisierte Anbieter (Bahli und Rivard 2003: 214). Dennoch obliegen die Verpflichtungen auf den Schultern des primär datenerhebenden Unternehmens, welches die Datennutzung mit dem Endkunden geregelt hat.

[114] Die gesamten Jahresemissionen von CO2 durch die weltweite Flugindustrie wurden bereits durch Rechenzentren eingeholt, bis 2020 werden diese voraussichtlich auf das Dreifache des aktuellen Ausstoßes ansteigen. Bis dahin wird der Energiebedarf der Clouds auf 1,9 Terawatt ansteigen, etwa 15 Prozent des weltweiten Energieverbrauchs, oder in anderen Worten, Cloud Computing würde zum fünftgrößten Elektrizitätskonsumenten aufsteigen (Bratton 2015: 92f.). Eine spezifische Computerarchitektur beispielsweise, welche Simulationen des Weltklimas durchführen könnte, würde im Ergebnis mit ihrer Infrastruktur die Fläche der Stadt Paris einnehmen und einen derartigen Energiebedarf aufweisen, „that it would be the single most significant anthropogenic climatic event that it itself would be modeling“ (Bratton 2015: 102). Dennoch ist anzumerken, dass die kulminierte Bilanz der Nutzung der Cloud energieeffizienter ausfällt als der Unterhalt vieler, dezentraler Einheiten, deren Kapazität bei gleichzeitigem Energieverbrauch beispielsweise nachts brachliegt (Jadeja und Modi 2012: 880).

Sensible Daten wie etwa Krankenversicherungsdaten (Vassilaki 2015: 28) oder mit rechtlichen Auflagen belegte Daten (EU-DSGVO 2016: 83) könnten die Nutzung einer öffentlichen Cloud a priori ausschließen (Velte, Velte und Elsenpeter 2010: 26). Diese Entscheidung über den Umgang mit dem spezifischen Risiko die Möglichkeiten des Cloud Computing zu nutzen inkludiert auch die Bewertung des zu erwartenden Schadens, maßgeblich das Vertrauensverlust seitens der Kunden. Daher wollen wir im Folgenden die Ebene der Nutzer betrachten, um die Interdependenzen zwischen Nutzerdaten und den virtuellen Wertschöpfungsketten von Unternehmen im Informationszeitalter zu verstehen.

3.2.5. Nutzer

Die Nutzerebene umschreibt den Bereich des Zusammentreffens von analoger und digitaler Sphäre, die Schnittstelle an der Informationen eingespeist und ausgelesen werden. Ein Nutzer generiert spezifische Informationen bewusst, aber wesentlich häufiger unbewusst über den Einsatz eines Endgerätes, beispielsweise über die Verwendung von IoT-Geräten, sozialen Medien, dem Abonnieren von Newsfeeds oder durch das frequentierte Aufsuchen bestimmter Webseiten. Diese Interaktionen sind die Mosaiksteine eines digitalen Profils[115]. Dies sind viele kleinen Bestandteile der digitalen Interaktion, die sich zu identitätsspezifischen Präferenzen zusammenführen lassen. Abstrakte Informationen, wie Klickzahlen können allerdings nicht einem bestimmten Profil zugeordnet werden. Unternehmen wie Facebook versuchen daher möglichst viele Informationen über die ihnen bekannten Profile zu identifizieren. Dazu werden Schnittstellen zu anderen Webseiten und Anwendungen[116] erstellt (Bratton 2015: 149).

Die Einbettung von Nutzern als Informationsschaffende erfolgt daher über die Bereitstellung von Dienstleistungen und Anwendungen, welche den Nutzern – häufig sogar kostenlose – Annehmlichkeiten zur Verfügung stellen. Der Entwicklungsprozess vieler Applikationen folgt allein diesem Ziel und ist eine Art der Anwendungspraktiken, um den Zugang zu effizient auswertbaren Informationen weiter auszubauen und mit dem neu gewonnen profunden Verständnis der Nutzerpräferenzen diesen wiederum interessante Angebote und Anwendungen zu offerieren. In diesem Kreislauf zeigt sich dass “[n]ew information technologies are not

[115]Das digitale Profil repräsentiert hier die analoge Identität einer Person oder Gruppe, die in Folge der Digitalisierung in den virtuellen Raum transzendiert ist und dort eine weitreichende Entscheidungsgewalt als Spiegelbild der Person etabliert, beispielsweise in Form von Meinungsäußerungen oder dem Abschluss von Verträgen über das Internet.

[116] Eine Möglichkeit der Verknüpfung ist die Anmeldung bei Applikationen wie beispielsweise Gesundheitsanwendungen, Bezahlsystemen oder Reiseportalen mithilfe des Facebook- oder etwa Google-Accounts. Diese Verbindung erlaubt die einfache Zuordnung von Klicks, besuchten Seiten und Interessensgebieten zu einem eindeutig identifizierten digitalen Profil. Daher versuchen Unternehmen möglichst viele Referenzen zu den Account-Daten ihrer Kunden zu generieren, wie beispielsweise Amazon Payment.

simply tools to be applied, but processes to be developed. Users and doers may become the same" (Castells 2010: 31). Die Konzeption dieser Prozesse erfordert jedoch Expertise und geeignete Fachleute. Wir wollen daher im Folgenden nach der Rolle der IT Kompetenz fragen und die Bedeutung von qualifizierten Personal für die Implementierung solcher Anwendungspraktiken in Augenschein nehmen und zudem das Spannungsverhältnis zwischen der angestrebten Allokation von Daten und dem Schutz des Privaten einschließen. Letzteres wird uns später im fünften und sechsten Kapitel erneut begegnen, wenn der Schutz von sensiblen, persönlichen Daten im Rahmen der resilienten Organisation diskutiert wird.

Ein Weg zur Monetisierung von Big Data erfolgt mittels der Zuordnung von Informationsbausteinen über eine natürliche Person zu einer bestimmten verhaltensäquivalenten Gruppe oder einem spezifischen digitalen Profil (Amoore und Raley 2016: 5). Diese Allokation geschieht in der Absicht diejenigen Themen herauszufiltern, welche für die Gruppe oder Person relevant sind, beispielsweise bestimmte Artikel oder individualisierte Werbung (Vassilaki 2015: 28). Dies schließt Rückschlüsse auf vermutete, mitunter auch zukünftige Interessen ein, deren Identifizierung auf der Grundlage zurückliegender Informationen und probabilistischer Modelle erfolgt (Amoore 2016: 18). Die spezifisch zugeordneten Profildaten sind der entscheidende Mehrwert der Cloud-Ökonomie, auf deren Schultern die virtuelle Wertschöpfungskette beruht (Bratton 2015: 137).

Der technologische Fortschritt erlaubt es Algorithmen die Raster der Nutzeridentifikation enger zu ziehen und ein deutlicheres Bild von Personengruppen und Individuen zu erhalten. Neben den Daten, welche beim Browsen oder Konsum im Internet gespeichert werden, setzt sich ein digitales Profil auch aus den Datenübertragungen der Schnittstellen des „Internet of Things" zusammen. In diesem dokumentiert beispielsweise das vernetzte Heim die Gewohnheiten und Verhaltensmuster seiner Nutzer.[117] Die Auswahl und Wiederholung von Informationen können auch konditionierend auf den Nutzer wirken. Dies beschreibt den Übergang „[f]rom user-centered design to the design of the user" (Bratton 2015: 284). Applikationen zur Überwachung der Gesundheit, Steuerung des Stromverbrauchs oder Dokumentation des Fahrstils stellen

[117] Dies kann annehmlich und gewünscht sein, etwa in Form der Speicherung von Cookies, kleinen Markierungen der individuellen Internethistorie, die den schnellen Zugriff auf das persönlich Interessante erlauben. Es kann aber auch problematisch sein, wie es die Manipulation von Nutzern und die Überwachung durch private und staatliche Organisationen zeigen (Aradau und van Munster 2007: 16). Ein Beispiel von Missbrauch – wenn nicht im legalen dann zumindest im ethischen Sinne ist die Auswertung von Gesundheitsanwendungen zugunsten von Marketing. Diese Methode erfreut sich großer Beliebtheit, wie beispielsweise in einer Anwendung zur Überwachung des ungeborenen Kindes während der Schwangerschaft, welche allerdings gleichzeitig das Konsumverhalten der werdenden Mutter über das Smartphone analysierte und individualisierte Angebote versendete (Gigerenzer, Schlegel-Matthies und Wagner, 2016: 25).

informationsgenerierende Schnittstellen aber auch Elemente der Rückkopplung dar, etwa wenn sie Impulse zur Anpassung des Nutzerverhaltens aussenden.[118] Die verfügbaren Daten können, sofern Internetkonzerne diese mit Strafverfolgungsbehörden teilen, Aufschluss über Verdächtige geben. Abweichende Verhaltensmuster oder anderweitig auffällige Informationen[119] können von der Rechenleistung der Cloud ausgewertet werden und bieten in dieser Hinsicht eine Möglichkeit Risiken, beispielsweise in der Verbrechensbekämpfung auf der Grundlage von Nutzerverhalten und Prädiktion zu steuern (Amoore und Raley 2016: 4).

Die Rolle von Big Data und Algorithmen werden aus diesem Grund zunehmend auch zum juristischen und politischen Gegenstand wie die Gesetzgebung zeigt (vgl. EU-Datenschutz-Grundverordnung - EU-DSGVO 2016).[120] Transaktionen, welche ausschließlich innerhalb dieser Jurisdiktion stattfinden würden, wären unbedenklich denn „[s]olange diese Rechtsräume halbwegs voneinander getrennt sind oder sich an ihren Grenzen kontrollieren lassen, ist das unproblematisch. Ein einziger, gemeinsamer Transaktionsraum mit unterschiedlichen Normen schafft jedoch automatisch zahlreiche Schwierigkeiten und Konflikte“ (Walter: 2008: 10). Dies resultiert aus der globalen Reichweite der Digitalisierung, welche als transnationales Phänomen Interaktionen und Transaktionen zwischen unterschiedlichen Rechtsräumen, aber mithilfe eines allgemein genutzten Kommunikationsmediums etabliert hat, ohne ausreichende und einheitliche Rechtsstandards nach sich gezogen zu haben (Bratton 2015: 123). Eine Diskrepanz die ebenso für den Schutz der Privatsphäre als auch der finanziellen Integrität gravierend sein kann (AGCS 2018: 3).

Sicherheitsstandards treten angesichts immer schneller werdender Produktions- und Entwicklungszyklen häufig in den Hintergrund: „IT-Sicherheitsmechanismen werden oft erst nachträglich – sozusagen als Add-on – in Systeme, Produkte und Dienste eingefügt. Sie haben

[118] Sogenannte Telematics-Technologien wurden ursprünglich entwickelt, um die Funktionen des Automobils und angebotener Services (insbesondere über den Bordcomputer) zu dokumentieren (Kulatilaka 2001: 5). Ein neueres Anwendungsmodell wird von Versicherungen eingesetzt um die Prämienberechnung eines KFZ-Versicherungsnehmers anhand seines Fahrverhaltens anzupassen. Die ausgewerteten Daten können – je nach Anbieter unterschiedlich – auch für Rückmeldungen an den Fahrer verwendet werden, etwa um auf eine riskante Verkehrsteilnahme hinzuweisen und das Fahrverhalten langfristig anzupassen.

[119] Beispiele für auffälliges Verhalten können durch Reisemuster, Transaktionen, Beiträge in Foren oder sozialen Medien im Allgemeinen beziehungsweise Unterhaltungen und Beziehungen zu verdächtigen Personen sein. So zeigte sich auch, dass ein „no fly“ Status “do not merely draw upon an archive of stored past known infractions, but are produced algorithmically, detecting patterns and clusters of possible associations (…)” (Amoore 2016: 22).

[120] Ein Beispiel für eine illegale Konfiguration eines Endgeräts bot 2017 eine Spielzeugpuppe namens „Cayla“ die Fragen von Kindern aufzeichnete, an einen Server sendete und die Antwort mittels einer Google-Abfrage im Kinderzimmer rezitierte. Die Puppe wurde in Deutschland von der Bundesnetzagentur verboten, da sie heimlich Aufzeichnungen ihrer Umgebung ohne Kenntnis der sie umgebenden Personen vornahm. Vgl. Neuerer, Dietmar, 17.02.2017, Handelsblatt: Behörde verbietet spionagetaugliche Puppe - Firma wehrt sich. Zuletzt aufgerufen am 20. Februar 2017 unter: http://www.handelsblatt.com/politik/deutschland/my-friend-cayla-behoerde-verbietet-spionagetaugliche-puppe-firma-wehrt-sich/19407840.html

somit zunächst keine unabhängige Funktion und erschweren die Nutzung von Informations- und Kommunikationstechnologien, im privaten wie im geschäftlichen Umfeld“ (Weber 2016: 29). Als Folge sind aufwendige „Patches“ – nachträgliche Verbesserungen der Software – notwendig um Sicherheitslücken zu schließen. Diese Diskrepanzen im Software-Release-Management auszunutzen ist das lukrative Geschäftsfeld von zunehmend professionalisierten Gruppen geworden, sogenannten Cyber-Kriminellen (Bonner 2012:273). Bereits vor der Corona-Pandemie stellte dies ein großes Sicherheitsproblem dar. Im Jahr 2013 wurden mehr als 550 Millionen Identitäten von Nutzern als Folge von Sicherheitslücken aus Netzwerken entwendet und diese Zahl könnte laut Schätzungen auf mehr als eine Milliarde ansteigen.[121] In anderen Worten, die Daten jedes siebten Menschen auf der Erde oder einer von drei Internetnutzern könnte von Unbefugten eingesehen und unter Umständen zweckentfremdet werden (McGuire 2015:46).

Der Digitalisierungsschub durch die Pandemie verstärkte diese Problematik weiter. Die gestiegene Nutzung von Fernverbindungen von Nutzern über das Internet erfolgte nun vermehrt, allerdings ohne ausreichenden Schutz der Verbindungen, insbesondere am heimischen Endgerät. Dies reicht von unzureichenden Firewall-Einstellungen, über Antivirenprogramme und veraltete Sicherheitsprotokolle bis zur (virtuellen) Zugangskontrolle (Chigada und Madzinga 2021: 4). Auch das Gesundheitswesen wurde verstärkt Ziel und Opfer von Angriffen, da die Schutzmaßnahmen in dieser Branche im Durchschnitt auf signifikante Weise hinter den Standards, wie beispielsweise durch nicht-aktualisierte Softwareprodukte, geringer IT-Sicherheitsstandards in der Nutzung von Systemen und fehlendem Personal zurückfällt (ebenda). Insbesondere Kliniken und Praxen stellen mit den im großen Umfang verarbeiteten sensiblen Daten von Patienten und Mitarbeitern ein lohnendes Ziel dar, deren Relevanz im Zuge des Digitalisierungsschubs auch im Gesundheitswesen weiter zugenommen hat (Dochow 2022: 105).

Dieser unautorisierte Einblick in die Daten anderer, der potentielle Schaden für die Betroffenen und der Reputationsschaden für die informationsverwaltenden Unternehmen, stellen eins der größten Risiken des digitalen Zeitalters dar. Dieser kann wirtschaftliche oder juristische Folgen haben, sich aber auch ebenso die individuelle Vulnerabilität von Nutzern negativ

[121] Ein bekannter Fall war der Datenverlust bei Sony, in dessen Folge etwa 77 Millionen Datensätze und 45 Millionen Kreditkarteninformationen entwendet wurden. Der Wert von Informationen kann von Angreifern monetisiert werden, indem sie die Kreditkarten zu betrügerischen Zwecken einsetzen oder auf dem (digitalen) Schwarzmarkt weiterverkaufen (Fisher 2013: 221).

beeinflussen.[122] Für Unternehmen bedeutet dies vorrangig, dass sie unter dem Druck der Digitalisierung ihre Produkte und Prozesse modernisieren müssen, aber zugleich unter dem Eindruck der Unsicherheit relevante Entscheidungen unter der Berücksichtigung von Sicherheitsstandards treffen sollten. Denn der Wert der auf ihren Systemen gespeicherten Informationen ist ein lohnendes Ziel für gezielte Angriffe (Choo, Smith und McCusker 2007: 6). Wenn es Angreifern gelingt, eine einzelne Servervulnerabilität ausfindig zu machen, können diese unter Umständen Zugriff auf die im Cloud-Netzwerk prozessierten Daten gewinnen.[123] Die Konsequenzen können erheblich sein, wie in der Vergangenheit mehrfach deutlich wurde[124] (Bonner 2012). Das sechste Kapitel wird die wichtigen Aspekte der Nutzer- und Mitarbeiterschulungen zur Informationssicherheit thematisieren und die Risiken auf Ebene der Nutzerschnittstelle verdeutlichen. Diese Maßnahmen sowie Bewusstseinsbildung sind insbesondere dahingehend zwingend notwendig, da etwa 90 Prozent aller Cyberangriffe mit Hilfe von Social Hacking, also unter (unbewusste) Manipulation von autorisierten Nutzern durchgeführt werden (Wentland und Klimburg-Witjes 2021: 168).

3.3. IT Kompetenz in Unternehmen

Die größtenteils durch Unternehmen betrieben technologische Grundlage der Digitalisierung umfasst neben physischen Strukturen wie Rechenzentren auch immaterielle Werte wie Prozesse, Dokumentationen und Fachwissen. Diese Werte sind von großer Bedeutung zum Betrieb und Weiterentwicklung der angebotenen Produkte und betreffen vor allem die zur Verfügung stehende Expertise, denn „[n]ew information technologies are not simply tools to be applied, but processes to be developed" (Castells 2010: 31). Für den Betrieb einer IT-Anwendung benötigt man beispielsweise die Expertise im Bereich der IT-Architektur zur Definition der strukturellen Konzeption der Software. Die konkreten Leistungsanforderungen werden durch das Anwendungsmanagement bestimmt, darüber hinaus werden Experten für das *Incident Management* beziehungsweise *Desaster Recovery Management* benötigt, welche den Betrieb sicherstellen sollen. Dies zeigt, dass die benötigte Kompetenz und Expertise in Unternehmen diverse Bereiche abdecken muss, um einen reibungslosen Anwendungsbetrieb

[122] Private Computer und das mobile Endgerät sind die schwächsten Glieder in der Sicherheitskette. Der Grund dafür ist, dass sich hier eine große Auswahl unterschiedlicher Applikationen von Unternehmen findet, die bereits Daten im Hintergrund sammeln und verarbeiten, deren Versionen und Programmelemente aber häufig nicht aktualisiert oder angemessen verwaltet werden (Provos et. al. 2007: 1).

[123] Wir werden uns im fünften und sechsten Kapitel dieser Problematik im Detail zuwenden. Das mobile Endgerät eines einzelnen Nutzers ist hingegen häufig der Eintrittspunkt eines Angriffes auf ein System, da die lokale Interaktionsschnittstelle zumeist unzureichend gesichert ist.

[124] Der Angriff auf Sony führte zur Entwendung von Millionen von Kundendaten (Bonner 2012: 273). Ebenso der Fall von British Airways im Frühjahr 2018, als eine Malware für zwei Wochen unentdeckt Kreditkarteninformationen von etwa 400.000 Kunden kopierte (vgl. BBC 2018)

erbringen zu können. Dies umfasst sowohl die Mitarbeiter, aber auch die Konzeption der Hardwareelemente und der definierte Prozeduren und Dokumentationen im Unternehmen, um komplexe Anwendungen im Betrieb zu halten. Diese umfassende Befähigung innerhalb eines Unternehmens bezeichnen wir im Folgenden als *IT-Kompetenz*, welcher eine signifikante Bedeutung für die Verteilung von Rollen und Verantwortung im Rahmen unternehmerischer Sicherheit hat.

Der weiträumige und kontextuale Informationsbegriff des Cyberzeitalters erfordert eine kognitive und kontextuelle Verarbeitung des Wertes von Informationen und sollte daher ebenfalls Eingang in die Beschreibung der IT-Kompetenz finden (Arnold et. al. 2016: 5). Aus Unternehmenssicht stellt sich ein zunehmender Bedarf an qualifizierten Mitarbeitern ein, denn die wachsende Bedeutung von Software, Datenanalyse und Anwendung in den Bereichen Service, Vertrieb oder Produktion verlangt nach geeignetem Personal zur Übernahme der sich verändernden Positionsbeschreibungen in Unternehmen (Krabel 2016: 102). Dazu zählen Aspekte wie die Beziehungen zwischen Kunden und Anbietern oder die Ableitung einer Strategie aus den Anforderungen der Marktinnovationszyklen. Letztere sind insbesondere von Bedeutung und benötigen Personal mit der geeigneten IT-Kompetenz, das über die Fähigkeit zur Folgenabschätzung verfügt (Buchholz und Wangler 2016: 181).

Diese zeichnet sich dabei wie bereits angemerkt sowohl durch ein profundes Verständnis der technologischen Veränderungen aus, als auch durch „Fach-, Methoden-, Sozial- und Selbstkompetenzen (…). In Abgrenzung zu den Begriffen ‚IT-Kenntnisse' oder ‚IT-Fertigkeiten', die eine spezifische Klasse individueller Eigenschaften beschreiben, lässt der Begriff der IT-Kompetenzen offen, welche Merkmale einer Person, ihr erfolgreiches Handeln bewirkt" (Hanft, Müskens und Muckel 2004: 21). Das Fehlen dieser Expertise kann versucht werden durch Neueinstellungen oder externe Unterstützung in Form von IT-Outsourcing zu kompensieren, allerdings bleibt das Risiko – beispielsweise im Falle eines vorzeitigen Endes der Zusammenarbeit mit dem Drittanbieter - die IT-Kompetenz zu verlieren. Dies kann seinen Ausgang in der Problematik finden, dass Unternehmen aufgrund fehlender Expertise oder alternativer Wissensträger auf einen externen Anbieter angewiesen sind und von dessen Verfügbarkeit beziehungsweise Risikokontrolle abhängig werden (Bahilia und Rivard 2003 214).[125]

[125] Siehe hierzu den Fall des Lock-in durch Drittanbieter (vgl. (Armbrust et. al. 2010: 55), welche im vierten und fünften Kapitel besprochen werden.

Der Mangel an einem fundierten Verständnis digitaler Risiken erschwert selbstredend den Prozess des digitalen Unternehmensumbaus, und forciert zusätzlich Unsicherheit im Umgang mit Partnern und Dienstleistern (Lee, Yeung und Hong 2012: 544). Insbesondere problematisch ist dies, wenn ein Unternehmen aufgrund mangelnder Fachkenntnisse seiner Entscheidungsträger die Risiken der Digitalisierung unzureichend oder selektiv berücksichtigen (McKinsey 2011: 11). Denn im Fall von technologischen Diskontinuitäten, also der Einführung disruptiver Verfahrenstechniken, können Unternehmen die Tragweite der Veränderung nicht beurteilen und zu kritischen, weil riskanten Entscheidungen führen (Bahli und Rivard 2003: 214). Eine weitere essentielle Anforderung wird es in diesem Zusammenhang sein, eine Verbindung zwischen technologischen Veränderungen und betrieblichen Abläufen herzustellen. Daher werden kompetente Mitarbeiter[126] benötigt, welche „die betriebliche[n] Abläufe der Unternehmen gut kennen und den Einsatz moderner Technologien den spezifischen betrieblichen Anforderungen anpassen können“ (Hammermann und Klös 2016: 10). Dies gilt insbesondere im Fall der fortschreitenden Vernetzung der Unternehmensstruktur, durch welche signifikante Sicherheitsrisiken entstehen können, wenn keine geeignete Expertise im Unternehmen vorhanden ist um die bestehenden, analogen Risikokontrollsysteme einer Revision zu unterziehen (Gaycken und Karger 2011: 5). Der Aufbau der entsprechenden Fachlichkeit, das heißt einer etablierten IT-Kompetenz auf allen Ebenen des Risikomanagements ist daher unerlässlich im Sinne der Sicherheitsproduktion.

3.4. Neue Dienstleistungsangebote, alte Probleme

Nachdem wir nun die Schlüsselbegriffe und Kernaspekte des digitalen Wandels eingeordnet haben, stellt sich die Frage, wie die Digitalisierung das Umfeld und die Leistungen von Unternehmen tangiert. In diesem Abschnitt wird die Gesundheitsbranche zum einen als Beispiel für diesen Wandel angeführt, da in ihr mehrere interessante Komponenten der Digitalisierung zusammenwirken und im Zuge der Corona-Pandemie dieser Branche besondere gesellschaftliche Aufmerksamkeit zu Teil wurde. Zum einen arbeiten Krankenhäuser, Arztpraxen, Forschungseinrichtungen, Pharmakonzerne und Krankenkassen mit sensiblen

[126] Diese Entwicklung könnte ein innovationsfreundliches Klima mit Blick auf die Arbeitsstrukturen und Förderungsmodelle von Unternehmen hervorbringen und somit indirekt die Arbeitserfahrung des Einzelnen beeinflussen (Eichhorst et. al. 2016: 10). Beispielsweise zeichnen sich auf dem deutschen Arbeitsmarkt derartige Engpässe ab. Aufgrund des demographischen Wandels geht die Zahl der Erwerbstätigen zwischen 30 und 49 Jahren zurück und gleichzeitig steigt der Anteil älterer Mitarbeiter, deren Eintritt ins Rentenalter aus Gründen der Lebensniveausicherung und allgemeiner volkswirtschaftlichen Determinanten der Rentenpolitik in Zukunft tendenziell weiter hinausgezögert werden wird. Hier wird für Unternehmen aber auch den individuellen Arbeitnehmern ein Umdenken in der Bildung und Fortbildung erforderlich sein. Dies gilt insbesondere für den peripheren Raum und klein- und mittelständige Unternehmen (Welzbacher et. al. 2015: 16). Ein Potential bietet sich ebenfalls durch digitale Lernprogramme und Inklusionsansätze, um Mitarbeiter aller Altersstufen am gemeinsamen Prozess der Unternehmensumgestaltung zu beteiligen (Apt und Wischmann 2016: 115).

Daten wie etwa Forschungsergebnissen, Patientendaten oder Befunden. Die Digitalisierung von Informationen bietet sich angesichts der Komplexität der Behandlungen, Einbeziehung von Dienstleistern beziehungsweise Akteuren und Konsolidierung von Gesundheitsdaten an und erzeugte große Datenbestände und deren Vernetzung (Manzei 2009: 39). Deren Schutzbedarf zeigt aber auch die möglichen, gravierenden Folgen im Fall einer Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität dieser Daten.[127] In Deutschland zählen Krankenhäuser zwar zur kritischen Infrastruktur und werden vom Gesetzgeber[128] zu besonderer Sorgfalt im Umgang mit sensiblen Daten verpflichtet (Dochow 2022: 103), aber es zeigte sich insbesondere während der Pandemie, dass sich ein enormer Anstieg gezielter Angriffe gegen die digitale Infrastruktur von Organisationen im Gesundheitswesen ereignete (Chigada und Madzinga 2021: 5). Deshalb sollen im Folgenden die Implikationen der Digitalisierung für den medizinischen Bereich exemplarisch beleuchtet werden[129], um die Kehrseite der technologischen Vernetzung an diesem Fall aufzeigen zu können. Dies soll helfen, den Anpassungsdruck von Unternehmen im Informationszeitalter zu erklären, um dadurch auf den eigentlichen Fokus in Form einer potentiellen Sicherheitsproblematik hinsichtlich der neuen Technologien überzuleiten. An diese Überlegungen werden wir in den folgenden Kapiteln anschließen.

Generell werden in der Gesundheitsindustrie viele personenbezogene, sensible Daten erhoben, verarbeitet und in der Kommunikation zwischen den beteiligten Akteuren übermittelt.[130] Jede medizinische Behandlung erfolgt so weit wie möglich auf der Grundlage von Informationen über den Patienten, sein Umfeld, seine Vorgeschichte, Befinden und Präferenzen. Eine mögliche Bündelung von relevanten Patienteninformationen könnte dem Behandlungserfolg

[127] Das australische Krankenversicherungsunternehmen Medibank war 2022 von einem großen Ransomwareangriff betroffen, in dessen Folge Lösegeldforderungen für die durch eine Schadsoftware verursachte Verschlüsselung von Daten gestellt wurden. Vermutlich um ihren Forderungen Nachdruck zu verleihen, veröffentlichten die Täter Auszüge aus den Datenbanken, einschließlich sensibler Daten wie Kreditkarteninformationen oder Diagnosebefunde von Patienten (Spiegel 2022).

[128] Das Patientendaten-Schutz-Gesetz (PDSG) wurde beispielsweise 2020 novelliert und erweiterte den Schutzumfang auch auf kleinere Häuser ausdehnte (Dochow 2022: 103)

[129] Der Themenkomplex Medizin und Gesundheitsvorsorge beschreibt eindringlich die potentiellen Vorteile eines verstärkten Einsatzes der neuen Technologien (Heinrich et. al. 2016: 57) aber auch die Schwierigkeiten einer Umsetzung aufgrund von rechtlichen und sicherheitsrelevanten Gründen (Dwertmann und Schürholz 2016: 172).

[130] Dieses Beispiel eignet sich durch das ökonomische Potential der Einsetzung von digitalen Technologien zur Verbesserung der Prozesse und Therapien, aber auch aufgrund der sensiblen Daten in diesem Bereich. Vor allem der Wandel der Krankenhausorganisation und die Verarbeitung von Patientendaten zum Zweck der ökonomischen Versorgung im Gesundheitswesen rückt dadurch in den Mittelpunkt (Gigerenzer, Schlegel-Matthies und Wagner 2016: 10).. Diese unterliegen durch die Privatisierung der Krankenhäuser, zum anderen Teil durch die Demographie und die steigenden Kosten der Gesundheitsversorgung einem immanenten Wandel. Dazu gehören die Umstellung und Zentralisierung der Organisation, die Auslagerung von Prozessen an externe Dienstleister in den unterschiedlichen Ausprägungen (vom Catering bis zum Labor) und vor allem die Einführung der digitalen Vernetzung und Datenverarbeitung (Manzei 2009: 39).

und ebenso der wirtschaftlichen Umsetzung von Prozessen in diesem Wirtschaftszweig[131] wesentliche Vorteile verschaffen (Gigerenzer, Schlegel-Matthies und Wagner 2016: 10). Denn „[d]ie potenziellen Möglichkeiten von Big Data in der Medizin liegen vor allem in der Nutzbarmachung und Integration von großen und komplexen Daten aus allen Gesundheitsbereichen, um eine verlässliche Evidenz für medizinische Entscheidungen zu generieren“ (Dwertmann und Schürholz 2016:171).

Für eine flächendeckende Umsetzung dieses Vorhabens müssen allerdings zwei Vorbedingungen geklärt werden, namentlich die technische Organisation und die regulatorischen Anforderungen im Umgang mit Daten (Manzei 2009: 40f.). Die unterstützende Funktion von Big Data im Bereich der Medizin kann durch die Reduktion der Daten und die Überprüfung der Praxisrelevanz sichergestellt werden (Horst 2012: 9f.). Um dem Patienten einen konkreten Vorteil aus der Auswertung komplexer Kennziffern zu Teil werden zu lassen[132], müssen sich die Patienteninformationen in umsetzbare Diagnose- und therapierelevante Werte umsetzen lassen (Dwertmann und Schürholz 2016:169). Vernetzung, Standardisierung und automatisierte Kontrollsysteme könnten hier Abhilfe leisten und Patienten wie Kostenträger gleichermaßen Vorteile verschaffen.[133]

Jedoch bestehen wesentliche Einschränkung zur Erfassung und Auswertung gesundheitsrelevanter Daten, beispielsweise in der Telemedizin[134]. Das Fernbehandlungs-verbot[135], das bedeutet das Interdikt der Diagnose und Therapieeinleitung ohne physische Anwesenheit eines approbierten Arztes, untersagte in Deutschland lange Zeit die mittelbare Behandlung von Patienten (Dwertmann und Schürholz 2016: 165). Ein aufwendiger Anpassungsprozess etablierter Strukturen im analogen und digitalen Bereich ist notwendig, um

[131] Der globale Markt für Fitness- und Gesundheitsapplikationen im Allgemeinen wird für 2017 auf 26 Milliarden US-Dollar geschätzt (Gigerenzer, Schlegel-Matthies und Wagner 2016: 12). Die Anwendungsfelder der neuen Technologie sind vielfältig. Es existieren bereits Angebote zur medizinischen Überwachung der Vitalfunktionen von Neugeborenen („Smart Baby monitoring“) oder Sensoren in Fußsohlen, welche das Gangprofil dokumentieren und im Fall von Abweichungen die Pflegekraft alarmieren (Rüegsegger 2016: 1149).

[132] Dazu ist ein standardisierter Prozess der Datenerfassung – und Speicherung ex ante erforderlich. Dies meint einen ortsübergreifenden Ansatz, der zudem das geordnete Informationswesen der separaten Krankenkassendatenbanken zu überwinden vermag. Dies inkludiert die Standardisierung des medizinischen Systems zu Gunsten einer einheitlichen Datendokumentation (Heinrich et. al. 2016: 57).

[133] Allerdings ist Vorsicht geboten, falls Dokumentationsinitiativen mehr der ökonomischen Kontrolle als der therapeutischen Verbesserung dienen (Manzei 2009: 46).

[134] Der nötige Austausch von Informationen unterlag allerdings bisher dem Fernbehandlungsverbot, welches erst 2016 mit dem „E-Health-Gesetz“ überarbeitet wurde. Dieses unternimmt erste Ansätze den legalen Rahmen für die digitale Krankenversorgung zu regeln, einschließlich der Zukunft der Telemedizin als auch der allgemeinen Verwendung von gesundheitsbezogenen Daten (Dwertmann und Schürholz 2016: 165).

[135] Das Bundesland Sachsen-Anhalt erteilte dem Krankenhaus Seehausen beispielsweise eine Ausnahme, welche die Versorgung der Patienten in einer strukturschwachen Region mithilfe der Befundung der lokal durchgeführten Computertomografie durch einen radiologischen Dienst in Magdeburg gestattet (vgl. Richter 2017).

die Anforderungen für ein einheitliches und sicheres Fernbehandlungssystem zu erfüllen.[136] Ein anderes Problemfeld ist der geforderte Zugriff von Patienten auf die Krankenakte, welcher die Erfordernis einer Veränderungsdokumentation („Change History“) des digitalen Dokuments deutlich macht,[137] denn die Nachvollziehbarkeit der Datenintegrität ist nicht nur für den Behandlungserfolg wichtig, sondern kann ebenfalls Konsequenzen für die Krankenversicherungen haben.[138] Des Weiteren ist die Bedeutung der Informationsvertraulichkeit hervorzuheben, da die Patientendaten zu den vertraulichsten und auch lukrativsten Datensätzen gehören: Patientendatensätze, welche zwischen Krankenhäusern, Praxen und Krankenversicherungen transferiert werden, können beispielsweise Informationen wie die vollständigen Personendaten, Kreditkartennummern, vergangene Zahlungsdaten und Krankheitsbefunde beinhalten, was sie für den (illegalen) Handel sehr wertvoll macht (Chigada und Madzinga 2021: 5).

Vor diesem Hintergrund zeigt sich, dass die Digitalisierung der Medizin ein gutes Beispiel für Chancen und Risiken des technologischen Wandels im Cyberzeitalter ist. Die Vorteile einer Vernetzung stehen auf der einen Seite, aber auch den Risiken einer unvollständigen oder übereilten Implementierung auf der anderen Seite gegenüber. Daher ist erneut hervorzuheben, dass medizinische Daten zu den sensibelsten Informationen von Privatpersonen gehören. Deren Vertraulichkeit muss ein hoher Schutz zugemessen werden (Dochow 2022: 103). Diagnosen und Behandlungen, beispielsweise physischer oder psychischer Natur, sind Teil der individuellen Privatsphäre und könnten für kriminelle Zwecke verwendet werden.[139] Mit dem zunehmenden Anstieg von elektronisch gespeicherten Patientendaten und im IoT erfassten Gesundheitsdaten ist der medizinische Betrieb für Hacker attraktiv geworden (Sittig und Singh

[136] Die Speicherung relevanter Daten auf der Chipkarte kann signifikante Vorteile für den Versicherten haben. Arztbriefe und Röntgenaufnahmen, Laborbefunde und bekannte Allergien können helfen Kosten und Untersuchungen zu reduzieren und dem Patienten eventuell unnötige Maßnahmen (Computertomographie, Lumbalpunktion) zu ersparen. Auch erhöht sich mitunter die Sicherheit des Patienten durch einheitlich erfasste Daten und Befunde (Gigerenzer, Schlegel-Matthies und Wagner, 2016: 22), unterliegt aber den Nachteilen des Zwei-Schlüssel-Prinzips und der lokalen Speicherung auf einer Chipkarte (Vgl. Bundesministerium für Gesundheit .2017).

[137] Vgl. Krüger-Brand und Osterloh für einen Überblick in die Diskussion unter Ärzten und Heilberufsverbänden zum Thema der elektronischen Patientenakte. Zum Beispiel zeigt sich, dass die bisherigen Ansätze zur Kommunikation zwischen Arzt und Patient mittels der elektronischen Patientenakte noch nicht geeignet sind, die prinzipielle Dokumentation von Befunden im Austausch zwischen Vertretern der Heilsberufe herzustellen. Falls die Akte von mehreren Nutzern editierbar sei, könne keine Gewährleistung für die Richtigkeit der Daten gegeben sein (Krüger-Brand und Osterloh 2017: 1659). Eine Dokumentation der Zugriffe und Veränderungen ist daher zwingend erforderlich, primär zum Schutz des Patienten und sekundär zum Schutz des Arztes.

[138] Die Berechnung von Kranken- oder Lebensversicherungen beruhen auf der Krankenhistorie des Versicherungsnehmers. Könnte dieser das zentrale Datenrepositorium seiner Krankendaten manipulieren, würde für das Versicherungssystem eine essentielle Quelle zur Berechnung der Versicherungsprämie entfallen.

[139] Die Kassenärztliche Bundesvereinigung unterstützt beispielsweise eine Abkehr vom „Zwei-Schlüssel-Prinzip“ nachdem nur Patient und Arzt gemeinsam die Daten auf der Karte entschlüsseln können (vgl. Kassenärztliche Bundesvereinigung 2017).

2016: 625). Ein unautorisierter Eingriff sowohl in die Vertraulichkeit der Daten, als auch in deren Integrität könnte fatale Folgen haben. Gleiches gilt für die Verfügbarkeit von Gesundheitsdaten, wie das folgende Beispiel zeigt.

Die Vernetzung in der Intensivmedizin zeigt das Risiko im Fall eines unzureichend konzipierten Sicherheitskonzeptes. Wenn die Steuerung und Überwachung einer Station durch ein Zentralsystem von Außenstehenden beeinflusst werden könnte, wären die Angreifer unter Umständen in der Lage die Infusionen oder Beatmungsgeräte der Intensivpatienten auszuschalten (Manzei 2009: 45). Ähnliches gilt für kriminelle Absichten wie in Form der Ransomware, das heißt die Verschlüsselung von Datenbanken zum Zweck der Erpressung von Lösegeld (Pathak 2016: 371). Ein Krankenhausbetrieb ohne Zugriff auf die digitalen Patientenakten wäre paralysiert, Operationssäle durch Blockierung der Steuerungssoftware unbrauchbar (vgl. Beuth 2017). Aus diesem Blickwinkel ist die sukzessive Annäherung an die Digitalisierung der Krankenversorgung nur unter Wahrung von Sicherheitsstandards ratsam. Zudem bleibt stets auf der anderen Seite die implizite Preisgabe sensibler Gesundheitsinformationen durch Internetnutzer selbst zu bedenken (Gigerenzer, Schlegel-Matthies und Wagner, 2016: 25).

Dies betrifft auch die Unterbrechung des Datenflusses oder gar der behandlungsnotwendigen Unterstützungssysteme im Gesundheitsbetrieb. Weltweit wurden Berichte über Unterbrechungen im Krankenhausbetrieb bekannt, etwa 2016 mit „Locky“, 2017 mit „WannaCry“ oder „Emotet im Jahr 2019 (Dochow 2022: 100). Im Zuge der Corona-Pandemie nahm nicht nur die Belastung des Gesundheitswesens durch hohe Fallzahlen zu, sondern kamen auch gezielte Angriffe gegen Unternehmen im Gesundheitswesen hinzu. Unternehmen wie beispielsweise Krankenhäuser und Praxen gelten in Fachkreisen als besonders verletzliche Ziele eines Cyberangriffes, da ihre Sicherheitsstandards, Ausstattung und die sicherheitsrelevante Schulung des Personals als niedrig eingestuft werden (Chigada und Madzinga 2021: 4). Auch die Hersteller von Impfstoffen oder Antigentests gegen den Corona-Virus gehöhrten mit Beginn der Pandemie neben Krankenhäusern zu den besonders stark betroffenen Unternehmen der Cyberbedrohungen (Dochow 2022: 101).

Zusammenfassend zeigt das Anwendungsbeispiel der digitalisierten Gesundheitsindustrie, dass die Auswertung der persönlichen Informationen sowohl in den Gesundheitsberufen wie auch für die Patienten zwar einerseits Vorteile verschafft (Dwertmann und Schürholz 2016: 168), aber andererseits auch in veritable Sicherheitsrisiken münden kann. Die Ansprüche von Kunden, Unternehmen, aber auch Investoren und Geschäftspartnern machen daher einem

weitreichenden Umbau von Prozessen und Strukturen im Rahmen der Digitalisierung notwendig. Allerdings ist dazu auch eine begleitende Strategie zur Etablierung einer umfassenden Risikokontrolle notwendig. Denn wenn Daten und Systeme zusammengeführt werden, ohne essentielle Schutzwerte und -Maßnahmen zu bestimmen, drohen in diesen Fällen sowohl Unternehmen als auch der Bevölkerung signifikante Risiken. Diese Implikation werden wir in den folgenden Kapiteln im Detail verfolgen. Die aufgezeigten Facetten der Digitalisierung sollen dazu als Grundlage dienen, um dem Anpassungsdruck von Unternehmen und der ökonomischen Rationalität im Informationszeitalter Ausdruck zu verleihen.

3.5. Zusammenfassung - Zäsur des digitalen Zeitalters

Wie wir gesehen haben versetzt die Digitalisierung etablierte Geschäftsmodelle und Erfahrungswelten in Bewegung. Branchen und Unternehmen geraten unter Druck und sehen sich gezwungen neue Technologien zu implementieren. Ökonomische Rationalitäten werden durch die Digitalisierung tangiert und passen sich der neuen Umgebung an, beispielsweise im Fall der Plattformökonomie. Der Veränderungsdruck kann auf fast jedes Segment übertragen werden und fordert bestehende Strukturen und Denkmuster heraus. „[T]he industrial economy had to become informational and global or collapse" (Castells 2010: 100). Das vorrangige Problem für Unternehmen ist die rasche Entwicklung einer digitalen Kompetenz und einer inhärenten Präsenz im digitalen Raum. Dazu sind und werden weitreichende Anpassungen von Produktion, Personalstruktur und Arbeitsorganisation erforderlich sein, sowie die gesamte Wertschöpfungskette wird auf ihre Komplementarität zum digitalen Anforderungsprofil zu prüfen sein (Buchholz und Wangler 2016: 181).

Die Umstellung auf die neuen Strukturen und Herausforderungen erfordern Innovation, Expertise und Kapital. Die notwendigen Kompetenzen werden zu umworbenen Ressourcen des digitalen Wandels (Hammermann und Klös 2016: 9). Denn „[d]ie Grundlage eines erfolgreichen digitalen Wandels ist eine leistungsfähige technische Infrastruktur […], welche flächendeckend geschaffen werden muss [und] innerbetrieblich sind IT-Sicherheit und Datenschutz essentiell für eine Digitalisierung der Wertschöpfungsprozesse" (Welzbacher et. al. 2015: 16). Diese Problematik betrifft ebenfalls den Risikobegriff in der digitalen Epoche. Die Folge sind neue Risikokategorien durch die Entscheidung zum Einsatz neuer Hochtechnologie, deren negative Folgen schwer abschätzbar sind. Diese komplexe Situation aufzulösen, das heißt Kontinuität und Widerstandsfähigkeit auf der einen Seite mit Fortschrittsfähigkeit und digitaler Technologienutzung auf der anderen Seite zu verbinden wird die eigentliche Herausforderung für Unternehmen dieser Zeit sein.

4. Organisations- und Risikobegriff in der soziologischen Organisationstheorie

Nachdem wir die Grundlagen und Facetten der Digitalisierung besprochen haben, widmet sich dieses Kapitel dem Organisations- und Risikobegriff. Die zuvor beschriebenen Implikationen der Digitalisierung auf die Prozesse, Kommunikation und Abgrenzung von Unternehmen legen daher die Frage nahe, wie diese Veränderungen in einem theoretischen Rahmen und Organisationsverständnis konzeptionell gefasst werden können? Die ökonomischen Rationalitäten der IPÖ und Anknüpfungspunkte unserer Fragestellung an die IPS treffen an dieser Stelle auf die soziologische Organisationsforschung. Dadurch bietet sich nun eine konzeptionelle Einrahmung der Sicherheitsdispositive für Unternehmen im Informationszeitalter mit Blick auf die theoretische Einordung von Organisationen an. Aus der Perspektive der soziologischen Organisationstheorie, eines etablierten Forschungszweiges, wollen wir nun die Rolle von Organisationen, ihre Beschaffenheit sowie inhärente Logik im Sinne der Anschlusskommunikation und Prozesskontinuität, um anschließend die Relevanz von Risikokontrollsystemen aus diesem Blickwinkel heraus zu klären. Aufbauend auf der Systemtheorie von Niklas Luhmann hat sich ein produktives Forschungsprogramm entwickelt (Luhmann 1991; 2000), welches auch innerhalb der Internationalen Politischen Soziologie Resonanz und Anwendung fand. Einer der Vorzüge der Organisationstheorie, welche auch in unserem Kontext relevant ist, liegt in der geschlossenen Entscheidungsfindung von Organisationen bei gleichzeitiger Interaktion mit der Außenwelt und ihrer Ausrichtung an Prozessen (Koch 2017 18ff.), wie sie auch in Unternehmen anzutreffen sind.

Eines der kennzeichnenden Elemente dieser Organisationstheorie ist das Verständnis von Programmen zur Entscheidungsfindung innerhalb von Organisationen (Luhmann 2000: 271). Die Differenzierung von Entscheidung- und Konditionalprogrammen haben in Luhmanns theoretischem Konzept die Bedeutung von beständiger Reproduktion und Kommunikation von Entscheidungen hervorgehoben, um die Selbstreferenz zu ermöglichen (Luhmann 1991: 202). An dieser Stelle bietet diese Arbeit eine Anpassung von Luhmanns Reihenfolge der kontinuierlichen Reproduktion und Kommunikation an, indem über die Begriffe Unsicherheit, Gefahr und Risiko die Veränderung des Risikobegriffs unter dem Eindruck der Digitalisierung aufgezeigt werden soll. Denn die entscheidende Lücke, wie es bereits im Abschnitt über die Literaturlage dargelegt wurde, liegt nach Ansicht dieser Arbeit in der Einbindung der Digitalisierung als technologisches Risiko, insbesondere in Folge der sprunghaft ausgedehnten

Vernetzung[140] und Virtualisierung von digitalen Netzwerken in Reaktion auf die Corona-Pandemie.[141] Zudem bietet sich die Untersuchung der bisher unterrepräsentierten Implikationen für die Sicherheitsproduktion in Unternehmen als alternative Perspektive auf das Feld der Organisationsforschung an, da es Themenkomplexe wie Entscheidungsfindung, Risiko oder Anschlusskommunikation als elementarere Voraussetzung des Organisationsverständnisses tangiert. Diese Begriffe werden wir in den nachfolgenden Abschnitten einführen und genauer aus der Perspektive der Organisationssoziologie betrachten.

In der Sprache der Systemtheorie stellt sich im Rahmen unseres Themas die Frage nach dem Risiko und der Gefahr eines Kommunikationsabbruchs[142] und damit zu einem Ende der Eigenbeschreibung und Fortexistenz der Organisation, oder anders ausgedrückt, dem Endes der Autopoiesis[143]. Diese Frage ist insbesondere mit Blick auf die durch die Corona-bedingten Maßnahmen zur Virtualisierung von Arbeitsplätzen und Kommunikation der Organisationsmitglieder über digitale Netzwerken interessant. Denn der Umgang von Unternehmen mit dieser Verlagerung ihrer Kommunikation und anderer relevanter Entscheidungen unter den Bedingungen der Unsicherheit über die möglichen Konsequenzen einer technischen oder organisatorischen Lösung, hat großen Einfluss auf ihre Funktionsfähigkeit. Dadurch übersetzt sich die Produktion von Sicherheit auf den Umgang von Unternehmen mit den möglichen Konsequenzen eines Kommunikationsabbruchs, also Entscheidungen hinsichtlich (neuen) nicht-ökonomischen, sondern sicherheitsrelevanten Sachverhalten.[144] Dies betrifft nicht nur die eigene, umfassende Organisationsdynamik,

[140] Dies zeigt sich beispielsweise in der sicherheitsrelevanten Rolle von Cloud Computing für die Verfügbarkeit und Vertraulichkeit von Daten, wie es im sechsten und siebten Kapitel genauer betrachtet werden wird. Die Attraktivität von Cloud Computing basiert auf seinen Synergieeffekten zur Lagerung, Auswertung und Bearbeitung von Informationen, welche zumeist von Drittanbietern angeboten werden (Armbrust et. al. 2010: 52).
[141] Die zunehmende Auslagerung von Prozessen in virtuelle Umgebungen ermöglichte es Unternehmen ihren Betrieb trotz der Corona-Maßnahmen fortzuführen (Kirk und McDonald 2021: 3) und bietet im Allgemeinen weitere Vorteile wie Skalierungseffekte und Senkung der Betriebskosten (Apt und Wischmann 2016: 111). Dies kann aber andererseits auch zu einer kritischen Geschäftsunterbrechung oder Reputationsrisiken wie etwa im Fall eines Datenverlusts führen wenn beispielsweise ein Schadprogramm zur Spionage, Verschlüsselung, Veränderung oder Löschung von Daten verwendet wird. Dieser Zusammenhang war mit Blick auf die durch die Corona-Pandemie beschleunigten Digitalisierung in der Forschung bisher unterrepräsentiert (Lallie et. al. 2020: 15).
[142] Die Rolle von Anschlussoperationen und Kontinuität der Kommunikation von Entscheidungen sind in Luhmanns Modell zentrale Begriffe der Organisationsbeschaffenheit und Autoreflexion (Luhmann 2000: 142f.).
[143] Dazu wird bei Luhmann der Begriff der Autopoiesis verwendet, welchen wir im Folgenden detailliert besprechen werden. Zusammengefasst beschreibt der Terminus die Eigenbeschreibung von organisationsinternen Entscheidungen durch Kommunikation an ihre Mitglieder, welche wiederum Anschlusskommunikationen ermöglicht und damit die Prozessaktivität der Organisation sowie sie selbst erhält (Luhmann 2000: 52f.).
[144] Dies versteht sich mit Vorrang auf die Folge von Privatisierung kritischer Infrastruktur mit zeitgleicher Verschiebung des Beitrags zur gesamtgesellschaftlichen Sicherheitsproduktion durch Risikokontrolle. Daher wird zudem die Frage zu klären sein, welche Auswirkungen die Aufweichung der methodischen Abgrenzung durch Luhmann im Laufe der organisationsübergreifenden Wertschöpfungskette und Monopolstellung von Akteuren auf die Risikomitigation durch die auslagernden Unternehmen und ihr Risikoverständnis haben, beispielsweise im Fall von Google, Amazon oder Microsoft im Markt für Cloud-Computing (Bratton 2015: 112)

sondern auch die Kommunikation mit anderen Organisationen, wie es zuvor exemplarisch mit Blick auf Cloud- und anderen Dienstleistern der digitalen Wertschöpfungskette angesprochen wurde. Daher richtet sich der Fokus des ersten Teils dieses Kapitels auf die organisationstheoretischen Grundlagen und der prozessorientierten Beschreibung von Organisationen.

Die Rolle dieser nicht-ökonomischen Fragestellungen wurde in der bestehenden Literatur zur Risikosoziologie teilweise angesprochen und wird im zweiten Teil dieses Kapitels vertieft. So bietet die Literatur über den Umgang mit Unsicherheit und Risiken für diese Fragestellung zwei unterschiedliche Antworten: Zum einen gibt es die hier als traditionelle Risikobewertung bezeichnete Sichtweise auf ein *objektbezogenes* Risikoverständnis, in dem Risikoobjekte unter Annahme einer Wahrscheinlichkeit des Eintretens einer möglichen Implikation betrachtet werden. Diesem traditionellen Bild unternehmerischer Risikobetrachtung werden wir ein alternatives Verständnis von Risiko gegenüberstellen, dass die Perspektive der zuvor artikulierten Organisationsbeschaffenheit in Form der *prozessgeleiteten* Kontinuität einnimmt und daher die Gefahr einer Unterbrechung der Kommunikation in Organisationen berücksichtigen muss. Dadurch soll der ursprüngliche Risikobegriff erweitert und auf die Fragestellung unter dem Eindruck der Digitalisierung konkretisiert angewendet werden, um die Sicherheitsproduktion in Unternehmen deutlicher beleuchten zu können. Auf dieser Grundlage wird auch ein Beitrag zur Organisations- und Risikosoziologie angeboten werden, der den Blick nun auch auf die unternehmerische Rolle in der Sicherheitsproduktion unter den sich beschleunigten Determinanten der technologischen Veränderung richtet.

Aus der obigen Exposition leitet sich die Struktur dieses Kapitels ab, welches über die Begriffe von Risiko und Unsicherheit das hier angewendete Verständnis von Organisationen entwickeln soll. Dies wird insbesondere für die in den vorrausgegangenen Kapiteln besprochenen Dynamiken der Digitalisierung anschlussfähig sein. Dazu wird im ersten Abschnitt die (1) Organisationstheorie von Niklas Luhmann eingeführt und die wesentlichen Elemente der Organisation für unseren Untersuchungsgegenstand vorgestellt. Aufbauend auf dem organisationstheoretischen Verständnis wird im zweiten Abschnitt auf den (2) Risikobegriff eingegangen und die in diesem Kontext relevanten Termini Risiko, Gefahr und Sicherheit aus der Perspektive der Unsicherheitsabsorption betrachtet. Beginnen wir daher nun mit dem Blick auf die Organisationstheorie.

4.1. Organisationssystematik und Selbstreflexion von Unternehmen

Um die Beschaffenheit von Unternehmen als Organisationen besser verstehen zu können, beginnen wir in diesem ersten Abschnitt mit einer Annäherung an den organisationstheoretischen Hintergrund. Aufbauend auf einer Diskussion der grundlegenden Organisationsystematik und des Risikobegriffs, können wir dann schließlich die notwendigen Risikokontrollsysteme in Reaktion auf die gestiegenen Sicherheitsdispositive für Unternehmen in den nachfolgenden Kapiteln erarbeiten. Dazu werden wir in diesem und den folgenden Abschnitten uns mit den Struktur- und Zuschreibungsformen von Unternehmen als handelnden Organisationen, sowie der Zuordnung von Entscheidungen innerhalb komplexer Entitäten beschäftigen. Die Anwendung von Luhmanns Idee der Risikoverarbeitung von Organisationen als autopoietische Systeme bietet sich in diesem Kontext an, eröffnet sie doch aufschlussreiche Erkenntnisse über den Umgang mit Risiken in Unternehmen, wie es beispielsweise von Dirk Baecker für Banken diskutiert wurde (Baecker 1991). Wir beginnen mit der selbstreferenziellen Betrachtung von Organisationen unter dem (1) Überbegriff der Autopoiesis und erarbeiten den Organisationsbegriff von Unternehmen über die Zuhilfenahme von Niklas Luhmanns Organisationssoziologie und der (2) Abgrenzung von Systemen gegenüber ihrer Umwelt.

4.1.1. Autopoiesis von Organisationen

Am Beginn steht die Frage durch was sich eine Organisation auszeichnet? Eine Organisation ist im Allgemeinen eine semantische Umschreibung mit unterschiedlichen Ausprägungsformen bezüglich einer definierten Entität von Abläufen, Regeln und Entscheidungen, derer sich sowohl ihre Mitglieder im Klaren sind, als auch die Umwelt von der Organisation Kenntnis nimmt. Letzteres kann in Form von Entscheidungen oder Außenprojektionen beziehungsweise Kommunikation erfolgen.[145] Dieser Begriff soll im Weiteren für Unternehmen konkretisiert werden. Dabei kann eine grundlegende Annahme Luhmanns helfen, welche auf einen Kernbegriff der biologischen Bewusstseinsforschung referenziert. Dieser legt, vereinfacht ausgedrückt, durch die Umschreibung der Autopoiesis ein komplexes Zusammenspiel von Zuordnung und Unterscheidung dar, auf dessen Basis lebendige Organismen von nicht-lebendigen differenziert werden können (Maturana und Varela 1980). Der einleitende Gedanke basiert auf der Frage was Objekte unterscheidet, wenn essentielle Funktionen ähnlich erscheinen, aber grundlegende Voraussetzungen nicht gegeben sind um das Objekt oder ein

[145] Vgl. Abgrenzung durch Entscheidungen bei Niklas Luhmann (Luhmann 2000: 45).

System als lebendig zu bezeichnen (Mingers 1989: 160)[146] Ein Problem, welches in der biologischen Literatur besonderer Beachtung wiederfuhr (Luisi 2003), aber auch für die soziologische Fragestellung in Richtung der Beschaffenheit von Organisationen relevant ist.

Das autopoietische System wird im originären, biologischen Kontext als selbst-referenzielle Komponenten beschrieben, welche durch eigene Interaktionen das System in dem sie agieren selbst erzeugen und dieses als System selbst anerkennen.[147] Übertragen auf ein System von soziologischer Betrachtungsrelevanz bedeutet dies, dass die Quelle autopoetischer Eigenbeschreibung über Kommunikation und Entscheidungen erfolgt, welche nur innerhalb des Systems als solche anerkannt werden und innerhalb eines Netzwerks in autorisierter Form produziert und reproduziert werden (Luhmann 1986: 173). Der Transfer aus dem originären Kontext in die Organisationssoziologie ist nicht als Analogie zwischen organischen und sozialen Systemen einzuordnen, sondern im Kontext einer angepassten Begriffsbesetzung und Umdeutung auf die Fragestellungen und Problematik der Organisationsforschung zu verstehen. Das durch Niklas Luhmann in seinem Werk *Soziale Systeme* zugrunde gelegte Gedankenkonstrukt selbstreferenzieller Systeme (Luhmann 1984) wurde in den folgenden Jahren mehrfach aufgegriffen, um die Sichtweise auf das Verständnis von Organisationen in der Literatur kritisch zu hinterfragen und um den Aspekt sich selbst erschaffender Systeme zu erweitern (Hernes und Bakken 2003: 1511f.).

Für die Definition von Organisationen als autopoietische Systeme ist Kommunikation von Entscheidungen neben der oben eingeleiteten Differenzierung zwischen Systemen und Elementen, in dem letztere durch ihre Reproduktion das System erschaffen (Baecker 1991: 34) zu nennen. Kommunikation fungiert als ein wesentliches Unterscheidungskriterium im Kontext von sozialen Systemen, das allerdings über das Verständnis der Übermittlung von Informationen zwischen einem Sender und einem Empfänger hinausgeht und Kommunikation als Prozess der Selektion beschreibt (Vanderstraeten 2000: 586). Als solche ist Kommunikation in Form der ihr beiwohnenden oder nachfolgenden Handlungen sichtbar und dadurch für den Beobachter in Kategorien zu fassen, welche die Eigenproduktion des Systems von innen heraus

[146] Ein Beispiel referenziert zur Erklärung des Konzepts auf den Unterschied zwischen einem Auto und einem Pferd, beide geeignet um Personen oder Ladung zu transportieren. Beide benötigen Energiezuvor und Unterhalt, aber dennoch wird gemeinhin nur eines der beiden Objekte als lebendig bezeichnet (Mingers 1989: 159f.).

[147] Die Autopoiesis als Konzept beschreibt bewusste, selbstreferenzielle Komponenten im Gegensatz zu Systemen, welche aus ihrer Umgebung und im Verlauf eines Prozesses der natürlichen Auswahl hervorgehen. Aus dieser Perspektive entstehen Organisationen als autopoietische Systeme aus einer Selbsterschaffung qua Eigeninteraktion. Die rekursive Produktion und Reproduktion der Systeme wurde später auch auf die Organisationsforschung übertragen und begründete einen angeregten Diskurs über die Angemessenheit des Transfers und seiner Anwendung auf die soziologische Forschung (Hernes und Bakken 2003: 1511f.).

beschreiben können (Hernes und Bakken 2003: 1514). Doch weil Kommunikation nur im Verbund mit anderer Kommunikationsakten verstanden werden kann, spielen die systeminhärenten Selektionsmechanismen eine zentrale Rolle (Luhmann 1984: 203), darunter auch die Akzeptanz oder Ablehnung einer Information. Inwiefern allerdings vorausgehende Kommunikationsmuster und Prägungen in die (Re-)Produktion von Kommunikation Einfluss finden ist nicht eindeutig. Exemplifizierend führen Seidl und Mormann dazu aus, dass jede Situation ihre eigene Erwartungshaltung an Kommunikation beinhaltet und jede Frage eine *angemessene* Reaktion erwarten lässt, welche auf vorausgehenden Normbeschreibungen und Erfahrungen[148] beruhen und jene Erwartungen vorbestimmen (Seidl und Mormann 2004: 17).

Im Rahmen der selbstreferenziellen Systemproduktion und Reproduktion werden Anschlussoperationen ermöglicht, welche erneute Entscheidungen und Operationen seitens der Elemente des Systems ermöglichen. Als essentieller Bestandteil der Systemfunktionsweise müssen diese Entscheidungen und Operationen kommuniziert werden um zur Kenntnis genommen zu werden und weitere Anschlussoperationen ermöglichen zu können (Baecker 1991: 34). Dies führt zu der Erkenntnis, dass die Zusammensetzung des Systems aus selbstreferenziellen Komponenten hervorgegangen ist, die sich ihrer Aktivitäten durch Kommunikation bewusst sind. Ferner müssen diese Komponenten fortwährend reproduzierend tätig bleiben, um dadurch das System wiederholt zu definieren. Diese Beobachtung von Niklas Luhmann werden wir im fünften Kapitel erneut aufgreifen, um den Zusammenhang von Informationsnetzwerken und Interdependenzen von (Informations-)Systemen, Technologiekomponenten und Organisationen im digitalen Zeitalter, sowie deren Risikoexposition aufzuzeigen.

Die aus der Autopoiesis hervorgehende Beschreibung von Systemen verbleibt daher zunächst Ausgangspunkt zur näheren Betrachtung von Organisationen. Denn die für unsere Arbeit interessante Fragestellung des organisationsinternen Umgangs mit Risiken unter besonderer Beachtung der Rolle von Entscheidungen wird in Luhmanns späterem Werk *Organisation und Entscheidung* (Luhmann 2000) entscheidend konkretisiert. Hier bezieht sich die Autopoiesis nun stärker auf Entscheidungen, durch welche sowohl die Handlungsfähigkeit von Organisationen nach innen, also gegenüber ihren Mitgliedern, als auch nach außen gegenüber

[148] Die Determination autopoietischer Systeme im Rahmen der Digitalisierung wurde bereits im vorausgehenden Kapitel thematisiert, als über die Entwicklung selbstlernender Algorithmen auf Basis einer selektiven empirischen Datenmenge gesprochen wurde, um die polizeiliche Arbeit und Straftatvereitelung zu unterstützen (Mohler et. al. 2015: 24). Das somit entstandene digitale Netzwerk bediente sich in diesem Fall der (vom Beobachter zunächst unterschätzten) Erkenntnisse und Erfahrungen der analogen Welt, war also wenig überraschend geprägt durch seine eigene Vorselektion.

der Umwelt artikuliert werden kann. Die hier entworfene Definition einer Organisation beruht maßgeblich auf der Rolle und Funktion von Entscheidungen. Dazu zählt auch die Unterscheidung des Zeitpunkts einer Entscheidung (ebd.: 45ff.). Denn ein in sich abgeschlossenes System „versorgt sich selbst über die rekursiven Vor- und Rückgriffe seiner Operationen mit den Informationen, die es braucht um seine Operationen rekursiv vernetzen zu können“ und dadurch die „eigentliche Reproduktionsleistung des Systems“ mithilfe einer temporalen Unterscheidung zu erbringen (Baecker 1991: 36).

Die genaue Bestimmung des Zeitpunkts einer Entscheidung sowie ihrer Folgen liefert einen signifikanten Beitrag zur Abgrenzung zwischen einem Vorher und einem Nachher in der Bewertung über den Organisationsbeitrag zur Reproduktion des Systems. Auch die Abgrenzung eines Systems zur Außenwelt und ihrer Perspektive auf ein Innen und ein Außen verläuft entlang der temporalen Differenzierung. Neben der Entscheidungsfähigkeit selbst ist daher das Vermögen zur Selbstreflexion als notwendige Bedingung anzutreffen. „Ein System, das sich selbst erzeugt, muss sich selbst beobachten, das heißt: sich selbst von seiner Umwelt unterscheiden können“ (Luhmann 2000: 47) und somit eine eigene von fremden Entscheidungen differenzieren können. Selbstbeobachtung und die Fähigkeit zur Entscheidungsfindung stehen somit in einem direkten Zusammenhang.[149] Umso mehr versteht sich eine Organisation als wandlungsfähige Entität im stetigen Austausch und Abgrenzungsvollzug zur Außenwelt.

Diese Eigenschaft ist für Unternehmen von großer Bedeutung, erst recht in einem kompetitiven Marktumfeld.[150] Diese Determinanten zu identifizieren und zu verstehen ist eine beständige Herausforderung für Unternehmen, geeignete Lösungen und Entscheidungen insbesondere innerhalb der zur Verfügung stehenden Zeit zu finden. Dies kann wie im Fall der Entscheidungen zum Einsatz neuer Technologien zu schwierigen Abwägungsprozessen führen, deren Ausgang im schlimmsten Fall das Ende der unternehmerischen Tätigkeit bedeuten kann (Buchholz und Wangler 2016: 182). Entscheidungen müssen daher auf der Grundlage des individuellen Verhältnisses von Unternehmen zur (subjektiv wahrgenommenen) Unsicherheit aufgrund einer unzureichenden Informationsgrundlage getroffen werden. „Allgemeiner gesagt: die Umwelt der Organisationen absorbiert nicht genug Kontingenz, sodass die Organisation

[149] Denn das Unternehmen wird nicht als unveränderliches Objekt verstanden, sondern aktiv auf seine eigenen Strukturen einwirken und auf Veränderungen reagieren. Das Unternehmen als autopoietisches System ist somit auch in der Lage seine Strukturen und Prozesse in Anpassung an die Umwelt zu modifizieren.

[150] Wie wir im zweiten Kapitel gesehen haben betrifft dies potentielle Marktanteilsverluste, Veränderungen der Kundenkommunikation (Welzbacher et. al. 2015: 18), Produktion- und Absatzmodalitäten sowie der internen Strukturen und Kommunikation von Entscheidungen innerhalb von Unternehmen. (Arnold et. al. 2016: 7).

sich nicht mit einem Errechnen von einzig-richtigen Entscheidungen begnügen kann. Sie muss ohne ausreichendes Wissen und mit abgekürzter Informationsverarbeitung selber entscheiden“ (Luhmann 2000: 27). Der Kommunikation der Entscheidung sollte daher besondere Beachtung geschenkt werden, da erst durch diese die Entscheidung wahrgenommen wird und als Anknüpfungspunkt für Nachfolgeoperationen im obigen Sinne zur Verfügung steht.

Die Formen und der Umfang der Kommunikation können in differenzierter Weise in Erscheinung werden und sich je nach Kontext unterscheiden. Ein häufiges Kommunikationsmittel von Unternehmen unter diesen Voraussetzungen ist einem Vorschlag von Dirk Baecker folgend durch Zahlungen repräsentiert. Die Höhe und die bilateral getroffene Einschätzung über die Rechtfertigung von Preisen im Verhältnis zu Leistungen bestimmen den Kommunikationsfluss, sie spiegeln vorausgegangene Entscheidung wieder und ermöglichen zudem Anschlussoperationen (Baecker 1991: 42f.). Eine mit Blick auf Unternehmen aufschlussreiche Feststellung, da der Kreislauf von Zahlungen und Verpflichtungserfüllungen den Handlungsrahmen vom Unternehmen vorgibt. Die Fortsetzung, also Anschlussoperation der finanziellen Transaktion erfolgt durch Verbuchungen und Wiederbereitstellung von Mitteln für erneute Zahlungen. Die Interaktion zwischen Organisationen über Zahlungen und Gegenleistung leitet zudem auf die Beziehung von autopoietischen Systemen zu ihrer Umwelt über, denen wir uns im Folgenden zuwenden wollen.

4.1.2. Abgrenzung von Systemen

Ein Versuch zur Eigenidentifikation von Organisation kann über die Abgrenzung zur Umwelt erfolgen.[151] Die Interaktivität zwischen den internen und externen Bereichen verläuft über Entscheidungen und die Kommunikation von Informationen. Letztere werden als Inhalte angesehen, deren Kenntnisnahme Einfluss auf das Ergebnis hat, so dass ein Unternehmen in seiner Wesensbeschreibung als „informationsverarbeitendes System“ in Erscheinung tritt (Luhmann 2000: 57f.). Dies gilt auch für die Kommunikation von Entscheidungen. Da sich letztere zum einen durch ihre zeitliche Unterscheidbarkeit, aber auch durch die Kommunikation ihrer (nicht getroffenen) Alternativen definiert, wird die Entscheidung gegenüber anderen möglichen Optionen abgesetzt (ebd. 64). Ohne die Kenntnisnahme einer Alternative, würde die Entscheidung nicht als solche hervortreten, sondern lediglich als Ereignis erscheinen.[152]

[151] Die Identitätsfindung des Unternehmens geschieht unter Einbeziehung der Außenwelt. „Was im Organisationssystem als Umwelt beobachtet wird, ist immer ein eigenes Konstrukt, also eine Ausfüllung der Fremdreferenz des Systems“ (Luhmann 2000: 52).

[152] Die Interaktion mit der Umwelt kann gestalterisches Potential aufweisen. Die Möglichkeiten des Informationszeitalters zur Schaffung und Formierung von Märkten zeigt sich in dem Beispiel von Handyapplikationen und Spielen: Mobile Device Games sind Handyspiele, die häufig kostenlos von einer

Die gewählte Form der Kommunikation eröffnet somit die Möglichkeit von Organisationen ihre Grenzen dank der Systeminhärenten Selbstreflexion zu erkennen und verändern zu können. Die Abgrenzung zur Umwelt erfolgt über die Beobachtung der Reaktionen auf Kommunikationsakte aus der Umwelt von Organisationen.[153] Dazu muss die Artikulation von Entscheidungen als exklusive Organisationskommunikation verstanden werden, denn „Organisationen erkennen nur Kommunikationen ihrer Mitglieder als eigene an, und nur, wenn sie qua Mitgliedschaft kommunizieren" (Luhmann 1991: 202). Die Unterscheidung zwischen Mitgliedern und Außenstehenden trägt ebenfalls zur Abgrenzung zur Umwelt bei, indem die vorherige Einigung über die Gruppe der Kommunikationsberechtigten, in Unternehmen wäre von Handlungsbevollmächtigen zu sprechen, die eigene Kommunikation autorisiert und die Reaktionen der Außenstehenden bewertet. Die Definition von Zuständigkeit und Mitgliedschaft sind auch dahingehend relevant, als dass die Etablierung einer resilienten Organisation auf der grundsätzlichen Entscheidung aufbaut, was genau zur Organisation gehört, folglich welche Werte zu schützen sind und welche Bereiche in die Entscheidung über mögliche Wiederherstellungsstrategien einzubeziehen sind.[154] Erst die Fähigkeit zur Selbstreflexion erlaubt diesen Schritt und eröffnet die Möglichkeit den Status quo zu dokumentieren und Prioritäten zu setzen (Braes und Brooks 2010: 17).

Diese Autoreflexion betrifft auch die Abgrenzung von Unternehmen nach Außen, denn es steht selbst im Austausch mit anderen Unternehmen, Regulatoren und Kunden, also anderen Interaktionspartnern.[155] Auslagerungen von Arbeitsschritten oder Prozessen sind Teil unternehmerischer Strategien zur ökonomischen Steuerung und Optimierung (Sako 2006: 503). Beispielsweise kann die Auslagerung von Prozessen in Unternehmen als rechtlicher und organisatorischer Schritt vollzogen werden, um Kosten zu senken[156] oder Effizienz durch

zentralen Plattform für Handyapplikationen wie dem iStore oder Playstore heruntergeladen werden können. Diese Spiele entfalten ihr Geschäftsmodell durch das Angebot von „Abkürzungen", etwa in Form von Spielgeld, welches sich durch den Tausch von realer in digitale Währung erwerben lässt. Erst die Entwicklung von kostenlosen Spielen dieser Art erschuf einen eigenen Markt zum nachträglichen und einträglichen Hinzukauf von Zusatzleistungen. Diese Methode wird in ähnlicher Form auch von Kriminellen verwendet um Nutzer zu erpressen (Hong 2012: 75) oder Malware aufzuspielen (Bhardwaj et. al. 2016: 2), wie wir im fünften Kapitel zeigen werden.

[153] Unternehmen betrachten die Beschaffenheit des Äußeren als logisches Resultat der internen Prozesse, da eine sie auf die Umwelt stets die eigenen Vorstellungen und Paradigmen projizieren. Was folgt ist eine Verschiebung der Verantwortung aus dem Bereich des Unternehmens hinaus in das Umfeld (Luhmann 2000: 37).

[154] Dies betrifft beispielsweise die Sequenz von Prozessen und Ressourcen, welche für die Erstellung von Schutzkonzepten unerlässlich sind (Tierney und Bruneau 2007: 17).

[155] Durch diese Interaktionen etabliert sich ein Wissensaustausch, aber es entstehen auch Abhängigkeiten, welche zu gegenseitigen Verpflichtungen führen. Im Allgemeinen gilt, dass ein Unternehmen allerdings seine Kernfunktionen, wie beispielsweise ein Risikokontrollsystem oder strategische Funktionen nicht an Drittanbieter auslagern sollte, um Einfluss auf die Umsetzung seiner Entscheidungen haben zu können (Sako 2006: 505).

[156] Dies dient dem Zweck einer Kostenreduktion durch Bezug von Dienstleistungen oder Wissen von formell – insbesondere steuerlich oder andere Kostenfaktoren betrachteten - externen Partnern zu erreichen (Goh, Lim und Meng 2007: 166).

Zentralisierung[157] zu steigern (Goh, Lim und Meng 2007: 166). Die Bildung von solchen Konstrukten kann die Verfügbarkeit und Effizienz der Auswertung von Wissen erleichtern und in technologischer Hinsicht zudem Skalierungseffekte von Plattformen und Cloud-Systemen zwischen Unternehmen bewirken (Armbrust et. al. 2010: 52). Daraus leitet sich die Frage ab, wie die ökonomische Rationalität der Digitalisierung aus organisationstheoretischer Sicht die Verantwortung, Kommunikation und Selbstbeschreibung von Unternehmen verändern? Dazu wollen wir im Folgenden die Abgrenzung zu anderen Systemen über die Vernetzung von Produktion und informationsverarbeitenden Prozessen betrachten. Wie wir im zweiten Kapitel gesehen haben, hatte die Einführung neuer Informationstechnologien – und das im beschleunigten Umfang seit Beginn der Corona-Pandemie – eine weitreichende Verknüpfung von Systemen und organisationsinternen Prozessen zu globalen vernetzen Systemen zur Folge.

Unter Vorwegnahme der später im Detail vorgestellten ethnographischen Erkenntnisse, wurden die Interdependenzen zu anderen Systemen und Selbstreferenz zunehmend als Teil der intraorganisationalen Gespräche und Strategiebesprechungen wahrgenommen. Dies betraf auch für das in diesem Fall beobachtete Unternehmen die Rolle von Verknüpfungen mit Organisationseinheiten über die Systemgrenzen hinaus, die entweder Teil der gleichen Unternehmensgruppe oder externen Unternehmen wie Dienstleistern darstellten. Allgemein gesprochen wird in dieser Arbeit die Vernetzung und Verknüpfung zu anderen Organisationen als eine wesentliche Auflockerung des Unternehmens- und Systembegriffs angesehen. Die Beziehungen zu anderen Organisationen können dabei in unterschiedlichen Rechtsformen und Operationsmodellen (zum Beispiel Near-, On-, oder Offshore-Modelle) in Erscheinung treten.

Die Entscheidung für solche Modelle wurde unter anderem dadurch vereinfacht, indem die Transaktionskosten dieser Modelle durch die Digitalisierung gesenkt wurden. So können beispielsweise Kommunikationskanäle und Datenschnittstellen automatisiert werden, um herkömmliche Interaktionsbarrieren und Kosten resultierend aus Sprach-, Kultur, oder Distanzproblemen zwischen den Organisationseinheiten zu überwinden (Choo, Smith und McCusker 2007: 2). Ein anderer Fall der Folgen der Digitalisierung bezieht sich auf die durch Technologie verursachte Verlagerung von konkreten Zuschreibung von Räumlichkeit im

[157] Die gedankliche Fortsetzung der Auslagerung von Prozessen und Organisationseinheiten eines Unternehmens zeichnet das Bild der „lean organisation“, welche sich durch eine Ausrichtung am existenziell notwendigen Organisationseinheiten und der Auslagerung aller anderen, nicht notwendigerweise in Eigenverantwortung betriebenen Prozessen auszeichnet. In einer weiteren Ausprägung kann dieses Modell auch den Einsatz von Automatisierung und Robotisierung bezeichnen, dessen Ziel ebenfalls die Profitabilitätssteigerung durch den Abbau von Lohnkosten ist. „In its most extreme manifestation, it created what has been labeled the ‘hollow corporation’“ (Castells 2010: 176).

Allgemeinen und Zugehörigkeit von Prozessen und Informationen im Speziellen. Denn die Konzentration und Auslagerung von Prozessen durch Plattformdienstleistungen (PaaS, SaaS) stellen das Konzept unveräußerlicher Kernfunktionen eines Unternehmens, durch deren Verlagerung die Eigenbeschreibung und Kommunikationskontinuität wesentlich betroffen wird, in Frage (Xue et. al. 2013: 332f.). Ökonomisch und technologisch kompetitive Cloud-Systeme bieten ihren Unternehmen Lösungen zur Kostenreduktion beziehungsweise Effizienzsteigerung (Armbrust et. al. 2010: 52), selbst für anspruchsvolle Aufgaben und Funktionen außerhalb ihrer nominellen Organisationsgrenzen.

Was bedeutet das für die Abgrenzung zu anderen Systemen und Produktion von Sicherheit in Unternehmen? Im Kontext der nicht-technischen Auslagerung von Prozessen und Leistungen an externe Dienstleister[158], sowie mit Blick auf organisationsübergreifende Wertschöpfungsketten ergaben sich bereits vor der Pandemie Herausforderungen für die Sicherstellung von Produktionsabläufen und Prozessen in Unternehmen (Lee, Yeung und Hong 2012: 543). Die Frage nach der Risikoverantwortung in globalisierten Produktions- und Handelsbeziehungen wurde jedoch durch die Corona-Pandemie erneut Gegenstand des organisationsinternen, aber auch des gesellschaftlichen Risikodiskurses. Dies zeigte sich beispielsweise in der Abhängigkeit des europäischen Marktes von asiatischen Herstellern von Schutzmasken (Ivanov und Dolgui 2020) oder die Produktionsschwierigkeiten von Unternehmen als Folge der Pandemie-bedingten globalen Transport- und Rohstoffengpässe im Frühjahr 2021[159]. Dadurch erweitert sich die Perspektive auf Schutzwerte von sicherheitsrelevanten Objekten in Unternehmen auf Prozesse und systemische Verknüpfungen zu anderen Organisationen. Zusammenfassend betrachtet, wird im Kontext dieser Arbeit vorrangig das Risiko unterbrochener Lieferketten interessant sein, insbesondere die durch die digitale Vernetzung[160] entstandenen Abhängigkeiten zu spezialisierten Infrastruktur- und

[158] Ein Beispiel ist die Externalisierung kritischer Systemkomponenten auf Infrastrukturplattformen von Drittanbietern wie im Fall von Plattform beziehungsweise Infrastructure as a Service (PaaS oder IaaS). In diesem Fall werden die Hardwaregrundlagen und damit eine essentielle Komponente der Wertschöpfung ausgelagert und der organisationsinternen Kontrolle entzogen (Armbrust et. al. 2010: 50).

[159] Die Corona-bedingten Produktionsengpässe bei asiatischen Halbleiterherstellern, die begrenzten Transportkapazitäten sowie die Blockade des Suezkanals im April 2021 durch ein havariertes Containerschiff führten zu einem erzwungenen Produktionsstopp in Produktionsstätten mehrerer Automobilhersteller. Dies ist ein gutes Beispiel für die komplexe Materie der Lieferkettenrisikomanagements. Diese Aspekte werden im vierten Kapitel vertieft (vgl. Handelsblatt 2021).

[160] Die Bereitstellung von technologischer Infrastruktur wie Rechenzentren, Betriebssystemen oder Anwendungen unterliegt hohen Kosten und aufwendiger Wissensakkumulation. Spezialisierte Anbieter wie Dell, IBM oder Amazon haben sich (oder einen Teil ihres Geschäftsmodels) auf die Bereitstellung dieser Infrastruktur als Dienstleistung spezialisiert und können über den Skaleneffekt sowie Informationsbündelung diese Leistungen günstiger anbieten (Nasiri et. al. 2020). In Folge sind die Außengrenzen eines Unternehmens durch die Inkorporation essentieller Bestandteile der Wertschöpfungskette verschoben worden oder zumindest unter anderen Voraussetzungen zu verstehen. Wenn die wichtigsten Bestandteile der Wissensgenerierung wie Algorithmen,

Servicedienstleistern. Dazu bietet sich die Abgrenzung von Organisationen aus Luhmanns Perspektive für die Rolle von Outsourcing und Drittanbietern an (vgl. Luhmann 2000: 236), das wir für das Selbstverständnis von Organisationen im interdependenten Umfeld des Informationszeitalters beleuchten werden. Dazu folgt nun eine detaillierte Betrachtung der organisationsinternen und –externen Schnittstellen von Wissens-, Informations-, und Prozesstransfers innerhalb von Unternehmen im Licht der Digitalisierung.

4.1.3. Technologie, Informationen und Kommunikationsabbruch

Der Transfer von Informationen ist von großer Bedeutung für Organisationen, da sie auf dem Prinzip der Bereitstellung von Anschlussoperationen und deren Kommunikation basieren. Eine erfolgreiche Strategie zur Sicherstellung des Betriebs baut daher auf der fortgesetzten Kommunikationsfähigkeit des Systems auf und benötigt dazu angemessene Risikokontrollsysteme. Letzteres ist allerdings selten vollumfänglich implementiert (Weber 2016: 29), insbesondere wenn systemische und prozessbezogene Risikofaktoren nicht bekannt oder in den Entscheidungen nicht berücksichtigt werden. Wie die Folgen der Vernachlässigung des Risikos der Entscheidung aussehen können zeigte sich in Folge der Corona-Pandemie mit Blick auf die Unterbrechung der physikalischen Lieferketten (Brzoska, Neuneck und Scheffran 2021: 3) oder IT-basierten Prozesse und Kommunikationsstrukturen durch Cyberbedrohungen (Huang et. al. 2021: 626). Wie wir im nachfolgenden Abschnitt im Detail betrachten werden, versuchen Unternehmen aus klassisch-ökonomischer Sichtweise ihre Operationen durchaus abzusichern und Konzepte der Sicherheitsproduktion zu generieren. Eine Strategie zur Reduktion des Risikos basiert auf der Akkumulation von verfügbaren Informationen, deren Verknüpfung durch Technologie und Einführung von Kontrollmechanismen (Luhmann 1991: 37). Diese Maßnahmen werden in Unternehmen als Prozesse der Sicherheitsproduktion durch Risikokontrollsysteme diskutiert und sollen im Folgenden betrachtet werden.

Die grundlegenden ökonomischen Berechnungsmodelle ziehen Rückschlüsse durch den Rückgriff auf Erfahrungswerte wie statistische Risikokalkulation[161], deren Ziel es ist Risiken mithilfe von vernetzen Informationen bestmöglich zu steuern (Best 2010: 38f.). Das Streben

Clouds oder Rechenzentren im Betrieb und Eigentum von Dritten steht, beruht die Organisationsgestalt auf externen Strukturen, mit interessanten Folgen für die Eigendefinition qua Abgrenzung.

[161] Das anthropologische Verlangen nach Sicherheit, trotz unzureichendem Wissen, begründet damit die Suche nach geeigneten Mitteln, um die Zukunft zu antizipieren (Ewald 1991: 289) und besser mit der temporalen Unterscheidung umzugehen, welche Entscheidungen im Sinne der komplexen Entscheidungsgrundlage autopoietischer Systeme innewohnt. Wenn Risiken und deren Kontrolle im Kontext der zuvor getroffenen Spezifizierung verstanden werden, dann sind Finanzinstitute per Definition gezwungen sich mit dem Risiko der Entscheidung auseinanderzusetzen, beispielsweise für oder wider einer Versicherungs- oder Kreditvereinbarung. „Denn von Risiko spricht man nur, wenn eine Entscheidung ausgemacht werden kann, ohne die es nicht zu dem Schaden kommen könnte“ (Luhmann 1991: 25).

nach einer möglichst exakten Risikobewertung spiegelt sich in der Literatur durch Vorschläge und Ideen zur Kalkulation von Risiken, Bewertungsschemata und Analysedesigns wider, deren Grundlage die Verknüpfung von Dateneckpunkten und Erfahrungswerten liegt (Power 2010: 309). An diesem Punkt könnten die Möglichkeiten, welche sich durch die Digitalisierung, ergeben, wie beispielsweise die Erfassung von Informationen, Data-Mining und dem Einsatz künstlicher Intelligenz eine neue Option eröffnen, auch wenn komplexe IT-Landschaften ihre eigenen Ungewissheiten erzeugen (Pauli, Schermann und Krcmar 2010: 259). Der generelle Gedanke folgt dem Narrativ der globalen Vernetzung als Folge der Digitalisierung, in welchem Organisationen wie beispielsweise Versicherungen die potentiellen Schäden in der Zukunft aufgrund der technologischen Innovation exakter und verlässlicher bewerten können (Stoeckli, Dremel und Uebernickel 2018: 287). Teil dieser Veränderung ist das „Big Data-Paradigma“[162], welches die Auswertung verfügbarer, aber unstrukturierter Daten im globalen Kontext durch den Einsatz spezialisierter Risikotechnologie erlaubt und für sich in Anspruch nimmt, das Risiko einer Fehlentscheidung zugunsten des Versicherungsgebers zu verschieben, indem Schadenskosten anhand von Grenzwerten den jeweiligen Risikoappetit des Unternehmens berücksichtigen (Cortis et. al. : 73).

Wenn technologische Lösungen das Wissen um die unzureichende Informationsbasis berücksichtigen, aber die Auswertung und die Transferleistung zwischen Datenmodellen als Grundlage für Risikoentscheidungen bereitstellen, wäre dies nach Niklas Luhmann ein Indiz für den Übergang zu probabilistischen Methoden der Risikomitigation (Luhman 1991: 28). Als Teil dieser Methodologie ist die Abwägung der Wahrscheinlichkeit eine Möglichkeit, die Unvermeidbarkeit von Risiken im Allgemeinen zu akzeptieren und dennoch dem Wunsch nach Sicherheitsmaximierung im Kontext der Ungewissheit nachzukommen (Baecker 1991: 121). Ein Kompromiss, der mit der schnell zunehmenden Zahl an Daten durch unterschiedliche Quellen und Referenzinstanzen, die Möglichkeit einer genaueren Risikobewertung trotz der unbekannten Auswirkungen derart genutzter Technologien zu erlauben scheinen lässt. Denn die Integration verschiedener Technologien, Eingabekanäle und Anwendungsfelder ermöglicht eine bisher unbekannte Informationsverknüpfung und eine darauf aufbauende Entscheidungshilfe. Die multiplen Systemebenen einer IT-Masterplattform oder des Internet-of-Things (das autopoietische System könnte dies als Summe verknüpfter Komponenten

[162] Die Komplexität der eingesetzten Technologie formt und reproduziert das System einerseits durch gegenseitige Kontrolle der involvierten Komponenten oder “Layers”, andererseits durch neue, ungeahnte Sicherheitsproblem: “[I]t can also absorb, dissipate, and deflect forms of risk that might make any one layer more vulnerable, but at the same time, that integration can also distribute and amplify destabilizing forces and factors. This is not a bug; it is axiomatic of platform logics” (Bratton 2015: 101).

betrachten) erlauben Transferoptionen, Reproduktionsgrundlagen und unzählige Opportunitäten für Anschlussoperationen, welche noch vor drei Dekaden unbekannt waren.

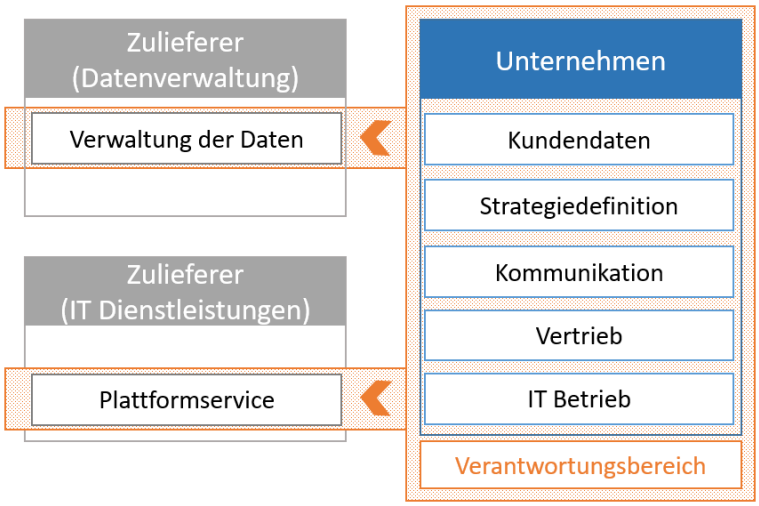

Abb. 4.1. Prozessauslagerung und Verantwortung. Eigene Darstellung.

Die Dateneinträge und Verknüpfungen der automatisierten Informationsbearbeitung generieren somit Anschlussoptionen innerhalb der Organisationskommunikation mithilfe eines technologiegestützten Systems. Das Streben um die Maximierung von Sicherheit führt Organisationen auf die Suche nach einem funktionalen und sicheren Repositorium für Informationen, Entscheidungen und kollektiven Lernerfahrungen. Denn die Dokumentation, Kommunikation und Erinnerung von Informationen beziehungsweise Entscheidungen ist eine wesentliche Voraussetzung für probabilistische Risikomodelle, auf die auch die Kontinuitätsplanung von Unternehmen, hier verstanden als Entscheidungen zur Risikokontrolle beruht.[163] Daher ist nicht nur die Erinnerung an Entscheidungen und die allgemeine Lernerfahrung in Unternehmen relevant, sondern stellt auch eine Steigerung des Schutzwerts zentraler Speichermedien innerhalb der digitalen Wertschöpfungskette zum Zweck der Geschäftsfortführung dar. Zudem verändert sich mit dem gestiegenen Wert auch die Risikoexposition des virtuellen Gedächtnisses in Form von Plattformen und Datenbanken selbst. Denn der durch den Vernetzungstrend geforderte Zusammenschluss von Netzwerken, Systemkomponenten und organisationsexternen Dienstleistern, dessen Vernetzung dem Zweck der besseren Entscheidungserinnerung und Risikosteuerung galt, erhöht auch das potentielle Schadensmaß (Krotofil und Cárdenas 2013: 167).

[163] Wir betrachten die genaue Übersetzung von Risikokontrollsystemen, Risikobewertungen und Kontrolle im Rahmen der Entwicklung von Resilienzstrategien im fünften und sechsten Kapitel.

Ein umfassendes Risikomanagement aller wissensbasierten Prozesse und Speicherbestände ist daher angebracht und sollte eine Bewertung der Risikofaktoren beziehungsweise der Relevanz von Geschäftsbereichen als nicht-ökonomische Entscheidungen in Unternehmen inkludieren (Linkov et. al. 2013: 472). Die Risikotoleranzgrenzen, das bedeutet die Grenzwerte einer noch lohnenden Entscheidung gegenüber der Wahrscheinlichkeit eines Schadensereignisses, können in einem solchen Fall mithilfe von Stresstests und Szenario-Analysen eine Vorstellung des geplanten Vorhabens vermitteln und hinsichtlich seiner Realisierbarkeit und ökonomischen Verhältnismäßigkeit Aufschluss geben. Ferner sind regulatorische Anforderungen branchenübergreifend zu beachten, welche die Weitergabe von Daten im Rahmen einer Kooperation mit Drittanbietern betreffen (BCBS 2012: 5). Dies ist insbesondere der Fall, wenn die Verarbeitung oder Speicherung von Daten über Drittanbieter[164] abgewickelt wird (Schwering 2010: 231). Dazu zählen beispielsweise die Sorgfaltspflicht für die bereitgestellten Daten und der Schutz der Vertraulichkeit, unabhängig von fahrlässigen oder vorsätzlichen Fehlverhaltens des im Auftrag des Unternehmens datenverarbeitenden Dienstleisters.[165] Die Delegierung der Datenverarbeitung an einen Outsourcing-Partners mag somit Kosteneffizienz versprechen, es bedeutet aber keine Aufhebung der Verantwortung und eventueller Rechtsansprüche[166] der Kunden (Gaycken und Krager 2011: 7).

Denn im Fall einer mangelnden Sachkenntnis von Sicherheitsrisiken wie beispielsweise im Kontext der Cloud-Technologie[167], bedeutet das Nicht-Wissen eine Unsicherheitsproduktion

[164] Im deutschen Rechtsraum regelt das Bundesdatenschutzgesetz (BDSG) die Weitergabe von Daten hinsichtlich der expliziten Verantwortung von Unternehmen. Das Bundesdatenschutzgesetz normiert durch seine Novellierung den Umgang mit Daten und trägt somit der Digitalisierung der Gesellschaft Rechnung. Es sind gängige Prozeduren im Fall der Betreuung von Drittanbietern mit der Datenverarbeitung von eigenen oder Kundendaten einzuhalten. Der Schutz und die Verfügbarkeit der Daten obliegt aber weiterhin dem mit den Kunden vertragsführendem Unternehmen, also dem auslagernden Konzern. Vgl. § 11 Abs. 2 Satz 2 Nr. 3 BDSG. Zuletzt aufgerufen am 04.12.2016 unter https://dejure.org/gesetze/BDSG.

[165] „Nach § 11 Abs. 2 Satz 5 BDSG hat sich der Auftraggeber vor Erteilung des Auftrags und auch später regelmäßig davon zu überzeugen, ob die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden; das Ergebnis der Überprüfung hat der Auftraggeber zu dokumentieren“ (Gaycken und Krager 2011: 7). Im Gegensatz zum Outsourcing, also der Ausgliederung von Arbeitsschritten in eine fremde Organisation, ist auch der Begriff des “Offshoring” geläufig. „(…) Offshoring occurs when firms move productive activities overseas, whether they are conducted by separately owned suppliers or by fully owned (captive) subsidiaries” (Sako 2006: 503). “Offshoring“ inkludiert demnach die Verantwortung und den zumindest mittelbaren Zugriff auf die geleisteten Services oder Produktion in einer anderen Region. „Offshoring“ wird zumeist für Produkte angewendet, die von Lohnkosten abhängen und dadurch in einem Niedriglohnland oder einem Rechtsgebiet mit vorteilhafter Rechtslage für die Produktionsbedingungen günstiger produziert werden können. Ein Ausspruch, welcher die Geläufigkeit dieser Praxis reflektiert lautet: „We live in an age of outsourcing” (Grossman und Helpman 2005: 135). Dies umfasst die Internationalisierung der Produktions- und Dienstleistungsabhängigkeiten von unterschiedlichen Akteuren, die zu einem globalen Netz verwoben sind.

[166] Die deutschen Aufsichtsbehörden fordern beispielsweise die pflichtgerechte Ausführung der Informationsschutzes, für die der Direktanbieter verantwortlich ist (Gewald und Dibbern 2007: 256).

[167] Dazu zählen (1) Zulieferer, welche für die Informationsakquise und –Übermittelung zuständig sind, etwa als „Software House“, IoT-Betreiber oder kommerzielle Anbieter, (2) Dienstleistern als Bereitsteller der Infrastruktur, Plattformen oder Anwendungen und (3) Kunden, welche als Privatpersonen in Gestalt von

seitens des Unternehmens. Diese Komponente in der Aufstellung einer digitalen Strategie zur Anpassung des Unternehmens an die Herausforderungen des Informationszeitalters bedarf angemessener Abwägung, denn sie kann im schlimmsten Fall fatale Auswirkungen auf die Bereitstellung von Leistungen oder Güter und somit auf die Existenz des Unternehmens haben. Wenn erst die Fortsetzung der Anschlussoperationen in Form von Kommunikation die Selbstbeschreibung der Organisation ermöglicht (Luhmann 2000: 60), verbindet sich mit ihrer Kontinuität die eigentliche Sicherheitsproduktion im Unternehmen. Umgekehrt bedeutet das, dass nur wenn der Kommunikationsabbruch verhindert werden kann, auch die Fortexistenz des Unternehmens und damit seiner gesellschaftlichen Rolle als Bereitsteller von Waren und Dienstleistungen dem Sicherheitsdespositiv gerecht werden kann.

Zusammenfassend kann damit festgehalten werden, dass die Entscheidung zur Auslagerung von vitalen, für das Unternehmen als elementarer Bestandteil ihrer Kommunikationsprozesse verstandenen Werte, wie beispielsweise Kundendaten, Algorithmen oder Prozessen auf die technologischen Systeme von Drittanbietern eine sicherheitsrelevante Rolle spielt. Dies sollte daher für die Selbstreflexion von Unternehmen und der Bedeutung im Kontext ihrer Autopoiesis berücksichtigt werden. Denn die Auslagerung über die definierten Außengrenzen des Unternehmens hinaus bedeutet auch erhebliche Konsequenzen für die Verantwortungszuschreibung von Schutzkonzepten und Kontrollsystemen (Armbrust et. al. 2010: 54). Damit ist nicht die Entkoppelung oder Rückführung von ausgelagerten Funktionen und Informationen gemeint, sondern zielt normativ auf die Etablierung funktionsfähiger Risikokontrollsysteme ab.

Die Vorteile einer Verknüpfung von Netzwerken und Informationsbeständen ermöglicht die Verbesserung der Wissenssteuerung in und zwischen Unternehmen, deren Resultat in Form von komplexen Kooperationsmodellen[168] in Erscheinung treten kann (Castells 2010: 172). Die strukturelle und prozessorientierte Auswertung der Daten muss aber systematisch geplant und implementiert werden, um der Sicherheitsproduktion dienlich zu sein. Eben diese Entwicklung fand - wie wir es im sechsten Kapitel verdeutlichen werden - in dem durch die Corona-

Informationsschaffenden, -Empfangenden oder Objekte der Information in Erscheinung treten. Ferner können kommerzielle Empfänger von Informationen als Abnehmer von Informationen etwa über private Kundengruppen als Prozessteilhaber erscheinen.

[168] Unternehmen wie Google, Microsoft oder Amazon konnten durch die Verknüpfung von Informationen und Systemen zwischen ihren Unternehmen, Sub-Unternehmen, Kooperationspartnern und Dienstleistern etabliert und „bewusst Bestehendes mit neuem Wissen [kombiniert], um in neue Märkte vorzudringen“ (Hettich, Schimmer und Müller-Stewens 2015: 60). Dadurch setzt sich ein Kreislauf der Datenakkumulation in Gang und resultiert in anhaltenden Interaktionsbeziehungen zwischen Anbietern, Produzenten und Kunden (Hettich, Schimmer und Müller-Stewens 2015: 55), deren Austausch auf der Wissensteuerung der verfügbaren Informationen beruht.

Pandemie bedingten Digitalisierungsschub in vielen Fällen nicht statt (Chigada und Madzinga 2021: 5) und führte zu den genannten problematischen Folgen für die Sicherstellung von Anschlussoperationen sowie einhergehende Sicherheitsproduktion. Während analog zu Luhmann die wesentliche Rolle in der Entscheidung über die Auslagerung von Prozessen oder Einführung von Technologien liegt, ermöglicht es die Etablierung von Risikokontrollsystemen Unternehmen dennoch in die Sicherheitsproduktion in ihren eigenen Organisationen eingreifen zu können. Daher wollen wir im zweiten Abschnitt dieses Kapitels die Begriffe Unsicherheit, Risiko, Gefahr und Entscheidung näher betrachten und eine Differenzierung zwischen „traditionellen" Anasätzen des Risikomanagements gegenüber einem prozessorientierten Verständnis von Risikokontrollsystemen im Sinne unserer Fragestellung vornehmen.

4.2. Unsicherheitsabsorption

Die Unsicherheit, unter deren Bedingung Unternehmen Entscheidungen zu treffen haben, betrifft beide Bereiche, das heißt klassisch-ökonomische, aber auch nicht-ökonomische Probleme und Situationen. Die ökonomische Rationalität in Führungsebenen von Unternehmen hat in den meisten Fällen für ökonomischen Entscheidungen Anwendung gefunden und wurde Teil der alltäglichen Routine (Pfeifer 2006: 11). Nicht-ökonomische Entscheidungen, etwa Fragen der Sicherstellung interner Prozesse und Anschlussoperationen trotz exogener Gefahren für den Betrieb, wie im Fall der Corona-Pandemie, stellen hingegen andere Herausforderungen an die unternehmensinterne Logik und ihre Entscheider. Für Luhmann bietet sich daher aus der Organisationssystematik und Autopoiesis kommend die Einführung der Unsicherheit und des Risikos an. Wie wir im Folgenden zeigen werden, ist für das Risiko „nur ausschlaggebend, daß der kontingente Schaden selbst kontingent, also vermeidbar, verursacht wird" (Luhmann 1991: 25). Durch die Entscheidung selbst wird das Risiko als Folge der Unsicherheit eingeführt, denn das Nicht-Wissen über den späteren Ausgang erschwert der Führungsebene die Auswahl unter möglichen Optionen (Baecker 1991: 119). Insbesondere für nicht-ökonomische Fragestellungen wie etwa sicherheitsrelevanter Entscheidungen stehen der ökonomischen Entscheidungslogik nur begrenzte Erfahrungswerte zur Verfügung.[169] Unter dem Eindruck der Corona-Pandemie war die Unsicherheit über die Wahl der angemessenen Maßnahmen und

[169] Dies gilt insbesondere für gewinnorientierte Unternehmen, welche über die Relevanz möglicher Verluste und Schäden möglichst verlässliche Gewissheit suchen, aber dennoch Entscheidungen unter den Bedingungen einer ungewissen Zukunft treffen müssen. Unternehmen sind zudem von ihrer Umwelt in zwei Wahrnehmungswelten separiert. Beide Wissensbereiche bewegen sich in unterschiedliche Sphären und speichern unterschiedliche Informationen über Risiken, was die Unsicherheit jeweils erhöht. Somit wäre die „Unerreichbarkeit der Umwelt die Quelle aller internen Unsicherheit" (Luhmann 2000: 209). Man denke beispielsweise an ein Unternehmen, welches im Ungewissen über Novellierungen der Aufsichtsbehörden von weiteren Investitionen Abstand nimmt.

Entscheidungen zur Sicherstellung der eigenen Prozessfortführung besonders hoch (Wentland und Klimburg-Witjes 2021: 185).

Im Gegensatz dazu stellen die Entscheidungsprogramme aus Luhmanns Organisationstheorie eine Verbindung zwischen der Entscheidung und bekannten Mechanismen, der Routine des Handelns, her. Doch im Fall der Entscheidungsprogramme sind Erfahrungen und Wissen notwendig, dass für die spezifischen Fälle der unternehmerischen Sicherheitsproduktion nur selten oder wie im Fall der Reaktionen auf die Pandemie und der Folgen des technologischen Risikos nur sehr geringfügig bekannt sind. In Luhmanns Worten macht das es unwahrscheinlich, dass „die Organisation es auf diese Weise vermeiden kann, aus dem unglücklichen Verlauf zu lernen. Lernen würde heißen: aus einem für unwahrscheinlich gehaltenen und vermutlich auch weiterhin unwahrscheinlichen Einzelfall Konsequenzen zu ziehen und die für alle Fälle geltenden Entscheidungsprogramme zu ändern“ (Luhmann 1991: 210). Dazu führt Luhmann auch an, dass das „Hauptproblem dieser Programme (…) ein Problem des Gedächtnisses [ist]. Sie müssen erinnert und gegebenenfalls rasch aktualisiert werden können, auch wenn sie nie angewandt werden“ (Luhmann 2000: 271f.).

Ein Zweig der Organisationsforschung hat daher den Begriff des Risikos und dessen Umgang in Organisationen stärker betrachtet und die Umwelterzeugung von Entscheidungs-problematiken analysiert. In deren Folge sind auch durch andere Disziplinen eine Vielzahl an Konzepten und Kategorien hervorgebracht worden (vgl. Baecker 1991: 117), über deren Typologie die Literaturübersicht im ersten Kapitel bereits Aufschluss gab. Der zentrale Charakter der Unsicherheit über eventuelle Ausgänge einer eingeschlagenen Richtung gibt daher den Anknüpfungspunkt für unsere nächsten Schritte, um die Herangehensweise an Risiken, sowie ihre Kategorisierung, Bewertung und Kontrolle weiter zu untersuchen, um die Entscheidungen und Vorbereitungen von Unternehmen auf exogene Problemfelder außerhalb ihrer gewohnten ökonomischen Expertise zu verstehen. Denn die Kontrolle von Risiken, welche im Sprachgebrauch von Unternehmen als Risikomanagement[170] verstanden wird, stellen den geläufigen Ansatz dar, um einen planbaren Umgang mit der Situation der Unsicherheit zu ermöglichen.

[170] Risikomanagement bezeichnet entweder eine Reihe von methodischen Maßnahmen, um ein Kontrollstruktur für Risiken in Organisationen zu implementieren oder als Funktion die zweite Schutzebene im internen Steuerungssystem nach der Definition des Institute of Internal Auditors (IIA 2013). Kritische Stimmen fügen jedoch mit Blick auf die Unsicherheitsabsorption an, dass Risiken im eigentlichen Sinne nicht gehandhabt werden, sondern lediglich kontrolliert werden können, da ihre inhärente Eigenschaft die Unvorhersagbarkeit ist (Krahmann 2007:8). Wir werden im Folgenden von einer solchen Kontrolle ausgehen, auch wenn der übliche Ausdruck des „Risikomanagements“ verwendet wird, welcher sich auf die unternehmensinterne Funktion bezieht.

Wir werden uns daher zunächst die (1) Entscheidungsgrundlagen unter den Bedingungen der Unsicherheit ansehen, bevor wir im nächsten Schritt auf die (2) Begriffe Risiko, Gefahr und Entscheidung näher eingehen. Anschließend werden die (3) Risikokontrollsysteme in Unternehmen und damit die geläufige, routinierte Antwort von Unternehmen zur Vorsorge gegen exogene Problemstelllungen vorgestellt. Dazu gehören auch die sich anschließenden Felder der Identifikation und Bewertung von Risiken, auf deren Grundlage Unternehmen Entscheidungen ihrer ökonomischen Logik folgend treffen. Die Übersicht über die bisherigen Praktiken der unternehmensinternen Risikobewertung werden wir hier als traditionelle Methodik vorstellen und in den anschließenden Kapiteln mithilfe der Ergebnisse unserer ethnographischen Untersuchung zeigen, warum und in welcher Form diese Herangehensweise in Unternehmen einen Änderungsprozess durchläuft. Es ist wichtig anzuführen, dass diese traditionellen Muster eine Beobachtung aus der unternehmensinternen Routine und Praktiken widerspiegelt und erst im Zuge der drängenden und globalen Implikationen der Digitalisierung einem signifikanten Wandel unterzogen wurden, wie die späteren Kapitel zeigen werden. Auf dem Weg zu diesem Teil unserer Argumentation über die Praktiken der Sicherheitsproduktion in Unternehmen müssen wir zunächst jene traditionellen Risikomuster beleuchten, um den Veränderungsprozess darlegen zu können.

4.2.1. Umgang mit Unsicherheit

Unternehmen haben die Möglichkeit mithilfe des Risikomanagements, also der im ökonomischen Umfeld etablierten Funktion eines Unternehmens zur Steuerung von Risiken, auf die sie umgebenden Unsicherheit zu reagieren (Ward 2003: 7). Die aus den Bedingungen der Unsicherheit resultierenden Risiken werden durch das Risikomanagement als Kategorien für die Unternehmensperformanz im Kontext ihrer ökonomischen Rationalität artikuliert (Pfeifer 2006: 11) und Strategien entwickelt diese im Rahmen ihrer Möglichkeiten bestmöglich zu steuern (Miller 1997: 312). Doch diesem Anspruch unterliegt die kontrovers diskutierte Möglichkeit, Risiken überhaupt objektiv bewerten und kontrollieren zu können (Clapton 2011: 281ff.). In diesem Themenkomplex finden sich verschiedene Interpretationen des Risikobegriffs, die von der klassischen Entscheidungstheorie in der Ökonomie bis hin zu post-strukturalistischen Ansätzen reichen (vgl. Clapton 2011). An dieser Stelle sollen die einzelnen Theorien allerdings nicht vertieft werden, sondern ausschließlich festgehalten werden, dass für die soziologische Organisationsforschung Risiken in verschiedenen Facetten diskutiert werden (Jarvis 2008; Faulkner et. al. 2021). Für unsere Fragestellung ist vor allem der Umgang mit exogenen Sicherheitsproblemen unter den Bedingungen der Unsicherheit und deren Übersetzung in die Sicherstellung von Prozessen und Anschlusskommunikation in

Unternehmen relevant. Für Unternehmen drückt sich dies vorrangig in der durch die ethnographische Untersuchung getätigte Beobachtung[171] aus, dass die Beschränkungen von Informationen und Folgeabschätzungen insbesondere im Fall unbekannter Risikokategorien im Denkmuster des traditionellen, objektbezogenen Risikobegriffs problematisch für die routinierten Risikopraktiken sein können (Petersen 2017: 130).

Die Unvorhersehbarkeit von Implikationen, etwa durch die Einführung oder schnellen Ausdehnung neuer Technologien, verlangen daher nach geeigneten Mechanismen zum Umgang mit der Unsicherheit. Sicherheitsproduktion unter diesen Umständen bedeutet daher auch einen adaptiven, agilen Anspruch an Strategien und Risikokontrollen zu stellen, um vitale Prozesse und Leistungen aufrechtzuerhalten (Blum et. al. 2016: 156). Bei Luhmann findet sich dazu die prägnante Aussage, dass die Wirksamkeit des Risikomanagement in Organisationen nicht ausreicht, „um ihnen Sicherheit zu gewähren; es dient nur dem bestmöglichen Umgang mit Unsicherheit“ (Luhmann 1991: 197). Dies steht der traditionellen Annahme gegenüber, dass die aus der Unsicherheit über zukünftige Entwicklungen abgeleiteten Risiken zu einem gewissen Grad zu klassifizieren und vorherzusagen sind (Bradbury 1989: 381). Für den Fall der unternehmensrelevanten Risiken, welche aus der zum Einsatz kommenden Informationstechnologie hervorgehen, besteht die spezifische Schwierigkeit die Tragweite und Folgen dieser Risiken auf der Grundlage der verfügbaren Daten einzuschätzen (Linkov et. al. 2013: 472). Schließlich kann jedes Berechnungsmodell nur die Daten sammeln, die dem Beobachter vorliegen, was auch für die IT-basierten Modelle der Sicherheitsproduktion durch Folgenabschätzung angeht.[172].

Das Feld der digitalen Domäne wird zudem durch die neuen Technologien und gerade wegen der Entwicklungen in Folge der Pandemie sowie beständigen Weiterentwicklung einem hohen

[171] Die hier angesprochene Beobachtung speist sich aus der im ersten Kapitel beschriebenen beobachtenden Teilnahme im operationellen Risikomanagement von MNU. Die Verschiebung vom traditionellen Risikomanagement über die Erfahrungen aus der Corona-Pandemie und der langjährigen Einführung digitaler Strukturen eröffneten im strategischen und operativen Entscheidungsprozess zuerst die Erkenntnis, dass die traditionellen Methoden keinen ausreichenden Schutz boten und daher durch eine neue Herangehensweise unter dem Überbegriff prozess-orientierter Risikokontrollsysteme schrittweise ersetzt werden (Hintergrundgespräch 08.06.2021).

[172] Da es sich bei den Risiken der Informationstechnologie um ein relativ neues Phänomen handelt, liegen weniger konkrete und risikorelevante Informationen vor, als beispielsweise über Naturkatastrophen oder andere traditionelle Risikokategorien (AGCS 2013: 7). Dennoch bestehen Ansätze die allgegenwärtige Quantifizierung und Auswertung von Daten zur Prädiktion einzusetzen. Die verfügbaren Ressourcen und Anwendungsfelder erlauben „to act decisively and procedurally in the face of radical uncertainty” (Amoore und Raley 2016: 2) und wecken Hoffnungen einer effektiven Reduktion von Risiken. Doch diese Technologie tragen selbst zu einem Risiko bei, wenn ihre Folgen nicht sorgfältig abgewogen werden.

Maß an Unsicherheit ausgesetzt sein.[173] Um diese Unsicherheit absorbieren zu können, suchen Unternehmen eine Lösung in Form der Risikomitigation, um somit den unternehmerischen Fortbestand zu sichern. Unternehmen müssen sich also insbesondere unter den Bedingungen Unsicherheit über deren Auswirkung für eine Form der Unsicherheitsabsorption entscheiden[174]. Für die dazu gewählten Ansätze der Risikokontrolle wird dies darüber hinaus eine Kartierung und Untersuchung der Ursprünge des Ungewissen ("sources of uncertainity") voraussetzen, also die Fokussierung auf die Quelle(n) und Kategorien von Risiken (Ward 2003: 13). Nach Luhmanns Systemtheorie wird hier die Frage nach der Unsicherheitsabsorption mit Blick auf die Kontinuität von Kommunikation gestellt (Luhmann 2000: 184). Unternehmen sind in Anbetracht eines drohenden Abbruchs der Kommunikation mit einem potentiellen Ende ihrer Selbstbeschreibung und damit Eigenexistenz konfrontiert, dass sie zu vermeiden versuchen, allerdings dabei ihre jeweiligen Entscheidung zum Umgang mit Unsicherheit finden müssen. Dies scheint mit Blick auf unsere Fragestellung nach der Kontinuität von Unternehmensprozessen und Sicherheitserzeugung in Unternehmen als direkt anschlussfähig an die organisationssoziologische Literatur. Daher lohnt es sich im Folgenden, die Implikationen aus der unter den Umständen der Unsicherheit operierenden Unternehmen genauer zu betrachten.

Bezogen auf den konkreten Fall der Unsicherheitsabsorption mit Blick auf das Nicht-Wissen über zukünftige Ereignisse erfasste Francois Ewald das zugrundeliegende Selbstverständnis treffend indem er feststellte, dass „[e]in Risiko zu kalkulieren heißt die Zeit zu beherrschen und die Zukunft zu disziplinieren" (Ewald 1991: 291). Trotz dieser hochgesteckten Ziele sind viele empirische Negativbeispiele bekannt. Vom Bhopal-Chemieunfall 1984, über die Finanzkrise 2007/2008 bis zum Reaktorunglück von Fukushima 2011 zeigen sich zahlreiche Momente des Versagens der beteiligten Organisationen und ihrer Institutionen zur Absorption von Unsicherheit (Horst 2012: 45). Unsicherheit bedeutet vor allem einen Mangel an Wissen über den zukünftigen Ausgang zu verwalten. Die traditionelle Herangehensweise des Risikomanagement in Unternehmen sieht daher vor, die Erfolgsaussichten einer

[173] Einzelne Entscheidungen und Ereignisse können in integrierten Systemen Kettenreaktionen zur Folge haben, welche die globale Gesellschaft vor ungeahnte Herausforderungen zu stellen vermag, beispielsweise IT-Fehler in vernetzten Handelssystemen (Rasmusen 1997: 186). Diese Interdependenzen nehmen mit der fortschreitenden Vernetzung zu und erhöhen den potentiellen Schaden, sofern keine Vorsorge getragen wird.

[174] Die Akzeptanz des Risikos wäre auch eine mögliche Option, auch wenn in diesem Fall eher darauf gehofft wird, dass der Schadensfall nicht eintritt.

Risikosteuerung[175] anhand einer Wahrscheinlichkeitsrechnung unter Verwendung existierender Daten oder Schätzungen zu artikulieren (Klinke und Renn 2002: 1072).

Doch es bleibt Vorsicht geboten, denn komplexe Sachverhalte – worunter Prozesse wie beispielsweise die Digitalisierung und die Übersetzung der Sicherheitsdispositive durch die Pandemie in Unternehmen zu zählen sind - zeigen gleichzeitig, dass deren Unkenntnis oder mangelnde Durchdringung zu einem unerwarteten Ausgang einer Entscheidung führen kann. Denn „Unsicherheit entsteht bei gleichzeitigem Anfall von Wissen und Nichtwissen, entsteht also auf Grund dieser Differenz. Dabei sind Wissen ebenso wie Nichtwissen jeweils soziale Konstruktionen, die in dem System erstellt werden, das sie benutzt“ (Luhmann 2000: 184). Das Verständnis von Nichtwissen, den unbekannten Problemfeldern und Determinanten im Zusammenhang mit einem Sachverhalt, setzt folglich Wissen voraus. Denn um sich ein Bild über mögliche Probleme zu verschaffen ist die Analyse des aktuellen Wissensbestandes erforderlich.[176] Das bedeutet zuvor eventuell unbeachtete Sachverhalte miteinzubeziehen und scheinbar gesicherte Informationen erneut zu überprüfen. Daher wurden Strategien und Maßnahmen entworfen, um die potentiellen Folgen der Unsicherheit zu mitigieren.[177] Klinke und Renn sprechen in diesem Zusammenhang von einem normativen Mandat, einer inneren Verantwortung der Menschen, andere vor Gefahren zu warnen und auch zu schützen (Klinke und Renn 2002: 1074).

Doch wie wird dies im traditionellen Risikomanagement gesteuert beziehungsweise realisiert? Aus der Unvorhersehbarkeit von umgebungsbezogenen oder organisationsinternen Prozessen, welche die Unternehmensperformanz beeinflussen können, leitet sich der Wert der Risikoexposition[178] von Unternehmen gegenüber internen und externen Risiken ab (Miller

[175] Der Diskurs über die Aussagefähigkeit von Risikobewertungen und die Fähigkeit der Risikosteuerung im Allgemeinen ist eine der wichtigsten Debatten innerhalb der Risikoliteratur (vgl. Clapton 2009).

[176] Mithilfe von empirischen Daten kann der Schritt hin zur Erfassung und Klassifizierung von Risiken gelingen Eine Überleitung zum *Modernen* in unserem Verständnis von Unsicherheit findet sich in Form der Aussage: „It is a technology of prediction which has a reciprocal relation to a world understood as uncertain. To conceptualise the world in such a way is specific to a secular and capitalist modernity” (Owen 2009: 19).

[177] Die Analyse von Sprache und Emotionen durch Anwendungen erlaubt eine weitreichende Suche nach Anzeichen einer möglichen, zukünftigen Bedrohung (Amoore 2016: 18), etwa wenn eine Radikalisierung von Individuen zu beobachten ist. Big Data wird bereits zur Strafverfolgung aber auch Kriminalitätsprävention in Testfeldern verwendet Die Polizei von Los Angeles versuchte in mehreren Testfeldern die Vernetzung ihrer Polizeiabteilungen zu erhöhen und die im Feld gesammelten Informationen zusammenzutragen. Polizeibeamte waren demnach angehalten Informationen über befragte Personen unmittelbar nach dem Gespräch in einem digitalen Netzwerk aufzuzeichnen, etwa Aussagen, Aussehen und Verhalten des Befragten sowie dessen Fahrzeug oder die Umgebung des Gesprächs zu dokumentieren (Mohler et. al. 2015: 24). Auf dieser Grundlage wurden Vorhersagen über mögliche kriminelle Aktivitäten durch Computermodelle entwickelt, welche an die Beamten ausgeteilt wurden. Das Ergebnis der Feldstudie wurde mit einer Verringerung der Kriminalitätsrate von 7 Prozent beziffert (Bennet-Moses und Chan 2016: 12).

[178] Risikoexposition bezeichnet die spezifische Wahrscheinlichkeit und den Schaden für ein Unternehmen in einem definierten Kontext, beispielsweise das jeweilige Risiko eines ausländischen Unternehmens in einem Markt durch

1992: 312). Doch die Komplexitätssteigerungen durch die digitalisierten Produktionsprozesse und Absatzstrukturen fördern die Unsicherheit für Unternehmen aufgrund technischer und organisatorischen Wissensanforderungen. Darunter sind die Einsatzzwecke, Modifikationen und Abhängigkeiten von Systemen zu verstehen, welche eine spezifische Form von Expertise erforderlich machen, die nur in seltenen Fällen ein organisationsumspannendes Feld abdecken. „Moderne Produktionsplanungen komplexer Art haben sich zum Beispiel nach so vielen verschiedenen Umwelten (…) zu richten, dass eine Zentralisierung des notwendigen Wissens und damit auch eine Zentralisierung der Unsicherheitsabsorption ausgeschlossen sind“ (Luhmann 2000: 211). Diese Überlegung wird uns später in Form des Risikokontrollsystems einer resilienten Organisation erneut begegnen.

An dieser Stelle sei festgehalten, dass gerade in der soziologischen Forschung die Bedeutung der Unsicherheit über die Folgen einer Entscheidung sich unter den Bedingungen des ungewissen Ausgangs im Informationszeitalter problematisch gestalten kann. Dies beruht unter anderem auf der Entwicklung, dass die Komplexität und Vernetzung von Systemen zu vielschichtigen Interdependenzen führten, durch welche Einzelentscheidungen große Schadenspotentiale bewirken können (Gaycken und Karger 2011: 5). Daher bedarf das Risiko, welches einen komplexen technologischen Wandel wie die Digitalisierung begleitet, einer genaueren Betrachtung und einer konkreten Definition der risikorelevanten Termini innerhalb dieses Themenkomplexes. Dies soll im folgenden Abschnitt mit den Begriffen von Risiko Gefahr und Sicherheit im Detail erklärt werden.

4.2.2. Risiko, Gefahr und Sicherheit

Im alltäglichen Gebrauch treten viele Begriffe, wie etwa Bedrohung, Gefahr, Schaden, Unsicherheit oder negative Konsequenzen, als Synonyme für das Wort Risiko in Erscheinung wenn auch nicht immer auf zutreffende Weise. Um die unterschiedlichen Bedeutungen besser abgrenzen zu können, ist eine Einordnung notwendig. Dabei treten im Licht unserer Fragestellung zwei Begriffskontexte in Erscheinung. Auf der einen Seite ist in der klassischen ökonomischen Literatur ein Risikobegriff anzutreffen, der die Variablen Schaden und Wahrscheinlichkeit in den Vordergrund stellt und objektbezogen operiert (vgl. Kaplan und Garrick 1981; Klinke und Renn 2002). Dieses Verständnis von Risiko wurde während der beobachtenden Teilnahme in Unternehmen angetroffen und wird im Folgenden unter dem Überbegriff (1) traditionelles Risikoverständnis im Detail thematisiert werden. Demgegenüber

regulatorische Willkür Schaden zu nehmen oder durch soziale Unruhen Geschäftsunterbrechungen erwarten zu können (Hood und Nawaz 2004: 9).

wurde im Verlauf der zunehmenden Vernetzung von Prozessen durch die Digitalisierung eine Verschiebung des Risikobegriffs beobachtet, welcher sich an der Prozesskontinuität, vorrangig festzumachen an der Fähigkeit zur (2) Fortsetzung von kritischen (Kommunikations-)Aktivitäten eines Unternehmens, orientiert.[179] Bevor wir jedoch diesen erweiterten, prozessorientierten Risikobegriff einführen, widmen wir uns zuerst dem traditionellen Risikobild in Unternehmen.

Zum (1) traditionellen Verständnis von Risiko lässt sich bei Kaplan und Garrick ein lesenswerter Ansatz zu einer quantitativen Definition finden. Risiko wird dort als Gleichung aus der Summe von Ungewissheit und Schaden dargestellt (Kaplan und Garrick 1981: 12). Daraus lässt sich ableiten, dass zwei Kernkomponenten des Risikos bestimmen. Erstens ist ein negatives Ereignis (beispielsweise ein Verlust) und zweitens die Ungewissheit, hier verstanden als fehlendes Wissen (Ungewissheit) über zukünftige Entwicklungen zu berücksichtigen. In anderen Beispielen findet sich die Bezeichnung Unsicherheit für das unvorhersehbare Element in der Gleichung. In beiden Fällen verringert diese die Vorhersagbarkeit jener Variablen, welche den Schaden verursachen (Miller 1992: 312). Der Schaden setzt sich aus den beiden Elementen zusammen[180], welche als Kausalität die zumeist negativen Konsequenzen bedingen (Klinke und Renn 2002: 1071). Die Faktoren, die dies verursachen, sind sorgfältig zu unterscheiden. Ein Erdbeben kann beispielsweise der Auslöser für Schäden an der Bausubstanz eines Bürogebäudes sein, in dessen Folge das Gebäude vorrübergehend nicht zugänglich ist. Die Kausalkette erstreckt sich von einem auslösenden Ereignis – dem Erdbeben – auf eine negative Konsequenz – dem Ausfall des Gebäudes. Der Schaden, als Bestandteil des Risikos, beinhaltet so gesehen sowohl die Ursache als auch die Konsequenz des negativen Effekts.[181]

[179] Diese Beobachtung stützt sich auf den sprachlichen und inhaltlichen Wandel des Risikodiskurses, aber auch durch die Ausweitung der relevanten Prozesse und Systeme für die Vorsorgeplanung, welche eine systemische Perspektive auf das Unternehmen und seine Selbstreferenz widerspiegelt. Dies betrifft sowohl die begriffliche Wandelung von „Prozesskontinuität“ hin zu Artikulationen der resilienten Organisation, als auch die inhaltliche Ausweitung von Prozessen von durchschnittlich fünfzehn Prozent aller Prozesse im Jahr 2015 auf etwa 60 Prozent im Jahr 2021 (Workshop 19.01.2021). Die detaillierten Erkenntnisse aus der ethnographischen Forschung werden im siebten und achten Kapitel reflektiert werden.

[180] In der Literatur wird zudem diskutiert, ob die Summe oder das Produkt der beiden Komponenten besser geeignet sei, das Risiko auszudrücken. Um die Schwere gewisser Konsequenzen in Abhängigkeit zu ihrer Wahrscheinlichkeit exakter zu bemessen wird die Risikodefinition auch in einigen Fällen als Multiplikation der zwei Komponenten dargestellt (Kasperson et.al. 1988: 177). Dieser Ansicht wiedersprechen die Vertreter der *Summen-Definition*, indem sie die menschliche Antizipation und Wahrnehmung der Ungewissheit anführen. Die Beziehung zwischen Wahrscheinlichkeit und dem potentiellen Schaden führen nicht zwingend zu dem Schluss des aus der Multiplikation der Komponenten resultierenden Extremergebnisses: “In the case of a single scenario the probability times consequence viewpoint would equate a low-probability high-damage scenario with a high-probability low-damage scenario- clearly not the same thing at all” (Kaplan und Garrick 1982: 13).

[181] Für BCM ist dieser Aspekt von besonderer Bedeutung, denn nicht die originäre Ursache des Schadens ist vorrangig (wenn auch nicht zu vernachlässigen), sondern die Wahrscheinlichkeit eines Ausfalls der benötigten

Hier ist auf Frank Knight zu referenzieren (vgl. Knight 1921: 23), dessen Unterscheidung zwischen beiden Begriffen auf ihrer Quantifizierbarkeit basiert und seine Aktualität zuletzt in einer Spezialausgabe des Cambridge Journal of Economics diskutiert wurde (Faulkner et. al. 2021). Aus dieser Perspektive liegt der entscheidende Unterschied in der Annahme, dass ein Risiko objektiv messbar sei, wohingegen die Unsicherheit der Subjektivität unterworfen sei.[182] Diese bestimme gewissermaßen als Unbekannte die eigentliche Qualität des Begriffs (Jakobsen 2012: 35). Das Dilemma in diesem Kontext ist die menschliche Eigenschaft der Antizipation, welche die Annahme über zukünftige Entwicklungen durch Schlussfolgerungen und Wahrnehmung weiter einengt und subjektiven, zu Teilen jedoch als *objektiv wahrgenommenen* Ansichten unterzuordnen droht (Jarvis 2011: 298). Wir werden uns diesem Problem unter dem Gesichtspunkt der Risikobewertung weiter unten erneut zuwenden.

Gegenüber der Ansicht, das Risiko als eindeutig kalkulierbares Objekt zu beschreiben, wie wir es primär in der ökonomischen Forschung kennen, heben soziologische Ansätze die Kontextabhängigkeit des Risikos hervor, welches die Reflexivität des Risikobegriffs betont und hier als (2) alternative Sichtweise auf den Risikobegriff eingeführt werden soll.[183] Daurch zweigt sich ein Paradox durch die im Kern unvorhersehbare Natur der Sache, denn "our general understanding of risks builds on the premise that they can be classified, quantified and to some extent predicted" (Aradau, Lobo-Guerrero und Van Munster 2008: 148). Aus dieser Perspektive sind Risiken immer auch Ausdruck einer aktiven Gestaltung und Fähigkeit zur Einflussnahme auf die Umwelt, weniger einer Schicksalsergebenheit gegenüber Ereignissen. In der Literatur werden dafür die Begriffe Gefahr oder Gefährdung („hazard") verwendet, gelegentlich auch als Synonym für das Risiko selbst. Eine Differenzierung zwischen beiden Begriffen ist dahingehend sinnvoll, als dass Gefahr die Grundlage oder der Ursprung für ein Risiko ist und

Ressource, beispielsweise der Büroflächen. Daher ist die Unterscheidung zwischen Ereignis und Schaden sinnvoll, um die Analyse des Ausfallsrisikos einer Ressource nicht durch zu viele Szenarien unübersichtlich zu gestalten.

[182] Für Luhmann hingegen besteht die Notwendigkeit zur Differenzierung des Begriffspaares Risiko und Sicherheit, welche „asymmetrisch" aufgebaut sind. „In beiden Fällen bezeichnet der Risikobegriff einen komplexen Sachverhalt, mit dem man es, zumindest in der modernen Gesellschaft, normalerweise zu tun hat". (…) „Die Gegenseite fungiert nur als Reflexionsbegriff mit der Funktion, die Kontingenz der Sachverhalte zu verdeutlichen, die unter den Begriff des Risikos fallen. Das ist im Falle Risiko/Sicherheit an den Messungsproblemen zu erkennen (Luhmann 1991: 32). Verwendung findet daher der „Begriff des Risikos, um (…) Sicherheitsstreben und das Ausmaß des vernünftigerweise Erreichbaren rechnerisch zu präzisieren. Dem entspricht der Übergang von deterministischen zu probabilistischen Risikoanalysen" (ebd.: 28) und somit dem verbleibenden Rest von Unsicherheit aufgrund der letztendlich ungewissen Entwicklung in der Zukunft.

[183] "Realisten" betrachten das Risiko als objektiven Sachverhalt und sehen den sozialen Hintergrund der Risikoherausbildung als irrelevant an, da das Risiko in sich sein Dasein definiert und ohne menschliche Antizipation oder Wahrnehmung existent sein kann. Die Diskussion zwischen Realisten und Vertretern des Gegenarguments, den „Konstruktivisten", wird an späterer Stelle detaillierter Rechnung getragen. Für einen guten Überblick über die Risikoobjektivität und die jeweiligen Perspektive siehe William Claptons aufschlussreichen Überblick über Risikoperspektiven in der IR (Clapton 2011: 281).

weniger als ein gleichbedeutender Ausdruck verstanden werden sollte (Kaplan und Garrick 1981: 12f.). Gefahr ist eine notwendige Voraussetzung für das Risiko (McLean, Patterson und Williams 2009: 4). Darryl Jarvis unterscheidet daher: "[h]azards — which are naturally occurring events that can produce harm — and risks, which evolve from deliberative calculations made in the use of science and technology to produce wealth" und schließt mit der prägnanten Feststellung, dass „[r]isks are made, hazards occur" (Jarvis 2007: 30f.).

Mit Blick auf die Finanzwirtschaft führte Dirk Baecker in diesem Zusammenhang an: „Banken machen ihr Geschäft nicht mit Risiken, die sie vermeiden, sondern mit Risiken, die sie übernehmen" (Baecker 1991: 118). Dieser Gedanke ist dahingehend interessant für unsere Unterscheidung, als dass die klassische ökonomische Risikoliteratur nicht ausreichend zwischen Entscheidungen und Ungewissheit differenziert und das Begriffspaar Risiko und Gefahr im Kontext der Organisationsautopoiesis nur unzureichend reflektiert (Luhmann 1991: 25). Das Risiko wird im Rahmen der unternehmerischen Risikosteuerung wahrscheinlichkeitstheoretisch bewertet, allerdings nicht unter Einbeziehung der Entscheidung des Handelns oder Nichthandelns oder die Unterscheidung von exogenen Gefahren und internen Entscheidungen betrachtet (Baecker 1991: 121). Der Aspekt der Entscheidung wird uns im Folgenden begleiten, um den Rahmen des neuen, prozessorientierten und auf die Anschlusskommunikation des selbstreferenziellen Organisationsmodells abzielenden Risikobegriff abzustecken. Dadurch soll es ermöglicht werden das zugrundeliegende Risikoverständnis für die Veränderungen der unternehmensinternen Sicherheitsproduktion durch die Digitalisierung[184] zu verstehen.

Die Differenzierung zwischen Risiko und Gefahr bietet den Vorteil den Begriff selbst mit einem höheren Abstraktionsgrad zu betrachten und weniger in einer zwingend negativen Konnotation des zu befürchteten Übels zu verstehen.[185] Ein Risiko ist abhängig vom Beobachter und dessen Erfahrungs- und Wahrnehmungshorizont, wie wir weiter unten im Rahmen der Risikobewertung sehen werden. Für den Moment bleibt festzustellen, dass in unserem Kontext die Artikulation des Risikos auch eine Relativität ausdrückt, da es in einer Beziehung zur

[184] Die traditionelle Interpretation des Risikobegriffs reflektiert durchaus technologischen Wandel auf gesellschaftlicher Ebene. So lautet eine Feststellung, „[…] that risk might in fact be increasing due to technology, science and industrialism rather than being abated by scientific and technological progress" (Jarvis 2007: 23) und damit eine fundamentale Rolle für die Perzeption von (Un-)Sicherheit spielen kann. Allerdings ist die Frage, ob eine Technologie eingesetzt werden soll, in demokratischen Gesellschaften von einem sozialen Prozess der Aushandlung (Plough und Krimsky 1987: 7) und gesellschaftlicher Konsensfindung abhängig (Bradbury 1989: 391).

[185] Denn ein Risiko ist im Kern immer eine Verbindung aus Unsicherheit und Schaden, aber damit noch keine Katastrophe, sondern die Antizipation einer solchen (Beck 2006: 332).

subjektiven Wahrnehmung steht (Kaplan und Garrick 1981: 12). Dies ist insofern relevant, als dass es wesentlichen Einfluss auf die Bewertung eines Risikos hat. Wenn ein Risiko im Kontext der sozialen, kulturellen oder moralischen Vorprägung des Beobachters gesehen wird, verändert sich auch die Konnotation der Einschätzung und somit auch der Entscheidung über den Umgang mit dem Risiko.[186] Ein von Niklas Luhmann vorgebrachter Ansatz unterscheidet daher zwischen der Auswirkung von Entscheidungen auf die zukünftige Entwicklung oder deren Ausgang ohne jedweden Einfluss durch Handlungen der Entscheidungsträger.[187] Die Beziehung zwischen Entscheidung und negativen Konsequenzen bezeichnet Luhmann daher als „Risiko der Entscheidung" (Luhmann 1991: 30f.). Wenn die Ursächlichkeit des Schadens in der Unausweichlichkeit, also ohne menschliche Interaktionsmöglichkeit verankert liegt[188], dann spricht man von Gefahr (ebd.: 111).

So gesehen bedeutet eine Entscheidung unter den Vorzeichen der Unsicherheit, dass jede einmal getroffene Entscheidung auf ihre nicht vollständig abzuwägende Wirkung hin überprüft wird. Da sich dies erst mit fortschreitender Zeit bestimmen lässt, muss die Entscheidung als Teil des kollektiven Gedächtnis präsent bleiben und im Falle neuer Erkenntnisse, also der Reduktion von Unsicherheit, erneut evaluiert werden.[189] Dies aufs Neue zu dokumentieren und als Teil des Wissensbestandes abzuspeichern ist eine ebenso anspruchsvolle Leistung wie die darauf aufbauenden Entscheidungen unter den Bedingungen der Unsicherheit zu treffen.[190]

---

[186] Demgegenüber stehen Beiträge in der Literatur, deren ‚realistische' Definition eines Risikos als objektives, existierendes Phänomen (Clapton 2011: 281), welche wir im Folgenden zu Gunsten der konstruktivistischen Perspektive vernachlässigen.

[187] Das Beispiel der im März 2015 durch den Piloten zum Absturz gebrachten Germanwings-Maschine zeigt diese Beziehung zwischen Entscheidung und Risiko. In Folge der erhöhten Sicherheitsstandards nach den Flugzeugentführungen des 11. Septembers 2001 wurden die Cockpittüren dergestalt modifiziert, dass diese zum Schutz vor Entführungen nur von innen zu öffnen waren. Diese Nachrüstung verhinderte, dass die Crew in das Cockpit gelangen konnte, um die Kontrolle über das Flugzeug zu übernehmen, nachdem der absichtlich herbeigeführte Sinkflug festgestellt wurde (Anthony 2016: 42).

[188] Organisationen müssen folglich nicht nur Risiken wie die Investition in eine Technologie oder Versicherung einer Tätigkeit, sondern auch die Entscheidung selbst als Risiko zu betrachten. Dadurch ergeben sich bestimmte, systemintrinsische Limitationen für Banken und Versicherungen hinsichtlich ihres Risikoappetits, denn „Banken machen ihr Geschäft nicht mit Risiken, die sie vermeiden, sondern mit Risiken, die sie übernehmen" (Baecker 1991: 118). Die Entscheidung der Unternehmung selbst muss folglich dem Kerngeschäft im Umgang mit Risiken hinzugerechnet werden und bedeutet eine umso bedeutendere Abhängigkeit hinsichtlich der Kommunikation der Entscheidung sowie deren Erinnerung im Organisationskontext.

[189] Aus Sicht von Internetkonzernen wie Google ist die technologische Innovation ein möglicher Lösungsansatz, um Sicherheit herzustellen. Für Google bedeutet das, „that a full-scale automobile automation system would save 'one million human lives per year' by preventing accidents. (…) [T]he interest in the engineering of global platforms would either begin or end up with transportation, but whether one sees the Internet as a "superhighway" or the hundreds of millions of cars in motion at any one time as very large 'data packets' makes all the difference in how the issue is problematized and formulated" (Bratton 2015: 281). Aus dieser Perspektive ist die Umsetzung der Verkehrssicherheit der logische Transfer einer Technologie auf ein weiteres Anwendungsfeld.

[190] Dem steht der Sicherheitsbegriff gegenüber. Die vollkommene, uneingeschränkte Umsetzung von Sicherheit ist indes nicht möglich. Wenngleich Vorschriften und technische Innovationen beispielsweise im Personenverkehr eine beachtliche Verbesserung der Unfallstatistik erreicht haben, kann doch immer etwas Unvorhergesehenes geschehen. So reduzierte sich deren Zahl in Deutschland zwischen 2005 und 2010 um etwa 25% (Vorndran 2010:

Zum besseren Umgang mit dieser Herausforderungen vertrauen Unternehmen auf die etablierten, traditionellen Kontrollsysteme ihres operationellen Risikomanagements, doch sollte stets im Blick behalten werden, dass deren Arbeit keine „Transformation von Risiko in Sicherheit“ bewirken kann, sondern lediglich „dem bestmöglichen Umgang mit Unsicherheit“ auf der Grundlage der Übersetzung von Risiken in solche eines „anderen Zuschnitts“ gestattet (Luhmann 1991: 197).

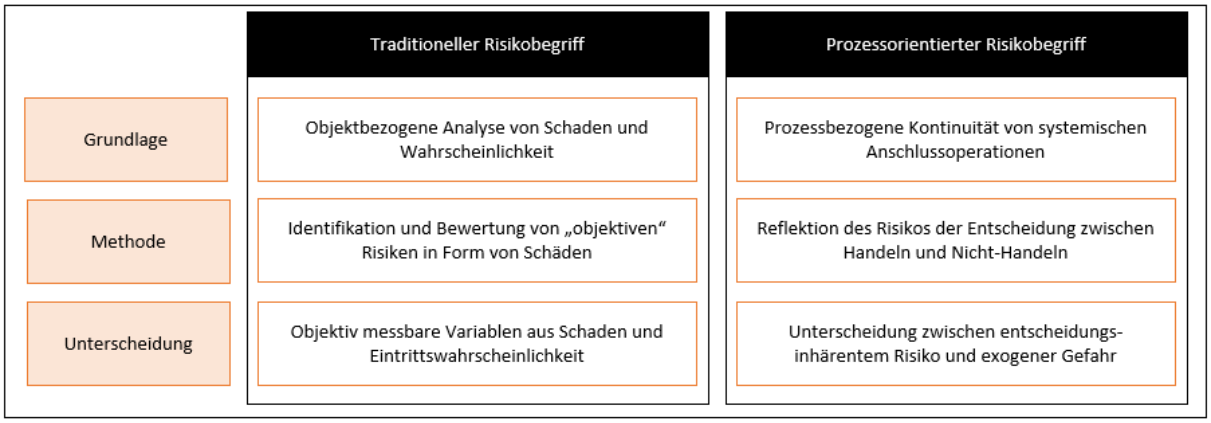

Abb. 4.2. Unterscheidung traditioneller und prozessorientierter Risikobegriff. Eigene Darstellung.

Zusammenfassend lassen sich zwei Risikobegriffe gegenüberstellen. Der traditionelle Risikobegriff deckt sich mit dem ökonomischen Verständnis von Risiko als objektbezogene, kalkulierbare und steuerbare Artikulation im Umgang mit Unsicherheit. Die Einführung neuer Technologien im Informationszeitalter und insbesondere seit dem Digitalisierungsschub durch die Corona-bedingten Maßnahmen führte zu einer Revision des Risikobegriffs im Unternehmenskontext. Dieser neue Begriff umfasst aus organisationstheoretischer Sicht eine prozessorientierte Sichtweise ein, in der die Entscheidung für oder gegen eine Handlung Gegenstand des Risikos ist und den Fokus auf die Aufrechterhaltung der systemischen Kommunikation und Prozesskontinuität legt. Für unsere Fragestellung bedeutet dies vor allem, dass der Umgang mit Unsicherheit durch die fortschreitende Vernetzung und Exposition von Systemen im Informationszeitalter durch neue Risikokontrollsysteme beschritten werden muss. Dazu werden wir die Beobachtungen aus der ethnographischen Teilnahme am Prozess der Sicherheitsproduktion durch Risikokontrollsysteme und ihrer Veränderungen anführen und besprechen. Im Folgenden soll der Blick zunächst auf die allgemeinen Grundlagen unternehmerischer Risikokontrolle gerichtet werden, um die Entwicklung der Novellierung im Rahmen der Digitalisierung später darlegen zu können.

1085). Doch diese relative Verbesserung erhöht nicht zwingend das „Sicherheitsgefühl“. Sicherheit findet sich zudem als Gegenstand des politischen Diskurses, etwa als Mittel der Kommunikation (Mythen und Walklate 2006: 129).

4.2.3. Risikokontrollsysteme

Innerhalb von Unternehmen tragen im traditionellen Verständnis Risikokontrollsysteme die Verantwortung zur Identifizierung, Bewertung und Überwachung von Risiken, um die schutzbedürftigen Werte („assets“) vor negativen Effekten zu bewahren (Power 2005: 578). Darunter zählen sowohl finanzielle Werte, wie Kapital, Ressourcen oder Eigentumsbeteiligungen, als auch immaterielle Werte, wie informelle Informationen, Praktiken oder Netzwerke, welche eine herausgehobene Bedeutung für das Unternehmen haben (Best 2010: 37). Für unsere Fragestellung liegt der Schwerpunkt auf solchen Werten, welche für die Fortführung der Geschäftsfähigkeit des Unternehmens relevant sind. Dies umfasst die klassischen vier Ressourcen[191], welche im Rahmen des Business Continuity Management betrachtet werden, um die Fortführung kritischer Geschäftsprozesse zu gewährleisten (Bonafede, Cerchiello und Giudici 2007: 80). Weitere Kontrollsysteme behandeln beispielsweise Risiken, welche einen Schaden aus der Verletzung der Vertraulichkeit und Integrität von Informationen zum Gegenstand haben. Diese Kontrollen beziehen sich häufig auf spezifische Regularien und Datenschutzgesetze und können empfindliche Strafen zur Folge haben (Gaycken und Karger 2011: 7). Ein Risikokontrollsystem soll in diesen Fällen beispielsweise vor einem Verlust von sensitiven Daten schützen und negativen finanziellen Effekten sowie einem Reputationsschaden vorbeugen.

Aus struktureller Sicht sind zwei Umsetzungsformen der Risikomanagementfunktionen[192] zu unterschieden: Der dezentrale Ansatz sieht die einzelnen Geschäftsfunktionen in der Verantwortung, welche eigene Kontrollen entwickeln und an die Unternehmensleitung berichten (Miller 1991: 320). Dieser Ansatz stößt mit zunehmender Größe eines Unternehmens an seine Grenzen, impliziert Redundanzen zwischen einzelnen Funktionen und Mehrarbeit Zudem erschwert der dezentrale Ansatz eine standardisierte Auswertung der Ergebnisse und

[191] Wie wir im vierten Kapitel zeigen werden, umfassen die vier BCM Ressourcen die Verfügbarkeit von Gebäuden, Mitarbeitern, der IT-Infrastruktur und externen Dienstleistern. Die jeweiligen Ressourcenanforderungen aus kritischen Geschäftsprozessen, das heißt solche Prozesse, deren Unterbrechung irreparablen Schaden für das Unternehmen bedeuten würde ist daher Bestandteil eines Risikokontrollsystems (Naill 2010: 276). Im Informationszeitalter schließt sich Informationen als fünfte Ressource an, wie wir im fünften Kapitel vertiefen werden.

[192] Risikomanagement als Überbegriff für Kontrollsysteme ist häufig das Resultat einer regulatorischen Anforderung, besonders im Bereich der Finanz- und Versicherungswirtschaft. In der Europäischen Union gelten beispielsweise nationale und supranationale Vorgaben zur Gestaltung des organisationsinternen Risikomanagements, wie etwa Solvency II, das wesentlichen Einfluss auf die Bedeutung der zuständigen Funktion durch Vorgaben und Dokumentationspflichten in den Unternehmen hat (Pfeiffer 2006: 13). Die Regulierung der Finanzmärkte nach den Erfahrungen der Finanzkrise 2007/2008 zielte auf eine Vereinheitlichung der Standards und Verhinderung von Unternehmensinsolvenzen aufgrund mangelhaften Risikomanagements (Luburić 2017: 31). Die zentralen Branchenakteure sollen durch diese Systeme ihre Risiken besser kalkulieren und trotz steigender Komplexität adäquate Kompensationsstrategien implementieren können (Best 2010: 36).

droht die Zusammenhänge zwischen einzelnen Risikokontrollen wie beispielsweise zwischen der Verfügbarkeit von Ressourcen und Vertraulichkeit von Informationen zu vernachlässigen (Ward 2003: 7). Der zentrale Ansatz hingegen basiert auf einem mehrstufigen, standardisierten Modell zur Einhaltung zentral definierter Kernkontrollen und dezentral erstellter Ausdifferenzierungen der spezifischen, funktionalen Risikokontrollen (Hood und Nawez 2004: 8). Ein solches zentral-organisiertes Risikokontrollsystem besteht aus drei Ebenen, welche alle gemeinsam zur Steuerung von Risiken und der Vorbereitung beziehungsweise Überwachung von Maßnahmen zur Mitigation von Risiken beitragen sollen.

Die Funktionsweise dieses unternehmensweiten Risikokontrollsystems basiert auf der Ausarbeitung von Kernkontrollen, welche durch die Risikomanagementfunktion in Zusammenarbeit mit den Fachfunktionen definiert werden. Auf der Grundlage dieser abstrakten Kernkontrollen entwickeln die jeweiligen Funktionen, wie beispielsweise der Informationsschutz detaillierte Kontrollen und Umsetzungsrichtlinien, deren Einhaltung gemeinsam mit den entsprechenden Kernvariablen für alle Funktionen des Unternehmens gelten sollten. Diese Kontrollen stellen zudem den Prüfungsrahmen dar, anhand dessen die Einhaltung des Regelwerkes gemessen wird. Für die Überprüfung untersuchen die Fachfunktionen die detaillierten Kontrollen und melden Verstöße an die Risikomanagementfunktion, welche ihrerseits regelmäßig die Einhaltung der Kernkontrollen im Unternehmen abprüft (Dierkes et. al. 2005: 39). Als zusätzliche Kontrollfunktion überprüft die interne Revision die Durchführung der zuvor aufgeführten Schritte und prüft in ausgewählten Schwerpunktbereichen die Einhaltung und Berichterstattung von Kontrollen nach (IIA 2013).

Betrachten wir ein konkretes Beispiel der Implementierung eines solchen zentralen Risikokontrollsystems: Die Risikomanagementfunktion einer Bank[193] definiert auf der Grundlage internationaler Standards Kernkontrollen im Bereich Business Continuity Management, welche besagt, dass Wiederherstellungspläne zu testen sind. Aus dieser allgemeinen Anforderung werden durch die BCM-Fachfunktion Umsetzungsrichtlinien etabliert, welche das Testen von Plänen konkretisieren, beispielsweise hinsichtlich der Frequenz, Kategorisierung und Dokumentationspflicht von Tests. Die BCM-Fachfunktion kontrolliert daraufhin die Einhaltung dieser Vorschriften in anderen Funktionen (z.B. in der

[193] Die Finanzbranche ist in Deutschland, aber auch im weltweiten Kontext streng reguliert was die Implementierung von Risiko- und Kapitalrücklagen betrifft. Diese Regelungen basieren auf der Solvency II Richtlinie und nationalen Pendants, wie etwa der Mindestanforderung an das Risikomanagement (MaRisk) für Kredit- und Finanzdienstleistungsinstitute (BaFIn 2009).

Personalabteilung, der Produktentwicklung und dem Investmentbereich) und dokumentiert eventuelle Abweichungen gegenüber den Anforderungen. Diese Befunde werden dem Risikomanagement gemeldet und im Fall eines signifikanten Defizits mit entsprechenden Anforderungen zur Bildung von Risikokapitalrückstellung versehen. Das dergestalt kalkulierte Risikokapital muss vom betroffenen Bereich (beispielsweise im Investmentbereich aufgrund fehlender Testdokumentationen) vorgehalten werden und kann Einfluss auf das Jahresergebnis des Bereiches haben.[194]

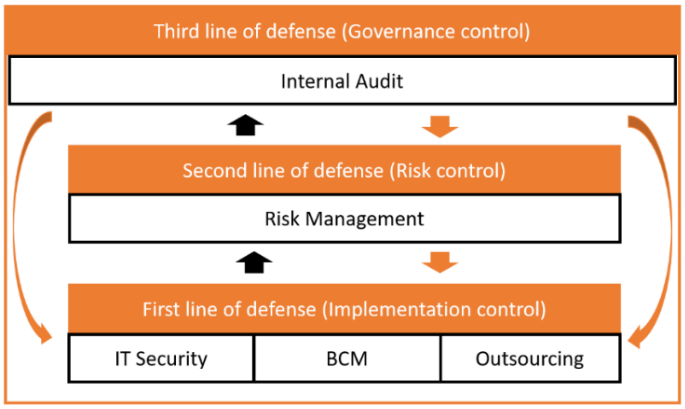

Abb. 4.3. Internes Kontrollsystem, bestehend aus drei Ebenen. Eigene Darstellung.

Ein solches Kontrollsystem reflektiert die Sichtweise von Unternehmen auf Risiken, welche als steuerbare Objekte verstanden werden.[195] Die Idee, durch ein effektives Risikomanagement die Möglichkeit zu haben zwischen „sicheren" und „riskanten" Optionen wählen zu können, liegt dem Systemansatz daher zu Grunde. Die darauffolgende Entscheidung zwischen Alternativen wird somit zum eigentlichen Gegenstand des Risikos (Luhmann 1991: 29). Auf Der Grundalge dieser Überlegung wurden Risikokontrollsysteme in den letzten zwei Dekaden mit dem Schwerpunkt auf eine funktionale Differenzierung von Verantwortung auf der horizontalen Linie (Fachfunktionen mit dezidierten Aufgabenfeldern) und einer vertikalen Integration in ein dreistufiges Risikokontrollsystem aus Kernkontrollen, Umsetzungsrichtlinien und Revisionen (Ward 2003: 9) konzipiert. Die Herausforderung im Informationszeitalter steht im Zusammenhang mit der Verknüpfung von Systemen, Anwendungen und Informationen wie im

[194] In einigen Fällen ist damit auch die Zielerfüllung der zuständigen Bereichsverantwortlichen gefährdet. Da sich deren Zielerfüllung auf die individuelle Bonusauszahlung auswirkt, darf hier ein starkes, persönliches Motiv vermutet werden, die Risikokapitalrückstellungen wenn nicht aus intrinsischen Gründen, dann aus Eigeninteresse durch geeignete Kontroll- oder Mitigationsmaßnahmen niedrig zu halten.

[195] Damit wird versucht die Lücke zwischen Sicherheit (verstanden als die durch das traditionelle Risikomanagement im obigen Sinne bereits identifizierten Risiken) und der Unsicherheit (verstanden als noch nicht identifizierte Risiken) mit monetären Anreizen und Kontrollmaßnahmen zu schließen (Power 2005: 580). Diese „securization" des Umfeldes in dem sich die Organisation bewegt (Best 2010: 34) vermittelt eine vermeintliche Absicherung gegenüber der unbekannten Zukunft und schafft Vertrauen in die eigenen Strukturen und Indikatoren. Dennoch bleibt der in dieser Logik inhärente Unterschied zwischen dem erreichten Sicherheitszugewinn und der tatsächlich realisierten Sicherheit evident.

Fall des Cloud Computing, in dem die Zuordnung von Elementen zu einzelnen Fachfunktionen zunehmend schwieriger wird (AGCS 2018: 3).[196] Daraus kann die Schlussfolgerung gezogen werden, dass die methodische Verantwortungsdelegation traditioneller Risikokontrollsysteme im Zuge der Digitalisierung und Veränderung der prozessualen und organisatorischen Strukturen an ihre Grenzen gerät (Braes und Brooks 2010: 17).

Dies betrifft insbesondere die Aufteilung von Risikokontrollen und deren Verantwortungszuweisung in Denkmuster von Fachfunktionen und isolierten Kontrolluniversen. Wenn IT-relevante Risiken beispielsweise ausschließlich aus Sicht der Fachfunktion für IT-Sicherheit bearbeitet werden, drohen Aspekte der auf operationeller Ebene priorisierten Anwendungen von Seiten der Geschäftsprozesse in den Hintergrund zu treten.[197] Gleichbedeutend sind bei einer getrennten Erstellung von IT-relevanten Risikokontrollen die umfänglichen Schutzdimensionen von Informationen, Anwendungen und Infrastruktur sowie gleichberechtigte Aspekte der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen nicht zu erwarten (Pauli, Schermann und Krcmar 2010: 259). Das Ziel sollte es stattdessen sein eine Vernetzung von Kontrollen über horizontale und vertikale Barrieren hinweg zu etablieren, allerdings nicht allein entlang funktionaler Aufgabenzuweisungen (Racz, Weippl und Seufert 2010: 245), sondern auf der Grundlage von Schutzwerten und deren Anforderungen an bestimmte Kontrollen. Diesen Aspekt eines integrierten Risikokontrollansatzes werden wir im sechsten Kapitel erneut aufgreifen und in ein idealtypisches Modell überführen.

4.2.3.1. Risikoidentifikation und –Kategorien

Innerhalb eines Risikokontrollsystems werden relevante Risiken durch die Risikomanagementfunktion eines Unternehmens identifiziert und kategorisiert, um die bestmögliche Absorption von Unsicherheit zu erleichtern (Scherrer 2018: 98). Dazu dienen standardisierte Risikokategorien, mit deren Hilfe Risiken gruppiert und Entscheidungen anhand von Grenzwerten getroffen werden können. In der Literatur findet sich eine Vielzahl an unterschiedlichen Risikokategorien (vgl. Kristensen, Aven und Ford 2005: 423; Miller 1992:

[196] Eine Information wird im Lauf ihrer Bearbeitung mit weiteren Informationen in Zusammenhang gesetzt und angereichert. Der Kauf eines Neuwagens ist im Unternehmensnetzwerk beispielsweise mit den Informationen des Kunden, seiner Anschrift, Kreditratenrahmen, Konfigurationsliste und weiteren Informationen verbunden. Diese Information zum Zweck des Datenschutzes zu klassifizieren fällt aufgrund der dynamischen Veränderung des Informationswertes ausgesprochen schwer und ebenso verhält es sich mit der Verantwortlichkeit einer Fachfunktion für die Bewertung des gesamten Informationsgehalts.

[197] Die Wiederherstellung von IT-Infrastruktur sollte sich nach den Anforderungen der kritischen Prozesse richten. „Problematisch ist hier die ganzheitliche Integration in die vorhandene Organisationsstruktur, da isoliertes Risikomanagement keine Verknüpfungen und Auswirkungen zwischen verschiedenen Risikobereichen im Unternehmen aufzeigen kann“ (Schermann und Krcmar 2010: 227). Zudem kommt erschwerend hinzu, dass eine unzureichende Verantwortungsdelegation zu Schutzlücken führen kann.

312ff.; Power et. al. 2009: 304; Renn und Klinke 2004: 41). Diese Kategorien beschreiben eine Einteilung in Fachdisziplinen, welche unterschiedlichen Berechnungsgrundlagen und Grundannahmen folgen. Eine solche Risikokategorie kann unter einem Überbegriff mehrere Variationen eines ähnlichen Schadensereignisses subsummieren, welche in einigen Punkten Gemeinsamkeiten aufweisen. Eine Risikokategorie kann beispielsweise die Gruppe der politischen Risiken sein, unter der sich mehrere Risikoszenarien wie die Instabilität des politischen Systems oder Enteignungen von Unternehmenseigentum wiederfinden können. Die nachfolgende Aufzählung an Risikokategorien und Szenarien trägt nicht die Intention abschließend zu sein und fokussiert sich ferner auf solche Gruppen und Szenarien, die eine Unterbrechung des Geschäftsbetriebs zur Folge haben können und daraufhin untersucht werden sollen. Die folgende Kategorisierung gliedert sich in fünf Gruppen, namentlich (1) ökonomisches Risiko, (2) gesundheitliches Risiko, (3) technologisches Risiko, (4) natürliches Risiko und (5) politisches Risiko.

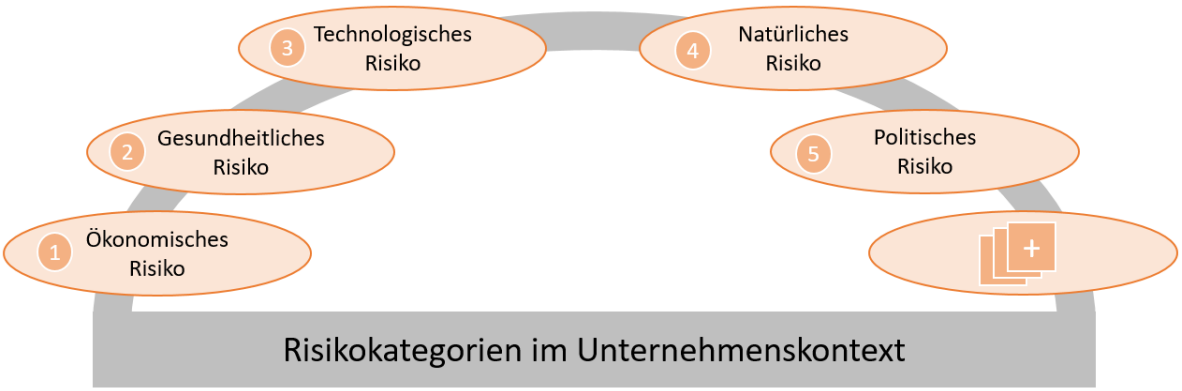

Abb. 4.4. Risikokategorien. Eigene Darstellung.

Beginnen wir mit dem (1) ökonomischen Risiko. Diese Kategorie bezeichnet das klassische Verständnis von Risiko als potentielle Abweichung von der prognostizierten Entwicklung der für die Unternehmenszahlen relevanten Gewinne und Verluste. Eine knappe Definition von Kent Miller umschreibt dieses Risikoverständnis als „uncertain environmental variables that reduce performance predictability“ (Miller 1992: 312). Dolche Risiken können beispielsweise die Bilanz durch überteuerte Unternehmenszukäufe, Rechtsstreitigkeiten oder Fehlinvestitionen negativ beeinflussen und im extremen Fällen sogar eine Insolvenz einschließen (Eliott et. al. 2000: 51). Diese Risikokategorie unterliegt dem unternehmerischen Risiko im Allgemeinen und wird für die nachfolgende Betrachtung nicht im Mittelpunkt stehen.

Anders verhält es sich mit (2) gesundheitlichen Risiken. Gemeint sind gesundheitliche oder auch medizinische Risiken, welche Einfluss auf die Verfügbarkeit von Mitarbeitern haben

können. In der öffentlichen Wahrnehmung werden diese Risiken[198] aufmerksam verfolgt (Elbe 2005: 115), reichen sie doch direkt an die Erfahrungswelt des Einzelnen heran[199] und sind aus der Sicht des unternehmerischen Krisenmanagements relevant. Diese Kategorie umfasst vor allem Infektionskrankheiten, welche aufgrund ihrer Ansteckungsrate ein potentielles Ausfallrisiko beziehungsweise Reputationsrisiko bewirken können.[200] Eine Gefährdung für die Belegschaft eines Unternehmens durch gesundheitliche Risiken erschien zwar bereits in der Zeit vor der Corona-Pandemie als relevante Risikokategorie (Günther, Ruhrmann und Milde 2011: 19), allerdings mit deutlich niedrigerer Bedeutung als heute. Nur drei Prozent der im Jahr 2019 an einer Umfrage teilnehmenden Risikoexperten werteten Gesundheitsrisiken und Pandemien als relevante Risiken für ihre Unternehmen (AGCS 2020). Diese Bewertung wurde mit Beginn der Pandemie, zunehmenden Fallzahlen und der Auswirkungen durch die veranlassten Schutzmaßnahmen revidiert (Menzel 2021: 5). Die konkreten Folgen und der Umgang mit dieser Risikokategorie wird im fünften Kapitel besondere Berücksichtigung finden.

Im Fall des gesundheitlichen Risikos und prägnant auch als Folge der Corona-Pandemie erstreckt sich das Risikofeld auch auf die Ausweitung und Beschleunigung der Digitalisierung. Die in Reaktion auf die Ausbreitung des Virus getroffenen Maßnahmen beschleunigten, wie wir es zuvor gezeigt haben, die Nutzung der Informationstechnologie und erweiterten in dessen Folge auch der Exposition von Unternehmen gegenüber einer weiteren Risikokategorie. So sind die (3) technologischen Risiken sind für unsere Fragestellung von großer Bedeutung, da unter

[198] Am Beispiel der BSE-Krise war der Reputationsschaden der Gesundheits- und Verbraucherschutzinstitutionen zu verfolgen. Die Aufdeckung, Regelung und Kommunikation der durch Tierfutter ausgelösten Rinderkrankheit erweckte den Eindruck eines eklatanten Verbesserungspotentials des interorganisationalen Risikomanagements im Gesundheitswesen (Mythen 2004: 61). Der Rückgang des Kalbfleischverbrauchs in Westeuropa hielt an und Fleisch von britischen Rindern war über Jahre mit einem zweifelhaften Image behaftet. Dabei war die Wahrscheinlichkeit für die Bevölkerung an der durch BSE beim Menschen ausgelösten Creutzfeld-Jakob-Krankheit zu erkranken sehr gering wie sich im Nachhinein herausstellte. Die Probabilität von 1 zu 30 Milliarden erscheint recht gering im Vergleich durch das Risiko durch einen Blitzschlag das Leben zu verlieren. Dieses liegt im europäischen Durchschnitt bei 1 zu 3 Milliarden (Gerrard und Petts 1998: 1).

[199] Eine Studie bezifferte etwa die Zahl der in Deutschland durch Behandlungsfehler zu Tode gekommen Personen im Jahr 2013 auf 19.000 Fälle, während im gleichen Zeitraum 3.339 Menschen an den Folgen von Verkehrsunfällen starben (vgl. AOK Krankenhausreport 2014; Statistischen Bundesamtes 2014).

[200] Eine allgemeine Stellungnahme zur Risikoperzeption von Infektionskrankheiten am Beispiel HIV/AIDS: Die Krankheit entwickelte sich zu einem Stigma der Dritten Welt. Im Jahr 2005 wurde die Anzahl der weltweit an HIV / AIDS infizierten Personen der UN-Organisation UNAIDS auf bis zu 46 Millionen geschätzt, wovon maximal 1,8 Millionen in Westeuropa, Nordamerika und Australien lebten. Im Gegensatz dazu wurde die Anzahl der Infizierten im Subsaharaafrika auf 28 Millionen geschätzt, gravierender allerdings ist die Neuinfektionsrate in dieser Region, die mit 3 – 3,4 Millionen Personen pro Jahr die mit Abstand größte der Welt ist (Elbe 2005: 113). Lange galten Homosexuelle und Personen mit häufig wechselnden Sexualpartnern als Risikogruppen und wurden als Risikoträger („Risk Carrier“) bezeichnet, deren Lebensstil als Grund für ihre Erkrankung ausgemacht wurde. Über die kausale Verkettung hinaus, umgab die Krankheit auch ein Nimbus der Eigenverantwortung, der Schuldhaftigkeit, da die zur Infektion führenden Aktivitäten nicht der sozialen Norm entsprachen. Somit verband die Diagnose der Krankheit auch eine moralische Deutung und soziale Stigmatisierung (Lupton 2006: 18).

dieser Kategorie alle Szenarien in Verbindung mit der Nutzung einer Technologie oder anderer, von Menschen zumindest mittelbar verursachten Ereignissen stehen (Luhmann 1991: 111). Doch die Komplexität der Zusammenhänge erschwert die Gefahreneinschätzung erheblich, wie es sich beispielsweise im Fall der zivilen Atomkraft oder der flächendeckenden Vernetzung der Gesellschaft durch die Digitalisierung zeigt. Die Implikationen der hier subsummierten Szenarien stehen im Mittelpunkt dieser Arbeit und thematisieren vorrangig die Risiken aus dem Einsatz der neuen Technologien im Kontext des digitalen Wandels (vgl. AGCS 2018: 3), wie wir im fünften Kapitel aufzeigen werden.

Anders verhält es sich mit dem (4) natürlichen Risiko, also klimatischen oder tektonischen Phänomenen welche einen Schaden auch ohne Interaktion und Entscheidung seitens des Menschen verursachen können, folglich natürlichen Ursprungs sind.[201] Aus Sicht der Assekuranz sind Naturkatastrophen die größten Bedrohungen für Unternehmen, da diese zu hohen Schadensansprüchen der Kunden führen[202], auch wenn dies eher in der erstgenannten ökonomischen Risikokategorie einzuordnen ist. Für die natürlichen Risiken lässt sich jedoch festhalten, dass die Gefahren eines Erdbebens, Wirbelsturms oder Überflutungen zu den häufigsten Ursachen einer Geschäftsunterbrechung im analogen Zeitalter zählten und aufgrund ihrer teilweise gravierenden Auswirkungen im Fokus zahlreicher Untersuchungen und empirischen Erhebungen stehen (AGCS 2013: 3). Die natürlichen Risiken gehören demnach zu den besser erforschten Risikokategorien (Lupton 2006: 11). Natürliche Risiken werden ebenfalls im vierten Kapitel eine Rolle spielen, um den Ursprung des BCM im Kontext relevanter Krisenszenarien zu erläutern.

Die fünfte Risikokategorie thematisiert (5) politische Risiken, welche ein weitreichendes und diversifiziertes Feld umfassen (vgl. (Jackobsen 2012: 32f.). Aus Sicht der Unternehmen kann das politische Risiko in zwei Gruppen aufgeteilt werden. Im Sinne der ersten Gruppe meint das politische Risiko vorrangig den Schutz der eigenen Investitionen, zumeist in ausländischen Märkten und beschreibt die spezielle Risikoexposition der Investition innerhalb der Grenzen

[201] Dies trifft beispielsweise zu, wenn an einem Berghang durch übermäßige Abholzung, sprich durch menschliche Einwirkung, Bodenerosionen und Erdrutsch Schaden verursachen. Ein technologisches Risiko wäre es aber dann, wenn das Absterben der Bäume an ebendiesen Hang durch chemische Substanzen aus menschlicher Produktion, beispielsweise als Abfallprodukt aus einer lokalen Fabrik hervorgerufen worden wäre. Dem technologischen Risiko liegt immer ein Anteil an Unberechenbarkeit der durch den Menschen erschaffenen Techniken zugrunde, deren Komplexität Schäden indirekt verursachen kann.

[202] Interessanterweise sind mittelständige Unternehmen im viel stärkeren Umfang als Großkonzerne von der Kreditverfügbarkeit als von Umweltkatastrophen bedroht. Denn der Zugang zu den internationalen Kapitalmärkten steht diesen Unternehmen im weitaus geringeren Umfang zur Verfügung als den global-agierenden und börsennotierten Gesellschaften (AGCS 2013: 3).

eines bestimmten Rechtsgebietes.[203] Diese kann sich aus ökonomischen und finanziellen Aspekten des betreffenden Landes zusammensetzen und die Stabilität, Sicherheit und Kreditwürdigkeit betreffen (Erb, Campbell und Tades 1996: 29). Politische Ereignisse, welche in der Lage sind Investitionen oder Geschäftsaktivitäten zu beeinflussen, bilden daher den Kern des politischen Risikos[204]. Ferner kann das lokale Risiko durch Naturkatastrophen, Umweltverschmutzung, Kriminalität, Rechtsunsicherheit oder andere Standortfaktoren, die ebenso nicht durch direkte Handlungen von politischen Akteuren verursacht werden, für diese Risikokategorie relevant sein.[205] Die Kenntnis über Regeln und Abläufe, insbesondere informeller Natur sind überaus hilfreich bei der Einschätzung der Marktentwicklung sowie der eigenen Erfolgsaussichten. Darunter ist vor allem Korruption und Unkenntnis der lokalen Verwaltungsabläufe zu nennen.[206] Dieser Nachteil äußert sich für ausländische Unternehmen als Unsicherheit (Delios und Heinsz 2003: 1154) und bedarf einer fundierten Risikobewertung der verfügbaren Informationen.[207]

Eine andere Gruppe stellt hingegen das politische Risiko für die Sicherheitsproduktion in Unternehmen dar. Dazu zählen Entwicklungen und Veränderungsprozesse, welche die Stabilität oder Versorgungssicherheit in einem Land oder einer Region betreffen. Soziale Unruhen, Demonstrationen oder gewaltsame Zusammenstöße können nicht nur Investoren verunsichern, sondern auch konkrete Implikationen für die Prozesskontinuität haben (Ortiz et.al. 2022). Wenn Unruhen oder gewaltsame Proteste den Verkehr oder die Transport-Knotenpunkte blockieren, kann dies gravierende Auswirkungen auf die Versorgungssicherheit

[203] Die zunehmende Internationalisierung von Produktions-, Vertriebs- und Steuerungsfunktionen hat die Bedeutung dieser Risikokategoire für Unternehmen gleichsam erhöht, da multinationale Konzerne im globalen Produktionsnetzwerken aktiv sind und ihre Investitionsrisiken im internationalen Kontext bewerten. Dies bezieht sich auch auf die Perzeption der Unternehmensführung (Castells 2010: 121).

[204] Exportversicherungen wie die Hermes-Bürgschaft der deutschen Bundesregierung oder Absicherungen der Investitionen im Gastland über Handels- und Rechtsverträge zwischen dem Herkunfts- und Gastland können helfen das Risiko eines Investitionsausfalls zu mitigieren.

[205] Stabilität bedeutet die planbare und damit risikoarme Investitionsumgebung innerhalb eines politischen und justiziellen Raums. Potentielle Faktoren für Instabilität sind einerseits politische Aktivitäten seitens der staatlichen Autoritäten im Gastland die auf der Basis regulativer Maßnahmen Einfluss auf das Geschäftsumfeld nehmen können. Auf der anderen Seite steht die Verschlechterung der Sicherheitslage, beispielsweise durch Bürgerkriege, soziale Unruhen oder Organisierte Kriminalität (Kahl 2011: 7). Instabilität kann auch durch gelenkte Veränderungen des Wettbewerbsumfeldes, der Ineffektivität oder Korruptionsaffektion der Bürokratie oder etwa durch den Bruch mit Entscheidungen der Vorgängerregierung in Entwicklungs- aber auch Industrienationen hervorgerufen werden (Hood und Nawes 2004: 9). Ferner sind die Kosten einer Verlagerung von Produktionsstätten aus einem Gastland zu beachten (Busse und Hefeker 2005: 16).

[206] Korruption kann nach Ansicht mancher Autoren unter Umständen kein relevanter Faktor zur Berechnung des politischen Risikos darstellen. Wenn die Korruption stabilen Verfahrensmustern folgt, dann ist sie für ausländische Unternehmen berechenbar und bietet als eine informelle Regel gewissermaßen Orientierungshilfe. Unvorhergesehene Ereignisse stellen das größere Risiko dar als Korruption auf einem stabilen, kalkulierbaren Niveau (Jakobsen 2012: 35).

[207] Diese Risikokategorie wird ebenfalls im fünften Kapitel thematisiert, da sie in Gestalt des internationalen Terrorismus wesentlichen Einfluss auf die Entwicklung von BCM hatte (vgl. Rose 2011: 98).

der Wertschöpfungs- und Lieferketten haben, beispielsweise durch die sogenannten Gelbwestenproteste in Frankreich (Chamorel 2019: 51) oder der Blockade der wichtigsten Brücke zwischen Kanada und den USA durch Lastwagenfahrer in Reaktion auf die Corona-bedingten Maßnahmen im Februar 2022.[208]. Auch bewaffnete Konflikte, Krieg und Sanktionen beziehungsweise Ressourcenverknappung als deren Folge avancieren zu wichtigen Faktoren der Bewertung des politischen Risikos in Unternehmen. Zum Beispiel führten die russische Invasion in die Ukraine und die in Folge von Sanktionen und Lieferausfällen entstandene Ressourcenverknappung auf dem Energiemarkt zu signifikanten Belastungen[209] und Herausforderungen für Unternehmen in Deutschland (Bardt, Grömling und Schmitz 2022).

Die Relevanz des politischen Risikos begründet sich für MNU folglich bei Weitem nicht nur auf Korruptions- und Demokratieindizes in Entwicklungsländern, sondern nimmt zunehmend Entwicklungen der politischen (Protest-)Kultur und Stabilität von Transportwegen und Lieferketten in den Blick.[210] Wie wir im fünften Kapitel zeigen werden, hatten die Corona-bedingten Maßnahmen erheblichen Einfluss auf den Welthandel und die Sicherheit von Lieferketten. Dies betrifft nicht nur medizinische Materialien oder Impfstoffe (Brzoska, Neuneck und Scheffran 2021: 3), sondern auch politische Maßnahmen wie Kontaktbeschränkungen bis hin zu massiven staatlichen Interventionen in die Produktionsabläufe, wie es in Form der chinesischen Null-Corona-Strategie zu beobachten ist (AGCS 2020a). Die Komplexität und Interdependenz globaler Lieferketten wird unter dem Eindruck der Corona-Pandemie, der politischen Einflussnahme auf Produktionsabläufe und der Auswirkungen auf den weltweiten Warenverkehrs zum Risiko für Betriebsabläufe und Prozesskontinuität in Unternehmen (Gereffi, Pananond und Pedersen 2022). Die Folge ist eine Priorisierung politischer Risiken für Unternehmen, die neben gestiegenen Cyberbedrohungen und dem allgemeinen Risiko von Betriebs- oder Lieferkettenunterbrechung am häufigsten genannt wurden, wie eine kürzlich veröffentlichte Umfrage unter 2600 Risikoexperten aus 89 Ländern aufzeigte (AGCS 2022).

[208] Über die blockierte Ambassador Brücke zwischen den Automobilproduktionszentren Detroit und Windsor werden im Jahresdurchschnitt etwa 27% des US-Kanadischen Handels abgewickelt. Eine andauernde Unterbrechung der Produktionskette zwischen beiden Standorten und Absatzmärkten könnte daher signifikanten Einfluss auf die wirtschaftliche Entwicklung der Region haben (Guardian 2022).

[209] Laut einer Erhebung des Instituts der deutschen Wirtschaft berichten 62 Prozent der befragten, in Deutschland ansässigen Unternehmen starke Belastungen durch erhöhte Energiepreise, sowie jeweils ein Drittel verknappte Gaslieferungen beziehungsweise Lieferungen durch Dienstleister (Bardt, Grömling und Schmitz 2022: 2).

[210] Dabei kann angemerkt werden, dass in einer Studie der Friedrich Eberhard Stiftung für die Periode 2006 bis 2020 ein starker Anstieg der weltweiten Proteste registriert wurde, insbesondere in Ländern mit mittlerem und hohem Einkommen (Ortiz et.al. 2022: 14).

Deshalb stellen die Risikokategorien eine Betrachtung und selektive Zuordnung von möglichen Schadensereignissen in Gruppen dar, um die Kommunikation und Entscheidung über Risiken in Unternehmen zu erleichtern. Diese Sichtweise repräsentiert die traditionelle Einordnung von Risiken in Kategorien und Mustern der objektbasierten Schadenswirkung und ihrer Eintrittswahrscheinlichkeit. Das Risiko der Entscheidung sowie die Perspektive auf die Prozess- und Kommunikationskontinuität gewannen im Fall der beobachteten Unternehmen durch die Krisen und exogenen Ereignisse wie Corona-Pandemie, Ukrainekrieg und vor allem der Cyberbedrohungen an Bedeutung. Diese Beobachtung beruht auf den im Rahmen der ethnographischen Studie festgestellten Veränderungen von Prioritäten und Beschlüssen zum Umgang mit Risiken durch Experten in den involvierten Unternehmen.[211] Im Rahmen der beobachtenden Teilnahme konnten die Unterschiede in Form und Zielsetzung von unternehmensinternen Risikodiskursen mitverfolgt und eine Verschiebung hin zu einem systemischen Risikobegriff kontempliert werden.

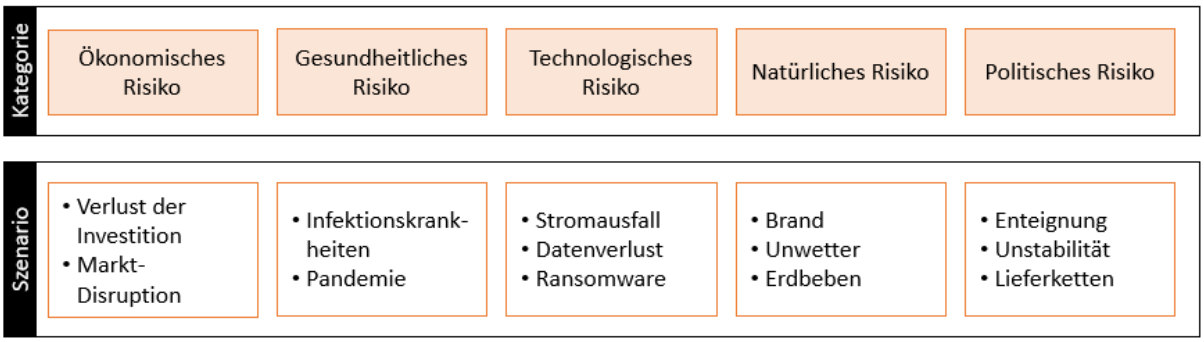

Abb. 4.5. Risikokategorien und Risikoszenarien zur Einordnung von Risiken im Unternehmenskontext. Eigene Darstellung.

Der Trend zu objektübergreifenden, das bedeutet in der Sprache der Unternehmenskommunikation holistischen - Risikobetrachtung reflektiert einerseits die Verbindung zwischen Risikokategorien, wie es etwa im Fall der gesundheitlichen, politischen und technologischen Risikokategorien, wie es im Zuge der Corona-Pandemie zu beobachten war. Andererseits rückte die Betrachtung von Prozessen und Betriebsabläufen in den Vordergrund der Risikoidentifikation. Dies zeigt sich beispielsweise an der Adaption von Risikokontrollen. Traditionelle Standards fragten im Unternehmenskontext nach Risiken und Kontrollen zu spezifischen Ereignissen innerhalb der zuvor genannten oder ähnlichen Risikokategorien, beispielsweise der Implikationen durch einen Stromausfall oder einer

[211] Zu diesem Zweck wurden 18 Landesgesellschaften zu den sicherheitsrelevanten Folgen der Corona-Pandemie im November 2020 befragt, deren Ergebnisse im siebten und achten Kapitel reflektiert werden. Mit Blick auf die Energiekrise zeigte sich in der Beobachtung intensiver Vorbereitungen auf relevante Krisenszenarien im Unternehmen die Bedeutung und Abhängigkeit von der IT-Infrastruktur zur Fortsetzung der Geschäftsprozesse, sowie folglich der ununterbrochenen Stromversorgung (Workshop 26.11.2020).

Naturkatastrophe.[212] Das neue, prozessorientierte Risikoverständnis orientiert sich an systemischen Risikobegriffen, welche die Kontinuität von Prozessen gefährden können, wie zum Beispiel im Fall der Nichtverfügbarkeit von Gebäuden oder Dienstleistern. Die sich anschließenden Fragen zur Risikobewertung und Einordnung werden im Folgenden vertieft werden, um die Ausgangsgrundlage und Veränderungen im Umgang mit Unsicherheit zu verstehen. Dies soll es schließlich ermöglichen die Sicherheitsproduktion in Unternehmen durch systemische Risikokontrolle nachzuzeichnen.

4.2.3.2. Risikobewertung

Die Risikobewertung schließt sich an die Identifizierung eines Risikos beziehungsweise einer Risikokategorie an. Die Anzahl der Schadensmöglichkeiten – der spezifischen Szenarien - ist theoretisch unbegrenzt. Die Risikobewertung arbeitet daher mit der Wahrscheinlichkeit des Eintretens eines Schadens. Dies ist der Bereich der Stochastik, das bedeutet der Berechnung wie wahrscheinlich ein bestimmtes Ereignis innerhalb eines definierten Zeitfensters stattfindet. Doch jede Kalkulation setzt gesichtete Daten voraus, falls diese fehlen oder nicht belegt sind, kommen andere Faktoren zum Tragen. Ein wesentlicher Aspekt ist die Beobachterebene selbst und beruht auf Überzeugungen und Erwartungen der Verantwortlichen der Risikobewertung (Douglas 1992: 12). Bereits in semantischer Hinsicht beinhaltet die Risikobewertung ein subjektives Momentum. Die Frage ob Risiken objektiv betrachtet werden können oder immer einer sozialkonstruierten Bewertungsebene unterworfen sind trennt die Vertreter des (1) „realistischen“ und des (2) „konstruktivistischen“ Ansatzes[213], welche wir beide im Folgenden vorstellen werden (Braes und Brooks 2010: 16).

Die (1) objektive Risikobewertung verdankt ihren Namen dem Vertrauen auf eine faktenbasierte und transparente Kalkulation des Risikos. Diese Überzeugung basiert auf zwei Annahmen, erstens, dass Risiken real und als solche zu beobachten sind und dass zweitens die Wahrscheinlichkeit ihres Eintretens vorherzusagen ist. Die erste Voraussetzung ist der zentrale

[212] Aus Workshops mit IT-Fachleuten und Experten der IT-Sicherheit im Dezember 2021 wurden zudem die Folgen des Log4j Zwischenfalls, eines fehlerhaften Patches der zu Sicherheitsrisiken führte, behandelt und die grundsätzliche Bedeutung systemischer Risikokontrolle artikuliert. Es zeigte sich dass Kontaktdaten von Dienstleistern nicht dokumentiert waren oder die Beziehungen zwischen Applikationen nicht bekannt waren, wodurch potentielle Sicherheitsrisiken entstehen hätten können.

[213] Erwähnenswert neben dem (a) modernistischen, objektiven Ansatz, dem (b) symbolisch-kulturellen, subjektiven Ansatz ist der (c) gesellschaftlich-manipulative Ansatz. Letzterer legt seinen Fokus auf die Rolle der sozialen Kontextbildung unter den Determinanten der modernen hochkomplexen Gesellschaft und der Ausübung von Macht über Risiken (vgl. Foucault 2005; Foucault 2006; Lemke 2000: 2). Hier wird die Risikoabwägung innerhalb einer gesellschaftlichen Ordnung vorgenommen (Krahmann 2007: 3), die durch die Folgen der Urbanisierung und beschleunigten Technisierung und Globalisierung durch Komplexität gekennzeichnet sind (Clapton 2011: 9). Dies führt zu potentieller Einflussnahme über die Artikulation von Risiken und Sicherheit (Owen 2009: 19).

Gegenstand der ontologischen Debatte über die Realität von Risiken (Clapton 2011: 281). Aus Sicht der Realisten sind Risiken reale Phänomene, deren Existenz auch ohne die Interpretation durch Individuen als wahr und an sich real angenommen würde (vgl. Lupton 2006: 14). Für die Bewertung eines Risikos sind demnach allein Fakten aussagekräftig und ausreichend.[214] Soziale und moralische Kontexte gelten als irrelevant, da das Risiko sich selbst definiert und der Beobachter nur eine Deskription der Realität vornimmt. Die Konstruktion eines sozio-kulturellen Rahmens wirke hingegen nur als Verzerrung der realen Beobachtung (McLean, Patterson und Williams 2009: 4).

Die zweite Annahme dieses Ansatzes stützt sich auf die prinzipielle Kalkulierbarkeit von Risiken aus realistischer Perspektive. Zum Beispiel können neue Technologien, deren originärer Zweck die Bezwingung der Natur und ihrer Risiken war, oft selbst Quellen für neue Risiken darstellen (Beck 2006; Kasperson 1988: 177). Mithilfe einer objektiven Risikoanalyse versuchen modernistische Ansätze daher unter Ausschluss von sozialen Komponenten und Perzeptionen die Folgenabschätzung durchführen (Horst 2012: 45). Dies wurde im methodischen Rahmens des BCM für die Bewertung der Risiken einer Geschäftsunterbrechung als ‚best practise' seit etwa zwei Dekaden angewendet (Torabi, Soufi und Sahebjamnia 2014: 309). Unter Beachtung von Standortfaktoren und einer räumlichen Eingrenzung der möglichen Schadensereignisse[215] wurden die Auswirkungen auf die Geschäftsprozesse innerhalb eines definierten Zeitraums bewertet. Die Wahrscheinlichkeit eines Eintretens wurde aufgrund der tatsächlichen Schadensfrequenz abgeleitet und in Verbindung mit dem gewählten Zeitrahmens gesetzt (Lam 2002: 23). Die Ergebnisse ergeben schließlich die prognostizierte Wahrscheinlichkeit des möglichen Minimal- und Maximalwerts eines Schadens für ein dezidiertes Gebiet.[216]

Diese Methode beinhaltet allerdings problematische Elemente. Denn wenn Szenarien in der Vergangenheit selten beobachtet und dokumentiert wurden, aber ein hohes Schadenspotential vermuten lassen, können über einen Annäherungswert hinaus nur schwer mit statistischen

[214] Im Fall einer Versicherung wird dieser Unterschied deutlich: Ein Versicherungsnehmer sichert sich gegen potentielle Schäden ab, weil er in seiner Vergangenheit Schäden erlebt hat, das bedeutet als unmittelbare Realität versteht. Die Verlängerung der Versicherungspolice entspricht somit Annahme einer realistischen Gefahr, ist jedoch eine tatsächliche Wiederholung der originär getroffenen Entscheidung zur Absicherung (Luhmann 1996: 280). Der Realitätsbegriff des Versicherungsgebers beruft sich hingegen auf Statistiken, also auf objektive Maßstäben in dessen Modellen Einzelfälle ausgeblendet werden und in Form der Standardabweichung das zumeist zu kalkulierende unternehmerische Risiko repräsentiert.

[215] Die Liste möglicher Schadensereignisse oder Szenarien wurde auf der Grundlage vergangener Ereignisse erstellt, sowie im erweiterten Verfahren als Transfer aus vergleichbaren Regionen (zum Beispiel tektonisch aktiven Gebieten) als mögliche Erstereignisse geführt.

[216] Dieses Ergebnis stellt beispielsweise den Ausfall kritischer Geschäftsprozesse für die Region Kalifornien durch ein Schadensereignis als maximaler Schadenswert mit einer Wahrscheinlichkeit von 1 in 20 Jahren aus.

Methoden[217] vorhergesagt werden (AGCS 2012: 5f.). In Ermangelung vergleichbarer Fälle ist die Datengrundlage unter Umständen zu klein, um verlässliche Modelle entwickeln zu können (Sarewitz 2003: 806). In der Literatur wird daher die Schwäche quantifizierbarer, objektiver Methoden der Risikobewertung betont (Sahebjamnia, Torabi und Mansouri 2015: 262), welche als ungeeignet scheinen, um die Risiken der Geschäftsfortführung praktikabel zu messen. Der objektive Ansatz basiert auf der Verfügbarkeit von exakten Daten. Dies kann allerdings im Fall von begrenzten Datenquellen, wie im Fall neuer, komplexer Technologien problematisch sein.[218] Die Abhängigkeit von Fakten impliziert die epistemologische Vorrausetzung der Anerkennung von real existierenden Risiken und deren Dokumentation zu Auswertungszwecken (Owen 2009: 21). Zudem unterliegt die objektive Risikobewertung immer einem subjektiven Eindruck der Situation. Zum Beispiel ist der zu untersuchenden Gegenstand zumeist mit Begriffen aus dem menschlichen Erfahrungshorizont versehen, deren Bedeutung auf das Objekt ausstrahlt und somit jede Beobachtung prägt (Lupton 2006: 12). Die Interpretation des Objekts ist somit mit einer subjektiven Assoziation verbunden, beginnend mit seiner sprachlichen Umschreibung.[219] Eine Risikobewertung ohne individuelle Vorprägung oder Konnotation ist daher nur schwer vorstellbar (Clapton 2011: 282).

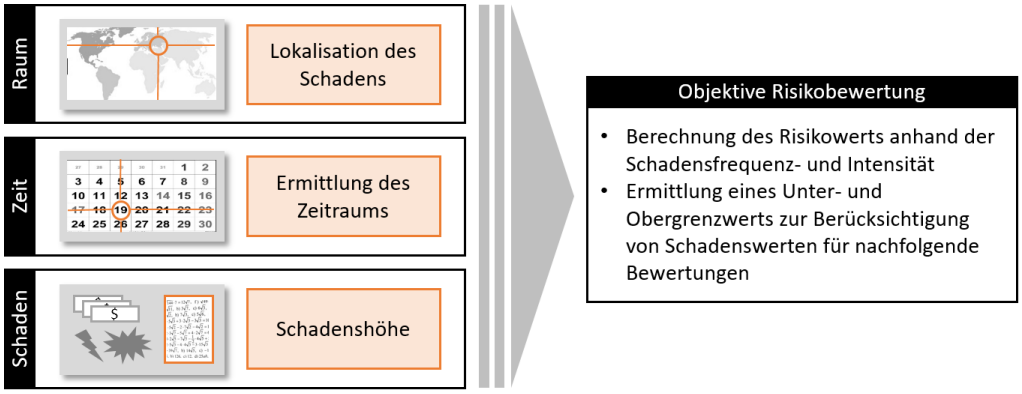

Abb. 4.6 Kriterien der anlogen BCM-Risikobewertung. Eigene Darstellung.

[217] Ebenso stehen Entscheidungsträger vor einer schwierigen Entscheidung nach objektiven Maßstäben, wenn Szenarien aufgrund der mangelnden Empirie abstrakt bleiben, wie beispielsweise im Vorfeld der Anschläge vom 11. September 2001 (vgl. Perrow 2011: 48).

[218] In diesem Fall wird auf die Expertise von Fachkundigen zurückgegriffen. Expertise kann als "(…) [a] special skill or knowledge that is acquired by training, study, or practice" verstanden werden (Bahlia und Rivard 2005: 178). Doch die Rolle des Experten wird im postfaktischen Raum des Informationszeitalters mit seinen zahlreichen, konkurrierenden Meinungsbildern schwieriger zur Deutung von Risiken. Mit Blick auf die Kritik an Entscheidungsträgern und von ihnen befragte Experten bemerkte Ulrich Beck an, dass die alten Autoritäten „(…) are no longer seen only as instruments of risk management, but also as a source of risk" (Beck 2006: 336).

[219] Wenn ein Zoologe beispielsweise eine Ameisenkolonie objektiv beobachten möchte, ist dennoch zu beachten, dass bereits die semantische Umschreibung des Ameisenstaates, mit einer Königin, Arbeiterinnen und Kriegerinnen in einen Wertekontext geprägt ist, welcher eine subjektive Konnotation gegenüber dem Untersuchungsgegenstand schwerlich ausschließen lässt.

Demgegenüber steht der kulturell-symbolische Ansatz aus der Gruppe der (2) subjektiven Risikobewertung (Douglas 1992). Individuellen Prägungen, welche durch Interpretation, Antizipation oder Assoziation das Ergebnis der Analyse beeinflussen, stehen im Vordergrund der Risikoperzeption (Horst 2012: 45). Es ist als sozialkonstruktivistischer Ansatz zu verstehen, der soziale Interaktionen und kulturelle Prägungen als ausschlaggebende Elemente der Risikobewertung identifiziert (Clapton 2011: 281). Die Interdependenz zwischen Individuen und Gruppen, die Auswirkungen sozialer Normen, kulturelle Erfahrungen und Traditionen beeinflussen die Risikowahrnehmung. Risiken werden demnach in starker Abhängigkeit von eigenen Erfahrungen, *Biases-Emotionen* oder vor einem spezifischen kulturellen Hintergrund bewerten (Lupton 2006: 5).

Die zwei wesentlichen Unterschiede zum objektiven Ansatz sind, dass erstens Risiken nicht per se als existent aufgefasst werden und zweitens die Bewertung durch eine subjektive Wahrnehmung geformt werden. Dadurch wird eine technische Bewertung des Risikos unwahrscheinlich, da die sozialkonstruktivistische Betrachtung eine anthropologische Perspektive auf die kulturell-symbolische Wertung des Risikoanalysten annimmt (McLean, Patterson und Williams 2009: 5). Daher werden bestimmte Risikoszenarien von Entscheidungsträgern anders wahrgenommen, wenn sie bereits eigene Erfahrungen in diesem Zusammenhang gesammelt haben oder eine Affinität für dieses Thema aufweisen (Kasperson u.a. 1988: 184). Diese Erfahrungen können wesentlichen Einfluss auf die Bewertung eines Risikos haben und sind unter Umständen für andere Experten[220] nicht in vergleichbarer Weise ersichtlich (Lupton 2006: 13).

Zudem beleuchten zwei verschiedene Beobachter das gleiche Risiko unter Umständen unterschiedlich und treffen bereits mit der Entscheidung über eine Beobachtung oder Nichtbeobachtung eine signifikante Vorauswahl. In diesem Fall wäre von einer Risikosozialisation zu sprechen (Luhmann 1991: 12), deren Einbettung auf Normen und einem (partiellen) gesellschaftlichen Konsens beruht. Das Eintreten eines unerwünschten Ereignisses erscheint für Betroffene relevanter als für Nicht-Betroffene, aber auch die Selektion der jeweiligen Risikokategorie kann vom Hintergrund des Beobachters aus verstanden werden. Die

[220] Experten tragen zum gesellschaftlichen Diskurs bei und vollziehen eine Definitions- und Beraterfunktion für die Identifikation, Bewertung und Mitigation von Risiken (Mythen 2004: 56). Fachliche Qualifikation, Methodenkenntnis und öffentliche Reputation sind entscheidende Kriterien der Kompetenzzuschreibung durch die Öffentlichkeit (Günther et. al. 2011: 53). im Fehlen an staatlicher Handlungsfähigkeit begründet werden, welche letztlich auf mangelnder Expertise und Risikokommunikation beruhe. Hier lautet es weiter: „Gerade deshalb bewertet die Öffentlichkeit Mediziner und Naturwissenschaftler, häufig anders als etwa Sozial- und Geisteswissenschaftler, als glaubwürdig. Kompetent gilt der Wissenschaftler, dem man zutraut, wissenschaftliche Probleme effektiv zu bearbeiten und zu lösen“ (Günther et. al. 2011: 53).

implizierte oder explizite Interessenszuwendung zu einer Risikokategorie kann ihre Relevanz aufwerten oder verringern, wie beispielsweise Risikoumfragen zu den Themen Klimawandel (AGCS 2018) und islamistischer Terrorismus in Deutschland (Bock 2017) für die jeweilige Gruppe von Individuen zeigen.[221] Vereinfacht gesprochen, verstärken das Weltbild und die Selektion der Risikokategorie eine Risikoperzeption und können über Deutungsvorlagen bereits steuernd wirksam werden. Dies geschieht beispielsweise durch die Thematisierung und Akzentuierung von Problemen, wie zum Beispiel der Migration durch populistische Akteure, welche den Diskursrahmen und einhergehende Emotionalisierung gezielt nutzen (Geiges 2018: 54).

Ein integrativer Ansatz zur Risikokontrolle sollte sich normativ gesprochen dieser unterschwelligen Beeinflussung entziehen, doch können gerade die nicht artikulierten und subjektiven Einflüsse jeder Entscheidung einen wesentlichen Anteil für die eine oder andere Richtung bedeuten. Dies wird an einem Beispiel aus der Finanzkrise 2007/2008 deutlich, als Investitionsentscheidungen auf der Grundlage von branchentypischen Standards und unter Berufung auf Ratingagenturen getroffen wurden. MacKenzie und Spears berichteten auf der Grundlage von Interviews mit Vermögensverwaltern und Fond-Managern, dass das Vertrauen in die Ratingagenturen für die betroffenen Unternehmen zum damaligen Zeitpunkt ausreichte und kaum eigene Risikomodelle als Referenz oder Kontrollinstrumente für Entscheidungen herangezogen wurden (MacKenzie und Spears 2014: 31). Das zu dieser Zeit übliche Outsourcing von Risikoentscheidungen wie im Fall der Bonität von strukturierten Kreditprodukten und Wertpapieren (Collateralized Debt Obligation) folgte der kulturabhängigen Logik der Branche, solche Entscheidungen einzig auf den Einstufungen der großen Ratingagenturen aufzubauen. Die Bedenken oder individuellen Risikokalkulationen wurden von den Experten der betroffenen Instituten nicht oder nur unzureichend artikuliert und die Kontrolle von Risiken im Umgang mit der Unsicherheit am Wertpapiermarkt durch externe Ratingvorgaben überschätzt (ebd.: 25f.).

Ein weiterer Aspekt betrifft die bewusste und unbewusste Selektion von Risiken, welche dem organisationsinternen Risikodiskurs bereitgestellt werden, sind eine Limitation auf die Handlungsfelder, welche von den Mitgliedern der Organisation als relevant wahrgenommen werden, beispielsweise wenn Cyberrisiken über Naturkatastrophen oder negative Marktentwicklungen priorisiert werden (vgl. AGCS 2020). Andere Risiken können zum

[221] Die perzeptive Bewertung des Terrorismusrisiken durch islamistische Akteure in Deutschland wird bei einer affinen Gruppe, in diesem Fall Unterstützer der Alternative für Deutschland (AfD) hinsichtlich der tatsächlichen, empirischen Bedrohung deutlich überbewertetet (Bock 2017: 245).

Zeitpunkt der Beobachtung noch nicht ausreichend beleuchtet worden sein, wie technologische Folgeabschätzungen oder geschäftsbezogene Risiken in volatilen Markt- oder Projektumgebungen (Boutellier et. al. 2007: 133). Wieder andere Risiken erschienen eingangs irrelevant wie die mögliche Knappheit medizinischer Schutzmasken wie im Fall der Pandemie zum Jahreswechsel 2019/2020[222] oder werden aus anderen Beweggründen vernachlässigt, so wie Sicherheitslücken in sensiblen IT-Systemen während des COVID-19 veranlassten Wechsels in das Home Office (BSI 2020: 33)[223]. Dies zeigt erneut die Bedeutung eines übergreifenden, systemischen Risikobegriffs zur Bestimmung von Handlungsfeldern und Koordination unternehmerischer Sicherheitsproduktion.

4.3. Zusammenfassung – Risikokontrolle und Organisation im Wandel

Die Unterscheidung von Risiko und Gefahr zeigt die Problematik des traditionellen Risikoverständnisses auf und bietet eine Alternative zur Risikokontrolle an, indem es die objektbezogene Betrachtung von Risiken durch eine systemische Differenzierung zwischen exogenen Gefahren und entscheidungsinhärenten Risiken ersetzt. Die systemische Betrachtung von Risiken orientiert sich aus organisationstheoretischer Sicht an der Prozess- und Kommunikationskontinuität. Denn während das Risiko durch eine Entscheidung determiniert wird, liegt im Fall der Gefahr schlicht ein Ereignis vor, für dessen Eintreten keine Interaktion oder Handlung erforderlich ist. Das Risiko, welches ein Unternehmen zu bewerten versucht, hängt vornehmlich von einer Entscheidung ab, egal ob Handlung oder Unterlassung. Am Ende ist das Risiko mit einer Entscheidung des Unternehmens verbunden, wie beispielsweise der Ausdehnung der Digitalisierung von Prozessen wie in Folge der Corona-Pandemie und bildet resultierend aus ihrer Selbstreflexivität einen Teil der Identität und Erinnerung des Unternehmens.

Die Einbindung in Produktions- und zunehmend auch Informationsnetzwerke zeigt diese Problematik auf. Denn die Abgrenzung zwischen autopoietischen Systemen einerseits und die Komplexitätssteigerung der Interdependenzen zwischen Entitäten andererseits erschweren die Risikoabwägung und Umsetzung von Kontrollmaßnahmen. Da jede Entscheidung auch einer

[222] Die deutsche Bundesregierung unterschätzte die Einschränkungen auf dem Weltmarkt durch die aufkommende Corona-Pandemie und suchte im Frühjahr 2020 mit allen Kräften nach verfügbaren Schutzmasken und anderer medizinischen Ausrüstung.

[223] Das Bundesamt für Sicherheit in der Informationstechnologie konstatierte in seinem Bericht zur IT-Sicherheit in Deutschland 2020, dass viele Unternehmen ihre IT-Sicherheitsarchitektur unter dem Eindruck von COVID-19 zu Gunsten eines für den Moment funktionsfähigen Fernzugriffs vernachlässigt hätten (BSI 2020: 33). Dieser Fall zeigt die Ausblendung von Risiken, welche in den vorausgehenden Jahren stetig an Aufmerksamkeit und Bedeutung im unternehmensinternen Risikodiskurs gewann und im selben Jahr erstmals die Spitze der meist-genannten Risiken erreichte (AGCS 2020), aber durch die Corona-Krise zum Wohle der Geschäftsfortführung unter den Bedingungen der Hygienemaßnahmen und Büroschließungen ausgeblendet wurde.

Kommunikation bedarf, um von den angesprochenen Mitgliedern registriert und umgesetzt zu werden, erweitert sich der Anforderungsumfang an intraorganisationale Sicherheitsproduktion. Dazu zählt auch, den Umgang mit Risiken entsprechend zu artikulieren um systemweit Akzeptanz zu finden, mindestens über die Tatsache der Entscheidung als Kommunikation und Anschlussoperation des Systems selbst. Kommunikation muss zudem autorisiert, das bedeutet durch die exklusive Mitgliedschaft bestätigt sein und erinnert werden. Letzteres adressiert einen Teil des kollektiven Gedächtnisses und Entscheidungen müssen dort bei Bedarf abrufbar sein. Dies ist die eigentliche Chance von Unternehmen mit Entscheidungen unter den Bedingungen der Unsicherheit im Informationszeitalter umzugehen. Die Bezugnahme auf entstandene Erfahrungswerte und eine möglichst abdeckende Verinnerlichung der Entscheidung innerhalb der Organisation kann das technologische Risiko erfolgreich zu kompensieren helfen und qua Erinnerungskultur und –Technologie, wie einem virtuellen Gedächtnis, der Zersplitterung der Organisationsidentität entgegenwirken.

Das bisherige, traditionelle Risikoverständnis, wie es im Fall der Risikokontrollsysteme des analogen Zeitalters zu beobachten war, ist als ein Resultat der Perzeptionsdeterminanten von Organisationen einzuordnen, deren prinzipielle Annahme auf der Abgrenzung, Kommunikation, Struktur und Arbeitsweise eines autopoietischen Systems unter Zuhilfenahme der Werkzeuge des analogen Zeitalters beruht. Das Novum der digitalen Umgebung liegt im Einsatz von Technologien, deren Risikobetrachtung eine sich weiterentwickelnde Methodik der Unsicherheitsabsorption erforderlich macht. Die hier beschriebenen traditionellen Arbeitsmittel der Identifikation und Bewertung von Risiken entsprechen einer Logik der analogen Risikofaktoren und –Umwelt aus organisationstheoretischer Sicht. Im folgenden Themenblock über die Risikomitigation im analogen und digitalen Zeitalter beginnt daher mit einem Rückblick auf die Ursprünge und Problematiken der unternehmerischen Risikokontrolle und zeigt die Anwendung der Erkenntnisse dieses Kapitels auf die Sicherheitsproduktion in Unternehmen.

III) Unternehmensinterne Sicherheitsproduktion im Wandel

Im letzten Kapitel wurde die Grundlage für das Organisationsverständnis dieser Arbeit entwickelt, in welchem die zentralen Annahmen von Luhmann reflektiert wurden und die Bedeutung und Problematisierung von Anschlusskommunikation für Organisationen herausgearbeitet wurde. Damit wurde der Weg zum Themenkomplex von Unsicherheit, Risiko und Gefahren eröffnet, in deren Kontext Risikokontrollsysteme in Unternehmen als die Organisationselemente identifiziert wurden, die diese Problematisierung thematisieren. Die Kontinuität der Prozesse und Verhinderung eines Kommunikationsabbruchs sind dadurch die zentralen Pfeiler der Sicherheitsproduktion von Unternehmen im Sinne unserer Fragestellung. Dadurch stellt sich nun die Frage, wie sich der traditionelle Risikobegriff im Zuge der Digitalisierung und Einführung neuer Technologie verändert, beziehungsweise wie eine neue Form der Risikokontrolle aussehen muss, um Unternehmen einen bestmöglichen Umgang mit der Unsicherheit im Informationszeitalter zu ermöglichen?

Diesem Komplex widmet sich dieser Themenblock, der aus zwei Kapiteln besteht. Das nun folgende fünfte Kapitel wird den Umgang mit Risiken im analogen Zeitalter zum Gegenstand haben, in dem die Grundlagen unternehmerischer Sicherheitsproduktion im Sinne der klassischen Vorsorge- und Krisenplanung Risiken nach traditionellem Muster erklärt werden sollen. Dieses Kapitel umfasst zudem drei Fallbeispiele, welche die Entwicklungen und Herausforderungen der (traditionellen) Risikokontrolle aufzeigen. Dazu sind zwei Begriffe relevant, welche im Folgenden vertieft werden sollen. Das Business Continuity Management (BCM) repräsentiert die klassische Ausrichtung der Vorsorgeplanung anhand objektbezogener Ressourcenplanung[224], beispielsweise der Nichtverfügbarkeit von Arbeitsflächen (Walser und Riedl 2010: 258). Der zweite Begriff thematisiert die ad-hoc Reaktionsfähigkeit von Organisationen in Form des Krisenmanagements (Pike, Dawley und Tomaney 2010: 60f.), welches aufbauend auf konkreten Bedrohungsszenarien die Handlungsfähigkeit von Unternehmen in spezifischen Situationen wie zum Beispiel Terroranschlägen oder Naturkatastrophen sicherstellen soll (Kahan, Allen und George 2009: 22). Anhand dieser Begriffe lässt sich die traditionelle Herangehensweise von Unternehmen an ihre interne Sicherheitsproduktion nachzeichnen und auch ihre Limitationen aufzeigen.

[224] Dies betrifft vorrangig die Sicherstellung der Kontinuität von Geschäftsprozessen (vgl. Braes und Brooks 2010: 16). Diese wiederum basierten auf vier Ressourcen, deren Verfügbarkeit durch die Methodik des Business Continuity Managements sichergestellt werden sollen. Dies umfasst die Verfügbarkeit von Gebäuden, Mitarbeitern, IT- und Kommunikationstechnologie sowie kritischer Dienstleister (BCM Academy 2016: 28),

In diesem Kapitel werden die methodische Verortung und Beschreibung der Risikokontrolle im analogen Zeitalter im Sinne seines zu diesem Zeitpunkt vorherrschenden Risikodiskurses aufgezeigt werden. Doch dieser Diskurs unterlag, wie zu zeigen sein wird, einem Veränderungsprozess durch die zunehmende Verflechtung von Prozessen und IT-Systemen, welcher sich auch in der Betrachtung der Experten auf die Herausforderungen und Sicherheitsdispositive, insbesondere hinsichtlich der Bedeutung von Informationen niederschlug, wie durch die ethnographische Beobachtung festgestellt wurden. Daher ist der Schwerpunkt des sechsten Kapitels die Nachzeichnung der Veränderungen durch die Abhängigkeit von Informationstechnologie für die Kontinuität von Prozessen und Anschlusskommunikation als Folge der Digitalisierung. Aus diesem Grund werden die konkreten Bedrohungsdimensionen im Informationszeitalter in diesem Kapitel aufgezeigt und ebenfalls in Fallbeispielen vorgestellt, um der Tragweite und Dringlichkeit einer Anpassung des traditionellen Risikoverständnisses zu verdeutlichen (vgl. Khan und Sepúlveda 2015: 8).

Die konzeptionelle Antwort zur Sicherstellung von Kontinuität unter den Bedingungen der Unsicherheit durch die Digitalisierung und globale Vernetzung[225] wird schließlich als Schlussfolgerung aus der ethnographischen Untersuchung im sechsten Kapitel als Selbstbeobachtung der Komplexität der organisationsinternen Prozesse unter dem Begriff Resilienz eingeführt. Mithilfe der theoretischen Grundlagen der vorrausgehenden Kapitel und der Beobachtungen der ethnographischen Untersuchung soll daher hier das Konzept von Resilienz im Kontext von Unternehmen verortet werden. Die Darstellung von Bedrohungslagen in den Fallbeispielen übernimmt dabei die Funktion einen objektiven Bewertungsrahmen der Sicherheitsdispositive im Informationszeitalter darzulegen und die Erkenntnisse der ethnographischen Untersuchung hinsichtlich dieser Bedrohungen aus Sicht der Organisation einbinden. Diese Erkenntnisse werden uns vorrangig im Abschnitt über die Veränderung des Risikodiskurses und der Kontrollsysteme, sowie zu den Hintergründen der Einführung von ITSCM als Implikationen für die Sicherheitsproduktion in Unternehmen begegnen. Dadurch wird der letzte Schritt zur Darstellung einer resilienten Organisation, welche durch Sicherstellung ihrer internen Prozesse und Anschlusskommunikation schließlich im siebten Kapitel eingeleitet.

[225] Die Einbeziehung internationaler Standorte und Absatzmärkte unterstützen ein globales Verständnis von Unternehmensführung, die jeweiligen Produktionsorte und Hardwarestandorte haben aber weiterhin einen lokalen Charakter (Castells 2010: 101).

5. Risikomitigation im analogen Zeitalter

Die bisherige Diskussion in dieser Arbeit behandelte den Wandel vom klassischen Verständnis der Organisationen mittels Entscheidungsprogrammen hin zum hier verwendeten Risikobegriff, der sich über die Unterscheidung von Gefahr, Unsicherheit und schließlich dem Risiko der Entscheidung vom klassisch-ökonomischen Risikobegriff in Unternehmen abgrenzt. Die organisationssoziologische Betrachtung von Anschlusskommunikation baute den Bogen zur Sicherheitsproduktion in Organisationen auf, das im Kontext von Unternehmen als Risikokontrollsysteme in Erscheinung tritt. Die sicherheitsrelevanten Fragen und Dispositive stellen dabei besondere Herausforderungen an die primär in ökonomischen Fragen routinierte Führungsebene von Unternehmen und erfordert eine Übersetzung von Entscheidungskriterien für nicht-ökomische, sicherheitskonnotierte Problemstellungen. Darunter werden im Folgenden Unterbrechungen von Prozessen, beziehungsweise deren organisationstheoretische Entsprechung in Form des Kommunikationsabbruchs, verstanden. Aus dieser Lage ist es nun möglich die soziologische Betrachtung der Begriffe Risiko, Unsicherheit und Gefahr analytisch umzusetzen und mit den Entwicklungen der Risikokontrolle innerhalb von Unternehmen zusammenzubringen.

Dieses Kapitel wird sich den traditionellen Mustern der Sicherheitsproduktion in Unternehmen widmen und die Risikokontrolle in Unternehmen anhand der bereits angedeuteten Methoden Business Continuity Management (BCM) und Krisenmanagement (KM) im analogen Zeitalter beschreiben. Diese seit etwa zwanzig Jahren im Kontext von MNU konkretisierten und anhand von internationalen Industriestandards genormten Praktiken erlebten eine stetige Genese ihrer Zielsetzung, Relevanz und Implementierung in Unternehmen (Christensen und Petersen 2017: 1443). Generell gesprochen fanden diese Praktiken und Methoden bisher nur geringfügig Beachtung in der Sicherheitsforschung (Hanson 2018: 136) und sollen hier eine Schnittmenge zwischen ökonomischen und sicherheitspolitischen Themenfeldern mit Blick auf Unternehmen und ihren Umgang mit geschäftsgefährdenden Risiken verdeutlichen. Die folgende Darstellung der traditionellen Entwicklung unternehmerischer Vorsorge und Sicherheitsproduktion beginnt daher mit dem Überblick über die zentralen Begriffe von BCM und KM und ordnet diese im Kontext unserer Fragestellung ein.

Dazu werden in diesem Kapitel zunächst die (1) traditionellen Muster der Sicherheitsproduktion vorgestellt, die im Unternehmenskontext eine Gradwanderung zwischen ökonomischer Entscheidungsrationalität als eingeübter Bestandteil der Führungsebene einerseits und der Herausforderung nicht-ökonomischer Problemstellungen wie

geschäftsgefährdender Gefahren oder Schadensereignissen andererseits darstellen. Darunter fallen auch die Abschnitte zur Einordnung der Schlüsselbegriffe und die konkreten Praktiken des traditionellen Risikobegriffs im Sicherheitsdiskurs innerhalb von Unternehmen. In diesem Abschnitt werden jeweils die rückblickenden Betrachtungen von Experten aus der ethnographischen Untersuchung angefügt, um die Perspektive der sich etablierten Routinen und Praktiken im analogen Zeitalter aufzuzeigen. Dem schließt sich ein Abschnitt über den (2) Verantwortungstransfer zwischen staatlicher und privater Ebene in Fragen der Sicherheitsproduktion an. Da private Unternehmen im Rahmen der kritischen Infrastruktur Aufgaben für oder im Auftrag von staatlichen Autoritäten, beziehungsweise im Interesse des Gemeinwohls ausführen (LaPorte 2007: 61), werden diese hier im Rahmen der geteilten Aufgabenwahrnehmung beleuchtet. Darauf aufbauend folgt im dritten Abschnitt dieses Kapitels eine (3) Analyse der Komplexitätssteigerung von BCM und KM im analogen Zeitalter anhand der drei Ressourcen Gebäude, Dienstleister und Mitarbeiter mit jeweils einem Fallbeispiel, welche im jeweiligen Abschnitt genauer erklärt werden.[226] Diese Fallbeispiele werden ebenfalls durch Erkenntnisse aus den Hintergrundgesprächen mit Experten ergänzt, um die Entwicklung des traditionellen Risikokontrolle aus der Retroperspektive nachzuzeichnen und abschließend den Übergang zu einem neuen Risikodiskurs im letzten Abschnitt dieses Kapitels als Folge der Erkenntnis zu den Implikationen der Digitalisierung einzuführen.

5.1. Risikokontrolle und Sicherheit nach traditionellem Muster

Wie wir im vorausgegangenen Kapitel gesehen haben, ist das Verhältnis von Unternehmen zu ihrer Außenwelt von den Bedingungen der Unsicherheit bestimmt, welche Entscheidungen unter der Prämisse unzureichender Informationen erforderlich machen. Diese Kondition ist zugleich das Fundament auf dem jede organisationinterne Risikoabwägung beruht (Baecker 1991: 119). Zwar verkehrt jedes Unternehmen auf unterschiedlicher Weise mit einer gegebenen Situation und entscheidet abhängig von verschiedenen Parametern, aber es unterliegt dennoch dem gleichen Risiko der Entscheidung für oder gegen eine Handlung (vgl. Luhmann 1991: 197). Maßgeblich zu erwähnen ist hier die zurückliegende Erfahrung der Mitglieder eines Unternehmens mit vergleichbaren Situationen. Durch die interne Erinnerungsfähigkeit des Unternehmens kann die Entscheidung gegenüber vorhandenen Erfahrungswerten abgeglichen werden und die Wahrscheinlichkeit eines erhofften oder eines ungewollten Ausgangs einer

[226] Die vierte Ressource IT- und Telekommunikationstechnologie wird aufgrund ihres Umfangs, des Schwerpunkts dieser Arbeit und veränderten Risikobegriffs separat im sechsten Kapitel adressiert.

Entscheidung zum Gegenstand der Abwägung werden lassen. Dies geschieht analog zu dem zuvor erörterten kollektiven Gedächtnisses in Unternehmen.

Wie eine Entscheidung ausfällt, hängt wesentlich von der Risikoabwägung und Bereitschaft zur Akzeptanz des residualen Risikos ab, welche auch als Risikoappetit von Individuen oder Organisationen bezeichnet wird (Elliott et. al. 2000: 50). Diese Risikoaffinität bezeichnet „the amount of risk that an organization is willing to pursue or retain'' (Torabi, Soufi und Sahebjamnia 2014: 314). Fällt der potentielle negative Ausgang einer Situation unter den Mindestwert organisationsinterner Risikoaffinität, können Maßnahmen zur Mitigation eines eventuellen Schadens getroffen werden. Diese sollen den Schaden entweder vollständig kompensieren oder zumindest auf ein tolerables Ausmaß begrenzen. Der umgekehrte Fall der Risikoaversion beschreibt eine konservative, das bedeutet risikominimierende Haltung, welche entsprechend hohe Sicherheitsdispositive artikuliert. Für beide Fälle ist eine grundlegende Entscheidung der Unternehmensführung wichtig, um die Zielvorgaben der internen Sicherheitsproduktion in Form des (traditionellen) Risikokontrollsystems zu definieren. Dazu werden in internationalen Branchenstandards für das Business Continuity Management wie der ISO 22301 die Verbindung zwischen Risikoexposition und –Kontrollmaßnahmen pointiert, auf dessen Grundlage Optionen zum Umgang mit relevanten Risiken[227] getroffen werden (BCM Academy 2016: 22).

In dieser Arbeit werden daher im Folgenden die Begriffe (1) traditionelle Risikokontrolle für geschäftsgefährdende Risiken, (2) Krisenmanagement und (3) Business Continuity Mangement verwendet, um den Umgang mit Unsicherheit innerhalb von Unternehmen im analogen Zeitalter zu beschreiben. Da diese Begriffe zudem einem Prozess der Veränderung und Anpassung während der letzten zwei Dekaden unterliefen, sollen die für unsere Fragestellung relevante Fallbeispiele die Genese und Bedeutung dieser Methoden unternehmerischer Sicherheitsproduktion verdeutlichen und in unserem Kontext einordnen. Business Continuity Management wird hier als Strategie der Risikobewertung und –Kontrolle verstanden, um den unverzüglichen Wiederanlauf von kritischen Geschäftsprozesse nach Eintreten eines unvorhergesehenen Ereignisses sicherzustellen.[228] Da das exakte Szenario der

[227] Ein BCM-relevantes Risiko bezeichnet ein Risiko welches nicht nur im Verständnis des klassischen Risikomanagements finanzielle Folgen von Unternehmensentscheidungen adressiert, sondern in der Logik des operationellem Risikomanagements spezifisch auf den Verlust einer der vier Kernressourcen des BCM blickt, welche geeignet sind die geschäftskritischen Geschäftsprozesse zu unterbrechen.

[228] Denn „[s]ince the task of 'knowing' the threat to vital systems is so hard, preventing them seems unachievable. In this context, [BCM] has become a concept that allows the security practitioner to have, or rather regain a sense of safety [or] security even though disruptions of various kinds are seen as inevitable" (Cavelty 2013: 116).

Betriebsunterbrechung allerdings nicht ex ante bekannt ist, handelt es sich bei dieser Methodologie der Risikokontrolle um eine Entscheidung unter den Bedingungen der Unsicherheit und bedarf daher aus der Perspektive des klassischen Risikoverständnisses einer flexiblen Erweiterung für ad-hoc Entscheidungen. Diese Aufgabe wird in unserem Verständnis von der organisationsinternen Funktion des Krisenmanagements übernommen. Denn Krisen umfassen Ereignisse, welche die Reputation, finanzielle Integrität oder Gesundheit und Wohlergehen der Mitarbeiter bedrohen können. Daher stützt sich Krisenmanagement als Anwendungspraktik beispielsweise im Fall einer Geschäftsunterbrechung auf die Pläne und Organisationsstrukturen des BCM, um die kritischen Geschäftsprozesse wiederherzustellen und schließt sich als reaktive, ausführende Komponente an die präventive Vorsorgeplanung des BCM an (Momani 2010: 272). Da die drei Begriffe der traditionellen Risikokontrolle, BCM und Krisenmanagement eine hohe Komplexität und Wandlungsfähigkeit aufweisen, soll eine weitere Betrachtung in den folgenden Abschnitten erfolgen. Anschließend werden ausgewählte Fallbeispielen die Entwicklung der Sicherheitsproduktion in Unternehmen in Gestalt dieser Anwendungspraktiken nachzeichnen und auch die Gespräche über die zurückliegende Entwicklung dieser Praktiken aus der ethnographischen Untersuchung einbinden.

5.1.1. Traditionellen Risikokontrollsysteme in Unternehmen

Wir verwenden den Begriff der traditionellen Risikokontrolle, um die Rationalität von Unternehmen im Umgang mit sicherheitsrelevanten Problemen im analogen Zeitalter zu beschreiben. Darunter ist hier eine Methodik zu verstehen, die einem ökonomisch-definierten Entscheidungsprinzip folgt, um nicht-ökonomische Herausforderungen zu lösen. Wie die nachfolgenden Beispiele zeigen werden, konnte sich diese Form der unternehmerischen Vorsorgeplanung durch Weiterentwicklung und Reflexion an die Krisen und Problemstellungen anpassen. Die Digitalisierung und weitreichende Vernetzung von Systemen stellte allerdings durch ihre Komplexität und systemische Problemstellung eine neue Herausforderung dar, welche eine grundlegende Veränderung der Risikokontrolle und ihrer Methodik erforderlich machte (Kaufmann und Blum 2011: 235). Die Weiterentwicklung der systemischen, prozessorientierten Risikokontrolle werden wir im nächsten Kapitel betrachten und uns in diesem Kapitel ganz auf die traditionellen Muster konzentrieren, um die Grundlagen der weiteren Untersuchung zu schaffen.

Ausgehend von den Problemfeldern der analogen Zeit, stellten sich die Herausforderungen an Unternehmen vorrangig in der Übersetzung der ökonomischen Entscheidungsrationalität und Profitabilitätsorientierung auf nicht-ökonomische Handlungsfelder der Sicherheitsproduktion.

Wie zuvor eingeleitet wurde, bezieht sich der traditionelle Risikobegriff auf Objekte, deren Wert oder Verfügbarkeit durch ein Schadensereignis negativ beeinflusst werden kann. Dessen Eintreten hängt wiederum von einer auf historischen Daten basierenden Wahrscheinlichkeitskalkulation ab (Braes und Brooks 2010: 17). Im klassisch-ökonomischen Verständnis steht die Führungsebene in Unternehmen den Investitionen in Schutzmaßnahmen allerdings skeptisch gegenüber (Carr 2016: 56), da die Anwendungspraktiken des traditionellen Risikokontrolle wie BCM oder Krisenmanagement vorrangig als Kostenfaktoren wahrgenommen werden (Christensen und Petersen 2017: 1443).

Eine Beobachtung aus der ethnographischen Untersuchung zeigte, dass sich das Zugeständnis der Führungsebene zur Investition in Vorsorgeplanung nach Schadensereignissen wie dem Reaktorunglück von Fukushima 2011 oder der Anschläge von Paris 2015 in ein Momentum für die Weiterentwicklung von BCM und Krisenmanagement übersetzte.[229] Diese Beziehung zwischen exogenen Ereignissen und unternehmensinterner Planung werden wir in den Fallbeispielen anhand der jeweiligen Situation beleuchten und reflektieren. Für diese Einordnung des traditionellen Begriffs der Risikokontrolle soll zunächst festgehalten werden, dass die Dynamik von Krisenereignissen und Weiterentwicklung von Maßnahmen und Funktionen in Unternehmen zu einer schrittweisen Etablierung der Sicherheitsproduktion als Bestandteil der unternehmerischen Tätigkeit und Organisation führte. Allerdings mit dem Unterschied zur heutigen Perspektive, dass die Annahme von Risiken in der traditionellen Risikokontrolle auf der „Vorstellung der Prognostizierbarkeit und statistisch-probabilistischen Kalkulierbarkeit von Risiken, gepaart mit dem Versprechen ihrer wissenschaftlich technischen Beherrschbarkeit“ beruhte (Blum et. al. 2016: 156).

Die traditionelle Risikokontrolle im analogen Zeitalter betrachtete bereits technische Risiken und verstand die Rolle der Informationstechnologie als Vorbedingung der Geschäftstätigkeit, da Datenbanken, virtuelle Applikationen oder elektronische Kommunikation die notwendigen Anschlussoperationen in der Organisation ermöglichen. Daher umfasste die traditionelle

[229] Ein langjähriges Mitglied der Organisation berichtete in einem Gespräch während der Corona-Pandemie im Herbst 2020 von den prägenden Krisen, welche die Entwicklung der Risikokontrolle in Form von BCM und Krisenmanagement vorangetrieben hätten. Dazu zählte die Expertin die Vogelgrippe, das Reaktorunglück von Fukushima und die Anschläge von Paris (bezogen auf das Incident Management) auf, allerdings habe die Corona-Pandemie schließlich den signifikantesten Beitrag zur Weiterentwicklung verursacht. Ein Gespräch mit einem BCM-Verantwortlichen aus einem anderem DAX-30 Konzern betonte 2017, dass im Fall seines Unternehmens hingegen der Ausbruch des isländischen Vulkans Eyjafjallajökull zu enormen Anspannungen in der Prozesskontinuität geführt habe, da die normalerweise über Flugverbindungen stattfindende Lieferkette aufgrund der Aschewolken über dem europäischen Luftraum unterbrochen wurde. Dieses Ereignis habe das Unternehmen zur umfassenden Vorsorgeplanung für die Prozess- und Lieferkettenkontinuität durch BCM veranlasst (Hintergrundgespräch 29.07.2017).

Risikokontrolle nicht nur die Domänen oder Anwendungspraktiken von BCM und Krisenmanagement, sondern auch andere spezialisierte Funktionen wie IT-Sicherheit, Datenschutz oder Compliance (Braes und Brooks 2010: 16). Das Zusammenwirken der unterschiedlichen Funktionen ist allerdings nicht immer als einfach oder effektiv einzuordnen. Persönliche Ziele und Ansichten von Entscheidungsträgern, konzeptionelle Unterschiede oder Schwerpunktsetzungen können die Entwicklung eines integrierten Risikokontrollansatzes erschweren (Ward 2003: 9).

Ein Beispiel aus der ethnographischen Beobachtung aus dem Frühjahr 2015 soll dies verdeutlichen.[230] Im Zuge einer bereichsübergreifenden Initiative zur Harmonisierung der Bewertung von IT- und operationellen Risiken[231] wurde während den gemeinsamen Workshops zwischen den Vertretern des BCM-Fachbereichs und der IT-Sicherheit deutlich, dass zwei verschiedene Vorstellungen hinsichtlich der Risikobewertung und Dokumentations-notwendigkeit innerhalb des gleichen Unternehmens vorherrschten. Es konnte keine Einigkeit gefunden werden, wie die gemeinsame Schnittenge von IT- und operationellen Risiken mit Blick auf die Kontinuitätssicherung von kritischen Geschäftsprozessen abgedeckt werden könnte. Die traditionelle, objektbezogene Sichtweise des IT-Risikomanagements kollidierte in dieser Initiative mit der beginnenden prozess-orientierten Perspektive des BCM auf die systemischen Verknüpfungen zwischen IT und Geschäftsprozessen. Im Ergebnis zeigte sich durch die Beobachtung nicht nur das unterschiedliche Verständnis der beiden Unternehmensbereiche auf den gleichen Anwendungsraum der Sicherheitsproduktion, sondern auch das zeitgleiche Bestehen von traditioneller, objektbezogener Risikokontrolle im IT-Bereich und beginnender systemsicher Sichtweise hinsichtlich der Beschaffenheit von Risikokontrolle auf der anderen Seite. Vor diesem Hintergrund ist es interessant sich die Schnittmenge der unternehmensinternen Sicherheitsproduktion zwischen Prozess- und Kommunikationskontinuität einerseits und klassischem Risikomanagement als ökonomisch-besetzter Begriff der Risikosteuerung anzusehen.

[230] Die Gespräche im Rahmen dieses Projekts wurden vom Autor dieser Arbeit als Mitglied des Projekts beobachtet. Neben den kulturellen Unterschieden in den Fachfunktionen hinsichtlich den Prinzipien der Projektsteuerung wurden mit der Zeit deutlich, dass unterschiedliche Schwerpunkte die Agenda jeder Seite bestimmte. Im Fall der IT-Sicherheitsfunktion war der Fokus auf die IT-Kontrollen gerichtet und involvierte die jeweiligen Anwendungen durch die Geschäftsprozesse nur im geringen Umfang während die BCM Funktion die gegensätzliche Position einnahm und aus Sicht der gesamten Prozesslandschaft argumentierte.

[231] Die Unterscheidung zwischen beiden Bereichen wurde anhand der funktionalen Steuerungseinheit abgeleitet. Operationelle Risiken sind all jene Schadenskategorien, welche den Betrieb betreffen und nicht IT-Applikationen oder -Infrastruktur betreffen

5.1.2. Schnittmenge zwischen Betriebskontinuität und Risikomanagement

Das Ziel der Risikokontrolle ist es die kritischen Geschäftsprozesse und Kommunikation vor Unterbrechungen zu schützen, beziehungsweise schnellstmöglich wiederherzustellen. Dazu werden wir im nachfolgenden Abschnitt die Methodik von BCM und Krisenmanagement genauer betrachten. An dieser Stelle gilt das Interesse zunächst der Einordnung von BCM und Krisenmanagement in den Kosmos der Unternehmensfunktionen, deren jeweilige Kompetenzzuschreibung aus den Notwendigkeiten der klassischen ökonomischen Rationalität abgeleitet werden kann. Dazu werden wir den Blick auf das Zusammenwirken von Unternehmensfunktionen wenden und die Schnittmenge, in der sich die durch die traditionelle Risikokontrolle eingeführten Anwendungspraktiken Business Continuity Management und Krisenmanagement ansiedeln. Dazu werden wir uns zunächst die Unternehmensfunktionen ansehen welche dieses Zusammenspiel prägen, einerseits die (1) Betriebsorganisation, welche Geschäftsprozesse im Unternehmen steuert und das (2) Risikomanagement.

Wie wir im vierten Kapitel gesehen haben, bedürfen Organisationen ständiger Anschlussoperationen und Kommunikation über getroffene Entscheidungen. Unternehmen erschaffen diese Operationen in ihrem eigenen Kreislauf von Prozessen und in ihrer Interaktion mit der Außenwelt. Im Fall von Banken zeigte beispielsweise Dirk Baecker, dass Zahlungen die "elementare Kommunikationsform" in der Wirtschaft darstellen und dadurch die Bestimmungen von Preisen und Leistungen getroffen werden kann (Baecker 1991: 42). Ob produzierendes Gewerbe, Technologiekonzern oder Finanzwirtschaft, jede Organisation folgt im Verständnis der Autopoiesis der Aufrechterhaltung von Anschlussoperationen und Kommunikation. Mit Blick auf die Produktion und Steigerung von Effizienz wurden zahleiche Initiativen und Ansätze entwickelt und in Unternehmen eingeführt, deren Ziel im klassische-ökonomischen Verständnis die Produktionssteigerung bei gleichzeitig möglichst hoher Kostenreduktion umfasst. Darunter fallen auch die Sicherstellung von Rohstoffen oder vorgelagerten Produktionsschritten und Abtransport beziehungsweise Fortsetzung durch die nachgelagerten Funktionen und Arbeitsschritten (Jüttner 2005: 121). Diese, auf Effizienzstandards fokussierte Aufgabe, fällt der (1) Betriebsorganisation (Operations) zu. Darunter verstehen wir hier alle Aktivitäten des Produktionsmanagement oder Wertschöpfungskettensteuerung, welche die Bereitstellung von Anschlussoperationen unter normalen Bedingungen organisieren.

Für den Fall von exogenen Beeinträchtigungen, beispielsweise durch den Ausfall oder die erhebliche Verzögerung in der Leiferung von Rohstoffen durch politische Instabilität in einem

Land, übernimmt die Funktion des (2) Risikomanagements die Steuerung von Risiken in Form der ökonomischen Risikovorsorge (Power et. al. 2009: 304). Hier sind zwei Begriffe zu unterscheiden: Unter (a) *Risikomanagement* verstehen wir hier die Funktion in einem Unternehmen, welche Risiken für das Unternehmen identifiziert und bewertet. Eine mögliche Kontrollmaßnahme für (ökonomische) Risiken kann die Risikovorsorge durch Rückstellung von Risikokapital sein (Pfeifer 2006: 11). Diese finanziellen Rücklagen sollen im Fall eines monetär zu beziffernden Schadensereignisses wie beispielsweise Vertragsstrafen oder Produktionsausfällen das einkalkulierte Risiko ausgleichen. Die Möglichkeiten dieser ökonomischen Risikorationalität enden jedoch mit Blick auf die Kontinuität von Operationen und Kommunikation im Sinne der Sicherstellung der Organisationsexistenz.[232] Operationelle Ausfälle oder Reputationsschäden können unter Umständen nicht mehr durch Kapitalrückstellungen *versicherbar* sein (Krüger 2016: 8). Deshalb ist an der Schnittmenge zwischen Betriebsorganisation und Risikomanagement eine Funktion zur (b) *Risikokontrolle* für geschäftsgefährdende, nicht-ökonomische Risiken in Gestalt des BCM und Krisenmanagement entstanden (Bonafede, Cerchiello und Giudici 2007: 80).

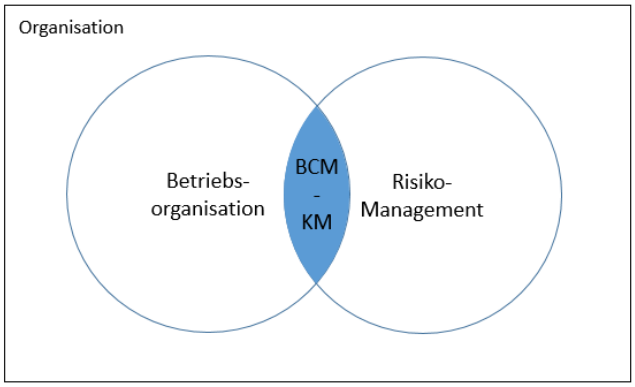

Abb. 5.1. Aus der Schnittmenge von Betriebsorganisation und Risikomanagement entstehen BCM und KM als Anwendungspraktiken der traditionellen Risikokontrolle. Eigene Darstellung.

Aus dem Risiko einer solchen potentiellen Unterbrechungen kritischer Geschäftsprozesse, welche weder durch rein reaktive Maßnahmen (vgl. ad-hoc Produktions- oder Lieferkettenanpassungen), noch durch Versicherungen[233] im befriedigenden Umfang

[232] Eine Anpassung der Arbeitsteilung wurde notwendig, da das funktional und methodisch separierte Risikomanagement maßgeblich finanzielle Risiken betrachtete, welche den Unternehmensgewinn gefährden konnten und plante die Risikomitigation primär mit Hilfe von Kapitalrücklagen zu steuern (vgl. Best 2010: 37). Für die Fortführung der Prozesse waren aber andere, operationelle Mitigationsoptionen notwendig.

[233] Die Versicherung bietet lediglich finanziellen Ausgleich für einen erlittenen Schaden, jedoch keinen elementaren Schutz vor der Gefahr selbst. Auch bleibt das Risiko der Versicherung selbst zu beachten, sprich den Abschluss einer Versicherung ohne tatsächlich eingetretenen Schadensfall, nicht versicherter Schadensereignisse oder ungünstige Prämienkonditionen. „Die Einrichtung von Versicherungen produziert also nicht mehr Sicherheit, sondern neue Risiken“ (Luhmann 1996: 273). In unserem Fall gilt dies insbesondere hinsichtlich dem

kontrolliert werden können (Schintler et. al. 2007: 292), entstand die Grundlage für BCM und Krisenmanagement als Anwendungspraktiken der traditionellen Risikokontrolle (Braubach 2011: 35). Doch welche Schäden beziehungsweise Konsequenzen sind aus einem ökonomischen Verständnis heraus zu erwarten? Die möglichen geschäftsgefährdenden Konsequenzen einer Unterbrechung können nach Außen in einen Reputationsschaden resultieren, wenn Dienstleistungen und Waren nicht mehr für Kunden zur Verfügung gestellt werden können[234] oder durch den finanziellen Schaden einer Geschäftsunterbrechung, wie im Falle einer Vertragsstrafe.[235] Diese Implikationen lassen sich in ökonomische Begriffe und Dimensionen übersetzen und der Entscheidungsrationalität der Führungsebene von Unternehmen darlegen. Wie während der ethnographischen Untersuchung zu beobachten war, lag ein Unterschied in der ökonomischen Rationalität von Unternehmen als profitorientierte Organisationen einerseits und dem Verständnis nicht-ökonomischer Implikationen für das Unternehmen und seiner Folgen vor. So stelle in einem vertraulichen Gespräch ein Manager die Sinnfrage hinsichtlich der oben dargestellten Risikokontrolle. Warum solle das Unternehmen in Vorsorgeplanung für Eventualitäten investieren, so der sinngemäße Tenor, wenn das dafür nötige Geld für den Ausbau der Produktivitätssteuerung verwendet werden könne. Ergänzend wurde von jenem Manager angefügt, dass letzteres immerhin in das Unternehmensziel aufgrund der zu erwartenden Profitsteigerung einzahlen würde.[236]

Diese Momentbetrachtung zeigt das Missverständnis zwischen ökonomischer Rationalität und dem Sicherheitsdispositiv, welches sich über die Jahre immer stärker entwickelte. Die Übertragung von Pflichten seitens der staatlichen Autoritäten und Herausentwicklung von Industriestandards hinsichtlich der Risikokontrolle von Geschäftsunterbrechungen werden in einem speziellen Abschnitt in diesem Kapitel detailliert betrachtet werden. Für den Beginn der sich herausbildenden, traditionellen Risikokontrolle durch BCM und Krisenmanagement kann jedoch festgehalten werden, dass der Interessenskonflikt zwischen abstrakter Risikoartikulation

Reputationsschaden und finanzieller Nachteile (Konventionalstrafen, Verluste von Marktanteilen) durch operationelle Rückstände in Folge eines Schadensereignis.

[234] Ein Beispiel aus der jüngeren Vergangenheit verdeutlicht dies: British Airways musste in Folge eines Ausfalls ihres Reisebuchungssystems im Frühjahr 2018 über zwei Tage hinweg 726 Flüge streichen. Durch diese Unterbrechung der Kerngeschäftsprozesse waren mehr als 75.000 Passagiere betroffen und es entstand ein geschätzter Schaden von mehr als 100 Mio. Euro. Vgl.: The Telegraph (2018): British Airways: Reports of delays and cancellations at Heathrow as airline reports 'systems issue'. Zuletzt aufgerufen online am 03.12.2018 unter: https://www.telegraph.co.uk/news/2018/07/18/british-airways-reports-delays-cancellations-heathrow-airline/

[235] Der finanzielle Schaden kann durch Umsatzausfall entstehen oder durch hohe Konventionalstrafen die Unternehmenssolvenz gefährden, wenn vertraglichen Verpflichtungen nicht nachgekommen werden kann (Cerullo und Cerullo 2004: 75).

[236] Das Gespräch fand im Juni 2016 während eines Projekts zur Neudefinition der finanziellen Schadenskategorien für kritische Prozesse statt. Die Ausgangsfrage thematisierte die möglichen Kosten zur Vorsorgeplanung von Prozessen, welche angesichts des Ausfallsrisikos vom Prozessverantwortlichen als zu hoch angesehen wurden.

und Investition in Vorsorgeplanung die Entwicklung der Funktionen innerhalb des traditionellen Risikomanagements prägte. Dazu war es notwendig die präventive Vorsorgeplanung in den ökonomischen Begriffskontext einzubetten und unter Einbeziehung der Methodik der Risikoidentifikation und -Kontrolle[237] die Relevanz von Geschäftsunterbrechungen für das Unternehmen und seine Fortexistenz zu begründen. Die Übersetzung der als abstrakt wahrgenommenen Risiken eines Operations- und Kommunikationsabbruchs in eine Risikomatrix sollte diese vermittelnde Aufgabe übernehmen, um die Akzeptanz innerhalb der ökonomischen Entscheidungsrationalität zu erhöhen.

5.1.3. Risikomatrix

Im Rahmen der traditionellen Risikokontrolle können nicht-ökonomische Problemstellungen wie beispielsweise eine Anordnung von möglichen geschäftsgefährdenden Risiken anhand ihrer Wahrscheinlichkeit und Schadenswirkung in einer Risikomatrix übersetzt werden. Diese Matrix entspringt dem traditionellen Risikoverständnis und sieht Risiken als kalkulierbare Objekte an. Dazu werden Risikoobjekte in einer Matrix zumeist in vier Kategorien eingeteilt (Braes und Brooks 2010: 16f.). Erstens ist die Gruppe aus Risiken mit einem hohem Schadenswert und sicherem Eintreten zu nennen, wie beispielsweise regional spezifische Umweltfaktoren oder Cyberkriminalität. Für diese Gruppe sind präventive und reaktive Maßnahmen zu treffen, wie zum Beispiel bauliche Maßnahmen in Form von gefederten Bauelementen, Feuerlöschsystemen und Brandschutzabschnitten zur Gefahrenabwehr beziehungsweise Schadensminimierung. Falls diese Maßnahmen versagen, können Reaktionsplänen die zeitnahe Verlagerung der Produktion an einen Ausweichstandort ermöglichen und die negativen Auswirkungen auf die Geschäftsprozesse reduzieren. Diese Risikogruppe beruft sich in der Regel auf eine empirische Erfahrungsgrundlage und verbindet eine hohe Risikoperzeption sowie Investitionsbereitschaft in Schutzmaßnahmen seitens der Unternehmen (Holmgren 2007: 37).

Die zweite Gruppe umfasst eine Kombination aus sehr geringem Schaden und sehr niedriger Eintrittswahrscheinlichkeit. Ein Risiko das einmal in tausend Jahren auftritt und kaum nennenswerten Schaden zu verursachen droht, scheint daher vernachlässigbar. In diesem Fall wird das identifizierte, wohlgleich unbedenkliche Risiko akzeptiert. Diese Entscheidung wird

[237] Denn diese Risiken sind nicht mit den Mitteln und Fähigkeiten der regulären Funktionen in einem Unternehmen zu bewältigen, sondern benötigen eine eigene, leistungsfähigere Notfallorganisation. Diese Entität innerhalb des organisatorischen Gebildes übernimmt die Aufgaben der Schnittmenge aus klassischer Resilienz und Risikomanagement. Aus dieser Überschneidung zweier Aufgabenfelder der Risikomitigation geht BCM als Disziplin hervor und bedient sich Methoden beider Quellen.

von einer Autorität, etwa einer Person mit Handlungsbefugnis oder etablierten Institution getroffen und kommuniziert. Damit wird die Irrelevanz dieses Risikos für mögliche Mitigationsoptionen dokumentiert. Anders verhält es sich mit der dritten Gruppe von hoch-wahrscheinlichen Ereignissen mit niedrigen Schadenserwartungen. Denn aufgrund der Frequenz von Ereignissen, kann ein vergleichbarer Schaden über eine längere Zeitspanne entstehen, beispielsweise durch kurzfristige Stromausfälle oder begrenzte IT-Probleme ((McGuire 2015: 47). Diese Gruppe ist unter den Aspekten des Störungsmanagements („Incident Management") zu betrachten[238], da keine Geschäftsunterbrechung über ein kritisches Zeitintervall besteht.[239]

Zuletzt bleibt die vierte Gruppe, welche einen hohen Schaden bei geringer Eintrittswahrscheinlichkeit inkludiert. Diese Gruppe ist in der BCM-Literatur umstritten, denn für Ereignisse mit niedriger Probabilität wird selten in Form von aufwendigen Schutzmaßnahmen vorgesorgt und zugleich liegen unzureichende Erfahrungswerte vor, was erheblichen Einfluss auf die Plausibilitätseinschätzung des Schadenszenarios haben kann (Holmgren 2007; Lam 2002; Sahebjamnia, Torabi und Mansouri 2015;). In diese Gruppe fallen Ereignisse wie Naturkatastrophen, Industrieunfälle oder durch Menschen verursachte Schäden, wie beispielsweise durch koordinierte Hackerangriffe[240] oder Terrorismus (Schintler et. al. 2007: 291). Ereignisse aus dieser Gruppe, welche aus seltenen Begebenheiten mit hoher Auswirkung besteht, haben am häufigsten Anlass geboten, BCM in Unternehmen zu etablieren beziehungsweise weiterzuentwickeln. Diese seltenen, aber gefährlichen Ereignisse sind eins starker Treiber für Investitionen in BCM und Krisenmanagement, da sie die Existenz des Unternehmens durch unvorhergesehene Ereignisse ernsthaft gefährden können (vgl. Braes und Brooks 2010: 16) und wie in der ethnographischen Studie zu beobachten war auch durch solche Ereignisse die ein Unternehmen direkt oder indirekt (beispielsweise Geschäftspartner oder Lieferanten) tangierten.[241] Ausgewählte Beispiele aus dieser Beobachtung werden weiter unten als Fallbeispiele vertieft werden.

---

[238] Das Incident Management umfasst zum einen den Umgang mit geringfügigen bis großen Störungen des Betriebs und zudem eine initiale Prüfung eines Zwischenfalls auf sein Potential hin, eine Krise oder eine Geschäftsunterbrechung zu bewirken. Für alle Ereignisse die unterhalb der definierten Grenzwerte für Krisen oder Geschäftsunterbrechungen bleiben (siehe unten), ist die jeweilige Incident Management Funktion (Fachfunktion oder dezidierte Koordinationsstelle, beispielsweise IT Support) zuständig.

[239] Wie später gezeigt werden wird, definiert sich die kritische Geschäftsunterbrechung durch eine dezidierte Dauer der Unterbrechung sowie einem signifikanten negativen Effekt, beispielsweise einem Schaden von mehr als 15 Prozent des Umsatzes innerhalb von einer Arbeitswoche.

[240] Unter koordinierten Hackerangriffen sind sorgfältig vorbereitete und komplexe Versuche gemeint die IT-Netzwerke eines Unternehmens mittels leistungsfähiger Malware zu infiltrieren (Cavelty (2013: 112).

[241] Hier sei auf das zuvor genannte Beispiel der Unterbrechung der Lieferkette über den europäischen Luftraum verwiesen, welches die Bereitschaft des betroffenen Unternehmens in Investitionen nachhaltig erhöhte.

Mithilfe der Risikomatrix kann der potentielle Schaden in ökonomische Begriffe übersetzt und der Zugang für Entscheidungsträger erleichtert werden. Die negativen Implikationen von geschäftsgefährdenden Risiken wurden beispielsweise als indirekter Schaden artikuliert, wenn Geschäftsprozesse unterbrochen werden. Finanzielle Verluste, die auf einer solchen Unterbrechung von Operationen oder Kommunikation in der Organisation beruhen sind zumeist schwer quantitativ zu beziffern, wenn Referenzzahlen im traditionellen Kontext von Schaden und Eintrittswahrscheinlichkeit fehlen. Das klassische Risiko eines Schadenfalls, wenn zum Beispiel eine Produktionsstätte durch Feuer zerstört wird, bedeutet für den Eigentümer eine quantifizierbare Summe, zusammengesetzt aus Gebäudewert und Neuanschaffungspreis der dort untergebrachten Güter. Der Ausfall der Produktion und die daraus resultierenden Konsequenzen sind in diese Rechnung jedoch nicht inkludiert.

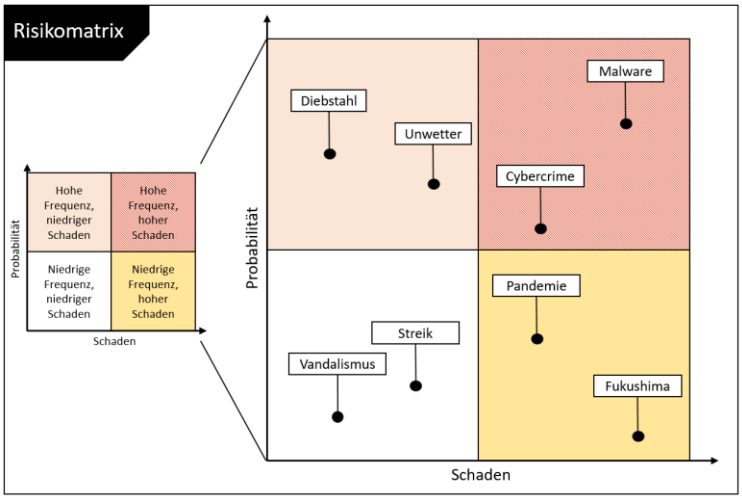

Abb. 5.2. BCM Risikomatrix. Eigene Darstellung.

Auch exogene Ereignisse wie die Anschläge des 11. September 2001 (Bram, Orr, und Rapaport 2002: 5), Hurrikane Katrina im August 2005 (Tierney und Bruneau 2007: 14) oder das Reaktorunglück von Fukushima am 11. März 2011 (Ho et. al. 2013: 774) verdeutlichten die Konsequenzen für die verantwortlichen und betroffenen Organisationen. So zeigte sich, dass eine unzureichende Vorbereitung auf die finanziellen, operationellen und reputierlichen Folgen negative Implikationen haben können, welche den quantifizierbaren Wert des Schadens übersteigen. Dadurch konnte eine gewisse Akzeptanz[242] in Unternehmen etabliert werden, dass es notwendig sei, eine verhältnismäßige Risikoidentifikation und -Kontrolle einzuführen[243],

[242] Die Akzeptanz von Funktionen zur Risikokontrolle kann anhand von bewilligten Budgets und Stellen beschrieben werden, welche in Folge der ethnographischen Beobachtung über den Zeitraum von 2017 bis 2022 verfolgt werden konnte.

[243] Eine angemessene Kompensation subsumiert alle Kosten die zur Wiederherstellung des Status Quo vor dem Ereignis anfallen, aber auch die Kosten des Prozessausfalls und gegebenenfalls des Wertverlusts an den Finanzmärkten und den Reputationsschadens. Im Fall einer Vermengung von Ereignissen wie im März 2011 im

durch deren Bewertung die Aufwände für Schutzmaßnahmen den möglichen quantitativen und qualitativen Aspekten des Ereignisses gerecht werden können (Norio 2011 et. al. 36).

Zur Akzeptanz der traditionellen Risikokontrolle trägt ebenfalls die Differenzierung zwischen verschiedenen Graden der Destruktivität eines Ereignisses bei. Die Beschreibung eines milde verlaufenden Szenarios („best case“) und einer fatalen Zuspitzung der Ereignisse unter widrigen Umständen („worst case“) können helfen die Facetten und Abstufungen des Risikos begreiflich zu machen (Church und Scaparra 2007: 239). Beispielsweise kann der Ausfall eines Zulieferers als Risiko betrachtet und eine Unterscheidung getroffen werden, ob das den Ausfall auslösende Ereignis nur eine räumlich begrenzte Wirkung aufweist oder einen großen Einflussbereich hat. Im ersten Fall kann der Schaden durch die lokale Begrenzung eingedämmt werden und eventuelle Alternativen für den Zulieferer unbeschädigt bleiben. Sollten jedoch alle Zulieferer der Region von dem Vorfall betroffen sein, werden die Anforderungen an eine erfolgreiche Risikokontrolle und Anwendung der Praktiken von BCM oder Krisenmanagement stark erhöht (Smith und Wenger 2007: 241).

Die Logik der traditionellen Risikokontrolle und ihrer Annahme der Kalkulierbarkeit von Risikoobjekten kann hier beobachtet werden. Aufbauend auf der Prämisse eines abgrenzbaren, objektbezogenen Risikoverständnisses, ermöglichen es Szenarien, die Konturen und Tiefen eines Krisenbildes ex ante zu erfassen und eine Planungsgrundlage für die Entscheidung des Unternehmens vorzubereiten. Dies lässt sich am Besten in der Logik des BCM unter den Anführungszeichen des traditionellen Risikokontrollverständnisses nachzeichnen, welches die einzelnen Objekte und Ressourcen in den Fokus nahm. Im Folgenden wollen wir uns daher die BCM-Methodik und die notwendigen Schritte zu ihrer Implementierung ansehen, um die inhärente Logik der Entscheidungsfindung im analogen Zeitalter mit Blick auf den Beginn der unternehmerischen Vorsorge zur Prozesskontinuität zu verstehen.

5.1.4. Business Continuity Management und Krisenmanagement

Business Continuity Management (BCM) und Krisenmanagement (KM) sind zwei Anwendungspraktiken innerhalb der traditionellen Risikokontrollsysteme in Unternehmen, durch welche die Sicherheitsproduktion in die Praxis umgesetzt wird. Wie wir im vorausgehenden Abschnitt gesehen haben, werden beide Domänen in dieser Arbeit als

japanischen Fukushima wird dies deutlich: “The world’s largest reinsurers, Munich Re and Swiss Re were speculated to suffer total reinsurance losses of 10 billion U.S. dollars (…) even after the losses absorbed by primary insurers and grants from the Japanese government” (Norio et. al. 2011: 36). Die Verknüpfung des Schadenspotentials aus Erdbeben, Tsunami, Reaktorunglück und Geschäftsunterbrechungen als Folge der Ereignisse übertrafen die zuvor antizipierten Vorstellungen eines möglichen Schadens (Perrow 2011: 48).

Kontrollmaßnahmen des Unternehmens verstanden, um auf exogene und vorrangig nicht-ökonomische Probleme zu reagieren. Beide Domänen interagieren in der Schnittstelle zwischen den im klassischen ökonomischen Kontext etablierten Linienfunktonen[244] wie Betriebsorganisation und Risikomanagement, um die Unterbrechung der Prozesse und Kommunikation im Fall von außerordentlichen Ereignissen zu verhindern oder minimieren zu können. Diese Unterscheidung ist für unsere Fragestellung dahingehend wichtig, als dass BCM und Krisenmanagement als Methodik konzeptionell für jene Ereignisse vorgesehen sind, welche die Linienfunktionen oder normale Ablauforganisation[245] nicht, beziehungsweise nicht mehr bewältigen können. Diese Unterscheidung wird in der Literatur allerdings kaum berücksichtigt (vgl. Braubach 2011) und entstammt der teilnehmenden Beobachtung im Rahmen dieser Arbeit, wie im Folgenden erklärt werden wird.

Im Normalbetrieb unterliegen den jeweiligen Linienfunktionen die Aufgaben und Verantwortung zur Sicherstellung des Betriebs und der Schaffung von Anschlussoperationen im organisationstheoretischen Sinn. Neben den routinierten Aufgaben, werden auch unvorhergesehene Ereignisse mit hoher Frequenz und niedrigem Schaden, analog zur Risikomatrix durch die Ablauforganisation geregelt (Rose 2004: 308). BCM und Krisenmanagement werden hingegen im Fall von Ereignissen aktiv, deren potentieller Schaden für die Prozesskontinuität die Fähigkeiten der Linienfunktion übersteigt oder die Existenzgrundlage des Unternehmens bedroht ist. Daher liegen BCM und Krisenmanagement an der Schnittstelle zwischen Betriebsorganisation und Risikomanagement und haben zum Ziel, die vitalen Geschäftsprozesse des Unternehmens im Notbetrieb auf einem zuvor definierten Mindestniveau des Prozessoutputs fortzuführen (Braes und Brooks 2010: 16).[246]

---

[244] Eine Linienfunktion wird hier als Begriff für alle etablierten Funktionen eines Unternehmens analog zum jeweiligen Betriebsmodell mit standardisierten Aufgabenfeldern und Abteilungen verstanden. Linienfunktionen entsprechen hier zumeist dem Modell der ökonomischen Rationalität und Beitrags zur Wertschöpfung.

[245] Die Ablauforganisation entspricht der operativen Führung von Prozesse im Normalbetrieb. Als solche decken sich die Kompetenzfelder häufig mit denen der Linienfunktionen. Im Rahmen der teilnehmenden Beobachtung konnte an Beispielen analysiert werden, wie die Linienfunktion diese Kompetenzen interpretieren kann. Während eines Projekts im Mai 2019 sollten die Prozesse eines Geschäftsbereichs mit Linienfunktionen in Deutschland und Frankreich auf ihre Kritikalität und mögliche Wiederherstellungsstrategien hin untersucht werden. Die Führungsebene der Linienfunktionen zeigte sich in beiden Fällen skeptisch gegenüber der BCM-Methodik, da sie in beiden Fällen überzeugt waren, Unterbrechungen mit den eigenen Ressourcen regeln zu können. Erst der Verweis auf große Schadensereignisse, beispielsweise der Nichtverfügbarkeit eines zentralen Rechenzentrums konnte die Linienfunktion zur Kooperation überzeugen, da das potentielle Schadensausmaß nicht mehr durch die Ablauforganisation zu bewältigen wäre.

[246] Diese ursprüngliche Zielsetzung vernachlässigt allerdings die anderen Schutzwerte des Unternehmens und fokussiert sich ausschließlich auf die Fortführung kritischer Prozesse. Diesen Mangel werden wir im nächsten Kapitel thematisieren und eine Lösung in Form eines integrierten Risikokontrollsystems im siebten Kapitel vorstellen. An dieser Stelle wird der Schwerpunkt auf BCM gelegt, um die Bedeutung der Außerachtlassung der anderen Schutzwerte im Verlauf der Untersuchung und Fallbeispiele herauszustellen.

Business Continuity Management definiert dazu die kritischen Geschäftsprozesse eines Unternehmens und arbeitet Strategien und Pläne aus, diese im Fall von Unterbrechungen schnellstmöglich im Notbetrieb wieder fortsetzen zu können. Hier kommen präventive und reaktive Aspekte zum Tragen. Ersteres, indem geschäftsgefährdende Risiken identifiziert und durch Pläne zur Wiederherstellung versucht wird, die Sicherstellung der Prozess- und Kommunikationskontinuität bestmöglich umzusetzen (Torabi, Soufi und Sahebjamnia 2014: 309). Zweitens koordiniert zum Zeitpunkt einer Geschäftsunterbrechung das Krisenmanagement die Wiederherstellung von Geschäftsprozessen bis zu dem Punkt, an dem die Prozessperformanz den definierten Mindeststandard erreicht hat. Die mittelfristige Rückführung zum vorherigen Status Quo fällt unter die BCM Überwachung, welche mit dem Erreichen des Normalzustandes abgeschlossen ist (Pike, Dawley und Tomaney 2010: 61), wie es dem Schaubild unten zu entnehmen ist.

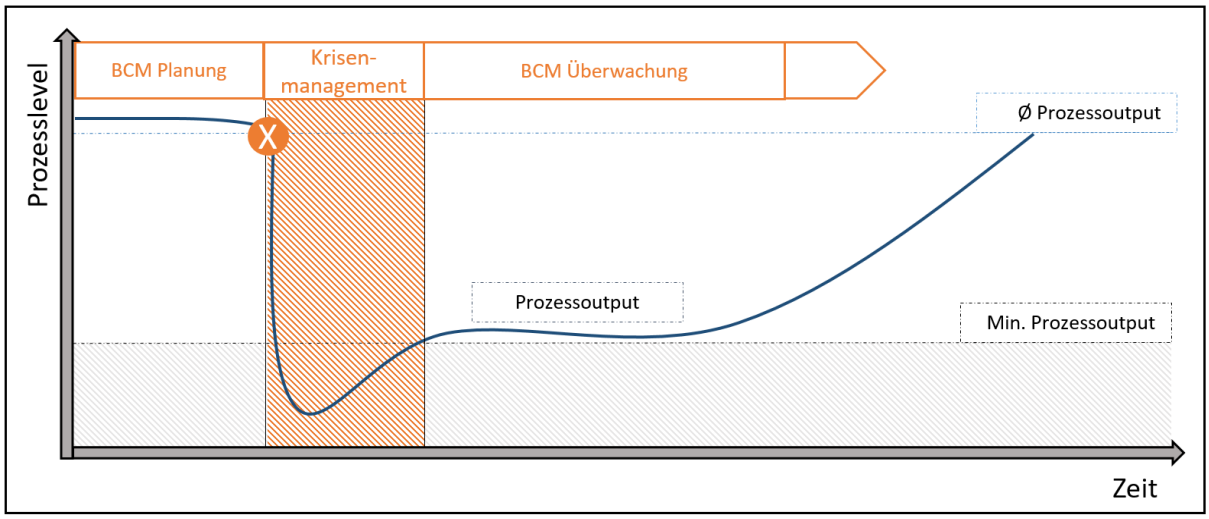

Abb. 5.3. Zusammenspiel zwischen Krisenmanagement und BCM Planung als Teil des ganzheitlichen Business Continuity Managements. Eigene Darstellung.

Somit stellt sich die Frage wie Unternehmen durch BCM und Krisenmanagement Geschäftsunterbrechungen konkret bewältigen können? Dazu soll an dieser Stelle noch einmal hervorgehoben werden, dass es sich bei dieser Darstellung um die Risikokontrolle zur Sicherheitsproduktion in Unternehmen nach traditionellem Risikoverständnis handelt. Dies wird im Folgenden im Detail erklärt und auch anhand des objektbezogenen Risikobegriffs im analogen Zeitalter in Form der Fokussierung auf Ressourcen innerhalb der BCM-Methodik verdeutlicht werden. Mit Blick auf die Genese von BCM reichen die Ursprünge zurück zum IT Disaster Recovery Management (ITDRM) oder auch „Disaster Recovery Planning“ (DRP) genannt (Sahebjamnia et. al. 2015: 262). Wie der Name bereits impliziert, stand die Verfügbarkeit der Informationstechnologie im Vordergrund. ITDRM fokussierte sich auf die

Stärkung der Widerstandsfähigkeit im Bereich der Elektronischen Datenverarbeitung (Brandt, Hermann und Groote 2011: 67). Zu dieser Zeit setzte die Digitalisierung der Unternehmensprozesse ein, deren Ausdehnung und Intensivierung seitdem enorm zugenommen haben (Langheinrich und Mattern 2003: 4). Die Einführung von Großrechnern zur Verarbeitung von Datenmengen und zur fortwährend gesteigerten Automatisierung von Arbeitsschritten ging einher mit der zunehmenden Abhängigkeit von Unternehmen hinsichtlich der Verfügbarkeit der Daten und Plattformen (Omar, Alijani, und Mason 2011: 127).

ITDRM setzte sich vom klassischen Betriebsmodell der IT dadurch ab, dass es für die Eventualität eines Ausfalls der IT Infrastruktur Wiederherstellungsprozeduren entwickelte. Diese Vorkehrungen unterschieden sich von dem etwa zeitglich entstehenden Funktionen des Informationsschutzes durch ihren Blick über die Schutzvorkehrungen der präventiven Risikomitigation hinaus, auf die Vorsorge für einen hypothetischen Ausfall der IT (Brandt, Hermann und Groote 2011: 67). Die Arbeitsbereiche bildeten sich um den Nukleus aus Rechenzentren und IT-Infrastruktur, deren Verfügbarkeit es sicherzustellen galt. Mit zunehmender Bedeutung wurden auch die Schnittstellen des Endnutzers in die konkreten Vorsorgebemühungen aufgenommen und Applikationen oder Plattformen im ITDRM bewertet und priorisiert. Risikobewertungen für Rechenzentren gewannen an Bedeutung und Sicherheitszertifikate wurden als Auszeichnungen für eine robuste Aufstellung der (IT-)Organisation einerseits, aber auch als Zeichen der Wertschätzung der Kontinuitätsvorsorge andererseits ausgestellt. Das übergeordnete Ziel des ITDRM war die Verfügbarkeit der IT und der dort gespeicherten Informationen sicherzustellen (Racz, Weippl und Seufert 2010: 249).

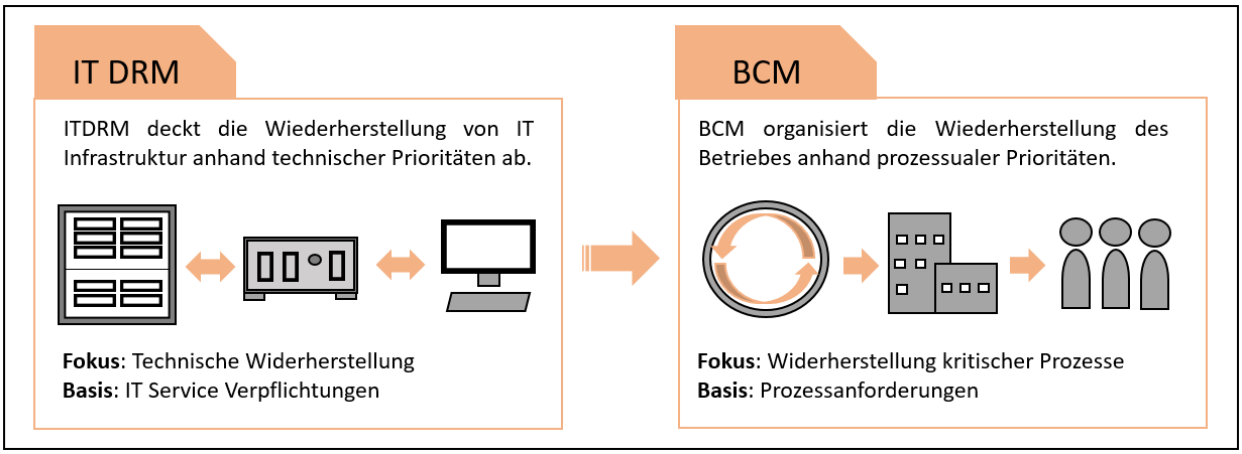

Abb. 5.4. Entwicklung des BCM aus dem ITDRM. Eigene Darstellung.

Aus diesem Kontinuitätsgedanken heraus entstand BCM.[247] Es übernahm die Logik der Verfügbarkeitssicherstellung des ITDRM und wendete sie auf den Bereich der Geschäftsprozesse, also der Betriebsorganisation an. Von den zwei wesentlichen Veränderungen lag der Erste in der Fokussierung auf weiteren Ressourcen, namentlich Gebäude und Personen, welche nun aus der Perspektive des Geschäftsprozesses heraus betrachtet wurden. Daraus entstand eine neue methodische Ausrichtung aus Sicht der Wertschöpfungskette und weniger an Unterstützungsfunktionen wie der IT ausgerichtet (Lam 2002: 21). Aber auch das ITDRM unterlag methodischen und konzeptionellen Veränderungen mit dem Fortschreiten der Digitalisierung. Aus ihm entstand unter dem Eindruck der zunehmenden Abhängigkeit von einer störungsfreien IT-Ressource das IT Service Continuity Management (Racz, Weippl und Seufert 2010: 249), dessen Fortgang wir im nächsten Kapitel näher beleuchten werden.

Das theoretische Konzept des BCM basiert je nach Quelle auf entweder fünf (Bonafede, Cerchiello und Giudici 2007: 80) oder wahlweise sechs Elementen (Torabi, Soufi und Sahebjamnia 2014: 309). Im klassischen Lifecycle-Modell des Business Continuity Institut sind ebenfalls sechs Elemente anzutreffen.[248] Dazu zählt erstens eine holistische Managementfunktion welche die Implementierung und den Unterhalt des (1) BCM Programms regelt. Zweitens folgt eine (2) Analyse der kritischen Geschäftsprozesse[249] und Risiken.[250]

[247] Drei Ansätze können als Erklärung auf die Frage dienen, warum Unternehmen in BCM investieren: Zum einem die (1) intrinsische Motivation zur Sicherung der eigenen Fortexistenz (Kahan, Allen und George 2009: 7; Schintler et. al. 2007: 293). Denn die Fähigkeit auf unvorhergesehene Ereignisse reagieren zu können, kann ein entscheidender Grund für den gewinnorientierten Konzern sein, trotz widriger Umstände seine Prozesse fortzuführen und seine Kunden mit Produkten und Dienstleistungen beliefern zu können (Braubach 2011: 38). Ferner können (2) regulatorische Erfordernisse wie Solvency II, VAG, DORA oder MaRisk den Ausschlag geben (vgl. Cook 2010; Fischer 2007; Gaycken und Karger 2011; Krotofil und Cárdenas 2013). Ebenso kann es auf der (3) Leistung des Organisationsgedächtnisses durch Erinnern der sie umgebenden Unsicherheit und daraus resultierenden Verwundbarkeit aufbauen (Rodriguez und García-Palomares 2014: 50). In einer Umfrage des Business Continuity Institut wurden 2016 deutsche Unternehmen nach den Gründen für ihr BCM Programm gefragt: 23 Prozent nannten gesetzliche Vorgaben, 22 Prozent Anweisungen der internen Revision oder externer Prüfer, weitere 20 Prozent eine unternehmerische Eigeninitiative, sowie ein Drittel machte andere Angaben zu den Gründen, beispielsweise Kundenvorgaben (BCM Academy 2016: 20).

[248] Der BCM Lifecycle wird in den einschlägigen Standards für BCM definiert. Der mittlerweile überholte BS 25999 galt lange Zeit als Referenz für die BCM-Methodik wurde aber durch den neueren ISO 22301 erweitert, der einen wesentlich breiteren Ansatz der Vorsorgeplanung anstrebt (BS 25999; ISO 22301).

[249] Zu Beginn der (2) Analysephase erfolgt die „Business Impact Analysis“ (BIA), um aus der Vielzahl an Prozessen diejenigen heraus zu filtern, welche das Unternehmen im Fall einer Unterbrechung ernsthaft gefährden können. Ebenfalls müssen Mindestgrenzwerte definiert werden, welche die minimal erforderliche Qualität des Prozessoutputs bestimmen und die Zeit erfassen, bis wann der Output oder das Leistungsniveau des Prozesses im Notfallbetrieb wiederhergestellt werden soll. Diese Zeit wird als „Recovery Time Objective“ (RTO) bezeichnet (Kahan, Allen und George 2009: 28). Die BIA-Analyse des Unternehmens ist der wichtigste Schritt des BCM Prozesses, da seine Durchführung über die Qualität der nachfolgenden Schritte entscheidet. Mit ihrer Hilfe werden die relevanten Risiken identifiziert und über die Kommunikation der Risikomitigation reflektiert.

[250] Ebenfalls in der Analysephase folgt die Bewertung der Risikoexposition des Unternehmens. Dieses Resultat aus der Schnittmenge zum Risikomanagement prüft die konkrete Ausfallprobabilität einer Ressource. Anhand der

Diese Analysephase basiert auf der Annahme, dass nicht für alle im Normalbetrieb durchgeführten Prozesse im Fall einer Geschäftsunterbrechung (zeit)kritisch wären (Lam 2002: 21f.). Durch die Selektion von kritischen, das heißt vitalen Prozessen und den relevanten Risiken einer Geschäftsunterbrechung wird der Rahmen für die (3) Wiederherstellungsstrategien[251] festgelegt (Torabi, Soufi und Sahebjamnia 2014: 311). Diese Strategien definieren die Wiederherstellungsziele und erforderliche Prozessperformanz im Notbetrieb (Bonafede, Cerchiello und Giudici 2007: 95).

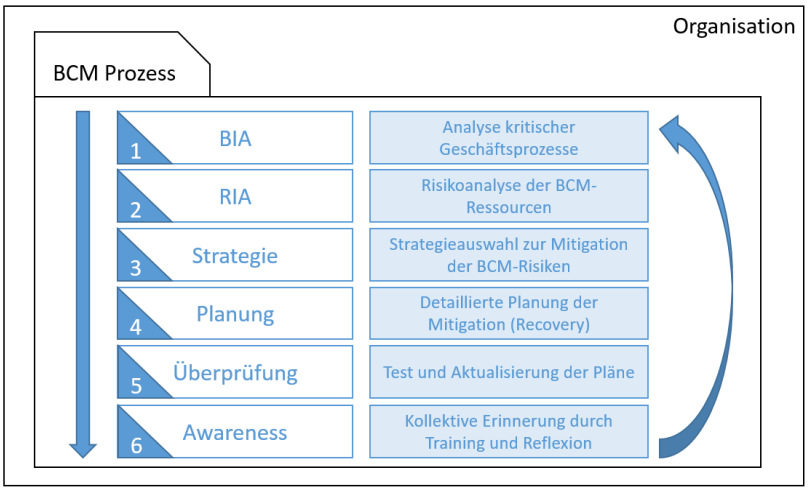

Abb. 5.5. Der detaillierte BCM Prozess, bestehend aus sechs Elementen. Eigene Darstellung.

Viertens folgt die Ausarbeitung von (4) Wiederherstellungsplänen auf der Grundlage der BCM-Strategie und resultieren in der Erstellung und Abstimmung von „Business Recovery Plans" (BRPs)[252] für jeden kritischen Prozess (Sahebjamnia, Torabi und Mansouri 2015: 261). Fünftens sollten diese Pläne kommuniziert und (5) getestet werden. Dies soll die Wirksamkeit der Pläne unter Beweis stellen, die Teilnehmer an den Ablauf gewöhnen und zur Aufrechterhaltung der Planqualität beitragen (Schintler et. al. 2007: 295). Als letzten Schritt des BCM-Prozesses erfolgt die (6) Einbettung in die Unternehmenskultur durch Fortbildungen und Inklusion in die kollektive Erinnerung der Vorsorgeplanung („Awareness"). Zudem ist eine

Methode des „Risk Idendification and Assessment" (RIA) können diejenigen Risiken identifiziert werden, welche Bedrohungen für den Betrieb der Prozesse darstellen können (Renn und Klinke 2004: 42).

[251] Anhand der identifizierten Prozesskritikalität, bestehend aus maximalen Schaden und RTO, kann die (3) Wiederherstellungsstrategien entwickelt werden (Bonafede, Cerchiello und Giudici 2007: 95). Diese sollten eine Priorisierung der Wiederherstellung an den genannten Kriterien berücksichtigen und ebenso die Reihenfolge der Prozesse und Ressourcen beachten. Dazu werden die von den Prozessverantwortlichen definierten Anforderungen analysiert und mit Mitigationsoptionen verglichen, welche als BCM Strategie bezeichnet werden.

[252] Wir werden uns mit dem Aufbau und Anwendung von Business Recovery Plans (BRPs), auch BCPs genannt in den folgenden Fallbeispielen genauer auseinandersetzen. "BCP aims to develop appropriate plans at pre-disaster in order to resume key business operations to a minimum acceptable predefined level" (Sahebjamnia, Torabi und Mansouri 2015: 261). Daher müssen BRPs die geeigneten Schritte beinhalten, um die Wiederherstellung des jeweiligen Prozesses innerhalb der RTO sicherzustellen. Die Herausforderung liegt darin diese Pläne einerseits vollumfänglich zu gestalten, aber andererseits auch einfach und lesbar zu halten (Schintler et. al. 2007:, 293).

Schnittstelle an das Krisenmanagement zur effektiven Umsetzung der Maßnahmen im tatsächlichen Schadensfall erforderlich. Das Modell des BCM-Lifecycles übersetzt sich daher in die Übersicht der oben genannten sechs BCM-Prozesskontrollen, anhand derer die Konformität von Maßnahmen zur Risikokontrolle im Unternehmen sichergestellt werden können (Lam 2002: 24).

Neben diesen Schritten des Lifecycle- Modells können zwei Prinzipien unterschieden werden, um die Wirksamkeit der traditionellen Risikokontrolle durch BCM und Krisenmanagement zu erhöhen. In der Literatur sind dazu die Begriffe (a) Robustheit und (b) Redundanz anzutreffen (Tierney und Bruneau 2007: 15). Beide Prinzipien sollen hier eingeleitet werden, um auch die Problematik zwischen Sicherheitsdispositiven und Profitabilität aufzuzeigen. Das erste Prinzip versucht unter dem Überbegriff (a) Robustheit die Eintrittswahrscheinlichkeit einer Geschäftsunterbrechung durch widerstandsfähige Systemarchitektur oder präventive Maßnahmen zu senken. So referenziert (a) Robustheit auf "(…) the capability and capacity of critical systems to withstand severe internal and/or external stresses and to maintain key functions" (Kahan, Allen und George 2009: 15). Diese Fähigkeit drückt sich durch die Widerstandskraft gegenüber den einwirkenden Einflüssen aus[253], ohne dabei einen Rückgang der Performanz zu erleiden oder in anderer Hinsicht Einschränkungen hinnehmen zu müssen. Darüber hinaus wird die ununterbrochene Funktionsweise von Schlüsselfunktionen hervorgehoben welche allen Veränderungen der Umwelt zum Trotz fortgeführt werden können (Linkov et. al. 2013: 472). Für unsere Zwecke soll die Robustheit daher die Fähigkeit ausdrücken, die negativen Folgen eines Ereignisses aufgrund solider Strukturen und Prozesse zu neutralisieren, ohne jedoch eine Reaktion auf das Ereignis zu initiieren oder Maßnahmen zur Wiederherstellung einzuleiten (Scherrer 2018: 98).

Der Begriff der (b) Redundanz hingegen bezieht sich auf die Spiegelung oder Doppelung von Prozessen und Ressourcen (Racz, Weippl und Seufert 2010: 245). Dies kann sich beispielsweise durch Niederlassungen an mehreren Lokationen ausdrücken, durch welche eine erfolgreiche Fortsetzung der Geschäftstätigkeit ermöglicht wird (Tierney und Bruneau 2007: 15) oder durch gespiegelte Rechenzentren, welche eine nahezu unterbrechungsfreie Fortsetzung der IT-basierten Geschäftsprozesse erlauben (Gaycken und Karger 2011: 6). Dem ist hinzuzufügen, dass die redundante Vorhaltung von Prozessen und Arbeitsmitteln lediglich eine Voraussetzung

[253] Eine kritische Sichtweise problematisiert das alleinige Vertrauen auf „Robustheit". Da im Vorfeld einer Krise meist nicht alle Informationen gegeben sind (vgl. Unsicherheit), ist eine adaptive Arbeitsweise notwendig, um Entscheidungen ad-hoc treffen zu können: "Instead of investing in robustness against adverse influences, resilience thinking favors more flexible responses that are based on the principle of adaptation (…)" (Cavelty 2013: 116).

für Prozesskontinuität bieten kann, nicht jedoch eine erfolgreiche Fortsetzung des Betriebs garantiert (Krotofil und Cárdenas 2013: 168). Ähnlich verhält es sich mit der Verfügbarkeit von Ressourcen, deren allgemeine Knappheit den Risikowert mitbestimmt.[254] Sowohl die Redundanz als auch die verfügbaren Ressourcenmenge stellen lediglich eine solide Ausgangslage dar und implizieren keine automatischen Handlungsabfolgen im Fall des Eintretens eines Ereignisses (AGCS 2013: 2).

Unter den Gesichtspunkten ökonomischer Rationalität erscheint die Doppelung von Ressourcen allerdings problematisch, da die ökonomische Ausrichtung in Unternehmen auf Effizienz und Kostenminimierung mit dem Zielbild der Sicherheitsmaximierung im Gegensatz steht. Die Bereithaltung nicht genutzter Kapazitäten wie zusätzliche Büroräume, Rechenzentren oder gespiegelte Teams an unterschiedlichen Standorten repräsentieren Kostenfaktoren, deren Rechtfertigung über die potentiellen Schäden einer Geschäftsunterbrechung ohne diese redundanten Strukturen im internen Entscheidungsprozess argumentiert werden muss (Christensen und Petersen 2017: 1443). Dazu kann die Übersetzung des Ausfallrisikos von Prozessen in der oben genannte Risikomatrix beitragen. Alternativ können Interessenskonflikte auch entschärft werden, indem kreative Lösungen zur Nutzung der doppelten Ressourcenvorhaltung eingeplant werden können. Weitere Büroflächen an anderen Standorten können zum Beispiel als Schulungs- oder Tagungsräume genutzt werden, um diese auch außerhalb eines (seltenen) Schadensereignisses ökonomisch sinnvoll einzusetzen.

Während der ethnographischen Untersuchung wurden auch andere kreative Ansätze besprochen, um die Kosten der Redundanz zu reduzieren beziehungsweise zu argumentieren.[255] Einige Beispiele dazu sollen die Flexibilität und Adaptionsfähigkeit der Wiederherstellungsstrategien zeigen und werden daher hier vorgestellt. Unter dem Prinzip des Verdrängungsarbeitsplatzes wurden beispielsweise dezidierte Büroflächen für Personal aus kritischen Prozessen an anderen Standorten reserviert. Die Nutzer dieser Räume und Hardware würden im Notfall nach Hause geschickt und ihre nicht-kritischen Tätigkeiten pausiert. Somit kann Redundanz für einen Standort ohne wesentliche[256] weitere Kosten im Normalbetrieb

[254] So ist es ein gewichtiger Unterschied für einen Automobilhersteller, ob ausschließlich ein Produktionsstandort für Motorbatterien vorhanden ist oder ob der Schaden durch ein Ereignis geringer ausfällt, wenn von vier verfügbaren Standorten, nur einer auszufallen droht. Auch im Fall der Verfügbarkeit von Ressourcen ist zu unterscheiden, dass ihr Wert nur die unmittelbare Resilienz des Unternehmens und den Risikowert in Form eines möglichen Schadens durch Ausfall einer Ressource betrifft.

[255] Im Rahmen eines Projekts in Deutschland im Jahr 2015 wurden von Experten Möglichkeiten entwickelt, kostensparende Redundanzoptionen zu identifizieren und in einer Kosten-Nutzen Rechnung zu bewerten.

[256] Kosten entstehen jedoch durch die „Beurlaubung“ von Mitarbeitern aus dem nicht-kritischen Prozess für die Länge der Unterbrechung.

erzeugt werden. Eine andere Beobachtung betraf die systematische Schulung von Mitarbeitern im Außendienst, um im Notfall die Nichtverfügbarkeit von Kollegen aus einer anderen Produktsparte zu kompensieren. Die Mehraufwände für die Fortbildung an zwei unterschiedlichen Produktkategorien konnten zu Stoßzeiten im Kundenkontakt beziehungsweise im Fall von Urlaub oder Abwesenheit in einem Team ausgeglichen werden.

Ein drittes Beispiel zeigt sich durch die Beibehaltung von IT-Anwendungen wie Kommunikationsplattformen. Der Ausfall einer Plattform könnte aufgrund der Architekturplanung auf unterschiedlichen Servern durch die Funktion einer anderen Plattform kompensiert werden. Die generelle Problematik von hohen Kosten im Fall von IT-Applikationen konnte in diesem Fall minimiert werden, da beide Anwendungen im Kundenkontakt notwendig waren und daher zur Erhöhung der Redundanz genutzt werden konnten. Eine Schlussfolgerung ist, dass der Rechtfertigungsdruck für Kosten der Risikokontrolle in Unternehmen auf einen potentiellen Interessenskonflikt mit dem Sicherheitsdispositiv und der Sicherheitsproduktion in Unternehmen hinweist. Daher stellt sich die Frage, wie Unternehmen diese Situation auflösen und welche Rolle staatliche Autoritäten in diesem Kontext spielen? Zu diesem Zweck wollen wir im Folgenden die Beziehung zwischen Unternehmen und staatlicher Ebene beleuchten und das Spannungsverhältnis zwischen ökonomischer Rationalität und gesellschaftlicher Erwartung an die Sicherheitsproduktion in Unternehmen zur Bereitstellungskontinuität von Waren und Dienstleistungen betrachten. Dies zeigt sich insbesondere im Fall der kritischen Infrastruktur, deren unterbrechungsfreie Versorgung der Bevölkerung ein besonders deutliches Beispiel für die Relevanz der Sicherheitsproduktion in Unternehmen durch effektive Risikokontrolle darstellt.

5.2. Verantwortungsdelegation

Die Relevanz der Beziehungen zwischen staatlichen Autoritäten und privaten Unternehmen zeigt sich in Gestalt der kritischen Infrastruktur, da hier gesamtgesellschaftliche Sicherheitserwartungen mit privatwirtschaftlicher Rationalität konfrontiert werden und ein möglicher Interessenskonflikt entsteht. Dieser Gegensatz aus klassisch-ökonomischer Gewinnorientierung und Gemeinwohl wird auch in der Literatur adressiert (Carr 2016; Cavelty und Suter 2009; Krahmann 2007) und ist für diese Arbeit interessant, indem das Zusammentreffen von Entscheidungsrationalitäten einerseits und die konkrete, exogene Anforderungsbeschreibung an Sicherheitsproduktion in Unternehmen anderseits deutlich werden. Zudem ist der gesamtgesellschaftliche Aushandlungsprozess von Risiken und deren Kontrolle im Fall der kritischen Infrastruktur und Schnittstelle zwischen staatlicher

Verantwortung und privater Trägerschaft besonders aufschlussreich, um den Beitrag von Unternehmen zur gesellschaftlichen Sicherheit zu beleuchten.

Unternehmen agieren innerhalb regulierter Rechtsräume, je nach Jurisdiktion unterschiedlich ausgeprägt, aber im Rahmen eines durch staatliche Autoritäten eingegrenzten und kontrollierten Handlungsrahmens. Ein Teil dieser Regulation betrifft die Sicherheitsproduktion in Unternehmen. Mit Blick auf die Sicherstellung der Kontinuität von Prozessen und Kommunikation in Unternehmen sind beispielsweise Solvency II, VAG, DORA oder MaRisk zu nennen (vgl. Cook 2010; Fischer 2007; Gaycken und Karger 2011; Hessel und Rebman 2021). Der rechtliche Gestaltungswille der Gesetzgeber und Aufsichtsbehörden entspringt auch einer wachsenden Vernetzung von staatlichen und privaten Aufgabenbereichen, sowie einer sukzessiven Ausweitung des Anteils der kritischen Infrastruktur[257] im Zuständigkeitsbereich von Unternehmen als privaten Betreibern (Carr 2016: 43; Fischer 2007: 53). Letztere übernehmen als Risikoträger der betreffenden kritischen Infrastruktur einen Teil des staatlichen Schutzauftrages gegenüber der Gesellschaft. Diese Delegation von Verantwortung im Kontext der öffentlich-privaten Partnerschaft („public-private partnership“ oder PPP) repräsentiert eine signifikante Verschiebung von Verantwortung und Verpflichtung mit normativen und überaus praktischen Folgen für Unternehmen (Cavelty und Suter 2009: 2). Der Verantwortungstransfer zur Sicherstellung der notwendigen Sicherheitsmaßnahmen erstreckt sich über weite Teile der kritischen Infrastruktur und verbindet gesellschaftliche Erwartungen an die staatliche Fürsorge mit den intra-organisationalen Risikokontrollsystemen. Daher wird die Zusammenarbeit zwischen öffentlicher und privater Sphäre in Form der Public-Private Partnership im Folgenden näher untersucht.

5.2.1. Public-Private Partnership

Wir verstehen BCM als Teil der Vorbereitungen einer Organisation auf Krisenereignisse, zu dessen Aufgabenprofil vorrangig die Prozesskontinuität zählt. Diese Krisenvorsorge trägt dem Schutz der kritischen Ressourcen eines Unternehmens Rechnung. Doch es handelt sich im Kern um Aufwände zur Aufrechterhaltung der organisationseigenen Funktions- und Handlungsfähigkeit, Entscheidungen zu treffen und zu kommunizieren, um dadurch Anschlussoperationen zu ermöglichen, ohne welche die Organisation aufhören würde zu bestehen. Dies entspricht der intrinsischen Motivation zum Selbsterhalt (Kahan, Allen und

[257] Der Begriff der kritischen Infrastruktur umschreibt Einrichtungen, welche Waren oder Dienstleistungen erbringen, deren Ausfall zu erheblichen Einschränkungen des öffentlichen Lebens führen würde. Dazu zählen unter anderem die Strom- und Wasserversorgung, Telekommunikationssysteme oder Finanzsysteme (Braubach 2011: 34).

George 2009: 7) und gleichzeitig kommt der Anspruch der Gesellschaft zum Tragen, welche den Staat und seinen ausführenden Institutionen zur Schutz- und Besitzstandswahrung verpflichtet.[258] Die für unsere Fragestellung relevanten staatlich regulierten Aufgaben betreffen den Schutz der von der Gesellschaft als essentiell betrachteten Güter und Leistungen und darunter im Speziellen deren stetige Verfügbarkeit. Dies wird als kritische Infrastruktur bezeichnet und im Folgenden vertieft.

Die Priorisierung von Risikobereichen unterliegt dabei einer gesellschaftlichen Konsensbildung, sich in zeitlicher Hinsicht verändernder Wahrnehmungen und der Platzierung im öffentlichen Diskurs, abhängig vom Grad der dazu die notwendigen technischen Expertise (Best 2010): 40). Im Allgemeinen werden unter der kritischen Infrastruktur und der vitalen Schutzwerten beispielsweise Anforderungen zur präventiven Risikomitigation wie Hochwasserschutzvorrichtungen oder Maßnahmen zur Vermeidung von Stromausfällen subsumiert (Braubach 2011: 36). Der Staat und seine Organe werden für die Aufrechterhaltung der Infrastruktur von den Bürgern verantwortlich gemacht und im Fall einer Krise wird dieses Vertrauen der Bürger einem Test unterzogen: „For substantially large parts of the global population, trust in public administration plays a crucial role in overcoming the challenges of a public emergency" (Ng und Lean 2012: 308). Noch zu Zeiten und Logiken des Kalten Krieges wurden auf staatlicher Seite in Westeuropa Vorbereitungen unter Verwendung des Begriffs Katastrophen- und Zivilschutz getroffen, um den Schutz der Infrastruktur im Fall einer möglichen militärischen Konfrontation zwischen beiden Machtblöcken zu verbessern (Amoore und Raley 2016: 2). Die Logik des Zivilschutzes folgte den Erfordernissen der militärischen Planspiele jener Zeit und ersuchte die Versorgung einer von elementaren Leistungen abgeschnittenen Bevölkerung sicherzustellen[259]. Mit den 1990er Jahren begann ein Wandel des Anforderungsprofils, welcher die zivile Kooperation der Krisenvorsorge und die systemische Grundversorgung in den Vordergrund stellte (Cavelty und Suter 2009: 2). Die kritische Infrastruktur wurde durch einen veränderten Gefahrenkatalog dennoch weiterhin als bedroht angesehen und rückte indes die Folgen technologischer Risiken in den Mittelpunkt der Wahrnehmung (Fischer 2007: 52).

[258] Diese Verantwortung rechtfertigt die besondere Machtstellung des Staates und begründet das staatliche Gewaltmonopol. Durch die originäre Aufgabe des Staates werden seine Institutionen in die Lage versetzt das Zusammenleben der Bürger zu regulieren und erschafft Anspruch auf Autorität und im Gegenzug deren Beachtung. Das hier skizzierte Bild setzt insbesondere den Schutz der Bürger in den Mittelpunkt.

[259] Man denke an die Folgen für die Zivilbevölkerung im Fall eines Ausfalls der Strom- und Wasserversorgung in Folge einer militärischen Auseinandersetzung. Die aktuelle Lage im Ukrainekrieg zeigt auf bedrückende Weise die Aktualität dieser Vorsorgeplanung für den Zivilschutz.

Die öffentliche Verwaltung übernahm lange die Rolle der entscheidenden und verantwortlichen Institution der Vorsorgeplanung. Jedoch wurde es zunehmend notwendig private Unternehmen in die Planungen einzubeziehen. Durch die weitreichende Privatisierung wechselten die verantwortungstragenden Akteure der kritischen Infrastruktur aus der alleinigen Zuständigkeit der Staatsbetriebe hinüber zu neuen, privaten Partnern.[260] Dies betraf auch Unternehmen, welche als Teil der kritischen Infrastruktur existenzielle Bedürfnisse der Bürger versorgen, darunter Energiekonzerne, Telekommunikationsunternehmen oder im Gesundheitswesen (LaPorte 2007: 60f.). Die Umwandlung der Krisenvorsorge etablierte eine Partnerschaft aus staatlichen Institutionen, unterstützt von semi-staatlichen Funktionsträgern wie dem Technischen Hilfswerk und privaten, marktwirtschaftlich orientierten Unternehmen, die an einer gemeinsamen Aufgabenteilung teilhaben. Die Aufgabenvermischung und darüber hinaus die Umwandlung der Trägerschaft ist allerdings mit der Frage verbunden, inwieweit die Verantwortung der öffentlichen Verwaltung dadurch betroffen ist. Denn es ist zu beobachten, dass die Professionalisierung und Technisierung der Gesellschaft auch zur Externalisierung von existenziellen Leistungen geführt hat (Krahmann 2005: 7). Deren Monopol über jene Güter und Aspekte des Allgemeinwohls sind zugleich Eigentum privater Akteure, aber aus Sicht der Bürger in der Verantwortung der öffentlichen Regulation und Teil des gesamtgesellschaftlichen Sicherheitsdiskurses (Carr 2016: 48).

Folglich läuft die Abwägung auf einen Kompromiss hinaus. Dieser formuliert die Überlegung, ehemals staatliche Unternehmen mithilfe von besonderen Verpflichtungen an der Krisenvorsorge zu beteiligen und durch Mindeststandards zu Investitionen und Vorkehrungen zu zwingen. Der Staat tritt dadurch als strategischer Impulsgeber in Erscheinung, welcher mit seinen Partnern aus der Privatwirtschaft zusammenarbeitet. Die zugrundeliegende Logik beabsichtigt die tendenziell gering ausfallende Investitionsbereitschaft für Sicherheitsstandards[261] von Unternehmen qua Normfestsetzung und -Kontrolle verpflichtend einzufordern (Schintler et. al. 2007: 291f.). Dafür gibt es eine zwingende Notwendigkeit, denn ein relevantes Element der kritischen Infrastruktur verlangt im Notfall nach einer engen Zusammenarbeit zwischen den Partnern auf privater und staatlicher Ebene (Holmgren 2007:

[260] Die Forderung der Gesellschaft zur Aufrechterhaltung des Sicherheitsniveaus basiert auf der Annahme dass der Staat zum Einen über die höhere Motivation zum Schutz der Infrastruktur verfügen würde, als auch zum Anderen die notwendige Qualifikation durch seine Organe einbringen könne. Dies zeigt sich beispielsweise im Umgang mit der abstrakten terroristischen Bedrohung, die in die Grundhaltung der Bevölkerung überleitet, den Staat für die Lösung der Makroprobleme der Gesellschaft in die Verantwortung zu nehmen (Krahman 2007: 9).

[261] Der ökonomische Blick auf MNU als gewinnorientierte Unternehmen stellt dabei die originäre Motivation von Unternehmen in Frage, ausreichende Vorkehrungen in Sicherheit zu tätigen (Carr 2016: 56). Dieser Interessenskonflikt bestimmt die Auseinandersetzung mit der PPP zur Einbindung privater Akteure in die Sicherheitsproduktion (Cavelty und Suter 2009: 7).

52). Darüber hinaus sind allerdings auch die internen Aktivitäten von MNU zum Schutz und Fortbestand der kritischen Infrastruktur relevant, da sich die betreffenden Ressourcen und Fähigkeiten in ihrer Verantwortung befinden. Daher ist es angezeigt die Rolle von Unternehmen für ihre eigene Sicherheitsproduktion in der Literatur der Internationalen Beziehungen stärker zu berücksichtigen, insbesondere im Fall der kritischen Infrastruktur, wie der nachfolgende Abschnitt zeigen soll.

5.2.2. Sicherheitsdiskurs und kritische Infrastruktur

Der Begriff der kritischen Infrastruktur bezieht sich auf die in einer Gesellschaft genutzten Leistungen, welche einen essentiellen Beitrag zur Erhaltung des lebensnotwendigen oder zivilisatorisch unverzichtbaren Standards beitragen (Braubach 2011: 34). In einer juristischen Dimension verstehen sich darunter „Einrichtungen, Anlagen, Dienste und Systeme, auf die Staat und Gesellschaft existentiell angewiesen sind und deren Ausfall bzw. Störung zu gravierenden Schäden für das Gemeinwesen, Wirtschaft und Bevölkerung sowie für den Einzelnen führen würde“ (Gaycken und Krager 2011: 5). Beispiele für Dienstleister kritischer Infrastruktur sind die Strombetreiber, Wasserwerke, Organe der öffentlichen Sicherheit, Lebensmittelversorger sowie Finanzdienstleister, welche den Fluss von Geldmitteln aufrechterhalten sollen, aber auch Internetunternehmen und Betreiber der IT-basierten Kommunikationsplattformen. Letzteres beschreibt auch einen semantischen Transfer der Begriffsdeutung von kritischer Infrastruktur, welche mit fortschreitender Digitalisierung weniger den Schutz traditionell physikalischer Liegenschaften meint, als vielmehr das technologische Kommunikationsfundament des Informationszeitalters einerseits und den Sammelbegriff der IT-Ressource andererseits (Huang et. al. 2021: 262), von deren Funktionstüchtigkeit die meisten Betriebsabläufe der oben genannten Versorgungseinrichtungen operativ abhängig sind (Beck et. al. 2014: 10f.).

Insgesamt werden etwa in den USA bis zu 85 Prozent der kritischen Infrastruktur im privaten Besitz gewähnt (Carr 2016: 52). Aus Sicht der staatlichen Behörden stellt diese aufgrund der bereitgesellten Waren und Dienstleistungen einen elementaren Teil der nationalen Sicherheit dar (Homeland Security Council 2007: 22). Auch in Deutschland wird von einer Eigentumsquote privater Unternehmen an der kritischen Infrastruktur von etwa 80 Prozent (Gaycken und Krager 2011: 5), in anderen Schätzungen von bis zu 85 Prozent ausgegangen (Braes und Brooks 2010: 17). Das *Internet* – das aus vielen Einzelkomponenten bestehende, elementare Kommunikations- und Steuerungselement des digitalen Zeitalters - wird zu 90 Prozent in privater Hand gesehen (Fischer 2007: 53). Zusätzlich sind Unternehmen

hinzuzurechnen, deren Hardware, Software oder Middleware[262] die Verfügbarkeit von Informationen und Dienstleistungen wie etwa das Verkehrswesen durch Navigations- und Lenkungssysteme oder die Sicherheit im Zahlungsverkehr ermöglichen (Beck et. al. 2014: 24).

Diese Unternehmen tragen eine wesentliche Rolle bei der Aufrechterhaltung und Weiterentwicklung einer zunehmend auf das Internet und den Austausch von Informationen spezifizierten Wirtschaft (Castells 2010: 69) und erweitern den Sicherheitsdiskurs der Gesellschaft im Informationszeitalter.[263] Dazu kann eine Unterscheidung zwischen konkreten und abstrakten Bestandteilen der kritischen Infrastruktur hilfreich sein, um einen differenzierten Blick auf die Einbindung von Unternehmen in staatliche Sicherheitsaufgaben zu erhalten. Zum einem sind Eigentums- oder Betriebsverhältnisse zu beachten, welche eine rechtliche Verantwortung der Unternehmen konkretisieren und beispielsweise eine weitere Delegation von Verantwortung und Risikokontrollen durch Outsourcing erschweren (Schwering 2010: 231). Zum anderen ist eine abstrakte Beteiligung von Unternehmen zu bedenken, wenn diese nur mittelbar am Bereitstellungsprozess des betreffenden Gutes mitwirken oder dienstleistend für staatliche Aufgaben- und Risikoträger tätig werden (Kahan, Allen und George 2009:7).

Im Rückblick auf die Entwicklungen der vergangenen drei Dekaden, qualifiziert sich die Rolle von Unternehmen in sicherheitsrelevanten Bereichen der kritischen Infrastruktur als Diskussionsgegenstand unter anderem auch aufgrund der hier wahrgenommen, sicherheitsrelevanten Schlüsselfunktion (vgl. Beck et. al. 2014). Diese Betrachtung blieb in der Literatur bisher von weitgehend untergeordneter Bedeutung, bedarf jedoch näherer Betrachtung und empirischer Aufarbeitung. Dies begründet sich aufgrund der weitreichenden Beteiligung der Unternehmen an der Vorsorgeplanung und Sicherheitsausübung in Gesellschaften, denn „[d]ie Aufgabe des Schutzes kritischer Infrastrukturen stellt sich trotz der unterschiedlichen Verteilung für Staat und für private Unternehmen in gleicher Weise. Dies führt zu einer faktischen Verantwortungsteilung“ (Gaycken und Krager 2011: 5). Diesen Transfer begleiten weitreichende strukturelle und organisatorische Implikationen hinsichtlich der Rollenverteilung zwischen staatlichen und privaten Akteuren, deren Auswirkungen auf den Sicherheitsdiskurs durch eine erweiterte Perspektive in der Forschung berücksichtigt werden sollten (Schintler et. al. 2007: 291).

[262] Die Infrastruktur-Hardware aus Rechenzentren, Clouds und Servern zählt zu den physikalischen Eckpfeilern der digitalen Sphäre. Auf ihnen baut die Middleware auf, Betriebsprogramme und Koordinationsanwendungen, welche einen Austausch zwischen den Anwendungen auf der Softwareebene ermöglichen.

[263] Die Relevanz der Thematik dehnt sich über verschiedene Bereiche der Literatur aus. So entwickelte sich beispielsweise eine Diskussion um die Rolle des Nahverkehrs als Bestandteil der kritischen Infrastruktur, dessen Verfügbarkeit ein Bestandteil des öffentlichen Lebens repräsentiert. (Rodríguez und García-Palomares 2014: 51).

Mit Blick auf die Corona-Pandemie ist zudem die globale Rolle von Produktionskapazitäten und technologischen Potentialen in den Vordergrund getreten, Der rasant angestiegene, global zeitgleich angemeldete Bedarf an beispielsweise Beatmungsmaschinen, Belüftungsanlagen oder Atemschutzmasken führte die Abhängigkeit von reibungslos funktionierenden internationalen Produktions- und Lieferketten vor Augen (Marom und Lussier 2020: 259). Darüber hinaus veränderte sich die Perspektive auf die Beschaffenheit der Lieferkettensicherheit und die Bedeutung nationaler Produktions-kapazitäten, das bedeutet dem Zugriff der eigenen Jurisprudenz auf Unternehmen zur Herstellung systemrelevanter Dienstleistungen und Güter (Kocher und Weyerstraß 2020: 6). Diesem Bereich ist auch die Frage nach der Verantwortung von Unternehmen zuzuordnen, wenn diese eine Entscheidung darüber zu treffen haben, die eigene Produktion den Bedürfnissen der Krisensituation anzupassen, indem beispielsweise Werke umgerüstet werden, um Waren des aktuellen Bedarfs und unabhängig von ihrer Wirtschaftlichkeit herzustellen. Abstrakt betrachtet fand das Stichwort *Systemrelevanz* zwar nicht im Jahr der Corona-Pandemie zum ersten Mal Eingang in den öffentlichen Diskurs, dennoch erhielt es einen vermutlich neuartigen Bedeutungsrang im gesellschaftlichen Risikospektrum (Burstedde et al. 2020: 5).

Zuletzt sollte die Debatte ebenfalls die Qualifikation von Unternehmen als Initiatoren der eigenen Sicherheitsproduktion beziehungsweise ihres Beitrages für die gesamtgesellschaftliche Sicherheitsarchitektur berücksichtigen. Eingedenk der im zweiten Kapitel adressierten IT-Kompetenz ergibt sich einerseits die Herausforderung auf Seiten der Unternehmen, die übertragenen, regulatorischen Anforderungen in Hinsicht auf die technische Umsetzbarkeit und mit Blick auf die verfügbare Expertise überhaupt erfüllen zu können (Arnold et. al. 2016: 5). Andererseits steht die Motivation von Unternehmen zur Disposition, Investitionen in ein Risikokontrollsystem zu leisten, wenn der regulatorische Druck an Eindeutigkeit und Konsequenz mangelt: „Die Rolle des Staates beim Infrastrukturschutz hat sich verändert, und das stellt alle Beteiligten vor neue Herausforderungen. Durch Liberalisierung (Elektrizitäts- und Gasversorgung) und Privatisierung (…) gehen Infrastrukturen aus dem staatlichen bzw. kommunalen in den Besitz von Privaten über, die im Wettbewerb untereinander stehen (sollen)“ (Fischer 2007: 52). Insbesondere der letzte Aspekt trifft den Kern des Problems: Eine Marktwirtschaft ist auf dem Prinzip des Wettbewerbs aufgebaut und private Akteure bedienen im ökonomischen Verständnis den Markt unter kompetitiven Bedingungen.[264]

[264] Das Spannungsfeld zwischen Kontinuität und Profitabilität zeichnet sich ebenfalls im Informationszeitalter ab: “Thus, firms will be motivated not by productivity, but by profitability, and growth of value of their stocks. (…) And political institutions, being shaped by a broader set of values and interests, will be oriented, in the economic

Unter diesen Vorzeichen ist die Annahme zu artikulieren, dass Unternehmen primär auf die Profitabilität ihrer Investitionen achten, aber auch den Fortbestand der Leistungserbringung berücksichtigen, insbesondere wenn diese von gesamtgesellschaftlicher Relevanz ist (Schintler et. al. 2007: 291f.). Nachhaltige Strategien implizieren selbstverständlich Maßnahmen zur Instandhaltung der erworbenen Objekte und den Schutz der Investition, doch bleibt es fraglich ob gewinnorientierte Konzerne alleine auf diesem Prinzip aufbauend, die entsprechende Vorsorge betreiben werden (Cook 2010: 23). Denn dies referenziert zuvorderst auf die zuvor thematisierten technologischen Risiken mit hohem Schaden und niedriger Frequenz, welche in der Risikomatrix des organisationsinternen Risikomanagements nicht als oberste Priorität erscheinen.[265]

5.2.3. Risikoträger und Verantwortung

Die Aufsicht über die Einhaltung der Verpflichtungen seitens der privaten Partner übernehmen Institutionen des Staates. Ihre Funktion unterstützt den Kompromiss des Verantwortungstransfers und folgt dem Ziel die Aufrechterhaltung notwendiger Mindeststandards sicherzustellen. Daher ist es die Rolle von Aufsichtsbehörden die regulatorischen Anforderungen zum Schutz der kritischen Infrastruktur einzufordern und zu überprüfen (Schwering 2010: 231). Dazu verfügen sie über besondere Kompetenzen zur Ausübung ihrer Kontrollaufgaben, beispielsweise im Sinne der generellen Rechenschaftspflicht der Risikoträger gegenüber den staatlichen Institutionen oder in Form von Begehungen und Revisionen (Shaw 2004: 24). Die Mitglieder dieser öffentlichen Einrichtungen sollen die zentrale Aufgabe in der Neugestaltung staatlicher Aufgabenwahrnehmung übernehmen und durch die Kontinuität der staatlichen Aufsicht soll der originäre Auftrag des Staates trotz des erstmaligen Eigentümerwechsels von kritischen Infrastruktur in oder später zwischen privaten Akteuren gewahrt bleiben.

Dies trifft insbesondere als Leitidee auf die Regulierung privater Träger der kritischen Infrastruktur zu. Doch bleiben Zweifel an der Qualität dieser Lösung. Denn zwischen unmittelbarer Verantwortung für die garantierte Bereitstellung einer kritischen Infrastruktur, welche zur Befriedigung elementarer öffentlicher Bedürfnisse beiträgt und der

realm, toward maximizing the competitiveness of their constituent economies. Profitability and competitiveness are the actual determinants of technological innovation and productivity growth“ (Castells 2010: 94).

[265] Denn obwohl Krisenereignisse der jüngeren Vergangenheit die Notwendigkeit zur effektiven Implementierung von Krisenvorsorge und BCM-Plänen aufzeigten, werden Risiken häufig unterschätzt und der alltägliche Erfüllungsdruck der Erwartungen der Märkte dem sporadischen Auftreten von Schadensereignissen übergeordnet. “The markets driving infrastructure are geared towards maximizing efficiency to increase profit and not maximizing protection, which can result in public vulnerabilities” (Schintler et. al. 2007: 291).

Verantwortungsdelegation an private Eigentümer, deren Krisenvorsorge durch staatliche Organe lediglich kontrolliert wird, besteht ein wesentlicher Unterschied. Die Kontrolle der ausführenden Instanz ist nicht gleichbedeutend damit, die Verantwortung selbst wahrzunehmen (Fischer 2007: 52) und kompensiert die organisatorische Trennung zwischen Risikoträger und delegierender Ebene nur geringfügig. Die öffentliche Akzeptanz hängt somit von der Erfüllung einer Aufsichtsfunktion und von der Einbindung der relevanten Akteure in gemeinsame Konzepte zur Kontrolle der Risiken ab. Betrachtet man die ausdifferenzierten Anforderungen an verschiedene Dienstleister der kritischen Infrastruktur, kann man einen Unterschied zwischen den Branchen und dem ihnen innewohnendem Gefährdungspotential erkennen (Holmgren 2007: 52). Die Verantwortung aus dem Bereich des Politischen in die Wirtschaft auszugliedern und die Einhaltung von Kontrollen über Aufsichtsbehörden oder von ihnen eingesetzten Dritten aufrechtzuerhalten, weist eine fragwürdige Einstellung der politischen Ebene auf.[266] Verantwortung ist seinem Prinzip nach nicht teilbar.

Im Fall eines Ereignisses kann in der Folge ein Reputationsschaden für die staatlichen Aufsichtsbehörden entstehen und im schlimmsten Fall der Verlust des Vertrauens in die Funktionsfähigkeit der öffentlich-privaten Partnerschaft. Die unsachgemäße Überwachung von privaten Trägern wie etwa des deutschen Zahlungsdienstleisters Wirecard durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und der beauftragten Wirtschaftsprüfergesellschaft führen zu eben solchen problematischen Verstrickungen (Schäfer 2021: 320). Gravierender erscheint noch die Kontrolle potentiell gefährlicher Einrichtungen, wie es etwa der havarierte Atomreaktor im japanischen Fukushima verdeutlicht.[267] Auch andere Beispiele des Versagens staatlicher Aufsicht verdeutlichen das Risiko, wenn die Verantwortungsdelegation nicht durch sachgemäße Kontrollfunktionen begleitet wird. Die Kontrollen müssen effektiv angewendet und nachgehalten werden, um effektiv zu sein (Meredith et. al. 2008: 4). Dies beginnt mit der ausreichenden Ausstattung der Behörden mit Ressourcen beziehungsweise unabhängiger Entscheidungsgewalt und dehnt sich bis auf die Wahrnehmung von Aufsichtsratsmandaten durch politische Amtsträger aus, deren Aufsichtsfunktion der Aufgabe gerecht werden sollte.

[266] Der Skandal um die mangelnde Kontrolle des Wirtschaftsprüferhauses Ernst & Young (EY) im Fall des Zahlungsdienstleisters Wirecard legte dieses Problem offen. Es steht die generelle Frage im Raum ob das gegenwärtige System der privaten Unternehmensprüfung Bestand haben kann, wenn Bilanzfälschungen trotz jahrelanger Buchhaltungsprüfungen fortgesetzt werden konnten (Schäfer 2021: 320).

[267] Hindemarsh stellt dazu treffend fest: "One clear example of a highly questionable or weak regulatory action, also reinforcing the notion of agency capture, was with regard to Fukushima Daiichi as an aging plant near the end of its lifespan with out-of-date safety systems" (Hindmarsh 2013: 5).

Dazu sind Kooperationen zwischen beiden Sphären notwendig, um entsprechende Lösungen in Fragen der Sicherheit und des gesellschaftlichen Risikoappetits finden. Insbesondere der prädominante Einfluss von Technologien macht die Inklusion privater Akteure notwendig, die als Eigentümer der technischen Infrastruktur und als Wissensträger[268] den Staat bei der Ausübung seiner Aufgaben unterstützen müssen (Cook 2010: 26). Dadurch wird die Unternehmensführung zum Teilhaber der gemeinsamen Aufgabenteilung und verpflichtet diese, geeignete Maßnahmen zur Fortsetzung der Kerngeschäftsbereiche zu finden und zu implementieren. Diese Aufgabe wird umso interessanter, als dass dies in den unternehmerischen Entscheidungsfreiraum wie etwas durch Anforderungen an die Budgetplanung einerseits eingreift und andererseits interne Entscheidungsmechanismen und Prozessvorgaben von externer Seite aus beeinflusst. Die Integrität des internen Organisationswesens nimmt somit eine andere Gestalt an und zeigt die Vermischung von inneren und äußeren Wahrnehmungsbereichen, welche sich auf die Abgrenzung der Unternehmen als Organisationen zur Außenwelt auswirkt.

Ferner sind komplexe Unternehmensstrukturen auf eine weitere Form der Verantwortungsdelegation innerhalb der Organisation angewiesen, um die operative Steuerung zu gewährleisten. Auch wenn die Inhaber und Geschäftsführer eine individuelle Verantwortung an den Entscheidungen des Unternehmens als Ganzes behalten, wird mit jedem weiteren Schritt der Delegation durch die Organisationshierarchie die klare Zuordnung von Verantwortung erschwert.[269] Denn durch die interne Delegation wird ebenfalls die Rolle des Risikoträgers verschoben und die Verantwortung über mehrere Ebenen der Entscheidungsfindung geteilt. Im Ergebnis können dadurch die Ebene der Entscheidungsträger mit Blick auf Organisationsentscheidungen und Budgethoheit einerseits und die Ebene mit operativer Verantwortung andererseits getrennt sein. Dadurch entstehen neue Herausforderungen an das organisationsinterne Gedächtnis und die Kommunikationsfunktion, um effektive Kontrolle ausführen zu können.

Im Folgenden wollen wir nun den Blick auf drei Fallbeispiele richten, die Krisenereignisse und ihre Auswirkungen auf die Entwicklung der Sicherheitsproduktion in Unternehmen hatten.

[268] Aus dieser Situation heraus entsteht eine asymmetrische Verteilung von Wissen, welche die Kontrolle erschwert. Wie im Fall von komplexen Finanzprodukten zu beobachten ist, entziehen sich diese mithilfe von Buchungsmethoden und geschickten Bündelungen einer regulatorischen Begrenzung und erfordern adäquates Wissen über diese Produkte auf der Seite des Regulators.

[269] Eine exemplarische Delegation gestaltet sich indem der formell zuständige Geschäftsführer die Risikomitigation in die Hände eines Bereichsvorstands gibt. Dieser adressiert einen Fachbereich, welcher erneut nach einer Abteilung Ausschau hält, die dafür geeignet scheint beziehungsweise über adäquate Ressourcen verfügt; das bedeutet Expertise, Personal und Budget (Schintler et. al. 2007: 291).

Diese betreffen die Anschläge vom 11. September 2001, das Reaktorunglück von Fukushima 2011 und die Pandemiewellen der Vogel- und Schweinegrippe zwischen 2003-2011 sowie des Corona-Virus zwischen 2019 und 2022. Insbesondere die Fallbeispiele zum Reaktorunglück von Fukushima und der Pandemie greifen zudem explizit die zuvor diskutierte Problematik der Sicherheitsproduktion im Spannungsverhältnis zwischen öffentlicher und privater Zuständigkeit für Vorsorgeplanung auf. Die drei gewählten Fallbeispiele werden zunächst im jeweiligen Abschnitt vorgestellt und ihre Rolle für die Entwicklung der unternehmerischen Risikokontrolle, sowie der Zusammenarbeit mit staatlichen Autoritäten thematisiert. Anschließend adressiert jeder Abschnitt eine spezifische Weiterentwicklung der Mitigationsstrategien und zeigt deren Einfluss beziehungsweise Auswirkungen auf. Beginnend mit den Anschlägen vom 11. September 2001 gehen wir im Folgenden auf die Problematik und die Reaktionsmechanismen der traditionellen Risikokontrolle dieser Zeit ein.

5.3. Fallbeispiel 1 - Ausfall von Gebäuden – New York 11.09.2001

Ein Schadensereignis mit hohem Schaden und geringer Wahrscheinlichkeit repräsentierten aus Sicht der unternehmensinternen Risikomatrix die Anschläge vom 11. September 2001[270] (LaPorte 2007: 61), in dessen Folge die Dringlichkeit von präventiver Schutzmaßnahmen Gegenstand einer breiten Diskussion in Unternehmen wurde (Smit 2005: 8). Die beständige, repetierte Wahrnehmung der abstrakten Terrorgefahr wurde zum medialen Leitmotiv und reproduzierte die Sorge um weitere terroristische Anschläge[271] (Myhen und Walklate 2006:

[270] Die Anschläge vom 11.September 2001 in den USA waren eines der ersten Schadensereignisse des anbrechenden 21. Jahrhunderts mit globaler Perzeption und prägten die Thematisierung des internationalen Terrorismus nun auch außerhalb von Sicherheitskreisen (Mendonça und Wallace 2006: 261). An diesem Tag wurden mehrere Passagierflugzeuge von Entführern dazu genutzt um symbolträchtige Ziele in den USA anzugreifen. Im kollektiven Gedächtnis blieben vor allem die zwei Flugzeuge präsent, welche die Türme des World Trade Centers in New York City zum Einsturz brachten. Mehr als 3.000 Personen verloren bei dem größten Terrorangriff des Landes ihr Leben. Die empfundene Unsicherheit titulierte ein Momentum der kollektiven Erinnerung. Und neben einer breiten Öffentlichkeit, waren es auch die Führungsebenen vieler Unternehmen, welche diese Erfahrung teilten (Smit 2005: 10).

[271] Es ist anzumerken dass der Terrorismus kein Novum der jüngeren Geschichte und noch weniger ein rein westliches Problem darstellt. Die Geschichte kennt viele Beispiele und Facetten des Terrorismus. Ob damit Gewalttaten russischer Anarchisten des 19. Jahrhunderts, marodierende Gruppierungen während der Weimarer Republik, der Versuch der gewaltsamen Umstürzung der Gesellschaftsverhältnisse wie durch die RAF in der Bundesrepublik Deutschland oder durch den Leuchtenden Pfad in Peru gemeint sind, sie alle zeigen, dass Terrorismus stets eine Herausforderung für Gesellschaften darzustellen vermochte (Dreyfus 1999: 378). Der ¨deutsche Herbst¨ von 1977 richtete sich beispielsweise mit der Entführung des Arbeitgeberpräsidenten Hans Martin Schleyer sowie der vorausgehenden und nachfolgenden Anschläge gegen andere Vertreter der Wirtschaft und gegen das von ihr diffamierte System. In den 1990er Jahren war das World Trade Center in New York bereits Ziel eines Anschlags gewesen, dennoch reichten diese oder andere Ereignisse nicht aus, eine tatsächliche Änderung der gesellschaftlichen Risikoexposition zu begründen. Denn der Terrorismus war Personen- oder Objektbezogen. Er zielte nicht auf die Funktionsfähigkeit einer Organisation ab und versuchte nicht die Lebensweise einer Gesellschaft durch Unsicherheit gesamtheitlich zu unterminieren (Boscarino et. al. 20006). So war eine Risikomitigation gegenüber dem Terror der RAF und anderer Gruppierungen möglich, indem diesem durch erhöhte Schutzmaßnahmen von Individuen begegnet wurden, beispielsweise mit Personenschutz.

129f.). Der Einsturz der beiden Türme wurde weltweit in Echtzeit übertragen und die Tragweite der Schäden im globalen Sicherheitsdiskurs rezipiert (Williams 2003: 512). Dies hatte signifikante Auswirkungen, sowohl auf das subjektive, wie auch das kollektive Sicherheitsgefühl (Krahmann 2007: 12). In ihrer Folge, führten die Anschläge zu einer verstärkten Auseinandersetzung von Experten und einem breiten öffentlichen Interesse an terroristischen Risiken im Allgemeinen (Fekete, Grinda und Norf 2016: 222) und der Verfügbarkeit von kritischen Ressourcen im Speziellen. Letzteres bezog sich für unternehmerische Vorsorgeplanung vor allem auf die Verfügbarkeit und Zugänglichkeit von Bürogebäuden und Produktionsstätten (Rose 2011: 98).

In Zahlen gesprochen verursachten die Anschläge einen Schaden von geschätzten 33 bis 36 Milliarden US-Dollar, wenn man den Ausfall von Prozessen, Gebäudeschäden, Trümmerbeseitigung, Hinterbliebenenrenten, Reinigung und Instandhaltung weiterer Gebäude addiert (Bram et. al. 2002: 5). Insbesondere der Ausfall der Geschäftsfähigkeit war aus Sicht von Unternehmen besorgniserregend. Der Aktienhandel der New Yorker Börse wurde für sechs Tage ausgesetzt und anschließend in einem improvisierten Betrieb wieder fortgeführt (ebd.: 8). Doch die durch den Anschlag zerstörten Räumlichkeiten waren leichter zu kompensieren als der Verlust der Infrastruktur und Daten aufgrund fehlender Fail-Over Systeme. Mehr als 2 Millionen virtuelle und physikalische Datenverbindungen mussten wiederaufgebaut werden, darunter 15.000 Komponenten alleine für die Betreiberfirma NYSE (Schintler et. al. 2007: 292). Die zerstörten Büroflächen, unterbrochenen Transportverbindungen, die durch die Zerstörung und Aufräumarbeiten gesperrten Gebiete in Manhattan und nicht zuletzt die getöteten Mitarbeiter verschärften die Situation. In den folgenden Wochen nahmen die Einschränkungen graduell ab, doch eine Rückkehr zur Normalität war lange Zeit nicht denkbar.[272] Der Krater am Standort des ehemaligen World Trade Centers symbolisierte die die Gefahr und war ebenso Grundstein für neue Gesetze zur Bekämpfung des Terrorismus, wie etwa zur Unterbindung der Terrorfinanzierung und Geldwäsche (Kahl 2011 :7), die vorrübergehende Sperrung des Luftraums oder Importbeschränkungen aufgrund erhöhter Sicherheitsüberprüfungen (Behnezhad, Connett und Nair 2013: 81), welche Auswirkungen auf die bestehende Geschäftspraktiken und Wertschöpfungsketten hatten.

[272] Die Unsicherheit drückte sich aber auch in individuellen Erlebnissen aus. Eine Studie aus dem Jahr 2002 bilanzierte die Risikoperzeption der Bürger New Yorks und dokumentierte bei 30 Prozent Indikationen für eine erhöhte Wahrnehmung einer terroristischen Bedrohung (Bram et. al. 2002: 9). Der psychologische Effekt war allgegenwärtig und für 11 Prozent der New Yorker Erwachsenen wurden im Folgenden Panikattacken attestiert. Nicht zu vergessen ist auch die umgreifende Sorge vor biologischen oder chemischen Anschlägen, wie zum Beispiel durch Anthrax (Boscarino et. al. 2006: 506).

Unter den betroffenen Wirtschaftszweigen in Manhattan erlitt das Bankenwesen die stärksten Einschnitte (Mendonça und Wallace 2006: 266). Dies war auf die enorme Unsicherheit an den Märkten zurückzuführen, aber auch auf die vorübergehende Schließung der Transaktionsmärkte, sowie im Besonderen auf unzureichende Vorsorgemaßnahmen zur Fortsetzung der Geschäfte an einem Ausweichstandort[273]. Ein Aspekt der öffentlich-privaten Zusammenarbeit offenbarte sich auch im Sinne der systemrelevanten Unternehmen an der Wall Street, deren bisherige Vorsorgeplanung die Wahrscheinlichkeit von Risikokategorien wie die der Anschläge vom 11. September 2011 unterschätzt hatten.[274] „The many problems in the financial sector resulting from the attack has brought new attention to the vulnerability of the US and global financial sector. The result is an impasse between government and the private sector. Most infrastructure providers do not have financial resources to protect their infrastructure from low probability events like terrorism and natural disasters" (Schintler et. al. 2007: 292).

Dieser Aspekt wiederholte sich ebenfalls in der Debatte über die nationale Sicherheit und die Fähigkeit von Staaten vergleichbare Ereignisse zu verhindern oder den Schaden effektiv zu begrenzen (vgl. Flynn 2008: 3ff.; Kahan, Allen und George 2009: 7f.; Homeland Security Council 2007: 28). Der Schutz der kritischen Infrastruktur evolvierte zum Politikum und stellte die Frage nach der Verwundbarkeit von essentiellen Strukturen des öffentlichen Lebens (Brunsdon und Dalziell 2005: 28). Zum Schutz der kritischen Infrastruktur wurden daher verstärkt Aufwände seitens der staatlichen Institutionen getroffen, um die Vernetzung von privatwirtschaftlicher und staatlicher Krisenvorsorge zu synchronisieren (Mendonça und Wallace 2006: 261). Die Anschläge gelten daher als Initialmoment der flächendeckenden Etablierung von BCM-Programmen in Unternehmen und als ein maßgeblicher Schritt zur Wiederaufnahme der Public-Private Partnership nach dem Ende des Kalten Krieges zur Sicherstellung der kritischen Infrastruktur (Schintler et. al. 2007: 291). Die neue Perzeption der Unsicherheit begünstigte diese Entwicklung, im Sinne eines ganzheitlichen Schutzkonzeptes

[273] Eine Schätzung bezifferte den Verlust an Arbeitsplätzen durch die Geschäftsunterbrechung im Bankenwesen auf etwa 11 Prozent bis zum Ende des zweiten Quartals 2002 (Bram et. al. 2002: 8). Ein wesentliches Problem war die Verfügbarkeit von Büroflächen mit geeigneter technischer Infrastruktur zur Wiederherstellung der betroffenen Geschäftsprozesse. Durch die Finanzkrise ab 2007/2008 entstanden jedoch überraschend freistehende Bürokapazitäten, deren Nutzung als Ausweicharbeitsflächen möglich wurde (Rose 2011: 98).

[274] "Historically, terrorist attacks have been considered low risk, because their likelihood was considered rare even though their consequences could be catastrophic. Given recent events, however, upgrading their risk rating is reasonable" (Lam 2002: 21).

für die Gesellschaft[275] (Homeland Security Council 2007: 26), aber auch der Unternehmen mit Blick auf die Risikokontrolle von möglichen Prozessunterbrechungen (Shaw 2004: 23).

5.3.1. Bedeutung von RIA und BIA

Die Entwicklung von BCM und seine Abgrenzung zum reaktiven Grundtenor des Krisenmanagements begann mit der Erkenntnis aus Schadensereignissen wie den Anschlägen vom 11. September 2001, dass die Kompensation der beschädigten oder ausgefallenen Ressourcen nur schwerlich ohne vorherige Analyse und Vorbereitung durchzuführen ist (Lam 2002: 21). Daher wurde eine methodische Weiterentwicklung durch die Unterscheidung zwischen der Risikobewertung von Ressourcen und der Kritikalitätsanalyse von Prozessen angeregt (BS25999). In ersterer werden Szenarien und ihre Auswirkungen auf die Verfügbarkeit von Ressourcen sowie die Wahrscheinlichkeit ihres Eintretens nach traditionellem Risikoverständnis betrachtet (Business Impact Analysis). Ressourcen in diesem Kontext sind die Verfügbarkeit von Gebäuden, Personal und der technischen Infrastruktur, mit fortschreitender Digitalisierung natürlich mehr und mehr die IT-Infrastruktur. Erkenntnisse aus der Abhängigkeit von unterbrechungsfreien Lieferketten, beispielsweise im produzierenden Gewerbe, fügten der Liste darüber hinaus die Verfügbarkeit von externen Dienstleistern hinzu (Torabi, Soufi und Sahebjamnia 2014: 310). Hingegen werden mithilfe der Methode des „Risk Identification and Assessment“ (RIA) mögliche Schadensszenarien und deren Wahrscheinlichkeit ermittelt, welche zu einer Geschäftsunterbrechung führen könnten (Behnezhad, Connett und Nair 2013: 82). Unter Einbeziehung von präventiven Schutz- und Kontrollmaßnahmen wird anschließend das residuale Restrisiko bestimmt und gegen den Risikoappetit des Unternehmens, sprich seine Bereitschaft zur Kontrolle oder Akzeptanz von Risiken abgewogen (Linkov et. al. 2013: 472). Das Ergebnis repräsentiert daher einerseits eine Liste kritischer Prozesse, deren Wiederherstellung von vitaler Bedeutung für das Unternehmen ist und eine Übersicht über die speifischen Risikokategorien andererseits, welche potentiell zu einer Unterbrechung von kritischen Prozessen führen können.[276]

[275] Es ist wichtig an dieser Stelle anzumerken, dass der Begriff „nationale Resilienz“ im US-amerikanischen Sprachgebrauch (Homeland Security Council 2007) und später auch in anderen Ländern Einzug fand. Darunter wurde die Widerstandskraft des Staates und der Gesellschaft verstanden, auf unvorhergesehene Ereignisse wie Terroranschläge oder Naturkatastrophen zu reagieren (Voss und Dittmer 2016: 179). Dieser Begriff deckt sich allerdings nicht vollständig mit dem in dieser Arbeit verwendeten Resilienzbegriff, da sich letzterer auf die Risikokontrolle in Unternehmen erstreckt und die Mittel und Methoden unternehmerischer Sicherheitsproduktion wie unter anderem BCM und ITSCM erstreckt.

[276] In den Fällen von niedriger Frequenz und hohem Schadenswert ist die subjektive Risikobewertung besonders auffällig. Denn wenn nur eine überschaubare Menge an Erfahrungswerten vorliegt, ist eine Entscheidung über die angemessene Risikobewertung auf der Grundlage rein objektiver Fakten problematisch. In diesen Situationen liegt es häufig an individuellen Vorprägungen, welche Entscheidung getroffen wird. Insbesondere wenn das Risikoszenario kaum bekannt ist, stehen Unternehmen und Risikogremien vor großen Herausforderungen die

Dieser in unserem Verständnis traditionelle, risikobasierte Ansatz entstand aus den Erfahrungen des 11. Septembers und intendierte die Identifikation von Risiken in ein strategisches Managementprogramm einzubeziehen. Dies betraf vor allem Risiken die bis dato unterschätzt wurden, darunter insbesondere solche mit niedriger Frequenz und hohem Schaden (LaPorte 2007: 61). Es wurde zudem attestiert, dass die Risikofunktion die Rolle der Risikokommunikation ausdehnen sollte, um Aufmerksamkeit und Zustimmung für BCM-Maßnahmen in allen Bereiche des Unternehmens erzeugen zu können (Braes und Brooks 2010: 17). Ferner wurde durch die Business Impact Analysis (BIA) die Rolle der Prozess- und Ressourcenverantwortlichen gestärkt und deren Expertise in den Planungsprozess eingebunden. Dadurch sollten die kritischen Prozesse gedanklich und planerisch von den Arbeitsschritten differenziert betrachtet werden, welche im Fall einer Geschäftsunterbrechung nicht die Zukunft des Unternehmens gefährden würden und folglich nicht im Zentrum der Vorsorgeplanung stehen sollten.[277] Die Kritikalität von Prozessen definiert sich folglich erstens durch den Schaden, der im Falle seines Ausfalls für das Unternehmen als Ganzes entstehen würde, beispielsweise einen signifikanten Umsatzeinbruch bewirken könnte. Zweitens ist die Zeit relevant, die zwischen Ereignis und tatsächlichem Eintreten des negativen Effekts liegt, um die Sequenz der Wiederherstellung zu planen (Bonafede, Cerchiello und Giudici 2007: 95). Betrachten wir daher zunächst die Bewertung des Schadens durch die Geschäftsunterbrechung im Detail.

Der potentielle Schaden durch den Ausfall eines Prozesses kann einerseits (1) finanziell quantifiziert werden. In dieser Schadenskategorie werden die direkten Verluste aus Umsatzeinbrüchen, Kosten durch den Ausfall von Systemen (Datenbanken, Kühlsystemen) und quantifizierbarer Schadensforderungen (Konventionalstrafen, Rechtsansprüchen, Geldstrafen) erhoben (Lam 2002: 21). Auf der anderen Seite gibt es Prozesse, wie beispielsweise die Schadensbearbeitung in einer Versicherung oder die Gehaltszahlung an Mitarbeiter, welche im Falle einer Unterbrechung sogar einen kurzfristig positiven Effekt auf die Unternehmensbilanz

Wahrscheinlichkeit seines Eintretens angemessen zu bewerten, ohne alle erdenklichen Bedrohungen gleichermaßen hoch einzustufen: „Too often warnings are imprecise, which was why Condoleezza Rice, as national security adviser at the time of 9/11, dismissed the warnings of a terrorist attack using airplanes. The warnings did not specify the time and place. Many warnings are, in fact, so general as to be useless, e.g., nuclear power is dangerous' or 'radical Moslems will strike the United States'" (Perrow 2011: 48).

[277] Die BIA erlaubt den Fokus auf die kritischen Prozesse zu richten und die begrenzten Ressourcen zielgerichtet einzusetzen. Grundsätzlich ist die Annahme zu treffen, dass alle Prozesse einer gewinnorientierten Organisation einen Mehrwert erbringen, ansonsten wären sie längst Spar- und Effizienzprogrammen zum Opfer gefallen. Kritikalität beziffert aber hingegen ein Produkt aus potentiellem Schaden und der Zeit, die verstreichen kann bis dieser Schaden durch die Nicht-Verfügbarkeit des Prozesses entsteht. Diese Kombination macht die BIA in Verbindung mit der vorausgehenden RIA zu einem probaten Mittel der Risikosteuerung (Torabi, Soufi und Sahebjamnia 2014: 310).

hätten. Denn wenn keine Versicherungsansprüche bearbeitet werden und keine Löhne gezahlt werden können, spart der Konzern durch den Ausfall der Schadensregulierung kurzfristig Ausgaben. Doch weil dies langfristig zum Verlust des Kundenbestandes und von Mitarbeitern führen kann, sind auch nicht-materielle Kategorien für die Durchführung der Kritikalitätsanalyse gefragt (Torabi, Soufi und Sahebjamnia 2014: 310).

Während der ethnographischen Untersuchung wurden interessante Beobachtungen zur finanziellen Schadensdimension gemacht. Während einer *Business Impact Analysis* in einer südeuropäischen Landesgesellschaft im November 2016 lehnten Prozessverantwortliche die Berechnung eines monetären Verlustszenarios mit Verweis auf die mangelnde Vergleichbarkeit zwischen den Prozessen ab.[278] Die Argumentation der Beteiligten besagte, dass beispielsweise die Unternehmenskommunikation keine direkten finanziellen Verluste im Fall einer Unterbrechung generiere, anders jedoch im Vergleich zur Vertriebsabteilung. Dennoch habe die Kommunikationsfunktion konkrete Auswirkungen auf die Außenwirkung des Unternehmens im Falle ihres Ausfalls. Auch andere Bereiche verwiesen auf die Komplexität und Interdependenzen der Prozesse, in deren Folge auch nicht-finanzielle Aspekte der Unterbrechung des Geschäftsbetriebs einbezogen werden sollten. Diese Erkenntnis resultierte in der gleichwertigen Betrachtung aller vier Schadenskategorien, welche im Folgenden weiter vorgestellt werden.

Zweitens ist daher die (2) operationelle Anhängigkeit des Prozesses zu anderen Prozessen und Funktionen zu betrachten und relevante Interdependenzen zu identifizieren. Die operationelle Abhängigkeit im Fall der IT-Infrastruktur ermöglicht beispielweise die Bereitstellung von Datenbanken, Applikationen und gespeicherten Informationen, auf die kritische Prozesse zurückgreifen. Drittens sind (3) regulatorische Anforderungen relevant, welche sich nach den jeweiligen Rechtsräumen richten (Gaycken und Karger 2011: 7). Potentielle Maßnahmen der Aufsichtsbehörden für den Fall einer Prozessunterbrechung sind ebenso zu betrachten wie Strafzahlungen und der potentielle Entzug von Betriebslizenzen.[279] Viertens ist der mögliche (4) Reputationsschaden bei Kunden und Geschäftspartnern durch eine Prozessunterbrechung

[278] Die hier beschriebene Darstellung basierte auf der Auswertung von 21 Interviews zur BIA in einer Landesgesellschaft im Jahr 2019, in deren Rahmen die kritischen Prozesse im Rahmen eines Projekts nach der neuen BIA-Methodik der Unternehmenszentrale ermittelt werden sollten.

[279] In einem expliziten Fall aus Polen besteht das Risiko, dass im Fall einer Geschäftsunterbrechung von mehr als 48 Stunden die Vertriebslizenz für Automobilversicherungen über einen Zeitraum von zwölf Monaten entzogen werden kann. Diese besondere Strafmaßnahme soll die Ausstellung und Verlängerung von Motorhaftversicherungen sicherstellen. In einem Gespräch mit einem polnischen BCM Officer aus dem September 2015 wurde diese Maßnahme als maßgeblicher Grund für die Kritikalität der Policen-Ausstellung im Motorversicherungsbereich genannt.

zu beachten. Solche nicht-materiellen Schäden können zumeist nicht angemessen in monetären Begriffen beschrieben werden. Der Ausfall des Kundenkontaktzentrums oder der generellen Leistungserbringung, welche der Kunde unmittelbar wahrnimmt können die Reputation des Unternehmens nachhaltig schädigen (Power et. al. 2009: 302).

Nach Auswertung der kritischen Prozesse anhand der obigen Schadensdefinitionen ist die maximal tolerable Ausfallzeit („Maximum Tolearble Period of Disruption“ - MTPD) zu bestimmen, also die Zeitspanne nach deren Ablauf der Schaden für das Unternehmen nicht mehr vertretbar ist (Böhmer, Brandt und Groote 2009: 3). So betonen die Industriestandards zu BCM, dass “According to the BS25999 and ISO22301 terminologies, the MTPD measure for each key product is briefly defined as the time interval after a disruption by which the disrupted functions should be resumed (…)” (Torabi, Soufi und Sahebjamnia 2014: 313). Davon zu unterscheiden ist die Zeitangabe der *Recovery Time Objective* (RTO), welche den spätest-möglichen Zeitpunkt[280] für den Beginn von Prozeduren zur Wiederherstellung der Prozesse festlegt (Lam 2002: 21). Auf der Grundlage der Ergebnisse aus RIA und BIA können Business Recovery Plans (BRPs) erstellt und geeignete Maßnahmen ergriffen werden, um die geschäftsgefährdenden Risiken zu steuern.

5.3.2. Nicht-Verfügbarkeit von Gebäude

Im Fall der Anschläge vom 11. September 2001 zeigte sich zudem, dass die ad-hoc Krisenbewältigung oder Versicherung der Geschäftsunterbrechung aus zwei Gründen als angemessene Risikokontrolle ausschieden. Erstens wäre das notwendige Kapital zur Wiederherstellung des versicherten Objekts im Fall eines vergleichbaren Großereignisses auf dem Versicherungsmarkt nur bis zu einer gewissen Grenze abrufbar. Doch Schadensfälle von der Größe des zerstörten World Trade Centers oder eines Anschlags auf ein Atomkraftwerk sind nicht von einer Versicherung alleine zu tragen (Sarewitz et. al. 2003: 806). Daher versichern Erstversicherer ihr Risiko, zumindest das Übersteigen eines bestimmten Grenzwertes („excess of loss“) für den Fall eines außergewöhnlichen Versicherungsfalls bei Rückversicherungen. Diese wiederum verteilen die potentielle Last auf mehrere Schultern, um einen seltenen Schadensfall dieser Größenordnung ausgleichen zu können (vgl. Norio et. al. 2011: 36). Fraglich ist nur ob in einem solchen Fall Rückversicherungsunternehmen, selbst vernetzte Gemeinschaften von unterschiedlichen Risikoträgern, in der Lage wären den

[280] Naturgemäß sollte der RTO-Wert kleiner ausfallen als die MTPD. Auch im Fall der benötigten Zeiteinheit ist auf die angemessene Definition von Grenzwerten zu achten. Falls sich ein relevanter Schaden durch den Prozessausfall erst nach mehreren Wochen abzeichnet, ist dieser Prozess nicht zwingend für die weiteren Schritte des BCM Prozesses zu beachten (Böhmer, Brandt und Groote 2009: 3).

notwendigen Ausgleich innerhalb der gegebenen Zeit zu zahlen.[281] Zweitens sind die indirekten Folgen einer Geschäftsunterbrechung nicht zu versichern. Der Reputationsschaden, das verlorene Vertrauen von Kunden und Geschäftspartnern oder die Implikationen für die Marktposition und Wettbewerbssituation können gravierende Folgen für das Unternehmen haben (Jüttner 2005: 128f.). Kunden hätten kurzfristig sicherlich Verständnis für eine vorrübergehende Notlage, insbesondere angesichts von Extremsituationen. Doch diese Nachsicht hält zumeist nicht über einen längeren Zeitraum an, insbesondere wenn die Kunden auf die Bereitstellung der Güter oder Dienstleistungen des Unternehmens angewiesen sind (Wasserversorgung, Auszahlung von Versicherungsschäden, Telekommunikationssysteme usw.), die Kundenbindung schwach ausgeprägt ist oder der Markt hochkompetitiv ist (Asnar und Giorgini 2008: 217). Daher erscheint die Vorsorgeplanung für eine mögliche Geschäftsunterbrechung die bessere Alternative zur Risikomitigation.

Nach den Anschlägen dominierte 2001 das Szenario eines Verlusts der Bürofläche die BCM-Methodik als wahrscheinlichste Schadensursache (Lam 2002: 23). Das produzierende Gewerbe hatte in dieser Hinsicht einen Erfahrungsvorsprung, da Fabriken mit investitionsintensiven Maschinen und Anlagen durch Streiks oder Unwetter vorrübergehend nicht verfügbar sein können. Für diesen Fall wurden hier bereits Methoden zur Kontinuitätsplanung in der Versorgungskette mit entsprechenden Redundanzen entwickelt (Jüttner 2005). Die Erfahrung lehrte, dass neben dem Vorhalten einer Alternativlokation auch mit erheblichen Widrigkeiten zu rechnen ist, da etwa die Verlagerung der Prozesse an den alternativen Standort durch die Verkehrssituation oder Zugänglichkeit des betreffenden Gebietes problematisch sein könnte.[282] Eine weitere Variable betrifft die aus der kritischen Infrastruktur bezogenen Leistungen, wie etwa die unterbrechungsfreie Stromversorgung.[283] So produziert „[e]ine Abschaltung der

[281] Der Umfang des entstanden Schadens war weder mit den gängigen Methoden der Risikoabschätzung vorhersehbar, noch wäre der Versicherungsumfang rechtzeitig und im notwendigen Umfang durch übliche Auszahlungsmodelle ohne Unterstützung von staatlicher Seite zu bewerkstelligen (Rose 2011: 98).

[282] Die Einschränkungen im öffentlichen und privaten Verkehr beispielsweise können ein prinzipiell verfügbares Gebäude dennoch unbrauchbar machen. Der Ausfall der Transportkapazitäten kann sich negativ auf die Produktionsbedingungen in einer Stadt und der hier beheimateten Unternehmen auswirken (Rodriguez und García-Palomares 2014: 50). Nach dem 11. September waren viele Straßen in Manhattan gesperrt, der öffentliche Nahverkehr über die Halbinsel stark eingeschränkt und selbst die Bürgersteige waren nicht passierbar (Mendonça und Wallace 2006: 261). Somit zeigte sich, dass ein intaktes Gebäude unter Umständen ohne direkte Beschädigung nicht verfügbar sein kann, wenn der Zugang dorthin versperrt ist.

[283] Vorsorgemaßnahmen wie Dieselgeneratoren bieten eine Kompensation für kurzfristige Unterbrechungen indem sie mit der Unterstützung von Akkumulatoren die Spannung und Versorgung über einen bestimmten Zeitraum aufrechterhalten können. Die Erzeugung und Verteilung in Deutschland unterliegt einem grundlegenden Wandel durch die Energiewende, an deren Ende Strom aus erneuerbaren Energiequellen als neue Systemkomponenten in das Gesamtnetz inkorporiert werden muss und im Fall einer unzureichenden Synchronisation der Komponenten und Absprache zwischen den verschiedenen beteiligten Akteuren zu einem längerfristigen Stromausfall führen könnten (Neumann, Moorfeld und Reulke 2016: 143). Die zunehmende Komplexitätssteigerung des

Stromversorgung (…) auf Grund der dichten Abhängigkeit von Strom (…) bereits nach 24 Stunden einen Abfall aller Leistungen“ (Gaycken und Karger 2011: 4). Daher wird ein Stromausfall weiterhin als eigenständiges Bedrohungsszenario[284] und potentieller Auslöser für einen BCM Fall genannt (BCM Academy 2016: 29).

Die Planungen für einen Ausweichstandort sollten folglich mehrere Parameter bedenken. Die Auswahl des alternativen Gebäudes muss die individuellen Kriterien der zu verlagernden Prozesse erfüllen (Ward 2003: 16), wie spezielle Maschinen, Konfigurationseinstellungen, die Anzahl von Arbeitsplätze oder deren Ausstattung. Abgesehen von den für den Wiederanlauf benötigten Ressourcen, ist die grundsätzliche Natur eines oder mehrerer Ausweichstandorte in der BCM Strategie festzuhalten, beispielweise durch einen Nutzungsvertrag mit kommerziellen Anbietern.[285] Als Alternative gelten andere Niederlassungen der gleichen Unternehmensgruppe, in denen Schulungs- oder Besprechungsräume mit weiteren Hardwarekomponenten ausgestattet werden, um im Notfall als Ausweichfläche zu dienen.[286] Ein Problem für viele Unternehmen stellt die Tendenz dar, die Überwindung der unmittelbaren Krise in den Vordergrund zu stellen, ohne dabei die langfristigen Folgen eines Ausfalls zu beachten. Denn nach der Verlagerung an einen Ausweichstandort müssen die kritischen Geschäftsprozesse gegebenenfalls von dort über einen längeren Zeitraum unter Einbeziehung komplexer Schnittstellen zu anderen Funktionen oder externen Partnern durchgeführt werden. Dieser Aspekt wurde von vielen Autoren und Praktikern[287] in der Vergangenheit vernachlässigt (Sahebjamnia et. al. 2015: 262).

Stromnetzbetriebs und der IT-basierten Steuerung kann als ein weiterer Grund für die Ausfallbefürchtungen gegenüber der Stromversorgung gesehen werden (Klick und Andruschak 2014: 90f.).

[284] Der Dieselgenerator benötigt nach Verbrauch der vorgehaltenen Menge Diesel weitere Zufuhren. Dies könnte sich aber als Problem herausstellen, wenn die Straßen beispielsweise nicht passierbar sind, die Leitungen zum Dieseltank beschädigt oder die Pumpen an der Tankstelle elektrisch betrieben sind. Eine Studie der TU Berlin zeigte, dass nur ein kleiner Teil der etwa 14.000 zivilen Tankstellen in Deutschland über eine stationäre oder mobile Notstromversorgung verfügt und die Bereitstellung von Kraftstoff an den Tankstellen im Fall einer längeren Stromunterbrechung stark eingeschränkt wäre (TU Berlin 2012: 6).

[285] Im Allgemeinen gibt es drei preislich abgestufte Modelle, welche sich allerdings in ihrem Preis-Leistungsverhältnis deutlich unterscheiden. Modell 1 sichert dem verlagernden Unternehmen maximale Sicherheit zum entsprechenden Preis zu. Die feste Anzahl an konfigurierten Arbeitsplätzen bleibt ausschließlich dem Kunden vorbehalten. Modell 2 reserviert Arbeitsflächen für mehrere Kunden und garantiert gleichzeitig, dass keines dieser Unternehmen aus dem gleichen Stadtteil kommt. Das Modell 3 ist als günstigste Variante auch die unsicherste. Hier werden Arbeitsplätze an mehrere Kunden vermietet. Falls ein Ereignis mehrere Kunden gleichzeitig betrifft, erhalten diejenigen die Arbeitsplätze, die die Büroflächen nach ihrem Eintreffen zuerst beziehen können.

[286] Eine Variation dieser Methode ist der designierte Verdrängungsarbeitsplatz. In diesem Fall werden Mitarbeiter aus nicht-kritischen Prozessen am Ausweichstandort nach Hause geschickt und überlassen ihren Arbeitsplatz den Notfallteams der migrierenden Prozesse. Die Entwicklung von virtuellen Desktops, deren Daten und Anwendungen über eine Cloud gesteuert werden, hat als neueste Variante den Prozess der Strategieentwicklung erweitert. In diesem Fall können Mitarbeiter ihre gewohnte Benutzeroberfläche von jedem beliebigen Punkt aus über öffentliche oder – bevorzugt – private Endgeräte verwenden.

[287] Als Teilnehmer bei Krisenstabsübungen und aus Gesprächen über Erfahrungen aus tatsächlichen Krisen im Rahmen dieser Arbeit stellte sich die Erkenntnis heraus, dass die Überwindung der unmittelbaren

Die Rückkehr zum Normalbetrieb ist das eigentliche Novum und Unterscheidungsmerkmal vom reinen Krisenmanagement. Letzteres strebt allein die Überwindung der akuten Notlage vor einem kurzen Zeithorizont an, BCM hingegen eine langfristige Transition der Prozesse bis zur vollständigen Wiederherstellung des Status Quo. Zu diesem Zweck ist die Ausarbeitung von Wiederherstellungsplänen (Business Recovery Plans – BRPs) wichtig, welche die Prozeduren zum Wiederanlauf eines Notfallbetriebes beschreiben und langfristig die Rückkehr in einen Normalbetrieb erlauben (Cerullo und Cerullo 2004: 71). Die Qualität der Pläne kann sich ebenfalls positiv auf die Kalkulation der Versicherungsprämien auswirken und als Referenz für Kundenanforderungen dienen (IFAA 2020: 2). Seit dem 11. September erkannten Versicherungen die Auswirkungen von großflächigen Schadensereignissen und verlangten in der Folge qualitative und aktualisierte BRPs von ihren kommerziellen Versicherungsnehmern (Jüttner 2005: 128f.). Der Inhalt eines Plans sollte sich nach seinem Zweck und der jeweiligen Zielgruppe richten. Ein BRP für einen kritischen Prozess sollte in Zusammenarbeit mit den potentiell betroffenen Fachabteilungen geschrieben werden und in klarer, einfacher Sprache die Rollen und Verantwortungen sowie jeweiligen Aufgaben dokumentieren.[288]

Zudem ist zu beachten, dass die Pläne Handlungsanweisungen für eine Ausnahmesituation beschreiben und daher sollte ihre Nutzung so intuitiv und verständlich wie möglich gestaltet sein und von den Beteiligten geübt werden, um deren Umsetzung unter erhöhten Stressbedingungen sicherzustellen (Sahebjamnia, Torabi und Mansouri 2015: 261). Ebenfalls zeigte sich durch die Betrachtungen von Schadensereignissen, dass Übungen und Fortbildungen für die Mitarbeiter regelmäßig durchgeführt werden müssen, um den gewünschten Effekt im Kontinuitätsmanagement zu erzielen (Lam 2002: 23f.). Die Lehren und Erfahrungen aus diesen Übungen erhöhen zudem die Qualität der Pläne und schärfen das Bewusstsein auf Seiten der beteiligten Mitarbeiter, wie sie sich in einer Krise verhalten sollten, um das beste kollektive Ergebnis[289] zu erzielen (Schintler et. al. 2007: 295).

Prozessunterbrechung häufig erst der erste Schritt zu einer erfolgreichen Wiederherstellung der Prozessverfügbarkeit ist, dem sich ein längerer Zeitraum anschließt, bis der Normalzustand wiederhergestellt ist. Dies wird in vielen Fällen von den Entscheidungsträgern unterschätzt.

[288] Viele Änderungen die zumeist der Fluktuation der Mitarbeiter oder organisatorischer Veränderungen verschuldet sind, werden erst in der Anwendung der Pläne ersichtlich. In einer Studie nach den Anschlägen vom 11. September ließen 42,6 Prozent der befragten Einwohner New Yorks verlautbaren, dass sie im Fall eines ähnlichen Ereignisses auf Anweisungen durch die Autoritäten warten würden. 34,4 Prozent äußerten hingegen, dass sie selbstständig die Flucht ergreifen würden, um Schutz zu suchen (Boscarino et. al. 2006: 511). Tests können helfen der natürlichen Verunsicherung der Mitarbeiter entgegenzuwirken, den initialen Schock zu überwinden und in einen koordinierten Prozess des Wiederanlaufs überzugehen.

[289] Auch im Fall der nationalen Risikovorsorge und Krisenplanung spielen Kommunikation und Übungen eine relevante Rolle, wie beispielsweise in Form von Erdbebenübungen oder Evakuierungssimulationen für Extremsituationen. Die beständige Wiederholung und Kommunikation können helfen unerwünschte und selbstgefährdende Effekte zu reduzieren (Boscarino et. al. 2006: 512).

Zusammenfassend lässt sich festhalten, dass der 11. September 2001 das subjektive Sicherheitsgefühl stark veränderte. Die Perspektive auf unbekannte oder seltene Risikoszenarien wurde durch die Anschläge zu einem der wichtigsten Faktoren für einen Strategiewechsel vieler Unternehmen hinsichtlich ihrer Kontrolle von Risiken, welche die Kontinuität von Prozessen und Kommunikation betreffen können. Die Bilder des Anschlags und die damit verbundenen Probleme für die Fortsetzung der Geschäftsprozesse führten die Verwundbarkeit der eigenen Existenzgrundlage vor Augen. Daraus entstand die Entscheidung in vielen Branchen, selbstständig für die Eventualität einer Geschäftsunterbrechung Vorbereitungen zu treffen. Mithilfe methodischer Weiterentwicklungen wie der BIA und RIA wurde es möglich die begrenzten Ressourcen für die kritischen, das bedeutet für die Existenz des Unternehmens essentiellen Prozesse einzuplanen. Ebenso zeigen Übungen, dass klare Verantwortlichkeiten, Konditionalprogramme sowie deren Kommunikation in das kollektive Gedächtnis eingehen müssen, um ihren Zweck erfüllen zu können. Mit Rückgriff auf Luhmann bedeutet dies, dass die entscheidende Problematik in der Erinnerung solcher Programme liegt. Denn „[s]ie müssen erinnert und gegebenenfalls rasch aktualisiert werden können, auch wenn sie nie angewandt werden“ (Luhmann 2000: 271). Die gleiche Formel gilt für die Implementierung einer erfolgreichen Krisenvorsorge und Risikokontrolle durch BCM. Im Folgenden wollen wir uns einem weiteren bedeutendem Schadensfall widmen, der wesentlich zur Bewusstseinsbildung regionaler Auswirkungen von Gefahren und der Problematik der Abhängigkeit von Dienstleistern beigetragen hat.

5.4. Fallbeispiel 2 - Ausfall von Dienstleistern – Fukushima 11.03.2011

Wie das vorausgehende Fallbeispiel zeigte, richtete sich der Schwerpunkt der unternehmensinternen Sicherheitsproduktion durch BCM und KM zu Beginn des 21. Jahrhunderts auf die räumliche Dimension der Ressourcenverfügbarkeit in Form der Sicherstellung von nutzbaren Arbeitsflächen. Die Fukushima-Krise aus dem Jahr 2011 erweiterte diese Logik um die Dimension der globalen Wertschöpfungskette einschließlich interner und externer Prozessbeteiligter. Dies hatte insbesondere Einfluss auf das Selbstverständnis von Unternehmen mit Blick auf ihre organisationale Abgrenzung, Wertschöpfungskette und der Interdependenzen zu anderen Organisationen, wenn kritische Prozesse aufgrund einer zurückliegenden Entscheidung ausgelagert worden waren und sich somit der unmittelbaren Risikokontrolle entzogen. Diese Problematik soll im Folgenden durch das Reaktorunglück von Fukushima verdeutlicht und zudem die Weiterentwicklung der traditionellen Risikokontrolle im analogen Zeitalter durch eine weiterreichende Betrachtung von Risiken und Schadensdimensionen im Zuge dieses Ereignisses aufgezeigt werden.

Am 11. März 2011 ereignete sich ein Seebeben etwa 77 Kilometer vor der japanischen Ostküste. Es galt als das bisher viertgrößte Erdbeben weltweit seit Beginn der Dokumentation tektonischer Aktivitäten (Todo, Nakajima und Matous 2014: 210). Ein durch das Hauptbeben ausgelöster Tsunami[290] näherte sich innerhalb von Minuten der Präfektur Fukushima und überflutete das Gebiet bis zu zehn Kilometer landeinwärts (Norio et. al. 2011: 34). Besondere Bedeutung erlangte dieses Ereignis durch die verursachten Schäden am Atomkraftwerk nahe der Präfekturhauptstadt Fukushima und die sich abzeichnenden Gefahr eines Austritts radioaktiver Partikel aus einem der havarierten Reaktoren.[291] Die Hochwasserschutzwälle des Atomkraftwerks, das direkt am Meer gebaut worden war, waren nicht für einen Tsunami dieser Größenordnung konzipiert und versagten ausreichenden Schutz. Das eindringende Wasser beschädigte die Reaktoren, insbesondere Reaktor 4, in dem es zu einer Kernschmelze kam. Der Vorfall wurde nach der internationalen Bewertungsskala für nukleare und radiologische Ereignisse in die gleiche Gefahrenklasse wie der Tschernobyl-Unfall 1986 eingestuft (Hindmarsh 2013: 3).

Die internationale Gemeinschaft war aufgrund der Krise alarmiert und befürchtete einen Absturz des YEN, doch noch größer waren die Zweifel am Erfolg des Krisenmanagements der japanischen Regierung[292] und des ebenfalls sichtbar überforderten Energieunternehmens TEPCO[293] (Norio et. al. 2011: 41). Die Meldungen über ein mögliches Entweichen von Radioaktivität aus Reaktor 4 und eine mögliche Kontaminierung des Landes, einschließlich des globalen Handels- und Wirtschaftszentrums Tokio würde nicht nur eine Katastrophe für das

[290] Schätzungen zufolge erreichte die Flutwelle im Moment des Auftreffens an der Küste der japanischen Hauptinsel Honshu eine Höhe von 24 bis zu 38 Metern. Die zerstörerische Energie des Tsunami richtete an Land schwere Schäden an, dessen Ausmaß der Menge von „9.32 × 1012t of TNT or about 600 million times that of the Hiroshima atom bomb" entsprach (Norio et. al. 2011: 34). Das Erdbeben und der Tsunami kosten etwa 15.000 Menschen das Leben (Hindmarsh 2013: 3). Andere Quellen gehen von 13.392 Verstorbenen aus und sprechen von ungefähr 335.000 Personen ohne Unterkunft und abgeschnitten von der Versorgung mit dem Notwendigsten (Norio et. al. 2011: 34).

[291] Erwähnenswert ist, dass die 11 Atomkraftwerke an Japans Nordostküste laut Norio et. al. nach dem Seebeben automatisch vom Netz getrennt wurden und die Reaktoren in Erwartung des Tsunami heruntergefahren wurden. Nur die Kühlsysteme von Reaktor 4 in Fukushima versagten durch unzureichende Schutzmaßnahmen. Von den vier Stromverbindungen des Kühlsystems waren die beiden überirdischen Leitungen durch den Tsunami zerstört worden und die Verbindung zum Reaktor nach dem Erdbeben getrennt worden. Die verbliebenen Akkumulatoren versagten ebenfalls ihren Dienst, da sie nicht gegen einen Durchbruch der Tsunami-Schutzmauer zusätzlich abgesichert waren (Norio et. al. 2011: 37f.).

[292] Die Reaktionen des Krisenstabs der Regierung in Tokio verliefen unkoordiniert und unterminierten das Vertrauen der Bevölkerung in die Fähigkeiten der Behörden die Krise zu lösen (Ng und Lean 2012: 307). "In the case of Fukushima, there was official denial and secrecy, refusal to accept outside help, the failure to evacuate citizens at risk, and an attempt by the prime minister to halt the cooling of the damaged reactors by seawater shortly after the process had been started" (Perrow 2011: 48).

[293] Der japanische Premierminister erklärte die Situation schließlich in Anbetracht des Ausmaßes zur schlimmsten Katastrophe seit dem Zweiten Weltkrieg und erbat internationale Hilfe durch andere Staaten und NGOs. Gleichzeitig begannen viele Staaten ihre Bürger aus dem nördlichen Teil Japans zu evakuieren und Sicherheitswarnungen für ihre Staatsangehörigen im Großraum Tokio herausgeben (Norio et. al. 2011: 39).

Land, sondern für die gesamte Weltwirtschaft bedeuten (Rose 2011: 99f.). Japan, die drittgrößte Volkswirtschaft der Welt drohte als Markt, Produzent und Lieferant auszufallen. Ein Land das bekannt für den Reifegrad seines Katastrophenschutzes war, drohte für einen Moment zu kollabieren.[294] Neben der Kritik am Krisenmanagement von Regierung und Betreiberunternehmen wurden schwerwiegende Fehler in der Energiestrategie identifiziert, insbesondere in Gestalt der Risikokontrolle durch die Public Privat Partnership mit TEPCO[295] im Vorfeld der Katastrophe (Todo, Nakajima und Matous 2014: 210).

Für die Weltwirtschaft drohte ebenfalls ein bisher für unwahrscheinlich gehaltenes Szenario Realität zu werden. In Folge der Naturkatastrophe waren 190.000 Gebäude in Japan beschädigt und 45.700 vollständig zerstört worden, mit spürbaren Folgen für die inländische Produktion und Transportkapazitäten, sowie für die Abwicklung des globalen Handels im Rest des Landes (Norio et. al. 2011: 34). "The Japanese earthquake (…) revealed just how vulnerable global supply chains have become. Overnight, companies were left without crucial components or raw materials, which dented profits and reputations of companies that were geographically remote from the sites of the actual catastrophes. Business continuity planning suddenly took on new relevance for companies that rely on third party suppliers for their trade to continue" (AGCS 2012: 14). Dies betraf mit Blick auf ausländische MNU vorrangig zwei Aspekte: Im Fall einer Eskalation der Krise, müsste ein (a) Wiederanlauf der in Japan ansässigen Dependancen, Firmen und Fabriken ausländischer Unternehmen unter Umständen außerhalb Japans geplant werden. Eine derartige regionale Ausweichstrategie war größtenteils unbekannt und stellte das Krisenmanagement vor große logistische und kulturelle Herausforderungen (Perrow 2011: 50). So lehnte ein Großteil der in ausländischer Unternehmen beschäftigten japanischen Mitarbeiter eine Evakuierung ab, da sie sich um ihre Reputation sorgten und ihre Heimat nicht verlassen wollten.[296]

[294] Die Erfahrungen Japans mit Erdbeben, Stürmen, Tsunamis und anderen Katastrophen in Kombination mit einem hohen Organisationsgrad waren die Treiber einer umfassenden Sensibilisierung der Bevölkerung, bestehend aus Alarmierungsübungen, automatischer Information der Bürger über SMS und Social Media, Frühwarnsysteme und Katastrophenschutzsimulationen. „Japan also invests heavily in public disaster education, making one of the highest disaster risk aware populations in the world" (Norio et. al. 2011: 40). Doch trotz dieser Vorbereitung scheiterte das Krisenmanagement an unzureichenden Absprachen zwischen Regierung und Kraftwerksbetreiber sowie unentschlossener und inkonsequent geführter Informationspolitik gegenüber der Öffentlichkeit (Todo, Nakajima und Matous 2014: 210).

[295] Dies wurde insbesondere durch die massiven Planungsfehler des Kraftwerks, die organisatorischen Pannen des Betreibers und die mangelhafte regulatorische Pflichtausübung durch die Atomaufsichtsbehörde in Tokio begründet (Ho et. al. 2013: 774).

[296] Aus Gesprächen mit beteiligten Personen aus dem Krisenmanagement in deutschen Unternehmen zeigte sich, dass die emotionale und kulturelle Einstellung ihrer japanischen Mitarbeiter falsch eingeschätzt wurde. Die Bereitschaft im Land zu bleiben, auch aus Sorge um den Gesichtsverlust durch die Evakuierung, wurde aus Sicht des europäischen Krisenmanagement nicht ausreichend beachtet.

Erschwerend kam hinzu, dass (b) viele japanische Unternehmen die einzigen Hersteller essentieller Bauteile für einige Produkte ausländischer Unternehmen waren. Ein signifikanter Teil der Elektronikindustrie war in Japan beheimatet und großflächige Lieferausfälle auf dem globalen Markt drohten in Folge der Katastrophe einzutreten (Todo, Nakajima und Matous 2014: 210). Für diesen Fall mussten Vorkehrungen getroffen werden, um die Abhängigkeit von einzelnen Anbietern zum Schutz vor Lieferausfällen zu reduzieren. Als die Krise nach drei Wochen glücklicherweise ohne weitere Eskalation abklang, zeigte sich Erleichterung, allerdings wurde auch offenkundig, dass Konzepte für eine regionale, das bedeutet über die Stadtgrenzen hinweg planende Fortsetzung von Geschäftsprozessen notwendig wurden. Zudem sollte die Abhängigkeit von Zulieferern und Dienstleistern überprüft wurde. Aus diesen Gründen waren eine Überarbeitung der Risikokontrolle von Lieferketten sowie die Einbindung von Zulieferern in die eigene BCM-Planung von Unternehmen angezeigt (AGCS 2012: 14).

5.4.1. Unerwartete Vermengung der Risikokategorien

Fukushima wurde bald zum Symbol mangelhafter Risikokontrolle (Lansdall-Welfare et. al. 2014: 6). Die Pläne für die Konstruktion potentiell gefährlicher Anlagen wie eines Atomkraftwerkes in den durch Erdbeben frequentierten Gebieten Nordostjapans waren im Allgemeinen Zeichen mangelnder Risikosteuerung (Horst 2012: 43).[297] Doch der eigentliche Fehler in der Risikobewertung war das Außerachtlassen einer möglichen Kombination von Naturereignissen, deren potenziertes Zerstörungspotential größer war, als beide für sich alleine genommen.[298] Durch Mängel in der Planung, Konstruktion sowie ausführende Kontrolle des Atomkraftwerks durch die Betreiberfirma und Aufsichtsbehörden verschlimmerte sich die Krise (Perrow 2011: 46), deren Ursprung auf eine unzureichende Risikoabschätzung des Standorts und der regionalen Risikoexposition zurückzuführen ist (Hindmarsh 2013: 4). „Obviously, a major tsunami was not in the plan of the designer and operator of the plant. This is a serious mistake because these plants are located exactly in the coastal and earthquake-prone region of the country" (Norio et. al. 2011: 40f.).

[297] Die Abhängigkeit Japans von Rohstofflieferungen aus dem Ausland prägten auch seine Energiepolitik, welche in Gestalt der Atomkraft eine Möglichkeit zur Autarkie für die Elektrifizierung seiner wachsenden Wirtschaft bot. Die Ereignisse des Jahres 2011 zeigten hingegen die Kehrseite der unzureichenden Umsetzung dieses Plans (Hindmarsh 2013: 4).

[298] Die Abschaltung der Kraftwerke und der geregelte Übergang in den Notbetrieb wurden ordnungsgemäß durchgeführt und verhinderten effektiv weitere Schäden durch Nachbeben (Norio et. al. 2011: 38). Auch die Gefahr einer Flutwelle war grundsätzlich berücksichtigt und mit Erkenntnissen über ähnliche Ereignisse in der Vergangenheit verglichen worden. Die Gefahr wurde erkannt und anhand von bestehenden Daten in ein Modell zur Risikobewertung überführt, aber dennoch die mögliche Schadenswirkung berücksichtigt (Perrow 2011: 47).

Eine Untersuchung brachte zu Tage, dass nur etwa zehn Prozent der Unternehmen in Japan während der Krise im Normalbetrieb arbeiteten konnten und der Mangel an Rohstoffen und zwischenverarbeiteten Materialen zu enormen Einschränkungen in der Produktivität führte (Todo, Nakajima und Matous 2014: 210). Viele Zulieferer der betroffenen Region im Nordosten von Honshu, deren Beiträge zum Gesamtproduktionsprozess überwiegend im vorgelagerten Bereich zu lokalisieren waren, erlitten Schäden durch die Naturkatastrophen. Die wirtschaftlichen Folgen dieses Ausfalls überstiegen die Erwartungen und Einschätzungen der Schadenswirkung vor der Krise (Norio et. al. 2011: 36). Etwa 90 Prozent der Produktionsstörungen waren unmittelbar durch die Unterbrechung von Lieferketten entstanden, denn abgesehen von der betroffenen Region Fukushima war kaum relevanter Schaden in anderen Landesteilen durch die Naturkatastrophen verzeichnet worden (Todo, Nakajima und Matous 2014: 210) und unterstreicht somit die Bedeutung der Risikokontrolle von Unterbrechungen der Lieferketten.

Somit stellt sich die Frage, welche Folgen diese Krise auf die Vorgaben und Koordination staatlicher Akteure hinsichtlich der Sicherheitsproduktion von Unternehmen hatte? Der Bericht der Internationalen Atomaufsichtsbehörde[299] (IAEA) attestierte dem japanischen Energieministerium eine mangelnde Beachtung der Tsunamigefahr und erklärte, dass das Unglück durch Konstruktionsfehler und einer mangelhaften Risikobewertung[300] durch TEPCO und die nationale Aufsichtsbehörde ermöglicht wurde (Hindmarsh 2013: 8). Die weltweiten Reaktionen auf das Ereignis wurden bald von Fragen bestimmt, welche die Sicherheit der Nukleartechnologie per se anzweifelten. In Deutschland vollzog die Bundesregierung die Kehrtwende ihrer Energiepolitik und kündigte den vollständigen Ausstieg aus der nuklearen Energieerzeugung an.[301] Der Diskurs zirkulierte um die Frage, ob die Erfahrungen aus Tschernobyl und anderer Katastrophen nicht ausreichende Ermahnungen wären, um Technikfolgeabschätzungen zu verbessen und damit die Nutzung von Technologie sicherer machen zu können (Ng und Lean 2012: 307).

[299] Der Bericht der IAEA über die Ereignisse wurde 2015 veröffentlicht und dokumentiert auf 1254 Seiten den Ablauf und die Hintergründe des Desasters (IAEA 2015).

[300] Die unzureichenden Schutzmaßnahmen vernachlässigten insbesondere die mögliche Vermengung eines schweren Seebebens und Tsunamis (Hindmarsh 2013: 8).

[301] Die Unsicherheit über den Umgang mit unbekannten Risiken erhält durch den technologischen Umbruch zu Beginn des 21. Jahrhunderts zusätzlichen Nachdruck. Zwar wurde es geschafft einen großen Teil der zerstörerischen Kraft der Natur zu zähmen oder zumindest durch Vorkehrungen einzudämmen. Doch die eigentlichen zivilisatorischen Risiken der Spätmoderne entstammen dem von Menschen verursachten Spektrum, insbesondere den unbekannten Folgen des technologischen Fortschritts (Beck 1991: 70). Deren Negativpotential unterstreicht die Notwendigkeit für effektive Risikomitigation, transnationale Lösungsansätze und eine effizientere Konzeption der Verantwortungsdelegation zwischen Staat und Privateigentümer kritischer Infrastruktur.

Im konkreten Fall wurde zudem ersichtlich, dass der Betreiber TEPCO die Situation nicht bewältigen konnte und das gemeinsame Krisenmanagement von japansicher Regierung und TEPCO nicht funktionierte.[302] Dieses Scheitern der öffentlich-privaten Partnerschaft wurde in diesem Fall umso bedrohlicher, als dass Japan im schlimmsten Gedankenmodell über etliche Jahrzehnte unbewohnbar geworden wäre (Lansdall-Welfare et. al. 2014). Somit ziehen Norio et. al. in ihrer lesenswerten Darstellung der Ereignisse von Fukushima die folgende Schlussfolgerung: „The severity and unexpectedness of large-scale disasters require a global, synergic, and efficient response system. The response needs to mobilize all available resources, from public and private sectors, affected and unaffected areas, domestic and abroad" (Norio et. al. 2011: 41). Daraus lassen sich deutliche Implikationen für das Modell der Public-Private Partnership ableiten, doch bevor wir auf diesen Punkt genauer eingehen, wollen wir die Bedeutung der Fukushima-Krise für die Einbeziehung der globalen Wertschöpfungskette in Risikokontrollsysteme erörtern.

5.4.2. Globale Produktionsprozesse und Abhängigkeiten

Wie im vierten Kapitel gezeigt wurde, basiert Outsourcing auf dem Konzept, Prozesse und Arbeitsschritte an günstiger operierende oder technologisch spezialisierte Dienstleister auszulagern und somit Wettbewerbsvorteile zu erzielen (Lee, Yeung und Hong 2012: 543).[303] Die entstehende Komplexität aus Waren- und Wissensströme sowie deren Steuerung sind Gegenstand der Betrachtung durch das Supply Chain Management (SCM) oder zu Deutsch der Lieferkettenorganisation (Behnezhad, Connett und Nair 2013: 77). Die damit verbundenen Risiken werden in Unternehmen durch das Supply Chaim Risk Management (SCRM) ermittelt. Letzteres identifiziert und handhabt die Lieferkette betreffenden inhärenten Risiken sowie externe Risiken, welche die Verfügbarkeit der bereitgestellten Waren und Dienstleistungen beinträchtigen könnten (Goh, Lim und Meng 2007: 164f.). Im Allgemeinen können zwei Varianten einer Unterbrechung der Lieferkette[304] unterschieden werden. Der (1) Ausfall von

[302] Die unzureichende Konzeption der Sicherheitsvorkehrungen und Sofortmaßnahmen wird anhand eines Beispiels deutlich: Das durch einen Gebirgszug geteilte Nordjapan verfügt über zwei autarke Stromnetze. Das westliche Gebiet operiert mit einer Stromspannung von 60 Hertz gegenüber einer Normalbetriebsspannung von 50 Hertz im östlichen Gebiet. Beide Netze sind durch zwei Transformationsstationen verbunden, welche allerdings nur in der Lage sind bis zu 1 Gigawatt umzuspannen, also nur etwa 1/8 der benötigten Menge (Norio et. al. 2011: 40). Eine redundante Stromversorgung war daher nicht vorhanden, um den Ausfall der Netzspannung nach einem Großereignis wie 2011 zu kompensieren.

[303] Seit den 1990er Jahren begünstigten einige Faktoren die zunehmende Ausgliederung von Aufgaben. Dazu zählen die Internationalisierung von Märkten und Produktionssystemen, Kostendruck, verschärfter Wettbewerb durch neue Marktteilnehmer und die technologische Spezialisierung von Produkten (Behnezhad, Connett und Nair 2013: 78). Für einige Komponenten wäre es zu kostspielig eine eigene Produktion zu unterhalten, für andere fehlt das technische Wissen (vgl. Rodrik 2001: 6).

[304] Ein Hinweis verdient die Spezifizierung der Begriffe Lieferketten und Netzwerke im Informationszeitalter. Eine Lieferkette im digitalen Umfeld oder „digital supply chain" bezeichnet eine 1:1 Zuweisung von Lieferanten

Produktionskapazitäten auf Seiten des Dienstleisters (AGCS 2013: 2) und (2) die Unterbrechung der Transportrouten (Church et. al. 2004: 493). Beide Varianten fanden Eingang in die Aufgabenbeschreibung unternehmensinterner Risikokontrolle (Todo, Nakajima und Matous 2014: 211) und sollen daher anhand dieser Unterscheidung genauer betrachtet werden.

Die (1) globale Verteilung der Produktionskette, die Reduzierung auf wenige Anbieter in hochspezialisierten Produktsparten und die Minimierung von Lagerbeständen zählen zu den erschwerenden Faktoren eines effektiven SCRM (Roitsch und Meyr 2008: 399), welches im Gegensatz zur ökonomischen Rationalität der Kosteneffizienz steht. Lieferkettenrisiken umfassen qua Definition eine breite Auswahl an Risikokategorien, darunter Lieferausfällen, Kostenveränderungen, Qualitätsmängel, Flexibilitätseinschränkungen oder allgemeine Probleme in der Lieferanten-Abnehmer Beziehung (Lee, Yeung und Hong 2012: 543). Welches Schadenspotential durch unzureichende Kontrolle des Ausfallrisikos besteht, zeigten die Überschwemmungen in Thailand 2011. Im gleichen Jahr wie die Fukushima-Krise unterbrach ein Hochwasser die dortige Produktion von Festplattenkomponenten, die für 45 Prozent der weltweiten Herstellung verantwortlich ist. Die Folgen der Geschäftsunterbrechung einer solchen Fertigungsetappe im globalen Wertschöpfungsprozess führte zu Produktionskostensteigerungen für PC-Hersteller und schlussendlich einen weltweiten Einbruch der Speicherkomponentenproduktion um 30 Prozent im gleichen Jahr (AGCS: 2012: 7). Der Schaden wurde maßgeblich auf eine Konzentration von Arbeitsschritten auf eine Region ohne geeignete Ausweichkonzepte und Produktionsalternativen zurückgeführt (Chongvilaivan 2012: 20).

Das SCRM, hier verstanden als Spezialisierung der unternehmerischen Risikokontrolle mit Bezug auf Dienstleister, hat daher zum Ziel die Risiken eines Ausfalls von organisationsfremden Lieferanten zu steuern. Dazu stehen Flexibilitätsfaktoren in Dienstleistungsverträgen („Service Level Agreement“ - SLA)[305] oder Vorsorgemaßnahmen zur

und Abnehmern, eventuell erweitert um mehrere Ebenen von Sub-Kontrakten. Dahingegen stehen Liefernetzwerke oder „Intertwined supply networks (ISN)“, deren Komplexität durch die interdependente Zuweisung von beispielsweise Komponenten eines Endproduktes durch mehrere Einzellieferanten, deren Sequenz nicht eindeutig linear verläuft und einzelne Schnittstellen im Verlauf eines (digitalen) Produktionsprozesses mehrfach tangiert werden können (Ivanov und Dolgui 2020: 2908). Für die folgenden Betrachtungen werden wir unter einer Lieferkette vorrangig die Beziehung zwischen einem Abnehmer und einem oder mehreren Zulieferern verstehen, um das Prinzip der Organisationsbeschreibung durch Abgrenzung nachzuzeichnen.

[305] Ein SLA kann ohne ausreichende Kontrolle zu Ungunsten des Auftraggebers ausfallen. Bietet der Vertrag keinen Gestaltungsspielraum, sinkt die Wahrscheinlichkeit auf Veränderungen am Markt oder technologische Disruptionen reagieren zu können. Setzt ein Anbieter auf die Bereitstellung einer bestimmten Technologie, welche aber nicht den erhofften Durchbruch liefert oder der Schnelllebigkeit von Trends zum Opfer fällt, entsteht ein „Lock-in“, beispielweise durch „Einschluss“ der Daten auf den Plattformen des Anbieters und eine erzwungene Fortsetzung der Geschäftsbeziehung durch die mangelnde Flexibilität des Vertrages (Bahli und Rivard 2003: 214).

originären Kontrolle des Ausfallrisikos, etwa durch alternative Anbieter (Kahan, Allen und George 2009: 22). Denn trotz vertraglicher Flexibilitätsoptionen sind viele Produktionsprozesse nur im beschränkten Umfang durch einen Wechsel auf andere Anbieter kurzfristig zu ersetzen (Bahli und Rivard 2003: 214).[306] Ein Beispiel soll dies illustrieren: Der globale Produktionsprozess von Computerkomponenten und Halbleitern beispielsweise basiert auf langen Transportwegen. Gleichzeitig erfolgt diese nach internationalen Standards auf einer wöchentlichen Basis und berechnet den voraussichtlichen Bedarf der nächsten Wochen zu den Preisen des volatilen Marktes für Computerchips (Kilger 2008: 392). Abweichungen von der Bedarfsplanung sind kaum möglich, wodurch der Ausfall eines Produzenten auf dem langen Weg der globalen Lieferkette zu erheblichen Komplikationen für den Abnehmer führen kann. Dies zeigte sich am Beispiel des japanischen Halbleiter- und Kontrollelementherstellers Renesas Electronics, dessen Ausfall weitreichende Folgen für die Automobilproduktion hatte.[307] Dieser Fall exemplifiziert die Bedeutung von SCRM, denn etwa 80 Prozent des produzierten Warenwertes der Computerproduktion hängt weltweit von einer kleinen Gruppe von 15 – 20 Zulieferern ab. Gemeinsam mit deren 30 – 40 Subunternehmen bestimmen sie bis zu 95 Prozent der globalen Produktion in dieser Branche (Ebd.: 381).

Die Reduzierung der Risiken erfolgt vorrangig über die Gestaltung des Vertrages mit dem Ziel, die zum Zeitpunkt des Vertragsschlusses unbekannte Faktoren ex post nachbessern zu können (Lee, Yeung und Hong 2012: 543).

[306] Ein anschauliches Beispiel zeigt dies: Die weltweite Produktion von Rohöl wird in den meisten Fällen auf dem Seeweg zu einer der wenigen Raffinerien transportiert, in manchen Fällen zusätzlich vom nächsten Hafen über eine Pipeline landeinwärts gepumpt. Allein der Beschaffungszeitraum des Rohprodukts erstreckt sich auf zwei bis acht Wochen. Würde es zu einem Ausfall einer Produktionskomponente kommen, wären keine Ausweichkapazitäten ad-hoc verfügbar. Die Globalität des Förder- und Veredelungsprozesses und die einhergehenden langen Transportwege erschweren zudem die Substituierbarkeit unterbrochener Elemente der Lieferkette (Roitsch und Meyr 2008: 401). Abhängig von der Rohölsorte können Raffinerien nur bestimmte Endprodukte herstellen, darunter Diesel, Benzin, Kerosin oder Heizöl. Zuletzt sind die Kapazitäten der Raffinerien stets ausgelastet und Erweiterungen der Produktion, beispielsweise falls eine Raffinerie ausfällt, sind aufgrund technischer Schwierigkeiten nur mit langen Vorlaufzeiten und Investitionen möglich (Ebd.: 399).

[307] Das Unternehmen Renesas verfügte 2011 über einen Anteil von 44 Prozent am Weltmarkt für Automobilkontrollchips. Das Erbeben von 11. März 2011 beschädigte das Hauptwerk in der Präfektur Ibaraki, eine Region zwischen dem Großraum Tokio und Fukushima. Der entstehende Produktionsausfall bedeutete eine ernsthafte Krise für Renesas, aber ebenso für seine Hauptabnehmer auf dem asiatischen und US-amerikanischen Markt, allen voran die Automobilbranche. Der drohende Lieferausfall war aufgrund der hohen individuellen Spezifikationen der Produkte nicht kurzfristig durch andere Anbieter auszugleichen. Somit entschlossen sich einige der betroffenen Automobilkonzerne dem strauchelnden Halbleiterhersteller zu helfen und insgesamt 80.000 Manntage in die Wiederherstellung der Produktion zu investieren. Diese Zahl entspricht der Monatsarbeitsleistung von 2.500 Mitarbeitern. Durch diese improvisierte Zusammenarbeit zwischen Produzenten und Kunden war eine späte, aber immerhin erfolgreiche Wiederherstellung der Produktionsprozesse möglich (Todo, Nakajima und Matous 2014: 220). Der Hintergrund dazu ist, dass die Computerindustrie ein materialabhängiger Wirtschaftszweig ist, in dessen Produktionsprozess die Verfügbarkeit einzelner Komponenten die Engpässe der Herstellung bestimmen. Komponenten wie Lesegeräte, Speicher, Prozessoren oder Platinen werden von einer überschaubaren Anzahl an Zulieferern bezogen, die den Markt hochgradig verdichtet haben (Kilger 2008: 381).

Ein weiteres relevantes Risiko im Kontext des SCRM sind wie bereits angesprochen die (2) Transportrisiken. Diese entstehen durch die Interaktionen mehrerer Hersteller von Zwischenprodukten und der Aufrechterhaltung eines konstanten Waren- und Datenstroms zwischen allen Partnern. Nur der ungestörte Austausch von Waren und Informationen ermöglicht eine effiziente Ausnutzung der Lieferkette (Jüttner 2005: 120). Insbesondere die Verkehrswege zwischen den Produktionsstandorten überbrücken häufig mehrere tausend Kilometer auf Frachtschiffen[308] oder an Bord von Flugzeugen. Jedoch unterliegen beide Verkehrsmittel natürlichen Gefahren. So zeigte zum Beispiel die vorrübergehende Sperrung des amerikanischen Luftraums und aller Grenzübergänge nach den Anschlägen vom 11. September 2001 spürbare Schwierigkeiten für Unternehmen auf dem amerikanischen Markt, ihre transnationalen Produktionsprozesse fortzuführen.[309] Der US-Fahrzeughersteller Ford erlitt 2011 einen Produktionsrückgang von 13 Prozent durch die ausbleibenden Lieferungen aus den Werken in Mexiko und Kanada. Toyota musste beispielsweise die unterbrochene Lieferkette für Steuerungssysteme kompensieren, da diese normalerweise per Flugzeug aus Deutschland geliefert wurden (Behnezhad, Connett und Nair 2013: 81). Diese Dimension der Lieferkettenplanung sowie des SCRM erhöhte folglich das Bewusstsein für die Risiken von knappen Lagervorräten und den Folgen von Verzögerungen in der globalen Produktionskette (Goh, Lim und Meng 2007: 166).[310] Im Folgenden wollen wir daher den Blick auf die Erweiterung der zuvor adressierten Verantwortungsdelegation im Kontext globaler Liefer- und Produktionsketten richten.

[308] Auch auf dem Seeweg ereigneten sich Unterbrechungen, etwa nach dem Tsunami von 2004, durch welchen sich die Wassertiefe in der Straße von Malacca von 4.000 Fuß auf 100 Fuß sank und somit für große Transportschiffe unpassierbar wurde (Behnezhad, Connett und Nair 2013: 80) oder der Havarie eines Containerschiffs im Suezkanal im Jahr 2021 (vgl. Handelsblatt 2021).

[309] Die geographische Position eines Lieferanten ist daher Bestandteil der Risikobewertung im Rahmen des SCRM. Neben der Position einer Produktionsstätte und ihrer lokalen Risikoexposition, sollte auch die Transportroute einer näheren Betrachtung unterzogen werden (Church et. al. 2004: 501). Allein der jährliche Warenverkehr in den USA entspricht laut Murray und Grubesic einem Wert von 13 Billionen US-Dollar bei 19 Milliarden Tonnen Frachtgut (Murray und Grubesic 2007: 2).

[310] Ein weiteres Beispiel soll dies verdeutlichen: Der Lufttransport ist naturgemäß nur für kleine und leichte Güter mit hohem Ertrag geeignet, Computerchips beispielsweise. Die Siliziumblöcke, aus denen die Platinen für Halbleiter (Wafer) geschnitten werden, stammen zu 90 Prozent aus China und werden in China, Taiwan und Japan zu polykristallinen Bausteinen für die Chipherstellung veredelt. Ihr Transport erfolgt überwiegend im Luftverkehr, der durch politische oder natürliche Ereignisse stark eingeschränkt werden kann. Der 11. September oder der Ausbruch des isländischen Vulkans Eyjafjallajökull drohten die eng getakteten Lieferketten des Luftfrachtverkehrs in erhebliche Schwierigkeiten zu bringen. Der Vulkanausbruch in Island von 2010 bewirkte, dass über 63.000 Flüge abgesagt wurden und Flughäfen in 23 europäischen Staaten vorübergehend nicht mehr auf dem Luftweg erreichbar waren. In beiden Fällen endete das Flugverbot jedoch rechtzeitig und nachhaltiger Schaden konnte abgewendet werden (Behnezhad, Connett und Nair 2013: 80). Wie das zuvor genannte Beispiel eines Praktikers aus einem anderen DAX-30 Unternehmen zeigte, war der Vulkanausbruch aber ein einschneidendes Ereignis für das Unternehmen und bewirkte eine Steigerung der Investitionen in BCM (Hintergrundgespräch 29.07.2017).

5.4.3. Risikokontrollsysteme und Verantwortungsdelegation

Welche Erkenntnisse sind daraus für die Verantwortung und Risikokontrolle von Unternehmen zu ziehen, deren organisatorische Struktur durch die Schnittstellen und Abhängigkeiten zu Dienstleistern entlang einer globalen Wertschöpfungskette tangiert wird? Eine wesentliche Schlussfolgerung aus der Fukushima-Krise und den Erfahrungen aus anderen Unterbrechungen der Lieferketten ist, dass ein unternehmensinternes Risikokontrollsystem die Identifizierung und Bewertung von geschäftsgefährdenden Risiken nicht auf den Rahmen der organisatorischen Verantwortung begrenzen sollte (Todo, Nakajima und Matous 2014: 220). Indes ist die umfängliche Inklusion relevanter Aspekte der Prozesskontinuität des Unternehmens selbst, seiner Zulieferer und deren Risikostreuung notwendig, um den potentiellen Schaden aus einer Geschäftsunterbrechung zu minimieren und das Risiko kontrollieren zu können. Dazu zählen die politischen und natürlichen Risiken der beteiligten Produktionsstandorte beziehungsweise Transportrouten (Behnezhad, Connett und Nair 2013: 85; Jokobsen 2012: 37), die finanzielle Situation von Dienstleistern[311] (Zsidisn et. al. 2005: 3401), deren Risikokontrollsysteme und interne Vorsorgeplanung zur Prozesskontinuität sowie die Ausgestaltung des Rahmenvertragswerkes der Kooperation (Wüllenweber, Jahner und Krcmar 2008 2008).

Dies bedeutet für Unternehmen, dass der gewählte Umgang mit der sie umgebenden Unsicherheit auf die hier angesiedelten Interaktionspartner, Kunden und vor allem Dienstleister Bestandteil eines Systems zur Kontrolle des Risikos sind. Dies erweitert einerseits den Bezugsrahmen für risikorelevante Entscheidungen und bedeutet andererseits, dass die unternehmensinterne Funktionsstruktur zur Zusammenarbeit mit externen Partnern aufgefordert ist (Lee, Yeung und Hong 2012: 543). Denn die Kontrolle geschäftsgefährdender Risiken, deren Schnittstelle zwischen der routinierten Betriebsorganisation und der Risikomanagementfunktion angesiedelt ist wird durch die Bedeutung globaler Wertschöpfungsketten um Risikokontrollen aus dem Bereich Outsourcing erweitert. Wie eine Untersuchung der Geschäftsunterbrechung japanischer Unternehmen 2011 zeigte, waren über 90 Prozent der betroffenen Fälle nicht primär durch die Naturkatastrophe geschädigt, sondern durch Ausfälle in der Lieferkette unter Druck geraten (Todo, Nakajima und Matous 2014: 210). Daraus resultierte die bis dato jüngste Erweiterung des Ressourcenkanons geschäftsrelevanter Ressourcen um die Bedeutung von kritischen Dienstleistern. Neben Mitarbeitern, Gebäuden,

[311] Die plötzliche Insolvenz eines Zulieferers kann auch zum kurzfristigen Ausfall der Lieferkette führen. Die Risikobewertung des Zulieferers sollte daher auch eine Prüfung der Bilanzen und Risikokapitalrückstellungen einschließen (Jüttner 2005: 120).

IT- und Kommunikationsinfrastruktur gehört die Kontinuität der Lieferkettenfunktionalität zum Repertoire des BCM und unternehmerischer Risikokontrolle mit Blick auf geschäftsgefährdende Risiken (AGCS 2013: 2).

Daran schließt sich die Frage an, welche Maßnahmen Unternehmen mit Blick auf die Sicherheitsproduktion und Kontinuitätsplanung ergreifen müssen, um eine mögliche Unterbrechung der Lieferkette zu bewältigen? Für kritische Zulieferer, das bedeutet dass durch deren Nichtverfügbarkeit Geschäftsunterbrechungen auf Seiten des abnehmenden Unternehmens entstehen können, sollte abhängig von der Spezifikation der gelieferten Waren oder Leistungen Alternativen gesucht werden.[312] Unter Einbeziehung von verfügbaren Alternativherstellern, Transportrouten und –Kapazitäten, sowie der Komplexität des Produkts und dessen Modifikationsextensivität kann die Entscheidung getroffen werden, den Anbieter zu wechseln oder die Vertragsbedingungen einer Revision zu unterziehen (Behnezhad, Connett und Nair 2013: 85). Risikokontrollen sollten nachfolgend harmonisiert und insbesondere die Bedeutung, Priorität und Wiederherstellungszeit (RTO) von kritischen Prozessen angeglichen werden (Brunsdon 2005: 31). Doch auch wenn alternative Dienstleister unter Vertrag sind und die Spezifikationen die Wiederherstellung explizit betitelt sind, ist die Prozessleistung dennoch schneller wiederherzustellen, wenn beide Unternehmen kooperieren. Das bedeutet vor allem eine frühzeitige Benachrichtigung und einen beständigen Kommunikationsfluss während der Krise sicherzustellen (Jüttner 2005: 122). Ferner sollten Mitarbeiter geschult werden und die gegenseitigen Organisationsformen und Ansprechpartner bekannt sein beziehungsweise in den Wiederherstellungsplänen berücksichtigt werden (Kahan, Allen und George 2009: 22). Insbesondere die Kommunikation, welche stets in zwei Richtungen erfolgt, trägt im Krisenfall entscheidend zur Zusammenarbeit zwischen beiden Partnern bei, wie wir bereits im vorausgegangen Fallbeispiel erörtert haben (Ng und Lean 2012: 308).

[312] Dies gilt umso mehr für die Auslagerung von kritischen Kernprozessen. Die Unterscheidung zwischen strategischen, auf unternehmerische Alleinstellungs- oder Steuerungsfunktionen fokussierte Prozesse und taktisch operative Prozesse mit repetitiven, nicht-innovativen Inhalt dient als Grundüberlegung der Vorbereitung der risikoorientierten Entscheidung über die Ausgliederung (Ghodeswar und Vaidyanathan 2008: 25f.). Doch trotz der Häufigkeit von gescheiterten Joint-Ventures und Outsourcing-Projekten, ermangelt die akademische Auseinandersetzung mit der Thematik noch standardisierter Vergleichsstudien, um die Risiken der Lieferkette durch Auslagerungen und komplexe Lieferketten zu analysieren (Lee et. al. 2012: 543) und sollte daher empirisch fortgesetzt werden.

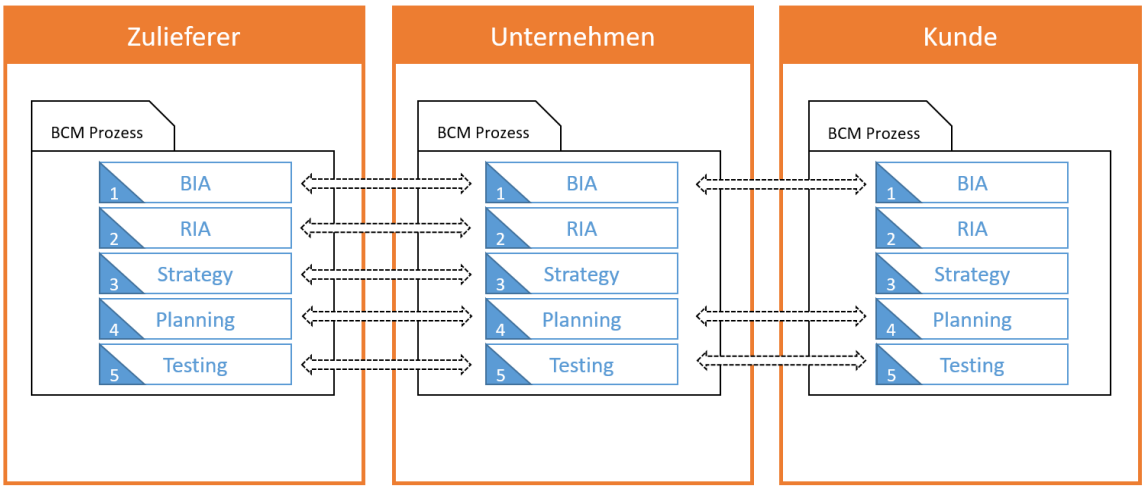

Abb. 5.6. Aufbau einer umfassenden Abdeckung von BCM-Risikokontrollen von Zulieferer, Unternehmen und Kunden. Eigene Darstellung.

Die Implikationen für das Risikokontrollsystem erstreckten sich zudem auf die Betrachtung und Gruppierung von Risikokategorien. Japan verfügte mit Blick auf die gesamtgesellschaftliche Ebene zum Zeitpunkt der Krise eigentlich über einen hochentwickelten Standard in der Krisenvorsorge, basierend auf einer sorgfältigen Risikoauswertung vergangener Ereignisse (Norio et. al. 2011: 40). Doch die Verkettung von unvorhergesehenen Ereignissen wie am 11. März 2011 führten die Fehler in der Vorsorgeplanung und der Risikokontrolle seitens der verantwortlichen Behörden und dem Risikoträger TEPCO vor Augen.[313] Vielmehr hatte das Vertrauen auf die Kontrolle bekannter Risiken in Verbindung mit einer schleichenden Verharmlosung der mangelhaften Risikobewertung und Zusammenarbeit zwischen staatlicher und privater Ebene zum desaströsen Ergebnis geführt, das vor dessen Eintreten keinen Raum im öffentlichen Diskurs[314] über den Umgang mit Unsicherheit in der japanischen Energiepolitik einzunehmen vermochte (Hindmarsh 2013: 4).

Somit stellt sich auch die Frage, was diese Erkenntnis aus dem Unglück von Fukushima für die Zusammenarbeit zwischen staatlicher und privater Ebene mit Blick auf die gesamtgesellschaftlichen Sicherheitsdispositive bedeutet? Die eingangs angesprochene Unterrepräsentation der Rolle von Unternehmen in der Sicherheitsliteratur innerhalb der IB hinsichtlich ihres Beitrages zum Schutz der kritischen Infrastruktur bedarf durch dieses

[313] "At Fukushima, the regulatory authorities required a seawall that was a bit taller than the largest tsunami that locale had experienced in the last 1,000 years. So the danger was, indeed, recognized. But the seawall design was based on probabilistic thinking, not thinking about what is possible, and the seawall was horribly inadequate to the 2011 tsunami" (Perrow 2011: 47).

[314] Die Krise bewirkte hingegen eine breite Diskussion in Fachkreisen und in der Öffentlichkeit, die sich über Japans Grenzen hinweg auswirkte. "After the Fukushima incident, many governments and nuclear operators started to realize the need to understand public perceptions as well as to improve risk communication and emergency messaging (…). Over the past 30 years, limited research has focused on risk perception associated with actual radiological emergencies" (Ho, Jung-Chun et. al. 2013: 774).

Fallbeispiel einer Aufwertung und genaueren Betrachtung. Denn Unternehmen befinden sich als organisatorische Entitäten in einem Spannungsfeld zwischen staatlicher Verantwortung und privater Trägerschaft. Dieses Verhältnis und die zwingende Einbeziehung von privaten Akteuren wie MNU als Träger zentraler Funktionen und Ressourcen in den gesellschaftlichen Risikodiskurs wurden in der Literatur allerdings nur untergeordnet betrachtet (Krahmann 2007: 3; Goldstein 2010: 492). Doch die Sicherheitsdebatte könnte an diesem Beispiel sowie der Rolle transnationaler Wertschöpfungskette im Allgemeinen um ein aufschlussreiches empirisches Forschungsfeld erweitert werden. Zudem ist der Forschungsstand zur Einbindung des Supply Chain Risk Managements in Kontrollsysteme zur Steuerung geschäftsgefährdender Risiken überschaubar (vgl. Behnezhad, Connett und Nair 2013: 77; Lee, Yeung und Hong 2012: 544) oder konzentriert sich auf spezifische Aspekte des Outsourcing-Vertragswerkes (vgl. Wüllenweber, Jahner und Krcmar 2008). Ähnliches gilt für das asymmetrische Verhältnis zwischen staatlicher und privater Ebene. Ein weiterer Aspekt des Problems findet sich in der Zuweisung und Annahme von Verantwortung in diesem Kontext: „The result is an impasse between government and the private sector. Most infrastructure providers do not have financial resources to protect their infrastructure from low probability events like terrorism and natural disasters" (Schintler et. al. 2007: 292). Dies kann mit Blick auf obiges Beispiel fatale Folgen für das Unternehmen und die Betroffenen der geschädigten kritischen Infrastruktur haben (Cook 2010: 23).

Der Bedeutungszuwachs globaler Wertschöpfungsketten, Produktionsstandorte und Transportrouten verschärft die Diskrepanz des Kooperationsmodells weiter (Behnezhad, Connett und Nair 2013: 78) und sollte Entsprechung in der Sicherheitsliteratur finden. Empirische Beispiele und theoretische Implikationen der Verantwortungsdelegation auf Seiten der Unternehmen bieten ausreichend Raum, um den sicherheitsrelevanten Diskurs auf eine bisher vernachlässigte Betrachtungsebene der Sicherheitsproduktion in Unternehmen, beispielsweise im Fall der Sicherstellung der Prozesskontinuität durch Kontrolle des Lieferkettenrisikos, zu lenken. Denn wenn ein Großteil der von privaten Trägern betriebenen kritischen Infrastruktur (Braes und Brooks 2010: 16) mit der klassischen ökonomischen Profitorientierung von MNU in Widerspruch tritt, entstehen Risiken für die Gesellschaft und ihrer Sicherheitsdispositive. „Denn es zeigte sich, dass „[…], much of the expertise and many of the resources required for taking better protective measures are located outside governments. […] Because the state has lost control over his body parts, it needs the private sector to localize them for him" (Cavelty 2013: 116).

Die Corona-Pandemie zeigte zudem mit Blick auf die globalen Warenströme, dass die Abhängigkeit von ununterbrochenen, globalen Produktionskapazitäten und Transportrouten essentiell ist. Der Mangel an Schutzkleidung und Desinfektionsmitteln wie zu Beginn der Pandemie (Ghanchi 2020: 806), die Produktion, Schutz von Know-How und Verteilung von Impfstoffen (Marom und Lussier 2020: 255) oder die Engpässe in bestimmten Branchen durch ausbleibende Vorprodukte oder Rohstofflieferungen wurden durch die nationalen Maßnahmen zum Schutz der eigenen Bevölkerung induziert (Menzel 2021: 4). Diese Problematik des analogen Zeitalters setzt sich zudem in der digitalen Sphäre fort. Vorausgreifend sei erstens auf die Rolle privater Unternehmen in Bezug auf die Infrastruktur des Internets und neuer Technologien (Fischer, 2007: 53), zweitens den Diskurs zur Eindämmung von Straftatbeständen im digitalen Raum[315] und drittens der Inklusion von privaten Unternehmen zum Zweck des Datenschutzes verwiesen (Cook 2010: 25). Die Relevanz privater Betreiber zur Sicherstellung der Netzsicherheit und Kontinuität kritischer Dienstleistung lassen daher eine weitere Metamorphose der Public-Private-Partnership erwarten (Vassilaki 2015: 22), in deren Mittelpunkt die Risikokontrolle von privaten Betreibern der kritischen Infrastruktur und ihrer Lieferkettensicherheit stehen werden. Bevor wir diese Herausforderungen im digitalen Zeitalter beleuchten, soll der Blick auf ein letztes Fallbeispiel gerichtet werden. Anhand von drei Pandemieverläufen zwischen 2003 und 2022 soll die Entwicklung unternehmerischer Vorsorgeplanung mit Blick auf die Verfügbarkeit von Mitarbeitern gezeigt werden.

5.5. Fallbeispiel 3 - Ausfall von Personal – Pandemie 2003 – 2022

Anders als eine Geschäftsunterbrechung durch die Nicht-Verfügbarkeit von Geschäftsräumen wie in Folge der Anschläge vom 11. September 2001 oder des Ausfalls von Dienstleistern, kam durch eine Reihe von Infektionskrankheiten eine weitere Dimension für die unternehmensinterne Sicherheitsproduktion durch den möglichen Ausfall des Personals hinzu (Osterholm 2005: 37). Einige Erfahrungswerte und eine gewisse Sensibilisierung für diese Risikokategorie wurden bereits während der SARS-Pandemie in Asien 2002 und 2003 beobachtet (Finlay, See und Brunham 2004: 602). Der Diskurs über die Gefahren einer Pandemie in Europa und Nordamerika wurde im Kontext der unternehmerischen Risikokontrolle durch die Mutation von H1N1- und H5N1-Grippestämmen zum Beginn des 21. Jahrhunderts auch als mögliche Szenarien einer Geschäftsunterbrechung durch eine hohe

[315] An der Impfforschung und Herstellung beteiligten Unternehmen wurden während der Corona-Pandemie vermehrt Ziel von Cyberattacken. Das Ziel dieser Angriffe wird in der Entwendung von Forschungsergebnisse vermutet (Bund und Leonard 2020:3). Die Rolle der privaten Unternehmen in dieser Krise ist von großer Bedeutung zur Bewältigung des medizinischen Risikos sowie der gesellschaftlichen, wirtschaftlichen und sozialen Einschränkungen.

Mortalität unter Infizierten geführt (Günther et. al. 2011: 32). Die Mutation der Virusstämme wurde seinerzeit im Fall der Übertragung von Vögeln beziehungsweise Schweinen auf den Menschen dokumentiert und als problematische Entwicklung eingestuft (Singer 2007: 102). Zusätzlich erfolgte die schnelle Ausbreitung über mehrere Länder in kurzen Intervallen, welche ein erhöhtes Risikobewusstsein für die Möglichkeit einer globalen Pandemie beförderte. Im Zuge der Überlegungen schienen Ausfälle der Produktion und Prozesse in Folge der Erkrankung von Mitarbeiter möglich und beeinflussten den Diskurs über geschäftsgefährdende Risiken (Meredith et. al. 2008: 3). Eine breite Thematisierung des pandemischen Risikos in den Medien und im öffentlichen Raum ereignete sich im Verlauf der Vogel- und Schweinegrippewellen zwischen 2003 und 2011 (Günther, Ruhrmann und Milde 2011: 15).

Im Fall der Vogelgrippe rief die Weltgesundheitsorganisation (WHO) 2003 und 2006 jeweils die höchste Pandemiewarnstufe aus. Zum Zeitpunkt der ersten Pandemiewelle wurde die Verbreitung von H5N1-Virusstammtypen in 51 Ländern dokumentiert (Singer 2007: 102). Im Kontext dieser Pandemiewellen sahen sich Unternehmen mit einem schwierigen Problem hinsichtlich ihrer BCM-Planung konfrontiert. Es wurde angenommen, dass Mitarbeiter im Fall einer Pandemie nicht mehr zur Arbeit kommen würden, wenn sie selbst erkrankt wären oder sich um Familienangehörige kümmern müssten. Die Fortführung des Betriebs würde in diesem Fall also nicht durch den Verlust von Bürofläche oder von Infrastruktur gefährdet, sondern durch den Ausfall von Personal (Braubach 2011: 36). Dieses Fallbeispiel ist interessant zu beobachten, da sich Unternehmen mit einer grundlegend anderen Kategorie der Vorsorgeplanung auseinandersetzten mussten. Fragen der Hygiene, Gesundheitsvorsorge und Therapie, waren zuvor die Domänen staatlicher Behörden. Dieses Monopol wurde aber durch Pandemieereignisse zwischen 2003 und 2011 aufgeweicht und Unternehmen an der Verantwortung zur präventiven Eindämmung beziehungsweise reaktiven Bekämpfung der Krankheiten involviert.[316]

In ihrer Auswirkung und Dimension überschattete jedoch die Corona-Pandemie die vorausgegangen Infektionsgeschehen. Darüber hinaus verdeutlichten die Reaktionen auf das Corona-Virus, dass die Anhängigkeit von globalen Warenketten und den einhergehenden Einschränkungen im Welthandel (beispielsweise für medizinische Schutzausrüstung) einerseits

[316] Die nationale Strategie des US-amerikanischen Homeland Security Council verlangt auch von privaten Unternehmen den Nachweis einer Krisenvorsorge aufgrund der Bedeutung der Privatwirtschaft für die öffentliche Ordnung und Sicherheit. Die Vorbereitungen auf eine Pandemie erhalten dabei besondere Erwähnung: “The threats facing our Nation in the 21st century, from pandemic influenza and the emergence of new diseases such as SARS, to terrorist attacks and naturally occurring disasters such as hurricanes and earthquakes, require an all-hazards approach to emergency planning and preparedness” (Homeland Security Council 2007: 26).

(Brzoska, Neuneck und Scheffran 2021: 3), sowie von IT-Ausrüstung und Kapazitäten andererseits, andere Risikokontrollen, als für lokal begrenzte Ereignisse wie terroristische Anschläge erforderlich machten (Kocher und Weyerstraß 2020: 4f.). Die folgenreichste Dimension der Corona-Pandemie im Rahmen dieser Arbeit, die Beschleunigung der Digitalisierung und weitreichenden Verlagerung von Arbeitsprozessen und deren Ressourcen in den virtuellen Raum, werden wir jedoch erst im nachfolgenden Kapitel über die Risikokontrolle im digitalen Zeitalter im Detail besprechen.

Für diesen Abschnitt stehen vielmehr die Auswirkungen auf die Schutzmaßnahmen von Unternehmen zur Sicherstellung ihrer Anschlussoperationen durch die traditionelle Risikokontrolle im analogen Umfeld im Vordergrund. Denn trotz der unterschiedlichen Dimensionen von Vogel- und Schweinegrippe einerseits und der Corona-Pandemie andererseits, zeigen diese Pandemien die themenspezifischen Gemeinsamkeiten mit Blick auf das Risiko der Entscheidung in diesem Szenario sowie der Unsicherheit aufgrund mangelnder Informationen und der sich dynamisch wandelnden Vorgaben durch staatlichen Autoritäten. Insbesondere im Fall des letztgenannten Aspekts bieten die, zum Zeitpunkt des Verfassens dieser Arbeit allerdings noch nicht abgeschlossenen, Aspekte der Corona-Pandemie aufschlussreiche Einsichten in die Beziehung der staatlichen-privaten Partnerschaft und der Folgen für die Sicherheitsproduktion in MNU.

Diese Überlegung übersetzt sich in die folgende Struktur und Ausrichtung dieses Fallbeispiels: Zunächst soll das Risiko der Entscheidung anhand der Maßnahmen in Unternehmen im Umgang mit den drei Pandemiewellen betrachtet werden. Denn anders als im Fall der Reaktion auf einen terroristischen Anschlag, verläuft eine Pandemie unter vorausgehender Beobachtung des Ereignisses und eröffnet mehr Möglichkeiten durch Entscheidungen auf das Geschehen innerhalb des eigenen Einflussbereichs einzuwirken, allerdings einhergehend mit der Problematik des Risikos der Entscheidung. Denn jede Entscheidung zum Handeln oder Nicht-Handeln vor und während eines Pandemiegeschehens tragen wesentlich zur Entwicklung der Krise für die jeweilige Organisation bei. Dies lässt sich anhand von drei maßgeblichen Problemfeldern aufzeigen: erstens die starre Struktur von Pandemiekrisenpläne, welche insbesondere angesichts des (1) Pandemiestufenmodells der WHO in einigen Fällen nur geringen Mehrwert entfalten konnten, zweitens das (2) präventive Ergreifen von Hygienemaßnahmen und drittens die (3) Problematik einer reaktiven Krisenkommunikation. Entlang dieser Problemfelder im Kontext der Pandemiewellen zwischen 2003 und 2011 beziehungsweise der Corona-Pandemie zwischen Dezember 2019 bis zum Ende der

Betrachtung dieser Arbeit im Jahr 2022[317] wollen wir die Weiterentwicklung in Richtung der unternehmerischen Risikokrontrolle analysieren.

5.5.1. Adaptionsfähigkeit der Vorsorgeplanung

Effektive Vorsorgeplanung erfordert wie wir zuvor gesehen haben eine Analyse der kritischen Prozesse im Rahmen der BIA sowie eine Strategieentscheidung auf der Grundlage von identifizierten Risikoszenarien (Torabi, Soufi und Sahebjamnia 2014: 311). Die Vorkehrungen für eine Krise, in welcher mit dem Tod oder der Erkrankung von Mitarbeitern gerechnet wird und für deren Arbeitsressource ein Ersatz gefunden werden soll, geraten leicht in Gefahr einer zynischen Argumentation.[318] Ein aus ethischen und humanistischen Gründen bestehender Imperativ zur Fürsorge verbindet sich in diesem Themenfeld mit der funktionalen Notwendigkeit der Prozesskontinuität und der arbeitsrechtlichen Fürsorgepflicht (Stowasser und Peschl 2019). Dazu stehen im Allgemeinen drei Methoden zur Disposition: Erstens den Schutz der Mitarbeiter durch präventive Schutzmaßnahmen[319] zu gewährleisten, zweitens erkrankte Mitarbeiter durch geeigneten Ersatz und Umschulungen zu kompensieren[320] oder drittens die Ressource entweder durch Zeitarbeitsfirmen oder Outsourcing-Partner zu externalisieren.[321]

---

[317] Der gewählte Endzeitpunkt der Beobachtung der Corona-Pandemie fällt mit dem Abschluss der Bearbeitung dieser Dissertation zusammen und versucht die bis dahin dokumentierten Erkenntnisse einzubringen.

[318] Die Vorbereitungen auf einen potentiellen Ausfall von Mitarbeitern orientiert sich primär am Szenario einer Pandemie. Auch andere Szenarien können die Verfügbarkeit der Mitarbeiter einschränken. Politische Veränderungen oder ein Anschlag sind gängige Szenarien in den Überlegungen, durch welche Ursache eine Unterbrechung der Prozesse verursacht werden könnte. Doch in den meisten Fällen ermangeln die gewählten Szenarien einer breiten Schadenswirkung, um einen signifikanten Mangel an Mitarbeitern zu bewirken, welcher die Fähigkeit zur Geschäftsfortführung ernsthaft gefährden könnte (Braubach 2011: 36).

[319] Der Schutz der Mitarbeiter gegen eine Infektion beziehungsweise deren sofortige Immunisierung benötigt neben den Mitteln zur Anwendung vor allem einen Annäherungswert, zu welchem Zeitpunkt mit diesen Maßnahmen begonnen werden sollte. Wir werden diese Option im nachfolgenden Hygienekonzept genauer betrachten. Bemerkenswert ist die Arbeit aus dem mobilen Arbeitsplatz heraus, welche zu den präventiven Methoden zu zählen ist. Während der Corona-Pandemie wurden innerhalb von wenigen Wochen Konzepte realisiert (wenn funktionell, finanziell und operationell möglich), um Mitarbeiter via einem virtuellen Zugriff auf Organisationsnetzwerke die Arbeit vom heimischen Arbeitsplatz aus zu ermöglichen und eine Ansteckung im Büro zu unterbinden (Bellmann et. al. 2021: 713).

[320] Diese Option setzt an dem Punkt an, ab dem neue Teammitglieder benötigt werden. Die Mitigation kann innerhalb des Unternehmens geplant werden, beispielsweise wenn Prozessredundanzen eine Verlegung der Arbeitslast ermöglichen oder Mitarbeiter mit dem notwendigen Wissen für diese Aufgaben abgestellt werden. Die entscheidende Variabel für den Erfolg ist die Qualifikation. In manchen Berufsfeldern, zum Beispiel im Fall der juristischen Beratung oder der Chirurgie in einem Krankenhaus sind formelle Anforderungen in Form der qualifizierenden Ausbildung unerlässlich. Andere Prozesse hingegen können durch Schulungen in ihrem Kern und innerhalb der notwendigen Zeit vermittelt werden. Mitarbeiter aus verwandten Themenbereichen können unter Umständen die Aufgaben ihrer Kollegen in der Nachbarabteilung übernehmen. Das notwendige Schulungskonzept ist ex ante zu erstellen, um keine Zeit zu verlieren.

[321] Die Kosten sowie die zu erwartenden mangelnden Kenntnisse über das Unternehmen fallen dementsprechend negativ ins Gewicht, Eine Alternative könnte auch die komplette Ausgliederung des Prozesses an einen externen Anbieter sein. So können Telefondienstleistungen vorübergehend an ein Call Center ausgelagert und die Mitarbeiter dort über ihre Aufgaben unterrichtet werden (Sako 2006: 505).

Eine erste Orientierungshilfe für die Aktivierung solcher Maßnahmen während der Vogel- und auch Schweingrippewellen war der Pandemiestufenplan der Weltgesundheitsorganisation, dessen Wirksamkeit einem Realitätstest unterzogen wurde (vgl. World Health Organization 2009). Das sechsstufige Modell war in drei Abschnitte gegliedert. Die „interpandemische Phase“ der ersten beiden Stufen beschrieb jährlich wiederkehrende Muster und Frühwarnindikatoren der Ausbreitung bekannter Infektionskrankheiten, wie etwa der saisonalen Grippe (Robert Koch Institut 2007: 89). Die „pandemische Warnphase“ der Stufen 3, 4 und 5 galt als Eskalationsstufe vor der eigentlichen Pandemie. In dieser Phase wären aktive Vorbereitungen zu treffen, während in der letzten Phase, der Stufe 6 die Pandemie im vollen Umfang zu beobachten wäre (ebd.: 32f.). Analog dazu war es vorgesehen, die entsprechenden, jeder Stufe zugewiesenen Maßnahmen umzusetzen. Während der ersten Phase, wäre die Situation durch medizinische Experten und Behörden zu beobachten und eine Auswertung der Berichterstattung von Medien und gesundheitsrelevanten Instituten wie dem Center for Desease Control (CDC) oder dem Robert Koch Institut durchzuführen. Die zweite Phase würde nun den Krisenstab von Unternehmen in Alarmbereitschaft versetzen, weitere Beobachtung der Entwicklung nach sich ziehen und in regelmäßigen Abständen Konsultationsgespräche der Entscheidungsträger ansetzen (Osterholm 2005: 28). In dieser Phase wäre zudem bereits über aktive Schutzmaßnahmen wie Hygienemaßnahmen und die Vorbereitung der Verteilung von Impfungen beziehungsweise Postprophylaxe-Medikamenten zu initiieren[322]. Die letzte Phase wäre schließlich der Startschuss für den Beginn der geplanten Maßnahmen im präventiven und reaktiven Spektrum (Fineberg 2014: 1336).

Die tatsächliche Ausbreitung der H1N1 und H5N1 Pandemie zeigten jedoch die Mängel des WHO-Modells auf, denn anstatt eine Anleitung für die Implementierung geeigneter Maßnahmen anzubieten, trug das Modell zur Verunsicherung bei. Das generelle Problem an den existierenden Pandemieplänen war, dass sie auf Szenarien und Annahmen von großflächigen Infektionsgeschehen aus dem 20. Jahrhundert angewiesen waren und es bis zum Ausbruch von H5N1 keine empirisch ausreichenden Daten zur Validierung der Vorsorgeplanung vorlagen (Hashim et. al. 2012: 287). Als schließlich die höchste Stufe im Fall der Schweinegrippe 2009 erreicht wurde, teilten nur wenige Beobachter in Europa diese Einschätzung (ebd.: 292). Denn obwohl die Kriterien der WHO zur Ausrufung einer Pandemie erfüllt waren, war das Bild in vielen Teilen der Welt ein gänzlich anderes. In dieser Phase wäre

[322] Eine Postprophylaxe ist unmittelbar auf eine Infektion folgend zu verabreichen, um eine Ausbreitung der Erreger im Organismus zu stoppen und so den Ausbruch der Krankheit zu unterdrücken (vgl. Singer 2007: 102). Die Hygienemaßnahmen werden im Folgenden weiter erläutert.

die „(…) zunehmende und anhaltende Übertragung des Virus in der Allgemeinbevölkerung in mindestens zwei der sechs WHO-Regionen“ anzunehmen und es galt als angezeigt bereits vor dieser Phase „die Auswirkungen der Pandemie zu minimieren“ (Günther et. al. 2011: 16).

Doch die erwartenden Auswirkungen der Pandemie blieben glücklicherweise aus. Die Autoren des Eskalationsmodells hatten mit einer stringent verlaufenden Entwicklung und Intensität der Pandemie gerechnet, doch die tatsächlichen Ereignisse wurden durch den Kriterienkatalog, der zur Definition der unterschiedlichen Stufen dienen sollte, zwar formell, aber nicht materiell erfüllt. Dies führte zu Verunsicherung in der Bevölkerung sowie einer angeregten Debatte über die Anwendbarkeit von Pandemieplänen unter Experten (Fineberg 2014: 1338). Während der Hochphase 2009 galt es nun zu entscheiden[323], ob man am ursprünglichen Plan trotz seiner bisher geringen Aussagekraft festhalten sollte und mit der Herausgabe von Medikamenten an die jeweiligen Mitarbeiter des Unternehmens beginnen solle? Die Alternative wäre, von dem vordefinierten Plan abzuweichen und weitere Schritte auf der Grundlage von ad-hoc Entscheidungen zu treffen.

Das Risiko lag also in der Entscheidung den vorgeschriebenen Weg des Pandemieplans zu folgen, obwohl die zugrunde liegenden Indikatoren nicht stichhaltig schienen, oder sich alternativ gegen die Ausgabe von Medikamenten und Impfungen auszusprechen. In Vorbereitung auf die Pandemie waren aus Erfahrungen mit H1N1 bereits große Bestände an Medikamenten wie Tamiflu angelegt worden. In den USA zählte man 2007 über 81 Millionen Behandlungseinheiten, in Deutschland immerhin 16 Millionen Einheiten (Singer 2007: 102). Doch welche Entscheidung sollte getroffen werden? Beide Optionen wiesen gewichtige Vor- und Nachteile auf. Sollte man das Zeitfenster zur Ausgabe von Medikamenten verpassen, könnte die Nichtverfügbarkeit der Mitarbeiter durch Erkrankung oder durch Krankheitsfälle innerhalb der Familien die Fortführung der Geschäftsprozesse gefährden. Nur die rechtzeitige Einnahme der präventiven beziehungsweise unmittelbar auf die Infektion wirkenden reaktiven Medikamente (Postexpositionsprophylaxe) würde Handlungsspielraum bieten, um eine Erkrankung zu verhindern (vgl. Ferguson et. al. 2006: 448).

Umgekehrt wäre die verfrühte Initiierung dieses Schritts aufgrund der noch unzureichenden Erforschung des Wirkstoffs von unsicherem Ausgang (Günther, Ruhrmann und Milde 2011: 28). Dies trug dazu bei, das Risiko der Entscheidung zu erhöhen. Hinzu kam, dass das

[323] Die eigenverantwortliche Planung von Unternehmen im Bereich der medizinischen Fürsorge Vorbereitungen zu treffen kann als Folge des schrittweisen Verantwortungstransfers von staatlicher auf die private Ebene verstanden werden.

Eskalationsmodell der WHO - der eigentlichen Autorität auf dem Gebiet – aufgrund der unzutreffenden Definition seiner Eskalationsstufen seines originären Zwecks entbehrte und dadurch die Unsicherheit vergrößerte (Fineberg 2014: 1338). Beide Optionen erforderten Fachwissen für das man auf den Rat von Experten angewiesen war. Betriebsärzte, meistens spezialisiert auf Arbeitsmedizin, waren keine Experten für Virologie oder Immunologie und daher nur eingeschränkt hilfreich.[324] Ein weiterer Aspekt waren die artikulierten Vorwürfe der Öffentlichkeit an die Verantwortlichen auf der politischen Ebene, ihre Verbindungen mit der Pharmaindustrie vor und während der Krise nicht im ausreichenden Umfang publiziert zu haben (Günther, Ruhrmann und Milde 2011: 31).[325] Für die Verantwortlichen in Unternehmen verblieb folglich das Risiko einer Entscheidung unter dem Eindruck von Unsicherheit unverändert.[326]

Im Fall der Corona-Pandemie wurde die Rolle der WHO und der von ihr vorgestellten (überarbeiteten) Pandemievorsorge erneut negativ konnotiert und in ihrem Verlauf durch politische Spannungen, mangelnde Autorität und fehlende Ressourcenlage kritisiert (Brzoska, Neuneck und Scheffran 2021: 3). Ferner wurde die Anpassungsfähigkeit der nationalen Gesundheitssysteme zwischen 2019 und 2022 einen noch größerem Stresstest unterzogen. Einerseits traten die Probleme der Lieferkettensicherheit und globalen Diversifizierung von Produktionsketten in Erscheinung (Menzel 2021: 26). Im europäischen Rahmen verdeutlichte sich, „dass wirtschaftliche Internationalisierung mit dem Prinzip der Risikovorsorge in Konflikt stehen kann. Selbst in Staaten mit großen und differenzierten Wirtschaften wurden Abhängigkeiten von Zulieferungen von Gütern manifest, die kurzfristig auf nationaler Ebene nicht ersetzbar waren“ (Brzoska, Neuneck und Scheffran 2021: 3). Andererseits zeigte die Herangehensweise an Impfkampagnen und Lock-Down Maßnahmen ein überaus heterogenes Bild ab, insbesondere während des ersten Pandemiejahres, in welchem staatliche Autoritäten aus Nationalstaaten und wie im Fall von Deutschland sogar Bundesländer unterschiedliche

[324] Pharmakonzerne boten sich als Experten an, doch bestand Skepsis gegenüber ihrer Neutralität. Tatsächlich erhöhten sich die Einnahmen auf dem Handel mit Grippemedikamenten nach dem Bekanntwerden des Vogelgrippevirus in Asien von 2003 und der Schweingrippe 2009 an und bewegten sich im Milliardenbereich. (vgl. Handelsblatt 2014).

[325] Beide Aspekte fanden während der COVID-19 Pandemie in Deutschland erneut Beachtung, einerseits in der Diskussion um geeignete Eskalationsstufen in Form des Inzidenzwertes und andererseits durch die sogenannte „Maskenaffäre“, in welcher Abgeordnete ihre Verbindungen nutzten, um Maskenhersteller mit Entscheidungsträger zusammenzubringen (Handelsblatt 2021a)

[326] Auch im Fall der COVID-19 Pandemie eröffneten private Unternehmen das Angebot, Schutzimpfungen gegen das Coronavirus anzubieten, da die unzureichenden Kapazitäten der nationalen Impfstrategie zu Verzögerungen führten (Tagesschau 2020). Ein interessanter Schritt, wenn man bedenkt, dass alle Impfmaßnahmen im Sinne der nationalen Koordination in Deutschland während der Corona-Pandemie durch staatliche Autoritäten organisiert werden sollten.

Maßnahmen analog zu den jeweiligen Pandemieplänen vorlegten. Die Kommunikation der angekündigten Maßnahmen gegen das Virus selbst entwickelte aufschlussreiche semantische Variationen, welche von Verharmlosung bis hin zur Kriegsrhetorik reichten (Kirk und McDonald 2021: 3). Der Sprechakt im Sicherheitsdiskurs zeigte hier eine eindrucksvolle Wiederkehr.

Mit Blick auf die Uneinheitlichkeit von Maßnahmen durch nationale und regionale staatliche Autoritäten ließ sich die Problematik für die Entscheidungsfindung innerhalb von Unternehmen eindrücklich während der Corona-Pandemie beobachten. Während der ethnographischen Untersuchung wurde die Unsicherheit im Umgang mit den von staatlichen Autoritäten vermittelten Lagebildern und Maßnahmen auch im Gespräch mit Teilnehmern der Krisenstäbe und untergeordneten Arbeitsgruppen (Task Forces), insbesondere für die erste Jahreshälfte 2020 festgestellt.[327] Die allgemeine Erschöpfung und Unsicherheit über die Entwicklung der Pandemie mischte sich mit Konfusion über die geltenden Maßnahmen, welche sich zum im Kontext des Unternehmens nicht nur über 16 verschiedene Bundesländer und deren Maßnahmen zum Infektionsschutz für Standorte in Deutschland, sondern auch über zahlreiche Niederlassungen in anderen Staaten ersteckten. Die Identifikation und Konsolidierung der unterschiedlichen Maßnahmen sowie die Sicherstellung der Prozesskontinuität bei gleichzeitiger Einhaltung der unterschiedlichen Corona-Maßnahmen im globalen Kontext wurden von Praktikern als große Herausforderung beschrieben. Die ambivalente Rolle von MNU zeigte sich zudem in dieser Krise, indem die Standardisierung und Angleichung von Prozessen innerhalb eines Unternehmens durch die Unterschiedlichkeit der Maßnahmen von staatlichen Autoritäten an den verschiedenen Standorten des Unternehmens erschwert wurde.

5.5.2. Die Angemessenheit von Maßnahmen

Die Folgen der Unsicherheit zeigten sich auch in einem zweiten Problembereich. In diesem Fall war die Frage für Krisenstäbe in Unternehmen zu klären, wann der richtige Zeitpunkt für Hygienemaßnamen und andere Schutzvorkehrungen der Belegschaft sei. Sowohl im Fall der Vogelgrippe, als auch während Schweinegrippe wiesen breite Bevölkerungsschichten ein

[327] Im Gespräch mit einem Mitglied des globalen Krisenstabes wurde 2021 rückblickend auf den Beginn der Lockdown-Maßnahmen im Jahr 2020 festgestellt, dass die Entscheidung zur Virtualisierung von Arbeitsplätzen zwischen den Landesgesellschaften nicht synchronisiert ablief. In einem Fall wurden drei Gesellschaften, die an einem Standort vertreten waren, an drei verschiedenen Tagen an den heimischen Arbeitsplatz geschickt worden, da keine zentrale Kommunikation durch den globalen Krisenstab zu diesem Zeitpunkt erfolgen konnte. Der Grund lag laut dem Krisenstabsmitglied in der Unsicherheit der Organisation aufgrund der mangelhaften Informationslage und Vorgaben durch die Behörden verschuldet. Dieses Ereignis im Frühjahr 2020 führte allerdings zu einer umfassenden Überprüfung und Standardisierung der Krisenkommunikation,

„defizitäres Hygienewissens und –verhalten“ auf (Günther et. al. 2011: 28). Daher waren entsprechende Maßnahmen in Pandemieplänen zum präventiven Schutz vorgedacht und sollten ebenfalls anhand des oben geschilderten WHO-Stufenmodels initiiert werden (Meredith et. al. 2008: 17). Doch die Hygienemaßnahmen waren während einer früheren Stufe der Pandemieausbreitung terminiert, die Medikamentenausgabe sollte hingegen erst kurzfristig eingesetzt werden, um die Mitarbeiter akut zu immunisieren. Die Hygienemaßnahmen umfassten hingegen die häufigere Reinigung der Büro- und Sanitärräume um eine generelle Ansteckungsprävention zu unterstützen (World Health Organization 2009: 28). Die Mitarbeiter wären dabei noch nicht involviert worden oder hätten davon kaum Kenntnis genommen, da die Reinigung meistens vor oder nach den Hauptgeschäftszeiten stattfindet (Robert Koch Institut 2007: 89) und anders als bei der Corona-Pandemie war weiterhin die Arbeit in den Büroräumen vorgesehen. Dazu waren spezielle Hygieneratgeber im Rahmen der Hygienekommunikation geplant, was zum Beispiel Plakate, Broschüren oder Ansprachen durch Vorgesetzte hinsichtlich einer angemessenen Prävention durch Hygiene. Ein weiterer Schritt in der Hygieneprävention wäre die Installation von Desinfektionsmittelspendern an öffentlichen oder häufig frequentierten Orten sowie die Bereitstellung und Bewerbung von Hygienemasken (ebd.: 91). Beide verbindet eine kennzeichnende Abhängigkeit vom Zeitpunkt ihrer Einführung, analog zum WHO-Eskalationsmodel.[328]

Für MNU reichte dieses Problem im Fall der Corona-Pandemie noch weiter, da sie über ihre Organisationsentitäten unter Umständen mit mehreren, sich teilweise wiedersprechenden Regulationen von hoher Volatilität gegenüber sahen. Die Rolle des Staates als Ordnungsmacht wurde durch die verhängten Lockdown-Maßnahmen eindrucksvoll hervorgehoben, doch Unternehmen aller Größen sorgten unter erschwerten Umständen größtenteils für eine erfolgreiche Überführung der Funktionsfähigkeit in den heimischen Arbeitsplatz (Kirk und McDonald 2021: 3). Diese Option wäre staatlichen Autoritäten in der Abwägung zwischen Gesundheitsschutz und wirtschaftlicher Existenzsicherung vor zehn Jahren vermutlich noch nicht zur Verfügung gestanden.[329] Wie bereits zuvor gezeigt, waren die technischen

[328] Die Einführung von Masken wäre daher nur mit einer entsprechenden Eskalation der H1N1 und H5N1 Pandemie verbunden. Im Allgemeinen zeichnet sich die Initiative zu verstärkten Hygienemaßnahmen durch das gleiche Charakteristikum aus wie schon die Ausgabe der Medikamente. Die Hemmschwelle zur Einführung von Schutzmasken während der Corona-Pandemie verlief niedriger und wurde durch staatliche Vorgaben, beispielsweise durch die Einführung der Mund-Nasen-Bedeckung beim Einkaufen vereinfacht.

[329] Zugespitzt kann gesagt werden, dass die durch Unternehmen eingeführte Digitalisierung in den Jahren vor der Pandemie, dem Staat eine neue Mitigationsstrategie zur Verfügung stellte, welche die volkswirtschaftlichen Kosten dieser Maßnahme abzufedern half. Gleichzeitig verpflichteten staatlichen Institutionen die privaten Unternehmen zur umfänglichen Nutzung dieser Technologie, deren Nutzen zuvor durch die Problematisierung des Arbeitens im heimischen Umfeld gegenüberstand (Wentland und Klimburg-Witjes 2021: 185).

Möglichkeiten für virtuelle Arbeitsplatzalternativen bereits in letzten Jahren vor der Pandemie weiterentwickelt worden[330]. Dies erlaubte es nun einigen Unternehmen die Arbeit dezentral fortsetzen zu können (Boland et. al. 2020), trotz aller Einschränkungen wie der Betreuungssituation von Kindern oder Familienangehörigen (Fries et. al. 2020: 19) oder der Geeignetheit des analogen Arbeitsplatzes im Haus der Mitarbeiter oder sozial-psychologischer Folgen der isolierten Arbeitsbedingungen (Wang et. al. 2021: 31).

Bemerkenswert ist hier auch der veränderte Fokus des betrieblichen Kontinuitätsmanagements. Zwar galten die Pandemievorsorge und die Entscheidung zur Schließung der Büroflächen vorrangig dem Schutz der Gesundheit der Mitarbeiter, aber die größte Herausforderung lag in der Bereitstellung der ausreichenden Verfügbarkeit von Endgeräten, Softwarekonfigurationen und VPN-Verbindungen. Allein bis Mai 2020 wurden weltweit Schätzungen zufolge mehr als 300 Millionen neue VPN Einzelverbindungen aufgebaut, um zusätzlich zu den bestehenden Kapazitäten Mitarbeitern den Zugriff auf Unternehmensplattformen zu ermöglichen (Alexander und Jaffer 2021: 19). In einer Umfrage deutscher Unternehmen sagten 41% der Unternehmen aus kurzfristigen Investitionen in Hardware für ihre Mitarbeiter und knapp die Hälfte zudem in Softwarekomponenten zur Kommunikation und virtuellen Zusammenarbeit vorgenommen zu haben (Bellmann et. al. 2021: 715). Mit fortschreitender Verfügbarkeit von Schutzmasken und Impfkampagnen eröffnete sich schließlich die Möglichkeit hybride Arbeitsmodelle, bestehend aus abwechselnd virtuellen und physischen Arbeitsplatz, für die Mitarbeiter anzubieten.

Nach Wiedereröffnung der Arbeitsflächen zeigte sich auch, dass die Angemessenheit von Hygienemaßnahmen ein interessanter Gegenstand der öffentlichen und intraorganisatorischen Diskussionen war. Die im Verlauf der Pandemie eingeführte Mund-Nasen-Bedeckung im öffentlichen Raum sowie die Ausweitung dieser Maßnahme auf einen höheren Schutzstandard (FFP2 oder äquivalente Schutzklasse) zeigte im Unterschied zu den Schutzkonzepten in den Fällen von H1N1 und H5N1, dass nun auch ein Großteil der Bevölkerung in ihrem Alltagsaktivitäten in die Hygienemaßnahmen verpflichtend einbezogen wurden. Ein zentrales Problem der staatlichen Krisenbewältigung galt der Beschaffung von Schutzkleidung und Masken im Speziellen, deren Anschaffung versäumt worden war beziehungsweise durch die

[330] Laut einer Studie arbeiteten 2017 bereits 22% der Beschäftigten in Deutschland, welche in Betrieben oder öffentlichen Einrichtungen mit mehr als 50 Mitarbeitern arbeiteten bereits regelmäßig von zu Hause. Die beiden Hauptgründe für Probleme mit dem Wechsel ins mobile Arbeiten waren einerseits fehlende technologische Infrastrukturen in den Organisationen und andererseits grundsätzliche Bedenken am Konzept des mobilen Arbeitens von Seiten der Arbeitgeber vorgebracht wurden (Fries et. al. 2020: 21)

globalen Lieferengpässe verschärft wurde (Menzel 2021: 5). Das Corona-Virus entwickelte sich zu einem weiteren Beispiel für ein Schadensereignis mit unterschätzter Eintrittswahrscheinlichkeit und großem Schadenspotential, auf das staatliche und private Akteure unzureichend vorbereitet waren, was sich insbesondere in der Anschaffung, Vorhaltung und Verteilung von Schutzausrüstung und Impfstoffen zeigte (Ghanchi 2020: 806).

Die Neuartigkeit des Virus, fehlende Datengrundlagen über Infektionswege und die Schwere der Krankheit erzeugten vor allem zu Beginn der Pandemie Unsicherheit auf Seiten der Entscheidungsträger. Informationen und Leitlinien von staatlicher Seite waren in den ersten Wochen und Monaten teilweise widersprüchlich und machten die Abwägung von Maßnahmen zum Schutz der Belegschaft ohne ausreichenden Kenntnisstand der Situation und Konsequenzen notwendig (Fries et. al. 2020: 22). Unter dem Stichwort der Verhältnismäßigkeit ließen sich auch viele weitere Maßnahmen anführen, deren Nutzen im Vergleich zu ihren Kosten während der Pandemie im öffentlichen Diskurs thematisiert wurden. Dazu können beispielsweise in Deutschland die ad-hoc Beschaffungsmodalitäten von Schutzkleidung, die Umsetzung der Impfstrategie oder die unterschiedlichen Restriktionen zum Schutz der Bevölkerung durch die einzelnen Bundesländer gezählt werden.[331] Bemerkenswert ist jedoch die Emotionalität und Vehemenz der Kritik an manchen Maßnahmen und dem artikulierten Vorwurf der Unverhältnismäßigkeit in Teilen des öffentlichen Risikodiskurses (Vieten 2020: 8). Dies wird im nächsten Abschnitt unter den Begriffen der Risiko- und vor allem Krisenkommunikation thematisiert.

5.5.3. Krisen- und Risikokommunikation

Unternehmen sind wie wir zuvor gesehen haben auf die Kommunikation von Entscheidungen angewiesen, um einerseits diesen zur Umsetzung zu verhelfen und andererseits als Organisation zu funktionieren. Andernfalls könnten sie schwerlich unter den Mitgliedern oder Außenstehenden registriert werden. Dies ist insbesondere für Unternehmen hervorzuheben, „die ihre Grenzen und damit den Modus ihrer Reproduktion dadurch markieren, [dass] sie zwischen Mitgliedern und Nichtmitgliedern unterscheiden. Diese Differenz fungiert als das organisationstypische Erkennungssignal“ (Luhmann 1991: 202). Wenn man sich folglich der

[331] Existierende Krisenpläne in sieben untersuchten EU Mitgliedstatten, darunter Deutschland und Frankreich, hätten zwar bereits vor der Corona-Pandemie die Bedeutung gemeinsamer Kollaboration und abgestimmter Impfstrategien gefordert, jedoch „concerns are expressed in some plans that countries manufacturing vaccines may demand that they are produced for their own needs at the expense of their non manufacturing neighbours” (Mounier-Jack und Coker 2006: 14). Aus dieser Sicht zeigt die nationale Pandemie-Krisenvorsorge in Europa bereits eineinhalb Dekaden vor dem Beginn der Corona-Pandemie ein problematisches Vorgehen der Mitgliedstaaten mit Blick auf die transnationale Kooperation.

Frage der Risikobetrachtung annimmt, dann betrifft dies auch die Kommunikation von Entscheidungen, namentlich den Umgang mit Risiken durch Entscheidungen. Dies kann bedeuten, etwa ein Risiko zu akzeptieren oder Vorsorge zu treffen. Ebenso wird die Entscheidung artikuliert, wie man sich gegenüber einem Risiko verhält.[332] Informationen aus der Umwelt und Entscheidungen anderer Organisationen werden ebenfalls im Rahmen der Koppelung externer Informationsrezeption wahrgenommen. Als solche boten sich die staatliche Krisenkommunikation während den H1N1 und H1N5 Infektionsgeschehen bereits als Beispiele von Informierungsansätzen, denen mehr Unsicherheit als Klarheit folgte (Günther, Ruhrmann und Milde 2011: 16). Im Fall der Corona-Pandemie wurde das Ziel einer klaren Kommunikationsstrategie zum Beginn der Pandemie verfehlt. „Communication by authorities was clearly inadequate. During the initial stages of the epidemic, there was a clear discordance between the message given by authorities and public perception" (Ghanchi 2020: 806). Für ein besseres Verständnis von Krisenkommunikation einerseits und Risikokommunikation andererseits wollen wir im Folgenden beide Begriffe voneinander abgrenzen.

Risikokommunikation bezeichnet einen langfristig ausgelegten, strukturellen Ansatz zur Vermittlung von Informationen über einen Risikogegenstand (Günther, Ruhrmann und Milde 2011: 18). Dabei stellt die Anerkennung eines Risikos als relevanten Diskussionsgegenstand bereits eine Entscheidung qua Vorselektion dar. Neben der initialen Identifikation und Bewertung eines Risikos tritt zudem die Herausforderung in Erscheinung, das Risiko an die betreffenden Zielgruppen zu kommunizieren (Klinke und Renn 2002: 1071). Dabei ist es vorrangig von Bedeutung diejenigen Gruppen zu informieren, die von dem Risiko betroffen sein könnten, beispielsweise durch Verhaltens- oder Umweltbedingungen (Lupton 2006: 17). Denn es gilt der Grundsatz, dass effektive Kommunikation der Einordnung und Konzeptualisierung von Unsicherheit unter gleichzeitiger Vermittlung von Handlungs-alternativen zur Verringerung der Eintrittswahrscheinlichkeit dient (Frewer 2004: 395).

Unter den Umständen einer akuten Krise, wie der Corona-Pandemie sind hingegen Aspekte einer immanenten Benennung von möglichen und wahrscheinlichen Konsequenzen als Teil der *Krisenkommunikation* notwendig. Diese fokussiert sich auf konkrete Anlässe und thematisiert

[332] Risikokommunikation ist ein dynamischer Prozess der Diskursführung. „(…) [It] is typically defined as an interactive process that involves the exchange of information between parties about a sensitive issue" (Meredith et. al. 2008: 4). Gegenstand der Risikokommunikation ist die Translationsleistung zwischen Experten, Entscheidern und Bevölkerung. So können etwa neue gesellschaftlich relevante Risikokategorien thematisiert werden, wie etwa der islamistisch-begründete Terrorismus (vgl. Aradau und van Munster 2007: 33) oder an bereits im Kern bekannte Risiken mithilfe langfristiger Kampagnen erinnert werden. Dies betrifft auch gesundheitliche Risiken wie beispielsweise AIDS/HIV. So konnte die HIV-Neuinfektionsrate in Europa mithilfe von Risikokommunikation stark gesenkt werden (Elbe 2005: 113).

die reaktiven Maßnahmen auf eine sich abzeichnende oder bereits eingetretene Krise und versucht die Reputation von staatlichen Institutionen oder Unternehmen zu wahren oder wiederherzustellen (Utz, Schultz und Glocka 2012: 41). Dies war in den jeweiligen Fällen der drei thematisierten Pandemiewellen zu beobachten, als Unternehmen mit der Außenwelt oder ihren Mitgliedern über geeignete Maßnahmen via Krisenkommunikationskanäle in Austausch traten.[333] Doch eben dieses Vertrauen durch schnelle mediale Veröffentlichungen zu erhalten, ist von ebenso elementarer Bedeutung in einer modernen Informationsgesellschaft, wie auch problematisch.[334] Die Komplexität der Pandemien, ungewisse empirische Entscheidungsgrundlagen und fixierte, adaptionsschwere Krisenpläne erschwerten eine einheitliche Kommunikation seitens der Behörden und Unternehmen (vgl. Scheer et. al. 2010: 41). Dies führte schlussendlich auch zu Konfusion unter jenen, die auf Anweisungen der Behörden oder ihrer Arbeitgeber warteten und mehr strukturierte Anleitung erwarteten (Fineberg 2014: 1338; Ghanchi 2020: 806). Eine Erfahrung aus den unerfüllten Erwartungen an die Krisenkommunikation während der Pandemiewellen ist demnach, dass die Erwartungshaltung der Zielgruppen einbezogen[335] und die Entscheidungen klar kommuniziert werden müssen (Utz, Schultz und Glocka 2012: 44f.).

In diesem Informationsumfeld muss jede Kommunikation eines Unternehmens oder einer Behörden abgestimmt sein, da sie einmal im Umlauf aufgegriffen und auch dank sozialer

[333] Krisenkommunikation ist ihrem Wesen nach auf die Schadensbegrenzung bedacht und intendiert die Inklusion der relevanten Interessensgruppen, um deren Vertrauen in die getroffenen oder noch folgenden Entscheidungen zu sichern (Frewer 2004: 395). Ein Blick auf die Risikoeinschätzung im Vorfeld der Pandemiewellen verdeutlicht dies. Die WHO rechnete mit 2 bis 7,4 Millionen Toten durch den H1N1-Virusstamm. Bis 2011 zählte man allerdings nur 18.366 Fälle die durch ein Labor bestätigt werden konnten (Günther, Ruhrmann und Milde 2011: 31). Die globale Dimension der Pandemie blieb zum Glück aus, doch das Risikobewusstsein für deren potentielle Schwere und Tragweite für die unternehmerische Vorsorgeplanung wurde trotzdem aus dieser Krise heraus sensibilisiert. Der tatsächliche Verlauf der Pandemiewellen fand zunächst kaum Beachtung in der Krisenkommunikation und erschwerte die objektive Betrachtung.

[334] Ein Beispiel für die Folgen schlechter Krisenkommunikation kann im Fall von Hurrikan Katrina nachgezeichnet werden. Nachdem der Hurrikan in der Stadt New Orleans 2005 schwere Schäden verursachte, wurde über die Krisenkommutation an die betroffene Bevölkerung nachgedacht. Es bestand das Risiko weiterer Überflutungen und grassierender Infektionskrankheiten durch das verunreinigte Wasser und mangelhaften Hygieneumstände. Doch wie konnte man die Betroffenen erreichen, wenn die normalen Kommunikationskanäle wie Fernsehen und Internet ausgefallen und viele pflegebedürftige Personen isoliert waren? Etwa 5000 Kinder, so wurde geschätzt, waren durch die Ereignisse von ihren Eltern getrennt, viele hilfsbedürftige Menschen in Altenheimen allein gelassen worden und bedurften Unterstützung und Informationen. Tatsächlich waren etwa drei Viertel der durch den Hurrikan Katrina zu Tode gekommenen Personen Senioren (Meredith 2008: 4). Im Allgemeinen wird die Reaktion auf diese Naturkatastrophe im Sinne der Zusammenarbeit zwischen den Akteuren und Organisationen negativ bewertet und weitestgehend als Beispiel für das Versagen einer staatlichen Notfallplanung genannt (Perrow 2011: 49).

[335] Dazu gehören auch die Integration mehrerer Kanäle und Informationswege in ein abgestimmtes Kommunikationskonzept, welches ebenso die in der Krisensituation vorherrschende Emotionalität adressiert: „Another important implication is that organizations and PR departments should not only focus on rationalizations, but also address emotions (…). Framing a crisis as victim crisis reduced the perceived responsibility and in turn anger" (Utz, Schultz und Glocka 2012: 45).

Medien und Kommunikationskanäle vervielfältigt werden kann. Den richtigen Inhalt, Medium oder Ton einer Nachricht nach Außen – aber auch nach Innen – zu treffen, erwies sich als schwierig. In dieser Abwägung lag auch das inhärente Risiko, durch die Kommunikation einen negativen Eindruck zu erwecken und der Unternehmensreputation zu schaden. Trotz des Verantwortungstransfers der staatlichen Einrichtungen auf die privaten Unternehmen bringt die Öffentlichkeit ihre Erwartungen gegenüber der staatlichen Ebene zum Ausdruck[336], auch da diese den gewohnten Rechtsrahmen über Verordnungen einschränken kann (Dullien et. al. 2020: 8), wie es im Fall der Reaktionen auf das Corona-Virus zu beobachten ist[337].

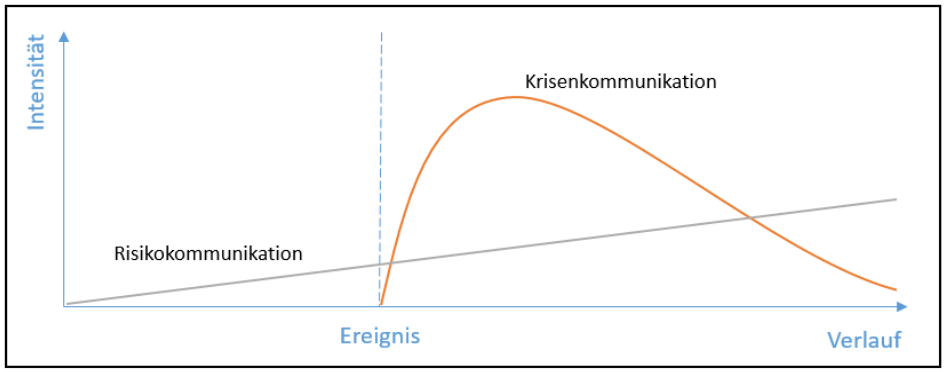

Abb. 5.7. Zeitlicher Verlauf der Risiko- und Krisenkommunikation. Eigene Darstellung.

Somit liegt ein schmaler Grat zwischen den Vorgaben der staatlichen Ebene und einer klaren Kommunikation innerhalb der Organisation mit dem Ziel eines proaktiven Schutzes der Mitarbeiter (Utz, Schultz und Glocka 2012: 41). Es ist von großer Bedeutung, auf den richtigen Zeitpunkt und Tonfall der Nachricht zu achten. Authentizität ist die Währung der Krisenkommunikation und erfordert auch die Erwähnung negativer Aspekte, um die Glaubwürdigkeit in den Augen der Zielgruppen zu bewahren (Ng und Lean 2012: 309). Die Übersetzung der Fachausdrücke und der Reduktion von Komplexität zur Abstraktion des Problems gelten hingegen als Grundvoraussetzung, um ein Basisverständnis der Öffentlichkeit und daraus Zustimmung zu entwickeln (Scheer et. al. 2010: 92). Denn die Öffentlichkeit registriert zumeist nur die Krisenkommunikation als Sprachrohr von Unternehmen, nicht aber deren (nicht nach außen kommunizierten) internen Prozesse und Entscheidungsgrundlagen.

[336] Im Frühjahr 2021 erregte das Angebot mehrerer Dax30-Konzerne in Deutschland Aufmerksamkeit, als diese die Bereitstellung ihrer Ressourcen und Strukturen zur Impfung von Mitarbeitern und Angehörigen anboten, um dadurch die unzureichenden Kapazitäten zur Umsetzung der Impfungen zur Verfügung zu stellen (Tagesschau 2020). Ein interessanter Schritt, wenn man bedenkt, dass alle Impfmaßnahmen im Sinne der nationalen Koordination während der Corona-Pandemie durch staatliche Autoritäten organisiert werden sollten.
[337] Als solche Beispiele können die sich teilweise widersprechende Bekanntmachung von Bund und Ländern in Deutschland zu Kontaktbeschränkungen oder zur Impfstrategie genannt werden (Tagesschau 2020).

5.5.4. Aktivierung von Krisenplänen

Wie in den drei zuvor skizzierten Problemfeldern mit Blick auf Pandemien zu sehen war, gereichte eine Entscheidung selbst zum Risiko und dies bedeutete in Zeiten der Unsicherheit vor allem, dass vorbereitete Strukturen und Erkenntnisse entweder nicht verlässlich waren oder aufgrund mangelnder Adaptionsfähigkeit nicht mit der Dynamik der Krise wachsen konnten. Eine weitere Problematik entstand aus der Bewertung des richtigen Zeitpunkts von Maßnahmen und deren Kommunikation. Im Fall einer Pandemie, trennt ein Graubereich die aktive Krisenphase und die vorrausgehenden Phase erhöhter Wachsamkeit. Während die zweite Phase des WHO-Modells zur Beobachtung der Entwicklung und Vorbereitung von Maßnahmen dienen sollte, wurde schnell klar, dass kaum einer der Beteiligten wusste, ob man sich noch in der Eskalationsphase oder bereits der Pandemiephase befand (Günther, Ruhrmann und Milde 2011: 10f.). Jedoch fällt dieser Unterscheidung große Bedeutung zu. Der Moment der Planaktivierung kennzeichnet den Übergang vom Normalbetrieb in einen Notfallbetrieb. Zudem besitzen Krisenstäbe häufig qua Natur explizite Sonderkompetenzen, welche die normale Hierarchie im Unternehmen vorrübergehend umgehen oder aussetzen können. Daher ist der formelle Schritt in den Notbetrieb dokumentationsrelevant.

Eine allgemeine Differenzierung bietet sich daher an: Allgemein gesprochen muss ein Vorfall noch keine Krise sein. Ferner muss eine Krise nicht automatisch in einem Schaden für ein Unternehmen resultieren, denn das Krisenmanagement und Krisenkommunikation können dazu beitragen die Entwicklung der Krise zu beeinflussen.[338]. So kann ein Feuer in einem Büroflügel noch unter Kontrolle gebracht werden, bevor Mitarbeiter oder de Prozesskontinuität gefährdet werden. Die Ausbreitung einer Influenza in einer Region kann als Gefahr erkannt und notwendige Maßnahmen rechtzeitig vorbereitet werden. Erst wenn der Vorfall einen Grenzwert überschreitet, zum Beispiel konkret die Gesundheit der Mitarbeiter bedroht oder die Reputation des Unternehmens gefährdet ist, entscheidet der Krisenstab über die Aktivierung der Krisenpläne beziehungsweise der nächsten Eskalationsebene. Erst dann handelt es sich um eine Krise und eine relevante Ausgangsgrundlage für Krisenmanagement.

Ebenfalls ist anzumerken, dass ein BCM-Fall zwar meistens auch eine Krise ist, aber dies nicht umgekehrt gelten muss. Die Entwendung und Veröffentlichung von sensiblen Unternehmensdaten beispielsweise ist keine Angelegenheit für die BCM zuständig wäre, solange die Informationen noch auf den Datenbanken verfügbar sind. Die Reputationskrise ist

[338] Eine Unterscheidung dazu lautet, dass „[t]he difference between an emergency and a disaster is in the system's capacity to respond to and manage the crisis. A capable system can respond to, manage, and prevent an emergency (or accident) from turning into a disaster" (Almedom 2011: 146).

aus Sicht der Kontinuitätsplanung irrelevant. Würden jedoch die Daten nicht mehr verfügbar sein, würde dies einen BCM-Fall und einen gleichzeitigen Krisenfall bedeuten. Durch eine Unterscheidung der Zuständigkeiten kann die richtige Personengruppe involviert werden, sobald sich eine mögliche Eskalation der Ereignisse abzeichnet Die Inkorporation der Mitarbeiter, sowie der externen Ansprechpartner sollte als Lehre aus den Pandemiekrisen ebenfalls nach einem Plan verlaufen. Wie das Beispiel des japanischen Energiekonzerns TEPCO im Fall von Fukushima zeigte, war eine desaströse Krisenkommunikation während einer der größten Krisen seit den Anschlägen vom 11. September 2001 geeignet, den Reputationsschaden und Vertrauensverlust zu steigern (Ng und Lean 2012: 309).

5.6. Zusammenfassung - Entwicklungsstand der Risikomitigation im analogen Zeitalter

Zusammenfassend lässt sich mit Blick auf die Evolution der traditionellen Risikokontrolle in Unternehmen in Form von BCM und Krisenmanagement im analogen Zeitalter festhalten, dass die unternehmensinterne Sicherheitsproduktion durch eine Verschiebung in der Wahrnehmung von seltenen Schadensereignissen vorangetrieben wurde (Braes und Brooks 2010: 16). Die Anschläge des 11. Septembers 2001 führten im globalen Umfang die Verwundbarkeit der kritischen Infrastruktur vor Augen. Die mediale Dimension des Ereignisses sowie seine Unmittelbarkeit veränderten die Risikowahrnehmung in der Gesellschaft ebenso wie in Unternehmen (Williams 2003: 512). Das daraus abgeleitete Zielbild einer verstärkten Widerstandsfähigkeit gegen diese Art von Ereignissen rückte in den Mittelpunkt der Aufmerksamkeit (LaPorte 2007: 60) und wurde durch die Erfahrungen aus der Corona-Pandemie um die Forderung nach Flexibilität und Agilität der Vorsorgeplanung erweitert. Die Herausforderungen der globalen Lieferkette erweiterte dieses Bild mit der Ausdehnung der organisatorischen Verantwortung auf exogene Zulieferer und Dienstleister (Behnezhad, Connett und Nair 2013: 78). In der ethnographischen Untersuchung konnte dieser entstehende, umfassende Blick auf die Risikoexposition seitens der Experten und Praktiker beobachtet werden und auch ein Bewusstsein festgestellt werden, dass die Sicherstellung der Kontinuität Vorsorge benötigt und dadurch die Bedeutung der Sicherheitsproduktion in Unternehmen hervorhebt. Als Konsequenz der kontinuierlichen Weiterentwicklung etablierte sich die traditionelle Risikokontrolle in Gestalt von BCM und Krisenmanagement als fester Bestandteil im Umgang von Unternehmen mit der Unsicherheit bezüglich exogener, geschäftsgefährdender Problemstellungen.

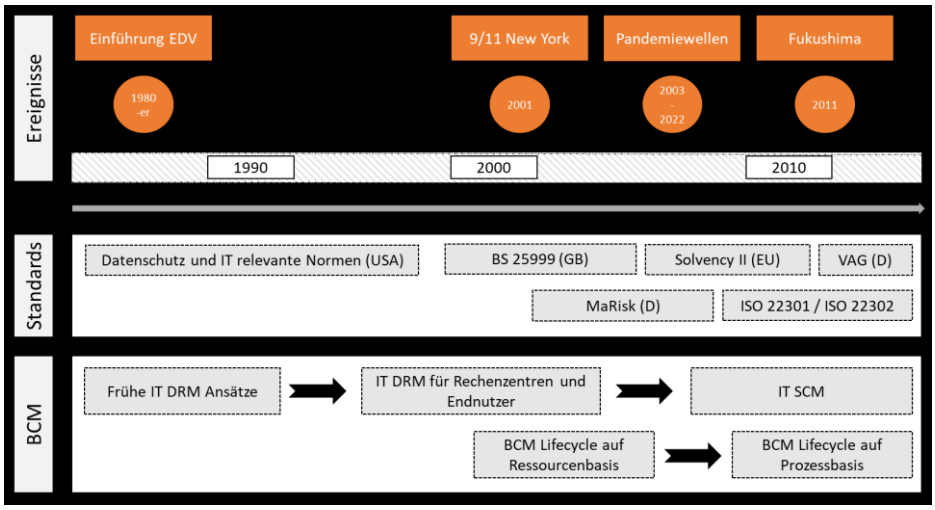

Abb. 5.8. BCM im Vergleich zu Ereignissen und der Entwicklung von nationalen und internationalen Standards. Eigene Darstellung.

Wie wir im nächsten Kapitel sehen werden, verändern vorrangig die Implikationen neuer Technologien den Schutzanspruch von Unternehmen und ihrer vitalen Schutzwerte. Der digitale Wandel hat wesentlichen Einfluss auf die Verwundbarkeit von Unternehmen durch unbekannte Risiken und Krisenszenarien.[339] Diese Perspektive wurde als Erkenntnis aus der ethnographischen Untersuchung, Hintergrundgesprächen mit Praktikern und Beobachtung eines sich verändernden Risikodiskurses festgestellt und soll im nächsten Kapitel eingeführt werden. Der sich im Zuge der Digitalisierung abzeichnende neue Ansatz zur Risikokontrolle verlässt das traditionelle Risikoverständnis des analogen Zeitalters, wie in diesem Kapitel beschrieben wurde, und setzt statt Objekten wie Ressourcen nun die Prozesse und systemischen Verbindungen der Organisation mit Blick auf die Prozess- und Kommunikationskontinuität in den Mittelpunkt. Die Methoden und Ansätze des analogen Zeitalters, vorrangig BCM und Krisenmanagement werden in diesem neuen Kontext immer noch benötigt, doch im Kontext des Informationszeitalters, der einhergehenden Bedeutung von Informationen und der diese verarbeitenden Systeme um die Dimensionen der Vertraulichkeit und Integrität erweitert. Diese Aspekte werden im nächste Kapitel erläutert und der Übergang vom traditionellen zum neuen, systemischen Verständnis der Risikokontrolle und Sicherheitsproduktion in Unternehmen eingeführt.

[339] Während der ethnographischen Untersuchung konnte auf Konferenzen in Europa (Workshop am 29.09.2015) und in Asien (Workshop am 10.11.2015) der Risikodiskurs unter den Experten beobachtet werden. Während die Experten in Asien verstärkt Naturkatastrophen und politische Risiken als Grundlage ihrer Vorsorgeplanung in den Blick nahmen, betonten Experten aus Europa eher die Rolle der unterbrechungsfreien IT. Dadurch konnte auch die subjektive Prägung des Risikodiskurses nachvollzogen werden, dessen Schwerpunktsetzung von lokalen oder regionalen Risikoexposition abhängt. Allerdings wurde auch übergreifend die Bedeutung der IT für die Prozesskontinuität hervorgehoben, insbesondere da die gleichzeitige Zusammenlegung von lokalen Rechenzentren die Dependenz von einzelnen IT-Infrastrukturstandorten erhöhte.

6. Digitalisierung als Chance und Gefahr - Risikokontrolle im Cyberzeitalter

Das vorausgehende Kapitel zeigte die Entstehung und Etablierung der traditionellen Risikokontrolle in Unternehmen, geprägt von den Herausforderungen und Sicherheitsdispositiven einer auf Objekte und Ressourcen fokussierten Risikoperspektive im analogen Zeitalter. Wie aus den ersten beiden Kapiteln dieser Arbeit hervorgeht, durchliefen Unternehmen, aber auch der traditionelle Risikobegriff im Informationszeitalter einen sukzessiven Wandlungsprozess, welcher durch die Reaktionen auf die exogenen Herausforderungen im Zuge der Corona-Pandemie beschleunigt und deutlicher als Zäsur manifestiert wurde. Daher soll in diesem Kapitel der Wandel und die Bedrohungslage durch die Digitalisierung für die Prozess- und Kommunikationskontinuität von Unternehmen dargestellt werden. Es wird daher davon zu sprechen sein, wie die Digitalisierung bestehende Normen der Risikokontrolle novelliert und welche Implikationen durch die Vernetzung von Systemen für die Sicherheitsproduktion in Unternehmen entstehen. Gleiches gilt für die Folgen, welche unter diesen Bedingungen für die Prozesskontinuität zu erwarten sind und vor allem welche Rolle die Verfügbarkeit von Informationen für die Risikokontrolle von Unternehmen haben wird. Zunehmende Gefahren wie die Cyberkriminalität oder komplexe technologische Risiken bilden das Gegengewicht zu ökonomischen Rationalitäten (Choras et. al. 2015: 689).

Wie sich im Rahmen der ethnographischen Beobachtung zeigte und hier im Folgenden dargelegt werden soll, veränderten sich die Konnotation und Praktiken des traditionellen Risikobegriffs erheblich. Informationen wurden nun als die Schlüsselkomponenten unternehmerischer Aktivität im Planungsprozess der Kontinuitätsvorsorge einbezogen.[340] Doch nicht mehr nur die Verfügbarkeit einer Information erscheint aus Sicht der Experten relevant zu sein, vielmehr entwickelten sich auch die Integrität und Vertraulichkeit zu gleichwertigen Schutzzielen und bewirkten dadurch weitreichende Änderungen der Anwendungspraktiken der unternehmerischen Risikokontrolle, welche wir hier als Resilienz einführen werden. Zu diesem Zweck werden in diesem Kapitel die (1) Anforderungen an eine effektive Risikokontrolle im

[340] Dies zeigte sich in Gesprächen mit den Fachfunktionen des Unternehmens, welche die Bedeutung von funktionsübergreifenden Kontrollen und Vorsorgemaßnahmen den sich ändernden Risikodiskurs insbesondere im Licht der Digitalisierung und Erkenntnis über die zunehmende Komplexität und Interdependenz der IT-Systeme begründete. Wie im zweiten Kapitel dargelegt wurde, erfolgte die ethnographische Untersuchung über einen langen Zeitraum in einem DAX-30 gelisteten Unternehmen. Dabei konnten vertrauliche Hintergrundgespräche geführt werden, sowie Beobachtungen im Rahmen von Projekten, Analysen und Workshops getätigt werden. Die Vertraulichkeit der beobachtenden Teilnahme erforderte jedoch, dass ausschließlich Gedächtnisprotokolle angefertigt werden konnte, welche hier – wie auch schon im Fall der Beobachtungen die im fünften Kapitel Eingang fanden – zur Erkenntnis der Veränderung des Risikodiskurses und der Selbstreferenz in Unternehmen in Form von Resilienz genutzt wurden.

Informationszeitalter unter den veränderten Bedingungen der Unsicherheit aufgrund technologischer Interdependenzen und Schutzwerte betrachtet. Dieser Abschnitt wird zudem die Reflektionen aus der ethnographischen Untersuchung beinhalten, welche sich in der Veränderung des Risikodiskurses im Unternehmen und Etablierung einer Selbstbeobachtung der Organisation im Sinne ihrer systemischen Gesamtheit basierend auf Anschlussoperationen und Kommunikation thematisieren. Dies wird insbesondere in der detaillierten Betrachtung des (2) Datenverlustes im Einklang mit dem Wert von Informationen von Bedeutung sein, welcher auf der Grundlage einer eigenen Kategorisierung unter Berücksichtigung der Beobachtungen und Erkenntnisse im Unternehmen basiert. Darauf aufbauend sollen (3) ausgewählte Fallbeispiele die Dimension potentiell geschäftsgefährdender Risiken die dringende Notwendigkeit zur Überarbeitung der traditionellen Methodik der Risikokontrolle und ihrer originären Anwendungspraktiken in Gestalt des BCM und KM auf der Grundlage einer Abbildung der aktuellen Forschungslage zu diesen Bedrohungen aufzeigen.[341] Durch die Kombination der ethnographisch ermittelten Erkenntnisse zum veränderten Risikodiskurs und der Bedeutung der Datenkontinuität sowie der objektiven Beschreibung der gegenwärtigen Cyberbedrohungen werden schließlich die Implikationen für die unternehmensinterne Risikokontrollsysteme im Cyberzeitalter abgeleitet. Die konkreten Umsetzungsempfehlungen werden sich im anschließenden Themenblock in Form der Handlungsfelder zur Implementierung einer resilienten Organisation im siebten Kapitel anschließen. Anhand dieser Struktur wollen wir die Risikoexposition für Unternehmen im Informationszeitalter beleuchten und die spezifischen Gründe zur methodischen Weiterentwicklung darlegen.

6.1. Die Orientierung an Prozessen und Systemen – der Resilienzbegriff

Beginnen wir mit einem fiktiven, aber mit Blick auf die Fallzahlen geläufigem Beispiel, um die Exposition von Netzwerken und Implikationen für Organisationen durch einen Angriff mit Schadsoftware zu verdeutlichen: Die Mitarbeiter eines Unternehmens betreten die Büroflächen ihres Arbeitgebers, starten die Computer und beabsichtigen den Arbeitstag zu beginnen. Doch die Monitore der Computer bleiben schwarz, die Laufwerke und Daten sind nicht abrufbar und statt der bekannten Bedienoberfläche erscheint lediglich eine Nachricht auf dem Bildschirm. Diese Nachricht wurde von einem Schadprogramm dort platziert und nennt eine Lösegeldsumme als Bedingungen zur Freigabe der Daten, welche mithilfe des eingeschleusten Programms verschlüsselt worden sind. Nur durch Eingabe eines Entschlüsselungscodes können

[341] Die Auswahl und Einordnung der vier Fallbeispiele werden zu Beginn des Abschnittes genauer erläutert. Die übergeordnete Gemeinsamkeit liegt in dem aus den Bedrohungskategorien abgeleiteten Anforderungskatalog an die resiliente Organisation im Informationszeitalter.

die Daten wiederhergestellt werden und die Zeit drängt, da die Produktion, Kommunikationssysteme und Schnittstellen zu Geschäftspartnern und Kunden betroffen sind. Die Entscheidungsträger des Unternehmens befinden sich in einem Dilemma: entweder sie bezahlen die geforderte Summe in der Hoffnung, dass daraufhin die Entschlüsselung erfolgt oder akzeptieren den Verlust von essentiellen Daten und eine Geschäftsunterbrechung kritischen Ausmaßes. In Ermangelung einer im Vorfeld etablierten Mitigationsstrategie verbleibt die Wahl zwischen zwei gefährlichen Extremen.

Dieses Beispiel zeigt die Implikationen einer unzureichenden ex-ante Bewertung des Risikos einer Geschäftsunterbrechung und überdies die ungenügende Abdeckung der unternehmensrelevanten Schutzwerte durch eine umfassende Vorsorgeplanung. Denn der Schutz von essentiellen, das bedeutet materiellen und immateriellen Werten zur Fortführung der operativen Tätigkeiten ist für Unternehmen von großer Bedeutung (Dierkes et. al. 2005: 39). Diese Werte umschreiben die vitalen, zum Selbsterhalt notwendigen Ressourcen, auf welchen die Wertschöpfungskette, Prozesse und vor allem Entscheidungsfreiheit von Unternehmen basieren (Kahan, Allen und George 2009: 7). Abgesehen von der starken Rolle des Cyberszenarios, deckt sich dieser Fall bis auf eine Ausnahme mit dem Verständnis der traditionellen Risikokontrolle.[342] Das Novum der durch die Digitalisierung eingeführten globalen, das heißt hier vor allem systemischen Vernetzung von Anwendungen, Plattformen und Infrastrukturkomponenten erweiterten das Schutzziel und den Risikobegriff erheblich.

Somit stellt sich die Frage, wie Unternehmen die interne Sicherheitsproduktion mit den Herausforderungen der vernetzten und prozessual-systemischen Funktionsweise der digitalen Umgebung und Funktionsweise zusammenbringen können? Die Antwort wird in den folgenden Abschnitten in Form eines differenzierten Ressourcen- und Informationsschutzverständnis vorgestellt werden, welches insbesondere die Beschleunigung der Vernetzung und inhaltliche Ausdehnung des Sicherheitsdispositivs gegenüber Unternehmen reflektiert. Dazu werden zunächst die entscheidenden (1) Veränderungen für den Risikobegriff im Informationszeitalter erläutert. Anschließend wird die (2) Risikoexposition für MNU durch die Digitalisierung reflektiert. Den Abschluss bildet die Einführung des (3) neuen Risikokontrollsystems, welches in dieser Arbeit als Resilienz bezeichnet wird und – wie zu zeigen sein wird – in Unternehmen

[342] In der traditionellen Risikoterminologie werden Risikoobjekte auf der Basis benötigter Ressourcen wie Gebäude, Mitarbeiter oder einzelner IT-Applikationen definiert, für die Kontrollen und Wiederherstellungspläne implementiert werden müssen, um den Kontinuität sicherzustellen (Almedom 2011: 150).

zur Beschreibung der internen Sicherheitsproduktion verwendet wird, um die Kontinuität von Prozessen und Kommunikation sicherzustellen.

6.1.1. Veränderung des Risikoverständnis

Die Vermeidung eines Prozess- und Kommunikationsabbruchs nach Luhmanns Organisationsverständnisses bildet eine Gemeinsamkeit zwischen analogem und digitalem Zeitalter aus organisationstheoretischer Sicht. Diese Konstante der unternehmerischen Sicherheitsproduktion unterscheidet sich allerdings mit der zunehmenden Einführung von digitalen Strukturen, indem die ressourcen-orientierte Risikokontrolle nach traditionellem Muster nicht mehr in der Lage ist, die systemische Verflechtung und prozessuale Komplexität abzudecken, welche allerdings im Informationszeitalter eine elementare Voraussetzung ist, um die Anschlussoperationen anzustoßen, beziehungsweise Entscheidungen zu kommunizieren. Dieser Unterschied zwischen traditionellem Risikobegriff und dem neuen, systemischen Verständnis kennzeichnet die Veränderung des Risikobegriffs im Informationszeitalter. Diese Erkenntnis beruht auf der ethnographischen Untersuchung, deren Schlussfolgerungen für die Selbstreferenz und Umsetzung über Resilienz in diesem Abschnitt verarbeitet werden. Ferner werden wir die genaue Betrachtung der Risiken und dem Wandel der unternehmensinternen Begriffsverwendung beziehungsweise Praktiken weiter unten mit den Fallbeispielen klären und dadurch eine objektive Auswertung des Forschungsstands zu den Bedrohungen im Informationszeitalter anfügen.

Aus der vorausgehenden Betrachtung des analogen Zeitalters haben wir gesehen, dass im Rahmen der traditionellen Risikokontrolle die Sicherheitsproduktion durch Anwendungspraktiken wie BCM und KM umgesetzt wurde. Dieses Verständnis hat auch weiterhin im digitalen Zeitalter Bestand und Relevanz. Allerdings wird der Blick auf die Schutzwerte und Schadensbegriffe erweitert und eine Differenzierung zwischen Verfügbarkeit von Ressourcen, insbesondere von Informationen einerseits und der Integrität und Vertraulichkeit anderseits vorgenommen. Der erste Aspekt wird weiterhin von BCM und KM umgesetzt, doch kommen die Praktiken des IT Service Continuity Management (ITSCM) hinzu, um die Prozesskontinuität in Anbetracht der Komplexität der IT-Systeme sicherzustellen. Ferner wird der Informationsschutz stärker einzubinden sein, um die Exklusivität und Integrität von Schutzwerten wie Informationen abzudecken Beide Anwendungspraktiken wurden bereits seit Längerem in Unternehmen eingesetzt, durch ihre Zusammenführung in ein Konzept der Risikokontrolle einerseits und dessen flächendeckenden Ausdehnung auf die gesamte Organisation andererseits repräsentieren sie jedoch materielle

Veränderungen. Dazu wollen wir beide Felder genauer betrachten und die Rolle der veränderten technischen und rechtlichen Rahmenbedingungen durch die fortschreitende Digitalisierung berücksichtigen. Zunächst stellt sich die Frage wie sich die Relevanz der Prozessverfügbarkeit im Informationszeitalter und bezogen auf die Abhängigkeit von IT-Systemen auswirkt.

6.1.1.1. Kritische Infrastruktur und rechtlicher Rahmen im Informationszeitalter

Die kritische Infrastruktur diente uns bereits im fünften Kapitel als Übersetzung der Sicherheitsproduktion in Unternehmen auf die Sicherheitsdispositive der Gesellschaft. Dies zeigt sich zwar auch in anderen Tätigkeitsfeldern, allerdings sticht im Fall der kritischen Infrastruktur die unmittelbare Abhängigkeit zwischen der Verantwortung privater Unternehmen und Existenzsicherung der Bevölkerung hervor (Brzoska, Neuneck und Scheffran 2021: 6f.). Die Beziehung zwischen staatlichen Autoritäten und MNU kann ebenfalls in diesem Fall betrachtet werden, beispielsweise auf dem Bereich der Steuerung von Cybersicherheit, hier verstanden als inhaltliche Gestaltung von Schutzkonzepten und –Ansprüchen im virtuellen Raum. Durch die Abhängigkeit von einer kontinuierlich funktionsfähigen IT-Infrastruktur zur unterbrechungsfreien Versorgung der Bevölkerung mit essentiellen Gütern und Leistungen, entwickelte sich auch ein Sicherheitsdispositiv, welches sich auf eine effektive Risikokontrolle des Cyberraum richtet (Gomez und Whyte 2021: 6). Die dominante Rolle von privaten Unternehmen im IT-Sektor, wie wir es im dritten Kapitel bereits unter dem Überbegriff IT-Kompetenz gesehen haben, demonstriert dabei die Aufgabenverteilung zwischen staatlicher und privater Ebene zur Sicherheitsproduktion des digitalen Raums (Kuerbis und Badiei 2017: 470).

Doch die Auslagerung der Verantwortung in die private Trägerschaft führte auch zu einem gewissen Grad an Intransparenz aus Sicht der Gesellschaft, da der Prozess der Sicherheitsproduktion in Unternehmen nach außen nicht kommuniziert wird (Carr 2016: 52). Auch bleibt eine asymmetrische Verteilung von Macht und Handlungsfähigkeit im Bereich der Gewährleistung von Cybersicherheit auf Seiten von Unternehmen (Huang et. al. 2021: 262), auf welche (supra-)staatliche Akteure mit der Definition von Rahmenwerken und rechtlichen Anforderungen reagieren (Kaufmann 2015: 514). Aufgrund der Bedeutung von Unternehmen für die Sicherstellung der Funktionsfähigkeit des virtuellen Raums stehen sie im Fokus der von staatlichen Autoritäten erlassenen Aufgabenbeschreibung und Regulation (Carr 2016: 50). Daher lohnt es sich im Folgenden einen Blick auf die Anforderungen der staatlichen Seite für die Sicherheitsproduktion von Unternehmen hinsichtlich ihrer IT-Infrastruktur, Anwendungen und Informationssicherheit zu werfen.

Vereinzelte Rechtsnormen regulieren die Anforderungen an datenverarbeitende Unternehmen und tragen der Bedeutung der Abhängigkeiten einerseits und der Beziehung zwischen staatlicher und privater Ebene andererseits Rechnung (Cavelty 2013: 116). Dies scheint jedoch unter den Bedingungen der Digitalisierung, globaler Geschäftsprozesse und komplexer Interaktionsbeziehungen, welche sich nicht nur deckungsgleich mit den Rechtsräumen von Nationalstaaten wiederfinden lassen, problematisch (Bratton 2015: 10; Huang et. al. 2021: 626). Praktiken und Technologien, welche in einem Land verboten sind, können über Server im Ausland angeboten werden. Die effektive Umsetzung diese Regeln flächendeckend kontrollieren zu können ist daher eine große Herausforderung (Lepping und Palzkil 2016: 19). In Folge versuchen Abkommen oder supranationale Lösungen die Regulation des Cyberraums anzugehen und so die Grenzen der Jurisdiktion des Nationalstaates sukzessive auszudehnen. Die Beanspruchung des Cyberraums folgt dem Regelungsanspruch im analogen Raum und kann weitreichendere Auswirkungen in der virtuellen Sphäre haben, wie es beispielsweise die Europäische Datenschutzgrundverordnung zeigt (Huang et. al. 2021: 626).

Unter der Regulation zur Cybersicherheit ist ebenfalls eine Verantwortungsdelegation von Vorschriften zu Schutzmaßnahmen auf Seiten der privaten Betreiber kritischer Dienstleistungen und Infrastruktur zu verstehen (Cook 2010: 25). Diese Unternehmen sind als verantwortliche Betreiber der relevanten IT-Systeme und Datenbanken dazu verpflichtet, Mindestschutzansprüche zu erfüllen (Carr 2016: 52), die neben dem Informationsschutz auch mit Blick auf die Sicherstellung der Prozesskontinuität über die Jahre an Qualität zugenommen haben. In Deutschland sind beispielsweise die Ausführungen der Paragraphen 91 und 93 im Aktiengesetz (AktG) von Relevanz, indem die Pflichten von Unternehmen zur Risikokontrolle geschäftsgefährdender Risiken hervorgehoben werden (Hessel und Rebman 2021: 266). Auch spezielle Vorgaben für Branchen wie beispielsweise das Gesundheitswesen konkretisieren mit Hinsicht auf deren Systemkritikalität seit 2020 gesonderte Standards zur IT-Sicherheit, wie beispielsweise durch das „Patientendaten-Schutz-Gesetz (PDSG)“ (Dochow 2022: 103).

In der Finanzbranche kann zudem auf die kürzlich abgeschlossene Konkretisierung und damit unmittelbar wirksame Überarbeitung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) verwiesen werden, welche Prüfungs- und Kontrollpflichten für die Betriebs- und IT Organisation zur Prozesskontinuität anführt (BaFin 2022). Besondere Bedeutung während der ethnographischen Beobachtungen wurde seitens der Experten der neuen DORA-Regulation[343]

[343] DORA steht für Digital Operational Resilience Act und verpflichtet Unternehmen in der Finanzbranche konkrete Maßnahmen in der IT-Sicherheit und im IT Service Continuity Management vorzunehmen, um Geschäftsunterbrechungen zu vermeiden. Die Gespräche mit Experten aus dem Unternehmen im Jahr 2022 zeigten

beigebracht, welche auf europäischer Ebene die IT-Standards für Finanzdienstleister in der EU und analog zur Datenschutzgrundverordnung (DSGVO) definiert und auch regulierenden Charakter auf Geschäftspartner außerhalb der europäischen Jurisdiktion erwarten lässt (Deloitte 2022). Die Aufmerksamkeit der Organisation gegenüber dieser neuen Regulation ähnelte der Bedeutung der DSGVO, welche durch eine maximale Strafzahlung von vier Prozent des Unternehmensjahresumsatzes auf Verletzungen der Vorgaben erheblichen Anpassungsdruck innerhalb von Unternehmen in der EU erzeugte. Auch in diesem Fall wurde während der beobachtenden Teilnahme eine ähnliche Reflektion der Fachfunktionen an dieser europäischen Gesetzgebung festgestellt.[344] Insbesondere die Anforderungen an das Testen von Wiederanlaufplänen (Art. 21-24 DORA) und anderer Spezifikationen unter dem Überbegriff „operational resilience" ließen die beteiligten Experten zur intensiven Überprüfung des Status Quo zu veranlassen, um eine Regeleinhaltung sicherzustellen.[345]

Die Komplexität von MNU macht die Umsetzung solcher Regulation zwar aufwendig, aber Großunternehmen verfügen zumeist über die finanziellen Möglichkeiten zur Umsetzung der Schutzstandards sowie Fachabteilungen für juristische und regulative Fragen. Problematisch ist jedoch die Abdeckung von kleinen und mittleren Betrieben, deren verfügbare Kapitalbasis keine substanziellen Investitionen in IT-Sicherheit zulässt (Schulze 2021: 4), aber dennoch wesentlichen Anteil an der gesellschaftlich relevanten Sicherheitsproduktion haben, wie dies beispielsweise kleinere Krankenhäuser oder Labore in der Corona-Pandemie gezeigt haben (Dochow 2022: 103). Die Notwendigkeit zur Regulation ergibt sich wie eingangs beschrieben haben aus dem Schutzanspruch der staatlichen Autoritäten, aber auch aus der gestiegenen Risikoexposition, welche in Referenz auf die staatlich-private Partnerschaft, auch die

die beigemessene Relevanz dieser Regulation für die Verbindung zwischen kritischen Prozessen und IT-Systemen für die umfangreiche Tests vorgeschrieben werden. Ein Manger aus dem Risikomanagement hielt dazu fest, dass Regulationen wie DORA die Struktur von Risikokontrollsystemen in Unternehmen stark beeinflussen werde und man daran sehen könne, dass die Regulatoren mehr Aufsicht über Unternehmen wahrnehmen würden (Workshop 02.12.2022).

[344] Anhand der Einführung der DSGVO ließ sich während der ethnographischen Untersuchung im Frühjahr 2017 durch Gespräche mit einem Unternehmensberater und der zuständigen Expertin in der Unternehmenszentrale für diese Thematik eine große Aufmerksamkeit für diese Regulation beobachten. Es war aufschlussreich zu betrachten, wie die ökonomische Rationalität des Unternehmens durch die Aussicht auf eine mögliche Strafzahlung von vier Prozent – immerhin im Extremfall mehrere Milliarden Euro im Fall des Unternehmens – mit Investitionen und Ressourcen für die Implementierung eines Incident Managementsystems sowie von Berichtswegen reagiert (Hintergrundgespräch 10.03.2017).

[345] Die ethnographische Beobachtung im Umgang mit den neuen Anforderungen der DORA zeigte auch den Übergang von singulären Lösungsansätzen hin zu einer systemischen Abdeckung von Sicherheitsrisiken im Unternehmen, wie durch die Regulation gefordert. Insbesondere die Einbindung von externen Dienstleistern wie Cloud-Betreibern, Software-Dienstleistern oder Infrastrukturanbietern wurde als signifikante Steigerung der unternehmerischen Verantwortung für die gesamte Wertschöpfungskette gewertet. Dadurch erstrecke sich laut einem Experten aus dem IT-Funktion die Selbstbetrachtung der Organisation weit über ihre Grenzen hinaus und fordere ein Umdenken, wie Dienstleister in die eigene Vorsorgeplanung in Form von Tests und Audits eingebunden werden müssen (Workshop 02.12.2022).

Sicherheitsdispositive der Bevölkerung berücksichtigen müssen. Daher stellt sich die Frage, welche konkreten Risiken und Kategorisierungen die gestiegenen Aufwände von Unternehmen in der internen Kosten-Nutzen-Abwägung rechtfertigen können und eine Weiterentwicklung der unternehmensinternen Risikokontrolle notwendig machen? Diese Frage soll der nächste Abschnitt mithilfe einer Einordnung relevanter Risiken im Informationszeitalter leisten.

6.1.1.2. Verfügbarkeitsrisiken im Informationszeitalter

Die Abhängigkeit moderner Produktionstechniken und Geschäftsprozesse von der IT-Ressource, wie wir es im dritten Kapitel gesehen haben, beeinflusste das Risikoverständnis unter zunehmender Inklusion des technologischen Risikos. In der bereits zitierten Studie der BCM Academy aus dem Jahr 2016 sagten 69 Prozent der befragten Unternehmen aus, dass ein Ausfall der IT-Infrastruktur das wahrscheinlichste Szenario[346] einer Geschäftsunterbrechung sei (BCM Academy 2016: 28). Bereits seit Beginn der Digitalisierung und der steigenden Verbreitung und Verknüpfung von IT-Systemen gewann eine Risikowahrnehmung der Abhängigkeit von digitalen Ressourcen an Gewicht. Der zu erwartende Schaden durch einen (zeitlich befristeten) Ausfall wurde zu Beginn des 21 Jahrhunderts bereits auf drei bis sieben Prozent der Kosten eines Rechenzentrums[347] geschätzt (Cerullo und Cerullo 2004: 75) und ist analog zu den Komplexitätssteigerungen des Technologieeinsatzes gestiegen.

Neben dem potentiellen Verlust, beispielsweise durch nicht getätigte Verkäufe oder verspätete Handelsaufträge an den Wertbörsen, zählen im IT-Umfeld insbesondere die Kosten eines Ausfalls der IT-Infrastruktur zu den finanziellen Belastungen. (Fischer 2007: 177). Die Länge eines Ausfalls des Rechenzentrums durch die Aufwände zur Reallokation der Daten, Schäden an Systemen oder der komplexen Wiederherstellung eines Normalzustandes nach einem Zwischenfall können zu weiteren, teilweise enormen Kosten führen und sollten in der Business Impact Analysis (BIA) berücksichtigt werden (Racz, Weippl und Seufert 2010: 250). Neben der finanziellen Dimension der BIA müssen mit Hinsicht auf einen IT Ausfall auch die anderen Dimensionen betrachtet werden. Ein operationeller Schaden ist unbedingt zu berücksichtigen, da fast alle Prozesse auf die Verfügbarkeit der IT-Ressource angewiesen sind.[348] Darüber

[346] Zum Vergleich, die beiden nächsten Szenarien waren mit 14 Prozent ein Ausfall von Gebäuden und der des, Personals mit 7 Prozent (BCM Academy 2016: 28). Die Deutlichkeit der Einschätzung tritt hier besonders zu Tage, wenn man die geringe Nennung anderer Ressourcenausfälle berücksichtigt.

[347] Zu den Kosten eines Rechenzentrums sind neben den initialen Aufwänden zur Errichtung der Gebäude, Hardware und Anbindung auch die Betriebskosten und hohen Strom- und Wartungsausgaben zu zählen. Insgesamt ist bei größeren IT Rechenzentren wie im Fall von Großunternehmen mit einem hohen dreistelligen Millionenbetrag zu rechnen.

[348] Die Kosten einer Unterbrechung können je nach Organisationsnetzwerk und -Größe unterschiedlich ausfallen. "Downtime is costing (…) $1400 per minute on average (Oracle). Typical medium-sized business downtime costs

hinaus bedeutet ein Datenverlust auch einen erheblichen Schaden für die kollektive Gedächtnisfunktion des Unternehmens. Deren virtuelle Realisierung in Form von Datenbanken und informationsverarbeitenden Systemen droht durch den möglichen Verlust ihrer Verfügbarkeit die nachhaltige Beeinträchtigung der Entscheidungsprozesse und damit der Leistungsfähigkeit des Unternehmens selbst.

Ferner bestehen regulatorische Anforderungen, welche eine Bearbeitung von Daten und deren unmittelbare Bereitstellung innerhalb von engen Zeitfenstern durch Regulatoren oder Verträge festschreiben und zu hohen Geldstrafen, Rückforderungen oder sogar regulatorischen Maßnahmen wie der Suspension oder im Extremfall sogar dem Entzug der Lizenz führen können.[349] Ähnlich verhält sich die Relevanz der IT-Verfügbarkeit für die Reputation des Unternehmens, da Partner und Kunden einen wesentlichen Teil ihrer Kommunikation über die elektronischen Schnittstellen pflegen und eine Unterbrechung die Glaubwürdigkeit und das Vertrauen in das Unternehmen erheblich schädigen kann. (Gaycken und Karger 2011: 6). Diese Dimension wird zwar im größeren Umfang von Informationsschutz tangiert wie wir im Folgenden sehen werden, spielt jedoch als Reputationsschaden auch in der bisherigen BIA-Methodologie der Prozessunterbrechung eine gewichtige Rolle. Zusammengefasst wird deutlich, welche Bedeutung eine unterbrechungsfreie IT-Infrastruktur und der darauf operierenden Anwendungen für die Zukunft eines Unternehmens haben. Der Schutz der gängigen Betriebssysteme blickt dabei bereits auf eine mehr als 20-jährige Geschichte zurück (Müller 2011: 548), dessen originäres Ziel der Aufrechterhaltung der digitalen Arbeitsplattformen in der Aufgabenbeschreibung des IT Service Continuity Management (ITSCM) aufgegangen ist, welches im vierten Fallbeispiel aufgrund seiner Komplexität im Detail besprochen werden wird. Mit Blick auf die bereits zuvor präsenten, allerdings seit der Corona-Pandemie gestiegenen Cyberbedrohungen, sollen zunächst die Aspekte der Vertraulichkeit und Integrität im Rahmen des Informationsschutzes berücksichtigt werden.

6.1.1.3. Bedeutung von Informationsschutz

Für Organisationen ergibt sich ein besonderes Risiko durch den Datenverlust, also die Nicht-Verfügbarkeit von Informationen, aber auch durch deren potentielle Preisgabe oder Manipulation. Vor allem Unternehmen deren Geschäftskonzept auf dem Prinzip von Vertrauen

average $78,000 per hour; these sites typically lose more than $1 million annually due to downtime" (Cerullo und Cerullo 2004: 75). Die Kosten für modernere Systeme und größere Unternehmen dürften deutlich höher ausfallen.

[349] Vergleiche Gaycken und Karger für eine Übersicht relevanter Gesetze im deutschen und europäischen Rechtsraum, deren Anforderungen den Schutzstandard für kritische Systeme beschreiben, etwa im Aktiengesetz (§ 25aAbs.1 und § 91 Abs. 2 AktG) oder dem Kreditwesengesetz für Kreditinstitute (§ 25a Abs. 1 KWG), welche spezifische Schutzmaßnahmen für IT-Systeme definieren (Gaycken und Karger 2011: 3ff.).

beruht, so zum Beispiel Banken, Krankenversicherungen oder Anwaltskanzleien, aber auch alle Unternehmen die vertrauliche Daten ihrer Kunden verwalten (Asnar und Giorgini 2008: 217), haben ein gesondertes Interesse an der Vermeidung eines möglichen Reputationsschaden. Ferner legen rechtliche Normen die Mindestregeln im Umgang mit sensiblen Informationen fest, wie zuvor besprochen wurde (vgl. Dochow 2022). Dies umfasst nicht nur die reine Verfügbarkeit, sondern auch die Vertraulichkeit und Integrität. Vertraulichkeit bezeichnet hier die ausschließliche Einsicht der Informationen durch autorisierte Nutzer. Die Integrität wird in dieser Arbeit als Unveräußerlichkeit von Informationen verstanden, deren Form und Inhalt vor Eingriffen von nicht-autorisierten Nutzern geschützt werden kann

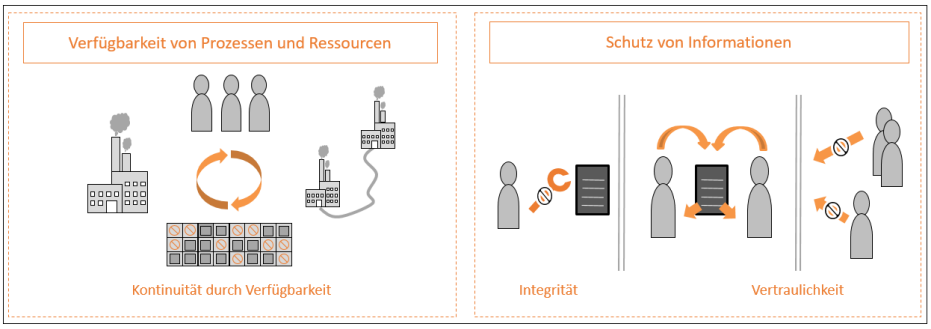

Abb. 6.1. Kernaufgaben von BCM, KM und Informationsschutz im Vergleich. Eigene Darstellung.

So zeigten einige der breiten Öffentlichkeit bekanntgewordene Fälle die Relevanz dieser Trias des Informationsschutzes, so zum Beispiel im Fall des Elektronikkonzerns Sony[350]. Das Unternehmen hatte den Verlust von vertraulichen Daten als Folge eines Hackerangriffs zu verantworten, welcher etwa 77 Millionen Kunden des Playstation-Onlineservice betraf (Bonner 2012: 258). Die Angreifer machten sich die mangelhaften Schutzstandards von Sony zu Nutzen und gelangten Zugang auf die Datenbanken dank einer weiteren Sicherheitslücke auf den angemieteten virtuellen Servern (PaaS) auf Amazons E2C Cloudservice (Chou 2013: 80). Dies zeigt eindrücklich die Verwundbarkeit von vernetzen Systemen, in welchen ein Unternehmen (Sony) die sensiblen Daten von Dritten (Nutzer des Onlineservice) auf Servern eines Dienstleisters (Amazon E2C) speicherten, ohne geeignete Schutzmaßnahmen der Daten durch Verschlüsselung oder eine Überprüfung der Sicherheitsvorkehrungen des Dienstleisters durchzuführen.

[350] Der Hacker-Angriff auf Sony führte zur Entwendung von etwa 77 Millionen Kundendaten über die Playstation-Spieleplattform, darunter etwa 45 Millionen Fälle möglichen Kreditkartenbetrugs (Fisher 2103: 220). Der Reputationsschaden durch den Angriff, welcher durch mangelhafte Sicherheitsstandards begünstigt wurde, verschlimmerte sich durch die verzögerte und unzureichende Kriseninformation. Sony entschied sich erst zwei Tage nach Bekanntwerden des Angriffs dazu die Kunden und Öffentlichkeit von dem Vorfall in Kenntnis zu setzen (Bonner 2012: 273). Hier zeigt sich exemplarisch die potenzierte Schadenswirkung aus unzureichenden Risikokontrolle und schlechtem Krisenmanagement. Dies unterstreicht die Bedeutung eines umfassenden Schutzkonzeptes.

An dieser Stelle sei im Kontext des Informationsschutzes auch auf den Begriff der Internetkriminalität hingewiesen. Darunter werden in dieser Arbeit Kriminalitätsformen zusammengefasst, deren Ziel im unautorisierten Zugang zu Informationen und Schutzwerten darstellt, um zumeist diese Werte zu monetisieren (vgl. Chigada und Madzinga 2021; Walter 2008). Diese Kriminalitätsform wurde bereits vor der Corona-Pandemie problematisiert, so wurden etwa im Jahr 2011 mehr als 60.000 Fälle mit Bezug zur Internetkriminalität in Deutschland dokumentiert, mit einem Anstieg um 16 Prozent zum Vorjahr (Vassilaki 2015: 7). Die kriminalitätsstatistische Analyse des Jahres 2017 zeigt ferner einen Anstieg auf 85.960 registrierte Fälle von Straftaten im Cyberraum, ein Anstieg zum Vergleichsjahr 2011 von mehr als 40 Prozent.[351] Die vermehrte Nutzung von virtuellen Strukturen während der Corona-Pandemie wurde in der Internetkriminalitätsstatistik für 2021 schließlich auch durch eine Steigerung auf 124.137 Fälle in Deutschland widergespiegelt (Statista 2022a).

Betrachtet man die Einschätzung von Unternehmen zur Bedrohungslage, finden sich zahlreiche Anknüpfungspunkte. Zum Jahr 2016 gaben beispielsweise 51 Prozent der in Deutschland tätigen Unternehmen an, bereits Opfer von Internetkriminalität geworden zu sein. Unter Unternehmern galten im gleichen Zeitraum Cyberattacken übereinstimmend als häufigste Gründe für Geschäftsunterbrechungen (BCM Academy 2016: 29) beziehungsweise als zweithäufigste Ursache für geschäftsgefährdende Krisen (AGCS 2018: 2). Im Zuge der Corona-Pandemie stieg diese Zahl schlagartig an, da bevorzugt Unternehmen aufgrund ihrer finanziellen Ressourcen im Fokus von Schadsoftware und Online-Erpressungen stehen (Lallie et. al. 2020: 3). Auch im jährlichen Risikobarometer stiegen Cyberbedrohungen nach Auswertung der Expertenmeinungen schließlich 2021 auf den höchsten Platz aller Risikokategorien (AGCS 2022). Die Schlussfolgerung aus diesen Punkten lässt sich daher im Zusammenwirken von BCM, KM und Informationsschutz zusammenfassen, durch welche sich die Anforderungen des digitalen Zeitalters und der Sicherheitsdispositive bewältigen lassen. Wir wollen im Folgenden der Frage nachgehen, inwiefern sich die Risikoexposition für Unternehmen im Informationszeitalter geändert hat und welche Rolle die beschleunigte Virtualisierung im Zuge der Corona-Pandemie dazu beigetragen hat?

[351] Die wichtigsten Tatbestände innerhalb dieses Überbegriffs bilden die Verbreitung von Schadsoftware, sogenannter Malware, welche in Deutschland mit 63 Prozent in einer Statistik von 2015 den größten Anteil hatte (Riekmann und Kraus 2015: 297). Ferner zählen der Waren- und Dienstleistungsbetrug, zumeist im Zusammenhang mit Waren die über das Internet auf digitalen Marktplätzen vertrieben werden mit einem Anteil von 16 Prozent sowie Identitätsdiebstahl mit 14 Prozent zu den nachfolgenden Gruppen. Ferner wird Phishing in seinen unterschiedlichen Ausprägungen mit 7 Prozent zur Internetkriminalität gezählt (Ebd.).

6.1.2. Risikoexposition im digitalen Raum

Wie wir im dritten Kapitel gesehen haben, müssen Arbeitsplätze aufgrund der Möglichkeiten der Digitalisierung nicht mehr an einem physikalischen Ort zentralisiert sein. Die Virtualisierung des Arbeitsumfelds erlaubt durch Modelle wie die Telearbeit („remote working“) den Mitarbeitern von jedem beliebigen Ort aus, die benötigten Anwendungen und Daten von einem (virtuellen) Server abzurufen. Ein weiterer Vorteil ist das die Mitarbeiter über Cloud-Lösungen dabei nicht auf die Performanz einer Großrechenmaschine verzichten zu müssen. Die bereitgestellten Programme sind lediglich virtuelle Replikationen der eigentlichen Bearbeitung der Daten auf einem virtuellen Servernetzwerk. Der Erfolg dieser Modelle führte dazu, dass physikalische Endgeräte aus den Bürogebäuden der meisten Unternehmen verschwanden und durch sogenannte „Thin Clients“ oder „Slim Clients“ ersetzt wurden. Diese Geräte sind auf die Leistung der Server angewiesen sind, um die benötigten Anwendungen abbilden zu können (Velte, Velte und Elsenpeter 2010: 7). Die finanziellen Vorteile[352] werden durch die „weichen“ Vorzüge der freien Gestaltung des Arbeitsumfeldes seitens der Mitarbeiter durch die Einwahl mittels eines privaten Endgeräts über den virtuellen Klienten oder den Miet- und Kosteneinsparungen durch eine Reduktion der physikalischen Arbeitsplätze erweitert.

Die Schließung der Arbeitsflächen im Zuge der Corona-Pandemie fügte dieser Aufzählung, wie wir es im ersten Kapitel bereits eingeführt hatten, einen weiteren Vorteil hinzu. Die Verlagerung der Arbeitsprozesse in ein virtuelles Umfeld, gestützt auf die technologischen Neuerung von virtuellen Arbeitsplätzen, Plattformrechenleistung und Kommunikations-anwendungen ermöglichte die Abwendung eines kritischen Kommunikationsabbruchs der meisten Organisationen während der Pandemie (Bellmann et. al. 2021: 713). Denn durch die technologischen Möglichkeiten wurde die Bewältigung dieser Krise überhaupt erst ermöglicht (Kirk und McDonald 2021: 3). Doch zeigte sich ebenso, dass durch die schlagartig gestiegene Virtualisierung und Anstieg des Datenverkehrs über das Internet (Engels 2020: 3) auch wesentliche Sicherheitsrisiken in Erscheinung traten (Chigada und Madzinga 2021: 4).

Die plötzliche Einwahl von Mitarbeitern aus dem Home Office ohne ausreichende Sicherheitsausstattung auf den verwendeten Endgeräte (Kirk und McDonald 2021: 3) oder fehlende Unterstützung durch IT-Support beziehungsweise improvisierte Sicherheitsprotokolle (Schulze 2021: 2) exponierte die IT vieler Unternehmen. Vor allem bedeutete die räumliche

[352] Unternehmen können teure Endgeräte wie Laptops oder Tower-Computer und deren Wartung durch billigere Thin-Clients ersetzen, zudem können technologische Weiterentwicklungen leichter auf der zentralen Serverlandschaft nachkonfiguriert werden, als die einzelnen Geräte an jedem Arbeitsplatz auszutauschen. Gleiches gilt für Sicherheitsupdates, Patches und insbesondere den Diebstahlschutz von Endgeräten, denn ein Thin Client ist als alleinstehendes Gerät wenig wert (Velte, Velte und Elsenpeter 2010: 7).

und IT-seitige Öffnung des vormals stärker geschlossenen Organisationsrahmens eine Gefährdung durch Cyberbedrohungen, welche sich im substantiellen Anstieg der Angriffe mit Schadsoftware und anderen Variationen zeigte (Lallie et. al. 2020: 3f.). Auch mit Blick auf die Prozess- und Kommunikationskontinuität zeigten sich erhebliche Probleme im neuen Arbeitsumfeld durch die Corona-Maßnahmen. Denn die Abhängigkeit von virtuellen Klienten bedeutete auch, dass wenn diese ausfallen, auch alle anderen Programme betroffen sind. Ebenso sind die Datenbanken nicht erreichbar, da das virtuelle Fenster nur eine Abbildung der Dateien auf dem Endgerät anzeigt, aber keine lokale Kopie anlegt. Dadurch würden die Nutzer am Telearbeitsplatz von den benötigten Ressourcen abgeschnitten. Durch die Lockdowns wäre auch der Zugang zu anderen Endgeräten oder alternativen Einwahlmöglichkeiten vom Unternehmensstandort nicht mehr möglich.

Die Negativseite der Digitalisierung zeigt sich auch durch die beschleunigte Vernetzung vormals isolierter Komponenten. Erst deren Zusammenführung ermöglichte einen potentiellen Dominoeffekt, der sich von einem lokalen Ausfall zu einer flächendeckenden Unterversorgung evolvieren kann (Müller 2011: 548).[353] Ein geeigneter Ansatz zur Risikosteuerung bedarf daher neben technischen Maßnahmen insbesondere auch einer tiefergehenden Sensibilisierung der involvierten Personen über die möglichen Auswirkungen der anstehenden Entscheidungen, beispielsweise über die Ausweitung der Vernetzung oder Inklusion von Systemen.[354] Die neue Bedrohungslage des Cyberzeitalters entwickelt sich schneller als das individuelle Risikobewusstsein in der Bevölkerung nachzuziehen scheint. Autoren wie Weber attestieren der modernen Gesellschaft daher „fehlende digitale Instinkte“ (Weber 2016: 28). Dadurch zeigt sich erneut auch das Zusammentreffen von unterschiedlichen Rationalitäten hinsichtlich der exogenen Gefahren. Um unter den Bedingungen der Unsicherheit Entscheidungen treffen zu können, müssen Unternehmen die ökonomischen und nicht-ökonomischen Herausforderungen berücksichtigen, aber auch zur gleichen Zeit die notwendigen Sicherheitsstandards implementieren (Walser und Riedl 2010: 258). Dazu bietet sich der Resilienzbegriff an, welcher im Folgenden für unsere Fragestellung konkretisiert werden soll.

[353] Die modernen Kommunikationssysteme der unterschiedlichen Spannungsnetze, deren Einführung in Deutschland vornehmlich zur Unterstützung der Energiewende eingeführt wurden, dient im Kern dem Ziel der Versorgungssicherheit indem der Energiebedarf zentral koordiniert und mit zur Verfügung stehenden Kapazitäten und Einheiten der Reserveenergieerzeugung kompensiert werden soll (Neumann, Moorfeld und Reulke 2016: 143). Doch eben diese Vernetzung erhöht die Gefahr eines systemischen Ausfalls, zudem erweitern sich die Angriffsflächen für Angreifer von außerhalb des Systems (Müller 2011: 548).

[354] Die Ausgangslage gibt Grund zur Beunruhigung, wenn das individuelle Sicherheitsbewusstsein von Nutzern im Umgang mit der digitalen Infrastruktur beobachtet wird. Dies reicht von der Unterkomplexität von Passwörtern bis zur bereitwilligen Preisgabe von sensiblen Daten im Internet (Weber 2016: 28).

6.1.3. Der Resilienzbegriff im Cyberzeitalter

Die Kontrolle von geschäftsgefährdenden Risiken im Informationszeitalter macht es für Unternehmen notwendig, die Definition einer umfassenden und vor allem konsequent umgesetzten Strategie zu artikulieren. Im Unternehmenskontext findet sich, nicht erst seit der Corona-Pandemie aber mit verändertem und nachdrücklicherem Gewicht, der Begriff der Resilienz zur Umschreibung der neuen Form der Risikokontrolle. Um diesen zentralen Begriff besser einzuordnen werden wir in diesem Abschnitt zwei Aspekte beleuchten. Zunächst die (1) Herkunft und allgemeine Begriffsbedeutung von Resilienz, um den Interpretationsrahmen zu klären. Darauf aufbauend soll der für (2) diese Arbeit relevante Begriff von Resilienz herausgearbeitet werden. Dies wird sich am Transformationsprozess des Begriffs in Unternehmen als Neuausrichtung der internen Sicherheitsproduktion ausrichten und die Verschiebung und Anpassung von Praktiken der Sicherheitsproduktion unter Einbeziehung der Erkenntnisse aus der ethnographischen Beobachtung ausleuchten.

Wie bereits im zweiten Kapitel zum Forschungsstand ausgeführt worden ist, umfasst der (1) Begriff Resilienz in der Literatur mehrere Bedeutungen und unterschiedliche Konnotationen. Der gemeinsame Nenner kann in der wörtlichen Bedeutung als Widerstandsfähigkeit eines Systems oder Objekts gegenüber Außeneinwirkungen gesehen werden. An dieser Stelle differenziert sich das Bild aber spätestens durch die spezifische Nutzung im den jeweiligen Disziplinen, worunter beispielsweise die Psychologie, Informatik oder Ökologie zu zählen sind (vgl. Pike, Dawley und Tomaney 2010; Voss und Dittmer 2016). In der ökonomischen Deutung des Begriffs ist die Widerstandsfähigkeit eines Unternehmens gegenüber unvorhergesehenen Verlusten gemeint, sowie diese im Zweifelsfall zu minimieren (Rose 2004: 307). Andere Verwendungen von Resilienz beziehen sich auf die räumliche Planung von Resilienz, beispielsweise im Katastrophenschutz von Regionen gegen Naturkatastrophen (Pike, Dawley und Tomaney 2010: 60) und wurde im US-amerikanischen Sprachgebrauch seit Hurrikane Katrina verstärkt in der Katastrophenforschung verwendet (Tierney und Bruneau 2007: 14).

Resilienz findet sich auch in der Sicherheitsforschung und kann zum Beispiel als politische Technik verstanden werden, um Sicherheit zu gewährleisten (Kaufmann 2013: 55; Chandler 2014: 52). Auch als Sprachakt zur Rechtfertigung von politischen Maßnahmen kann der Begriff gefunden werden. So lautet eine Interpretation, dass „(…) resilience is a transcending form of securitization, as it assumes a need for immediate action [or] adaption“ (Petersen 2017: 129). Ferner unterscheidet die sprachliche Nutzung von Resilienz ebenfalls die sicherheitspolitische Einordnung des Begriffs, entweder als Zustand oder als Prozess der Implementierung dieses

Zielbildes. Resilienz kann als Reaktion auf Katastrophen, wie oben angedeutet, verstanden werden, durch welche exogene Gefahren minimiert werden (Kaufmann und Blum 2011: 235) oder aber als Zustandsbeschreibung verwendet werden, um die schnelle Wiederherstellung der Funktionsfähigkeit nach einem – als unvermeidlich wahrgenommenen – Schadensereignisses zu ermöglichen (Blum et. al. 2016: 157).

Im zweiten Aspekt finden wir bereits eine geeignete Formulierung für unsere Fragestellung. Resilienz kann als Antwort auf die Ereignisse mit hoher Schadenswirkung und niedriger Frequenz wie Terroranschläge vom 11. September 2001 oder dem Reaktorunglück von Fukushima im März 2011 verstanden werden (Braes und Brooks 2010: 16). Doch mit Blick auf die zunehmende Vernetzung und Komplexität von Infrastrukturkomponenten macht eine Unterscheidung zwischen „einfacher Resilienz" zur schnellen Reaktion auf Schadensereignisse einerseits und der „reflexiblen Resilienz" andererseits Sinn. Letzteres bezeichnet eher den langfristigen und holistischen Ansatz zur Eindämmung oder Bewältigung von Großschadensereignissen (Blum et. al. 2016: 156). Diese Unterscheidung ermöglicht daher zwei Konzepte oder Ideen von Resilienz, einmal als Methode und Anwendungspraktik in Reaktion auf spezifische, eventuell planbare Ereignisse. Der zweite Aspekt thematisiert Resilienz als reflexiven Prozess in dem sich eine Gesellschaft, auf zukünftige, eventuell noch unbekannte Gefahren vorbereitet (Kaufmann 2013: 55). Dadurch wird Resilienz als Richtung oder Vorsorge interpretiert, durch welche die Bevölkerung unter Berücksichtigung der gegenwärtigen Unsicherheit geschützt werden soll (Fekete, Grinda und Norf 2016: 220), indem flexible Strukturen und Prozeduren zur Bewältigung eines noch zu entdeckenden, aber anzunehmenden Ereignisses implementiert werden.[355] Dies kann auch als eine „Abkehr von der tradierten Sicherheits- und Ordnungsfixierung" verstanden werden, welche Gesellschaften „(…) einen veränderten Umgang mit Unsicherheit erlaubt" (Blum et. al. 2016: 155).

Wie wir in der Diskussion über die kritische Infrastruktur gesehen haben, dient deren Schutz der Sicherstellung der Versorgungssicherheit mit vitalen Gütern und Leistungen, welche in modernen Gesellschaften durch eine Vielzahl an Organisationen erbracht werden. Daher bedeutet dieser Schutz der kritischen Infrastruktur auch einen Beitrag zur Existenzsicherung der Bevölkerung (Brzoska, Neuneck und Scheffran 2021: 6f.). Die Einführung von neuen

[355] Hier wird auf den sich wandelnden Risiko- und Sicherheitsbegriff referenziert. Die in der Wahrnehmung verhältnismäßig stabilen Bedrohungsfaktoren im Kalten Krieg basierten auf der Logik der militärischen Ökonomie und dem objektiven Vergleich von Kräfteverhältnissen (vgl. (Daase und Kessler 2007: 422). Nicht erst die Risikogesellschaft nach Beck erwähnt die veränderten Parameter durch beispielsweise technologische Risiken, welche die hergebrachten Lösungsmuster als nicht mehr ausreichend erscheinen lassen (vgl. Beck 1991).

Technologien zur Sicherheitsproduktion, von denen wir einige bereits im dritten Kapitel kennengelernt haben, hat zum Zweck, den Schutz der Gesellschaft über ihre kritischen Infrastruktur zu gewährleisten (Davidshofer, Jeandesboz und Ragazzi 2016: 212). Resilienz kann in diesem Kontext als Strategie verstanden werden, den Schutzdispositiven der Gesellschaft Rechnung zu tragen und dabei die Unsicherheit über technologische Risiken und die Komplexität der interdependenten Komponenten zur Bereitstellung von Gütern und Leistungen berücksichtigen.

Dies führt uns zum (2) relevanten Verständnis von Resilienz für unsere Arbeit. Wie wir in den vorausgehenden Kapiteln sehen konnten, fokussierte sich die Auffassung im Sicherheitsdiskurs der Internationalen Beziehungen auf die Sicherheitsproduktion von Staaten und Gesellschaften. Im klassischen Verständnis, konnten Unternehmen daran durchaus teilnehmen, aber vorrangig als Bereitsteller von Sicherheitsleistungen in Vertretung oder im Auftrag von Autoritäten. Die Sicherheitsproduktion in Unternehmen wurde in diesem Zusammenhang kaum wahrgenommen, jedoch verwenden Unternehmen als kritische Betreiber von Infrastrukturen zunehmend den Begriff Resilienz, um eine Weiterentwicklung der unternehmensinternen Risikokontrolle zur Sicherstellung ihrer Prozess- und Kommunikationskontinuität zu beschreiben. Dieser Zusammenhang soll im Folgenden vertieft werden, um den Resilienzbegriff in Unternehmen und auch in Bezug auf unsere Fragestellung zu beleuchten und die Erkenntnisse aus der ethnographischen Untersuchung einfließen lassen.

Resilienz bedeutet für Unternehmen eine Erweiterung ihres Risikomanagements, welches ihnen hilft mit exogenen Gefahren umzugehen, für deren Bewältigung die bisherige ökonomische Rationalität keine geeigneten Vorgehensweisen zur Verfügung stellt. Daher ist Resilienz eine Strategie von Unternehmen, um den Umgang mit Unsicherheit in Luhmanns Sinn bestmöglich zu organisieren, aber auch der Verantwortung für die Gesellschaft im Sinne ihres Beitrags zum Sicherheitsdispositiv über die Produktion von Sicherheit in ihrer eigenen Organisation gerecht zu werden. Resilienz bietet das konzeptionelle Rahmenwerk für Unternehmen, um der rechtlichen, gesellschaftlichen und intrinsischen Motivation zur Sicherstellung der eigenen Handlungsfähigkeit durch die Kontinuität von Prozessen gerecht zu werden (Kaufmann und Blum 2011: 236).

Die Komplexität in der kritischen Infrastruktur durch interdependente Komponenten entspricht durch die Digitalisierung auch der systemischen Verknüpfung und Abhängigkeit von IT-Elementen. Dadurch wird nach den Schlussfolgerungen unserer Beobachtung und Analyse ein ganzheitliches, auf Prozesse statt Objekte fokussiertes Konzept der Risikokontrolle notwendig.

Folglich wird Resilienz in dieser Arbeit als Konzeption dieser Aufgabe verstanden und in Unternehmen als Reaktion auf die exogenen Sicherheitsrisiken in Folge der Digitalisierung beobachtet.[356] Dennoch ist es wahrscheinlich nicht möglich einen einzigen, für alle Unternehmen treffenden Begriff von Resilienz vom Anfang bis Ende des Prozesses unternehmensinterner Sicherheitsproduktion zu finden. Allerdings können in einigen Fachbereichen und Funktionen entsprechende Metabeschreibungen von Resilienz angetroffen werden. Dazu sollen hier drei Beispiele aus dem (a) Informationsschutz, (b) Krisenmanagement und (c) Business Continuity Management angeführt werden.

Im (a) Informationsschutz findet sich Resilienz beispielsweise durch die Datenschutzgrundverordnung verortet, in der eine „Resilienz der Verarbeitung" für datenverarbeitende Systeme angeführt wird, „(…) die einerseits durch eine Belastbarkeit der Systeme und andererseits durch die rasche Wiederherstellbarkeit bei Vorfällen gewährleistet werden soll" (Hessel und Rebman 2021: 267). Die durch die Digitalisierung angestiegene Vernetzung und Durchdringung von datenbasierten Entscheidungen in Systemen reflektieren ebenfalls den Gedanken von Resilienz (Kaufmann und Blum 2011: 235). Denn die Vielfalt an Sensoren zur Steuerung von Maschinen wie selbstfahrenden Autos oder Unterstützungssystemen in Flugzeugen hängen von der fehlerfreien und widerstandsfähigen Konzeption der Hardware ab, um Manipulation[357] oder technisches Versagen durch Redundanzen oder Kontrollsysteme zu verhindern (Krotofil und Cárdenas 2013: 166). Das systemische Gesamtbild gewinnt daher an Bedeutung, indem die Entwicklung von Informationen in einem Lebenszyklus reflektiert und dadurch eine prozessuale Sicht ermöglicht wird.[358]

Der (b) Resilienzbegriff im Krisenmanagement konnotiert die Frage der (Un-)Vorhersagbarkeit von Risiken unter den bereits eingeleiteten Aspekten der Unsicherheit. "In the context of resilience, risk mitigation is not a matter of making the unknown known; rather, the premise is

[356] Diese Erkenntnis leitete sich aus den Gesprächen mit Experten und Verantwortlichen des Unternehmens im Zuge der Ethnographischen Untersuchung ab, in welchen die Praktiker eine Verschiebung des Risikodiskurses hin zu einer Selbstbetrachtung der Organisation und Umsetzung der Sicherheitsproduktion durch Resilienz in Reaktion auf die gestiegenen Komplexität von Systemkomponenten und dies insbesondere seit der Corona-Pandemie attestierten (Hintergrundgespräch 03.03.2021; Hintergrundgespräch 13.12.2021).

[357] Die Zunahme an veröffentlichten Akten von Cyberkriminalität, aber auch von Verdachtsfällen staatlicher Intervention mithilfe von Cyberwaffen ist auch in der Literatur zu beobachten (vgl. Cavelty 2013: 108). Während vor zehn Jahr noch kaum Fälle von Cyberterrorismus und direkter Verbindungen von staatlichen Diensten mit Cyberzwischenfällen vermerkt wurden (Choo, Smith und McCusker 2007: 2), zeichnen aktuelle Fälle wie Stuxnet, die Attacke auf die Telekomrouter oder anderer Formen der Einflussnahme über das Internet (US-Präsidentschaftswahlen 2016) ein anderes Bild.

[358] Dies zeigte sich auch in der Betrachtung von möglichen Zwischenfällen mit systemweiter Wirkung, wie in den Gesprächen mit Experten diskutiert wurde (vgl. Hintergrundgespräch 26.07.2022).

that we will never know (…)" (Petersen 2017: 130). Die Bedeutung von Resilienz für das Krisenmanagement liegt daher in der Abkehr vom Szenario-spezifischen Krisenstabsplan, hin zu einer durch die Corona-Pandemie aufgezeigte Notwendigkeit, auch die Abhängigkeiten oder Gleichzeitigkeit von Krisen zu durchdenken (Brzoska, Neuneck und Scheffran 2021: 5). Dies zeigte sich beispielsweise nicht nur mit der Verbindung von Erdbeben, Tsunami und Reaktorsicherheit in Fukushima oder den Auswirkungen der Corona-Pandemie auf die Arbeitsplatzzugänglichkeit, sondern etwa auch in den während der letzten Jahrzehnte gering betrachteten Risiken wie kriegerischer Auseinandersetzungen in Europa. Im Krisenmanagement beschreibt der Begriff daher den Prozess der Optimierung und Vorbereitung auf ein, unter Umständen noch unbekanntes, Ereignis. Die Fähigkeit der Organisation auf das Unvorhergesehene zu reagieren, wird daher als Schlussfolgerung aus der ethnographischen Untersuchung als Selbstreferenz verstanden, welche auf die Gesamtheit der Prozesse und Kommunikationen zur Existenzsicherung referenziert und durch Resilienz umgesetzt wird.[359]

Vergleichbar verhält es sich im Fall des Verständnisses von Resilienz für das (c) Business Continuity Management. Während Unternehmen die Investitionen für Widerherstellungsstrategien im Sinne einer ökonomischen Rationalität als vermeidbare Kosten ansahen[360], wandelte sich das Verständnis hin zu einer Umdeutung der Methodik als *business enablement function*, durch welche die Kontinuität von Prozessen und Kommunikation im Unternehmen sichergestellt wird (Christensen und Petersen 2017: 1443). Resilienz bedarf daher nicht mehr allein der Translationsleistungen des Risikomanagements mit Matrizes und probabilistischen Modellen (Blum et. al. 2016: 156), als vielmehr der konstanten Vorbereitung der Organisation auf ein zukünftiges Ereignis. Resilienz sieht man hier in doppelter Perspektive, einerseits als Prozess zur Sicherstellung der Kontinuität von Prozessen (Fekete, Grinda und Norf 2016: 220), aber anderseits auch das Zielbild in Gestalt der resilienten Organisation.

Abschließend fällt somit der Blick auf die Veränderungen der Risikolandschaft und der Einordnung von Resilienz in den Funktionsaufbau von Unternehmen. Die Digitalisierung und insbesondere die beschleunigte Ausweitung der Virtualisierung in Folge der Corona-Pandemie

[359] Vergleiche hier die Auswirkungen von komplexen Lagen, in denen beispielsweise wie in der Corona-Pandemie der Ausfall von Personal vom zuvor nicht beachteten Konsequenz der Nicht-Verfügbarkeit von Arbeitsflächen als essentielle Implikation für die Kontinuitätsplanung abgelöst wurde (Workshops September bis Dezember 2020

[360] Vor allem unterliegt die Entscheidung zur Einführung einer Sicherheitsmaßnahme einer ökonomischen Logik der Kosten-Nutzen Rechnung, welche als Hindernis auftreten kann: „Es wird entsprechend nur so lange in IT-Sicherheitsprodukte investiert, wie jeder zusätzlich investierte Euro den erwarteten Schaden um mehr als einen Euro reduziert. Man spricht von Grenzkosten und Grenzschaden" (Weber 2016: 30). Eine vergleichbare Aussage konnte auch aus der ethnographischen Untersuchung abgeleitet werden Hintergrundgespräch (16.06.2014).

zeigten die Grenzen des traditionellen, objekt-bezogenen Risikobegriffs. Die Komplexität und Vernetzung erfordert einen systemischen Begriff von Risiko, welcher die Schutzkomponenten ganzheitlich integriert und die Kontinuität von Anschlussoperationen im Unternehmen durch eine Verkettung und Verknüpfung von Aktivitäten betrachtet, anstatt nur die Einzelaspekte von Komponenten zu berücksichtigen. Für diese Aufgabe wird Resilienz im Unternehmenskontext verwendet und in unserer ethnographischen Beobachtung als Ergebnis einer längeren Begriffsgenese von etwa 10 Jahren identifiziert.[361] Durch den Begriff verändern sich allerdings auch Praktiken und Zielbeschreibungen, deren Größenordnung, finanzielle Belastungen und organisatorische Implikationen seit der Corona-Pandemie im Licht der Beobachtung noch deutlicher in den Mittelpunkt des unternehmensinternen Risikodiskurses traten. Als Folge wird Resilienz hier in der Schnittstelle zwischen den Funktionen der Betriebsorganisation, dem Risikomanagement und der IT-Betriebsorganisation sowie Informationsschutz verortet.

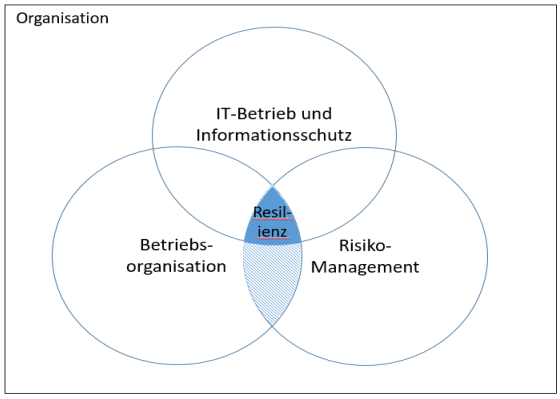

Abb. 6.2. Der Resilienzbegriff als Schnittmenge zwischen Resilienz, Risikomanagement und Informationsschutz. Eigene Darstellung.

Zusammenfassend kann damit für die weitere Bearbeitung der Fragestellung festgehalten werden, dass die Veränderung des Risikobegriffes wie eingangs beschrieben als Übergang von objekt-orientierten Problemstellungen auf eine prozess-geleitete Betrachtung verstanden wird. Durch die erweiterten Risiken der (Nicht-)Verfügbarkeit von Systemen und Informationen, sowie die Bedeutung von Netzwerken und die Exposition gegenüber exogenen Bedrohungen, entwickelte sich ein Bewusstsein in Unternehmen, den Schutz ihrer kritischen Prozesse unter dem Aspekt der Resilienz neu zu gestalten. Resilienz umfasst dabei die systemische Selbstreferenz der Organisation in Verbindung mit Maßnahmen und Risikokontrollen, um Unternehmen einen Umgang mit der sie umgebenden Unsicherheit anzubieten, welche wir im

[361] Resilienz entwickelte sich seit der ersten Nennung im Unternehmen 2012 im Zuge der regionalen Wiederherstellbarkeit von Prozessen nach dem Reaktorunglück von Fukushima im Vorjahr und verknüpfte sich im Laufe der zunehmenden Digitalisierung und insbesondere in Folge der Corona-Pandemie zu einer unternehmensweiten Strategie zum Umgang mit Unsicherheit. (vgl. Hintergrundgespräch 15.11.2021).

Folgenden genauer beleuchten werden. So schließt sich die Frage an, wie sich die Bedrohungslage durch die Digitalisierung änderte und insbesondere welche Rolle Informationen und deren Verlust oder Kompromittierung für die Sicherheitsproduktion spielen? Auf der Grundlage dieser generellen Einordnung werden dann im darauffolgenden Abschnitt die konkreten Fallbeispiele detailliert beschreiben und die Risikoexposition für Unternehmen im Informationszeitalter herausarbeiten.

6.2. Informationen und Daten als Schutzziel

Die bisherige Argumentation in diesem Kapitel zeichnete die Veränderungen des Risikobegriffs im Informationszeitalter und die Entwicklung von Resilienz als Konzept zur Beschreibung der Sicherheitsproduktion in Unternehmen nach. Im Folgenden werden wir nun auf die Risikoexposition von Unternehmen durch die Digitalisierung eingehen und dabei immer wieder auf die Vorarbeit des dritten und vierten Kapitels referenzieren. Der Schwerpunkt dieses Abschnittes ist die Implikationen und Systematik der Verfügbarkeit von Informationen und Daten[362] für die Kontinuität von Anschlussoperationen zu beleuchten. Dies geschieht insbesondere mit Blick auf den (1) Wert von Daten und des einhergehenden Risikos eines Datenverlusts. Dies ist aufgrund des ökonomischen Wertes von Informationen für beide Seiten relevant, einerseits für das die Information (legal) erhebende Unternehmen und anderseits für unautorisierte Dritte, welche versuchen darauf zu zugreifen.[363] Zweitens wird der Abschnitt über das (2) Risiko des Zugriffs auf Daten die unterschiedlichen Kategorien verdeutlichen, durch welche sich Schäden für Unternehmen ereignen können.

6.2.1. Der sicherheitsrelevante Wert von Daten

Das dritte Kapitel zeigte bereits die inhärente Logik der Plattformökonomie im Informationszeitalters, in der die Plattform mit den meisten Nutzern und den meisten (qualitativen) Daten als wertvollstes Investitionsobjekt gehandelt wird. Jedoch gilt auch, dass je mehr Daten gesammelt werden, desto größer ist auch das potentielle Risiko eines Datenverlusts. Einerseits ist die zu erwartende Beute für den unautorisierten Dritten attraktiver, andererseits erhöht die Masse an prozessierten Informationen auch das Risiko, dass irgendwann Daten aufgrund eines internen technischen oder menschlichen Fehlers verloren gehen. Der Schaden kann sich in diesem Beispiel in zweierlei Form äußern. Zum einen, wenn die Daten

[362] Zur Wiederholung und wie im dritten Kapitel angesprochen unterscheiden sich Informationen und Daten. Erstere bezeichnen das Wissen, Daten hingegen enthalten Informationen und definieren darüber ihren Wert.
[363] Gemeint sind mit diesem Begriff jede Form des Zugriffs auf die Daten einer Organisation oder Person, welche nicht autorisiert wurde. Im Allgemeinen bezieht sich dies hier auf kriminelle Akteure.

nicht mehr zur Verfügung stehen und dies zu einer Prozessunterbrechung[364] oder einer arbeitsaufwendigen Wiederherstellung zur Datensicherung führt (Cerullo, und Cerullo 2004: 75). Zum anderen, wenn diese Daten der Öffentlichkeit zugänglich gemacht werden („data leakage“) oder an interessierte Dritte weiterverkauft[365] werden (Vassilaki 2015: 28).

Daher stellt sich die Frage, welche Bedeutung der unautorisierte Zugriff auf Daten hat? Die jährlichen Schäden durch Datenverlust im allgemeinen Sinn wurden 2015 im globalen Kontext auf einen Wert zwischen 375 und 573 Milliarden US-Dollar geschätzt (Khan und Sepúlveda 2015: 7). Die Gesamtschäden durch Internetkriminalität stiegen von 3 Billionen US-Dollar im gleichen Jahr auf geschätzte 6 Billionen US-Dollar für das Jahr 2021 (Chigada und Madzinga 2021: 8) Die Gegenüberstellung zu aktuellen Zahlen mangelt zwar einer exakten Vergleichbarkeit aufgrund der exponentiellen Steigerung von möglichen Angriffsflächen in Folge des Corona-bedingten Digitalisierungsschubes einerseits und der sie begleitenden unzureichenden Sicherheitsmaßnahmen andererseits (Schulze 2021: 5). Allerdings zeigt es den möglichen monetären Gewinn, welchen Kriminelle aus den Datenbeständen und virtuellen Arbeitsprozessen von Unternehmen erzielen können.

So gehört beispielsweise ein vollständiger medizinischer Datensatz, das bedeutet die digitale Krankengeschichte eines Patienten mit Diagnosebefunden und Therapieverlauf, zu den wertvollsten, massenhaft verfügbaren Datensätzen (Sittig und Singh 2016: 625). Die hohen Stückpreise[366] für diese zumeist auf illegalen Wege organisierten Daten begründen sich dadurch, dass Daten nicht ohne die Einwilligung des Nutzers weitergegen werden können (Gaycken und Karger 2011: 7) und vor allem die Vollständigkeit eines Datensatzes eine effektive Prädiktion verspricht.[367] Informationen können allerdings auch für betrügerische Handlungen entwendet werden, etwa im Fall des Identitätsdiebstahls und des Kreditkartenbetrugs, zwei Varianten bei denen die entwendeten Informationen zur Bestellung von Waren oder dem unautorisierten Geldtransfer dienen.[368] Die Informationen haben in diesen

[364] Die Nichtverfügbarkeit kann sich in unterschiedlichen Formen ausdrücken: „Verfügbarkeit meint den Schutz vor Informationsverlust, Informationsentzug, Informationsblockade und Informationszerstörung“ (Gaycken und Karger 2011: 6). Wir werden dies weiter unten unter IT Service Continuity Management (ITSCM) adressieren.
[365] Im Fall zuvor beschriebenen Datenverlusts von British Airways konnten die Angreifer für etwa zwei Wochen unbemerkt Daten kopieren und aus den Systemen des Unternehmens entwenden (vgl. Telegraph 2018).
[366] In Gesprächen mit IT-Sicherheitsverantwortlichen wurden Schätzungen von 2.000 – 3.000 US-Dollar für einen medizinischen Datensatz genannt. Im Fall von Prominenten kann der Wert deutlich höher ausfallen, da die betroffenen Personen mit der Androhung einer Veröffentlichung vertraulicher Details aus der Patientenakte erpresst werden können (Sittig und Singh 2016: 625).
[367] Die Vernetzung von Komponenten durch ein Informationssystem im medizinischen Bereich kann unterschiedliche Aspekte wie Patientenakte, Behandlungshistorie, Befunde, Wohnort, Gewohnheiten und Herkunft berücksichtigen (Dwertmann und Schürholz 2016: 170).
[368] Kreditkarteninformationen sind vergleichsweise leicht zu beschaffen. Selbst ohne elektronische Hilfsmittel, bieten Unaufmerksamkeit und Routinegewohnheiten von Nutzern häufig ausreichend Angriffsfläche, wie

Fällen somit keinen Eigenwert, sondern dienen lediglich als Werkzeuge zum Betrug (Borges et. al. 2011: 23). Im Folgenden wollen wir nun das Risiko hinsichtlich der Verfügbarkeit, Vertraulichkeit und Integrität von Daten in Kategorien ordnen und vorstellen.

6.2.2. Das Risiko der Daten

Aus Sicht von Unternehmen lässt sich das Risiko der Verfügbarkeit, Vertraulichkeit oder Integrität von Daten in eine Vielzahl von Szenarien differenzieren, in denen Informationen aus unterschiedlichen Gründen den geschützten und autorisierten Bereich des Unternehmens ungewollt verlassen, verschwinden oder durch Manipulation Schaden verursachen können. Daher kann man zwei Differenzierungen vornehmen, erstens anhand der Art des Schadens und zweitens über die Ursache des Datenverlusts. Die *Schadensart* kann durch den (a) unmittelbaren Wissensverlust oder durch den (b) Reputationsschaden in Folge der veröffentlichten Informationen beziehungsweise des Bekanntwerdens ihrer Entwendung entstehen. Hingegen kann die Unterscheidung der *Ursache* des Datenverlusts auf Grundlage der Beschaffenheit des Datenverlusts vorgenommen werden. Dazu zählen die unbeabsichtigte Publikation von Daten aufgrund eines (1) technischen Fehlers, beziehungsweise intendierte (2) externe Angriffe, (3) interne Angriffe und den Verlust des Zugriffs auf die Daten aufgrund einer fehlerhaften (4) Prozessausgliederung. Mithilfe dieser Struktur soll das breite Themenfeld des Datenverlusts systematisiert werden.

Beginnend mit dem (a) unmittelbaren Wissensverlust zeigt sich, dass internes Wissen nach Außen gelangt und der negative Effekt vorrangig durch den Verlust der Exklusivität des Wissenszugangs begründet ist (Vassilaki 2015: 23). Das kann zur Folge haben, dass interne Geheimnisse, Strategien, Patente oder andere vertrauliche Unterlagen nicht mehr dem Zugangsmonopol des Unternehmens unterstehen.[369] Diese Schadensart gereicht auch ohne eine Veröffentlichung der Daten zum Nachteil für das Unternehmen, da die entwendeten Daten den Wettbewerbern Vorteile verschaffen können (Khan und Sepúlveda 2015: 7). Der (b) Reputationsschaden ist hingegen eng mit der öffentlichen Rezeption der verloren gegangenen

beispielsweise im Fall des „Dumpster-Diving“. In diesem Fall werden Papierkörbe beispielsweise in Bankfilialen nach (teilweise) ausgefüllten Überweisungsscheinen durchsucht, welche sensible Informationen wie Namen oder Kontonummern beinhalten (Borges et. al. 2011: 26).

[369] Der Begriff der Industriespionage beschreibt den unerlaubten Zugriff auf Geschäftsgeheimnisse oder Technologien durch Konkurrenten, um dadurch Entwicklungskosten und -Zeit zu sparen, dessen Abfluss zum Schaden des ersten Unternehmers durch den Verlust der Wissensexklusivität beiträgt (Vassilaki 2015: 23). Schätzungen aus dem Vereinigten Königreich bezifferten den Verlust durch Industriespionage auf einen Jahresdurchschnitt von umgerechnet 8,5 Milliarden Euro (Khan und Sepúlveda 2015: 7). Eine ähnliche Schätzung für die deutsche Wirtschaft berechnete die jährlichen Schäden durch Industriespionage auf 4.2 Milliarden Euro (Vassilaki 2015: 23).

oder entwendeten Informationen verbunden.[370] Die entscheidende Komponente ist hier der Vertrauensverlust in die Fähigkeiten des Unternehmens mit den Daten in geeigneter Weise umzugehen (Riekmann und Kraus 2015: 296).

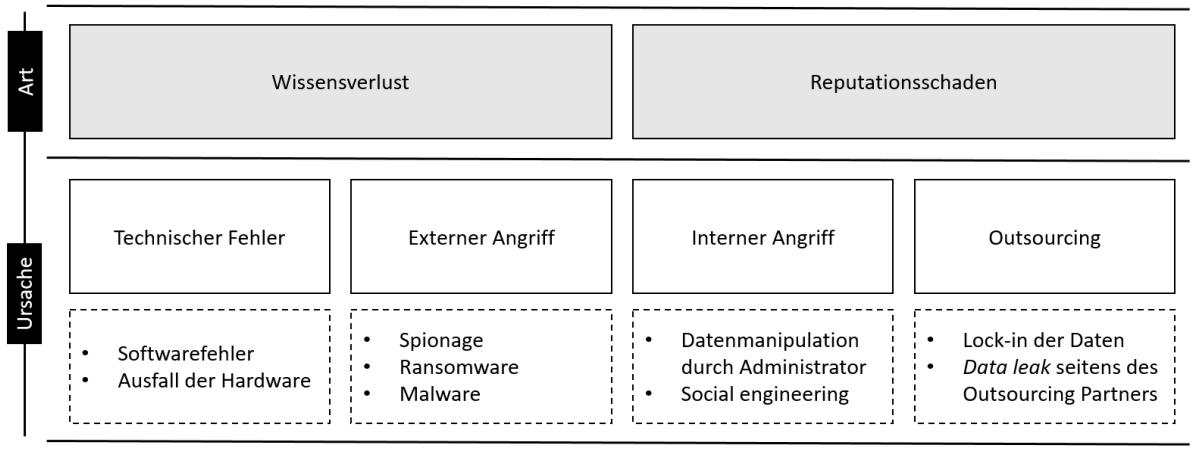

Abb. 6.3. Art und Ursachen des Risikos der Daten. Eigene Darstellung.

Betrachtet man die Ursachen für einen Datenverlust ist die Möglichkeit des (1) technischen Fehlers zu nennen. Komplexe Netzwerke und Systeme wie Unternehmensdatenbanken oder virtuelle Serverfamilien beziehungsweise Clouds operieren auf der Basis von interpendenten Komponenten, über welche Informationsbits versendet, empfangen und verarbeitet werden. Diese komplexe und quantitativ umfangreiche Umgebung ist fehleranfällig für unbeabsichtigte Auswirkungen, die durch nicht vollständig implementierte Serverupdates, inkompatible Sicherheitseinstellungen oder Anwenderfehler entstehen (Cerullo und Cerullo 2004: 72). Etwa 40 Prozent der Unternehmen schätzen die unbeabsichtigte Weitergabe von Informationen nach Außen durch eigene Mitarbeiter als größtes Sicherheitsbedenken ein (Greitzer 2014: 236). Der beständige Druck zur Weiterentwicklung der Netzwerke, aber auch eine unübersehbare Anzahl an angedockten Endanwendungen erhöht den Grad der Komplexität und folglich auch die Möglichkeit für unbeabsichtigte Fehler. In dieser Konstellation eröffnen sich viele Möglichkeiten für ungewollte Kettenreaktionen, Fehlerkulminationen oder Sicherheitslücken durch die Daten verloren gehen können.[371]

[370] Der Hackerangriff auf das amerikanische Versicherungsunternehmen Anthem im Jahr 2015 war der bis dahin größte Vorfall im Gesundheitsbereich, in dessen Folge sich Außenstehende Zugang zu den sensiblen Daten von etwa 80 Millionen Kunden verschafften. Der Angriff kostete den Konzern vermutlich bis zu 100 Millionen US-Dollar und unterminierte vor allem das Vertrauen der Kunden in das Unternehmen (vgl. Zeit Online 2015).

[371] In großen Unternehmen fehlt aufgrund des rasanten Ausbaus der Systeme, personeller Fluktuation oder der Unübersichtlichkeit und Weitläufigkeit der technologischen Komponenten nicht selten eine solide Dokumentation der vorgenommenen Veränderungen. In einer solchen Dokumentation sollten die Administratoren, also Nutzer mit besonderen Schreibrechten, die getätigten Schritte und Anpassungen niederschreiben und mit anderen Akteuren innerhalb des Unternehmens teilen. Häufig jedoch unterbleibt auch dieser Schritt, so dass in Folge kein umfassendes Wissen über den Wissensstand eines Unternehmens und insbesondere der Funktionsweise des

Daran schließt sich die zweite Gruppe der Schadensursachen in Gestalt eines (2) Angriffs von außen an. Fehlende Sicherheitsstandards, nicht aktualisierte Firewalls oder Sicherheitslücken bieten Hackern ausreichend Möglichkeiten in Systeme einzudringen und Daten zu entwenden (Mosin, Prajapati und Vohara 2010: 22). Zwei Beispiele werden wir in den nachfolgenden Fallbeispielen in Form von Malware und Ransomware im Detail betrachten. Selbstlernende Algorithmen können Systeme auf mögliche Sicherheitslücken überprüfen und sich Stück für Stück vortasten und eigenständig evaluieren, an welcher Stelle ein Angriff Erfolg versprechen könnte.[372] Die Häufigkeit dieser Angriffe steigt zunehmend an, doch hat dies aus Sicht mancher Autoren auch einen Gewöhnungseffekt, wenn Medien und Öffentlichkeit eine Routine im Umgang mit diesen Vorfällen entwickeln.[373] Doch eben diese Akzeptanz des Risikos – man könnte dann auch von Ignoranz sprechen – korreliert auch mit der verbesserungsbedürftigen Bereitschaft von Unternehmen in Schutzvorkehrungen zu investieren (Weber 2016: 31). Ein anderes Beispiel ist, wenn Informationen unbemerkt und mit implizierter Zustimmung des verwaltenden Unternehmens abfließen, etwa wenn der Dienstleister oder Partner bestimmte Parameterdaten erhebt.[374] Die im Rahmen dieser durch die Allgemeinen Geschäftsbedingungen gedeckten Praxis gehört zu den leisen Formen des Datenverlusts, in dem eine niedrige, aber beständige Größe an Informationen an den Betreiber der Betriebssoftware oder anderer digitaler Anwendungen beziehungsweise Hardware übergeht, ohne dass der Kunde davon unmittelbar Kenntnis nehmen würde (Armbrust et. al. 2010: 55).

Die dritte Ursachenkategorie liegt in der (3) Datenmanipulation durch Innentäter, das bedeutet Mitglieder der Organisation. Die Mitarbeiter eines Unternehmens könnten versucht sein, eigene betrügerische oder im Allgemeinen kriminelle Handlungen durch Manipulation der Datenbanken zu verbergen oder sich durch den Verkauf von Informationen zu bereichern

---

virtuellen Gedächtnisses existiert. Dies ist eine wesentliche Anforderung an die IT-Kompetenz der Mitarbeiter (vgl. Hanft, Müskens und Muckel 2004: 21).

[372] Denn auch ein Datendiebstahl muss gut vorbereitet sein, so darf der Eindringling nicht zu früh entdeckt werden, um einem frühzeitigen Abschalten des Systems zuvorzukommen. Zudem ist der Weg zum Ziel noch nicht mit dem Eintritt in die Datenbank frei und die Sicherheitslücke sollte den Sicherheitsarchitekten des Unternehmens nicht durch auffällige Aktivitäten im System frühzeitig aufgezeigt werden (vgl. Krotofil und Cárdenas 2013: 167).

[373] Ein interessanter Aspekt der systemischen Perspektive von Resilienz im Allgemeinen ist, dass etwa 80 Prozent der deutschen mittelständischen Unternehmen immer noch Windows XP als Betriebssystem ihrer Produktionsanlagen und sogar der Systemadministration verwenden. Dieses Betriebsprogramm gilt aus Sicht des Informationsschutzes veraltet, ist aber dennoch weit in der Wirtschaftswelt verbreitet. Es verhalf der Schadsoftware „Wannacry" im Mai 2017 zum Erfolg, da wesentliche Sicherheitslücken des Programms zwar dem US-Geheimdienst NSA bekannt waren (vgl. Eckert 2008: 423f.). Die NSA leitete das Wissen über dieses Problem aber nicht an Microsoft weiter, um die Lücken selbst für Spionagetätigkeiten nutzen zu können (AGCS 2018: 3).

[374] Windows 10 steht beispielsweise im Verdacht neben Daten zur Verbesserung der Performanz auch andere Daten der Nutzer des Betriebssystems auf seinen Cloud-Datenbanken abzulegen. Dies stellt eine Möglichkeit zur intendierten Verletzung der Datenvertraulichkeit dar, kann aber auch von anderen Akteuren genutzt werden um die Daten nicht auf den Systemen des Nutzers, sondern auf den Datenbanken von Microsoft auszulesen (vgl. Sachsinger 2017).

(Mosin, Prajapati und Vohara 2010: 19).[375] Neben diesen Innentätern, kommen Aktivitäten von Außenstehenden hinzu, welche sich mithilfe der Manipulation von Mitarbeitern, sogenanntes Social Engineering, Zugang zu vertraulichen Informationen verschaffen (Choo, Smith und McCusker 2007: 3). Die vierte Kategorie liegt vor, wenn Datenbanken durch die (4) Ausgliederung an externe Partner nicht mehr zur Verfügung stehen oder Informationen über die gemeinsamen Schnittstellen vom Drittanbieter unerlaubt aufgerufen werden. Dabei kann ein sogenannter „Lock-In", das bedeutet ein Einschluss der Daten auf den Systemen des Drittanbieters, unbeabsichtigt durch einen technischen Fehler, unzureichendes technisches Verständnis seitens des Geschäftspartners, Überlastung der Systeme aufgrund von Mehrfachbuchungen oder mit Intention geschehen (Bahli und Rivard 2003: 215). Solche Beispiele des Datenverlusts aufgrund von Risiken des IT-Outsourcings können Unternehmen zum Bruch mit bestehenden Praktiken der Auslagerung veranlassen.[376] Auf der Grundlage staatlicher Regulationen in der Europäischen Union müssen sich Unternehmen vergewissern, dass ausgelagerte Prozesse von IT-Dienstleistern in Form eines angemessenen Kontrollsystems[377] behandelt werden (Gaycken, und Karger 2011: 5).

Durch die vorrausgehende Einordnung haben wir nun eine solide Ausgangsbasis für die Anwendung eines neuen Risikokontrollsystems, welches durch die Erweiterung des Risikobegriffs die Informationen und Daten in die Sicherheitsproduktion einschließt. Zur weiteren Verdeutlichung der Sicherheitsproblematik im Informationszeitalter wollen wir im Folgenden vier Fallbeispiele betrachten, um Funktionsweisen und Reaktionsmuster im Umgang mit geschäftsgefährdenden Risiken unter Berücksichtigung der Digitalisierung zu verstehen. Dadurch sollen die konkreten Anforderungen eines geeigneten, integrativen Risikokontrollsystems im digitalen Zeitalter identifiziert und im nachfolgenden Kapitel über die Implementierung einer resilienten Organisation erarbeitet werden. Das erste Fallbeispiel thematisiert den (1) Identitätsdiebstahl und das Social Engineering. Dieses Beispiel illustriert den potentiellen Schaden welcher für die Reputation und finanzielle Integrität von Unternehmen entstehen kann (Abraham und Chengalur-Smith 2010: 187).

[375] Ebenfalls ist zu berücksichtigen, dass Administratoren mit weitreichenden Rechten auf den Plattformen des Unternehmers auch aus Frustration oder anderer Motivation heraus schädliche Handlungen vornehmen können, beispielsweise nach einer Entlassung sensible Informationen zu entwenden oder Datenbanken zu manipulieren.
[376] In diesem Fall ist das technologische Risiko vorrangig in der unzureichenden IT-Kompetenz sowie mangelhaften Supply Chain Risk Management zu verorten (Xue et. al. 2013: 334).
[377] Das Bewusstsein über Risikoszenarien wie beispielsweise einen „Lock-in" von geschäftskritischen Daten zeigt sich beispielsweise dadurch, dass 60% der Banken beispielsweise auf Prüfungsberichte und eine Dokumentation der Risikokontrollsysteme seitens ihrer IT-Dienstleister verlangen (Schwering 2010: 236).

Ferner werden Schadprogramme, sogenannte (2) Malware im zweiten Beispiel thematisiert, und erheblichen Schaden durch die Verletzung der Datenvertraulichkeit oder Verfügbarkeit verursachen können (Provos et. al. 2007: 1). Dem folgt die Betrachtung der (3) Ransomware, welche erpresserischen Absichten durch die Verschlüsselung von Daten mithilfe eines eingeschleusten Schadprogramms folgt. Dieses Fallbeispiel zeigt eindrücklich, welche Konsequenzen für die Fortsetzung der Geschäftsaktivität aus unzureichenden Schutzstandards[378] entstehen können (Salvi und Kerkar 2015: 2). Als viertes Fallbeispiel wird die Bedeutung der (4) IT-Prozesskontinuität, repräsentiert durch die Anforderungen des IT Service Continuity Management (ITSCM) vorgestellt.[379] Die Fallbeispiele sollen aufzeigen, durch welche sicherheitsrelevanten Problemfelder Im Zuge der Digitalisierung entstanden sind und auf welche Art sie die Risikokontrolle von Unternehmen herausfordern, um die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen sicherzustellen.

6.3. Fallbeispiel 1 - Identitätsdiebstahl und Social Engineering

Identitätsdiebstahl und Social Engineering sind zwei verschiedene Varianten, um sich Zugang zu vertraulichen Informationen zum Zweck betrügerischer Handlungen zu beschaffen. Hier kann sowohl die Intention zur Spionage durch Konkurrenten (McGuire 2015: 47) oder die Suche nach vertraulichen Informationen zur Vorbereitung einer Erpressung, als auch die Aneignung von Daten zur Durchführung eines Betrugs als Motivation auschlaggebend sein (Vassilaki 2015: 23). Auch die Informationsaneignung zum Zweck der Reputationsschädigung einer Person, Gruppe oder eines Unternehmens kann mit Hilfe dieser Techniken erfolgen. Beide Felder, der Identitätsdiebstahl und Social Engineering, stellen vorrangig Techniken dar, welche eine relevante Gefahr für Unternehmen wie Individuen darstellen (Abraham und Chengalur-Smith 2010: 183). Die Zunahme dieser Praktiken während der Corona-Pandemie erklärt sich auch aus der Herausforderung, welche Mitarbeiter im neuen virtuellen Arbeitsumfeld, bei gleichzeitiger Belastung durch die Lockdowns zu bewältigen hatten. Die Ausnutzung dieser Situation durch Kriminelle zeigte sich in den Fallzahlen, in denen sich ein Großteil der Angriffe sozialer Mechanismen und Exploitation („social hacking“) bedienten (Wentland und Klimburg-Witjes 2021: 168). Die folgenden Beispiele von Identitätsdiebstahl und Social Engineering sollen helfen diese Problematik für die Sicherheitsproduktion in Unternehmen zu illustrieren.

[378] In diesem Beispiel wird die Krise durch den erfolgreichen Angriff der Schadsoftware auf die Integrität der Netzwerke eines Unternehmens begründet. Die Verschlüsselung der Daten zum Zweck der Erpressung von Lösegeld kann zudem eine Unterbrechung der Geschäftsprozesse zu verursachen.

[379] Die in Form des ITSCM formulierten Anforderungen an die unterbrechungsfreie Funktionalität von IT-Infrastruktur, Middleware und Anwendungen sowie der darüber prozessierten Daten sollen die Komponenten eines geeigneten Risikokontrollsystems zur Sicherstellung der Kontinuität von Geschäftsprozessen aufzeigen.

6.3.1. Digitale Maskerade - Identitätsdiebstahl

Der Identitätsdiebstahl repräsentiert eine Vorgehensweise, durch die sich unbefugte Dritte Zugang zu den persönlichen Authentifizierungsdaten einer Person verschaffen und in deren Namen Handlungen im Internet vornehmen (Willems: 2013: 3). Dies wird bevorzugt für betrügerische Handlungen eingesetzt, indem unter der Vorspiegelung einer falschen Identität Geschäftsbeziehungen eingegangen oder Aussagen im Namen anderer getätigt werden.[380] Dazu können zwei Bereiche differenziert werden, die nach Borges et.al. als „Identitätsmissbrauch" und „Identitätsdiebstahl" gruppiert werden. Ersteres beziffert das Vortäuschen einer fremden Identität in betrügerischer Absicht. Das umfasst „das Handeln gegenüber einem Dritten unter einer anderen als einer eigenen Identität" ohne jedoch eine Befugnis dafür innezuhaben (Borges et. al. 2011: 23)[381]. Der Begriff des Identitätsdiebstahls hingegen wird „als missbräuchliche Nutzung personenbezogener Daten verstanden", aber darüber hinaus auch in der Literatur als eigentlicher Akt der Aneignung einer fremden Identität beschrieben: „Nach einer anderen Auffassung soll Identitätsdiebstahl als die Aneignung von Daten verstanden werden, mit denen man sich im Rechtsverkehr identifizieren kann" (ebd.). Wir wollen im Folgenden den Identitätsdiebstahl in den Fokus fassen und als Summe der Elemente verstanden wissen, in deren Folge eine unbefugte Person sich mithilfe einer fremden Identität Vorteile verschafft.

Die unautorisierte Aneignung einer fremden Identität wird im Cyberzeitalter durch zwei wesentliche Entwicklungen begünstigt. Zum einen müssen sich Betrüger nicht mehr die Mühe machen eine andere Person in einer physischen Interaktion zu imitieren, sondern können mithilfe des Internets unter deutlich sparsameren Einsatz von Ressourcen die relevanten Informationen über die Zielperson zusammentragen und durch Manipulation der Identifizierungsverfahren in deren Namen handeln (McGuire 2015: 46). Im analogen Zeitalter war dies durch den persönlichen Verkehr zwischen Individuen aufwendiger und von spezifischen Voraussetzungen wie einer optischen und sprachlichen Ähnlichkeit beziehungsweise bestimmten Fähigkeiten abhängig, wie etwa andere Personen von der Authentizität der Personenimitation zu überzeugen.[382] Die Aufwände der

[380] Auch die „Identität" von Unternehmen oder staatliche Behörden kann von Kriminellen imitiert werden, um ihre Opfer zur Preisgabe von Informationen oder Zahlung einer Rechnung zu bewegen. Die unternehmerische Reputation ist somit als Identität zu verstehen, deren Handlung und Interaktionen mit der Umwelt als solche von anderen Akteuren verstanden werden (Serrat 2011: 1). Auch in politischer Hinsicht ist die Fälschung von Identitäten relevant, etwa als Technik zur Verbreitung von Falschnachrichten.

[381] Identität wird wie folgt verstanden: „Menge an Daten, durch die eine Person in einem bestimmten Zusammenhang eindeutig bezeichnet und von anderen unterschieden werden kann" (Borges et. al. 2011: 17).

[382] Darunter können Dokumentenfälschungen zum Zweck der Vortäuschung einer unberechtigten Authentizität, beispielsweise durch Fälschung von Urkunden, Identifikationsausweisen wie einem Reisepass oder fremder Anspruchsleistungen verstanden werden. (Borges et. al. 2011: 25). Andere Methoden der Kommunikationsübertragung wie dem Briefverkehr und dem Telefon boten ebenso die Möglichkeit eine fremde

Informationsbeschaffung wurden jedoch durch die frei zugänglichen oder über Big Data leicht abrufbaren Informationen im Internetzeitalter signifikant reduziert. Ferner ist die Vortäuschung einer falschen Identität über Automatisierungstechniken wie Spam, Chatbots oder KI gesteuerte Applikationen ökonomisch rationalisiert worden (Huber et. al. 2009: 119). Der zweite begünstigende Umstand ist die Anonymität des Netzes, welche betrügerischen Handlungen stärkeren Schutz vor Entdeckung und Strafverfolgung bietet als das unter analogen Bedingungen möglich gewesen wäre. Folglich können geringere Investitionskosten, höhere Gewinnaussichten und vor allem der Mantel der Anonymität wesentliche Aspekte repräsentieren, die einen Identitätsdiebstahl in der digitalen Epoche für unterschiedliche Skalierungen und Anwendungsvariationen interessanter erscheinen lassen.

Die Herausforderung ist vielmehr die Erlangung der zumeist elektronischen Identifikationsmerkmale, wie Passwörter oder anderer Zugangskanäle auf digitale Profile[383]. Letztere gelten als identifizierte Entitäten der digitalen Kommunikation und werden nach einmal erfolgter Authentifizierung als echte, das bedeutet legitime Abbilder der natürlichen Identität wahrgenommen (Huber et. al. 2009: 119). Auf dieser Grundlage sind die digitalen Profile formell berechtigt, Handlungen im Namen des Unternehmens vorzunehmen und beispielsweise Verträge oder Abtretungen einzugehen, im Fall von Smart Contracts[384] sogar automatisiert. Durch die Authentifizierung im Internet können sich Unbefugte über den Zugriff auf die digitale Identität die Möglichkeit eröffnen, Gewinne im analogen Raum zu erzielen (Orebaugh 2012: 5). Folglich liegt das Gros der initialen Aufwände in der Suche nach einer Methode, die Zugangsidentifikation zu überlisten und Zugriff auf das digitale Profil zu erhalten (Sittig und Singh 2016: 626). Denn mit dem Zugriff auf ein fremdes Profil kann eine digitale Maskerade in Gang gesetzt werden, an deren Ende ein Vorteilsgewinn für die unbefugten Dritten beabsichtigt ist.[385]

Identität vorzutäuschen, unterlagen jedoch ebenso dem hohen Aufwand entsprechende Informationen über verschiedene Kanäle zu erlangen, um eine überzeugende Hintergrundgeschichte aufzubauen.

[383] Das digitale Profil repräsentiert daher die analoge Identität einer Person oder Gruppe, die in Folge der Digitalisierung in den virtuellen Raum transzendiert ist und dort für die analogen Raum Entscheidungen treffen kann. Die Manifestationen eines digitalen Profils können sich in den Zugangsmöglichkeiten zu einem Bankkonto, Wählerregister, Benutzerkonto oder einer sozialen Plattform wiederspiegeln. Ebenfalls Benutzer- und vor allem Administratorenkonten von Unternehmen oder Organisationen im Allgemeinen zählen zu den interessantesten Profilen, derer sich Kriminelle zu bemächtigen versuchen.

[384] Ein Smart Contract ist ein durch ein Computerprogramm gesteuertes Vertragsdokument, zumeist in Verbindung mit der Verschlüsselungstechnologie Blockchain. Es erlaubt die Erfüllung von Bedingung zur Rechtmäßigkeit des Vertragsgegenstandes unter zuvor definierten Voraussetzungen für die Vertragspartner zu prüfen und automatiisert freizugeben. (Kolvart, Poola und Rull 2016: 134).

[385] Zum Beispiel übernahmen Kriminelle die digitale Identität eines Anbieters auf der Plattform eines Online-Warenhaus und boten nicht existente Waren zum Verkauf an, deren Erlöse vom gekaperten Profil auf andere Konten umgeleitet wurden (Vassilaki 2015: 17).

Zu diesem Zweck versuchen Angreifer die Identifikationsschranken durch unterschiedliche Techniken zu überwinden. Die klassische Methode der Identifikation ist die Vergabe eines Passwortes, durch dessen Eingabe ein eindeutig zugewiesener Nutzer den Zugang zum digitalen Profil erhält. Neben unzureichenden Standards im Rahmen der Passwortauswahl[386], können Mitarbeiter durch sozio-technische Verfahren verleitet werden das Passwort preiszugeben (vgl. Hong 2012). Die unterschiedlichen Methoden zur Erschleichung von Informationen und Zugangsdaten werden als „Phishing" bezeichnet, welches dem „Ausspionieren oder/und dem Missbrauch vertraulicher Daten" dient (Walter: 2008: 19). Der Begriff subsummiert somit unterschiedliche Techniken, wie etwa die Abfrage von Kennwörtern unter Vortäuschung falscher Tatsachen.[387] Ebenso können SPAM Emails – das sind massenhaft versendete Werbenachrichten mit dem Ziel Nutzer auf Internetseiten zu locken – die Neugier oder auch nur reine Gier von Personen auszunutzen und die Eingabe von sensiblen Informationen für etwa ein Gewinnspiel zu bewirken (Riekmann und Kraus 2015: 299).

Der Schaden aus „Phishing" für Unternehmen wurde in den USA auf bis zu 3 Milliarden US-Dollar pro Jahr[388] geschätzt (Hong 2012: 76) und hat sich seit der Corona-Pandemie verhundertfacht (Lallie et. al. 2020: 3). So erfolgt mittlerweile jeder vierte Angriff statistisch gesehen als Phishing-Versuch (Dreißigacker, von Skarczinski und Wollinger 2020: 946). Für Unternehmen können sowohl entweder direkte als auch indirekte Schäden entstehen. Direkt sind Unternehmen beispielsweise durch den Verlust von Informationen, Erpressung mit erbeuteten Informationen oder der Manipulation des Systems betroffen. Indirekte Schäden und Belastungen können darüber hinaus durch die notwendigen, nachfolgenden Sicherheitsüberprüfungen und Updates der Systeme resultieren, sowie durch den Reputationsschaden im Fall des Bekanntwerdens eines erfolgreichen Angriffs.

Auch andere Identifikationsmethoden können von Außenstehenden überlistet werden. Biometrische Identifikationsmerkmale wie ein Fingerabdruck können ohne Wissen des Nutzers

[386] Der gegenwärtige Standard für die Vergabe eines Passwortes umfasst die folgenden Kriterien: Mindestens acht Zeichen, von denen mindestens ein Zeichen eine Zahl sein muss und sowohl Groß- als auch Kleinbuchstaben verwendet werden sollten. Ein weiteres Kriterium ist die Verwendung eines Sonderzeichens, welches allerdings unter Umständen auf fremdsprachigen Tastaturen zur Unzufriedenheit einiger Nutzer nicht aufzufinden ist. Erweiterte Sicherheitsstandards können den Ausschluss der Wiederholung der letzten fünf bis zehn Passwörter beinhalten und eine fortführende Nummerierung oder Buchstabenfolge auf der Tastatur ausschließen. Gleiches kann für die Wiederholung von Buchstaben im Passwort gelten. Nach diesen erweiterten Vorgaben wäre ein Passwort mit auf- oder absteigender Zahlenfolge wie „XX123456" ungültig. Ferner sind aufeinanderfolgende Wiederholungen von gleichen Zeichen untersagt, wie beispielsweise „AAAA2017".

[387] Beispielsweise kann sich ein Anrufer oder Absender einer Email als Systemadministrator ausgeben und nach den Passwörtern zur Installation eines Systemupdates fragen.

[388] Eine Hochrechnung aus dem Jahr 2015 bezifferte die durchschnittlichen Kosten für eine Privatperson, die Opfer einer „Pishing"-Attacke wurde auf 814 Euro, etwa durch Waren- oder Kreditkartenbetrug der mithilfe der erbeuteten Daten durchgeführt werden kann (Riekmann und Kraus 2015: 299).

im öffentlichen (analogen) Raum abgenommen werden oder von digitalen Datenspeichern ausgelesen werden.[389] Der biometrischen Abdruck kann physikalisch durch 3D-Drucker nachempfunden werden oder unter Manipulation einer analogen Schnittstelle über einen Eingriff in die Steuerungssoftware vorgetäuscht werden (Ruiz-Albacete et. al. 2008: 2). Doch der letzte Schritt des „Phishing" ist stets die Monetisierung der gesammelten Informationen, entweder durch den Weiterverkauf an andere Gruppen oder zur eigenen Nutzung der Zugangsdaten zum Zweck der weiteren Informationsbeschaffung oder anderer kriminellen Aktivitäten unter Missbrauch des somit übernommenen Profils (Hong 2012: 75). Die Kreditkartennummer beispielsweise gilt als besonders leichtes „Phishing"-Ziel, da sie vielfach von Nutzern in Kontaktformularen und zur Buchung im Internet eingegeben wird. Als Folge soll der Wert eines vollständigen Kreditkartendatensatzes, einschließlich des Gültigkeitsdatums und der Prüfziffer für relativ geringe Summen gehandelt werden (Borges et. al. 2011: 27).

Grundlegende Schutzmaßnahmen gegen den Identitätsdiebstahl gelten für Privatpersonen wie für Unternehmen gleichermaßen: Eine durchgehende und anhaltende Sensibilisierung aller Beteiligten für die Risiken eines unbedarften Umgangs mit vertraulichen Identifikationsschlüsseln sowie die unbedingte Notwendigkeit zur Einhaltung der Sicherheitsstandards kann wesentlich dazu beitragen, das Sicherheitsniveau zu erhöhen. Dies wurde insbesondere während des ersten Jahres der Corona-Pandemie unter den herausfordernden Bedingungen des Home Office und fehlender Sicherheitsprotokolle beziehungsweise deren Unkenntnis durch Mitarbeiter in einigen Unternehmen berichtet (Chigada und Madzinga 2021: 5). Im Allgemeinen dienen umfassende Risikokontrollen wie etwa standardisierter Kriterien von Passwörtern, Bewusstseinsschaffung und Sensibilisierung von Mitarbeitern (Greitzer 2014: 240), sowie automatisierter Erkennungssoftware in den Netzwerken, welche verdächtiges Verhalten und Normabweichungen entdecken und melden (Mosin, Prajapati und Vohara 2010: 18).[390] Insbesondere die Schnittstelle zwischen analoger und digitaler Sphäre, in welcher der menschliche Faktor als Schwachstelle in Erscheinung tritt, ist von großer Bedeutung und wird im Folgenden untersucht werden.

[389] Für viele Fingerabdruckscanner reicht bereits eine zweidimensionale Abbildung, da diese nicht zwischen zwei- und dreidimensionalen Abdrücken (wie im Fall des originären Abdrucks) unterscheiden können. Eine dreidimensionale Lesefähigkeit der analogen Schnittstellen ist vielfach zu teuer und wird selten eingesetzt (vgl. Erdogmus und Marcel 2014: 1087).

[390] Überwachungssysteme können auf der Grundlage von Metadaten und der Verarbeitung spezifischer Informationen Schutzschranken einziehen. Dies kann beispielsweise bei unautorisierten Kreditkartenzahlungen zum Einsatz kommen, wenn die regulären Verhaltensmuster eines Karteninhabers plötzlich abweichen. Kreditkartennutzungen außerhalb des individuellen Musters können eine besondere Beobachtung aktivieren und gegebenenfalls in der vorübergehenden Sperrung der Karte resultieren.

6.3.2. Der menschliche Faktor - Social Engineering

In mancher Hinsicht überschneidet sich der Identifikationsdiebstahl mit dem zweiten Feld dieses Abschnittes, da die notwendigen Informationen zur Authentifizierung für ein fremdes digitales Profil durch eine Kombination von analogen und digitalen Mitteln, den Social Engineering einer Spezifikation des Social Hacking erlangt werden können. Die Besonderheit dieser Methode liegt in der Verbindung unterschiedlicher Elemente, durch deren Zusammenspiel Schwachstellen des Schutzkonzepts eines Unternehmens identifiziert und ausgenutzt werden können (Mosin, Prajapati und Vohara 2010: 18). Verstanden werden soll Social Engineering hier als betrügerische Methode zur Erlangung von Informationen, deren Zugang durch Vortäuschung fremder Identitäten oder dem Ausnutzen zwischenmenschlicher Kontakte in Kombination mit Techniken der analogen oder elektronischen Infiltration eines Unternehmens oder Gruppe verstanden werden. Das explizierte Ziel von Social Engineering ist die Umgehung technischer Schutzschranken durch die Manipulation des schwächsten Gliedes der Sicherheitsarchitektur, dem menschlichen Faktor (Borges et. al. 2011: 103).

In unserem Kontext sind weitere relevante Merkmale des Social Engineering zu nennen, wie die verhältnismäßig lange Vorbereitungs- und Durchführungszeit, das hohe Anforderungsprofil an die beteiligen Personen und das Risiko der eigenen Exposition durch einen direkten Kontakt zum Zielobjekt. Die folgenden Elemente eines Social Engineering Angriffs können extrapoliert werden. Am Beginn der Initiative steht die (1) Identifikation der gesuchten Informationen und relevanter Akteure, über welche die Daten bezogen werden könnten. Als zweiten Schritt dient die (2) initiale Kontaktaufnahme, in deren Verlauf den potentiellen Opfern Anreize vermittelt werden, die Angreifer in die Räumlichkeiten des Unternehmens einzuladen (Mosin, Prajapati und Vohara 2010: 19). Im dritten Schritt beginnen die Angreifer die (3) Infiltration des Unternehmens und versuchen über ihre Direktkontakte, „Phishing“ oder durch Suche nach ungeschützten Schnittstellen wie Computern oder Datenträgern Schadsoftware innerhalb des geschützten Netzwerks zu etablieren. Mithilfe der eingeschleusten Trojaner und Schadsoftware können die Angreifer ihre Suche nach relevanten Personen oder Akteuren ausdehnen (Abraham und Chengalur-Smith 2010: 185) und ein (4) profundes Verständnis der Organisationsstruktur erlangen, welches als Schlüssel zur Vorbereitung des eigentlichen Vorhabens dient. Denn im fünften Schritt, werden die (5) relevanten Daten entwendet und Spuren bei Bedarf verwischt, beziehungsweise falsche Fährten gelegt, um einer Aufdeckung des Angriffs entgegenzuwirken (Greitzer 2014: 236). Anhand dieser Punkte wollen wir nun die Techniken und Besonderheiten des Social Engineering genauer betrachten.

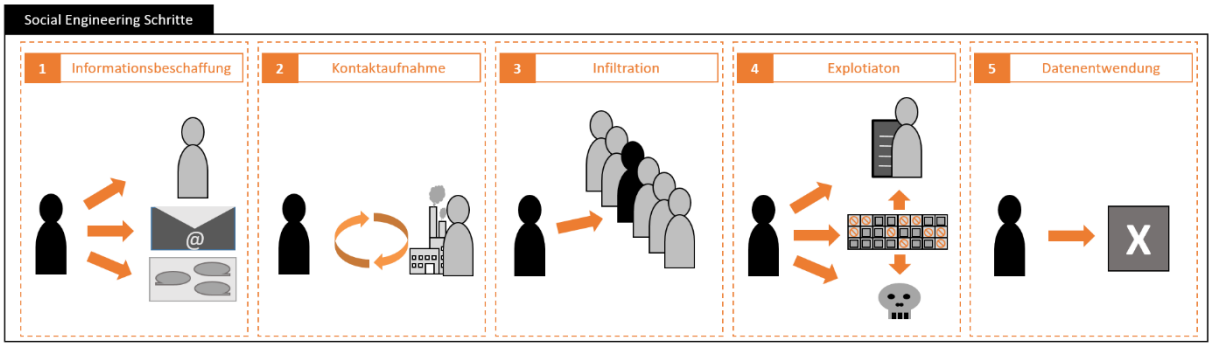

Abb. 6.4. Idealtypische Schritte des Social Engineering. Eigene Darstellung.

Die (1) Identifikation möglicher Angriffspunkte in Gestalt von Personen oder Plattformen ist durch das Internet wesentlich erleichtert worden. Durch den Schutz der Anonymität des Netzes können professionelle Angreifer wesentliche Informationen sammeln und ihre Scheinidentität vorbereiten (Huber et. al. 2009: 117). Netzwerke wie Facebook oder LinkedIn sowie andere Einträge verraten den Angreifern Präferenzen und Interessen ihrer potentiellen Opfer, welche entsprechend eingesetzt werden, um deren Aufmerksamkeit zu erlangen (Greitzer 2014: 237). In diesem Schritt können ähnliche Methoden wie im Fall des Identitätsdiebstahls sowohl für die Informationsbeschaffung, als auch zur Vorbereitung einer Tarnidentität eingesetzt werden. Das sogenannte „Dumpster Diving" kann ebenfalls in der Informationsbeschaffungsphase zum Einsatz kommen (Borges et. al. 2011: 104), in welchem der Müll von Unternehmen oder auch von potentiellen Opfern nach verwertbaren Informationen ausgewertet wird.

Nicht nur geschäftsbezogene Interessen können für die (2) initiale Kontaktaufnahme in Frage kommen, sondern ebenso private Vorlieben eingeflochten werden. Die Vorspiegelung gemeinsamer Hobbies oder anderweitiger Scheinverbindungen kann zur Vertrauensbildung seitens des Opfers eingesetzt werden. Auch Testanrufe bei Mitgliedern des Unternehmens können weitere Informationen über den Aufbau und das Organigramm verschaffen (Huber et. al. 2009: 119) und somit in folgenden Gesprächen Authentizität vermitteln. Ferner kann die Nachahmung von echten oder fiktiven Mitgliedern („Impersonation") eine Möglichkeit sein, Kontakte aufzubauen, Informationen anzufordern und ein weiteres Vordringen in die Organisation zu ermöglichen (Willems: 2013: 4). Der "(m)ost powerful and danger trick for gaining physical access to the system is to pretend to be someone from inside the company (…). It is the most time consuming attack as it requires research to get information regarding target to establish the legitimacy in the mind of target" (Mosin, Prajapati und Vohara 2010: 19).

Die initiale Kontaktaufnahme ist ein kritischer Punkt, da die potentiellen Opfer mithilfe psychologischer Tricks und Vortäuschung falscher Tatsachen dazu gebracht werden sollen, den

Angriff ohne deren Kenntnisnahme zu unterstützen. Dies kann entweder durch Informationen über das Unternehmen, Folgeeinladungen zu weiteren Besprechungen oder im Idealfall durch unwissentliches Ermöglichen eines Identitätsdiebstahls zur Kaperung eines digitalen Profils beitragen (Abraham und Chengalur-Smith 2010: 186). Mithilfe des Profils gewinnen die Angreifer einen wichtigen Brückenkopf innerhalb des Unternehmens und überwinden somit die Schutzschranken wie Firewalls und Virenscannern. Das Opfer kann auch in einen Agenten im Sinne der Angreifer gewandelt werden, wenn sein digitales Profil als „Zombie-Nutzer" Aufträge der Angreifer übernimmt oder das Opfer selbst durch Bestechung oder unter Ausnutzung anderer Motive der individuellen Illoyalität wie aufgrund von Unzufriedenheit und Ausgrenzungswahrnehmung erreicht werden (Choo, Smith und McCusker 2007: 3). Die Erfolgsaussichten der letzteren Variante sind allerdings ebenso schwierig einzuschätzen, wie auch extrem risikoreich, da der Angriff durch einen solchen Rekrutierungsversuch eines Innentäters entdeckt und das gesamte Vorhaben verhindert werden kann.

Die (3) Infiltration des Unternehmens beginnt über den Kontakt, der unter einer falschen Identität und Agenda, mit dem eigentlichen Ziel erfolgt, Zugang zu den Räumlichkeiten und internen Informationen des Unternehmens zu erhalten. Im Fokus dieses Schritts steht die Etablierung eines Zugangs zu internen Informationen, also solchen die nicht von der Außenwelt aufgerufen werden können. Hierbei ist zwischen einem einmaligen Angriff („single stage attack") und einem komplexeren, multidimensionalen Angriff („multi stage attack") zu unterscheiden. Gelingt dem Angreifer bereits beim ersten Kontakt oder in dessen unmittelbarer Folge der Zugriff auf die gesuchten Daten, spricht man von einem einmaligen Angriff. Sind hingegen mehrere Anläufe, Ebenen und Kontaktpersonen involviert, ist von einem multidimensionalen Angriff auszugehen, dessen Länge sich am Komplexitätsgrad der Aufgabe orientiert und zwischen einigen Stunden bis zu mehreren Wochen andauern kann (Greitzer 2014: 237). Bemerkenswert ist, dass Individuen häufig in ihrer Eigenwahrnehmung davon ausgehen, auf Techniken des Social Engineering, einschließlich „Pishing" und „Whaling"[391]

[391] Eine Methode inkludiert es sich am Telefon als Führungskraft des Unternehmens auszugeben und Mitarbeiter zur Preisgabe von sensiblen Informationen zu bewegen (Mosin, Prajapati und Vohara 2010: 19). Auch das „Whaling", eine Form des „Pishing" von Daten wichtiger Entscheidungsträger zählt in diese Kategorie. Der Name leitet sich von den „big whales" ab und umschreibt die Adressierung von Handlungsbevollmächtigten unter dem Vorwand einer Rechtsstreitigkeit oder anstehenden Anklage, vorzugsweise in Sachzusammenhängen in denen eine persönliche Haftung des Opfers möglich wäre, um deren Interesse zu wecken (Abraham und Chengalur-Smith 2010: 187). Die einmal geöffnete Interaktionsebene dient dem Zweck der Informationsbeschaffung und zur Vorbereitung weiterer Schritte zur Infiltration des Unternehmens.

ausreichend vorbereitet zu sein und deren Intention rechtzeitig erkennen zu können(Huber et. al. 2009: 118). Die Realität weist jedoch häufig ein anderes Bild auf.[392]

Mithilfe der erbeuteten Informationen können die Angreifer die nächsten Schritte vorbereiten und mit der (4) Auswertung der gesuchten Daten beginnen.[393] Die gesammelten Informationen eröffnen jeweils eine weitere Option die gesuchten Informationen zu lokalisieren und Akteure oder Datenbanken für weitere Angriffe zu identifizieren. Wenn die Angreifer ihr Ziel erreicht haben, können sie die (5) Daten entwenden und falsche Fährten legen, um den Vorgang ihres Angriffes zu verschleiern oder versuchen die Spuren ihres Handelns gänzlich zu beseitigen. Letzteres könnte vorteilhaft für den Wert der entwendeten Informationen beziehungsweise aus der Perspektive der Auftraggeber erwünscht sein. Geschäftspläne und Strategiepapiere gewinnen ihren eigentlichen Mehrwert aus dem einseitigen Einblick in die Absichten der Konkurrenz, ohne dass diese davon Kenntnis nimmt. Gleiches gilt für technische Daten, Forschungsergebnisse und Geschäftsgeheimnisse, die nur unter der Voraussetzung der Geheimhaltung der Informationsbeschaffung für den Auftraggeber von Vorteil sind. Die Mehrheit der Fälle von Social Engineering operiert mithilfe von einmaligen Interaktionen, deren Zweck die Implementierung einer Schadsoftware ist, auch um das Risiko einer Aufdeckung und Strafverfolgung für den Angreifer zu reduzieren (Pathak 2016: 372).

Zusammenfassend lässt sich der Begriff Social Engineering folglich auf eine Vielzahl an Angriffsvariationen anwenden, bei denen Nutzer unter Verwendung psychologischer Methoden zur impliziten oder expliziten Preisgabe von sensiblen Informationen verleitet werden sollen. Ein Grund für deren Erfolg kann in der geringen Aufmerksamkeit von Nutzern hinsichtlich Gefahren liegen (Weber 2016: 28). Gerade im Fall von Nachrichten von (angeblichen) externen Partnern und Dienstleistern scheint die Toleranz von Nutzern im Fall von Normabweichungen

[392] Ein tatsächliches Beispiel offenbarte dies deutlich, als ein Angreifer sich als Vertreter der Hausbank eines Unternehmens ausgab und aufgrund einer angeblichen Sicherheitslücke Informationen bei Mitarbeitern abfragte. Ein Mitarbeiter folgte der Aufforderung und gab sensible Daten unwissentlich an den Angreifer weiter, darunter auch Einwahldaten für dessen digitales Profil. Mithilfe dieser gekaperten Identität konnte sich der Angreifer als eben jener Mitarbeiter ausgeben und sowohl Kunden des Unternehmens als auch dessen Vorgesetzte kontaktieren und in einem vermeintlich sicheren Umgebung weitere Informationen abfragen, beziehungsweise seiner ersten Tarnidentität zur Glaubwürdigkeit verhelfen, so dass auch andere ihre Daten bereitwillig an den als Sicherheitsdienstleister der Hausbank getarnten Angreifer weitergaben (Greitzer 2014: 242). In einem anderen Fall gaben sich Kriminelle als Vertreter des Bundeskriminalamtes (BKA) aus und forderten Internetnutzer per Telefon und zusätzlich über Email auf, einer Vorladung Folge zu leisten. Über einen Link wurden mögliche Termine angeboten, welcher in Wirklichkeit eine Schadsoftware zur Erschleichung der Passwörter und Einblick in den Kalender des Opfers ermöglichte (Vassilaki 2015: 16).

[393] Ungeschützte Zugänge zu den Datenbanken bieten ideale Voraussetzungen. Auch können Mitarbeiter unter vorgespielten Vorwänden gebeten werden den Angreifern ihre Arbeitsplätze zu überlassen oder beispielsweise durch einen von den Angreifern ausgelösten Feueralarm zum Verlassen des Gebäudes veranlasst werden. Bis zum Eintreffen der Feuerwehr und Überprüfung des Alarmauslösers vergeht in der Regel ausreichend Zeit zur Ausspähung der in Eile möglicherweise ungesicherten Arbeitsplätze (Mosin, Prajapati und Vohara 2010: 19).

höher zu sein, beispielsweise wenn die Namen der verwendeten Emailserver abweichen oder statt der eigentlichen Emailadresse eine semantisch nahestehende Variation verwendet wird. Ein wichtiger Aspekt laut Greitzer ist auch die allgemeine Risikoperzeption durch die Nutzer selbst, beispielsweise wenn die Wahrscheinlichkeit eines Angriffs durch Social Engineering unterschätzt, beziehungsweise die Leistungsfähigkeit der eigenen Sicherheitsstandards überschätzt wird (Greitzer 2014: 240). Soical Engineering und der zuvor thematisierte Informationsdiebstahl sind wirkungsvolle Methoden um vertrauliche Informationen zu erhalten und stellen für Unternehmen wesentliche Risiken hinsichtlich der Vertraulichkeit und Integrität von Informationen dar. Diesen Aspekt werden wir im nächsten Fallbeispiel anhand von automatisierten Angriffen durch Malware weiterverfolgen.

6.4. Fallbeispiel 2 – Malware

Das zweite Fallbeispiel thematisiert die klassische Schadsoftware (Malware), welche ein Kernaspekt der Risikoexposition im digitalen Zeitalter ist. Eine Malware ist eine „Software, die ohne Wissen und Zustimmung des Nutzers in einen Computer eingeschleust wird und dort Schäden verursacht (…) [beziehungsweise] sich unter Rückgriff auf E-Mail-Daten des Computers selbst weiterverbreitet“ (Walter: 2008: 19). Dieser Begriff kann verschiedene Evolutionsstufen des Computerprogramms umfassen und von simplen Softwareprogrammierungen bis zu komplexen, selbstlernenden Algorithmen reichen. Gemeinsam ist den Programmen ihre intendierte Schädigung von Systemen zum Nutzen ihrer Anwender (Moser, Kruegel und Kirda 2007: 231), entweder um Zugang zu sensitiven Daten zu erhalten, Sicherheitssysteme zu überwinden oder Schaden innerhalb eines Systems zu verursachen. Malware sind beständige Begleiter des digitalen Zeitalters und generieren hohe Umsätze auf Seiten der Kriminellen auf Kosten der geschädigten Personen, Gruppen oder Unternehmen (Walter 2008: 19). Privatpersonen, politische Gruppierungen oder Regierungen benutzen Schadsoftware zur unlauteren, aber ebenso effektiven Umsetzung ihrer jeweiligen Agenda oder geben diese bei Herstellern von Malware in Auftrag (Gaycken und Karger 2011: 4). Im Ergebnis ist ein breites Feld an involvierten Akteuren und Schadsoftwaretypen zu beobachten. Wir wollen im Folgenden den Blick auf die Kategorisierung der Malware wenden und anschließend einige Beispielfälle zurückliegender Angriffe mithilfe dieser Methode analysieren. Den Abschluss bildet eine Betrachtung der dynamischen Beziehungen zwischen Risiken und Kontrollen für Unternehmen auf diesem Feld beleuchten.

6.4.1. Schadsoftwaretypen im Überblick

Für die Programmierung einer Malware gilt es drei prinzipielle Fragen zu klären: Erstens muss (1) das Ziel der Software von Beginn an klar definiert werden, um die nachfolgende Programmierung[394] zielgerichtet abzuschließen (Walter 2008: 19). Zweitens ist die (2) Infiltration eines Systems die größte Herausforderung. Es gibt unterschiedliche Arten ein Netzwerk von außen zu penetrieren, die eleganteste Methode ist jedoch einen Nutzer selbst dazu zu verleiten, einem Malware-Trojaner die virtuellen Pforten zu öffnen. Für diesen Schritt muss der Angreifer einen Nutzer etwa durch Spam-Nachrichten, Social Engineering, Umleitung auf gefälschte Webseiten oder anderen Wegen dazu bringen, die Malware durch die Firewall zu bringen und auf seinem Endgerät zu öffnen. Die weiteren Schritte werden anschließend vom Schadprogramm im Hintergrund eingeleitet (Felt et. al. 2011: 2). Die dritte Herausforderung ist das (3) Verhaltensmuster des Programms innerhalb des fremden Systems zu bestimmen. Denn die Aktivitäten der Schadsoftware sollten vor den Detektionsmechanismen des Netzwerks verborgen bleiben, um die gewünschten Maßnahmen auszuführen (Borges et. al. 2011: 67). Nach Beendigung des Vorhabens kann eine optionale Funktion eingebaut werden um die Spuren zu verwischen, bei Bedarf durch Schadaktivitäten für Ablenkung zu sorgen oder unter Ausnutzung der systeminternen Vernetzung weitere Systemabschnitte oder Profile zu befallen (Abraham und Chengalur-Smith 2010: 185).

Anhand dieser Vorüberlegungen können verschiedene Typen von Schadsoftware unterschieden werden, beginnend mit der zuvor genannten (1) Zielausrichtung. Die wahrscheinlich meist verbreitete Variante ist eine „Spyware“ oder Spionageprogramm, welche die vertraulichen Daten von Nutzern in Erfahrung zu bringen versucht (Walter: 2008: 19). Zu den relevanten Zielen zählen Passwörter, persönliche Informationen bis hin zu Verhaltensmustern und Gewohnheiten.[395] Etwa zwei Drittel aller bekannten Malwaretypen dienen diesem Zweck (Felt et. al. 2011: 1). Eine Spezifizierung dieses Typs ist die „personal spyware“ welche explizit nach persönlichen Daten sucht, so zum Beispiel Textnachrichten auf Mobilfunkgeräten oder das

[394] Der Zweck einer Malware kann beispielsweise nur die Infiltration eines Systems zur Implementation von Spionagesoftware sein, welche den Datenverkehr ausließt (Felt et. al. 2011: 2). Andere Absichten mit spezieller Konfiguration der Malware können die Einschleusung von anderen Schadprogrammen sein (Exploits) oder auf die Manipulation von Netzwerken ausgelegt sein (Krotofil und Cárdenas 2013: 167). Selbst „ready-to-use“ Schadsoftwares, welche andere Nutzer gegen Bezahlung für deren individuelle Ziele einsetzen können, wurden eben für diesen Zweck konzipiert und entsprechend konfiguriert.

[395] Mit Entwicklungen wie dem Internet of Things sind immer größere Datenmengen mit qualitativ hochwertigen Verknüpfungen auf den Endgeräten der Nutzer und den Datenbanken der Unternehmen als mögliche Ziele adressierbar. Dazu zählen der über Smart Meters dokumentierte Energieverbrauch eines Haushalts, um Abwesenheitszeiten zu identifizieren und für beispielsweise Einbrüche zu nutzen (Müller 2011: 547). Ähnlich können Netzwerke oder Datenbanken durch Spyware infiltriert werden um persönliche Informationen, beispielsweise für Social Engineering zu nutzen (Huber et. al. 2009: 117).

Bewegungsmuster einer Person dokumentiert. Diese Applikationen können von spezialisierten Angreifern, beispielsweise im Rahmen von Social Engineering genutzt werden (Huber et. al. 2009: 117), finden aber mit Blick auf ihre quantitative Anwendung zum allergrößten Teil im privaten Bereich zum Zweck der Überwachung des Lebenspartners oder anderer Familienangehörige, häufig unter Verletzung deren Persönlichkeitsrechten statt (Felt et. al. 2011: 2). Sogenannte „Keylogger" gehören ebenfalls zur Gruppe der Spionageprogramme (Rahim et. al. 2018: 3). Sie protokollieren im Hintergrund die Eingabe des Nutzers mittels haptischer Schnittstellen, wie Tastatur, Maus, Touchpad oder Sprachbefehl, um an sensible Daten wie Passwörter zu gelangen (Borges et. al. 2011: 37).

Im Graubereich zu den Spionageanwendungen sind jene Programme, die in ihrem Aufgabenspektrum neben der primären, hilfreichen Funktion auch Verhaltensmuster ihrer Nutzer protokollieren. Die Ergebnisse dieser Auswertung können zur Produktverbesserung, Marktforschung oder Marketing verwendet werden, allerdings in der Regel nicht um dem Nutzer zu schaden (Rahim et. al. 2018: 4). Die rechtliche Stellung dieser „Grayware" hängt entscheidend von den Nutzungsbedingungen und lokalen Regularien zum Datenschutz ab (Felt et. al. 2011: 2). Andere Schadprogramme dienen nur als Türöffner in ein System, dem ein anderes Programm nachfolgen soll um den eigentlichen Auftrag zu erfüllen. Diese Infiltrationsmalware können Trojaner sein, welche sich als ein anderes Programm tarnen, um zu einem späteren Zeitpunkt ihre Aktivitäten zu beginnen (Salvi und Kerkar 2015: 1). Es kann eine Software sein, welche in ein unscheinbares Programm (Office-Programme, Virenscanner, etc.) eingebunden werden, um unbemerkt Lücken in der Sicherheitsarchitektur eines Netzwerkes zu öffnen (Moser, Kruegel und Kirda 2007: 231).

Eine wichtige Gruppe unter den Malwaretypen sind „Botnets", auch wenn es sich bei dem Begriff eigentlich um den Zielzustand der Schadsoftware handelt. Eine dergestalt konzipierte Applikation infiziert ein Endgerät und übernimmt die Kontrolle darüber (Brand, Valli und Woodward 2011: 2). Mithilfe von automatisch versendeten Nachrichten versucht das infizierte Gerät andere Nutzer aus dem Adressbuch zu kontaktieren und die Schadsoftware auch auf deren Computern oder Mobilfunkgeräten zu installieren. Gelingt dies auf einer ausreichend großen Menge an Einzelkomponenten, schließt das Programm diese Geräte zu einem Botnet-Netzwerk zusammen, um unter Ausnutzung der somit akkumulierten Rechenkapazität schadhafte Angriffe gegen andere Systeme durchführen zu können (Orebaugh 2012: 5). Ein Beispiel für eine Anwendung von Botnets ist der „Distributed Denial of Service" (DDoS oder DoS) Angriff, welcher ein Netzwerk durch eine extreme Anzahl von Anfragen überlastet und zum

vorübergehenden Zusammenbruch des Systems führen soll (Brand, Valli und Woodward 2011: 2). Man spricht aufgrund der ferngesteuerten Natur der willfährig gemachten Fremdgeräte auch von einem Netzwerk von „Zombie-Computern“ (Choo, Smith und McCusker 2007: 4). Diese Methode ist eine der effektivsten Varianten, um die Verfügbarkeit von Plattformen und Datenbanken zu unterbrechen. So stehen Botnets zudem im Verdacht für etwa 80 Prozent der weltweiten Spamverteilung verantwortlich zu sein (Walter: 2008: 10) und stellen eine der hochentwickeltsten Bedrohungen dar (Tuan et. al. 2020: 283).

Über die (2) Methoden der Infiltration lassen sich ebenfalls Programmtypen unterscheiden. In den meisten Fällen wird eine Schadsoftware über einen „drive-by“ Download auf das Endgerät geladen (Provos et. al. 2007: 1). Dabei handelt es sich um eine Infektion des Systems über die Navigation auf Internetseiten, deren Besuch ein verstecktes Programm aktiviert und über den Internetbrowser auf dem lokalen Gerät installiert.[396] Die Verteilung von Malware über Emails, worunter insbesondere Spam-Nachrichten eine gewichtige Rolle einnehmen ist ebenso prominent vertreten.[397] Emails können Verlinkungen zu infizierten Webseiten enthalten oder über einen Anhang die Schadsoftware beinhalten (Orebaugh 2012: 4). In beiden Fällen ist das Öffnen des Links oder des Anhangs von entscheidender Bedeutung, kann aber auch in höher entwickelten Fällen bereits in der Email selbst versteckt sein. Eine unauffällige Schnittstelle kann sich dadurch auf dem Endgerät installieren und lädt zu einem späteren Zeitpunkt die eigentliche Schadsoftware eigenhändig aus dem Internet runter (Sittig und Singh 2016: 626). Emails können auch als Social Engineering Variante geeignet sein, um dem User unter Vortäuschung eines Vorwandes, wie etwa eines Sicherheitsrisikos, dazu zu bewegen die Sicherheitseinstellungen manuell zu modifizieren. Wenn der Nutzer den Anweisungen folgt, kann sich die Schadsoftware sogar noch einfacherer im infiltrierten System fortbewegen (Abraham und Chengalur-Smith 2010: 185). Dies ist einer der Gründe, warum auf Netzwerkrechnern stets ein Administratorenpasswort abgefragt werden sollte, wenn Sicherheitsstandards verändert werden.

Auch Neugier ist ein geeignetes Motiv, um Nutzer auf Infektionsquellen zu locken. Dazu werden Suchanfragen nach Prominenten, Sonderangeboten oder Sensationsnachrichten

[396] Durch eine Suchmaschinenoptimierung oder „Google-Hacking“ können Angreifer auch die Order der Suchanfragen von Suchmaschinen wie Google manipulieren, um Nutzer auf „drive-by“ Webseiten zu locken (Borges et. al. 2011: 115).
[397] Infizierte Webseiten können auch bewusst den Originalen nachempfunden sein und versuchen unachtsame Nutzer zum Besuch zu verleiten (Hong 2012: 74).

verwendet, um das Interesse der Nutzer zu wecken (McAfee 2018).[398] Insbesondere Social Media Plattformen werden zunehmend attraktiver für die Platzierung von Malware, welche dem Nutzer unter Vortäuschung einer Aktualisierung von Applikationen oder Sicherheitsabfrage auf Webseiten mit versteckten Schadprogrammen lenken (Orebaugh 2012: 5).[399] Insbesondere mobile Browser bieten sich für diese Methode an, da der komprimierte Bildschirm häufig weniger Möglichkeit bietet gewohnte Seitenmerkmale festzustellen und die Authentizität zu verifizieren (Felt et. al. 2011: 2). Zudem wurden Fälle beschrieben in denen Angreifer einen Link in Form eines Like-Buttons auf Facebook oder anderen Plattformen unter einem aufmerksamkeitserregenden Beitrag präsentierten, welcher jedoch in Wirklichkeit einer Malware Zugang über die Website oder Applikation auf das Endgerät gestattete (Thomas und Nicol 2010: 3). Eine dieser Varianten wurde unter dem Namen „Koobface" bekannt, welche die erfolgreiche Infiltration einer Vielzahl von Profilen und Betriebssystemen gelang[400], indem über gefälschte Eingabemasken Zugangsdaten zu Social Media Plattformen gespeichert und über Spam-Nachdichten weiterverbreitet wurden.[401] Die gekaperten Profile dienten anschließend einem Botnet für DoS Angriffe auf andere Systeme (Orebaugh 2012: 5).

Der dritte Aspekt der Schadsoftware, die (3) Infiltration des Systems bietet ebenfalls eine Option zur Differenzierung. Das sogenannte „Packing" beschreibt eine Methode zur Platzierung von Komponenten einer Schadsoftware im Sekundärspeicher des Zielsystems, um sie vor dem aktiven Zugriff eines Virenscanners zu verbergen. Zu einem späteren Zeitpunkt stellt die Datei ein Abbild des Schadprogrammes erneut zusammen und lädt dieses in den aktiven Arbeitsspeicher, um seinen eigentlichen Zweck zu folgen (Alazab et. al. 2010: 3). Das Prinzip des Polymorphismus erlaubt es einer Schadsoftware sich mithilfe von gängigen

[398] MacAfee, ein Anbieter für Virenschutzprogramme veröffentlichte für 2009 die „riskantesten" Suchbegriffe von Prominenten, welche nach dessen Auswertung am häufigsten zu infizierten Webseiten geführt hätten. Darunter waren die US-Schauspieler Brad Pitt und Jessica Biel an der Spitze gelistet (Abraham und Chengalur-Smith 2010: 187). Diese Liste wird jedes Jahr als Topranking fortgeführt, Im Jahr 2018 waren Diane Krüger und Ruby Rose auf den ersten Plätzen der riskantesten Prominenten im Internet, deren Suche mit neunprozentiger Wahrscheinlichkeit auf eine mit Malware infizierte Webseite führen (McAfee 2018).

[399] Angreifer können beispielsweise personalisierte Nachrichten anhand der auf der Plattform zugänglichen Informationen wie Namen und Interessen versenden, beispielsweise dabei Ankündigen von politischen Parteien oder Angebote von präferierten Marken imitieren. Kriminelle verwenden auch gefälschte Profile, um andere Nutzer zum Öffnen von Links oder Anhängen zu bewegen, beziehungsweise die Preisgabe von Daten zu erbeten (Orebaugh 2012: 5). Die Interaktion auf der Social Media Plattform wirkt dabei auf frequentierte Nutzer weniger verdächtig und veranlasst häufiger zur Aufnahme einer Unterhaltung, in deren Ablauf die infizierte Datei unterbreitet wird.

[400] Die Malware konnte im Jahr 2008 auf Facebook mehr als 217.000 Profile infizieren. Die zu der Zeit zur Verfügung stehenden Virenscanner konnten nur etwa 27 Prozent der Koobface Spamnachrichten nach einer durchschnittlichen Bearbeitungszeit von 4 Tagen identifizieren (Thomas und Nicol 2010: 1).

[401] Im originären Verständnis der Social Media Plattformen Klickzahlen zu generieren, wurden diese Likes" automatisch auch auf der Pinnwand des gehackten Profilinhabers angezeigt und verleitete Freunde und Follower es dem Opfer ähnlich zu tun (Orebaugh 2012: 4).

Verschlüsselungstechniken beziehungsweise Komprimierungsanwendungen vor einer Erkennung durch Virenschutzprogramme zu verbergen (Cavelty 2013: 111). Diese Malware kann sogar seine Komposition anpassen, wenn die Datei im Fall einer Weiterverbreitung auf andere Systeme wechselt, um somit die Wahrscheinlichkeit einer Entdeckung weiter zu reduzieren (Kharraz et. al. 2015: 4). Applikationen mit der Fähigkeit zur Metamorphose können diesen Schritt noch effektiver vollziehen und verbergen ihre wahre Bestimmung durch eine sich unregelmäßig ändernde Komposition der Möglichkeit zur Detektion (Alazab et. al. 2010: 3).

Hochentwickelte Malware kann zudem nach dem erfolgreichen Erstkontakt ein System nach anwenderseitigen Schachstellen absuchen, beispielsweise durch nicht aktualisierte Sicherheitsstandards („Patches“). Als solche kommen vor allem veraltete Browserversionen oder weitverbreitete, aber aus der Perspektive der IT-Sicherheit unzureichend weiterentwickelter Programme wie beispielsweise PDF-Reader in Frage (Borges et. al. 2011: 151). Über diese Hintertüren kann die Schadsoftware in den gesicherten Bereich des Gerätes oder Netzwerks vordringen und sein Werk fortsetzen. Diese Betrachtung ist keine abschließende Liste der unterschiedlichen Malwaretypen, gestattet jedoch einen Einblick in die Vielzahl und Varietät der Materie. Als Zusammenfassung kann festgehalten werden, dass die im Cyberzeitalter signifikant gesteigerten Möglichkeiten mit Malware ökonomische Vorteile zu erzielen, mit einem enormen quantitativen und qualitativen Anstieg an Schadsoftware einhergehen (Moser, Kruegel und Kirda 2007: 231; Lallie et. al. 2020: 3). Diese Entwicklung sollte durch das unternehmerische Risikokontrollsystem berücksichtigt und durch präventive beziehungsweise reaktive Kontrollen gesteuert werden. Diese Kontrollen wollen wir im Folgenden anhand des Bedrohungsbildes entwickeln.

6.4.2. Malware als komplexe Bedrohung

Die häufigste Fehleinschätzung im Zusammenhang mit Malware betrifft die bereits genannte Überschätzung der Abwehrfähigkeiten des Systems, welche durch Firewalls und Virenscanner einen Zustand vermeintlicher Sicherheit suggerieren (Borges et. al. 2011: 152). Eines der bekanntesten Beispiele für die Infiltration einer vermeintlich geschützten Produktionsumgebung durch eine Schadsoftware ist der Stuxnet-Virus.[402] Diese aufwendig

[402] Unter den betroffenen Ländern trat besonders der Iran in den Vordergrund, in welchem gerade das industrielle Analgen kompromittiert wurden, welche im Verdacht standen für das inoffizielle Atomwaffenprogramm im Einsatz zu stehen. Die öffentlich diskutierten Schlussfolgerungen bauten rasch eine Verbindung zwischen den nuklearen Ambitionen des Irans und den US-amerikanischen Absichten auf, eben diese zu unterbinden. „Neben der trotz neuer Hinweise noch sehr spekulativen Interpretation eines gezielten Angriffs auf den Iran weisen die technischen und der taktischen Merkmale vor allem auf eine Nutzung von Stuxnet als Waffentest hin“ (Gaycken und Karger 2011: 4).

programmierte Malware wurde 2010 dokumentiert, als mehrere industrielle Steuerungssysteme aufgrund der Infektion mit dem Virus ausfielen (Gaycken und Karger 2011: 4) und ein Diskurs über den gezielten Gebrauch von Malware in der Sicherheitspolitik entwickelte (vgl. Cavelty 2013: 111).[403] Auch Unternehmen sind gezwungen das Risiko eines Malwareangriffs zu berücksichtigen und geeignete Schutzmaßnahmen zu implementieren. Diese Angriffe können auf die Datenbanken, Strategiepapiere oder Produktionsgeheimnisse abzielen oder schlicht dem Ziel der Beschädigung der virtuellen Infrastruktur folgen. Ein Beispiel könnte ein Angriff mittels eines kompromittierten Http-Client auf das Netzwerk eines Unternehmens sein.[404] Eine handwerklich anspruchsvollere und zeitlich aufwendigere Methode ist die gezielte Attacke auf diesen Client mit Hilfe von „Exploits" oder „Shell-Codes" (Krotofil und Cárdenas 2013: 181).[405] Nach erfolgreicher Vorbereitungsphase und eingeleiteter Infektion, kann der Angreifer eine Malware auf dem Endgerät eines oder mehrerer Mitarbeiter des Unternehmens installieren und durch eine Lücke in der Sicherheitsarchitektur des Client-Systems freien Zugang für weitere Softwaretransfers zu erhalten.

Über einen „Reverse-Shell-Code"[406] kann es dem Angreifer zudem gelingen eine dauerhafte Verbindung zwischen einem externen Server und der Schnittstelle innerhalb des abgeschirmten Systembereichs herzustellen (Borges et. al. 2011: 152). Diese Hintertür kann für einen geheimen Datentransfer genutzt werden, über den neue Befehle eingespielt oder Informationen abgeleitet werden können (Alazab et. al. 2010: 2). Der „Reverse-Shell-Code" kann im befallenen System metastasieren und bei Bedarf die Kontrolle über Komponenten oder Profile, wie beispielsweise einer Administratorenrolle übernehmen. Alternativ könnte auch ein „Keylogger" implementiert werden um die Passworteingabe von Administratoren oder privaten

[403] Ähnliche Meldungen über elektronische Kriegsführung unter Einsatz von Cybertechniken waren in den letzten Jahren frequentierter und detaillierter zu verzeichnen. Insbesondere Russlands Interventionen in anderen Nationen mithilfe einer intensiven Cybertaktik wurden öffentlich diskutiert und noch mehr darüber spekuliert. Die Spionagetätigkeit US-amerikanischer Geheimdienste wurde in Deutschland im Rahmen des „NSA-Skandals" vergleichbar intensiv debattiert.

[404] Ein geeigneter Http-Client ist das anwenderseitige Endgerät, dessen potentiell veraltete Software eine Sicherheitslücke für die Penetration durch das Programm erlaubt. Im Rahmen der Suche nach potentiellen Schwachstellen ist jedoch aus Sicht des Angreifers Vorsicht geboten. Falls sich der Angreifer automatisierter „persistent attacks" bedient, das sind multiple, von einem Programm gesteuerte Versuche eine Sicherheitslücke auszunutzen, erhöht er auch das Risiko entdeckt zu werden (Borges et. al. 2011: 151).

[405] „Shell-Codes" dienen ähnlich wie „Exploits" als Türöffner innerhalb des infiltrierten Systems und etablieren eine Aktionsbasis für den Angreifer innerhalb des geschützten Bereichs hinter den Firewalls (Brand, Valli und Woodward 2011: 4).

[406] Eine „Reverse-Shell" erweitert den geläufigen Shell-Code, welcher eine Kommandozeile in mühevoller Detailarbeit in einen bestehenden Systemcode einbindet, um diesen darüber zu steuern. Der „Reverse-Shell" etabliert eine vom Angreifer programmierte Schnittstelle zu einem dezidierten Server hinter der Firewall des angegriffenen Systems, über welche eine ad-hoc Verbindung von außerhalb aufgenommen werden kann und gleichzeitig die Chancen auf Detektion gering einzuschätzen sind. Jedoch droht die aufwendige Handarbeit mit einem einfachen Update der Systemkonfiguration (bereits ein Bibliotheksversionsupdate reicht dafür aus) obsolet zu werden, da der Shell-Code auf eine spezifische Konfiguration angewiesen ist (vgl. Heise Security 2006).

Nutzern zu speichern (Rahim et. al. 2018: 3) oder das zentrale User Management Systemen mithilfe eines gefälschten digitalen Profils zu kapern und sich dort mithilfe von nun legitimen Einwahldaten Zugang zu weiteren Bereichen des Netzwerks zu verschaffen (Borges et. al. 2011: 152).

Durch diese Attacken können verschiedene schadhafte Aktionen ermöglicht werden, beispielsweise Daten von den Datenbanken herunterladen und auf dem Schwarzmarkt zum Verkauf anbieten. Informationen können auch für eine Erpressung des Unternehmens verwendet werden, beispielsweise durch die Androhung relevante Geschäftspapiere an die Konkurrenz weiterzugeben oder sensible Kundeninformationen zu veröffentlichen (Hong, 2012: 75). Für einen Kenner der Materie könnten auch Compliance-Berichte oder Dokumente zu Rechtsstreitigkeiten auf den internen Datenbanken interessant sein, deren Publikation durch das Unternehmen nur gegen Zahlung abgewendet werden kann. Allerdings setzen alle genannten Beispiele eine hohe Professionalität des Angreifers oder seiner Auftraggeber voraus und benötigen eine intensive Vorbereitung auf das Ziel. Es kann zudem in der Absicht der Angreifer liegen, Systeme zu manipulieren und durch einen Softwarefehler direkte Schäden in den Systemen oder hohe Reparaturkosten an beschädigten Endgeräten zu verursachen, beispielsweise durch Übersteuerung einer Produktionsanlage (Kundur et. al. 2010: 1).

Angriffe auf Sensoren, welche ein relativ einfaches Ziel verglichen mit den Hauptsystemen darstellen, können hohe Kosten durch die Betriebsunterbrechung verursachen. So wäre es auch denkbar, über die Vielzahl an Schnittstellen und der am Betrieb beteiligten Sub-Unternehmen über Umwege Zugriff auf Steuerungselemente oder spezifische Konfigurationen von Sensoren zu erhalten. Insbesondere wenn unterschiedliche Hersteller und Produkttypen zu einem Netz zusammengeschlossen werden, steigen die Chancen auf ungeschützte Einzelkomponenten. (Pauli, Schermann und Krcmar 2010: 259). Die Manipulation von Sensoren oder Steuerungseinheiten könnte standardisierte Sicherheitsprotokolle aktivieren, welche den Betrieb automatisch herunterfahren (Krotofil und Cárdenas 2013: 173). Auch ein koordinierter Angriff auf die Stromversorgung entweder auf Seiten der Stromerzeuger oder der Netzbetreiber könnte durch die - wenn auch nur vorübergehende - Abschaltung der Energieversorgung zu signifikanten Problemen führen, insbesondere im Fall der kritischen Infrastruktur (Braubach 2011: 47). Dieses Beispiel illustriert überdies die Kausalbeziehung zwischen analoger und digitaler Welt, zwischen virtuellen Befehlen und physikalischen Konsequenzen mit hohem Schadenspotential (Cook 2010: 28).

Die maßgeblichen Sicherheitslücken, welche sich Angreifer zu Nutzen manchen können bleiben in ihrer Masse hingegen ebenso simpel wie effizient. Die größten Schwachstellen bilden nicht gepatchte Applikationen und unzureichende Sicherheitsupdates auf den Clients (Mosin, Prajapati und Vohara 2010: 22; Chigada und Madzinga 2021: 5). Deren eigentlich leicht zu behebenden Defizite erlauben Angreifern den Zugriff über ein einzelnes kompromittiertes Element auf das gesamte System (Borges et. al. 2011: 151). Des Weiteren sind ungeschützte Schnittstellen ein Risiko für die Systeme, etwa indem offene USB-Ports oder gekoppelte Endgeräte ohne entsprechend aktualisierte Sicherheitszertifikate Schwachstellen darbieten (Krotofil und Cárdenas 2013: 167). Gleiches gilt für mangelhaft programmierte Applikationen, deren Konfigurationen Angreifern ein leichtes Spiel ermöglicht. Das „Cross Site-Scripting" macht sich diese Lücke zu nutzen und verwendet „schlecht programmierte Serverscripte (…), wobei Informationen aus einem nicht vertrauenswürdigen Kontext in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig gelten" (Borges et. al. 2011: 109). Besonders die Vielzahl und Heterogenität von Plattformen und Endgeräten erhöht die Wahrscheinlichkeit, dass ein nicht-gepatchtes Glied in der Kette von Angreifern ausfindig gemacht wird und einen Angriff über diese Schwachstelle ermöglicht. Dieser Aspekt referenziert direkt auf die Gefahren der Vernetzung und Digitalisierung für die Sicherheitsproduktion in Unternehmen.

Malware besitzt daher das Potential die größte Bedrohung für Unternehmen im vernetzten Informationszeitalter zu sein, insbesondere wenn komplexe Systeme ein weitreichendes Angriffsziel darstellen. Diese Risikodimension bedarf besonderer Beachtung für die unternehmerische Risikokontrolle, insbesondere wenn Entscheidungen wie der Zusammenschluss zu zusammenhängenden Netzwerken zu treffen sind (Walser und Riedl 2010: 258). Eine geeignete Risikokontrolle sollte daher die Einbeziehung von Systemkomponenten in ein Gesamtsystem auf mögliche Schwachstellen ex ante prüfen, sowie eine reguläre Auditierung der Systemdurchlässigkeit vorsehen. (Schermann und Krcmar 2010: 227). Das folgende Beispiel wird sich nun mit der Ransomware beschäftigen und deren potentielle Folgen für die Anschlussoperationen in Unternehmen erläutern.

6.5. Fallbeispiel 3 – Ransomware

Eine besondere Variation der Malware ist die sogenannte Ransomware, eine Methode um Computer und Festplatten durch Codierung zu sperren und für deren Entschlüsselung Lösegeld zu fordern. Der weltweite Schaden durch Lösegeldforderungen mithilfe einer Ransomware summiert sich zwar jährlich nur auf dreistellige Millionenbeträge (Scaife et. al. 2016: 303), doch steigen die Belastungen für Unternehmen. Während der Corona-Pandemie zahlte zum

Beispiel das US-amerikanische Softwareunternehmen Kaseya 70 Millionen US-Dollar Lösegeld, da die Geschäftsunterbrechung das Fünf- bis Zehnfache der Lösegeldzahlung gekostet hätte (Schulze 2021: 2). In Deutschland meldeten zwischen 2019 und 2022 vor allem Krankenhäuser und andere Betriebe aus der Gesundheitsversorge Ransomware-Angriffe, auch weil die IT-Sicherheitsarchitektur in Folge des Spardrucks hinter internationalen Standards auf diesem Gebiet zurückfällt (Dochow 2022: 100). Laut Statistik, befindet sich Ransomware nach Phishing und allgemeiner Malware mit 22,3 Prozent auf dem dritten Platz der häufigsten Methoden[407] der Internetkriminalität (Dreißigacker, von Skarczinski und Wollinger 2020: 946).

Die Erfolgsaussichten dieser Methode sind überaus lukrativ (Pathak 2016: 371). Somit verwundert es nicht, dass seit dem ersten dokumentierten Auftreten von Ransomware-Programmen vor etwa zehn Jahren ein signifikanter Anstieg der jährlichen Fallzahlen um 500 Prozent bis 2015 dokumentiert wurde (Kharraz et. al. 2015: 1) und seit der Corona-Pandemie erneut um 485 Prozent angestiegen ist. Aufsehenerregende Fälle erreichten in jüngster Vergangenheit mehrere Male die Schlagzeilen und zeigten zudem auf, dass es sich um ein globales Problem handelt.[408] Dabei sind die eingesetzten Algorithmen häufig leicht zu erstellen beziehungsweise zu modifizieren, um sie vor einer frühen Erkennung durch Virenschutzprogramme zu verbergen. Der konkrete Einsatz von Ransomware verbindet sozio-technische Elemente wie dem Social Engineering und einer Schadsoftware welche einen Verschlüsselungsalgorithmus auf die Datenbanken des Ziels eskortiert, um dort relevante Informationen durch Codierung unbrauchbar zu machen (Sittig und Singh 2016: 625). Wir wollen uns im Folgenden ansehen, aus welchen Elementen ein Ransomware-Angriff besteht und welche Risiken dieser für Unternehmen bedeuten kann.[409]

6.5.1. Analyse einer modernen Lösegelderpressung

Ransomware ist ein globales Phänomen, dessen Opfer sowohl private Nutzer, öffentliche Institutionen, Unternehmen, NGOs oder Organe der kritischen Infrastruktur sein können (Bhardwaj et. al. 2016: 2). Die frühen Ursprünge der Idee eines Krypto-Virus reichen in das

[407] Entgegen der kulturellen Darstellung von individuellen Hackern, fällt „manuelles Hacking“ mit nur 3 Prozent bedeutend hinter den anderen, industrialisierten Angriffsmethoden zurück (Dreißigacker, von Skarczinski und Wollinger 2020: 946).

[408] Der zuvor bereits erwähnte Trojaner „WannaCry“ sowie die Ransomware „GoldenEye“ entwickelten ein beachtliches Schadpotential und bedrohten insbesondere die kritische Infrastruktur verschiedener Staaten. Diese Fälle offenbaren allerdings auch den volatilen Charakter der modernen Gesellschaft im digitalen Zeitalter, in dem die Gewöhnung an die Verfügbarkeit von Waren, Services und Leistungen zunehmend von der Performanz des digitalen Netzes abhängt.

[409] Man denke an den Angriff auf die Datenbanken des Bundestages oder die Ransomware-Attacke „WannaCry“ auf das britische Gesundheitssystem, welche in beiden Fällen auf veraltete Sicherheitsprotokolle und unzureichender Schutzvorkehrung der staatlichen Betreiber zurückzuführen waren (vgl. Handelsblatt 2019).

Jahr 1989 zurück und sind mit seinem Erfinder Joseph Popp verbunden. Der erste „PC Cyborg Trojaner“ trug den Namen „AIDS“ und führte erstmals das Prinzip einer Kodierung fremder Informationen mit Hilfe einer Schadsoftware öffentlich zur Schau (Salvi und Kerkar 2015: 1). Der Virus wurde auf einer Diskette auf dem Postweg versendet und führte sein Programm nach dem Einführen des Datenspeichers in ein Lesegerät aus (Sittig und Singh 2016: 625). Einige Jahre später wurde die Idee um ein zusätzliches Element erweitert, indem ein öffentlicher Schlüssel verwendet wurde, um die Informationen zu verschlüsseln. Diesen Prozess konnte man nur durch einen geheimen oder privaten Schlüssel reversibel machen und eben dieses Element ermöglichte die effiziente finanzielle Nutzung der Software für erpresserische Absichten (Scaife et. al. 2016: 303).

Allgemein gesprochen ist das Ziel eines Angriffs mittels Ransomware eine Verschlüsselung von Daten auf fremden Laufwerken, die dadurch dem Zugriff durch den Nutzer entzogen werden. Das Besondere an dem Virus ist, dass die Datenverfügbarkeit nur wieder herzustellen ist, indem der spezielle Schlüssel eingegeben wird, um die Codierung rückgängig machen zu können (Pathak 2016: 371). Eben diesen Schlüssel, das bedeutet einen Freigabecode, bietet der Erpresser gegen Zahlung einer Lösegeldsumme an (Scaife et. al. 2016: 303). Um das Opfer unter Druck zu setzen wird zudem die Drohung in den Raum gestellt, die durch die Ransomware kompromittierten Daten entweder zu veröffentlichen (Schulze 2021: 3) oder innerhalb einer kurzen Frist unwiederbringlich zu löschen, falls kein Lösegeld gezahlt werden sollte.

Ransomware funktioniert im Prinzip wie andere Malware, indem sie nach einer Schwachstelle auf fremden Systemen sucht.[410] Die Einspielung der Schadsoftware kann den üblichen Wegen wie einer Verteilung über Emailanhänge, Links auf infizierte Webseiten oder dem mehr oder weniger zufälligen „drive-by“ Infektionen folgen (Bhardwaj et. al. 2016: 2). Die Ransomware kann sich auch einer weiteren Software bedienen, deren einziger Zweck die geheime Einschleusung in ein Netzwerk ist. Ein solches Programm kann eine „Rogueware“ sein, die sich beispielsweise als kostenloser Virenscanner präsentiert. Folgt ein Nutzer der Verlockung eine notwendige Software zum Virenschutz ohne Bezahlung zu erhalten, erlangt anstelle des

[410] Ein Exkurs soll zwei weitere Methoden der Nutzung von Ransomware verdeutlichen: Ein (1) „Ransomware Locker“ zum Beispiel sperrt nur die haptischen Schnittstellen und erlaubt dem Nutzer beispielsweise nur noch eine ausgewählte Webseite zu besuchen, auf der die geforderte Lösegeldforderung eingegeben werden kann (Bhardwaj et. al. 2016: 2), während die eigentlichen Daten auf der Festplatte selbst von dem Erpressungsversuch unberührt bleiben. Auch wer sich in diesem Fall für eine Zahlung über die gewählte Webseite entscheidet, muss allerdings damit rechnen, dass die Einwahldaten (Kontonummer und PIN) ebenfalls protokolliert werden und sich der Angreifer danach am Konto des Opfers bereichern kann. Ein weiterer Typ, der als (2) „Scareware“ bekannt ist, lässt eine Warnbenachrichtigung aufblitzen, die vor einer angeblichen Bedrohung warnt und gegen Bezahlung Hilfe durch die Installation einer Software anbietet, welche jedoch häufig selbst ein Trojaner zur Installation einer Ransomware ist (Borges et. al. 2011: 104).

erwarteten Programms eine Applikation Zugriff auf das Endgerät, welche die Datenbank in Ruhe nach wertvollen Informationen durchsuchen kann (Borges et. al. 2011: 68). Durch die weitreichenden Rechte eines (vermeintlichen) Virenschutzprogrammes erlaubt der Nutzer der „Rogueware“ zudem weitere Schadsoftware ohne dessen Kenntnis aus dem Internet zu beziehen und den Angriff vorzubereiten.

Ähnlich zu einem biologischen Virus versucht die Ransomware eine unauffällige Position im Programmcode zu finden, von wo aus sie möglichst unbehelligt die Verschlüsselung der Daten einleiten kann (Bhardwaj et. al. 2016: 2). An dieser Stelle kommt im Fall von komplexen Angriffen auch der sozi-technische Aspekt zum Tragen, mit dessen Hilfe sich Informationen zum Verhaltensmuster der Ransomware ex ante im Sinne seines Erschaffers an die Struktur seines Ziels implementieren lassen, um der Suche nach geeigneten Primärzielen ausreichend Raum und Zeit zu sichern (Pathak 2016: 372). Denn der Krypto-Virus kann nicht davon ausgehen, alle Daten eines Netzwerks unentdeckt für die Verschlüsselung vorzubereiten. Daher ist die Suche nach wertvollen Daten und vitalen Programmschnittstellen von übergeordneter Bedeutung. Werden beispielsweise in einem Unternehmen durch Ransomware nur die Kantinenpläne oder das Parkhausmanagementsystem verschlüsselt, besteht kaum Leidensdruck für das Unternehmen auf die Forderungen einzugehen. Transaktionslisten und Kundendaten sind hingegen wertvoller, Patientenakten und Steuerungssysteme für Operationssäle darüber hinaus unverzichtbar.

Nach erfolgreicher Identifikation der Primärobjekte wird die Erstellung eines privaten Schlüssels vorbereitet, mit dessen Hilfe die Informationen auf den ausgewählten Datenbanken codiert werden sollen (Kharraz et. al. 2015: 17). Neuere Versionen entwickelten für diesen Zweck leistungsfähige Verschlüsselungstechniken, die es für das Opfer unmöglich gestalten sollen die kompromittierten Daten innerhalb der Zahlungsfrist selbstständig entschlüsseln zu können. In dem Moment in dem der Verschlüsselungsprozess beginnt, engen sich die Optionen für den erpressten Nutzer signifikant ein. Die Ransomware gestattet dem Nutzer nur einen rudimentäreren Informationszugriff, durch welchen die Lösegeldforderung nebst der Zahlungsmodalitäten bekannt gegeben wird.[411] Für Unternehmen kann eine Ransomware-Attacke einen weitrechenden Ausfall der Geschäftsprozesse bedeuten, da Datenbanken nicht mehr verfügbar sind oder Steuerungssoftware für automatisierte Produktionsprozesse

[411] Des Weiteren kann eine Ankündigung im Falle der Nichtzahlung die befallenen Daten endgültig zu löschen oder alternativ alle 10 Minuten eine arbiträr ausgewählte Datei zu entfernen auf die Zahlbereitschaft des Opfers einwirken. Für Privatpersonen können wichtige Dokumente wie Arbeitsunterlagen oder persönliche Unikate wie Familienfotos und private Emails in Gefahr stehen verloren zu gehen.

ausgefallen ist.[412] In den meisten Fällen versprechen ein Neustart im abgesicherten Windowsmodus oder andere Initiativen zur Zurücksetzung der Plattformen keine Lösung des Problems (Borges et. al. 2011: 107).

Die favorisierte Bezahlungsmethode für das Lösegeld sind Bitcoins oder andere Kryptowährungen, da für die Einlösung der Kryptowährungen[413] kein registriertes Bankkonto notwendig ist (Bornholdt und Sneppen 2014: 2). Dadurch bedient sich das Geschäft mit Ransomware in zweierlei Hinsicht der neuen Technologien des digitalen Zeitalters, zum einem durch die technischen Möglichkeiten eines Krypto-Virus und dem rasant steigenden Wert von Informationen für seine Nutzer. Zum anderen profitiert es von der Anonymität einer digitalen Währung, um sich der Strafverfolgung zu entziehen (Kharraz et. al. 2015: 14). Das Dilemma für das Opfer ist, dass es nicht wissen kann, ob der oder die Erpresser den privaten Schlüssel zur Decodierung der Daten tatsächlich nach Zahlung des Lösegelds aushändigen werden. Insbesondere für ein institutionelles und finanzkräftiges Opfer wie ein Unternehmen könnte die einmalige Zahlungseinwilligung seitens des Opfers zu weiteren Forderungen führen.[414] Darüber hinaus kann der Angreifer auch drohen, sensible Daten zu veröffentlichen, deren Publikation einen signifikanten Reputationsschaden bedeuten könnte. In diesem Fall wäre neben der Verfügbarkeit auch die Vertraulichkeit beziehungsweise Integrität der Unternehmensdaten betroffen. In diesem Fall spricht man auch von einer „double extortion“ (Schulze 2021: 3).

[412] Das Beispiel eines britischen Anbieters für Online-Sportwetten aus dem Jahr 2004 zeigte, wie effektiv eine Verschlüsselung der internen Datenbanken das Unternehmen von seinem Geschäftsbetrieb abtrennen konnte. In diesem Fall waren alle Schnittstellen zu Wettannahmen und Quoten verschlüsselt und dadurch unbrauchbar gemacht wurden, wodurch sich unmittelbare und geschäftsgefährdende Auswirkungen auf die Wertschöpfungskette des Unternehmens ergaben (Walter 2008: 21).

[413] Kryptowährungen wie Bitcoin basieren auf einem Netzwerk von dezentralen Rechenleitungen, dessen Wert vom Vertrauen der Nutzer zur Verschlüsselungstechnologie hergestellt wird. Auch andere Bezahlmethoden wie „Ukash“ können für diese Zwecke genutzt werden, indem der online ausgestellte Wertcoupon über verschlüsselte Kommunikation oder anonyme Foren gegen harte Währungen eintauschen (Kharraz et. al. 2015: 14).

[414] Ein offener Brief von IT-Sicherheitsexperten an die Bundesregierung erweckte 2022 Aufmerksamkeit, da in diesem Ransomware als „geostrategisches Risiko“ bezeichnet wurde und – allerdings nicht unwidersprochen - gefordert wurde, die Versicherung von Lösegeldzahlungen zu unterbinden, um diese grassierende Methode weniger lukrativ zu machen (Ransomwareletter 2022).

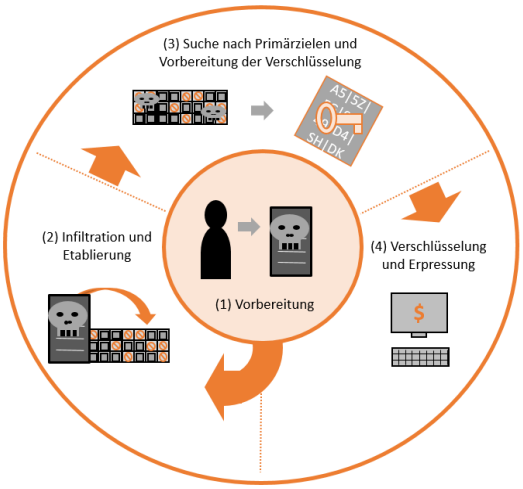

Abb. 6.5. Verlauf eines Angriffs mit Ransomware. Eigene Darstellung.

Die Entwicklungskosten einer Ransomware fallen relativ niedrig aus.[415] Die eingesetzte Software bedient sich entsprechend simpler Methoden zur Codierung von Informationen oder Funktionalitäten.[416] Wie zuvor angedeutet, sind größere Unternehmen trotz ihrer höheren Schutzstandards ebenso attraktive Ziele (Salvi und Kerkar 2015: 4), da diese einerseits über potentiell höhere finanzielle Reserven verfügen und andererseits als ausgewählte Ziele von professionellen Anbietern von Schadsoftware („Ransomware as a Servie" – RaaS) gegen Bezahlung auf Wunsch eines Auftraggebers ausgewählt werden können (Bhardwaj et. al. 2016: 3). Allerdings sind die Kosten der IT-Sicherheit in Unternehmen um ein vielfaches höher als zur Entwicklung einer Ransomware. Der durchschnittliche Wert eines Ransomware-Programms liegt zwischen wenigen hundert und eintausend Euro, während eine solide IT-Sicherheitsarchitektur zur Identifizierung und Abwehr von Ransomware im Mittel 0,5 Prozent des Jahresumsatzes[417] von Unternehmen kostet (Schulze 2021: 3). Daher wollen wir uns im Folgenden präventive und reaktive Optionen ansehen, welche Unternehmen im Fall eines Ransomware-Angriffs zur Verfügung stehen.

---

[415] Etwa die Hälfte der bekannten Ransomware-Familien stellte Forderungen zwischen 150 und 250 US-Dollar (Kharraz et. al. 2015: 14), der überwiegende Rest zwischen 300 und 500 US-Dollar (Salvi und Kerkar 2015: 1) und nur ein kleiner Anteil mehr als 1.000 US-Dollar in Bitcoins. Dieser Wert unterscheidet sich auch nach der Art der Software.

[416] Eine Variante konzentriert sich auf individuelle Kleinziele, wie etwa Computerspieler. Durch Zugriff auf die Einwahldaten zu einem Onlinespiel beispielsweise können sich die Angreifer des virtuellen Spielgeldes oder anderer Wertgegenstände des Avatars bemächtigen und dem Spieler einen Austausch gegen reale Währung anbieten (Hong 2012: 75). Außenstehende würden auf die Zahlung für den digitalen Inhalt verzichten, aber ein Spieler der viele dutzend bis hundert Stunden mit dem Spiel verbracht hat, kann anders denken. Ebenso können die entwendeten Spielschätze anderen Spieler angeboten werden, die sich brennend für die angebotenen Spielinhalte interessieren können (Choo, Smith und McCusker 2007: 4). Es sind auch Fälle bekannt in denen eine von außen platzierte Dauerwerbung den Spielspaß derart einschränkte, dass Spieler freiwillig eine kleinere Summe zu zahlen bereit waren (Borges et. al. 2011: 108).

[417] Gemessen am Jahresumsatz von beispielsweise Google würde dies 1,3 Milliarden US-Dollar an Gegenwert für defensive Maßnahmen bedeuten (Statista 2022b).

6.5.2. Strategische und praktische Krisenvorsorge

Aufgrund der schwindenden Handlungsoptionen mit fortschreitender Verschlüsselung von Daten und Systemen ist es elementar, einen möglichen Angriff frühestmöglich zu erkennen und entschieden gegen diesen vorzugehen. Der Grund dafür liegt in der technologischen Ausgereiftheit der Ransomware, welche reaktive Maßnahmen des Ziels nach erfolgreicher Infiltration auf Schadensbegrenzung limitiert. Folglich sind proaktive Planungen in Unternehmen essentiell, um das Risiko angemessen zu steuern. Zu diesen zählen (1) infrastrukturelle Maßnahmen, (2) Investitionen in die Fähigkeiten zur Schadsoftwareerkennung und (3) eingeübte Reaktionsmechanismen auf verdächtige Aktivitäten im organisationsinternen Netzwerk. Anhand dieser Schritte kann das eigentliche Krisenmanagement, welches nach Bekanntwerden des Angriffs seine Aktivitäten aufnimmt, auf eine geordnete Vorsorgeplanung zurückgreifen und die Chancen zur Schadensminimierung deutlich erhöhen.

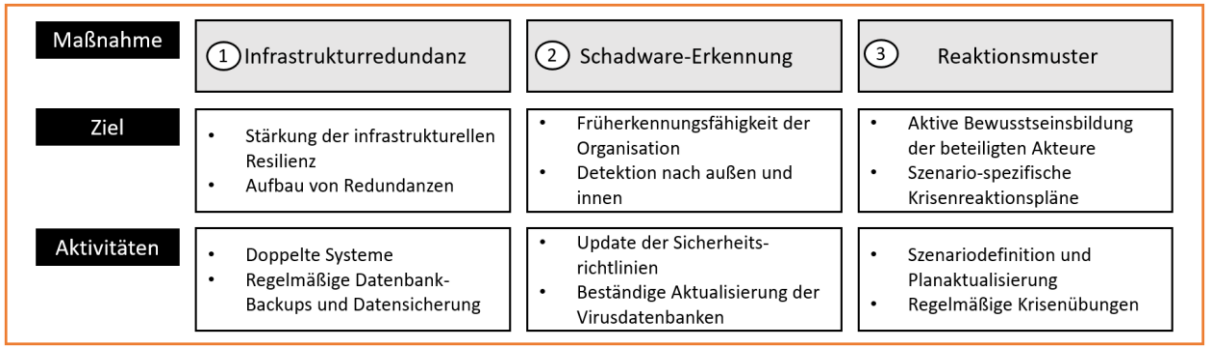

Abb. 6.6. Maßnahmen zum proaktiven Schutz vor Ransomware-Angriffen. Eigene Darstellung.

Die aus finanziellen Gesichtspunkten aufwendigsten Maßnahmen sind die (1) infrastrukturellen Redundanzen. Das Ziel dieses grundlegenden Schrittes ist die Aufstellung der unternehmensinternen IT-Infrastruktur, das heißt Server, Datenbanken, Betriebssysteme und Kernanwendungen nach dem Prinzip einer redundanten Struktur oder in anderen Worten die Schaffung einer parallelen technischen Infrastruktur (Krotofil und Cárdenas 2013: 168). Diese doppelte Hardwareausführung soll es einem Unternehmen ermöglichen den Verlust der primären Infrastruktur zu kompensieren. Eine gesamtheitliche Strategie muss demnach auch die Inhalte der Datenbanken sowie ihrer Anwendungen berücksichtigen. Damit sind vorrangig Datenbackups und Standards zur Datensicherung gemeint, deren Informationen zum einem auf unterschiedlichen virtuellen Systemen gespeichert und zum anderem auf physikalisch getrennten Hardwarekomponenten vorgehalten werden (Sittig und Singh 2016: 626). Diese Techniken werden wir im vierten Fallbeispiel anschließend genauer betrachten. An dieser Stelle sei darauf verwiesen, dass die infrastrukturelle Redundanz hohe Investitionen voraussetzt (Riekmann und Kraus 2015: 296), schließlich gehören Rechenzentren und deren Ausstattung

zu den größten Kostentreibern der digitalen Wirtschaftswelt, dicht gefolgt von ihren Betriebsausgaben bestehend aus Energie-, Wartungs-, Anpassungs- und Personalkosten (Cerullo und Cerullo 2004: 75).

Eine Alternative zum physikalischen Trennungsansatz ist die Speicherung von Informationen auf zwei getrennten, unterschiedlichen Systemen beziehungsweise Anwendungen. Wie die Ransomware „WannaCry“ offenbarte, ermöglichten Sicherheitslücken im Windows XP Betriebsprogramm dem Virus die Infiltration von vitalen Systemen (AGCS 2018: 3). Eine duale Systemkonfiguration hingegen würde die Informationen, zum Beispiel die Kundendaten oder die Personaldatenbank auf einer Windows-Oberfläche speichern, aber zusätzlich dazu in kompatiblen Anwendungen auf einem Linux-Betriebssystem Duplikate der Daten verwalten. Dadurch wäre das Unternehmen in der Lage, trotz eines erfolgreichen Angriffs auf die Primärsysteme mithilfe der dualen Konfiguration auf die aktuellen Daten des Sekundärsystems zurückzugreifen und kritische Geschäftsprozesse fortzuführen (Gaycken und Karger 2011: 6). Der bedeutende Nachteil dieser doppelten Systemführung liegt in den Anschaffungs- und Lizenzkosten für zwei getrennte Betriebsprogramme, sowie in den Wartungskosten für deren Betrieb und die Aufrechterhaltung ihrer Kompatibilität im Gesamtkontext der organisationsinternen Systemadministration beheimatet.[418] Ferner bedeutet diese Methode einen Mehraufwand für die Belegschaft, welche die Dateneingabe auf zwei Systemen beherrschen und zudem auch im alltäglichen Gebrauch anwenden oder zumindest Datenimporte vom primären in das sekundäre System durchführen muss (Hammermann und Klös 2016: 9).

Eine weitere Idee der infrastrukturellen Absicherung der Systeme ist die Trennung, das heißt Entnetzung von kritischen Anwendungen und Datenbanken vom Gesamtnetz des Unternehmens. Diese Trennung könnte die elementaren Informationsbestände des Unternehmens vor einem Zugriff der Ransomware bewahren und ähnlich eines Wasserschotts auf einem Schiff einzelne Sektoren vor dem Ausbreiten des Krypto-Virus bewahren (Ministr, Ńtevko und Fiala 2009: 138). Eine derartige Aufteilung des Netzwerkes oder zumindest die Trennung zwischen Kernbereichen und Drittsystemen wie dem Internet werden ebenfalls mit Blick auf die kritische Infrastruktur gefordert[419], um die notwendige Versorgung der

[418] Die Datenwiederherstellung inkludiert verschiedene Typen wie die “Local Replication and Remote Replication” welche ein Datenbackup entweder in der näheren Umgebung oder einem entfernten Ersatzrechenzentrum vorhalten. Das Wiedereinspielen von Daten kann über DBMS, Applikationen, beziehungsweise Host- oder Storage-basierte Versionen erfolgen (Carvalho e Silva et. al. 2012: 147).

[419] Problematisch wird diese Forderung im Bereich der privatisierten kritischen Infrastruktur aufgenommen, da das Credo der vernetzten Organisation und „Internet of Things“ eine durchgängige Anbindung aller

Bevölkerung aufrechterhalten zu können (Gaycken und Karger 2011: 8). Wie in anderen Beispielen zuvor, wird eine Entscheidung eines Unternehmens von ihrer Risikoexposition abhängig sein, welche zwischen dem möglichen Schaden, der Wahrscheinlichkeit seines Eintretens und den Investitionen in Schutzvorkehrungen diametral gegenüber gesetzten konkreten Gewinnerwartungen abzuwägen hat. Dazu wird ebenfalls eine Reflektion des Informations- und Sicherheitsbegriff im digitalen Zeitalter mit den einhergehenden elementaren Bedrohungen der Geschäftsfortführungen notwendig sein.

Die zweite Ebene des proaktiven Schutzes gegen Ransomware-Angriffe ist die (2) Früherkennungsfähigkeit des Unternehmers, was maßgeblich im Zusammenhang mit Virusscannern und Sicherheitsprotokollen zu sehen ist. Man kann diese Ebene in drei Kategorien einteilen, namentlich erstens in die (2.1) Arbeit von Virusscannern und Firewall-Konfigurationen, zweitens die (2.2) Sensibilisierung von Nutzern und drittens in die Durchführung einer Bestandsaufnahme der (2.3) akuten Bedrohungslage. Beginnend mit der ersten Kategorie, ist von den Fähigkeiten des Unternehmens zu sprechen (2.1) fremde Programme und Malware frühzeitig zu erkennen. Diese originäre Aufgabe eines Virendetektors ist die Erkennung verdächtiger Aktivitäten oder Quellcodes, verbunden mit den notwendigen Rechten diese Aktivitäten vom Rest des Systems zu isolieren und gegebenenfalls zu löschen (Borges et. al. 2011: 67). Eine gängige Methode derer sich Antivirusprogramme bedienen, ist ein Abgleich der Codesignatur einer verdächtigen Anwendung mit einer Datenbank registrierter Signaturen und Codecharakteristika (Scaife et. al. 2016: 304). Die Schwäche des Scanners liegt naturgemäß in der Aktualität der Datenbank und ihres Fundus aus der Vergangenheit bekannter Virenexemplare. Gelingt es einem Angreifer etwa die Schadsoftware im ausreichenden Maße zu modifizieren, kann diese die direkte Detektion durch den Scanner vermeiden, da nur die bekannten Variationen spezifischer Malware-Familien auf der schwarzen Liste des Antivirusprogramms stehen (Moser, Kruegel und Kirda 2007: 231).

Dieser Sicherheitslücke können statische Datenanalysen entgegenwirken, indem verdächtige Systemaktivitäten umgehend einem Administrator gemeldet werden, welcher eine manuelle Untersuchung des betreffenden Programms vornimmt, unterstützt von automatisierten Auswertungen der Dateinamen, eingebundenen Ressourcen und Inhalte sowie weiterer Programmelemente (Bhardwaj et. al. 2016: 3). Malwareprogrammierer haben dieses Problem erkannt und reagierten ihrerseits indem sie versuchen die Virenschutzeinstellungen der

Einzelkomponenten fordert. Des Weiteren sind gerade die kritischen Anwendungen und Prozesse notwendigerweise im ständigen Betrieb, was ihre Abkoppelung und Entsetzung aus der Perspektive einer globalen, virtualisierten Unternehmensstruktur unattraktiv macht.

Organisation durch beständiges Austesten auf Schwachstellen abzuprüfen.[420] Dynamische Analysetools können auf diese Lücke reagieren und beispielsweise verdächtige Dateien auf spezifische Fingerabdrücke oder Verhaltensmuster scannen und Signaturen besser mit der Datenbank auf Ähnlichkeit zu bekannten Malwarefamilien abgleichen (Bhardwaj et. al. 2016: 3). Zudem können die Sicherheitseinstellungen vorsehen, eine Datei im Graubereich zunächst auf eine geschützte Umgebung zu laden und deren Verhalten zu überwachen. Dieser Sandkastenmodus verzögert zwar die fließende Kommunikation, bietet aber durch seine Quarantänefunktion einen besseren Schutz vor (noch) unbekannten Bedrohungen.[421]

Neben diesen Maßnahmen, sind auch Anordnungen an die Hardwarekompatibilität erwähnenswert, da sich ein großer Anteil der Ransomware-Angriffe auf mobile Endgeräte fokussiert. Mobilgeräte erweitern das Unternehmensnetzwerk um eine Vielzahl von Einzelkomponenten, deren Sicherheitsstandards häufig einfacher zu überwinden sind als die Systemkomponenten auf den Servern des Unternehmens (Salvi und Kerkar 2015: 4).[422] Zudem besteht eine beständige, häufig kabelfreie Verbindung zum Rechenzentrum, welche Zugriff auf vitale Informationen und Datenbanken gestattet (Borges et. al. 2011: 151). Auch können die Sendefunktionen von Datenschnittstellen auf Smartphones oder Tablets von Angreifern ausgenutzt werden (Pathak 2016: 373). Der präventive Schutz gegen diese Variation erfordert die mobilen Endgeräte regelmäßig mit Patches auf den aktuellen Stand zu bringen, durch Einstellungen den Zugang zu unautorisierten Applikationen wie Online-Spielen zu untersagen und vor allem die Nutzer mobiler Endgeräte zu schulen (McGuire 2015: 47).

Diese zweite Kategorie hebt die Bedeutung der (2.2) Sensibilisierung von Nutzern hervor, welche sich der Bedrohungen bewusst sein müssen, um von den Vorteilen einer rigiden

[420] Wenn beispielsweise ein Prozess den Austausch von Dateien unterschiedlichen Formats mit Kunden voraussetzt, wie im Online-Vertrieb oder Kundencenter einer Versicherung, garantiert dies einen regen Austausch an Daten, in dessen Masse und Variabilität an Dokumententypen sich das Programm zu verstecken versucht. In diesem Kontext bietet zudem die auf Effizienz ausgerichteten Betriebsmodelle von Unternehmen eine gute Chance für eine unentdeckte Infiltration. Denn wenn die Malware-Erkennungsvorgaben zu strikt sind, können einige der von Kunden eingesendete Dateien nicht geöffnet werden, mit Konsequenzen für die operativen Performanzkennzahlen, beispielsweise wie oft der Kunde aufgrund fehlender Dokumente erneut kontaktiert werden musste. In Folge muss die Signaturerkennung des Virenscanners spezifiziert und der Graubereich eingehender Dateien im Zweifelsfall als vertrauenswürdig einstuft werden. Diese Maßnahmen aus dem operativen Betrieb erhöhen die Chancen für leicht überarbeitete Malwareexemplare unerkannt Zugang zum System zu finden (Scaife et. al. 2016: 304).

[421] Für diese Zwecke können auch kommerzielle Cloud-Dienste in Anspruch genommen werden (IaaS), auf denen die betreffenden verdächtigen Dateien installiert und beobachtet werden können, ohne eine direkte Interaktion mit den eigenen Netzwerken einrichten zu müssen (Bhardwaj et. al. 2016: 3).

[422] Spezialisierte Ransomware-Anwendungen wie „Android.Lockdroid.E“ imitieren den Sperrbildschirm eines Android-Tablets und behaupten, dass dieses Gerät von der lokalen Polizei wegen Besuchs verbotener Webseiten gesperrt sei, häufig in Referenz auf Erwachsenenunterhaltung. Gegen Zahlung einer Gebühr könne diese Sperrung rückgängig gemacht werden, welche in manchen Fällen nur vorgetäuscht ist, in anderen hingegen tatsächlich den Zugang zur Bedienoberfläche kontrolliert (Salvi und Kerkar 2015: 4).

Befolgung der Verhaltensrichtlinien überzeugt werden zu können (Weber 2016: 28). Zu den Richtlinien sollte stets die Aufforderung gehören, verdächtige Aktivitäten umgehend zu melden und „Phishing"-Versuche ebenso wie auffällige Anfragen nicht zu beantworten, sondern die Absender für eine Organisationsweite Sperrliste zu empfehlen. Nutzer sollten zudem nie Dateien herunterladen, Anhänge von unbekannten Sendern öffnen oder gar ihr Passwort an vermeintliche Administratoren weitergeben (Sittig und Singh 2016: 627). Auch wenn diese Sicherheitsvorkehrungen umgangen werden können, wie wir zuvor beispielsweise anhand der Methoden des Identitätsdiebstahls oder Social Engineering zeigten, tragen sie dennoch wesentlich dazu bei Bedrohungen frühzeitig zu erkennen und zu verhindern.

Daraus folgt, dass die Sensibilisierung der Nutzer einer (2.3) angemessenen Bedrohungsanalyse des Unternehmens folgen muss. In regelmäßigen Abständen sollte diese Evaluation durchgeführt werden, um sowohl die kritischen Komponenten der Hardwarekonfiguration, als auch die vitalen Informationen und die diese beheimatenden Datenbanken zu dokumentieren, welche für einen Angriff interessant sein könnten (Pauli, Schermann und Krcmar 2010: 260). Diese Analyse muss die wesentlichen von den unwesentlichen Daten trennen und die Angriffsrichtung eines Angriffes antizipieren, indem kritische Datenbanken oder Netzwerksektoren einer gesonderten Beobachtung oder erweiterten Zugangsbeschränkung unterworfen werden. Dennoch zeigt sich, dass Unternehmen selbst nach einem erfolgreichen Angriff auf wesentliche Sicherheitslücken nur unzureichend reagieren (Linkov et. al. 2013: 472). Eine Analyse der Folgen der „JBoss" Schadsoftware offenbarte, dass 2,1 Millionen Systeme trotz erfolgter Infektion nicht ausreichend aktualisiert wurden, um einen erneuten Angriff mit dem gleichen Virus abwehren zu können (Sittig und Singh 2016: 626). Daher zeigt sich die Relevanz von Bedrohungsanalysen, welche sowohl die Sicherheitslücken offenlegen, als auch die Kosten eines Angriffs, wie beispielsweise der Geschäftsunterbrechung oder des Reputationsschaden mit den initialen Aufwänden für Anpassungen der Hardware oder Anwendungsschutz in Kontext setzen (Riekmann und Kraus 2015: 296).

Dies führt uns zum letzten Punkt der präventiven Planung eines Unternehmens, um sich auf diese Bedrohung vorzubereiten. Im Vorfeld definierte und standardisierte (3) Reaktionsmuster können wesentlich zur Behebung des Schadens und der schnellen Rückkehr zu einem Normalzustand beitragen. Gleichwohl wenn diese Maßnahmen erst nach dem Eintreten einer Krise zum Tragen kommen, ist die Hauptlast der Plan- und Ablauforganisation zuvor aufzubringen. (Scaife et. al. 2016: 303). Diese Maßnahmen umfassen die Definition der Schutzziele, beispielsweise der vitalen Datenbanken oder der für kritischen Geschäftsprozesse

benötigten Informationen und Anwendungen, dem Erstellen von Krisenplänen, welche konkrete Schritte des Krisenmanagements einschließen und letztlich von Entscheidungshilfen durch ex ante beschlossenen Strategien zur Reaktion auf eine dynamische Situation (Bhardwaj et. al. 2016: 3). Allen Elementen gemeinsam ist, dass sie in ruhigen Zeiten, sprich vor der Krise, eine geeignete Reaktion auf eine noch unbekannte Situation unter Annahme wahrscheinlicher Rahmenbedingungen antizipieren, um deren Umsetzung im Krisenfall zeitnah und ohne Klärungsbedarf von Sachverhalten, Hierarchien oder juristischer und technischer Restriktionen zu erlauben (Walter 2008: 8f.).

Ein wichtiges Element der reaktiven Krisenbewältigung ist zunächst das „Incident Monitoring" in welchem die Entwicklung einer Situation beständig verfolgt wird, um weitere Schritte vorwegzunehmen oder zumindest unmittelbar nach deren Detektion identifizieren zu können. Die Ergebnisse der Bedrohungsanalyse, Identifikation von Schutzzielen sowie die Dokumentation vergangener Krisen können die Antizipation des Verlaufs positiv unterstützen (Sittig und Singh 2016: 628). Im akuten Krisenfall sind diese Erkenntnisse wertvoll, um mit Blick auf die eng bemessenen Handlungsfreiräume und begrenzter Überlegungszeit, Entscheidungen auf der Grundlage von im Vorfeld erstellten Optionen und zu erwartenden Konsequenzen schnell treffen zu können. Auf Grund der Tragweite eines sich abzeichnenden Ransomware-Angriffs, denn im schlimmsten Fall droht die Handlungsunfähigkeit des Unternehmens, sind Schlüsselpositionen und Entscheidungsträger umgehend zu informieren und bereits in die Planvorbereitungen einzubeziehen.[423] Das zuständige Entscheidungsgremium sollte aus mindestens ein Mitglied der Geschäftsleitung oder ein von dieser benannter Handlungsbevollmächtigter, sowie Vertreter der Betriebsorganisation, der IT-Sicherheit, der Resilienz- und der Rechtsabteilung bestehen. Zusätzlich sind Experten aus dem IT-System- und Administrationsumfeld ferner beratend zur Verfügung stehen, um die fachliche Expertise und Umsetzung der Entscheidungen unmittelbar mit dem Krisenstab abstimmen zu können.

Anschließend können aktive Gegenmaßnahmen ergriffen werden, worunter die intensive Untersuchung des Systems mit der Codesignatur des identifizierten Virus sowie Aktivierung von Geschäftsfortführungsplänen zur Kompensation von nicht verfügbaren Systemen zu verstehen ist. Die folgende Umschaltung auf die Datenbanken der Backupsysteme sollte erst nach sorgsamer Überprüfung des Bedrohungspotentials geschehen, da eine versteckte und unter Umständen inaktiv gebliebene Variante der Schadsoftware eben diesen Schritt zu antizipieren

[423] Ein sogenanntes „Gold Image", kann als Spiegelung der IT-Datenbankbestände eines Unternehmens die Option zur Verfügung stellen, per Knopfdruck auf den Informationsstand vor Beginn der Krise zu zurückzugreifen (Sittig und Singh 2016: 626).

versucht. Daher ist die Aktivierung eines isolierten Teils der Backupdateien als Sandkastentest zu verstehen, dessen positive Abwicklung den Weg für die restlichen Bereiche ebnen sollte (Borges et. al. 2011: 68). Ferner sind Maßnahmen zu ergreifen, um eine mögliche Kompromittierung von sensiblen Daten wie etwa der Buchhaltung oder Bankanweisungen auszuschließen und das Reputationsrisiko durch Kommunikationspläne zu berücksichtigen. Zusammenfassend kann festgehalten werden, dass die Erfolgsaussichten der Risikokontrolle mit Blick auf eine Ransomware-Attacke auf beachtliche Weise von den Vorbereitungen in allen drei Bereichen, namentlich den (1) infrastrukturellen Grundlagen, (2) aktualisierten Virenscannern und effektiven Sicherheitsprotokollen sowie einer (3) profunden Bedrohungsanalyse und Vorsorgeplanung abhängen.[424]

6.6. Fallbeispiel 4 – ITSCM zwischen Anspruch und Wirklichkeit

Das vierte Fallbeispiel thematisiert die Folgen eines Ausfalls der IT-Applikationen und Datenbanken. Unter dem Begriff „IT Service Continuity Management“ (ITSCM) wird die Anwendungspraktik zur Risikokontrolle der Verfügbarkeit von kritischen Anwendungen, Infrastruktur und Daten umschrieben. ITSCM schließt an die originären Aufgaben des IT Desaster Managements (ITDRM) (Ministr, Ńtevko und Fiala 2009: 131) an, welches wir bereits im fünften Kapitel angesprochen haben. Sein Alleinstellungsmerkmal verdankt das ITSCM einerseits seiner Fokussierung auf durch das BCM identifizierte, geschäftskritische Prozessanforderungen an die IT und andererseits ein holistisches Betrachtungsmodell potentiell gefährdeter IT-Komponenten, zu denen neben den Hardwareelementen wie Rechenzentren auch Middleware wie Server und Datenbanken bis hin zu softwarebezogenen Schutzzielen zählen (Carvalho e Silva et. al. 2012: 140). Die Abhängigkeit von verfügbaren Anwendungen und Daten zeigt schließlich die Bedeutung der IT für die Prozess- und Kommunikationskontinuität in Unternehmen und wird durch das ITSCM als Anwendungspraktik der Risikokontrolle abgedeckt.

6.6.1. ITSCM - Rückkehr zum Ursprung

ITSCM verdankt seine Bedeutung der steigenden Abhängigkeit modernder Wertschöpfungsketten von der fehlerfreien, das bedeutet unterbrechungsfreien Verfügbarkeit der IT-Infrastruktur, Software und weiterer Komponenten (Asnar und Giorgini 2008: 217).

[424] Mit Blick auf die Justiziabilität eines Ransomware-Angriffs kann attestiert werden, dass sollte ein Beschuldigter identifiziert und der Fall tatsächlich verhandelt werden, Gerichte einer rein digitalen Beweisführung unter Umständen kritisch gegenüberstehen. Die Prüfung der Dokumentation durch Experten kann zunächst einer Einzelfallprüfung unterzogen werden, deren Fachkompetenz im speziellen Fall und unter Betrachtung der komplexen Zusammenhängen von Infrastrukturkomposition und eingesetzter Malware problematisch werden kann, um ein gewünschtes Ergebnis der Verhandlung zu erreichen (Choras et. al. 2015: 690).

Darüberhinausgehend stellten sich jedoch auch komplexer werdende Anforderungen an die Middleware sowie Softwareumgebung und Vernetzung von Endgeräten heraus (Carvalho e Silva et. al. 2012: 136). Dadurch betrachtet ITSCM ein holistisches Bild der IT-Landschaft als interaktives System von Komponenten und inkludiert einen signifikant größeren Schutzbereich als das traditionelle ITDRM (Karim 2011: 183). Das wurde notwendig, weil die technologische Realität aus Cloud Computing, Datenbanken, virtuellen Netzwerken und Serverfarmen eine neue Methode der technischen Verfügbarkeitsplanung voraussetzte (Järveläinen 2012: 583).

Die Risikoexposition im digitalen Zeitalter spiegelt in Form der unmittelbaren Interdependenz von ehemals separierten Elementen die Schattenseite der globalen Interkonnektivität wieder. Die gewohnten Schutzmechanismen eines isolierten Rechenzentrums gehören seit einiger Zeit ebenso der Vergangenheit an wie die Vorstellung abgeschottete Lösungen bei gleichzeitiger Teilnahme an der weltweiten Vernetzung in einen sinnstiftenden Zusammenhang setzen zu können (Wijnia und Nikolic 2007: 3548). „Denn das, was die Angriffe auf die Rechnersysteme so attraktivmacht, sind die Kernfunktionen der vernetzten IT selbst: zentralisierte Steuerungen und Verwaltungen“ (Gaycken und Karger 2011: 5). Durch eine kompromittierte Komponente kann unter Umständen die Kontrolle auf das gesamte Netzwerk ausgedehnt werden und über die Schnittstellen der weltweiten Vernetzung ebenfalls andere Systeme tangieren. [425]

Wie das dritte Kapitel zeigte, begünstigte die ökonomische Rationalität des Informationszeitalters die Ausdehnung und Verzahnung von Systemen.[426] Aufgrund der potentiellen Folgen eines Sicherheitsproblems innerhalb der vernetzten Systeme gewann ITSCM mit Blick auf die Prozessverfügbarkeit und der daraus abgeleiteten Determinanten für ein resilientes IT Management an Bedeutung (Brandt, Hermann und Groote 2011: 67). Im einschlägigen Standard für Informationstechnologie (ISO 27301) wird die enge Verzahnung von prozessorientierter Kritikalitätsanalyse und Ressourcenkontinuitätsplanung betont. Das Ergebnis der methodischen Zusammenführung, welches als der ITSCM Lebenszyklus beziffert

[425] Öffentliche Clouds ermöglichen beispielsweise auch Einzelnutzern als Mitglied einer Gemeinschaft die als Anbieter oder Nutzer von geteilten Serverkapazitäten zu werden und die Einzelkomponenten in einen permanenten und sehr intimen Austausch mit dem Netzwerk zu bringen (Armbrust et. al. 2010: 51). Diese Funktionalität schafft weitere Dependenzen zwischen Systemen, über welche sich Malware leichter und schneller verbreiten können. Auch wenn die Mehrheit der Systemlösungen zum gegenwärtigen Zeitpunkt ihre Vorteile mit Zuversicht präsentieren kann, steigt durch die Vernetzung der Welt auch das Risiko eines durchschlagenden Effekts, falls eine Komponente ins Wackeln gerät.

[426] Die Entwicklung moderner IT-Systeme basiert häufig auf einer iterativen Erweiterung von bestehenden Systemkomponenten. “The IT systems landscape was not built from a grand design, but is more the result of an evolutionary growth, in which elements were added to existing systems to deal with new demands. This means parts of the landscape are heritage systems, potentially not understood by the company anymore as the original programmer/designer has retired/left the business. As the amount of knowledge about the system decreases, the likelihood of emergent (and potentially unwanted) behaviour increases” (Wijnia und Nikolic 2007: 3548).

werden kann, umfasst einzelne Schritte der iterativen Annäherung zwischen Geschäftsanforderung, Ressourcenbetrachtung und deren Harmonisierung (Ernest und Nisavic 2007: 393). Die folgende Grafik zeigt den Ablauf der ITSCM Planung anhand von vier Schritten.

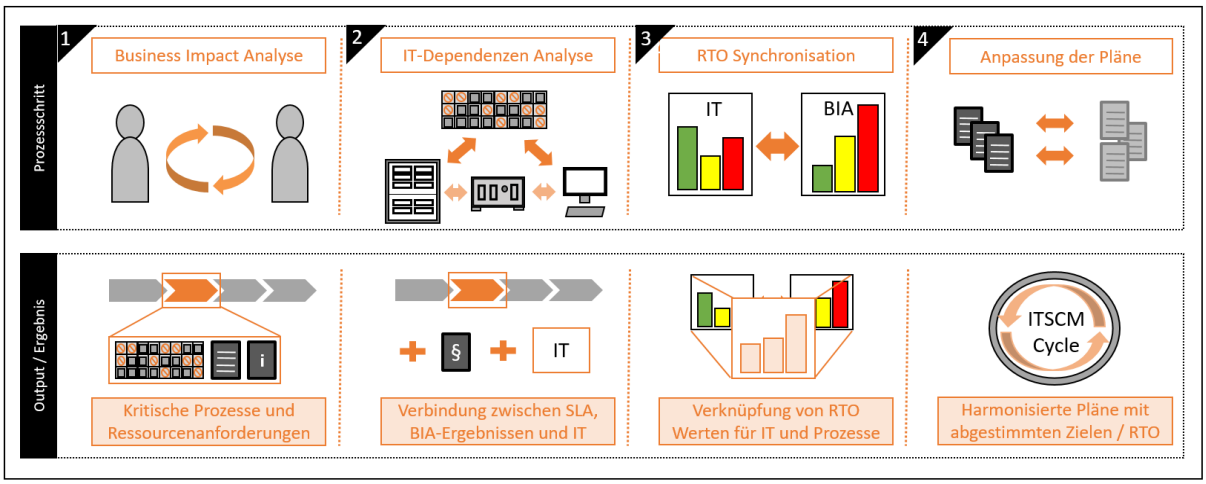

Abb. 6.7. ITSCM Planungsschritte. Eigene Darstellung.

Der erste Schritt der ITSCM Planung ist die (1) Abstimmung der Ergebnisse der Business Impact Analysis (BIA), in der die kritischen Geschäftsprozesse bestimmt und deren Ressourcenabhängigkeit dokumentiert werden. Daraus lassen sich die kritischen Ressourcen aus Sicht der Prozessverantwortlichen darstellen, deren Verbindung im Fall der IT-basierten Ressourcen mit den Einzelkomponenten der drei Ebenen verknüpft werden (Wijnia und Nikolic 2007: 3548). Diese Ebenen beziffern die IT Infrastruktur, IT Middleware und Anwendungen beziehungsweise die darauf verwendeten Daten, deren Verfügbarkeit für den Prozessoutput relevant sind (Sittig und Singh 2016: 627). Diese Informationen sind anschließend (2) mit den internen oder externen Anbietern dieser Services in Kontext zu setzen und im Fall von externen Dienstleistern noch mit den Anforderungskatalogen der „Service Level Agreements“ (SLA), den Dienstleistungsverträgen abzugleichen (Ernest und Nisavic 2007: 401). Auf der Basis dieses Wissensstandes ist es anschließend möglich die (3) Recovery Time Objective (RTO), also deren maximale Ausfallzeit bis zu einer erfolgreichen Wiederherstellung, der einzelnen Ebenen in Einklang zu bringen. Als vierten Schritt gilt es abschließend die gewonnenen Erkenntnisse in den (4) ITSCM Cycle zu überführen, welcher als zirkulärer Prozess eine beständige Selbstkontrolle und –Optimierung verfolgt. Bestandteile des ITSCM Cycle sollten vorrangig die Kernkontrollen abdecken (Nijaz und Moon 2009: 76), welche mit regelmäßigen BIAs, angeglichenen Resilienzstrategien und Wiederherstellungsplänen sowie dem Testen der selbigen die Minimalanforderungen erfüllen sollten.

6.6.2. ITSCM - Theorie in der Praxis

Diese methodischen Rahmenanforderungen an das ITSCM eines Unternehmens sind jedoch von Begleiterscheinungen der praktischen Anwendung flankiert, deren Auswirkungen sich als problematisch herausstellen können. Während der ethnographischen Untersuchung wurde in Gesprächen mit IT-Praktikern und Prozessverantwortlichen ein differenziertes Bild der Bereitschaft zur Teilhabe einerseits und zur Umsetzbarkeit von Wiederherstellungsprozeduren andererseits beobachtet. Während der Implementierung eines ITSCM Lebenszyklus zwischen Mai und Juli 2018 stellte sich heraus, dass die vornehmlich gepflegten Servicekataloge der IT nicht die gleichen Terminologien verwenden, wie sie auf Seiten der Prozessebene bekannt und gebräuchlich waren.[427] Durch die Beobachtung entwickelte sich die Erkenntnis, dass beide Seiten, IT und Betrieb, ihre Verantwortung auf ihren jeweiligen Kompetenzbereich fokussierten. Die Risikokontrolle wurde einerseits als ein IT-spezifisches Kontinuitätssystem und auf der anderen Seite ein getrenntes Planungsmuster für die Wiederherstellung von Geschäftsprozessen verstanden. Die Folge wäre ein ressourcen-, also objektspezifisches Risikoverständnis gewesen, allerdings war die Bereitschaft zur systemischen Planung durch die veränderten Risikodiskurse innerhalb des Unternehmens voran geschritten[428] und resultierte in einer schrittwiesen, semantischen und inhaltlichen Anpassung der beiden Bereiche.

Als Konsequenz kann festgehalten werden, dass mitunter erhebliche Aufwände zur einheitlichen Benennung und Verknüpfung der in der BIA identifizierten Anwendungen, deren IT-Servicebezeichnung sowie die darunter liegenden IT-Komponenten wie Middleware oder Hardware (Ernest und Nisavic 2007: 388), teilweise auch weitere Software und Systemschnittstellen zu erbringen sind. Als nächster Schritt folgt die Kontextualisierung von Applikationen mit deren Dienstleistern, was durch die zumeist unterschiedlichen, in manchen Fällen divergierenden Anforderungen an die RTO-Zeiten erschwert wird. Denn auch wenn ein Prozessverantwortlicher eine RTO von beispielsweise vier Stunden für unabdingbar hält, muss diese vertraglich festgeschrieben sein, um den Anbieter dieser Anwendung von dieser Sichtweise zu überzeugen (Wijnia und Nikolic 2007: 3548). Höhere Verfügbarkeiten durch

[427] Insbesondere Applikationen unterliegen der begreiflichen Metamorphose aus Sicht ihrer Endanwender, aus der sich eigene Wortschöpfungen und Begriffsvariationen ergeben. Diese Informationen mit der Liste kryptischer Applikationsbezeichnungen in einen sinnvollen Einklang zu bringen, erfordert nicht zu selten ein vorgelagertes Projekt zur Harmonisierung der Nomenklatur von Services, Anwendungen und Nutzerinterpretationen der vorrangig genannten Elemente (Hintergrundgespräch 08.05.2018).

[428] Die Veränderung der verwendeten Risikoterminologie und auch der darauf aufbauenden Praktiken konnte während der beobachtenden Teilnahme über einen längeren Zeitraum festgestellt werden. Die rezitierte Benennung von „emerging risks“ und systemischen Risikokategorien begünstigten den schrittweisen Diskurswechsel von objektbezogenen Risikokontrollvorstellungen hin zu einer Prozessbeschreibung zur Sicherstellung der Betriebskontinuität unter Einbeziehung aller Komponenten in einen systemischen und resilienten Vorsorgeplan für das Unternehmen (Hintergrundgespräch 26.07.2022).

eine effektive Risikomitigation haben auch auf Seiten der IT ihren Preis, welcher sich im SLA und dem dazugehörigen Preisschild des Service auszudrücken vermag.[429] Eine Abwägung der unterschiedlichen Preisspannen für Anwendungen mit einer RTO von 4 Stunden und für 72 Stunden können den Prozessverantwortlichen die monetären Auswirkungen der Verfügbarkeitsdetermination vor Augen führen.[430]

Diesem mühsamen Aushandlungsprozess sollte sich im dritten Schritt die technische Anpassung der RTO-Werte anschließen. Im Fall von großen Unternehmen können mehrere hundert Servicefamilien mit zehntausenden Services und dahinter liegenden Anwendungen die Gesamtperspektive unübersichtlich gestalten (Ernest und Nisavic 2007: 390). Daher ist eine Fokussierung auf die relevanten, das heißt kritischen Anwendungen und Informationen als Ergebnis der ersten beiden Schritte von großer Bedeutung (Racz, Weippl und Seufert 2010: 250). Im Fall der oben wiedergegebenen beobachtenden Teilnahme im Unternehmen zeigte sich auch, dass die Komplexität der vernetzten und aufeinander aufbauenden Soft- und Middleware-Komponenten von kaum einem Individuum im Unternehmen vollständig erfasst werden konnte. Die gängige Praxis unter den beteiligten Praktikern ging dazu über, die identifizierten IT-Anwendungen einzeln und in Absprache mit den jeweiligen IT-Architekten beziehungsweise den Desaster-Recovery-Verantwortlichen der jeweiligen IT-Infrastrukturfunktionen auf Widerherstellungsklassen und Abhängigkeiten zu anderen Anwendungen abzuklären. Allerdings stellte sich ein Lerneffekt ein, der die anfängliche Bearbeitungszeit pro Anwendung von 2 Wochen (einschließlich Arbeits- und Wartezeit) auf 2 Tage verkürzen konnte. Dadurch konnten die relevanten Kennzahlen, ausgedrückt als die Gegenüberstellung von prozess-abhängiger RTO und IT-basierter Desaster Recovery Class (DRC), schließlich ermittelt werden.[431]

---

[429] Die Einbeziehung von ausgegliederten Prozessen und IT-Dienstleistungen unterstehen zudem rechtlichen Anforderungsprofilen, denen Unternehmen durch ihr ITSCM Rechnung tragen sollten, wozu auch die regelmäßigen Überprüfungen der Wiederherstellungskapazitäten und Einhaltung der vereinbarten Maßnahmen gezählt wird (vgl. Gaycken und Karger 2011: 7).

[430] Eine weitere Dimension ist die Auswahl sicherer Dienstleister und Plattformen zur Unterstützung der Prozesskontinuität. Die auf den mittlerweile 30 Jahren alten TCSEC Stufen (Trusted Computer Evaluation Criteria) basierenden Einstufungen von sicheren IT-Umgebungen können heute noch als Referenz dienen, um auf einer vierstufigen Skala die Sicherheit eines Systems bewertet und könnten einer Ausschreibung als Grundlage dienen, beziehungsweise die Verwendung von Typ D und C, den beiden geringsten Schutzklassen als Hosts für kritische Anwendungen ausschließen. Die Schwäche des ursprünglichen Modells liegt in der Weiterentwicklung der Netzwerke, für welche dessen originärer Fokus auf Betriebsprogramme nicht mehr gerecht wird und folglich um die Dimension von offenen Kommunikationssystemen wie im Fall des „IoT“ zu erfassen (Eckert 2008: 203f.).

[431] Die Entwicklung einer einheitlichen ITSCM Methodologie trug erheblich zur flächendeckenden Betrachtung von IT-Systemen und Infrastrukturkomponenten bei. Durch die Repetition von ähnlichen Anwendungen, stellte sich zudem eine Effizienzsteigerung ein, welche einen schnelleren Abschluss der Implementierung erlaubte (vgl. Hintergrundgespräch 20.02.2018).

Neben den Angleichungen von IT- und Betriebskennzahlen bedeutet die Etablierung eines ITSCM-Programms auch die Erstellung und Harmonisierung von Wiederherstellungsplänen. Eine Aufgabe die ebenfalls unterschiedliche interne Zuständigkeitsbereiche tangiert und allein daher zu einer Herausforderung werden kann. Darüber hinaus müssen gegebenenfalls externe Partner in die Aufgabe einbezogen werden (Ernest und Nisavic 2007: 393). Hierbei ist insbesondere zwischen Unterstützungsfunktionen, wie dem Einkauf von operationellen Dienstleistungen bei Dritten oder elementaren Ausgliederungsgeschäften wie dem vollständigen Betrieb von IT-Infrastruktur oder Systemadministrationsaufgaben durch Dritte zu differenzieren (Bahli und Rivard 2003: 215). Die Anpassung der Pläne sowie die Kontrolle ihrer korrekten Umsetzung erfordern in beiden Fällen unterschiedliche Aufwände und binden vorrangig im zweiten Fall weitere Ressourcen (Karim 2011: 184). Selbst wenn angenommen wird, dass der Dienstleister im höchsten Maße mit Verlässlichkeit ausgezeichnet ist und seine vertraglichen Obligationen einhält, sind dennoch Harmonisierungsdefizite durch die Tatsache zu erwarten, dass zwei (oder mehrere) getrennte Unternehmen geteilte Aufgaben wahrnehmen, ohne jedoch die organisatorische oder disziplinarische Autorität übereinander innezuhaben. Zuletzt sind noch die Fort- und Bewusstseinsbildung der Nutzer hervorzuheben (Nicoll und Owens 2013:54), deren Einstellung zum ITSCM Lebenszyklus die Schnelligkeit und allgemeine Effizienz des Prozesses erheblich beeinflussen können. ITSCM bedeutet daher auch, Nutzer in die Planung miteinzubeziehen und Erwartungen anhand der Kosten-Nutzen-Rechnung in einem verhältnismäßigen Ausgleich zu bringen (Sittig und Singh 2016: 627).

Als abschließender Gedanke kann daher festgehalten werden, dass ITSCM als Anwendungspraktik zur Verringerung der Ausfallwahrscheinlichkeit von Prozessen durch eine umfassende Analyse der IT-Ressourcenanforderungen, Infrastruktur, Middleware und Anwendungen zur systemischen und prozessgeleiteten Risikokontrolle beiträgt. Jedoch hat ITSCM keinerlei Einfluss auf den Schutz des Unternehmens vor Angriffen, welche sich nicht auf die Verfügbarkeit der Daten richten, beispielsweise im Fall des unautorisierten Zugangs zu vertraulichen Informationen. Dieser Punkt ist von großer Bedeutung für unsere Fragestellung, weil die Ökonomie des Informationszeitalters auf Komplexität und systemischen Zusammenhängen wie der Cloud und Mehrebenen-Architektur der IT basiert.[432] Die Sicherheitsproduktion in Unternehmen beschränkt sich daher nicht nur auf die ohnehin

[432] Die Risikoexposition von Cloud-Lösungen offenbart die Bedeutung von Schutzvorkehrungen, welche vor einer möglichen Auslagerung von kritischen Informationen an Dienstleister reflektiert werden sollten. Insbesondere „Denial of Service“ Angriffe (DoS) haben ein großes und destruktives Potential mit Blick auf die Verfügbarkeit von Daten auf Cloud-Datenbänken. (Krotofil und Cárdenas 2013: 177).

anspruchsvolle Sicherstellung der Verfügbarkeit von interdependenten Prozessen und Anschlussoperationen, sondern muss darüber hinaus auch die Integrität und Vertraulichkeit von Informationen berücksichtigen muss. An dieser Stelle offenbart sich eine methodische Lücke zwischen der Disponibilität von Prozessen und deren IT-Grundlage einerseits, umgesetzt durch BCM, ITSCM und KM, aber auch der konkreten Schutzzielen des Informationsschutzes andererseits.[433] Diese Problematik wollen wir im nächsten Kapitel aufgreifen und die Einführung eines neuen, systemischen Risikokontrollsystems beschreiben.

6.7. Zusammenfassung- Risikomitigation im analogen und digitalen Zeitalter

Im Rückblick ist zu erkennen, dass die ökonomische Rationalität der Digitalisierung in einem Prozess, der keine zwei Dekaden bedurfte, ein essentielles Abhängigkeitsverhältnis von Dateneigentümern, deren Nutzern und den Betreibern der Infrastruktur- und Anwendungsschnittstellen etabliert hat. Die Veränderungen in den Beziehungen zwischen Unternehmen haben ebenso einem Veränderungsprozess durchlaufen, wie die für die Selbstbeschreibung von Organisationen notwendige Abgrenzung zur Außenwelt. Der systemische Charakter von interdependenten Komponenten, welche die Anschlussoperationen und Kommunikation im Informationszeitalter erst ermöglichen, bestimmt die Risikoexposition von Unternehmen. Als Folge waren weitreichende Veränderungen des Risikodiskurses zu beobachten, welche insbesondere im Fall unserer beobachtenden Teilnahme auf die Verschiebung der Praktiken der unternehmensinternen Risikokontrolle verstanden wurden.[434]

Die zentrale Schlussfolgerung der ethnographischen Untersuchung fand daher in diesem Kapitel Einzug, indem durch die Gespräche und Beobachtungen festgestellt wurde, dass die Chancen und vielversprechenden ökonomischen Möglichkeiten der Digitalisierung nicht ohne deren Risiken betrachtet werden können. Die im Unternehmenskontext beobachtete Einführung des Begriffs der Resilienz kann daher helfen, die Anforderungen an ein neues Risikokontrollsystem zu konkretisieren und Unternehmen eine Richtung vorzugeben, wie sie sich auf einen möglichen Kommunikationsabbruch vorbereiten können. Der Begriff Resilienz beschreibt im Sprachgebrauch von Unternehmen die Neuinterpretation der internen Sicherheitsproduktion und, wie im Fall der ethnographischen Beobachtungen festzuhalten war,

[433] Diese methodische Lücke war die Schlussfolgerung aus der ethnographischen Untersuchung und resultierte als Erkenntnis aus verschiedenen Gesprächen mit IT-Architekten (Hintergrundgespräch 29.09.2020; Hintergrundgespräch 27.10.2022) und Verantwortlichen der Sicherheitsproduktion (Workshop 19.01.2021; Hintergrundgespräch 15.11.2021).
[434] Vgl. Hintergrundgespräch 26.07.2022.

auch einer Neudefinition von Risiken im Zuge der Digitalisierung.[435] Der Übergang von objektbezogenen Risikokontrollen hin zu einem systemischen Verständnis schlägt sich auch in den Anwendungspraktiken nieder, welche BCM, KM, ITSCM sowie Informationsschutz in ein einheitliches, vernetztes Risikokontrollsystem überführen.[436]

Durch diese Ausrichtung der Risikokontrolle kann zudem der Beitrag von Unternehmen zur Sicherstellung vitaler Grundanforderungen der Bevölkerung im Fall der kritischen Infrastruktur anders betrachtet werden. Mithilfe von Resilienz kann die Sicherheitsproduktion in Unternehmen als bisher unterrepräsentierter Aspekt des gesellschaftlichen Sicherheitsdiskurses neu bewertet werden. Dies zeigt sich insbesondere am Fall der kritischen Infrastruktur, für die private Träger aufgrund ihrer operativen und rechtlichen Verantwortung einen signifikanten Beitrag zum Sicherheitsdispositiv der Bevölkerung leisten (Brzoska, Neuneck und Scheffran 2021: 6f.), allerdings im Interessenskonflikt zwischen ökonomischer Rationalität und konkreter Schutzmaßnahmen stehen. Aus dieser Situation übersetzt sich die Bedeutung von Unternehmen für die Sicherheitsforschung in ein hier neu-besetztes Problemfeld, welches durch die Risiken der Digitalisierung einerseits und die Rolle der Sicherheitsproduktion in Unternehmen anderseits als Beitrag zur gesamtgesellschaftlichen Existenzsicherung gekennzeichnet sind. Wie diese Übersetzung konkret aussehen soll und welche Schlussfolgerungen daraus zu ziehen sind, wird der letzte Themenblock adressieren. Dieser wird die Umsetzung der Risikokontrolle in Unternehmen unter Berücksichtigen der vorausgehenden Problemfelder erörtern, sowie im Anschluss einen Ausblick über die Folgen und Anschlussmöglichkeiten unserer Arbeit für weitere Studien geben.

[435] Die ethnographische Untersuchung zeigte, wie sich Praktiker und Unternehmensführung, insbesondere unter dem Eindruck der Corona-Pandemie, zunehmend einer systemischen Betrachtung von Sicherheit zuwendeten. Ein Manager sagte dazu, dass der Schutz einzelner Komponenten keinen sinnstiftenden Beitrag liefere, wenn nicht die gesamte Organisation und ihre Fähigkeit zur Bereitstellung von Leistungen an den Kunden im Blick der Vorsorgeplanung seien (Hintergrundgespräch 15.11.2021).

[436] Im Zuge der ethnographischen Beobachtung wurde auch eine Veränderung der semantischen Verwendung hinsichtlich der Sicherheitsproduktion im Unternehmen festgestellt. Während in den Jahren 2012 bis 2018 vorrangig von den Fachabteilungen wie BCM oder Informationsschutz gesprochen wurde, kam der Begriff Resilienz immer mehr in der internen Kommunikation auf. Mit der Corona-Pandemie ab Ende 2020 beherrschte der Terminus Resilienz schließlich als Überbegriff die Komponenten der Sicherheitsproduktion und wurde auch von der Unternehmensführung als Zielbild vorgestellt, wodurch die anderen Begriffe als Sinnbilder der objektbezogenen Risikokontrolle immer mehr zugunsten des systemischen und adaptiven Resilienzbegriffs an Bedeutung verloren (Hintergrundgespräch 15.11.2021).

IV) Implementierung der resilienten Organisation

Dieser finale Themenblock umfasst zwei wesentliche Schlussfolgerungen aus den zuvor dargestellten Beobachtungen und Erkenntnissen. Die erste Schlussfolgerung wird auf der Grundlage der ethnographischen Untersuchung zur Selbstbeobachtung der Organisation und Umsetzung ihrer systemischen Sicherheitsdispositive mithilfe von Resilienz aufbauen. Diese wird als (1) Umsetzung einer resilienten Organisation, basierend auf den zuvor skizzierten Voraussetzungen der Sicherheitsproduktion in Unternehmen und unter Berücksichtigung der in Gesprächen mit Experten artikulierten Schutzziele und Anforderungen dargestellt. Diese Beschreibung umfasst im siebten Kapitel die Handlungsfelder und Umsetzung einer neuen Risikokontrolle unter dem Überbegriff Resilienz. Dieses Kapitel wird die praktischen Herausforderungen sowie die Aspekte eines integrativen Risikomanagements beschreiben, welches Unternehmen in die Lage versetzen soll, die exogenen Sicherheitsprobleme in effektive Maßnahmen und Methoden zur Sicherstellung der Prozess- und Kommunikationskontinuität zu übersetzen. Dazu zählen sowohl die Herausforderungen aus organisationstheoretischer Sicht, welche die Organisation bewältigen muss, als auch der Umgang mit der Unsicherheit im Informationszeitalter, welches Auswirkungen auf das Risikokontrollsystem erwarten lässt.

Diese Überlegungen werden wie bereits eingeleitet durch Beobachtungen aus der ethnographischen Untersuchung ergänzt, welche die Diskurse und Problemthematisierung der Experten und Praktiker im Zuge einer solchen Umsetzung von Resilienz widerspiegeln sollen. Zweitens werden im achten Kapitel die Schlussfolgerungen für die (2) weitere Forschung relevanten Anschlussfragen diskutiert werden. Darunter fällt eine Reflektion der Methoden, des Theorieverständnisses und der ermittelten Schlussfolgerungen durch die vorausgehenden Kapitel. Am Ende soll ein Ausblick auf die möglichen Anschlussfelder in der Literatur gegeben werden, durch welche unter anderem die Bedeutung und Relevanz der Sicherheitsproduktion in Unternehmen hervorgehoben werden wird. Die Betrachtung von Unternehmen und ihrer internen Risikokontrolle soll den Blick auf private Akteure im Sicherheitsdiskurs lenken, deren Rolle nicht durch ihre Umsetzung von Sicherheit im Auftrag durch staatliche Autoritäten erfolgt, also Sicherheit *durch* Unternehmen, sondern durch die Sicherstellung der Prozesskontinuität *in* Unternehmen selbst zum gesellschaftlichen Sicherheitsdispositiv beiträgt.

7. Handlungsfelder und Umsetzung

Die vorrausgegangenen Kapitel betrachteten die Exposition und Veränderung des Risikobegriffs in Unternehmen, welcher im Zuge der Digitalisierung und Exposition von geschäftsgefährdenden Risiken neu besetzt wurde, wie die letzten beiden Kapitel zeigten. In der Sicherheitsliteratur fällt allerdings auf, dass der Blick selten auf, noch weniger in Unternehmen vorgenommen wird. Diese Perspektive soll in diesem Kapitel durch den Blick auf die konkrete Umsetzung der Risikokontrolle durch Resilienz gezeigt werden und dadurch auch einige Problemfelder für die Implementierung diskutiert werden. Gespräche mit Experten, insbesondere im Zuge der intensiven Beschäftigung mit dem Ziel zur Schaffung resilienter Strukturen während der Corona-Pandemie zwischen Frühjahr 2020 und Herbst 2022, zeigten die Verschiebungen des Risikodiskurses auf.[437] Dazu soll dieses Kapitel weiter beitragen, indem anhand von konkreten Handlungsfeldern der Umbau der Risikokontrolle in Unternehmen und der normativen Gestaltung von Prozessen und Praktiken aufgezeigt werden soll.

Dieses Kapitel ist daher in drei Sinneinheiten gegliedert. Der erste Abschnitt umfasst die (1) Implikationen der umfassenden Virtualisierung von Prozessen im Zuge der Corona-Pandemie, welcher Unternehmen vor die Herausforderung stellt, die Folgen der technologischen Grundlagen durch Kontrollsysteme zu steuern.. Nach dieser Darstellung werden die (2) konkreten Handlungsfelder eingeführt, welche sich als integrativer Ansatz zur Risikokontrolle zusammenfassen lassen. Darunter fallen Überlegungen und Aufgaben der Kritikalitätsbewertung, Prozess- und Ressourcendefinition, Strategie- und Planungsaufwände, sowie das Testen und Einüben von Praktiken und Verhaltensmustern zur Einbindung in das Gedächtnis der Organisation. In diesem Abschnitt werden die Erkenntnisse der ethnographischen Untersuchung reflektiert und als Schutzziele und Ansprüche an die neue Sicherheitsarchitektur in Unternehmen artikuliert

Da solche Vorhaben in der Regel aufwendig und komplex ablaufen, sollen im dritten Teil die (3) Herausforderungen für eine erfolgreiche Umsetzung genauer beleuchtet werden. Hier

[437] Nach der ersten Bewältigung der Fortführung von Prozessen ergaben sich weitere Herausforderungen im hybriden oder rein virtuellen Betrieb. Während eines Projekts, welches sich vom Mai 2020 bis November 2022 erstreckte, ergaben sich mehrfach Gelegenheiten mit Experten und Managern aus verschiedenen Funktionen des Unternehmens zur angestrebten Struktur und Gestalt des Risikosystems zu sprechen (vgl. Hintergrundgespräch 26.11.2020). Darunter fielen Gespräche, welche an späterer Stelle wieder aufgegriffen werden, wie beispielsweise mit einer Verantwortlichen für die Kontinuitätsplanung der IT (Hintergrundgespräch 27.06.2022) oder einem Experten aus der IT-Infrastruktur zur Redundanz von Rechenzentren und deren Ausfallsicherheit (Hintergrundgespräch 23.11.2022).

werden Aspekte der zeitlichen Planung sowie der Anpassungen der hierarchischen Strukturen einer erfolgreichen Implementierung reflektiert werden. Ebenfalls wird die Bedeutung von Entscheidungen, Kommunikation und Erinnerung mit Blick auf Resilienz erneut besprochen werden, da die ganzheitliche Einbindung von Risikokontrollen unter dem neuen, prozessorientierten Risikoverständnis auch eine strukturelle Ausrichtung innerhalb der Organisation benötigt. Für diese Betrachtung werden ebenfalls die Schlussfolgerungen aus der ethnographischen Untersuchung, aufbauend auf Gesprächen mit Experten, eingebunden, um die Perspektive der unternehmensinternen Praktiken und Diskursverschiebungen im normativen Bild der resilienten Organisation einfließen zu lassen. Beginnen wir mit der Reflektion der technologischen Möglichkeiten für Unternehmen und dem Spannungsfeld zwischen Möglichkeiten und Problemen zur Sicherstellung von Kontinuität für Prozesse und Kommunikation.

7.1. Fortschritt und Schutz im Widerspruch?

Nicht zuletzt die Corona-Pandemie eröffnete den Blick auf die Möglichkeiten des technologischen Fortschritts zur Bewältigung einer Krise. Der Einsatz neuer Impfstoffe auf mRNA Basis oder die methodische, wenn auch nicht immer abschließend erfolgreiche, Nachverfolgung des Infektionsgeschehens zeigten, wie technologischer Fortschritt zur Sicherheitsproduktion in einer Gesellschaft beitragen kann. Eine wesentliche Entwicklung war in diesem Kontext auch die zuvor beleuchtete Virtualisierung von Arbeitsprozessen in Reaktion auf die Kontaktbeschränkungen (Bellmann et. al. 2021: 713). Im Zuge der ethnographischen Beobachtung wurden zwischen Oktober und Dezember 2020 Hintergrundgespräche mit Experten geführt, deren Einschätzung Aufschluss über die bis zu diesem Zeitpunkt erfolgten Maßnahmen gab. Die überwiegende Meinung der Experten befürwortete den rasanten Umstieg von analogen Arbeitsumgebungen zu virtuellen Kooperationsmodellen im Licht des drohenden Kommunikationsabbruchs innerhalb der Organisation durch die Kontaktbeschränkungen.[438]

Der Diskurs eröffnete ebenfalls den Blick auf eine kritische Betrachtung der getroffenen Maßnahmen, welche in zwei Gruppen eingeteilt werden können. Die erste Gruppe thematisierte

[438] Es wurden 2020 Interviews mit Praktikern aus 18 Landesgesellschaften geführt, welche die unterschiedlichen Herausforderungen im Umgang mit der Corona-Pandemie und der einhergehenden Lockdown-Maßnahmen schilderten (Workshops September bis Dezember 2020). Übergreifend wurde die Existenzsicherung in den Vordergrund der Handlungsmotivation während der Monate März bis Juni 2020 gestellt. Ein Gesprächspartner aus einer westeuropäischen Entität verdeutlichte den Handlungsdruck, indem die Mitarbeiter der IT in den nächsten Elektrofachhandel geschickt wurden, sobald sich die Ankündigung des Lockdowns abzeichnete, um alle geeigneten Notebooks aufzukaufen. Ein Experte aus einer südeuropäischen Landesgesellschaft beschrieb hingegen, dass die achtköpfige IT-Abteilung über das Wochenende notdürftig alte Computer im Lager neu aufsetze, um sie an die Belegschaft am Montag auszuteilen (Workshop 26.11.2020)

die Krisenkommunikation und Aktivierung von Plänen, welche im nächsten Abschnitt beleuchtet werden. Die zweite Gruppe umfasst hingegen die Risikoabschätzung hinsichtlich der Einführung neuer Technologien, deren mögliches Schadenspotential durch die ungeplante und unverzügliche Implementierung von beispielsweise Systemzugängen, virtuellen Arbeitsprozessen oder Verknüpfung von Plattformen nicht ausreichend ex ante berücksichtigt wurde. Dieser zweiten Gruppe wollen wir uns in diesem Abschnitt widmen und den Blick auf die langfristige Entwicklung der Digitalisierung mit Blick auf ihren Einfluss auf die Sicherheitsproduktion lenken.

Allgemein betrachtet, besteht der potentielle Widerspruch zwischen ökonomischen Vorteilen der Digitalisierung und der Investition in antizipierende Schutzmaßnahmen schon seit Längerem (Cook 2010: 23). Die Unsicherheit über Risiken im Cyberzeitalter unterliegt einem wie bereits aufgezeigten paradoxen Wirkungszusammenhang, in dem die mittelfristige Anforderung zu schneller Anpassung an den technologischen Wandel und die langfristige Aufstellung der resilienten Organisation in einen Wettbewerb um Ressourcen treten (Weber 2016: 30). Ebenso wie im Fall der traditionellen Risikobetrachtung leisten unterschiedliche Logiken und Denkweisen über den geeigneten Umgang mit den Risiken des Informationszeitalters ihren Beitrag für einen Diskurs über die geeignete Vorgehensweise und Abwägung zwischen Investitionen und Ertrag präventiver Schutzmaßnahmen

Die Logik der objektiven Risikobewertung, deren Grundprämissen auf der Verfügbarkeit von Daten und der *realen* Existenz von Risiken beruhen, wird auf diesem Feld in zweierlei Hinsicht enttäuscht. Der Mangel an Fallzahlen dokumentierter Risiken und deren Schadenswirkungen ist evident und die Menge der bisher verfügbaren Informationen zeitlich beschränkt (Linkov et. al. 2013: 472). Denn trotz der quantitativen und qualitativen Beispielfälle der digitalen Risikoexposition in der jüngsten Vergangenheit, sind die Mess- und Sensorik-Parameter einer analytischen Risikokomparatistik im Cyberzeitalter noch relativ unausgereift (Krotofil und Cárdenas 2013: 179). Anders als andere Risikokategorien wie den Naturrisiken oder dem politischen Risiko sind daher die mittel- bis langfristigen Prognosechancen weniger verlässlich als andere, bekanntere Kategorien. Zweitens kann die virtuelle Dimension der digitalen Risiken mit ihrer transzendenten Eigenschaft zur Interaktion zwischen analoger und digitaler Welt die Risikobewertung problematisch gestalten. Die Suche nach der *realen*, objektiv messbaren Existenz des Risikos gereicht unter den Bedingungen der Unsicherheit zum Nachteil der traditionellen, objektiven Methode.

Die fehlende Einordnung der Materie in einen weiteren Kontext erschwert die Betrachtung der Risiken im virtuellen Raum, da die soziale Aufladung von Begrifflichkeiten, Zusammenhängen und Konsequenzen hinter einer technischen Begriffsanwendung versteckt liegt (Schermann und Krcmar 2010: 227). Die scheinbare Rationalitätsmaximierung der digitalen Welt basiert auf einer Zuschreibung von Sachlichkeit, welche tatsächlich auf die Maschinen, Programme oder künstliche Intelligenz anzuwenden ist.[439] Gesellschaftliche Kontextualisierung von Risiken können dahingegen in zwei anderen Teilaspekten der Digitalisierung gefunden werden, zum einem in Form der gesellschaftlichen Vorprägung und Wertorientierung der Entwickler von Algorithmen (Cavelty 2013: 110) und zum anderen in der Auswirkung der technologischen Implementierung für die Gesellschaft in der analogen Welt (Fischer 2007: 53). Diese Perzeption der Bedeutung und Tragweite des technologischen Wandels eröffnet somit eine reflektierte Sichtweise auf die möglichen Konsequenzen der Digitalisierung, welche sich neben sachlich-terminierten Aspekten auch in Form eines gefühlten, emotional aufgeladenen Wahrnehmungsaspekts manifestiert (AGCS 2018: 8).

Entscheidungsträger, welchen die Aufgabe obliegt zwischen den diametralen Optionen einer Investition in Schutzmaßnahmen abzuwägen, wären somit gut beraten den subjektiven Kontext im Rahmen ihrer Bewertung der geschäftsgefährdenden Risiken zu berücksichtigen. Denn nur mithilfe des tiefgreifenden Verständnisses des technologischen Wandels und seiner technischen, aber auch seinen sozialen und emotional wahrgenommenen Folgen für die analoge Welt kann, die Risikobewertung verwertbare Ergebnisse erzielen, deren Auswertung für die Implementierung einer resilienten Organisation unentbehrlich sein wird (Weber 2016: 33). Falls die IT-Kompetenz nicht in Personalunion mit den Entscheidungsträgern einhergeht, sind geeignete Experten im Unternehmen oder in Form von externem Sachverstand heranzuziehen, um eine angemessene Bewertung der Risikokategorie zu erhalten (Xue et. al. 2013: 339). Der digitale Wandel erschafft eine ähnliche Entkoppelung von den wichtigsten Schutzwerten eines Unternehmens – den Informationen – welche durch Cloud-Lösungen und Datenbanken zwar Einzug in ein leistungsfähigeres virtuelles Organisationsgedächtnis nehmen, aber auch größeren Risiken unterliegen.

Die örtliche Umschreibung dieser veränderten Umwelt erfolgt in logischer Konsequenz der gesellschaftlichen Semantik der Digitalisierung und wird wie wir es bereits anführten als

[439] Die Fähigkeit von Algorithmen zur Empathie ist zum aktuellen Zeitpunkt der Entwicklung noch nicht dokumentiert. Die Kompetenz die Gefühlslage, Motivation oder soziale Einbettung von Meinungen und Handlungen in einen gesellschaftlichen oder emotionalen Kontext zu stellen, übersteigt die Leistungsfähigkeit von Maschinen, auch wenn die intellektuellen Fähigkeiten der künstlichen Intelligenz, beispielsweise die Rechenfähigkeit und Logikkapazität die des Menschen bereits zu übersteigen vermögen.

Cyberspace oder virtueller Raum bezeichnet.[440] Hier liegt für Unternehmen nach traditionellem Verständnis die Außenwelt der digitalen Sphäre. Dort wo das Werkstor die analoge Außenwelt vom Inneren trennt, bezeichnet der Cyberspace das Externe in der digitalen Welt, welches vom Inneren des virtuellen Gedächtnisses und seiner Datenbanken und verarbeitenden Anwendungen mental abgegrenzt wird (Cavelty 2013: 107). Dies entspricht jedoch einer Einschätzung, die mit Blick auf die technologische Durchdringung von Gesellschaft, Wirtschaft und Informationsverflechtungen anachronistisch erscheint. Die paradoxe Verknüpfung der unmittelbaren Lösung exogener Problemsituationen und langfristigen Risiken zeigte sich vor allem während der Corona-Pandemie. Die Einführung neuer, allerdings aus sicherheitsspezifischer Sicht nicht abschließend ausgereifter Technologien zur Abwendung des bevorstehenden Kommunikationsabbruchs auf der einen Seite, steht den zukünftigen Sicherheitsrisiken dieser Technologien in Folge dieser Entscheidung auf der anderen Seite gegenüber.[441]

Doch nicht die Digitalisierung oder ihre räumliche Materialisierung in Form des Cyberspace sind ursächlich für die neue Risikoexposition zur Verantwortung zu ziehen (Kahan, Allen und George 2009: 8), sondern die explizite oder implizite Entscheidung von Unternehmen die aufkommenden Technologien einzusetzen und angemessene Schutzvorkehrungen zu vernachlässigen. Die Entscheidung zum Einsatz der technischen Mittel, die Entscheidung zum Umbau eines Unternehmens und schließlich auch die Entscheidung für oder wider Investitionen zur Etablierung einer resilienten Organisation, sind die originären Gründe für die spezifische Risikoperzeption (Cook 2010: 23), deren Beantwortung durch Unternehmen in Form des Begriffs der Resilienz diskutiert wird. Die paradoxe Dualität des Risikobildes im digitalen Zeitalter basiert auf der Zunahme an tatsächlichen oder versuchten Angriffen auf das virtuellen Gedächtnis von Unternehmen in Form ihrer Datenbanksysteme attestiert werden (Schulze

[440] Unter dem Begriff Cyberspace wird die Hardware verstanden, welche als infrastrukturelle Basis die Betriebsgrundlage für Programme und Applikationen bietet, welche sich dieser Leistungsbereitstellung bedienen und Nutzern eine Bedienoberfläche für deren Anfragen und Aufträge bereitstellen (Kahan, Allen und George 2009: 8). Gleichzeitig ist diese räumliche Vorstellung aber auch ein Lokalisierungsversuch der immensen Leistungsfähigkeit einer technologischen Veränderung, deren digitale Sphäre den wesentlichen Teil der ökonomischen und technischen Weiterentwicklung der analogen Welt bestimmt und über diverse Schnittstellen wie Roboter, Aktienhandelsalgorithmen oder mobile Endgeräte direkt in diese eingreifen kann (Krotofil und Cárdenas 2013: 166).

[441] Die Betrachtungsweise auf das Risiko im Cyberspace wird dabei von talentierten Individuen oder Gruppen geprägt, deren Schöpfungen in Gestalt von Schadprogrammen die digitale Außenwelt zu einem gefährlichen Ort für Unternehmen machen (können). Ihre Motivation wird wechselweise zwischen Gier, anarchistischer Grundgesinnung oder in einer Form modernen Söldnergeschäfts zu verorten. Somit sind Hacker „increasingly branded as criminals in government circles, not least because computer break-ins seemed to become more widespread, and received a lot of media attention" (Cavelty 2013: 112).

2021: 2), deren Ausprägung als APT[442], Ransomware, DoS oder anderer Variationen großes Schadenspotential beherbergt (AGCS 2022).

In diesem Fall stößt auch das traditionelle Verständnis von Risikokontrollsystemen mit fachlicher Segregation an seine Grenzen. Sein originäres Schutzziel, namentlich die Fortsetzung des Geschäftsbetriebs, reduziert sich auf die Verfügbarkeit von Ressourcen. Informationen sind als Teil dieser essentiellen Ressourcen ebenfalls dem Verfügbarkeitsdiktum unterworfen, jedoch nicht anderer Schutzdimensionen, wie etwa der Vertraulichkeit und Integrität. Diese Kategorien dem Verantwortungsbereich des Informationsschutzes, eine in vielen Unternehmen in funktionaler und operationeller Hinsicht getrennte Domänen (Wolf und Goeken 2010: 239). Investitionen und Anstrengungen zur Anpassung der unternehmensinternen Steuerung geschäftsgefährdenden Risiken sind daher aus intrinsischen Gründen der Selbsterhaltung notwendig.[443] Auch die Rolle von Prozessen und ihrer systemischen Anschlussoperationen für Organisationen sollte Teil eines gesamtheitlichen, integrativen Ansatzes zur Risikokontrolle sein, um die Sicherheitsproduktion in Unternehmen zu gewährleisten. Die Ausgestaltung eines solchen Systems werden wir im folgenden Abschnitt nun detailliert besprechen und ebenfalls den Prozess der Abwägung zwischen Investition und Ertrag im Sinne der resilienten Organisation thematisieren.

7.2. Integrativer Risikokontrollansatz

Unsere vorausgehende Untersuchung zeigte, dass die Risikokontrolle im Informationszeitalter einerseits die Kontinuität von Prozessen und Kommunikation aufrechterhalten muss und andererseits die Methoden und Elemente der Anwendungspraktiken ausdehnen sollte, um den Sicherheitsdispositiven gerecht zu werden. Diese in Unternehmen als Resilienz verstandene Form der Risikokontrolle übersetzt sich in der Praxis in ein integratives Risikokontrollsystem, welches den ehemals objektbezogenen Risikobegriff durch einen neuen, an Prozessen und Kommunikationskontinuität orientierten Ansatz ersetzt. Diese zentrale Schlussfolgerung der ethnographischen Beobachtung zeigte sich während des Untersuchungszeitraums von 2012 bis 2022 durch die Verschiebung des zuvor artikulierten Risikodiskurses. Zu beobachten war die

[442] APT steht für Advanced Persistent Threat und umschreibt eine technisch anspruchsvolle, häufig wiederholte Angriffswelle gegen die Firewall eines Systems in der Hoffnung, eine Schwachstelle auszumachen und nutzen zu können (Cavelty 2013: 112).

[443] Die Einführung geeigneter Maßnahmen zum Schutz der Unternehmenswerte gilt als „(…) Grundbedingung für das Gelingen der Digitalisierung“ und somit als wesentlicher Bestandteil des Konzeptes, da ein Großteil der zu schützenden Werte eines Unternehmens mit Informationen assoziiert ist (Weber 2016: 33). Neben der intrinsischen Motivation zur Kontinuitätsplanung sind zudem Anforderungen von Erst- und Rückversicherungen, regulatorische Bedingungen zum Erhalt einer Lizenz und wachsender Ausführungsspezifika, welche sich aus den Anforderungen von Geschäftspartnern und Industrieverbänden ableiten (Khan und Sepúlveda 2015: 9).

Neuausrichtung der Vorsorgeplanung und die Haltung von Experten der Unternehmenszentrale, welche in Hintergrundgesprächen die Erweiterung des Risikobegriffs artikulierten.[444] Dies wurde insbesondere anhand der zunehmend holistisch verstandenen Betrachtung der Schutzziele und der Komponenten eines nun als Gesamtbild interpretierten Systems kritischer Prozesse deutlich.[445] Dies bedeutete konkret, dass die Abstimmung zwischen den Fachfunktionen, insbesondere seit der Corona-Pandemie, häufiger und enger stattfand.[446] Insbesondere das Zusammenwirken von Prozessen und IT-Anwendungen wurde gründlicher untersucht, welche in Form von ITSCM-Strategien vom Betriebsvorstand (COO) abgezeichnet werden mussten.[447] Diese Formalisierung der Vorsorgeplanung begründete auf der Grundlage der hier vorliegenden Hintergrundgespräche den Beginn eines neuen Risikokontrollsystems, welches die Vorsorgeplanung im beobachteten Fall durch einen ganzheitlichen Ansatz erstmals auf alle drei Schutzziele des Informationszeitalters bezog. Diese Schutzziele wurden durch die Anwendungspraktiken des BCM, KM, und Informationsschutz repräsentiert und durch neue Vorgaben unter dem Überbegriff Resilienz standardisiert. In anderen Worten, die Essenz der resilienten Organisation reflektierte den Wert der verwalteten Informationen in einem integrativen Ansatz zur umfassenden Sicherstellung ihrer Verfügbarkeit, Vertraulichkeit und Integrität und verhalf damit der Steuerung von

[444] Ein Experte schilderte die Notwendigkeit zur adaptiven Einbeziehung anderer Funktionen in ein einheitliches Kontrollsystems, da ansonsten die Effektivität der einzelnen Anwendungspraktiken nicht die Komplexität der Cyberbedrohungen und der damit verbundenen Kommunikationsabbrüche bewältigen könne. Insbesondere wurde hervorgehoben, dass Vorfälle wie Log4j oder der gestiegenen Zahl an Ransomware-Angriffen die Selbstbetrachtung der Organisation herausforderten und ein holistisches Bild auf die Risikkokontrollen notwendig sei (Hintergrundgespräch 13.12.2021).

[445] Im Gespräch mit Vertretern der IT, erzählte ein erfahrener IT-Architekt, dass die Zusammenlegung von Rechenzentren die Risikoexposition vergrößere, falls nicht ausreichende Maßnahmen zum umfänglichen Schutz der Infrastruktur, Middleware und Software vorgenommen werden würde. Dabei bezog er sich auf die Notwendigkeit Wiederherstellungspläne nicht nur auf der Ebene von einzelnen Komponenten zu erstellen, sondern die Komplexität eines großflächigen Desasters („disaster event“) durch entsprechende Master-Pläne für alle im Rechenzentrum verwalteten Systeme abzudecken. Dieses Vorgehen wurde schließlich 2020 als verpflichtender Standard eingeführt, der über die Rechenzentren hinaus, auch die Geschäftsfortführungspläne in die Planung miteinbezog und dadurch zur resilienten Organisation durch flexible Vorbereitung beitrug (Hintergrundgespräch 27.10.2022).

[446] Während der Corona-Pandemie wurde ein ständiger Krisenstab eingerichtet, welcher der am längsten aktive Krisenstab der Unternehmensgeschichte wurde. Die Einbindung von Fachfunktionen in den „gemeinsamen Krisenstab“ führte anfangs zu Abstimmungsschwierigkeiten, etablierte aber bald eine hilfreiche Steuerung der Krisenaktivitäten durch Einbindung von BCM und ITSCM zur Sicherstellung der Prozesskontinuität, Kommunikation- und Krisenmanagement zur Steuerung der Aktivitäten und Informationsschutz, um die fortschreitende Virtualisierung von Daten und Prozessen abzusichern (Hintergrundgespräch 26.11.2020).

[447] Die formelle Berichtslinie an den Vorstand für die neu geschaffene „Resilienz-Funktion“ sowie die Einführung von formalisierten Strategien und Dokumenten standardisierte die Risikokontrolle aus Sicht der Experten deutlich, allerdings auch die Arbeitsaufwände. Die Erstellung einer ITSCM-Strategie für eine einzelne IT-Anwendung konnte bis zu zehn Tage in Anspruch nehmen und bedeutete im Licht von einem geschätzten Gesamtbestand von 20.000 Systemen, wenn auch nicht alle kritisch waren, einen signifikante Aufwand für die Organisation (Workshop 18.02.2019).

geschäftsgefährdenden Risiken als ganzheitliches Konzept über traditionelle funktionale Trennelemente innerhalb der Organisation hinweg.

Im Folgenden wollen wir diese Erkenntnis aus der ethnographischen Untersuchung auf die Erstellung eines allgemeinen Risikokontrollsystems beziehen und die relevanten Elemente analysieren. Ein solches Risikokontrollsystem basiert aufbauend aus den zurückliegenden Schlussfolgerungen auf der Definition und Überprüfung von Risikokontrollen, welche im Unternehmen bestimmt und anschließend in regelmäßigen Zyklen dokumentiert werden. Die hier relevanten Risikokontrollen vereinen dazu Anforderungen aus mehreren Fachfunktionen des Unternehmens. Das traditionelle Risikomanagement, die zweite Instanz des organisationsinternen Risikokontrollsystems (Luburić 2017: 31), inkludiert Kontrollen der (1) Rechts- und Compliance-Funktionen, sowie aus dem Bereich des Geheimnisschutzes.[448] Darüber hinaus sind Aspekte des (2) Datenschutzes, insbesondere des Schutzes sensibler, personenbezogener Daten zu nennen, sowie physische Aspekte der Sicherheit wie Zugangskontrollen[449] und des analogen Informationsschutzes miteinzubeziehen (Braes und Brooks 2010: 17). Ferner sind Kontrollen aus den Bereichen (3) Business Continuity Management, (4) Krisenmanagement und (5) Incident Management relevant, deren Anforderungen die Implementierung von präventiven und reaktiven Schutzmaßnahmen anlog zu den jeweiligen Lifecycle-Schritten der entsprechenden internationalen Industriestandards enthalten sollten (vgl. ISO 22301; ISO 22302). Darüber hinaus sind Kontrollen aus dem (6) Informationsschutz einzubeziehen, deren Implementierung und Überwachung die Vertraulichkeit und Integrität von Daten zum Schwerpunkt haben (Schermann und Krcmar 2010: 227).[450]

Dem sollten sich ebenfalls Anforderungen aus dem Bereich des (7) ITSCM anschließen, welche ausgewählte Kontrollen der (8) IT-Governance und IT-Architekturmanagements einerseits und der IT-Sicherheit (9) andererseits voraussetzen, um eine verlässliche Planung der IT-

[448] Der Geheimnisschutz ist eine Untergruppe der Informationssicherheit und definiert technische und nicht-technische Ansätze zur Sicherstellung der Vertraulichkeit von sensiblen strategischen Dokumenten in einem Unternehmen (Braes und Brooks 2010: 17).
[449] Der Schutz der Vertraulichkeit von Informationen ist nicht nur zur Vermeidung eines Reputationsschadens und einhergehenden Vertrauensverlusts in das Unternehmen zu verstehen, sondern auch vor dem Hintergrund strenger Anforderungen der Regulatoren zum Datenschutz und den daraus folgenden Sorgsamkeitspflichten des verarbeitenden Unternehmens (vgl. Gaycken und Karger 2011). Die Wertdisposition der Informationen eines Unternehmens umfasst neben den Geschäftsgeheimnissen wie etwa Strategiepapieren oder Algorithmen und Technologien auch die sensitiven Daten von Mitarbeitern, Geschäftspartnern oder Kunden.
[449] Der Schutz der Vertraulichkeit von Informationen ist nicht nur zur Vermeidung
[450] Dazu sind auch Aspekte des Dokumentenmanagements und Outsourcing relevant, deren Anforderungen die Verfügbarkeit von Ressourcen und den Informationsschutz von an Dritte übermittelte Daten berücksichtigen (Schwering 2010: 231).

Wiederherstellung sicherzustellen (Walser und Riedl 2010: 254). Der Aspekt der (10) physikalischen Sicherheit und des analogen Informationsschutzes sind mit Blick auf beispielsweise Identitätsdiebstahl und Social Engineering relevant, da die Einbeziehung physikalischer Schutzvorkehrungen das Unternehmen vor Schaden bewahren können. Dazu zählen Kontrollen zur Zugangssteuerung, Liegenschaftsschutz oder bautechnischer Aspekte wie dem Feuerschutz oder Notfallmanagement. Die Zusammenführung von Kontrollen aus den genannten Funktionen kann einen holistischen Kontrollansatz ermöglichen, welcher in der Etablierung geeigneter präventiver und reaktiver Maßnahmen zum Schutz der unternehmensrelevanten Werte resultiert.

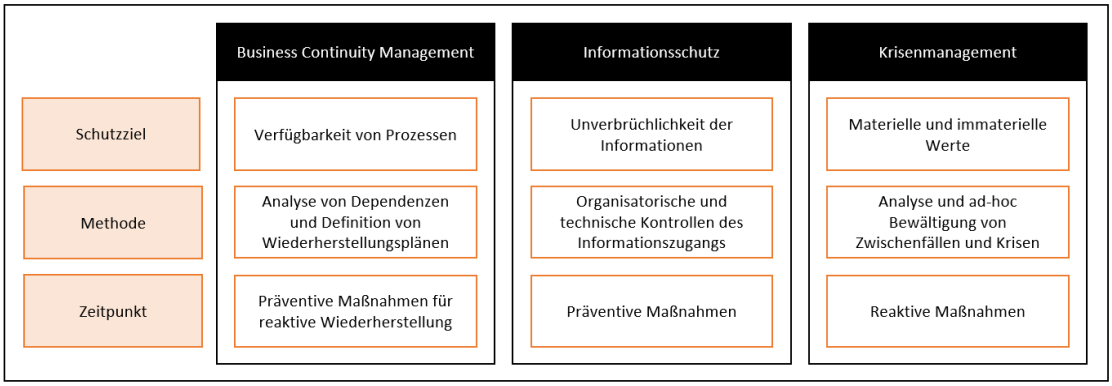

Abb. 7.1. Ziele und methodische Ausrichtung von BCM, KM und Informationsschutz. Eigene Darstellung.

Im Folgenden wollen wir die Bestandteile dieses integrativen Konzeptes eines Risikokontrollsystems vorstellen, an dessen Ende die resiliente Organisation in die Lage versetzt sein wird, eine effektive Risikomitigation unter den Bedingungen der Unsicherheit leisten zu können. Die Herausforderung eines solchen integrativen Ansatzes liegt in der funktionalen Differenzierung von Kontrollverantwortlichkeiten innerhalb von Unternehmen (vgl. IIA 2013). Die Zusammenführung der unterschiedlichen Anforderungen wird daher nicht über eine funktionale Umstrukturierung von Steuerungsfunktionen in Unternehmen umzusetzen sein, sondern sich einer alternativen Herangehensweise bedienen müssen.[451] Diese Aufgabe sollen Kernkontrollen und spezifische Anforderungen aus weiterhin fachlich abgegrenzten Funktionen übernehmen, welche entlang eines abgestimmten Schutzzieles

[451] Ein historischer Entwicklungshintergrund kann als vorrangige Erklärung für diese partikuläre Struktur genannt werden, aber auch das Fehlen eines kollektiven, von allen Mitgliedern akzeptierten Gedächtnisses, welche die in einem Bereich beschlossenen Entscheidungen in anderen Bereichen reflektieren und gemeinhin zur Akzeptanz beitragen. Karrieremodelle, Ressourcenknappheit und individuelle Verhaltensmuster von Entscheidern und Subentitäten der Organisation tragen ebenfalls ihren Teil zu einer Segmentierung der beteiligten Funktionen bei. Selbst im Bereich des Informationsschutzes treten artverwandte, aber funktionell separierte Bereiche wie der Datenschutz, IT-Sicherheit oder Zugangskontrolle in Erscheinung, deren strukturelle, organisatorische und schließlich inhaltliche Harmonisierung hinsichtlich einer ernsthaften, konsequenten und auf effektive Risikomitigation ausgerichteten Strategie des Unternehmens notwendig ist.

entwickelt werden. Dieses Modell basiert weiterhin auf dem dreistufigen Modell aus (a) Fachfunktionen, (b) Risikomanagement und (c) internes Audit (Luburić 2017: 31), welches aus dem analogen Zeitalter bekannt ist. Die Fachfunktionen definieren Risikokontrollen sowie spezifische Anforderungen, welche allerdings anhand der strategischen Schutzwerte des Risikomanagements ausgerichtet sind. Die Angleichung der relevanten Kontrollen an eine risikogeleitete Schutzstrategie bietet den Vorteil, dass die individuelle Risikoexposition und Akzeptanz reflektiert werden kann und es unterschiedliche Prioritäten ermöglicht. Von zentraler Bedeutung sind zudem die Zusammenführung der Kontrollen und deren Überprüfung in einem einheitlichen Berichtsrahmenwerk, welches den Entscheidungsträgern des Unternehmens eine harmonisierte, nach abgestimmten Parametern definierte Übersicht der Maßnahmen und deren Fortschritt aufzeigt. Das daraus entwickelte Reifegradmodell eines Unternehmens kann als Gradmesser dienen, um die Weiterentwicklung zu dokumentieren und Schwachstellen beziehungsweise das Ausmaß der Unsicherheit zu bestimmen.

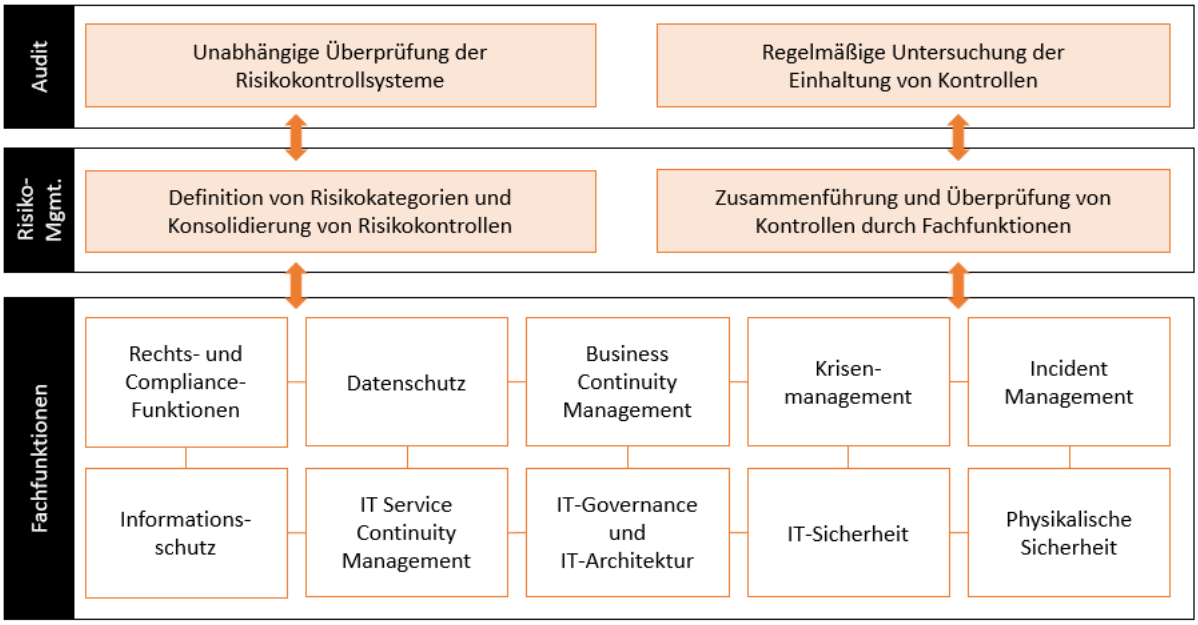

Abb. 7.2. Risikokontrollsystem im Informationszeitalter. Eigene Darstellung.

Die oben dargestellten Funktionen und Ebenen eines Kontrollsystems bilden die inhaltliche und funktionale Vorgehensweise ab, aus denen sich eine resiliente Organisation zusammensetzt und woran ihre Fähigkeit zur Absorption der Unsicherheit zu messen ist. Daraus ergibt sich nach unserer Schlussfolgerung ein neues Prozessmodell zur Sicherheitsproduktion in Unternehmen. Dieses Modell beruht auf den Erkenntnissen der ethnographischen Beobachtung und den Gesprächen mit Experten aus den unterschiedlichen Fachfunktionen. Die nun folgende idealtypische Prozessbeschreibung beruht auf den Ergebnissen unserer beobachtenden Teilnahme und der Schlussfolgerungen hinsichtlich eines normativen Modells zur Umsetzung

eines neuen, prozess-orientierten Risikokontrollsystems, das mithilfe von Resilienz die Sicherheitsproduktion in Unternehmen lenkt und die Kontinuität von Prozessen und Kommunikation durch einen umfassenden Risikokontrollansatz sicherstellt. Aus unserer Sicht sollte daher ein solcher integrativer Ansatz die Kontrollen der unterschiedlichen Funktionsbereiche in einen fünfstufigen Prozesszyklus verbinden. Dieser umfasst die Kernkontrollen aus den Phasen der (1) Kritikalitäts- und Risikoanalyse, (2) die Ressourcenerfassung, (3) Strategieformulierung, (4) Plandefinition und Testen sowie die (5) Planaktivierung und das aktiven Krisenmanagement. Anhand dieses Prozesses wollen wir im Folgenden die Umsetzung von Resilienz in Unternehmen mit dem Ziel der der effizienten Risikosteuerung im Informationszeitalter praktisch aufzeigen.

7.2.1. Kritikalitäts- und Risikoanalyse

Ausgehend vom übergeordneten Ziel einen Prozess- und Kommunikationsabbruch zu vermeiden, beginnt der erste Schritt des integrativen Ansatzes mit der initialen Identifikation der kritischen Prozesse durch die (1) Kritikalitätsanalyse oder „Business Impact Analysis“ (BIA). In diesem Schritt werden wie im ursprünglichen Modell des BCM die Prozesse des Unternehmens einer Prüfung unterzogen und die Konsequenzen ihrer Unterbrechung für das gesamte Unternehmen ermittelt. Zur Erinnerung, die BIA betrachtet den Schaden eines Prozessausfalls, ohne jedoch Maßnahmen zur Reduktion des Schadens bereits miteinzubeziehen. Das bedeutet, dass die Bewertung der Unterbrechung ohne inhärente Alternativmaßnahmen oder Reaktionen seitens des Unternehmens erfolgen sollte, um das originäre Schadenspotentials des Prozessausfalls ermitteln zu können.[452] Die Bewertung der Prozesse sollte für das gesamte Unternehmen durchgeführt werden und alle vier Schadenskategorien berücksichtigen. Dies umfasst die quantitative Dimension des finanziellen Verlustes durch den Prozessausfalls, welcher beispielsweise im Vertrieb besonders deutlich zum Tragen kommt. Ferner sind die drei qualitativen Kategorien zu berücksichtigen, deren Fokus auf den operationellen oder regulatorischen Konsequenzen liegt und zudem den möglichen Reputationsschaden durch einen Ausfall in die Bewertung einbezieht. Diesen möglichen Schadenswert wird anschließend das zeitliche Wiederherstellungsziel gegenübergestellt.

[452] Ein Beispiel wäre die Bewertung der Personalverwaltung als Prozess. Eine der Aktivitäten dieses Prozesses ist die Gehaltsauszahlung an die Mitarbeiter. Ein Ausfall des Prozesses wird häufig durch die Möglichkeit einer Anweisung an die ausführende Bank zur Gehaltsfortzahlung als unkritisch angesehen. Doch der originäre Schadenswert wird durch diese Betrachtung nicht reflektiert, da eine Mitigation bereits in die BIA einbezogen wird.

Das Wiederherstellungsziel wird als Recovery Time Objective (RTO) bezeichnet und definiert die Zeit bis zur spätmöglichsten Wiederherstellung der minimal akzeptierbaren Performanz der wichtigsten Prozessleistung.[453] Die Kombination aus Schadenswert und RTO bestimmt gemeinsam die Kritikalität eines Prozesses. Vertretbare Kritikalitätsgrenzwerte sollten aus der Erfahrung von Unternehmen individuell und unter Berücksichtigung der jeweiligen Risikoexposition für alle Prozesse definiert werden. Eine etablierte Größe zur Bestimmung des Grenzwertes ist ein sehr hoher Schadenswert in Verbindung mit einer RTO von bis zu einer Woche.[454] Dies bedeutet, dass alle Prozesse, deren Kritikalität über diesem Wert liegen für eine weitere Vorsorgeplanung in Frage kommen. Im Umkehrschluss folgt daraus auch, dass alle Prozesse mit einem niedrigen Schadenswert oder einer RTO von mehr als einer Woche als unkritisch angesehen werden und für die primäre Wiederherstellung ausgeklammert werden können. Der ursprüngliche Zweck der BIA ist es diejenigen Prozesse aus der Masse der im Normalzustand durchgeführten Prozesse zu identifizieren, deren Ausfall eine entscheidende, das heißt kritische Konsequenz für das Unternehmen bedeuten würde und sich unter dem Gesichtspunkt begrenzter Ressourcen[455] für eine priorisierte Wiederherstellung, beziehungsweise proaktiven Schutz qualifizieren (Sahebjamnia, Torabi und Mansouri 2015: 265). Kritische Prozesse[456] werden durch die BIA für die weiteren Vorsorgeplanungen innerhalb des BCM und ITSCM[457] berücksichtigt.

[453] In der Literatur findet sich zudem der Wert der „maximal tolerable period of disruption“ (MTPD), welche die maximale Zeit reflektiert, bis zu der sich der entstehende Schaden zu einer nicht mehr akzeptierbaren Größe akkumuliert. Die RTO beziffert im Gegenzug den Zeitpunkt bis zu dem der Wiederherstellungsprozess initiiert beziehungsweise abgeschlossen sein muss, um den prognostizierten Schaden abzuwenden (Torabi, Soufi und Sahebjamnia 2014: 313).

[454] Diese Verbindung reflektiert einerseits den Schaden, welcher sich in anhaltender, internationaler Kritik von Medien oder Kundenverbänden am Unternehmen, finanziellen Belastungen von mehr als 10-15 Prozent des Jahresumsatzes, erheblicher Qualitätseinbußen des Kundenservice, einer signifikanten Veränderung des Börsenwerts oder einer negativen Bewertung durch Investoren und Analysten ausdrücken kann. Die RTO definiert andererseits die Zeit des Prozessausfalls, innerhalb derer dieser Schaden auftreten kann und Wiederherstellungsmaßnahmen nicht ad hoc zu leisten wären. Daher unterliegen Prozesse innerhalb dieser Kritikalitätsdefinition der Notwendigkeit zur Vorsorgeplanung.

[455] Die Aufgabe der BIA ist folglich eine Filterung der Gesamtzahl an Prozessen durch eine standardisierte und an vergleichbaren Kriterien ausgerichtete Bewertung. Diese Selektion ist notwendig, da die Vorsorgeaufwände des Unternehmens durch die natürliche Ressourcenknappheit eines kompetitiven Umfeldes einerseits und der Exklusivität spezifischer Ressourcen wie Informationen andererseits strategisch begrenzt sind (Karim 2011: 183).

[456] Unkritische Prozesse werden hingegen aus dem weiteren Vorgehen exkludiert und nur durch die regelmäßigen Überprüfungen der BIA auf eine veränderte Kritikalität hin erneut betrachtet. Falls sich keine Änderungen, beispielsweise in quantitativer oder qualitativer Hinsicht oder durch organisatorische Umstrukturierungen ergeben haben, bleiben nur die kritischen Prozesse im Fokus der weiteren Schritte.

[457] Kritische Prozesse stellen Anforderungen an vier Kernressourcen und darüber hinaus spezifische Erfordernisse zur Wiederherstellung im Notbetrieb an Informationen. Die speziellen Wiederherstellungsprioritäten und Abläufe der komplexen IT-Ressource werden vom ITSCM abgedeckt und sind daher an dieser Stelle zu dokumentieren (Ernest und Nisavic 2007: 387).

Die Limitation von Ressourcen wie Rechenzentren, redundanten Servern oder alternativen Arbeitsplätzen durch die fortwährende ökonomische Rationalität führt aber auch in dem hier vorgeschlagenen Modell zur Notwendigkeit der Priorisierung für eine geplante Wiederherstellung von Prozessen anhand der Kritikalitätsanalyse. Dabei gilt zu beachten, dass Prozesse nicht von selbst ihre Unterbrechung verursachen, sondern aufgrund einer Nichtverfügbarkeit ihrer Ressourcen gezwungen sind auf alternative Maßnahmen oder Technologien zurückzugreifen. Diese Ressourcen werden in vier Bereiche eingeteilt. Neben der (a) Informationstechnologe zählen dazu auch die (b) Verfügbarkeit des Personals dazu, welche auch trotz der zunehmenden Automatisierung und Robotisierung der Betriebe eine essentielle Notwendigkeit für die Aufrechterhaltung der Geschäftsprozesse darstellt. Des Weiteren sind (c) Gebäude für die Produktion von Gütern oder Bereitstellung von Dienstleistungen bedeutsam und auch die Abhängigkeit von (d) Dienstleistern wird im Rahmen der globalisierten Outsourcing- und Offshoring-Wirtschaft zunehmend wichtiger.[458]

Daraus resultiert auch die Bewertung der potentiell gefährdeten Schutzziele im Rahmen der (2) Risikoanalyse, welche als „Risk Identification and Assessment" (RIA) bezeichnet werden kann. Da der Ausfall von Ressourcen eine Prozessunterbrechung verursachen kann, werden Faktoren identifiziert, welche helfen können das Risiko einer Nicht-Verfügbarkeit von Ressourcen zu bestimmen. Dieser Prozessschritt bezieht dabei die Dimensionen der Risikokategorien, Schadenswirkung und Wahrscheinlichkeit eines Eintretens in die Bewertung ein. An diesem Punkt bietet sich eine Differenzierung entlang der unterschiedlichen Risikokategorien an. Für bekannte Kategorien kann auf der Basis vergangener Fallzahlen eine Schadens- und Wahrscheinlichkeitsschätzung abgegeben werden, welche verhältnismäßig verlässliche Ergebnisse zur Prädiktion der zukünftigen Entwicklung erlauben. Als solche Kategorien sind das natürliche, politische und gesundheitliche Risiko zu nennen, auch wenn spezifische oder neue Gefahren auch in diesen Gruppen aufgrund fehlender Empirie zur Unsicherheit beitragen können.[459] Ein gänzlich anderes Bild bietet sich jedoch durch technologische Risiken und insbesondere im Fall der Digitalisierung, welche zwar auf den ersten Blick nur eine Untergruppe aller relevanten Risiken für ein Unternehmen darstellen (Wolf und Goeken 2010:

[458] Eine Limitation der verfügbaren Ressourcen bedeutet folglich, dass redundante Investitionen in Gebäude, Mitarbeiter oder IT-Hardware nicht der ökonomischen Gewinnorientierung des Wirtschaftssystems entsprechen, wenn sie nur der Vorhaltung für einen Notfall dienen und daher als Reserve nur für die vitalen Prozesse des Unternehmens als präventive Maßnahme berücksichtigt werden können (Nijaz und Moon 2009: 77).

[459] Ungewöhnliche Wetterphänomene als Folge des Klimawandels, neue politische Konstellationen oder erst kürzlich entdeckte Krankheitserreger können trotz großer Datenmengen für die restlichen Gefahren innerhalb der jeweiligen Risikokategorie die Unsicherheit für diese spezifischen Fälle vergrößern.

239), aber durch ihr bisher nur im Ansatz erfasstes Schadenspotential mit einem Alleinstellungsmerkmal ausgestattet sind.

Der Kerngedanke der Risikobewertung liegt in der Identifizierung von Schwachstellen, also der Bereiche in denen eine Ressource besonders anfällig für Unterbrechungen des Gesamtprozesses sein könnte und daher eine signifikante Ursache für eine Geschäftsunterbrechung darstellt.[460] Als Konsequenz können strategisch begrenzte Ressourcen bewusst für priorisierte Ziele anhand ihres Ausfallrisikos eingesetzt werden. Auf dieser Grundlage können auch Krisenszenarien entwickelt werden, welche durch spezifische Krisenpläne abgedeckt werden, um im Fall ihres Eintretens unmittelbare Schritte einleiten zu können. Durch diese Analyse können folglich spezifische Szenarien vorbereitet werden, welche eventuell nicht berücksichtigt werden würden, wenn deren Eintreten beispielsweise keinen Einfluss auf die Ressourcenverfügbarkeit hätten (Reputationskrise, Compliance-Fall, Datenverlust). Zudem spielen die ökonomische Rationalität des traditionellen Risikoverständnisses, bestehend aus den Variablen Schaden und Eintrittswahrscheinlichkeit immer noch eine Rolle für Entscheidungsträger (Cavelty 2013: 116), insbesondere im Fall von ungewohnten, nicht routinierten Entscheidungen über exogene Risiken. Demnach verfolgt die Risikoanalyse auch den Zweck, relevante Risiken einem unternehmensinternen Diskurs zuzuführen und in einem Aushandlungsprozess zu einem konsensfähigen Ergebnis über die spezifische, zumeist lokal-verortete Risikoexposition zu gelangen.

Dieser Aspekt bringt erneut den Aspekt von Räumlichkeit in die Diskussion ein. Bestimmte klimatische Phänomene wie Taifune, politische Determinanten wie das Enteignungsrisiko in einem Gastland oder die örtliche Kriminalitätsrate, sind eindeutig begrenzter, lokaler Natur. Auf der anderen Seite resultieren Entkoppelungsprozesse wie die Internationalisierung von Märkten und Produktionsketten oder die Digitalisierung in einem transnationalen Wirkungszusammenhang.[461] Dies zeigt sich beispielsweise in Gestalt von internationalen Konflikten, dem Klimawandel, Folgeerscheinungen technologischer Risiken wie Betriebsunfällen in Atomkraftwerken oder Chemiefabriken, oder der Corona-Pandemie um nur eine Auswahl zu nennen. Im Zuge der Digitalisierung spitzte sich dieser Prozess weiter zu, da

[460] Ein Rechenzentrum in einer Erdbebenregion ist von einem höheren Ausfallrisiko gekennzeichnet als eine vergleichbare Einrichtung in einer tektonisch inaktiven Region. Die Verfügbarkeit von Daten kann in Ländern mit besonderen Datenschutzregelungen oder Sicherheitsauflagen wie im US-amerikanischen respektive chinesischen Beispiel Einschränkungen unterliegen und aufgrund politischer Entscheidungen einem Ausfallrisiko unterliegen.
[461] Die Rolle des lokalen Aspekts einer Ressource ist ebenfalls nicht zu unterschätzen, da sich die meisten Risikokategorien entlang einer mentalen Karte der räumlichen Risikoexposition bewegen. Natürliche oder politische Risiken werden häufig einem lokalen Wirkungskreis zugeschrieben, globale Wirkungsketten jedoch vernachlässigt.

wesentliche Elemente der digitalen Risikoexposition losgelöst vom physikalischen Standort einer Ressource zu betrachten sind (Pauli, Schermann und Krcmar 2010: 259). Schadprogramme, Spionageversuche oder Wirkungsketten von Softwarefehlern sind als globale Risiken zu betrachten und über den Anschluss an das Internet der lokalen Begrenzung entzogen, während Hardwareelemente wie Rechenzentren, Glasfaserkabel oder Endgeräte hingegen an einem Standort lokalisierbar sind (Bratton 2015: 29). Folglich obliegt dem Schritt der Risikoanalyse stets die Aufgabe, Entscheidungsträger von der Risikoexposition einer Ressource zu überzeugen und dabei insbesondere die schwindende Bedeutung der lokalen Positionierung des Risikoobjekts zu betonen.

Eine weitere Herausforderung liegt in der Fähigkeit des Unternehmens die unterschiedlichen Risikokategorien und Bewertungsmethoden erstens miteinander in Verbindung zu bringen und zweitens auf die Gesamtheit des Unternehmens zu beziehen (Pauli, Schermann und Krcmar 2010: 227). Eine ganzheitliche Risikobewertung sollte daher globale Risiken, wie etwa Cyberrisiken standardisieren und im Falle eines hierarchischen Organisationsmodelles der lokalen Entität zur Überprüfung und Zustimmung vorlegen.[462] Denn auch vorrangig lokale Schadensereignisse sollten im Rahmen des gleichen standardisierten Prozesses durchgeführt werden, allerdings unter Federführung der lokalen Verantwortlichen und Beachtung relevanter Faktoren in der räumlichen, rechtlichen oder sozialen Umgebung des Ressourcenstandortes.[463]

Die globale Risikodimension der Cyberrisiken zeigt zudem die Notwendigkeit zur Inklusion von Informationen als (e) fünfte Kernressource in die Risikoanalyse, welche zudem in der nachfolgenden Ressourcenidentifikation Eingang finden sollte. Informationen umfassen sowohl elektronisch als auch analog gespeicherte und bearbeitete Daten. Die Ressource umfasst die für die kritischen Geschäftsprozesse benötigten Grundlagen wie Datenbanken oder Kontoinformationen, aber auch die Dokumentation von formellen und informellen Prozessen, also in anderen Worten die Gesamtheit des Wissensbestandes eines Unternehmens. Mit der steigenden Zentralisierung dieser Informationen in einem virtuellen Gedächtnis auf der

[462] Eine Besonderheit der Cyberrisiken ist die relative Unsicherheit über mögliche Gefahren und die Beschränkung auf vergleichbare Schadensfälle aus der jüngeren Vergangenheit. Die Berechnung der Risikowerte basiert häufig auf der Summierung individueller Schadenserwartungen, ohne jedoch eine ganzheitliche Betrachtung einzubeziehen. Zusätzlich korreliert der relative Mangel an Daten mit der Subjektivität der Einschätzung: „For example, individual vulnerability scores tend to be subjective and potentially inaccurate; simple sums do not consider how vulnerabilities are distributed over hosts or over time" (Linkov et. al. 2013: 472). Standardisierte Risikobewertungen mit vorgegebenen Werten können die globale Natur der Bedrohung berücksichtigen und der subjektiven Bewertung eine zentral gesammelte und ausgewertete Risikomatrix zur Seite stellen, um die Risikoexposition besser bewerten zu können.

[463] Eine Gewissheit, deren Aussagekraft sich in der Marktkapitalisierung von informationsverarbeitenden Unternehmen wiederspiegelt (Choo, Smith und McCusker 2007: 2).

Grundlage von digitalen Strukturen gewinnt die Informationsressource zunehmend einen IT-bezogenen Schwerpunkt. Dennoch sollte die analoge Komponente des notwendigen Wissensbestandes nicht übersehen werden, wenn die Risikobewertung und Ressourcenplanung von Informationen durchgeführt wird. Die Bestimmung des Risikos für die Verfügbarkeit von Ressourcen reicht allerdings mit Blick auf eine resiliente Organisation nicht aus, da ebenfalls die Aspekte der Vertraulichkeit und Integrität berücksichtigt werden müssen. Mit Blick auf den Schutz von Informationen zeigt sich, dass die übergreifende Schnittstelle zwischen nicht-technischen Risikokategorien und den Cyberrisiken in vielen Unternehmen ein Beispiel für Optimierungsbedarf darstellt (Wolf und Goeken 2010: 239). Dies liegt auch an der unzureichend klar artikulierten Verantwortung für IT-Ressourcen, welche zwischen Geschäfts- und IT-Funktionen verortet werden (Walser und Riedl 2010: 258). Da jedes Risikokontrollsystem von der eindeutigen Benennung von Verantwortlichkeiten abhängt, wird die Zuweisung einer Risikoträgerschaft eine Vorbedingung zur effektiven Adressierung von potentiellen Risiken sein. Wie im Fall der Evaluation von Informationen gilt dies auch für die anderen Risikokategorien und Ressourcen.

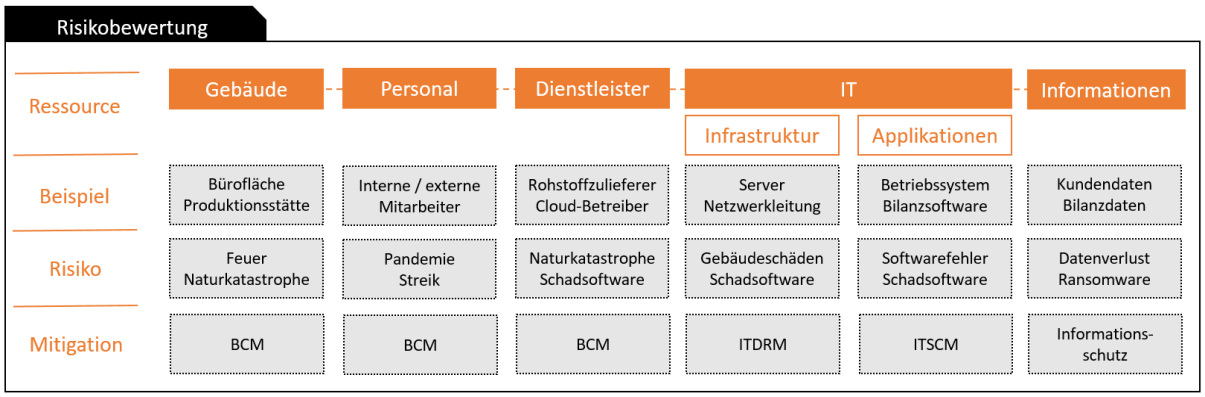

Abb. 7.3. Risikobewertung der Ressourcen und Ermittlung der Mitigation. Eigene Darstellung.

Zusammenfassend kann die Bedeutung beider Prozessschritte durch die Erstellung einer essentiellen Informationsgrundlage für die nachfolgende Ressourcendefinition und Strategieformulierung erklärt werden. Daraus folgen die Kernkontrollen, welche die Durchführung und Dokumentation von BIA und RIA beinhalten, ferner die materielle Überprüfung der vier Schadenskategorien für den mögliche Unterbrechung von Prozessen, sowie die einheitliche Kategorisierung der Kritikalitätsdefinition über das gesamte Unternehmen einschließen. Dazu sind auch die Schadenshöhe, RTO und RPO zu vergleichen und Standards für das gesamte Unternehmen zum Zweck der Vergleichbarkeit zu erstellen. Die BIA sollte ferner die Verfügbarkeit von fünf Ressourcen, einschließlich der Informationen sicherstellen, deren Relevanz als spezifische Schutzziele für das Unternehmen durch die

Informationsevaluation als standardisierten Prozess abgedeckt werden kann. Die RIA sollte zudem die wichtigsten geschäftsgefährdenden Risiken auf globaler und der lokalen Ebene der Ressourcenstandorte erfassen und spezifische Krisenszenarios definieren. Die Risikobewertung sollte zu diesem Zweck auch Aspekte des Datenschutzes und der physikalischen Sicherheit einschließen, um ein ganzheitliches Risikobild zu entwickeln. Ferner sind mit Blick auf die Relevanz von Informationen die Datenvertraulichkeit und Integrität über eine Verwundbarkeitsüberprüfung von IT-Systemen seitens des Informations- und Datenschutzes durchführen, zum Beispiel in Form von Penetrationstests. Abschließend sind die Ergebnisse der BIA und RIA durch Entscheidungsträger des Unternehmens[464] zu bestätigen und an die Risikomanagementfunktion zu übermitteln. Diese Kernkontrollen der Phase Kritikalitäts- und Risikoanalyse erlauben die flächendeckende Evaluation der relevanten Schutzziele eines Unternehmens, ausgehend von den kritischen Anforderungen der Prozesskontinuität und der individuellen Risikoexposition eines Unternehmens.

7.2.2. Ressourcenerfassung

Im zweiten Prozessschritt ist zunächst die Quantifizierung und Zuweisung der für kritische Prozesse oder im Rahmen der RIA identifizierten Ressourcen durchzuführen. Beginnend mit den Ergebnissen der Kritikalitätsanalyse umfasst dies alle Ressourcen, die ein kritischer Prozess im Notbetrieb zur Erfüllung des definierten, minimalen Leistungsniveaus benötigt. Dazu ist es notwendig den exakten Ressourcenbedarf für einen Notfall zu konkretisieren und als Grundlage der nachfolgenden Strategiedefinition mit den Prozessverantwortlichen abzusprechen. Zu diesen Ressourcen gehören in den meisten Fällen Arbeitsplätze, Mitarbeiter, IT-Applikationen und Informationen. Ferner können interne und externe Dienstleister notwendig werden, um einen bestimmten Prozessoutput zu ermöglichen. Allerdings sollte mit Blick auf die ökonomische Rationalität und Kosten von Redundanz und Robustheit nur der essentielle Bestandteil der Ressourcen in der Wiederherstellungsplanung berücksichtigt werden. Ein Prozess wird analog zum Industriestandard im Notbetrieb mit etwa 40 Prozent der ursprünglichen Belegschaft planen können, indem nicht kritische Aktivitäten des Prozesses ausgesetzt werden. Da die Mitarbeiter auch Arbeitsplätze und Hardware für einen potentiellen Ausfall des Gebäudes benötigen, ist die Gesamtzahl der benötigten Mitarbeiter eine essentielle Kennziffer für die Kostenplanung der Risikokontrolle (Karim 2011: 183).[465]

[464] Für diese Rolle eigenen sich je nach organisatorischen Aufbau Mitglieder des Topmanagements wie CEO, COO oder CRO, deren Wissen um die allgemeine Geschäftsstrategie des Unternehmens, der relevanten Risiken und potentiellen Bereitschaft des Unternehmens Risiken zu akzeptieren oder zu mitigieren von Bedeutung ist.

[465] Die Anzahl der benötigten Mitarbeiter ist eine wichtige Kennziffer für die Investition in alternative Arbeitsplätze. Allerdings kann die Zahl der Arbeitsplätze und ihre Ausgestaltung mit der gewählten Strategie

Eine generelle Schwierigkeit liegt in der Artikulation der Minimalanforderungen, um Erwartungen und Anforderungen der verantwortlichen Prozesseigentümer an den definierten Mindestservicestandard und nicht an Performanzkennzahlen des Normalzustandes auszurichten. Während der ethnographischen Beobachtungen drückten einige Prozessverantwortlichen eine Sichtweise aus, welche die individuelle Priorisierung mit Blick auf die Benennung von Mindestanforderungen widerspiegelte. Die Sichtweise der hier befragten Prozessverantwortlichen stellte die Handlungsfähigkeit des jeweiligen Bereichs in den Vordergrund, während die Prozesskontinuität durch eine auf das Unternehmen bezogenen Ressourcendefinition sekundär verstanden wurde. Die Reduktion der Ressourcen im Notfall auf ein minimal-akzeptierbares Niveau wurde häufig mit der Begründung abgelehnt, dass ansonsten Sparmaßnahmen die aktuelle Ressourcenausstattung in Reaktion auf diese Entscheidung betreffen könnte. Zusätzlich können monetäre Anreize wie erfolgsabhängige Bonuszahlungen verstärkend auf die individuelle Perspektive wirken.[466] Daher sind standardisierte Erhebungsverfahren und Kennzahlen für jeden Prozess, sowie die Ausrichtung an einem kostenorientierten Planungsziel der verfügbaren Ressourcen hilfreich, um einen effizienten Mittelweg zwischen ökonomischer Rationalität und Sicherheitsdispositiv zu finden.[467]

Die Analyse kritischer Dienstleister orientiert sich ebenfalls an dem Gedanken, welche internen oder externen Zulieferer einen signifikanten Beitrag zum Prozessoutput beitragen. Dienstleister, die lediglich operative Aufgaben für das auslagernde Unternehmen ausführen, können suspendiert werden. Andere Dienstleister, die strategische oder in Bezug auf die Reputation des Unternehmens relevante Aufgaben wahrnehmen, sind hingegen kritischer Natur. Es ist daher zu eruieren, welche Folge ihr Ausfall für die Geschäftsfortführung haben könnte.[468] An dieser Stelle ist eine Erweiterung der traditionellen BCM-Methodik

variieren, beispielsweise indem Heimarbeits- oder Verdrängungsoptionen gewählt werden, wie im Folgenden Abschnitt gezeigt werden wird.

[466] Diese Erfahrung sammelte der Autor in zahlreichen BIA-Interviews. Es zeigte sich, dass die Kontextualisierung des holistischen Ansatzes und der individuellen Erwartungshaltung zielführend ist, um die Prozessverantwortlichen durch das Interview zu leiten. Während der ethnographischen Beobachtung zeigte sich zudem, dass viele Prozessverantwortliche unter Bezugnahme auf eine ökonomische Rationalität auch die BIA als Rationalisierungsmaßnahme wahrnahmen. Eine offene Kommunikation des Zielvorhabens zeigte sich als nützlich und wurde im Rahmen von Workshops im Herbst 2019 mit mehreren Prozessverantwortlichen besprochen (vgl. Workshop 17.10.2019).

[467] Dies kann insbesondere hilfreich sein, wenn Ressourcenanforderungen früher gefordert werden, als diese in der BIA festgehalten sind. Zum Beispiel wurde eine RTO von 72 Stunden definiert. In diesem Fall besteht keine Notwendigkeit, Mitarbeiter oder IT-Anwendungen bereits nach 4 Stunden einzuplanen.

[468] Ein wichtiger Aspekt der Dienstleisterverfügbarkeit ist neben dem Risiko eines Ausfalls seiner Gebäude, des Personals oder IT, die technologische Weiterentwicklung, an die der Dienstleister Anschluss verlieren kann. Dadurch können die Daten oder Kapazitäten des Auftrag gebenden Unternehmens durch den Vertrag auf absehbare Zeit an den Dienstleister gebunden sind (lock-in) oder durch dessen Ausfall nicht verfügbar sein (Bahilia und

vorzunehmen, da insbesondere im Fall des externen Auftretens im Namen des Unternehmen Risiken auftreten können, deren Kern nicht unmittelbar die Verfügbarkeit, sondern beispielsweise die Reputation des Unternehmens betreffen können.[469] Gleiches gilt für die Verarbeitung von Informationen durch Dienstleister, deren Umgang mit den Daten nicht nur aus der Perspektive der Verfügbarkeit, sondern aus einem ganzheitlichen Ansatz im Sinne des Informationsschutzes heraus betrachtet werden sollte. Diesen Fall werden wir weiter unten im Kontext der Informationsressource genauer betrachten. Für die Ressourcenerfassung kritischer Dienstleister ist jedoch festzuhalten, dass neben der reinen Verfügbarkeit, relevante Dienstleister ebenfalls aus dem Gesichtspunkt der Informationsverarbeitung und der Teilhabe im analogen und digitalen Wertschöpfungsprozess in die nachfolgende Planung einbezogen werden sollten.[470]

Den Ressourcenklassen Gebäude, Mitarbeiter und Dienstleistern ist gemeinsam, dass sie quantifizierbar sind. Eine bestimmte Anzahl an Arbeitsplätzen, Geräten, Dienstleistern und Personal kann trotz eventueller Diskussionsschleifen mit den Prozesseigentümern als detaillierte Angabe und Gesamtzahl in die Planung übernommen werden. IT Applikationen und deren Infrastruktur sind hingegen in der Regel nur einmal vorhanden und werden als Anforderung für den Notbetrieb als nichtzählbare Unikate referenziert. Denn eine kritische Applikation wird nicht als Mengenbeschreibungen durch die Prozessverantwortlichen artikuliert, sondern als qualitative Beschreibung einer benötigten Ressource für einen Prozessschritt mit Mindestleistungskriterien. Dies schließt die Verfügbarkeit der darüber verarbeiteten Informationen, sowie die darunter liegenden Ressourcen der IT-Infrastruktur und Middleware ein (Nijaz und Moon 2009: 75). Die zumeist funktionale Trennung von Prozessverantwortlichen und IT-Funktion kann jedoch die eindeutige Identifikation der benötigten IT-Ressource erschweren. Insbesondere die von Prozessverantwortlichen artikulierten Applikationsanforderungen wichen im Verlauf der ethnographischen Beobachtung

Rivard 2003: 215). Dies gilt ebenso für die Steuerung einer komplexen digitalen Wertschöpfungskette, welche auf Leistungen von Dienstleistern beruht. Diese Prozesskette durch ein integratives Risikomanagement zu steuern, bedarf geeigneter Strukturen und übergreifender Risikokontrollmaßnahmen durch das Unternehmen und die beteiligten Akteure (Xue et. al. 2013: 328).

[469] Der Umfang der ausgelagerten Funktionen kann enorme Ausmaße annehmen: "The new production system relies on a combination of strategic alliances and ad hoc cooperation projects between corporations, decentralized units of each major corporation, and networks of small and medium enterprises connecting among themselves and/or with large corporations or networks of corporations" (Castells 2010: 123). Daraus erfolgen entsprechende Anforderungen an die Steuerung des Zuliefernetzwerkes, welches im Fall einer Unterbrechung auf die Ressourcen von alternativen Quellen ausweichen muss oder andere Mitigationsmaßnahmen im Unternehmen zu treffen hat,

[470] Relevante Kontrollen aus dem funktionalen Bereich des Outsourcings wären daher zu berücksichtigen, darunter maßgeblich zur Ausgestaltung des SLAs mit Dienstleistern, Offenlegung von Vorsorgemaßnahmen und Einsicht in Testergebnisse (Ernest und Nisavic 2007: 387).

vielfach von der tatsächlichen Leistungsbeschreibung[471] zwischen IT und Fachbereich ab (Wijnia und Nikolic 2007: 3552).

Diese Lücke intendiert das IT Service Continuity Management zu füllen, indem für die Erfassung, Priorisierung und Wiederherstellung der IT-Ressource ein gesonderter Prozessschritt eingefügt wird. Die Grundlage für die ITSCM-Planung wird durch die Kritikalitäts- und Risikoanalyse der kritischen Prozesse gelegt, indem die Endanwender in den Fachbereichen die kritischen Anwendungen definieren. Da die Fortsetzung der Geschäftsprozesse im Vordergrund steht, wird die Kritikalität der Prozesse auf die Verfügbarkeitsanforderungen der Ressourcen vererbt. Daraus folgt, dass Applikationen ihre Kritikalitätsidentifikation in Folge der Prozessbewertung, also als Resultat der BIA erhalten. ITSCM setzt an diesem Punkt an und übernimmt die Verantwortung für die Translationsleistung des Anforderungsprofils der kritischen Prozesse auf Seiten der Endnutzer in die konkrete Ressourcenerfassung in der IT-Terminologie. [472] Die erste Herausforderung ist die Endanwendung einer eindeutigen Applikation sowie einem IT-Service[473] zuzuordnen und diese Information mit den Servicefamilien des internen oder externen Infrastrukturbetreibers abzugleichen (Racz, Weippl und Seufert 2010: 249). Das zweite Hindernis liegt in der Intransparenz des Prozesses der Servicevereinbarungen, in dessen Folge Fachbereiche und IT zumeist unterschiedliche Anforderungen und Leistungsbeschreibungen über Wiederherstellungsklassen annehmen.

Trotz Verschriftlichung der vereinbarten Leistungen sind diese Informationen vielen Fachbereichen nicht bekannt (Ernest und Nisavic 2007: 387) oder wurden unter Federführung der jeweiligen Schnittstellenverantwortlichen abgeschlossen, dessen Ausscheiden aus dem Unternehmen zum Verlust dieses Wissens führen kann. Eine Lösung kann daher ein virtuelles Gedächtnis in Form einer IT-Servicedatenbank sein, welche Eingaben von beiden Seiten archiviert und Verantwortlichkeiten, Anforderungsbeschreibungen, Komponentenkomposition

[471] Die vertragliche Leistungsbeschreibung zwischen internen oder externen IT-Dienstleister und Fachbereich spezifiziert den Umfang und Inhalt des IT-Service, darunter auch die Wiederherstellungszeit einer Applikation oder IT-Ressource. Doch häufig können nach Erfahrung des Autors keine Wiederherstellungsziele identifiziert werden oder der genaue Umfang der involvierten Komponenten bestimmt werden. In einigen Fällen stimmte nicht einmal der von den Endanwendern verwendete Applikationsname mit dem technischen Namen der IT-Umgebung überein.

[472] Die mitunter deutlichen Preisunterschiede zwischen zwei Verfügbarkeitsklasse (beispielsweise zwischen 24 und 72 Stunden) können auch zu einer Evaluierung auf Seiten der Prozessverantwortlichen führen, die angesichts der Mehrausgaben die initiale Angabe in der Kritikalitätsanalyse einer erneuten Überprüfung unterziehen.

[473] Ein IT-Service ist die Verknüpfung von mehreren Anwendungen oder IT-Komponenten einschließlich Lizenzen und Middleware (Ernest und Nisavic 2007: 388). Die Verknüpfung zwischen Prozessanforderungen, IT-Service und darunterliegenden Komponenten der IT-Infrastruktur repräsentieren die umfangreichste Leistung des ITSCM und legen den Grundstein für eine effektive Planung der Wiederherstellung der IT-Ressource.

und insbesondere Wiederherstellungsklassen im Sinne von konkreten RTO und Prioritäten dokumentiert. Eine derartige Vernetzung von Informationsbruchstücken kann helfen, die virtuelle Sphärentrennung zwischen Prozess- und IT-Ebene aufzuheben und eine transparente Betrachtung der vereinbarten Leistungen zu ermöglichen, auf deren Basis Nachverhandlungen und Adjustierungen mit den involvierten Dienstleistern oder IT-Betreibern erfolgen können. Da Wiederherstellungsprioritäten mit infrastrukturellen Aufwänden einhergehen, können veränderte Verfügbarkeitsanforderungen den Preis in der internen Verrechnung der Leistungsbereitstellung verändern.

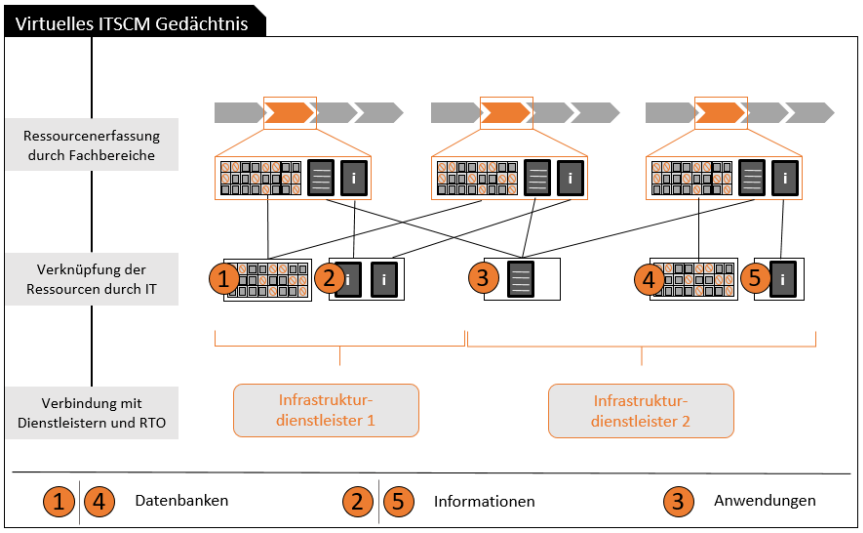

Abb. 7.4. Virtuelles ITSCM Gedächtnis und Fachbereichs- bzw. IT-Sphäre. Eigene Darstellung.

Ferner ist auf die Rolle von Informationen als Ressource einzugehen. Zwar können Informationen wie etwa Kundendaten quantifiziert werden, beispielsweise in der Anforderung die 2.000 umsatzstärksten Kundendatensätze im Notfallbetrieb bereitzustellen. Allerdings ist die Aussagekraft der Information selbst qualitativ, denn ob alle Kundendatensätze vergleichbar sind oder welche Teilinformationen in den Kundendaten enthalten sein müssen, um diese für den Prozess nutzen zu können ist nicht in der gleichen Weise zu erfassen. Informationen weisen zudem eine weitere Dimension auf, da ihr Schutz neben der Verfügbarkeit auch die Kriterien der Vertraulichkeit und Integrität inkludiert. Die Informationsressource hebt sich durch diese Eigenschaft von den anderen vier Ressourcen ab, da in diesem Fall effektive Mitigationsmaßnahmen die reine Verfügbarkeitsnotwendigkeit übersteigen. Mit Blick auf die Ressourcenidentifikation können Informationen ebenfalls ein Teil des virtuellen Gedächtnisses sein und als qualitative Bestandteile in den Anforderungskatalog eingebunden werden. Die Ergebnisse der Risikoanalyse in Gestalt der Informationsevaluation sollten mit den darauf aufbauenden Prozessen, Informationseigentümern und Verantwortlichen der relevanten IT-Infrastruktur und Anwendungen geteilt werden, um eine ganzheitliche Perspektive über den

Schutzwert von Informationen innerhalb des Unternehmens zu erhalten. Der daraus abgeleitete Risikowert setzt sich folglich aus dem Verfügbarkeitsanspruch der Fachbereiche und dem Integritäts- und Vertraulichkeitsanforderungen der Evaluation zusammen.

Zusammenfassend können die folgenden Kernkontrollen für die Phase der Ressourcenerfassung festgehalten werden. Erstens ist die exakte Dokumentation der Ressourcenkategorien Gebäude, Mitarbeiter, Dienstleister, IT-Infrastruktur und Informationen für alle kritischen Geschäftsprozesse beziehungsweise als Folge der durch die RIA identifizierten relevanten Risiken sicherzustellen. Ferner ist aus formeller Sicht die Bestätigung der Ressourcenbeschreibung von allen Beteiligten (Prozess-, Ressourcen- und Schnittstellenverantwortliche) einzuholen und von Entscheidungsträgern gegenzeichnen zu lassen. In materieller Hinsicht ist darüber hinaus die Identifikation der IT-Ressourcen aus Sicht des ITSCM über IT-Service-, Anwendungs-, Middleware- und Infrastrukturebene durchzuführen, welche ebenfalls die Komponentenzusammensetzung der von internen oder externen Dienstleistern bereitgestellten IT-Services und deren Wiederherstellungszeiten dokumentiert. Darauf aufbauend kann mithilfe eines umfassenden Bildes der zu schützenden Ressourcen zur Strategiedefinition übergeleitet werden.

7.2.3. Strategieformulierung

An die Kritikalitätsbewertung und Ressourcendefinition schließt sich die Frage an, wie diese Erkenntnisse in Strategien zur Vorsorgeplanung übersetzt werden können? Strategien können für die jeweilige Ressourcenkategorie, beispielweise der Strategie zur Kompensation des Ausfalls der IT-Ressource, detaillierte Maßnahmen und Ablauforganisationen für den Notbetrieb in Form von Wiederherstellungsplänen erarbeiten. Die Strategieformulierung dient daher vorrangig der Entscheidung über die maßgebliche Richtung der Vorsorge und sollte aufgrund ihrer Tragweite in finanzieller Hinsicht, sowie der Bedeutung für eine erfolgreiche Handhabung einer Krise von den obersten Entscheidungsträgergremien des Unternehmens gefällt und anschließend durch diese kommuniziert werden (Nicoll und Owens 2013: 50). Das Ergebnis dieses Schrittes sollte in klaren (1) Zielen, (2) Handlungsoptionen und (3) Verantwortlichkeiten für mindestens fünf Strategien, das bedeutet mindestens eine Strategie für jede der kritischen Ressourcenkategorien des Unternehmens resultieren.

Die Strategien für Gebäude, Personal, Dienstleister und IT folgen mit Blick auf ihre Struktur der traditionellen BCM-Methodik. Deren (1) Ziel sollte dahingehend definiert werden, als dass sich das zu erreichende Mindestserviceniveau der betroffenen Ressourcen und Prozesse innerhalb der definierten Wiederherstellungszeit und Qualität wiederspiegelt. Die Neuerung

mit Blick auf eine resiliente Organisation ist ein Verständnis von Geschäftsprozessen im Sinne einer kontinuierlichen Bereitstellung von Anschlussoperationen in der Organisation. Auch wenn ein einzelner Prozess kritisch ist, wird erst seine Bedeutung für die Folgenutzung im Unternehmen und dessen Prozesskontinuität zum relevanten Beitrag zur internen Sicherheitsproduktion. Die (2) Handlungsoptionen dienen der Kosten-Nutzen Abwägung zwischen denkbaren Alternativen zur betroffenen Ressource, welche zudem in infrastrukturelle und taktische Optionen hier weiter unterschieden werden können (Karim 2011: 183). Infrastrukturelle Maßnahmen bezeichnen präventive Strategien, welche vor dem Eintreten eines Zwischenfalles implementiert sein müssen, um ihre Wirkung entfalten zu können, wie zum Beispiel Backup-Rechenzentren. Taktische Optionen stehen hingegen auch nach dem Ausfall einer Ressource und ohne vorausgehende Einplanung zur Verfügung, beispielsweise Hotel- und Konferenzräume für die Unterbringung von Mitarbeitern. Die Beschreibung von (3) Verantwortlichkeiten soll dem nachfolgenden Prozess der Plandefinition Struktur und den durchführenden Verantwortlichen Autorität verleihen, diese Aufgabe in der Planung und in der späteren Ausführung wahrzunehmen.[474]

Wie wir in den vorrausgegangen Kapitel gesehen haben, fällt der Bestimmung von Organisationsgrenzen eine besondere Bedeutung zu, welche im Informationszeitalter unter Einbeziehung von Dienstleistern wie beispielsweise Cloud-Anbietern gesonderte Anforderungen an die Sicherheitsproduktion stellt. Diese Konstellation wollen wir im Folgenden in einem Schwerpunkt betrachten und die Einbindung der Kontrollen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen im Fall von Dienstleistern besprechen. Aus der ethnographischen Untersuchung zeigte sich die Beobachtungen, dass die aufgrund einer ökonomischen Rationalität getroffene Auslagerung von Prozessen und Systemen an externe Dienstleister wie Cloud-Anbieter oder

[474] Eine Zielbeschreibung für die Mitigation des Ausfallsrisikos eines wichtigen Automobilteilzulieferers könnte zum Beispiel lauten, dass der zu kompensierende Output vom Unternehmen zu 80 Prozent des Normalsolls durch die Bereitstellung von Kapazitäten von nicht-kritischen Prozessen übernommen wird. Die Servicequalität soll mit einer Fehlerquote von maximal 0,5 Prozent durch ein Dreischichtenmodell innerhalb von 72 Stunden gewährleistet werden und unter Verantwortung des Produktionsleiters geschehen. Andere Mitigationsoptionen könnten die infrastrukturelle Verteilung der Zulieferbezüge auf mehrere Dienstleister sowie der Vorratshaltung größerer Stückzahlen der gelieferten Produkte berücksichtigen, um die Produktion ungestört fortsetzen zu können. Doch aufgrund der höheren Kosten - im ersten Fall durch schlechtere Konditionen im Einkauf, im zweiten Fall durch die höheren Lagerkosten - könnte sich das Unternehmen auch für die taktische Option der internen ad-hoc Umverteilung von Arbeitslasten und Kapazitäten entscheiden. Die benötigten Warenteile könnten auf dem Markt bezogen und vom Unternehmen selbst weiterverarbeitet werden. Zu diesem Zweck müssten abschließend Verantwortlichkeiten definiert werden, indem beispielsweise der Account Manager für die betreffende Produktsparte die Ausarbeitung der Wiederherstellungspläne und die Absprachen mit dem Dienstleister in der Krise übernehmen soll.

Plattformbetreiber von Experten skeptisch betrachtet werden[475], sofern kein angemessenes Rahmenwerk zur Risikokontrolle vorliegt. Einen solchen Rahmen kann ein dreistufiger Prozess anbieten, welcher als Teil der Strategieformulierung für den möglichen Ausfall von Dienstleistern konzipiert werden sollte.

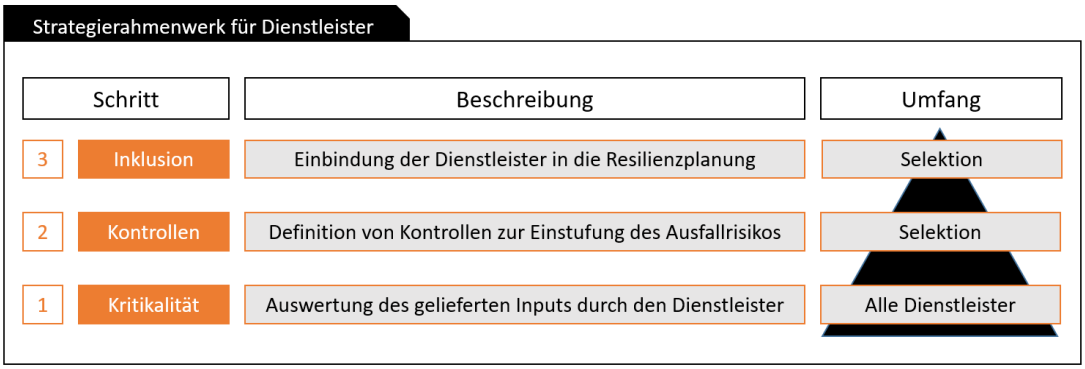

Abb. 7.5. Spezifisches Strategierahmenwerk für Dienstleister. Eigene Darstellung.

Der erste Schritt umfasst die (a) intensive Ressourcenerfassung kritischer Prozesse mit Blick auf interne und externe Dienstleister unter besonderer Berücksichtigung der gelieferten Waren oder (virtuellen) Dienstleistungen und deren spezifischer Grad an Exklusivität. Wenn eine gelieferte Dienstleistung oder ein Gut nur von einem oder einer kleinen Auswahl an Anbietern bezogen wird, kann der Wechsel zu alternativen Anbietern aufgrund der vertraglichen oder technischen Anpassungen zu aufwendig sein (vgl. Kilger 2008: 381). Auch kann die technologische oder prozessuale Verknüpfung zwischen dem liefernden und dem abnehmenden Unternehmen zu eng verflochten sein, um geeignete Alternativen innerhalb der RTO aufzubauen. In diesen Fällen wird von einem kritischen Dienstleister gesprochen. In einem zweiten Schritt werden kritische Dienstleister mithilfe eines (b) durch einheitliche Kontrollen standardisierten Fragebogens auf ihr jeweiliges Ausfallrisiko hin untersucht. Interne und externe Risikofaktoren sollten ebenso Bestandteil der regelmäßig durchgeführten Befragung sein, als auch die von dem Dienstleister getroffene Vorsorgeplanung auf mögliche Unterbrechungen. Im dritten Schritt sollten ausgewählte Dienstleister, zumeist solche mit einem hohen Schadenspotential für den Kunden in (c) gemeinsame Planungen und Tests einbezogen werden (Gaycken und Karger 2011: 7). Im Rahmen dieser Absprachen und Übungen sollte die geteilte Verantwortung und Abhängigkeit für die Wiederherstellung der

[475] Dies zeigte sich im Gespräch mit einem Experten aus dem Krisenmanagement, welcher auf die Erkenntnis aus dem Log4j-Zwischenfall mit Blick auf die Verwundbarkeit der Organisation durch nicht-gepatchte Systeme von Dienstleistern referenzierte (Hintergrundgespräch 13.12.2021).

ausgefallenen Servicelevels getestet werden und helfen Mängel zu identifizieren beziehungsweise zu korrigieren (Nicoll und Owens 2013: 54).

Dieses Strategierahmenwerk für Dienstleister ist zudem im Bereich der modernen Outsourcing- und Offshoring- Industrie von kaum zu unterschätzender Relevanz, da investitionsintensive Technologien wie die IT-Infrastruktur, Big Data Analysenetzwerke oder Clouds zumeist von externen Dienstleistern bezogen werden (Schwering 2010: 231). Auch die Virtualisierung von Arbeitsprozessen im Zuge der Corona-Pandemie basierte zum großen Teil auf den skalierbaren Angeboten der großen Cloud-Anbieter wie beispielsweise Azure oder AWS, wodurch sich die Daten dem direkten Zugriff und der Kontrolle des Unternehmens entziehen (Kirk und McDonald 2021: 3). Daher sind neben den Elementen einer Outsourcing-Strategie im Sinne der sorgfältigen Vorbereitung einer neuen Kooperation, wie beispielsweise der Auswahl verlässlicher Partner, Bestimmung der Spezifika der Produktdetails und Antizipation möglicher Veränderungen der technologischen Grundlagen oder Anforderungen (Grossman und Helpman 2005: 137) auch eine Vorbereitung auf den möglichen Ausfall des Dienstleisters frühzeitig in den Auswahlprozess einzubeziehen. Jenseits des durch das Strategierahmenwerk für Dienstleister abgesteckten Felds der Ressourcenverfügbarkeit[476], sind ebenfalls die Aspekte des Informationsschutzes im Fall der Fremdverarbeitung von Daten zu beachten. Die Betreiber von Cloud-Lösungen sind beispielsweise für die Applikations- und Datensicherheit auf ihren Plattformen verantwortlich (Dochow 2022: 101). Dies umfasst sowohl den Schutz der Nutzerdaten gegen Angriffe von außen, aber auch gegen Angriffe durch andere Nutzer innerhalb der Cloud, zumeist durch eine Virtualisierung, das bedeutet die Segmentierung in virtuelle Sphären ohne direkte Verbindungen untereinander (Armbrust et. al. 2010: 55).

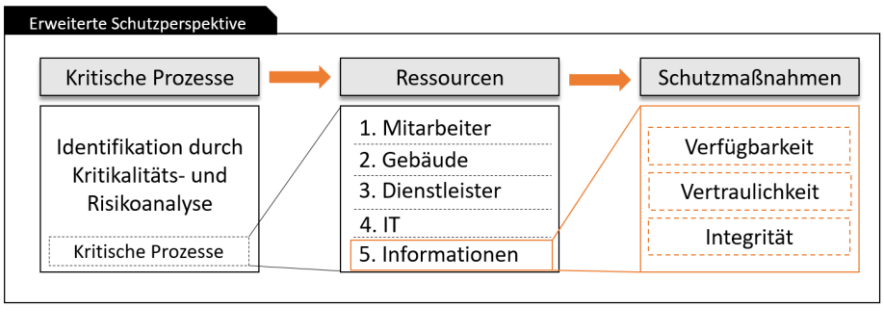

Abb. 7.6. Erweiterte Schutzperspektive für Informationen und Strategieentwicklung. Eigene Darstellung.

[476] Der Datenverlust kann durch präventive Maßnahmen antizipiert werden, beispielsweise durch kryptografische Verfahren oder durch eine Kategorisierung der Dateien in Schutzklassen („Labeling“) deren Schutzniveau entsprechend der Einstufung erweiterter Vorkehrungen bedarf. Ferner sollte die Zahl der Lese- und Schreib-Berechtigten Nutzer reduziert werden (Eckert 2008: 10). Diese Beschreibungen der Sicherheitsstandards sind als Teil der Strategieformulierung unverzichtbar, da ihr Beitrag zu einer sicheren Umgebung nur durch eine Implementierung vor dem Eintreten eines Zwischenfalls genutzt werden kann.

Die Notwendigkeit den Schutz der Informationen aus den drei Perspektiven der Verfügbarkeit, Vertraulichkeit und Integrität zu sehen, ist insbesondere wichtig, um die unterschiedlichen Strategieoptionen in den Kontext eines integrativen Ansatzes unter dem Überbegriff Resilienz setzen zu können. Die auf der Strategieformulierung aufbauenden Pläne setzten eine umfassende Analyse und Auswertung der zur Verfügung stehenden infrastrukturellen und taktischen Möglichkeiten voraus. Im Fall der Informationssicherheit betrifft dies insbesondere investitionsintensive Alternativen, welche die Verfügbarkeit, aber auch Exklusivität der zumeist elektronisch gespeicherten Daten adressiert. Den größten Einfluss auf eine resiliente Organisation nehmen infrastrukturelle Maßnahmen (Wijnia und Nikolic 2007: 3549), deren Implementierung in der präventiven Planungsphase verortet werden kann und auf deren Grundlage später das Spektrum taktischer Optionen und damit der Handlungsspielraum des Unternehmens während einer Krise offengehalten werden kann (Cavelty 2013: 111).

Doch es zeigte sich insbesondere während der Corona-Pandemie, dass Unternehmen die unmittelbare Fortsetzung von Prozessen priorisierten, indem zügig neue virtuelle Strukturen geschaffen wurden (Engels 2020: 2). Die Bereitschaft zu Investitionen in IT-Sicherheitsschulungen für die Nutzer, Ausweitung des IT-Sicherheitspersonals oder in Maßnahmen zum Datenschutz fiel hingegen deutlich geringer aus (Bellmann et. al. 2021: 715). Wie wir im vorausgegangenen Kapitel über die Bedrohungen des digitalen Zeitalters gesehen haben, bedeuten Schadprogramme eine große Unsicherheit für den Informationsschutz und ebenso zählen die Angriffe auf Netzwerke dazu, welche durch die beschleunigte Digitalisierung erneut zunahmen (Kirk und McDonald 2021: 3). Die primäre Abwehr dieser Angriffe wird üblicherweise von infrastrukturellen Maßnahmen[477] wie Virenscannern und Firewalls übernommen (Eckert 2008: 30). Die Implementierung und Aktualisierung dieser infrastrukturellen Schutzmaßnahmen bedeuten für komplexe Systeme einen erheblichen organisatorischen und finanziellen Aufwand, insbesondere da täglich mehrere hundert neue

[477] Eine automatisierte Schutzvorkehrung gegen von Programmen generierte Anfragen, beispielsweise zum Schutz vor DoS-Angriffen, bieten CAPTCHA Felder (Completely Automated Public Turing test to tell Computers and Humans Apart). Diese Pflichtfelder erfordern die Eingabe eines Codes, welcher als Bild dargestellt wird und die analytischen Fähigkeiten einer künstlichen Intelligenz mit dem Zweck zu überfordern gedenkt, die Erstellung von Profilen oder Anfragen durch nicht-menschliche Nutzer zu verhindern. Diese Schutzvorkehrung kann beispielsweise von Bot-Netzwerken mithilfe von automatisierten Social Engineering Techniken umgangen werden, wie eindrucksvoll bei Huber et. al. nachzulesen ist (Huber et. al. 2009: 118f.). Eine andere Methode wurde von Google anhand massenhafter Einwahlversuche zu ungewöhnlichen Zeiten festgestellt, welche von einem Bot-System orchestriert wurden, die Eingabe des CAPTCHA-Feldes jedoch von Menschen in Niedriglohnländern übernommen wurden. Bei Tageslöhnen zwischen drei und acht US-Dollar boten die menschlichen Arbeitskräfte eine günstige Alternative, um die Anfragen stellen zu können (Borges et. al. 2011: 56). Die Kuriosität dieses Falles liegt insbesondere in der modernen Arbeitsteilung zwischen einem Computerprogramm und menschlichen Hilfskräften, bei dem die künstliche Intelligenz des Bot-Netzwerks im Auftrag seiner Schöpfer die Federführung übernahm und sich der billigen Arbeitsleistung von Menschen für eine repetitive Tätigkeit bediente.

Modifikation von Schadprogrammen gemeldet werden[478], deren Alteration der Identifizierung vorbeugen soll (Anant, Caso und Schwarz 2020: 2). Die Risikoperzeption der Entscheidungsträger wird im Fall von Virenscannern ebenfalls zum Tragen kommen, falls die detaillierte Prüfung der verdächtigen Dateien und Anwendungen in Kosten der Systemperformanz (Moser, Kruegel und Kirda 2007: 231) und eventuellen Verzögerungen der Bearbeitungszeit seitens der Geschäftsprozesse resultiert.

Die Notwendigkeit einer effektiven Präventivstrategie basiert auf Investitionen und Prozessmodifikationen des Unternehmens, zu denen Antivirenprogramme einen elementaren Beitrag liefern, aber auch „nur einen Basisschutz bieten können", wenn man die Leistungsfähigkeit und Dynamik von Schadprogrammen reflektiert (Borges et. al. 2011: 81). Insbesondere mangelnde Früherkennungsfähigkeiten der Virenscanner und Firewalls stellten sich als problematisch heraus, während systemische Schwachstellen wie offene Hardwareschnittstellen oder Sicherheitspolicen an zweiter Stelle zu nennen sind (Krotofil und Cárdenas 2013: 179), deren Bedeutung für die IT-Sicherheit sich im Zuge der Corona-Pandemie weiter herausgestellt hat (Chigada und Madzinga 2021: 5).

Andere Maßnahmen zielen auf die Konditionierung des Nutzerverhaltens ab (Wentland und Klimburg-Witjes 2021: 169), sind allerdings sorgfältig zu planen und umzusetzen. Eingebettet in ein umfangreiches Portfolio an IT-Sicherheitskonzepten könnte dies als Strategie formuliert bedeuten, Mitarbeitern die Risikoexposition des Cyberraums zu verdeutlichen und durch regelmäßige Wiederholung, Schulungen oder praktische Beispiele und Kampagnen deren Perzeption zu schärfen (Kahan, Allen und George 2009: 22). Diese ebenfalls präventive Bewusstseinsbildung kann durch technische Maßnahmen unterstützt werden, beispielsweise durch die Sperrung verdächtiger Seiten[479] oder Etablierung von virtuellen Sandkastenräumen zur sicheren Öffnung von Dateien in abgetrennten Bereichen des Netzwerkes (Borges et. al. 2011: 68). Diese Maßnahmen können zusammengefasst als Rahmenwerk gesehen werden, um eine verinnerlichte Vorsicht der Endnutzer zu etablieren und eine weitreichende Akzeptanz der

[478] Die bekannte Schwäche von Virenscannern ist, dass die Signatur von Schadprogrammen in einer Datenbank registriert sein muss, um die Identifizierung als unerwünschte Anwendung zu ermöglichen. Ferner können die begrenzten heuristischen Fähigkeiten des Scanners durch elaborierte Programme umgangen werden, deren Code die eigentliche Intention des Programms vor dem Virenscanner verborgen hält (Alazab et. al. 2010: 2). Proaktive Scanner hingegen ermöglichen die Etablierung eines verdächtigen Programms in einer „Sandbox", also einem Sandkastenabschnitt, in dem die Verhaltensweise in einem sicheren und isolierten Netzwerkbereich getestet wird, bevor es auf die eigentlichen Systeme geladen wird, allerdings auf Kosten der Systemperformanz und mit eventuellen Fehlalarmen, deren Einzelfallprüfung durch einen geübten, menschlichen Entscheider durchgeführt werden muss (Borges et. al. 2011: 68).

[479] Google betreibt seit einigen Jahren ein Projekt zur Kartografierung infizierter Webseiten im Internet, um einen „drive-by download" von Schadprogrammen während des Webseitenbesuchs zu verhindern. Zu diesem Zweck analysieren Algorithmen von Google jährlich Milliarden von Webseiten (Provos et. Al. 2007: 1).

Sicherheitsvorkehrungen zu erreichen. Diese Strategieoptionen können als erste Abwehrlinie gegen potentielle Bedrohungen von Informationen verstanden werden[480], denn obwohl in diesen Beispielen der Schutz der IT-Infrastruktur im unmittelbaren Fokus stehen, liegt die primäre Absicht in der Bewahrung der auf diesen Systemen beheimateten Informationen.

Abschließend sind Maßnahmen unter dem Gesichtspunkt der infrastrukturellen Vorkehrungen zu nennen, deren Implementierung zwingend vor dem Eintreten eines Zwischenfalls abgeschlossen sein muss. Dazu zählen infrastrukturelle Redundanzen wie sie im vorausgegangenen Kapitel im Kontext der Bedrohungen durch Ransomware erörtert wurden und Teil der ITSCM-Vorsorge sein können.[481] Darunter sind die physikalische Trennung von Systemkomponenten[482], die Frühwarnindikation von Bedrohungen auf Endgeräten und deren sofortige Isolation[483], standardisierter Sicherheitsprotokolle[484], sowie bauliche, strukturelle und organisatorische Vorkehrungen für den Fall einer erfolgreichen Überwindung der präventiven Schutzvorkehrungen zu nennen. Auch wenn sich manche Autoren kritisch gegenüber einer Präventivstrategie zeigen (vgl. Gaycken und Karger 2011: 4; Weber 2016: 29), ist sie trotz ihrer Unvollständigkeit angesichts der dynamischen technologischen Weiterentwicklung eine wichtige Komponente in der Antizipation von Angriffen. Auf ihrer Grundlage können

[480] Zu unterscheiden sind technische Maßnahmen wie Antivirenprogramme und Firewalls auf der einen Seite (McGuire 2015: 47) und verhaltensorientierter Maßnahmen wie Schulungen von Nutzern auf der anderen Seite. Letztere sind ebenfalls eine gesamtgesellschaftliche Aufgabe, da der Schutz der Bürger im Informationszeitalter die Schutzperspektive auch auf die individuelle Ebene erweitert werden muss (Willems: 2013: 4).

[481] Darunter können zusätzlich Failover-Systeme für Applikationen verstanden werden, welche die Wiederherstellung durch vorprogrammierte Wechsel zwischen Infrastrukturen und technischen Zwischeninstanzen erleichtern, insbesondere hinsichtlich der zeitkritischen Determinanten. Auch geeignete Techniken sind hierunter zu verstehen die eine Manipulationserkennung von Daten ermöglichen, um im Fall einer Integritätsverletzung die betreffenden Informationen identifizieren und gegebenenfalls einschränken zu können (Eckert 2008: 8).

[482] Sogenannte AirGap Systeme, deren Zweck in der Isolierung eines Computervirus liegt, können eine Trennung zwischen verschiedenen Systembereichen herstellen, aber dennoch die Übertragung von Daten zwischen beiden Einheiten erlauben (Gaycken und Karger 2011: 8).

[483] Der von Facebook verwendete Virenschutz isoliert zum Beispiel ein infiziertes Endgerät umgehend vom restlichen Netz. Der Verdachtsmoment einer Infizierung mit Schadsoftware basiert auf der Erkennung von Nutzungsprofilen, deren Abweichen etwa durch die Fremdsteuerung einer Malware erkannt und als Bedrohung klassifiziert wird. Diese verhaltensbasierte Überprüfung von normabweichenden Aktivitäten benötigt ein hohes Maß an Empirie, Zustimmung der Nutzer zur diskreten Überwachung ihrer haptischen und teilweise auch inhaltlichen Tätigkeit am Endgerät, sowie eine Aufzeichnung der Verhaltensprofile in Echtzeit, welche auf einer entsprechenden Rechenleistung aufbauen muss. Der Vorteil liegt in der Überwachung von Aktivitäten hinter der Firewall, welche auf verdächtige Programme frühzeitig reagieren kann. Denn der vermeintlich sichere Bereich hinter den Virenscannern und Firewalls könnte einem Schadprogramm große Bewegungsfreiheit in Netzwerken und Servern im Rechenzentrum erlauben, wenn keine regulierende Instanz in diesem Bereich aktiv ist (Borges et. al. 2011: 153).

[484] Dazu gehören automatisierte Reaktionsmuster auf potentielle Bedrohungen, aber auch grundsätzliche Vorschriften und Regeln, wie den Ausschluss verdächtiger Webseiten oder der Reduzierung herunterladbaren Inhalts auf lizensierte und geprüfte Seiten, wie beispielsweise den AppStore von Apple (Felt et. al. 2011: 2).

Reaktionspläne entwickelt werden und Entscheidungs- und Handlungsspielräume für den Fall eines Zwischenfalls oder einer Krise offengehalten werden.

Zusammenfassend sind für diesen Abschnitt die folgenden Kernkontrollen für die Phase der Strategieformulierung aufzuzählen. Unternehmen sollten zunächst einheitliche und klar strukturierte Strategien für alle fünf Ressourcen, die kritischen Prozesse sowie die identifizierten Informationen entwerfen. Die Strategien sollten einheitlich die Ziele, Handlungsoptionen und Verantwortlichkeiten beschreiben und anhand einer Kosten-Nutzen-Rechnung geeignete Lösungen zur Sicherstellung der Prozesskontinuität auswählen. Dazu zählt insbesondere ein gesondertes Rahmenwerk zur Überprüfung kritischer Dienstleister und deren Einbindung in die Risikosteuerung des Unternehmens. Die Ansätze zur Kontrolle geschäftsgefährdender Risiken sollten zudem die besonderen Anforderungen der jeweiligen Ressourcen im Detail berücksichtigen und insbesondere im Fall relevanter IT-Anwendungen und Infrastruktur die detaillierten Kontrollen der ITSCM-Methodik, aber auch des Informationsschutzes berücksichtigen, um geeignete Wiederherstellungszeiten zu gewährleisten. Abschließend empfiehlt sich die Erstellung einer einheitlichen Datenbank zur Zusammenführung und Synchronisation der unterschiedlichen Strategien des Unternehmens, welche von den Entscheidungsträgern des Unternehmens zu bestätigen lassen sind.

7.2.4. Plandefinition und Testen

Für alle identifizierten Schutzziele sollten anschließend Reaktionspläne entwickelt werden, welche definierte und eingeübte Aktivitäten in Reaktion auf das Eintreten eines Ressourcenausfalls, einer Kompromittierung von Informationen oder einer Krisensituation im Allgemeinen beschreiben. Die Plandefinition bestimmt auf der Grundlage der Strategieformulierung die Details der Vorsorgemaßnahmen und artikuliert über deren Zusammenführung in einer holistischen Vorsorgeplanung die prozessuale Orientierung an der Sicherstellung von Prozessen und Kommunikation im Unternehmen.[485] Wiederherstellungspläne für Ressourcen oder Prozesse sollten die Rahmenbedingungen der Entscheidung thematisieren, ob und unter welchen Umständen der Plan von wem aktiviert werden kann. Dies übersetzt sich in eine möglichst konkrete Beschreibung der Abläufe und Verantwortlichkeiten und voraussichtlichen Auswirkungen auf die Prozesskontinuität der Organisation. Anhand dieser Einschätzung und zuvor definierten Kriterien können

[485] Die Strategieformulierung für den Ausfall eines Gebäudes würde etwa eine Ausweichlokation vorsehen, auf dessen Grundlage der spezifische Wiederherstellungsplan die Rahmenbedingungen der Aktivierung des Plans, die Maßnahmen für die Vorbereitung einer Ausweichlokalität und den Transport der Mitarbeiter beschreibt.

Entscheidungsträger wie beispielsweise der Krisenstab leichter Entscheidungen über die Fortsetzung der Geschäftsprozesse treffen und die Aktivierung der Pläne bestimmen.

Im Allgemeinen erfüllt die Vorsorgeplanung eine wichtige Funktion, indem sie die Ergebnisse der Kritikalitäts- und Risikoanalyse, der Ressourcenerfassung und der Strategieformulierung in eine prägnante Anleitung für die Notfallteams zusammenführen. Zu diesem Zweck sollten die Pläne die Komplexität der vorausgegangenen Erhebungen so weit wie möglich vereinfachen und den Lesern dieser Dokumente eine konkrete Unterstützung beispielsweise zur Wiederherstellung einer Ressource, Bewältigung eines Ransomware-Angriffs oder der strukturierten Reaktion auf eine Reputationskrise ermöglichen. Dazu gehören klare Zielvorgaben, eine einfache und eindeutige Sprache, der Verzicht auf überflüssige Informationen und detaillierte Angaben zur praxisnahen Umsetzung der theoretischen Planung. Die Pläne bauen insbesondere auf den vorherigen, präventiven Entscheidungen der Strategieformulierung auf, indem beispielsweise Wiederherstellungspläne die Umsetzung einer konkreten Re-Lokation von Büroflächen regeln oder Krisenpläne für Cyberrisiken auf einer infrastrukturellen Grundlage operieren, welche aufgrund der Risikoexposition eingerichtet wurde.[486]

Dazu eignet es sich, eine Differenzierung zwischen Plantypen vorzunehmen, die jeweils einen spezifischen Zweck erfüllen und eine dezidierte Zielgruppe adressieren.[487] In unserem integrativen Ansatz werden insgesamt vier Plantypen als relevant erachtet, von denen drei Typen die Wiederherstellung der Geschäftsprozesse und Ressourcen thematisieren und ein Typ die Handhabung von Zwischenfällen und Krisen ergänzt. Die Wiederherstellungspläne werden als (1) Koordinationsplan, (2) Geschäftsfortführungsplan (Business Recovery Plan – BRP) und (3) Ressourcenwiederherstellungsplan (Resource Recovery Plan – RRP) bezeichnet. Der entsprechende Plantypus für die Bewältigung von spezifischen Krisenszenarien, welche auch die Dimensionen des Informationsschutzes berücksichtigen, ist der (4) Krisenszenarioplan.

[486] Als solche sind die Modalitäten der Datenbackups oder die Segmentierung von Systemkomponenten zu verstehen. Alle strategischen und infrastrukturellen Maßnahmen welche ex ante implementiert werden, sollten in den Plänen referenziert werden. Das Ziel der Pläne ist es ihre Nutzer über die Anwendung der Maßnahmen zu informieren oder die Reaktion auf einen Zwischenfall zu beschreiben, in dem die präventiven Maßnahmen versagt haben, wie beispielsweise in einer Reputationskrise.

[487] Die maßgebliche Unterscheidung der Plantypen kann anhand ihrer Zielsetzung und der Gruppen erfolgen, welche diese Pläne im Ernstfall verwenden sollen. Da viele Planeigentümer auf Seiten der Geschäftsprozesse in ihrer alltäglichen Arbeit nur selten in Kontakt mit den Plänen kommen, ist eine einfache und zielgerichtete Beschreibung des Ablaufs und der Verantwortlichkeiten notwendig.

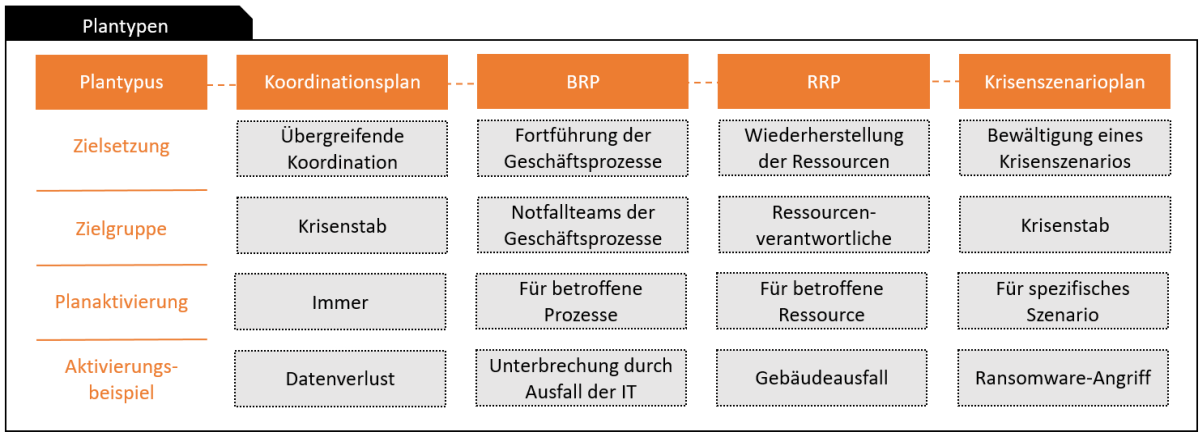

Abb. 7.7. Unterscheidung der Plantypen. Eigene Darstellung.

Der Koordinationsplan ist ein übergreifendes Dokument, welches die zentralen Entscheidungen und Aktivierungsprozeduren für die anderen Plantypen enthält. Es bietet dem Krisenstab als wichtigstem Entscheidungsgremium eine Übersicht über die relevanten Handlungsfelder und Entscheidungsoptionen. Dieser Plan sollte die Aktivitäten der anderen drei Plantypen, sprich die Wiederherstellungspläne und Pläne für Krisenszenarien zusammenführen und dem Krisenstab den Überblick über die Fortschritte in den jeweiligen Bereichen ermöglichen. Die Aktivierungsrichtlinien und Grenzwerte sollen eine Entscheidung zur Aktivierung weiterer Pläne[488], beziehungsweise Initiierung von Maßnahmen in Reaktion auf die Krisendynamik ermöglichen. Der ressourcen-orientierte RRP richtet sich hingegen an die Verantwortlichen einer bestimmten Ressource, beispielsweise der IT-Abteilung, welcher die IT-Infrastruktur unterliegt. Sollte ein Zwischenfall die Verfügbarkeit der Ressource gefährden oder unterbrechen, beschreibt dieser Plantypus die detaillierten Schritte des Expertenteams zur Wiederherstellung eines notwendigen Betriebsniveaus, das den betroffenen Geschäftsprozessen ermöglicht, ihre Aufgaben fortführen zu können. Hier ist es wichtig anzumerken, dass der Plan für eine Ressource, beispielsweise die IT-Infrastruktur, auf den Ende-zu-Ende-Prozess zur Kontinuität durch alle dieser Ressource als relevant zugewiesenen Komponenten beruht. Der Plan orientiert sich demnach nicht an einzelnen Objekten, sondern an einem systemischen Zusammenwirken der Komponenten zur Sicherstellung seiner

[488] Der Koordinierungsplan kann im Fall einer Wiederherstellung von Prozessen oder Ressourcen aktiviert werden, aber auch wenn eine Krise vorliegt, beispielsweise durch eine Ransomware-Attacke. In diesem Szenario wäre auch eine Aktivierung aller vier Plantypen denkbar. Der Koordinierungsplan ist immer zu aktivieren, um die übergreifende Steuerung der Maßnahmen sicherzustellen. Der Krisenszenarioplan für Ransomware ist in diesem Beispiel notwendig, um eine möglichst schnelle Reaktion auf die Kodierung der Daten zu ermöglichen und um die Vertraulichkeit und Integrität der noch nicht kompromittierten Informationen zu berücksichtigen. Da eine Ransomware-Attacke auch die Verfügbarkeit der IT- und Informationsressource sowie der Geschäftsprozesse bedrohen kann, sind ebenfalls die Aktivierung der RRPs für die betroffenen Ressourcen und die BRPs der kritischen Geschäftsprozesse in Erwägung zu ziehen.

elementaren Funktionsweise, um einen Prozess- und Kommunikationsabbruch zu vermeiden beziehungsweise zu minimieren.

Der BRP adressiert die Prozesseigentümer eines kritischen Geschäftsprozesses und sollte neben den notwendigen Schritten zur Wiederherstellung der relevanten Prozessaktivitäten auch die verantwortlichen Teamleiter und Mitglieder benennen. Der BRP sollte die wesentlichen Reaktionsschritte des jeweiligen Teams benennen und konkretisieren, welche Aktivitäten aufgrund mangelnder Redundanzen oder Kompensationsalternativen suspendiert werden sollten beziehungsweise welche Ressourcen für die Wiederherstellung benötigt werden. Letztere umfassen in der Regel die Anzahl an Arbeitsplätzen und Mitarbeitern, welche zur Sicherstellung der Anschlussoperationen essentiell benötigt werden. Darunter können IT-Anwendungen und Informationen, besondere Geräte und Ausrüstung, sowie Dienstleister und relevante Ansprechpartner fallen.

Der Krisenszenarioplan unterscheidet sich von den anderen Plänen durch seine Adressierung an den Krisenstab, sowie die spezifische Gruppe von Experten für das jeweilige Szenario. Zudem orientiert sich die inhaltliche Ausrichtung an einem bestimmten, vordefinierten Szenario, wie etwa einer Pandemie oder einer ATP. Der hohe Detailgrad der Definition des Szenarios ist zum Zweck konkreter Handlungsschritte auf der Grundlage der RIA definiert worden, um im Moment des Eintretens keine Zeit zu verlieren und umgehende Reaktionen einleiten zu können. Durch seine Fokussierung auf ein Szenario stellt dieser Plantypus nicht die Verfügbarkeit einer Ressource oder eines Prozesses in den Vordergrund, sondern ermöglicht zum Beispiel die Reaktion auf eine Reputationskrise, die Abdeckung der Integrität und Vertraulichkeit der Informationen oder der weiteren Schutzwerte des Unternehmens.[489] Diese Szenario-orientierten Pläne können detailliertere Inhalte als die anderen Plantypen einschließen, da sie für spezifische Situationen und Bedrohungen konzipiert wurden, etwa im Beispiel der Ransomware-Attacke die konkreten Schritte nach Identifizierung eines Angriffsversuchs als Checklisten präsentieren, welche insbesondere auch die Krisenkommunikation berücksichtigen sollte (Nicoll und Owens 2013: 53).

Diese Pläne sollten von allen beteiligten Akteuren verstanden und eingeübt wurden. Ersteres referenziert auf Trainings und Schulungen, welche die Motivation, Zielsetzung und Planinhalte verdeutlichen sollen. Das zweite Element thematisiert Übungen zur Verinnerlichung der

[489] Diese Abdeckung kann über spezifische Szenarien erreicht werden, etwa durch in Plänen definierte Reaktionsmuster auf Malware-Angriffe, Datenverlust, Erpressungen, Terrorismus, Naturkatastrophen oder politische Instabilität.

theoretischen Trainings und soll zudem die Effektivität der gewählten Strategien und Pläne unter Beweis stellen (Scherrer 2018: 89). Diese Überprüfungen durch Tests sind in der Regel eine regulatorische Anforderung an Unternehmen und sollten regelmäßig durchgeführt und dokumentiert werden (vgl. BCBS 2010: 2; Gaycken und Karger 2011: 6f.; Lam 2002: 24; Schintler et. al. 2007: 295). Ein weiterer Effekt der Involvierung der Geschäftsprozesse und beteiligten Akteure ist zudem eine proaktive Bewusstseinsschaffung für die Vorsorgeplanung, welche zur Vermeidung eines Ereignisses oder der frühzeitigen Identifizierung von Bedrohungen beitragen kann (Cook 2010: 23).

Im Fall von Dienstleistern sollten regelmäßige Design- und Effektivitätsüberprüfungen stattfinden. Dies bedeutet in anderen Worten die Verifizierung von strukturellen und inhaltlichen Gesichtspunkten der Vorsorgeplanung - auch die kritischen Zulieferer im Kontext der Tests einzubeziehen. Eine Auslagerung von sensitiven Informationen an einen Dienstleister bedeutet daher, dass Unternehmen sich ihrer Verantwortung nicht entledigen können und der Sorgfaltspflicht in Form einer Auditierung der Risikokontrollsysteme ihres Dienstleisters nachzukommen haben (Schwering 2010: 231; Dochow 2022: 101). Daraus lassen sich zusammenfassend die folgenden Kernkontrollen für diese Phase hervorheben: Die Dokumentation aller vier Plantypen sollte sichergestellt werden, deren Zielsetzung, Verantwortlichkeiten, Aktivierungsgrenzwerte und Zuständigkeitsbereiche klar definiert sind. Ferner sollte die inhaltliche Abdeckung aller kritischen Ressourcen, Prozesse, Krisenszenarien und Schutzwerte sichergestellt sein. Die Pläne sollten in einer zentralen Datenbank für das ganze Unternehmen dokumentiert werden. Die Abstimmung zwischen den Plänen sowie deren Effektivität können durch eine geeignete Teststrategie und -Planung, sowie spezifische Fortbildungen und Übungen verifiziert werden. Die Pläne und Tests sollten von den Entscheidungsträgern bestätigt und detaillierte Testberichte, sowie insbesondere Korrektivmaßnahmen dokumentiert werden.

7.2.5. Planaktivierung und Krisenmanagement

Für die Planaktivierung ist zwischen einem Zwischenfall und einer Krise zu unterscheiden. Ein Zwischenfall („Incident“) ist ein Ereignis, durch welches eine Gefahr für die Abläufe des Unternehmens entstehen kann. Der Zwischenfall kann, aber muss nicht zu einer Krise führen, welche als außerordentliche Situation beschrieben werden kann, durch welche das Unternehmen Schaden in seiner finanziellen oder strukturellen Integrität nehmen kann, eine Gefährdung der Gesundheit seiner Mitglieder, der Fortführung der Prozesse beziehungsweise Reputation erleiden kann. Eine Krise kann folglich eine Unterbrechung kritischer Ressourcen

und Prozesse einschließen, muss jedoch nicht zwingend diese beinhalten, wie das Beispiel des Datenverlusts zeigt. Das Krisenmanagement inkludiert folglich die akute Bewältigung von Ereignissen, welche nicht mehr im Rahmen der gängigen Organisationsstrukturen und Abläufe bewältigt werden können.

Die Identifizierung einer Krise wird durch die Entscheidungshilfen in den Koordinations- und spezifischen Pläne für Krisenszenarien unterstützt. Dadurch soll eine Differenzierung zwischen bedrohlichen, aber noch durch die Fachabteilungen zu bearbeitenden Zwischenfällen einerseits und einer Krise, welche ein hohes Schadenspotential für das Unternehmen einschließt anderseits ermöglicht werden. Die in den Plänen ex ante definierten Aktivierungsgrenzwerte können den Entscheidungsträgern Referenzwerte bieten und Entscheidungshilfe sein, bevor die jeweiligen Pläne aktiviert werden und die eingeübten Prozeduren anlaufen. Die Reaktionsgeschwindigkeit ist im Krisenmanagement von großer Bedeutung, da die eingeleiteten Maßnahmen eine proaktive, gestaltende Rolle ermöglichen sollen, anstatt nur auf die Dynamik der Situation zu reagieren. Zu diesem Zweck ist ein internes Kontroll- und Überwachungssystem notwendig, um Meldungen über Zwischenfälle auf ihr Krisenpotential hin zu untersuchen („incident monitoring system“). Denn die Historie einer Krise beginnt in der Regel mit einem Zwischenfall, dessen Feststellung am Wahrscheinlichsten durch eine Fachabteilung oder einen Ressourcenverantwortlichen getroffen wird.[490]

Im Incident Management bestimmt die initiale Bewertung der Situation – welche häufig unter einer unzureichenden Informationslage verläuft - welche primäre Reaktion folgt. Ist der Zwischenfall, etwa ein Applikationsausfall, zeitlich begrenzt und vermutlich schnell zu beheben, wird der Ressourcenverantwortliche mit der Lösung des Problems beauftragt. Zeichnet sich allerdings die Prognose ab, dass der Ausfall länger andauern und kritische Geschäftsprozesse durch den Ausfall der Applikation unterbrochen werden könnten, ist von einem Krisenpotential auszugehen. Dies bedeutet, dass eine zentrale Koordinationsstelle, vorzugsweise mit funktionaler oder personaler Schnittstelle zum Krisenstab in die Bearbeitung des Problems federführend eingebunden wird. Alle folgenden Entscheidungen sollten zentral

[490] Ein Sonderfall ist das Szenario des Datenverlusts. Durch die EU-DSGVO sind unternehmen in der EU verpflichtet eine Verletzung der Vertraulichkeit sensibler Kundendaten innerhalb von 72 Stunden an die Kommission zu melden, falls Risiken für die betroffenen Personen bestehen. Unterbleibt diese Benachrichtigung sind Strafzahlungen von bis zu vier Prozent des Jahresumsatzes möglich (EU-DSGVO 2016: 33). Diese knappe Frist ist nur durch ein effektives System zur Identifizierung und Meldung von Zwischenfällen möglich, denn vom ersten Indiz bis zur Verifizierung eines Datenverlusts kann die Zeitmaßgabe zur Bekanntmachung verstreichen und zu einer Reputationskrise beziehungsweise einem hohen finanziellen Schaden führen.

dokumentiert werden, um die Kommunikation der getroffenen Entscheidungen im Unternehmen, mindestens aber mit den relevanten Fachbereichen sicherzustellen.

Wie Krisen während der ethnographischen Beobachtung zeigten, erfordert die Arbeit des Krisenstabs ein hohes Maß an Dynamik und Flexibilität von den beteiligten Akteuren.[491] Die beständige Analyse der Situation und möglicher Lageveränderungen ist daher ebenso von großer Bedeutung, wie auch die Bereitschaft vom eingeschlagenen Pfad der Krisenreaktion abzuweichen, wenn die Situationsbewertung eine Alteration des Handelns suggeriert. Während der Corona-Krise oder Energiekrise in Folge des Kriegs in der Ukraine zeigte sich zudem die Notwendigkeit zur langfristigen Lagebeobachtung und Beurteilung. Unternehmen sollten daher auch ausreichendes geschultes Personal und Einrichtungen vorhalten, um solche Ereignisse über einen längeren Zeitraum hinweg zu beobachten und Entscheidungen für die Organisation vorbereiten zu können. Die Funktion des Krisenmanagements versteht sich zwar als Ausführung der vorbereiteten Lösungsoptionen für dezidierte Szenarien, muss aber auch stets die Besonderheit jeder einzelnen Krisensituation berücksichtigen. Daher sollte Wert darauf gelegt werden, sowohl den Mitgliedern des Entscheidungsgremiums die notwendige Ausbildung zu Teil werden zu lassen, als auch durch Übungen und Modifikationen der Szenarien die adaptiven und agilen Anforderungen der Krisenstabsarbeit im Vorfeld zu erlernen (Scherrer 2018: 89). Zusammenfassend können als Kernkontrollen für die letzte Phase die klare Definition von Aktivierungsrichtwerten für Pläne und ein Früherkennungssystem in der Lage sein, eine Krise eindeutig zu erkennen und einzuordnen. Abschließend ist hervorzuheben, dass alle Mitglieder des Krisenmanagements an Fortbildungen und Maßnahmen zur Einübung der Aktivitäten im Krisenfall partizipieren sollten, um effektiv reagieren zu können.

7.3. Herausforderungen einer erfolgreichen Implementierung

Nachdem wir nun die Kernkontrollen zur Umsetzung eines integrativen Risikokontrollsystems betrachtet haben, wollen wir im Folgenden die Herausforderungen und möglichen Probleme einer erfolgreichen Implementierung thematisieren. Die konkreten Schritte und Schwierigkeiten werden sich je nach Unternehmen unterschiedlich darstellen, aber dennoch können als Schlussfolgerung unserer ethnographischen Beobachtung einige Problemfelder identifiziert werden, deren individuelle Lösung wesentlichen Anteil an der erfolgreichen Sicherstellung der Prozess- und Kommunikationskontinuität in Unternehmen haben. Wie die Erfahrung zeigt, trägt größere Veränderung in einem Unternehmen die inhärenten Herausforderungen in sich, bestehende Strukturen anzupassen (vgl. Kotter 2008), der

[491] Vgl. (Hintergrundgespräch 26.11.2020).

Komplexität der Veränderung Rechnung zu tragen, sowie die beteiligten Akteure zuerst von der Notwendigkeit und im zweiten Schritt von den Vorteilen der gewählten Lösung zu überzeugen.

Dazu werden wir im Folgenden zwei wesentliche Aspekte der Herausforderungen zur Umsetzung der Risikokontrolle durch Resilienz in Unternehmen ansprechen. Zuerst werden wir uns auf das (1) hierarchische Modell und seine Auswirkungen auf die Akzeptanz von Veränderung beziehen. Zweitens soll die (2) zeitliche Dimension der Veränderung reflektiert werden, um die Anpassungsfähigkeit der Organisation zu gewährleisten. Mit Blick auf die umfassenden Folgen der Corona-Pandemie auf die Organisation während der ethnographischen Beobachtung zeigt sich auch, dass es ein entscheidender Schritt innerhalb einer erfolgreichen Veränderung ist, die Dringlichkeit aufzuzeigen und diese Erkenntnis bei den Entscheidungsträgern aufrecht zu erhalten. Die folgenden Herausforderungen stellen Erkenntnisse der ethnographischen Untersuchung dar und beinhalten Beobachtungen und Einsichten aus den Gesprächen mit Experten zu dieser Thematik. Unter dem Eindruck einer allgemeinen Anschlussfähigkeit werden diese Erkenntnisse verallgemeinert und mit Blick auf das hierarchische Modell und die zeitliche Perspektive der Implementierung von Resilienz im Folgenden dargestellt, um die möglichen Probleme in Unternehmen auf diesem Weg aufzeigen zu können.

Dies ist insbesondere wichtig um zu verhindern, dass der Veränderungsprozess nach kurzer Zeit nachlässt. Diesen Aspekt wollen wir im Folgenden als (1) hierarchische Herausforderung betrachten und insbesondere die Artikulation der Notwendigkeit zur Adaption an die Risiken des Cyberzeitalters thematisieren. In hierarchischen Modellstrukturen hängt die Umsetzung von der Unterstützung durch die Entscheidungsträger ab. Letztere bilden die primäre Zielgruppe der Veränderungen, da ihr Votum über die Fortsetzung des Veränderungsprozesses entscheidet und die notwendige Ressourcenzuteilung für den Erfolg einer auf infrastrukturellen Redundanzen und Ressourcen beruhenden Vorsorgeplanung essentiell ist (Wüllenweber, Jahner und Krcmar 2008: 2). Der erste Schritt der Realisierung einer resilienten Organisation beruht daher auf drei Säulen, erstens der Vermittlung von Dringlichkeit[492], zweitens der

[492] Insbesondere die Lücke zwischen bekannten Risiken und (noch) unbekannten Bedrohungsszenarien sollte eine argumentative Aussagekraft entwickeln, um die geschäftsgefährdenden Risiken einer informationsbasierten Wertschöpfungskette darzustellen (AGCS 2018: 9). Ferner sollten Rückschlüsse auf die Mitigationsoptionen bestehender Lösungen zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen gleichberechtigt neben der Vorsorgeplanung für den potentiellen Ausfall der anderen vier Ressourcen sichergestellt werden können. Diese Lücken sind folglich der Anknüpfungspunkt zur Harmonisierung von Schutzvorkehrungen und Investition in infrastrukturelle und organisatorische Veränderungen zur effektiven Mitigation der Risiken (Karim 2011: 183).

Zusammenführung eines integrativen Kontrollsystems entgegen der Widerstände der bestehenden Organisationsstruktur und drittens der Entscheidung zur proaktiven Bereitstellung von infrastrukturellen Ressourcen, auf deren Basis das Risikokontrollsystem aufgebaut werden kann. Wenn die Kontrollen aus unterschiedlichen Fachfunktionen in ein Rahmenwerk oder übergeordnetes Risikokontrollsystem überführt werden können, kann ein Kompromiss zwischen Fachfunktionen, Risiko- und Auditfunktion gefunden werden.

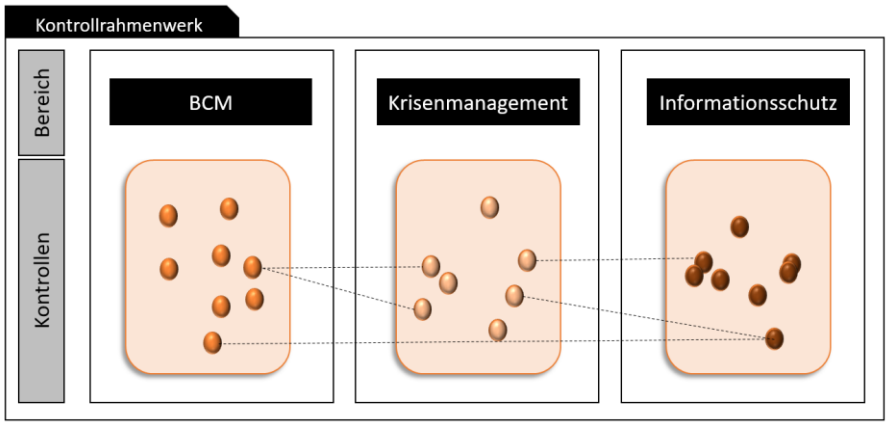

Abb. 7.8 Kontrollrahmenwerk für das Zielbild einer resilienten Organisation. Eigene Darstellung.

Die Zusammenführung unterschiedlicher Verantwortlichkeiten innerhalb eines Unternehmens zu einem integrierten Kontrollsystem verspricht Abhilfe für die identifizierten Schutzlücken an den Schnittstellen der beteiligten Verantwortungsbereiche. Die Kernidee basiert auf der Vernetzung aller relevanten Risikokontrollen aus dem Resilienz-, Risiko-, Kontinuitäts- und Krisenmanagement, der IT-Strategie sowie dem Informationsschutz, unter welchem zusätzlich Aspekte aus den Bereichen Datenschutz, IT-Sicherheit, Outsourcing-Steuerung und physikalischer Sicherheit zu subsummieren sind. Die Verknüpfung aller Kontrollen aus diesen Bereichen ermöglicht ein zusammenhängendes und abgestimmtes Steuerungssystem für die Schutzziele der resilienten Organisation, während die individuellen Zuständigkeiten weiterhin funktional-getrennt verwaltet werden können. Dies kann helfen, die Akzeptanz für die Veränderungen zu heben und die Beteiligung aller involvierten Akteure für die Implementierung effektiver Schutzmechanismen sicherzustellen.

Daher ist es auch wichtig zu verdeutlichen, dass Resilienz als Konzept weniger auf die Bewältigung einer konkreten Bedrohungslage oder einzelnen Ressource abzielt (Cook 2010: 28), sondern sich durch die Fähigkeit ausdrückt, auf dynamische Situationen flexibel reagieren zu können (Fekete, Grinda und Norf 2016: 220). Diese (2) zeitliche Dimension reflektiert die Ausrichtung von Resilienz am fortwährenden Prozess der Sicherheitsproduktion. Daher ist es notwendig in hierarchischen Modellen nach klassischer ökonomischer Rationalität die Vorteile

des konstanten Veränderungs- und Anpassungsprozesses (Nicoll und Owens 2013: 50) hinzuweisen, welcher am Ende die Funktionsfähigkeit und Existenz des Unternehmens sichern kann und dadurch die fortlaufenden Investitionen rechtfertigt (Christensen und Petersen 2017: 1443). In diesem Kontext kann zwischen „harten“ und „weichen“ Resilienzaspekten“ unterschieden werden. Infrastrukturelle Maßnahmen, wie redundante Datenbanken, physikalisch oder virtuell isolierte Server oder bauliche Abtrennungen werden unter dem Aspekt der „harten“ Investitionen verstanden (Kahan, Allen und George 2009: 5). Die zweite Gruppe von „weichen“ Aspekten umfasst verhaltensorientierte Maßnahmen, durch welche die Risikoperzeption der Mitglieder geschärft und Reaktionsmuster im Unternehmen eingeübt werden sollen. Beide Aspekte bedürfen materieller und immaterieller Ressourcen, welche durch Entscheidungsträger zugewiesen können.

Nachdem die Zustimmung der Entscheidungsträger zum Veränderungsprozess gesichert ist, sollte auch deren fortschreitender Unterstützung Rechnung getragen werden, was auf die zeitliche Dimension der Umsetzung abzielt. Da wir hier Resilienz als Richtung und weniger als Zustand verstehen sind fortwährende Anpassungen an die Dynamiken der exogenen Risiken vorzunehmen. Wie die Corona-Pandemie oder die Energiekrise in der ethnographischen Beobachtung zeigten, stehen Prozesse und Anwendungspraktiken in einer sich ändernden Umweltsituation unter Anpassungsdruck.[493] Resilienz beschreibt als Konzept die Abkehr vom traditionellen Risikoverständnis und verfolgt mit Blick auf die prozess-orientierte Risikokontrolle einen Ansatz, der gleichermaßen agil und adaptiv auf die Umwelt reagiert(Blum et. al. 2016: 155). Die zeitliche Länge der notwendigen Bereitschaft zur Veränderung ist dabei unbefristet. Dieser Prozess wird insbesondere zur Herausforderung, wenn die verfügbaren Ressourcen in einem Unternehmen bereits mit der Adaption an die digitale Umgebung in laufenden Projekten und Reformprogrammen gebunden sind und zusätzlich auf resiliente Strukturen und Anpassungen achten müssen.[494]

7.4. Zusammenfassung- Handlungsfelder und Prioritäten

Zusammenfassend lässt sich festhalten, dass die Erkenntnisse der ethnographischen Untersuchung in diesem Kapitel zusammengeführt wurden und in der Betrachtung der Anforderungen an die Umsetzung von Resilienz resultiert. Als zentrale Schlussfolgerung aus

[493] Vgl. Hintergrundgespräch 23.11.2022.

[494] Dies zeigte sich mit Blick auf Investitionen und Veränderungsbereitschaft während der ersten Monate der Corona-Pandemie, über die eine Verantwortliche sagte, dass zu dieser Zeit keine strukturellen Veränderungen möglich waren, da der Anpassungsdruck auf die Organisation durch die Krise zu groß gewesen sei (Hintergrundgespräch 11.05.2020).

der beobachtenden Teilnahme konnte konkludiert werden, dass der Übergang vom traditionellen Risikoverständnis und der einhergehenden Anwendungspraktiken in einen systemischen Ansatz zur Risikokontrolle mithilfe der Resilienz aufwendig ist und Unternehmen vor Herausforderungen stellt, um den Umgang mit Risiken im Informationszeitalter zu bewältigen. Resilienz bedeutet daher auch die „Abkehr von der tradierten Sicherheits- und Ordnungsfixierung“ (Blum et. al. 2016: 155) durch den Perspektivenwechsel von objektbezogenen Risikoverständnis hin zur Existenzsicherung der Organisation durch die Vermeidung eines Kommunikationsabbruchs. Dieses Konzept basiert auf der Einbeziehung der komplexen Komponenten der unternehmensinternen Sicherheitsproduktion in einen integrierten Ansatz zur Risikokontrolle, namentlich durch die Selbstreferenz der Organisation und Umsetzung durch Resilienz. Dazu ist es erforderlich die drei Schutzdimensionen der Verfügbarkeit, Vertraulichkeit und Integrität zusammenzuführen und ihre Anwendungspraktiken und Kontrollen zu verknüpfen. Die nachfolgende Übersicht zeigt die notwendigen Komponenten und Kernkontrollen der jeweiligen Anwendungspraktiken auf.

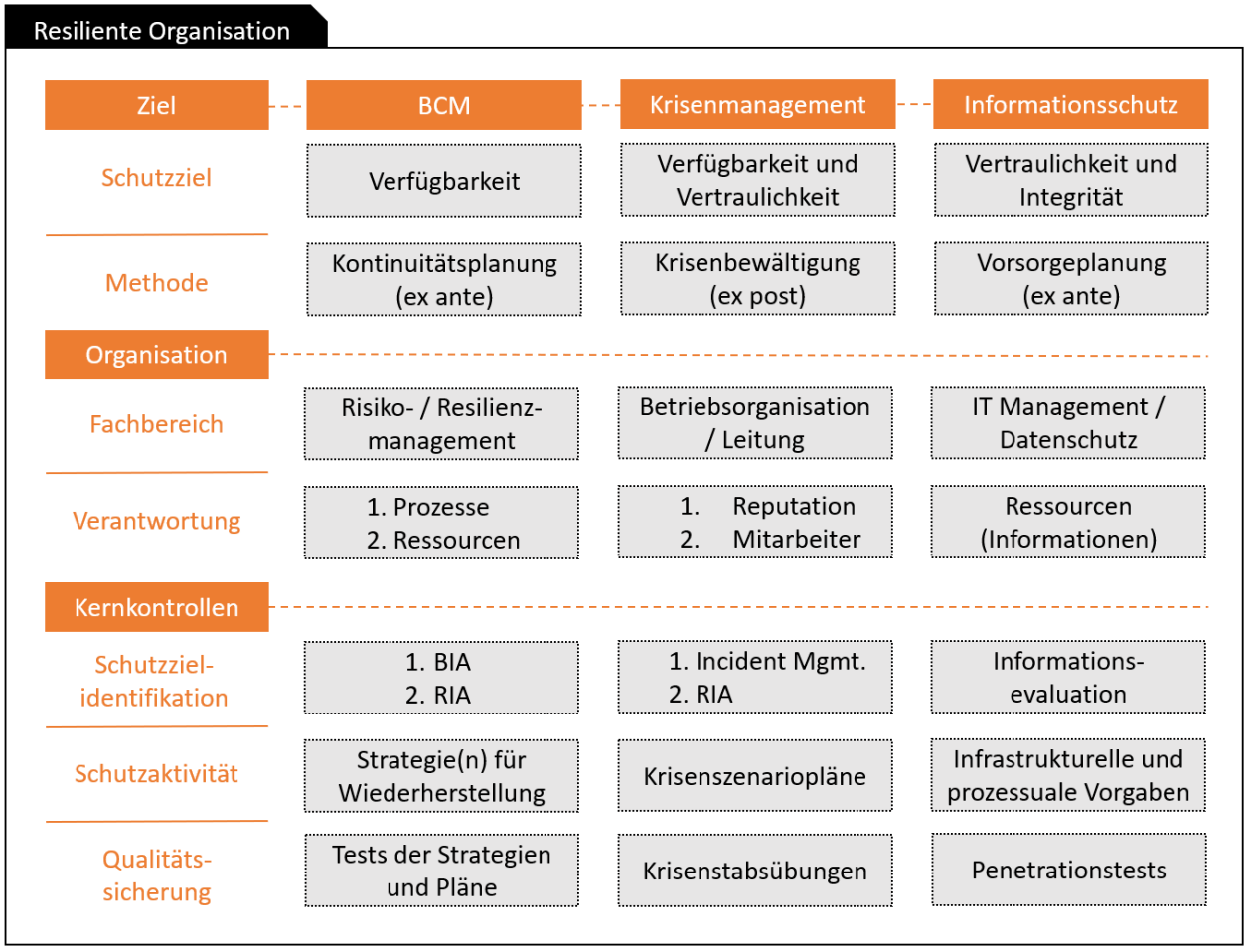

Abb. 7.9. Integrativer Ansatz einer resilienten Organisation. Eigene Darstellung.

Das in diesem Kapitel vorgestellte integrative Risikokontrollsystem einer resilienten Organisation baut daher auf den Erkenntnissen der Untersuchung auf und intendiert die dadurch abgeleitete Verbindung der Komponenten und Kontrollen auszubauen, ohne jedoch den strukturellen Umbau im Unternehmen zu überreizen.[495] Die kontrollbasierte Logik eines ganzheitlichen Schutzniveaus für die kritischen Prozesse bietet sich daher an, um angesichts der Herausforderungen der Veränderungen durch die Digitalisierung die Implementierung voranzutreiben. Neben den hierarchischen Herausforderungen der Umsetzung ist die zeitliche Dimension zu beachten, deren kurz- oder langfristige Ausrichtung über die Nachhaltigkeit der angestrebten Veränderung entscheiden kann. Die Einbeziehung aller relevanten Akteure in den Entscheidungsprozess ist daher ebenso wichtig, wie eine grundlegende Positionierung und Kommunikation der Entscheidungsträger hinsichtlich der angestrebten Risikoexposition des Unternehmens. Auch mit Blick auf Krisenereignisse wie der Corona-Pandemie oder der Energiekrise bestätigten sich im Gespräch mit den Experten während der ethnographischen Beobachtung die Relevanz von Flexibilität und Adaptionsfähigkeit, um auf die Risiken und veränderten Bedingungen der Umwelt zu reagieren. Der Umgang mit der Unsicherheit im Kontext des Informationszeitalters und der gestiegenen Bedrohungen sind somit ein relevanter Anlass für Unternehmen, um ihre Sicherheitsproduktion zu überdenken und die eigenen Rationalitäten mit den Sicherheitsdispositiven der Gesellschaft, für deren Grundbedürfnisse und Sicherheit zunehmend auch Unternehmen relevant werden, in Einklang zu bringen.

[495] Eine Expertin schilderte die aus ihrer Sicht schwierigen Gespräche mit ihrer Führungsebene aus dem Jahr 2020 über Investitionen in Projekte zur Vereinheitlichung von Kontrollen über Funktionsgrenzen hinweg. Zeitgleich zur ersten Welle der Corona-Pandemie und inmitten der Einstellung der Organisation im neuen Arbeitsmodus erwies sich die Bereitschaft zur Umstrukturierung aus ihrer Sicht begrenzt zu sein (Hintergrundgespräch 11.05.2020). Zwei Jahre später berichtete die gleiche Expertin über wesentliche Fortschritte auf diesem Bereich, da sich die Organisation nun an die Belastungen und (dauerhafte) Krise gewöhnt zu haben schien (Hintergrundgespräch 28.07.2022).

8. Abschlussbetrachtung

Zum Abschluss der Arbeit sollen die Erkenntnisse und Schlussfolgerungen reflektiert und zusammengefasst werden. Daher gliedert sich dieses letzte Kapitel in zwei Abschnitte, welche die wesentlichen Erkenntnisse zusammentragen und weitere Forschungsmöglichkeiten in diesem Bereich ansprechen. Der erste Abschnitt wird die (1) Ergebnisse dieser Arbeit reflektieren und die Entwicklung der Sicherheitsproduktion in Unternehmen und ihres Beitrags zum gesellschaftlichen Sicherheitsdispositiv zusammenfassen. Darunter wird auch der abschließende Überblick über die Bedeutung der Digitalisierung für diese Entwicklung, sowie die Verschiebung des Risikoverständnisses in Unternehmen unter dem Eindruck der Vermeidung eines Kommunikationsabbruchs thematisiert werden. Der zweite Abschnitt wird einen (2) Ausblick über die möglichen Anschlussbetrachtungen zu dieser Arbeit geben. Darunter wird auch die Relevanz der Sicherheitsproduktion in Unternehmen für die IPS, IPÖ und Organisationsforschung beleuchtet und auf die Anschlussfähigkeit in diesen Disziplinen eingegangen werden.

8.1. Ergebnisreflektion

Die folgende Reflektion der Erkenntnisse soll die Vorgehensweise und den Aufbau der vorliegenden Arbeit nachzeichnen und dabei die Schlussfolgerungen und Kernaussagen der jeweiligen Kapitel in einen Kontext setzen, welcher die Folgen der Digitalisierung für die Sicherheitsproduktion in Unternehmen herausstellt. Darunter nimmt die Reflektion der Vorgehensweise und insbesondere der methodischen Struktur eine wichtige Rolle ein, um den Pfad zu den nachfolgend dargelegten Schlussfolgerungen zu erklären. Daher werden erstens die Exposition und Einordnung der Arbeit in die Forschung und Literatur zusammengefasst und zweitens das methodische Vorgehen reflektiert. Auf dieser Grundlage des ersten Themenblocks werden wir drittens die Folgen der Digitalisierung für Unternehmen und ihre ökonomischen Rationalitäten zusammenfassen. Zum anderen soll auf die Erkenntnisse aus der theoretischen Betrachtung durch die soziologische Organisationsforschung eingegangen werden, welche die theoretische Struktur zur Analyse der Sicherheitsproduktion in Unternehmen als Reproduktion von Anschlussoperationen einführte. Abschließend wird viertens auf die Erkenntnisse der ethnographischen Untersuchung für die Sicherheitsproduktion in Unternehmen und dem daraus hervorgehenden Schlussfolgerungen für die Selbstbetrachtung der Organisation und der Umsetzung durch Resilienz referenziert werden. Dadurch soll die Kombination aus theoretischer Einordnung zum Organisationsverständnis einerseits und der ethnographischen Auswertung zur Sicherheitsproduktion andererseits komplementiert werden.

8.1.1. Exposition und Einordung in die Forschung

Unsere Überlegungen zu der vorliegenden Arbeit begannen mit dem unternehmensinternen Risikodiskurs zu Herausforderungen im Zuge der Corona-Pandemie, welche sich aufgrund der Problematik aus exogen vorgegebenen Sicherheitsdispositiven einerseits und ökonomischer Rationalität und Entscheidungsfindung in Unternehmen andererseits stellten. Dies führte zu der Frage, wie sich dies in die (1) Produktion von Sicherheit in Unternehmen übersetzt und welche Folgen sich in diesem Zusammenhang durch die Digitalisierung ergeben? Die Beschleunigung der Virtualisierung von Arbeitsprozesse und Ausdehnung der Vernetzung von Systemen in Folge der Corona-Pandemie gaben diesem Feld schließlich eine neue, erweiterte Kontur. Die Herausforderungen durch exogene Problemsituationen schufen in Unternehmen eine in diesem Kontext neue Betrachtung der internen Risikokontrollsysteme. Eine ökonomische Rationalität auf den Führungsebenen von Unternehmen traf auf der einen Seite mit der Notwendigkeit nicht-ökonomischer Fragestellungen zur Sicherstellung der eigenen Handlungsfähigkeit auf der anderen Seite zusammen und machten, wie im ersten Kapitel dargelegt wurde, eine Veränderung der Risikokontrolle in Unternehmen notwendig.

Allerdings war die Rolle von Unternehmen in der Sicherheitsproduktion durch die Literatur der Internationalen Beziehungen bisher vorrangig auf die Erbringung eines Beitrags zur Sicherheit durch Unternehmen und im Auftrag einer staatlichen Autorität ausgerichtet. Die Unterscheidung zwischen Sicherheitsproduktion *durch* Unternehmen einerseits und anderseits durch Einbeziehung der sicherheitsrelevanten Aktivitäten *in* Unternehmen um ihre eigenen Prozesse und Kommunikation aufrechtzuerhalten, bot daher eine neue Perspektive auf die Rolle von Unternehmen für das gesellschaftliche Sicherheitsdispositiv. Diese Differenzierung und das Zusammentreffen von ökonomischen Rationalitäten und exogenen Sicherheitsdispositiven ermöglichte zudem eine Verortung dieser Arbeit in der Schnittmenge aus Internationaler Politischer Ökonomie, der Internationalen Politischen Soziologie sowie der soziologischen Organisationsforschung über die theoretische Betrachtung von Organisationen und der Bedeutung von Anschlussoperationen.

8.1.2. Methodisches Vorgehen und Erkenntniseinbindung

Diese Einordnung wurde im zweiten Kapitel weiter betrachtet und dabei die (2) Fragestellung und ihre Anschlussfähigkeit des Forschungsthemas zu den Forschungsfeldern der IPÖ, der IPS Soziologie und der organisationstheoretischen Forschung im Detail besprochen. Die Rolle privater Autoritäten war daher ein wichtiger Schritt, um die Betrachtung von Unternehmen als Akteure der Sicherheitspolitik nachzuzeichnen. Diese Perspektive wurde zwar bisher der

staatszentrierten Perspektive in der Sicherheitsliteratur untergeordnet, doch veränderte sich dieses Bild durch die Verantwortung von privaten Betreibern kritischer Infrastruktur wie Wasser- oder Elektrizitätswerken. Einen wichtigen Schritt in der veränderten Perspektive konnte durch die zunehmende Bedeutung der Digitalisierung für das gesellschaftliche Leben attestiert werden und die Rolle von Unternehmen in der Bereitstellung der dazu notwendigen (IT-)Infrastruktur und Plattformen für die öffentliche Grundversorgung beobachtet werden.

Daher stellte sich die Frage wie die Betrachtung von Unternehmen und ihrer internen Sicherheitsproduktion methodisch verortet werden kann? Mit Rückgriff auf die Kopenhagener Schule und ihrem Verständnis der Versicherheitlichung beziehungsweise der ethnographischen Methodik der Pariser Schule bietet sich hier eine Vorgehensweise an, um den Blick in die Organisation zu richten und die Praktiken und Prozeduren der handelnden Akteure innerhalb von Unternehmen und ihrer Bedeutung für die Sicherheitsproduktion unter dem Eindruck ihrer besonderen Rolle für die Digitalisierung zu untersuchen. Daraus leitete sich die Strukturierung der ethnographischen Untersuchung ab, welche in dieser Arbeit angewendet wurde, um die Prozesse zur Risikokontrolle in Unternehmen zu beobachten und Schlussfolgerungen für den Umgang mit den zuvor genannten exogenen, nicht-ökonomischen Problemfeldern einerseits und dem klassisch ökonomischen Rationalitäten routinierter Entscheidungsfindung in Unternehmen zusammenzubringen.

Mit Blick auf die Methodik der ethnographischen Untersuchung bot sich durch die Position in einem im DAX-30 gelisteten Unternehmen über einen langjährigen Zeitraum hinweg und in wechselnden Rollen die Möglichkeit, die Praktiken und Diskurse innerhalb eines Unternehmens mit Blick auf die Sicherheitsproduktion genau zu beobachten. Die Erhebung der Daten erfolgte über den Zeitraum von 2012 bis 2022 und untergliederte sich in die Auswertung von Dokumenten wie Branchenstandards und Positionspapieren, Fragebögen und Gesprächen mit Experten im Rahmen der beruflichen Tätigkeit[496], sowie Hintergrundgesprächen zum dezidierten Zweck der Datenerhebung für diese Arbeit. Dennoch ergab sich die Einschränkung, dass alle Informationen vertraulich behandelt werden mussten und keine Mitschriften oder Aufzeichnungen während der Hintergrundgespräche angefertigt werden durften. Allerdings

[496] Dokumente und Informationen, die im Rahmen der Tätigkeit im Unternehmen zu beruflichen Zwecken erstellt wurden sind aufgrund des Arbeitsvertrages Eigentum des Unternehmens. Diese Informationen dürfen daher nicht direkt zitiert oder außerhalb des Unternehmensnetzwerkes abgelegt werden. Allerdings ermöglichten diese Gespräche eine allgemeine ethnographische Beobachtung über strukturelle Veränderungen im Unternehmen mit Blick auf die Sicherheitsproduktion, deren wichtigste Elemente über Hintergrundgespräche zum dezidierten Zweck der wissenschaftlichen Arbeit konkretisiert und dokumentiert wurden.

wurden Gedächtnisprotokollen nach den Gesprächen angefertigt, welche eine systematische Auswertung der Erkenntnisse ermöglichen.

Die Erkenntnisse für die Entwicklung des Risikodiskurses und Veränderung der Risikokontrolle durch die Digitalisierung, insbesondere die Etablierung der Selbstbetrachtung der Organisation und Umsetzung in Form von Resilienz wurden über die ethnographische Untersuchung im Unternehmen verfolgt und dokumentiert. Diese Erkenntnisse wurden zum Einem als Rückblick auf die Entstehung von BCM und KM in den jeweiligen Abschnitten des fünften Kapitels eingebunden. Zum Anderen wurden die Erkenntnisse aus der Beobachtung im sechsten beziehungsweise siebten Kapitel als Folge der veränderten Risikokontrolle und Umsetzung von Resilienz im Unternehmen angewendet, um den Prozess der Veränderung im Risikodiskurs und Risikokontrolle zu beschreiben. In der hier nachfolgenden Betrachtung der Kapitel und ihrem Beitrag zur Bearbeitung der Fragestellung werden wir erneut auf die spezifischen Erkenntnisse der ethnographischen Betrachtung eingehen. Zuvor wurde die Ausgangslage für die Veränderungen und Implikationen der ökonomischen Rationalitäten für Unternehmen durch die Digitalisierung vorgestellt, welche im Folgenden reflektiert wird.

8.1.3. Folgen der Digitalisierung für Unternehmen und Organisationstheorie

Auf der Grundlage der exogenen Sicherheitsproblematik in Folge der Corona-Pandemie und der Einordnung der Fragestellung in die Literatur der Internationalen Beziehungen folgte im dritten Kapitel die Analyse der weitreichenden Veränderungen durch die (3) Digitalisierung. In diesem Kapitel wurden die relevanten Begriffe in diesem Kontext definiert, um ein allgemeines Verständnis der Veränderung und Bedeutung für die ökonomische Ausrichtung von Unternehmen im Informationszeitalter zu gewinnen. Aufbauend auf der Vernetzung von Daten, Konfigurationskomponenten und Systemen, bedeutet die fortschreitende Digitalisierung vor allem die Erhöhung von globalen Interdependenzen und den schrittweisen Abbau lokaler (Risiko-)Autarkie, wie es die Beispiele und Facetten im dritten Kapitel beleuchteten. Das ökonomische Potential des akkumulierten Wissensbestandes aus einer Vielzahl an generierten Daten liegt in der Möglichkeit die gesammelten Informationen in zielgerichtete Produktion, individualisierte Vermarktung und Produktplatzierung zu überführen. Daher wurden Informationen hier als der eigentliche Wertmaßstab des digitalen Zeitalters verstanden. Der Zugriff auf die durch zunehmende Vernetzung und Dokumentation gekennzeichneten Informationen, legt den Grundstein für die moderne Informationsgesellschaft. Auf der anderen Seite fordert dies aber gleichzeitig Anpassungsleistungen und Investitionen von Unternehmen,

um mit den Veränderungen Schritt zu halten, aber gleichzeitig die eigene Risikokontrolle weiterzuentwickeln.

Wie die Analyse und Differenzierung der Risikokontrollsysteme im analogen und dem digitalen Zeitalter zeigte, sind divergente Normen und Grundsätze zu beachten, welche das Verhalten und die Entscheidungen von Unternehmen prägen. Allen voran artikuliert sich diese Entwicklung im Fall von Informationen, deren Wert durch die virtuellen Wertschöpfungsketten und Logik der Informationsgesellschaft signifikant an Bedeutung gewonnen haben. Dies drückt sich folglich in der Definition von Schutzwerten von Unternehmen aus, in denen der Schutz von Informationen neben anderen kritischen Ressourcen eine essentielle Relevanz für die jeweiligen Unternehmen und ihre Prozess- und Kommunikationskontinuität hat. Dies übersetzte sich im vierten Kapitel in die Auseinandersetzung mit dem (4) Organisations- und Risikobegriff im Informationszeitalter. Mit Blick auf das organisationstheoretische Modell von Niklas Luhmann bedeuteten die Veränderungen durch die Digitalisierung vor allem eine Verschiebung der Außengrenzen von Unternehmen durch die Vernetzung und Einführung neuer Technologien wie dem Cloud-Computing, durch dessen Nutzung die Anschlussoperationen und Kommunikation nicht nur exklusiv die Mitglieder der Organisation erreicht, sondern auch Infrastruktur von externen Teilnehmern des Systems tangiert und voraussetzt. Dies hat Auswirkungen auf die Autopoiesis von Unternehmen, deren Selbstreflexivität und Bedeutung von Anschlussoperationen und Kommunikation bestimmt wird. Die auf die Differenzierung von Entscheidung- und Konditionalprogrammen folgende Reproduktion und Kommunikation von Entscheidungen nach Luhmann wurde in unserer Anwendung leicht adaptiert, um die Selbstreferenz in direkte Verbindung mit den Begriffen Unsicherheit, Risiko und Gefahr zusetzen und dadurch den Blick auf die für Unternehmen sicherheitsrelevanten Implikationen der Digitalisierung zu ermöglichen.

Dies leitet zum hier verwendeten Risikobegriff über, welcher zwischen dem traditionellen Verständnis und dem neuen, systemischen Einordnung von Risiko unterscheidet. Der traditionelle Risikobegriff fokussierte sich auf die Verbindung von Schaden und Eintrittswahrscheinlichkeit hinsichtlich der betrachteten Risikoobjekte. Dieses Verständnis von Risiko wurde in Unternehmen im analogen Zeitalter durch das Risikomanagement funktionell in eine Risikokontrolle übersetzt, deren Aufgabe die Identifikation und Bewertung von Risiken sowie einer nach klassisch ökonomischer Rationalität entsprechende Risikokapitalkalkulation gegenüber gestellt wurde. Dieses Risikoverständnis unterlag einer Veränderung, als nicht-ökonomische Problemstellungen mit Blick auf die Prozess- und Kommunikationskontinuität

durch Krisenereignisse, wie den Anschlägen vom 11. September 2001 oder dem Reaktorunglück von Fukushima 2011, die operationelle Notwendigkeit zur Vorsorgeplanung mithilfe von Anwendungspraktiken des BCM und Krisenmanagements aufzeigten. Durch die theoretische Verortung von Risiko und Risikokontrolle wurden im vierten Kapitel die maßgeblichen Aspekte der unternehmerischen Sicherheitsproduktion im Sinne der soziologischen Organisationstheorie beleuchtet und dadurch die Differenzierung zwischen traditionellem und neuem Risikoverständnis vorgenommen.

8.1.4. Erkenntnisse der ethnographischen Untersuchung

Die prozessorientierte Perspektive der neuen Risikokontrollsysteme setzte sich somit konzeptionell vom traditionellen, auf Ressourcen und objekt-fokussierten Ansatz ab, um dadurch die notwendige Erweiterung des Risikobegriffs vorzunehmen, welcher auf die für Unternehmen essentiellen Anschlussoperationen und deren Kommunikation aufbaut. Diese theoretische Betrachtung wurde im fünften Kapitel durch die (5) Anwendungspraktiken und Fallbeispiele, aber insbesondere durch die Erkenntnis der ethnographischen Untersuchung reflektiert. Die Beobachtungen und Hintergrundgespräche zeigten, dass die thematisierten Krisen und Ereignisse den Risikodiskurs im Unternehmen nachhaltig in Richtung eines neuen Risikokontrollsystems beeinflussten. Dieser Zusammenhang wurde durch die beobachtende Teilnahme deutlich, in der die Erlebnisse und Erfahrungen von Praktikern mit Blick auf die Anschläge vom 11. September 2001 und dem Reaktorunglück von Fukushima 2011 zunächst aus der Perspektive des traditionellen Risikoverständnisses heraus reflektiert worden. Diese Ereignisse fanden vor der eigenen aktiven Beobachtung im Unternehmen statt, wurden aber mit Blick auf die Effektivität des traditionellen Umgangs mit Risiken in Gestalt der Wiederherstellungspläne für einzelne Ressourcen in Gesprächen mit Experten rückblickend evaluiert.[497]

Allerdings änderte sich dieser Eindruck bei einigen Experten bereits durch die komplexen Verknüpfungen von Prozessen und Systemen, welche im Zuge der Digitalisierung an Bedeutung gewannen und die Eindämmung eines Schadens auf eine Ressource oder Domäne

[497] In einem Gespräch wurde von einem Experten geschildert, der zwischen 2004 und 2007 die maßgeblichen Strategien zum Umgang mit Ereignissen wie Terroranschlägen oder Naturkatastrophen definierte, wie die Aushandlung von Rationalitäten stattfand. Der Experte schilderte im Sommer 2014 den Widerstand auf der Führungsebene, die nötigen Investitionen für die angestrebten Maßnahmen zu bewilligen. Daraus prägte sich für den Experten das Bild, dass die ökonomische Rationalität des Unternehmens durch ein Risikonarrativ angesprochen werden muss, um Entscheidungsträger von der Notwendigkeit der Investitionen zu überzeugen (Hintergrundgespräch 16.06.2014).

immer schwieriger erscheinen ließen.[498] Die zeitgleiche Ausdehnung von Prozessen im Unternehmen auf der Grundlage von verknüpften Systemen und der Zusammenlegung von IT-Infrastruktur reflektierte zwar die ökonomische Rationalität, nicht aber das Sicherheitsdispositiv im Informationszeitalter. Aus diesen Gründen merkten in den Gesprächen zwischen 2017 und 2018 einige Gesprächspartner den Aufbau einer systemischen Risikokontrolle für IT-Systeme an, welche die Interdependenzen zwischen IT-Applikationen, Middleware, IT-Infrastruktur und schließlich die Endanwendungen auf Seiten der Geschäftsprozesse berücksichtigte.[499] Die wichtigste Erkenntnis der ethnographischen Beobachtung während dieser Phase war die Bedeutung der beginnenden Selbstbeobachtung des Unternehmens als eine durch Anschlussoperationen interagierende Organisation, deren Existenz von der unterbrechungsfreien Kommunikation mittels der interdependenten IT-Strukturen abhing.[500]

Diese Erkenntnis basierte maßgeblich auf der zunehmenden Vernetzung und Standardisierung von Systemen zur Unterstützung der Geschäftsprozesse, durch welche allerdings auch die potentielle Schadenswirkung in einer Komponente Auswirkungen auf das gesamte System haben würde.[501] Dadurch wurde der Risikodiskurs in eine neue Richtung gelenkt und durch die ethnographische Beobachtung weiter verfolgt, als die Etablierung von (6) Resilienz als Anwendungspraktik ein neues, systemisches Risikoverständnis markierte. Die Entwicklung der Bedrohungslage und Umgang mit der Unsicherheit im Informationszeitalter wurde daher im sechsten Kapitel weiter vertieft. Durch die beobachtende Teilnahme konnte auch die

[498] Ein IT-Architekt erzählte im Rahmen eines informellen Gesprächs über die Implikationen der während dieser Zeit durchgeführten Zusammenlegungen von Rechenzentren, dass zwar die Kosten für den operativen Betrieb dadurch gesenkt werden können, die Risikoexposition des IT-Betriebs und einer möglichen Unterbrechung von Geschäftsprozessen allerdings gestiegen sei. Insbesondere die Abdeckung von einzelnen Prozessen und Applikationen durch Wiederherstellungspläne sei unzureichend, sollte das gesamte Großrechenzentrum durch ein Schadensereignis ausfallen, da die Komplexität eines großflächigen Desasters („disaster event“) durch die gegenwärtigen Risikokontrollen nicht abgedeckt sei (Hintergrundgespräch 27.10.2022).

[499] Zwischen 2017 und 2018 wurden über zwei Dutzend Gespräche im Rahmen einer Arbeitsgruppe mit IT-Experten, BCM-Praktikern und Prozess-Verantwortlichen durchgeführt, um die Rahmenparameter eines systemischen Ansatzes zur Risikokontrolle von großflächigen IT-Unterbrechungen durch die Konzentration des Risikos in den zusammengelegten Rechenzentren abzustimmen. Die Einführung eines unternehmensweiten ITSCM-Standards unterstützte schließlich die methodische Umsetzung eines neuen Risikoverständnisses auf der Basis von prozess-orientierten Maßnahmen zur Verhinderung eines Kommunikationsabbruchs (vgl. Hintergrundgespräch 20.02.2018).

[500] Hier wurde in Gesprächen auf die Relevanz eines systemischen Blicks auf die Organisation vorgebracht, welche schließlich als Resilienz im Unternehmen umgesetzt wurde (Hintergrundgespräch 15.11.2021).

[501] Aus Gesprächen ging hervor, dass eine kurze Geschäftsunterbrechung in einer nordamerikanischen Landesgesellschaft im Jahr 2016 durch einen Angriff mittels Ransomware verursacht wurde und mit Blick auf einen zeitkritischen Prozess die Abhängigkeit von einer unterbrechungsfreien IT aufzeigte. Dieser Zwischenfall, dessen finanzielle oder reputierliche Wirkung begrenzt blieb, wurde von einem Manager als „Warnschuss“ verstanden, die systemischen Interdependenzen der IT besser zu dokumentieren und zu schützen (Hintergrundgespräch 21.09.2016).

Entscheidung zur Ausweitung der Virtualisierung von Arbeitsprozessen von Unternehmen in Reaktion auf den drohenden Kommunikationsabbruch durch Kontaktbeschränken während der Corona-Pandemie begleitet und untersucht werden.[502]

Aus Gesprächen mit Verantwortlichen wurde zudem der Eindruck bestätigt, dass der Handlungsdruck angesichts der zunehmenden Cyberbedrohung und Vernetzung von Komponenten zu komplexen Systemen eine grundlegende Überarbeitung der Risikokontrollsysteme notwendig machen würde.[503] Dies führte zu der Schlussfolgerung, dass die Verschiebung des Risikodiskurses in einer veränderten Selbstbeobachtung des Unternehmens mündete, deren Zweck die ganzheitliche, systemische Betrachtung der Prozesse und Kommunikationen innerhalb der Organisation zum Zweck der Sicherheitsproduktion zum Ziel haben müsse.[504] Aus theoretischer Sicht kann daher das konzeptionelle Bild des Kommunikationsabbruchs und dessen Vermeidung als existentielle Notwendigkeit der Organisation betrachtet werden. Als Erkenntnis aus der ethnographischen Untersuchung wird dies durch Resilienz als Begriff zur Selbstbeobachtung des Unternehmens ergänzt und ist die zentrale Erkenntnis unserer Analyse.

Im Zuge der Untersuchung konnte ferner beobachtet werden, wie Experten im Unternehmen den Begriff Resilienz zunehmend verwendeten, um einen prozess-bezogene Risikokontrolle zu bezeichnen und die systemische Planung aufeinander abgestimmter Anwendungspraktiken wie beispielsweise BCM, KM, Informationsschutz zu benennen.[505] Resilienz bedeutete als Konzept für die Sicherheitsproduktion von Unternehmen, die kritischen Prozesse, welche zur Reproduktion von Anschlussoperationen benötigt wurden, sowie die zugrundeliegenden IT-

[502] Vgl. Workshops September bis Dezember 2020.

[503] Aus den Hintergrundgesprächen mit Experten stellte sich heraus, dass die Fokussierung auf einzelne Ressourcen ungenügend sei, um die Komplexität von Prozessen und der Verwertung von Informationen entsprechenden Schutz zu bieten. Ein Praktiker kommentierte zum traditionellen Risikoverständnis im Rahmen eines Gesprächs zur Konzeption der Backup-Lösungen für das Rechenzentrum sinngemäß, dass man 10 verschiedene IT-Systeme mit 10 Wiederherstellungsplänen abdecken könne. Doch wenn das eigentliche komplexe Unterfangen der Wiederherstellung des Rechenzentrums nicht in einer abgestimmten Reihenfolge definiert sei, wäre die Mühe vergebens, weil die einzelnen Pläne ohne übergeordnete Struktur nicht der generellen Funktionsweise der Systemsequenz entsprechen würden. Dadurch zeigte sich im Rahmen der ethnographischen Beobachtung die Notwendigkeit zur übergreifenden Planung und Bezugnahme auf das systemische Bild zur Sicherstellung der Anschlussoperationen (Hintergrundgespräch 29.09.2020).

[504] Als Teil eines Projektteams aus verschiedenen Fachfunktionen konnte die Arbeit an einem neuen Standard zur Angleichung von Kontrollen aus den Anwendungspraktiken BCM, KM, ITSCM sowie Informations- und Datenschutz beobachtet werden. Die zugrundeliegende Logik basierte auf der Anpassung von Methoden zur besseren Abdeckung des systemischen Risikospektrums und Betrachtung des Unternehmens als Entität (Workshop 02.03.2017).

[505] Während der Untersuchung äußerten Praktiker im Unternehmen die Absicht, die einzelnen Domänen und Anwendungspraktiken aufzulösen und eine einheitliche, interdependente und auf Kontrollen aufgebaute Vorsorgeplanung zu schaffen, welche die Sicherstellung der Prozesse als Ganze berücksichtigen könne. Ein wiederkehrendes Motiv war sinngemäß, die Silos einzureißen und die Domänen enger zu verknüpfen (Hintergrundgespräch 03.03.2021).

Systeme in der Vorsorgeplanung als komplexe Ökosysteme[506] zu betrachten und ihre ununterbrochene Funktionsweise durch flexible und adaptive Planung zu gewährleisten. Die akute Gefährdung dieser Systeme konnte im zweiten Teil des sechsten Kapitels durch die aufgezeigten Fallbeispiele verdeutlicht werden, deren Schadensreichweite potentiell einen gesamtsystemischen Kommunikationsabbruch bedeuten könnte und für deren Bewältigung daher ein integrativer Ansatz gefordert wurde.

Die Erkenntnisse aus der theoretischen Verortung des vierten Kapitels und die ethnographische Untersuchung zu den Herausforderungen des analogen Zeitalters im fünften Kapitels sowie die einhergehenden Veränderungen des Risikobegriffs und der Bedrohungen im Informationszeitalter im sechsten Kapitel führten schließlich zu der Schlussfolgerung über die Anforderungen an die resiliente Organisation. Deren konkrete Gestalt basiert auf dem Zielbild eines (7) integrativen Ansatzes zur Risikokontrolle in Unternehmen und wurde im siebten Kapitel vorgestellt. Dieser neue Ansatz verbindet die Funktionen des Business Continuity Managements, Krisenmanagements und Informationsschutz unter dem Überbegriff der Resilienz und bezieht über eine kontroll-basierte Zusammenführung weitere Bereiche des Unternehmens mit ein. Auch hier flossen die Erkenntnisse aus der ethnographischen Untersuchung insbesondere mit Blick auf die Selbstbeobachtung einer resilienten Organisation als Bestandteil einer sich dynamisch entwickelnden Umwelt ein.[507] Wie Gespräche mit Experten aus dem Unternehmen im Zuge der Corona-Pandemie ferner zeigten, bezeichnet Resilienz in diesem Zusammenhang nicht einen finalen Zustand der Risikokontrolle, sondern eine sich entwickelnde Richtung der unternehmerischen Vorsorgeplanung, welche die Möglichkeit eines Schadensereignisses antizipiert und die Anpassungsfähigkeit und Flexibilität der internen Sicherheitsproduktion hervorstellt.[508] Dadurch entwickelte sich das normative Bild

[506] Der Begriff Ökosysteme wurde von Experten in Gesprächen seit 2018 häufiger benannt und entstammt der Informatik („Ecosystems"). Er bezeichnet hier die Konzeptualisierung von IT-Systemen, Middleware und Infrastruktur in einem zusammenhängenden Komplex, durch welchen die Interdependenz der einzelnen Komponenten und ihres Zusammenwirkens als Prozess deutlich wird. Durch diese Verknüpfung können im Sinne der Resilienz kritische Konglomerate von Systemen identifiziert und als Folge der Selbstbeobachtung effektiver durch Vorsorgemaßnahmen geschützt werden (Hintergrundgespräch 08.05.2018).

[507] Im Zuge der Corona-Pandemie stellten die Interviews mit Praktikern aus 18 Landesgesellschaften die unterschiedlichen Herausforderungen im Umgang mit der Corona-Pandemie und der einhergehenden Lockdown-Maßnahmen heraus, wie beispielsweise fehlende Hardware oder unklare Vorgaben seitens der staatlichen Autoritäten. Dennoch gelang es allen Ländergesellschaften innerhalb von zwei Wochen ausreichende VPN Verbindungen aufzubauen, um allen Mitarbeiter die Fortsetzung ihrer Prozesse am Heimarbeitsplatz zu ermöglichen. Gemeinsam waren den Schilderungen die dynamische Entwicklung der Krise und die Erkenntnis, dass Resilienz in diesem Kontext eine flexible und adaptive Herangehensweise auf die sich fortwährend verändernde Situation durch das Unternehmen bedürfe (Workshops September bis Dezember 2020).

[508] Eine der Erkenntnisse aus der Corona-Pandemie zeigte, dass die Auswahl von kritischen Prozessen zur Wiederherstellung der Sicherstellung der Prozesskontinuität unzureichend war, um die Organisation im Fall von längerfristigen Unterbrechungen, wie beispielsweise der monatelangen Kontaktbeschränkungen effektiv zu schützen. Daher wurde im Jahr 2021 die Ausweitung des Kritikalitätsbegriffs erlassen, welcher nun alle Prozesse

einer resilienten Organisation, deren Elemente hier vorgestellt und mit Blick auf die Herausforderungen zur Implementierung unter dem Licht der ökonomischen Rationalität einerseits und dem Sicherheitsdispositiv andererseits diskutiert wurden.

Das zuvor beschriebene Zusammenwirken der gegensätzlichen Systemrationalitäten zeigt daher auch das Spannungsverhältnis zwischen ökonomischer Entscheidungslogik in Unternehmen und den notwendigen Investitionen in den Schutz der Infrastruktur und Systeme zur Sicherstellung der Prozesskontinuität. Dies wurde auch aus der Perspektive des möglichen Interessenskonflikts zwischen unternehmerischen Zielen und gesellschaftlichen Sicherheitsdispositiven diskutiert, deren Schlussfolgerungen schließlich die Bedeutung von Unternehmen und der internen Sicherheitsproduktion für den gesellschaftlichen Risikodiskurs aufzeigt. Insbesondere das Forschungsfeld der Resilienz als Übersetzung der Sicherheitsproduktion in Unternehmen bietet eine aufschlussreiche und anschlussfähige Perspektive auf die Beziehung zwischen staatlicher und privater Ebene, wie der nächste Abschnitt vertiefen wird. Mit Blick auf die Verteilung von Eigentum, Wissen und Betriebssteuerung sind Unternehmen aber bereits wesentlicher Teil der staatlichen Sicherheitsbereitstellung, insbesondere wie wir für die kritische Infrastruktur sehen konnten, aber auch im Allgemeinen als Bereitsteller von mehr als 85 Prozent der Infrastruktur und Komponenten der Digitalisierung (Carr 2016: 52) und daher ein wichtiger Bestandteil der Sicherheitsarchitektur.

8.2. Ausblick

Wie die Literaturauswertung und Verortung im zweiten Kapitel zeigte, erhielten MNU in den vergangenen Jahren mehr Aufmerksamkeit in den internationalen Beziehungen, wenn auch allerdings ein staaten-zentrierter Ansatz vorherrschte. Neue Forschungsbereiche in der Internationalen Politischen Soziologie und in der Internationalen Politischen Ökonomie betrachteten nun die Teilhabe von Unternehmen an der Sicherheitsproduktion, etwa durch die Verhinderung von Geldwäsche und Terrorfinanzierung im Auftrag staatlicher Autoritäten. Auch die Bekämpfung von Korruption oder die Übernahme staatlicher Funktion durch beispielsweise private Sicherheitsunternehmen fanden Eingang in die Diskussion. Jedoch zeichnet sich hier eine notwendige Unterscheidung zwischen Sicherheitsproduktion *durch* Unternehmen einerseits, das bedeutet im Auftrag staatlicher Institutionen oder für bestimmte sicherheitsrelevante Aspekte in der Gesellschaft und Sicherheitsproduktion *in* Unternehmen

in den Anwendungsrahmen des BCM stellte und eine sequenzielle Wiederherstellung über alle Prozesse des Unternehmens einführte, um die Qualität des Prozessoutputs sicherzustellen (Workshop 19.01.2021).

andererseits ab. Eben diese Differenzierung erlaubt einen neuen Blickwinkel und Anstoß für die Sicherheitsforschung, da die Aktivitäten und Handlungsmuster von Unternehmen zur Sicherstellung ihrer eigenen Funktionsfähigkeit bisher kaum beachtet wurden.

Daher bietet sich durch die Unterscheidung zwischen Sicherheitsproduktion *durch* beziehungsweise *in* Unternehmen ein breites Feld für weitere Forschung an. Ebenso erlaubt die Betrachtung von Unternehmen in diesem Kontext an der Schnittstelle von IPS und IPÖ die jeweiligen Forschungsthemen enger zu verbinden und anschlussfähige Erkenntnisse in beide Richtungen zu entwickeln. Mit Blick auf die Methodik kann auch auf die Vorgehensweise der Pariser Schule verwiesen werden, deren Perspektive auf die internen Praktiken von Unternehmen aufschlussreich sein kann, um Unternehmen nicht nur als geschlossene Systeme von außen zu betrachten, sondern auch die Rationalitäten und Entscheidungsfindung zu reflektieren. Wie sich in dieser Arbeit zeigte, kann der potentielle Interessenskonflikt zwischen ökonomischen Rationalitäten in Unternehmen und den exogenen Sicherheitsbedrohungen einen Beitrag zum besseren Verständnis der interdependenten Sicherheitsarchitektur zwischen staatlicher und privater Ebene beitragen. Insbesondere die Betrachtung der Innenperspektive durch die ethnographische Untersuchung ließ Einblicke in die zusammentreffenden Systemrationalitäten und deren Aushandlung im Unternehmen zu.

Wie im zweiten Kapitel angeführt wurde, orientiert sich die ethnographische Untersuchung dieser Arbeit an Beispielen der teilnehmenden Beobachtung wie denen von Horacio Ortiz oder Douglas Holmes. In beiden Fällen zeigten die Autoren Erkenntnisse auf der Grundlage der eingebetteten Beobachtung in den jeweiligen Organisationen auf, die dazu beitrugen, die internen Praktiken und Rationalitäten nach außen verschlossener Gruppen beschreiben zu können. Die Anwendung von ethnographischen Methoden in dieser Arbeit erlaubte die Herausbildung von relevanten Schlussfolgerung über den internen Risikodiskurs, dessen Verschiebung über die Jahre und schließlich in der zentralen Erkenntnis über die angewendete Selbstbetrachtung von Unternehmen und Umsetzung in Form der Resilienz. Diese Erkenntnisse basierten auf der Perspektive und involvierten Beobachtung der Organisation von innen heraus und wäre von außen aufgrund des Anspruchs an Vertraulichkeit kaum möglich gewesen. So bietet sich die ethnographische Methode auch für andere Forschungsvorhaben an und kann, wie es beispielsweise im Fall der Pariser Schule vorgestellt wurde, auch in anderen Organisationen und Bereichen angewendet werden und ist aus Sicht der Ergebnisse dieser Arbeit auch anschlussfähig für weitere Forschung auf diesem Gebiet .

Mit Blick auf die Bedeutung der Digitalisierung ergeben sich ebenfalls spannende Folgefragen für weitere Forschungstätigkeit. Beispielsweise sollten die Implikationen der weiteren Anwendung von Technologie in der Sicherheitsforschung hinsichtlich der zentralen Stellung von Unternehmen als Betreiber und Eigentümer kritischer (IT-)Infrastruktur berücksichtigt werden. Dazu kann diese Arbeit einen Beitrag leisten, indem die Folgen der Digitalisierung auf den Umgang mit Unsicherheit in Unternehmen und den daraus abgeleiteten Herausforderungen für eine bestmögliche Steuerung von geschäftsgefährdenden Risiken beschrieben wurden und als Ausgangsbasis dienen können. Dieser Gedanke bedarf weiterer Konkretisierung in der Forschung, welche über die zuvor formulierte Unterabdeckung der Rolle von Unternehmen im Rahmen der kooperativen Sicherheitsproduktion von staatlicher und privater Ebene hinausgeht. Da die vorliegende Literatur im überwiegenden Umfang der traditionellen Aufteilung der Materie nach Fachfunktionen folgt, fehlt eine übergreifende Betrachtung von Risikokontrollen aller relevanten Bereiche. Die Analysen und Anleitungen für den Informationsschutz gliedern sich zum Beispiel nach IT und Nicht-IT Bereichen, differenzieren sich ferner nach den Zuständigkeitsbereichen der Konzernstrukturen, so etwa in die Felder IT-Sicherheit, Zugangskontrolle, Datenschutz oder Dokumentenverwaltung. Ebenso verhält es sich mit der Ausrichtung des BCM am Verfügbarkeitsanspruch von Ressourcen und Prozessen. Die Rolle der Information als zentrale Wertegröße des Cyberzeitalters findet ebenso wenig Beachtung in vielen Betrachtungen zu Wiederherstellungsplänen, wie die Reflektion der Vertraulichkeit und Integrität nur selten in einen sinnvollen Zusammenhang mit der Verfügbarkeitsabsicherung gesetzt wird.

Die Erarbeitung und Vertiefung einer resilienten Organisation erfordern wie wir in den vorausgehenden Kapiteln sehen konnten hingegen ein ganzheitliches Verständnis der methodischen Zusammenführung von Risikokontrollen aus allen funktionalen Bereichen. Dieses Zielbild sollte in der Literatur stärker herausgebildet werden und bietet eine Ausgangsgrundlage zur Zusammenführung der Konzepte zu einem stimmigen Schutzansatz, welcher je nach Branche und Kontextabhängigkeit Änderungen unterliegen wird. Ferner umfasst die Konkretisierung der Umsetzungsschritte für die unterschiedlichen Wertschöpfungsprozesse sowie ihrer Implikationen für Unternehmen selbst weiteren Bedarf an empirischen Studien zur Einführung von Resilienz. Dies betrifft insbesondere die mittel- und langfristigen Folgen technologischer Risiken und der Entwicklungen aus der Corona-Pandemie und Energiekrise, welche zum gegenwärtigen Zeitpunkt noch nicht abschließend zu beurteilen sind. Zuletzt bietet sich die Digitalisierung aufgrund ihrer weitreichenden Veränderungen in unterschiedlichsten Bereichen als Forschungsgegenstand an. Trotz zahlreicher Publikationen,

welche unter dem Titel der Digitalisierung erschienen sind, bleibt der Bedarf an weiteren Forschungsarbeiten groß, nicht zuletzt aufgrund der dynamischen Fortentwicklung des Themas. Denn so wie die Digitalisierung zu einem alltäglichen Bestandteil des Lebens und des Sprachgebrauchs im globalen Kontext geworden ist, sind die Risiken des technologischen Wandels ebenfalls in holistischen Kategorien zu betrachten.

Diese Erkenntnis ist der Ausgangspunkt für einen weitreichenden Anpassungsprozess von Unternehmen, deren Zukunft mittelfristig von der schnellen Adaption an die neuen technologischen Anforderungen abhängig sein wird. Langfristig jedoch wird der Fortbestand von einzelnen Unternehmen von der Fähigkeit abhängen, die Auswirkungen des Wandels auf die individuelle Risikoexposition reflektieren zu können und die geeigneten Maßnahmen einzuleiten, welche es Entscheidungsträgern erlauben wird, sich auch trotz der Bedingungen der Unsicherheit auf potentielle geschäftsgefährdende Risiken vorzubereiten. Diese Entwicklung weiter zu verfolgen und die empirische Forschung an der Schnittstelle von öffentlicher und privater Kooperation fortzusetzen, kann eine vielversprechende Ausgangsgrundlage für weitere Forschung und Analysen bilden. Denn Resilienz reflektiert nicht nur die Abwehrfähigkeit gegenüber potentiellen Schäden, sondern stellt als fortwährender Prozess der Anpassungsfähigkeit und Flexibilität im Umgang mit Risiken ein Beispiel nachhaltigen Handelns dar. Als solches kann die weitere Betrachtung von Resilienz in Unternehmen auch dazu beitragen die Grundversorgung von Gesellschaften als Teil eines langfristigen und widerstandsfähigen Modells zu schützen. Daher gilt es die kontinuierliche Bereitstellung von Waren und Gütern, insbesondere im Fall der kritischen Infrastruktur zu reflektieren und geeignete Maßnahmen als Teil der gesellschaftlichen Risikoabwägung, Sicherheitsdispositiven sowie der erforderlichen Sicherheitsproduktion in Unternehmen zu unterscheiden und weiter zu verfolgen.

9. Anhang

9.1. Abbildungsverzeichnis

Abb. 1.1. Differenzierung von Sicherheitsproduktion durch und in Unternehmen. Eigene Darstellung.

Abb. 3.1. Digitalisierung, Automatisierung und Robotisierung. Eigene Darstellung.

Abb. 3.2. Facetten der Digitalisierung und Einordnung der nachfolgenden Abschnitte. Eigene Darstellung, aufbauend auf dem Modell von Benjamin Bratton (Bratton 2015).

Abb. 3.3. Bezugsquellen von Informationen durch Big Data, welche über das heimische oder Gast-Wlan, Nachrichten, Social Media, Postings oder Einkäufe im Internet Daten sammelt. Eigene Darstellung.

Abb. 3.4. Elemente der Cloud. Eigene Darstellung nach Frank Doelitzscher et. al. (Doelitzscher et. al. 2011).

Abb. 3.5. Die Funktionsweise der Cloud. Eigene Darstellung basierend auf Heinrich et. al. (Heinrich et. al. 2016: 53).

Abb. 4.1. Prozessauslagerung und Verantwortung. Eigene Darstellung.

Abb. 4.2. Unterscheidung traditioneller und prozessorientierter Risikobegriff. Eigene Darstellung.

Abb. 4.3. Internes Kontrollsystem, bestehend aus drei Ebenen. Eigene Darstellung.

Abb. 4.4. Risikokategorien. Eigene Darstellung.

Abb. 4.5. Risikokategorien und Risikoszenarien zur Einordnung von Risiken im Unternehmenskontext. Eigene Darstellung.

Abb. 4.6. Kriterien der anlogen BCM-Risikobewertung. Eigene Darstellung.

Abb. 5.1. Schnittmenge von Resilienz und Risikomanagement begründen BCM als Disziplin der resilienten Risikomitigation. Eigene Darstellung.

Abb. 5.2. BCM Risikomatrix. Eigene Darstellung.

Abb. 5.3. Zusammenspiel zwischen Krisenmanagement und BCM Planung als Teil des ganzheitlichen Business Continuity Managements. Eigene Darstellung.

Abb. 5.4. Entwicklung des BCM aus dem ITDRM. Eigene Darstellung.

Abb. 5.5. Der detaillierte BCM Prozess, bestehend aus sechs Elementen. Eigene Darstellung.

Abb. 5.6. Aufbau einer umfassenden Abdeckung von BCM-Risikokontrollen von Zulieferer, Unternehmen und Kunden. Eigene Darstellung.

Abb. 5.7. Zeitlicher Verlauf der Risiko- und Krisenkommunikation. Eigene Darstellung.

Abb. 5.8. BCM im Vergleich zu Ereignissen und der Entwicklung von nationalen und internationalen Standards. Eigene Darstellung.

Abb. 6.1. Kernaufgaben von BCM und Informationsschutz im Vergleich. Eigene Darstellung.

Abb. 6.2. Der Resilienzbegriff als Schnittmenge zwischen Resilienz, Risikomanagement und Informationsschutz. Eigene Darstellung.

Abb. 6.3. Art und Ursachen des Datenverlusts. Eigene Darstellung.

Abb. 6.4. Idealtypische Schritte des Social Engineering. Eigene Darstellung.

Abb. 6.5. Verlauf eines Angriffs mit Ransomware. Eigene Darstellung.

Abb. 6.6. Maßnahmen zum proaktiven Schutz vor Ransomware-Angriffen. Eigene Darstellung.

Abb. 6.7. ITSCM Planungsschritte. Eigene Darstellung.

Abb. 7.1. Ziele und methodische Ausrichtung von BCM, KM und Informationsschutz. Eigene Darstellung.

Abb. 7.2. Risikokontrollsystem im Informationszeitalter. Eigene Darstellung.

Abb. 7.3. Risikobewertung der Ressourcen und Ermittlung der Mitigation. Eigene Darstellung.

Abb. 7.4. Virtuelles ITSCM Gedächtnis und Fachbereichs- bzw. IT-Sphäre. Eigene Darstellung..

Abb. 7.5. Spezifisches Strategierahmenwerk für Dienstleister. Eigene Darstellung.

Abb. 7.6 Erweiterte Schutzperspektive für Informationen und Strategieentwicklung. Eigene Darstellung.

Abb. 7.7 Unterscheidung der Plantypen. Eigene Darstellung.

Abb. 7.8 Kontrollrahmenwerk für das Zielbild einer resilienten Organisation. Eigene Darstellung.

Abb. 7.9. Integrativer Ansatz einer resilienten Organisation. Eigene Darstellung.

9.2. Verzeichnis der Hintergrundgespräche

Hintergrundgespräch am 16.06.2014. Thema: Investitionen und ökonomische Rationalität. Gespräch mit BCM Experten in Deutschland.

Workshop am 29.09.2015. Thema: Wiederherstellungspläne und Ressourcendefinition. Gespräch mit 9 BCM Experten aus verschiedenen Landesgesellschaften auf einer Konferenz in Europa.

Workshop am 10.11.2015. Thema: Angleichung von Ressourcendefinitionen in Landesgesellschaften. Gespräch mit 11 BCM Experten aus verschiedenen Landesgesellschaften auf einer Konferenz in Asien.

Hintergrundgespräch am 21.09.2016. Thema: Ransomware und Investitionen. Gespräch mit BCM Experten in Nordamerika.

Workshop am 02.03.2017. Thema: Einführung eines neuen Risikokontrollsystems. Gespräch mit globalem BCM Verantwortlichen in Deutschland.

Hintergrundgespräch am 10.03.2017. Thema: Einführung der DSGCO und Incident Management System. Gespräch mit einem Berater und einer globalen Incident Management Verantwortlichen in Deutschland

Hintergrundgespräch am 29.07.2017. Thema: Globale Lieferketten und Prozesskontinuität. Gespräch mit BCM Verantwortlichen eines anderen DAX-Unternehmens in Deutschland.

Hintergrundgespräch am 20.02.2018. Thema: Methodische Diskussion über die Kontrollen von ITSCM. Gespräch mit einem IT-Berater und einem globalem ITSCM Verantwortlichen in Deutschland.

Hintergrundgespräch am 08.05.2018. Thema: Definition von IT-Ökosystemen in einer Landesgesellschaft. Gespräch mit IT-Architekt einer Landesgesellschaft in Deutschland.

Workshop am 18.02.2019. Thema: Einführung einer Governance, Risk und Compliance (GRC) Software. Gespräch mit ITSCM-Expertin in Deutschland.

Workshop am 17.10.2019. Thema: Beispiel einer Business Impact Analysis mit Prozessverantwortlichen. Gespräch mit BCM-Verantwortlicher und zwei Prozessverantwortlichen aus einer Ländergesellschaft in Südeuropa.

Hintergrundgespräch am 11.05.2020:. Thema: Umsetzung von virtuellen Ausweicharbeitsplätzen während der ersten Phase der Corona-Pandemie. Gespräch mit Managerin einer Landesgesellschaft in Deutschland.

Hintergrundgespräch am 29.09.2020. Thema: Desaster Recovery Pläne für das Rechenzentrum. Gespräch mit IT-Infrastruktur Experte in Deutschland.

Workshops September bis Dezember 2020: Thema: Interviews und Workshops mit insgesamt 18 BCM und KM Experten zur Umsetzung der Corona-Pandemie bedingten Verlagerung ins Home Office. Gespräche mit 18 Experten aus verschiedenen Ländern in Europa, Nordamerika und Asien.

Hintergrundgespräch 26.11.2020. Thema: Krisenstabsarbeit unter den Bedingungen der Corona-Pandemie. Gespräch mit KM-Expertin in Deutschland.

Workshop am 19.01.2021. Thema: Ausweitung des Kritikalitätsmodells auf eine größere Anzahl an Prozessen m Unternehmen. Gespräch mit globalem BCM Verantwortlichen in Deutschland.

Hintergrundgespräch am 03.03.2021. Thema: Aufbrechen von Silos zwischen Fachfunktionen in einer Landesgesellschaft zur Umsetzung von Resilienz. Gespräch mit Managerin einer Landesgesellschaft in Deutschland.

Hintergrundgespräch am 08.06.2021. Thema: Etablierung einer ganzheitlichen Resilienz-Strategie für Betrieb und IT. Gespräch mit IT-Berater in Deutschland.

Hintergrundgespräch am 15.11.2021. Thema: Resilienz als systemsicherer Ansatz zur Risikokontrolle. Gespräch mit globalen BCM-Verantwortlichen in Deutschland.

Hintergrundgespräch am 13.12.2021. Thema: Auswirkungen von IT-Sicherheitslücken am Beispiel Log4j für Unternehmen und Konsequenzen für die Krisenkommunikation. Gespräch mit KM-Experte aus einer nordeuropäischen Landesgesellschaft.

Hintergrundgespräch am 27.06.2022. Thema: Verknüpfung von Kontrollen aus Betrieb und IT zur Sicherstellung eines resilienten Umgangs mit der Energiekrise. Gespräch mit einer Managerin aus einer Landesgesellschaft in Deutschland.

Hintergrundgespräch 28.07.2022. Thema: Umsetzung von Resilienz und Einrichtung einer informationsverarbeitenden Spezialfunktion im Unternehmen zur Analyse geschäftsgefährdender Risiken. Gespräch mit einer Managerin aus einer Landesgesellschaft in Deutschland.

Hintergrundgespräch am 27.10.2022. Thema: Planung und Problematik der Backup-Lösungen für die globalen Rechenzentren unter dem Eindruck der Energiekrise. Gespräch mit IT-Infrastruktur Experten in Deutschland.

Hintergrundgespräch am 23.11.2022: Thema: Sicherstellung der Datenverfügbarkeit hinsichtlich der Netzstabilität. Gespräch mit einem IT-Infrastruktur Experten in Deutschland.

Workshop am 02.12.2022. Thema: Einführung und Anpassungen der Risikokontrolle durch DORA. Workshop mit 8 Beratern aus der IT- und Operationsberatung in Deutschland.

9.3. Bibliografie

A-F

Abdul-Kader, Sameera und John Woods (2015): Survey on Chatbot Design Techniques in Speech Conversation Systems. In: (IJACSA) International Journal of Advanced Computer Science and Applications. Vol. 6, No. 7, 2015. S. 72-80.

Abraham, Sherly und Indushobha Chengalur-Smith (2010): An overview of social engineering malware: Trends, tactics, and implications. In: Technology in Society, August 2010. S. 183-196.

Acemoğlu, Daron und James A. Robinson (2015): Warum Nationen scheitern. Die Ursprünge von Macht, Wohlstand und Armut. Fischer, Frankfurt am Main.

Alazab, Mamoun, Robert Layton, Sitalakshmi Venkataraman und Paul Watters (2010): Malware detection based on structural and behavioural features of API calls. Conference paper International Cyber Resilience Conference, Perth 23. Aug. 2010.

Alcaraz, Cristina und Sherali Zeadally (2015): Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. In: International Journal of Critical Infrastructure Protection (IJCIP). Vol. 8, S. 5366 – 5400.

Alexander, Keith und Jamil Jaffer (2021): Covid-19 and the cyber challenge. In: Defense Review. Vol. 6. Nr. 2. S. 17 – 28.

Almedom, Astier M. (2011): Profiling Resilience: Capturing Complex Realities in One Word. In: The Fletcher Forum of World Affairs. Vol. 35, Nr. 1, 2011. S. 145 – 154.

Amoore, Louise und Volha Piotukh (2015): Life beyond big data: governing with little analytics. In: Economy and society, 44 (3). S. 341-366.

Amoore, Louise und Rita Raley (2016): Securing with algorithms: Knowledge, decision, sovereignty. In: Security dialogue, Vol. 48, 1. S. 3-10.

Amoore, Louise (2016) 'Cloud geographies: computing, data, sovereignty. Progress in human geography. Zuletzt aufgerufen am 17.02.2018 unter: http://dro.dur.ac.uk/19468/1/19468.pdf?DDD14+dgg4lp+d700tmt

Anant, Venky, Jeffrey Caso und Andreas Schwarz (2020): COVID-19 crisis shifts cybersecurity priorities and budgets. Zuletzt aufgerufen am 01.06.2022 unter: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets

Anthony, Thomas (2016): Human Factors in extremis The Rogue Pilot Phenomenon. In: Semi-annual publication on Air Accident Investigation from UAE General Civil Aviation Authority. Zuletzt aufgerufen am 19.04.2017 unter:: http://viterbi.usc.edu/aviation/assets/003/100246.pdf. S. 43 – 48.

Apt, Wenke und Steffen Wischmann (2016): Neue Gestaltungsmöglichkeiten für die Arbeitswelt. In: In: Volker Wittpahl (Hrsg.). Digitalisierung. Bildung.Technik. Innovation. Springer. Berlin, 2016. S. 109 – 117.

Aradau, Claudia und van Munster, Rens (2007). Governing terrorism through risk: Taking precautions, (un)knowing the future. European Journal of International Relations, 13(1), S. 89–115.

Aradau, Claudia, Luis Lobo-Guerrero und Rens Van Munster (2008): Security, Technologies of Risk, and the Political: Guest Editors' Introduction. In: Security Dialogue 2008 39: 147. S. 147-154.

Aradau, Claudia und Tobias Blanke (2017): Politics of prediction: security and the time/space of governmentality in the age of big data. In: European Journal Of Social Theory. Vol. 20, Nr. 3. S. 373-391.

Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica, und Matei Zaharia (2010): A View of Cloud Computing. In: Communications of the ACM, April 2010, Vol. 53,Nr. 4. S. 50 – 58.

Arnold, Daniel, Melanie Arntz, Terry Gregory, Susanne Steffes und Ulrich Zierahn (2016): Herausforderungen der Digitalisierung für die Zukunft der Arbeitswelt. In: ZEW policy brief, Nr. 8, 2016.

Asnar, Yudistira und Paolo Giorgini (2008): Analyzing Business Continuity through a Multi-layers Model. In: Dumas M., Reichert M. und Shan MC. (Hrsg.): Business Process Management. BPM 2008. Lecture Notes in Computer Science, Vol 5240. Springer, Berlin 2008.

Axworthy, Lloyd (2001): Human Security and Global Governance: Putting People First. In: Global Governance 7 (2001). S. 19-23.

Babic, Milan, Jan Fichtner und Eelke Heemsker (2017): States versus Corporations: Rethinking the Power of Business in International Politics. In: The International Spectator. Nr. 52, Vol. 4. S. 20-43.

Baecker, Dirk (1991): Womit handlen Banken? Eine Untersuchung zur Risikoverarbeitung in der Wirtschaft. Suhrkamp Verlag, Frankfurt am Main, 2. Auflage, 2008.

Baele, Stephane und Diana Jalea (2022): Twenty-five Years of Securitization Theory: A Corpus-based Review. In: Political Studies Review. Jan. 2022. S. 1–14.

Bahlia, Bouchaib und Suzanne Rivard (2003): The Information Technology Outsourcing Risk: A Transaction Cost and Agency Theory-Based Perspective. In: Journal of Information Technology. September 2003. S. 211 – 221.

Bahlia, Bouchaib und Suzanne Rivard (2005): Validating measures of information technology outsourcing risk factors. In: Omega, Vol. 33, Nr. 2. S.175 - 187.

Bamert, Tobias, Christian Decker, Lennart Elsen, Roger Wattenhofer und Samuel Welten (2013): Have a Snack, Pay with Bitcoins. In: 13-th IEEE International Conference on Peer-to-Peer Computing. 2013. Aufgerufen online zuletzt am 27.06.2017 unter: https://www.researchgate.net/profile/Christian_Decker5/publication/261467797_Have_a_snack_pay_with_Bitcoins/links/5578293208aeacff200191f1.pdf.

Bardt, Hubertus, Michael Grömling, Edgar Schmitz (2022): Russlands Krieg in der Ukraine belastet deutsche Unternehmen. In: IW Kurzbericht. Institut der deutschen Wirtschaft (IW). Nr. 19.

Beck, Ulrich (1991) (Hrsg): Politik in der Risikogesellschaft. Essays und Analysen. Frankfurt am Main, 1991.

Beck, Ulrich (2002): The Terrorist Threat. World Risk Society Revisited. In: Theory Culture Society 2002; 19; 39. S. 39-55.

Beck, Ulrich (2006): Living in the world risk Society. In: Economy and Society Volume 35 Number 3 August 2006: 329- 345.

Beck, Roman, Jörg Caumanns, Jürgen Großmann, Ulrich Meissen, Jochen Schiller, Sönke Schulz, Jens Tiemann, Jakob Tischer, Armin Wolf, Markus Wollina (2014): IT und Internet als kritische Infrastruktur. Vernetzte Sicherheit zum Schutz kritischer Infrastrukturen. Lorenz-von-Stein-Institut für Verwaltungswissenschaften. Kiel.

Best, Jacqueline (2010): The Limits of Financial Risk Management: Or What we Didn't Learn from the Asian Crisis. In: New Political Economy. 15:1, 29-49.

Behnezhad, Ali, Brian Connett und Manjula Nair (2013): The Evolution of Supply Chain Risk Management. In: Journal of Supply Chain and Operations Management, Vol. 11, Nr. 1, Feb. 2013. S. 77 – 89.

Bellmann, Lutz, Pauline Bourgeon, Christina Gathmann, Christian Kagerl, David Marguerit, Ludivine Martin, Laura Pohlan und Duncan Rot (2021): Digitalisierungsschub in Firmen während der Corona-Pandemie. In: Wirtschaftsdienst 2021. Vol. 101, Nr. 9. S. 713-718.

Bernard, Julie und Mark Nicholson (2020): Reshaping the cybersecurity landscape. How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions. Zuletzt aufgerufen am 25.06.2022 unter: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

Bhardwaj, Akashdeep , Vinay Avasthi**1**, Hanumat Sastry and G. V. B. Subrahmanyam (2016): Ransomware Digital Extortion: A Rising New Age Threat. In: Indian Journal of Science and Technology, Vol 9(14), S. 1-5.

Bennett Moses, Lyria und Janet Chan (2016): Algorithmic prediction in policing: assumptions, evaluation, and accountability, Policing and Society. S. 1-17.

Bigo, Didier (2000): When two become one. Internal and external securitisations in Europe. In: Morten Kelstrup und Michael Williams (Hrsg.): International Relations Theory and the Politics of European Integration. Power, Security and Community. Routledge, London. S. 171-204.

Bigo, Didier und Emma McCluskey (2018): What Is a PARIS Approach to (In)securitization? Political Anthropological Research for International Sociology. In: Alexandra Gheciu und William Wohlforth (Hrsg.): The Oxford Handbook of International Security. Oxford University Press, 2018. S. 116-130.

Bitaab, Marzieh, Haehyun Cho, Adam Oest, Penghui Zhang, Zhibo Sun, Rana Pourmohamad, Doowon Kim, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupe und Gail-Joon Ahn (2021): Scam Pandemic: How Attackers Exploit Public Fear through Phishing. Zuletzt aufgerufen am 14.05.2021 online unter: https://arxiv.org/pdf/2103.12843v1.pdf

Blum, Sabine, Martin Endreß, Stefan Kaufmann und Benjamin Rampp (2016): Soziologische Perspektiven. In: Rüdiger Wink (Hrsg.): Multidisziplinäre Perspektiven der Resilienzforschung. Springer, Wiesbaden 2016. S. 151-178.

Boas, Taylor und Thad Dunning (2000): Classic Questions, New Context: Development in an Era of Bits and Bytes. In: Studies in Comparative International Development, Summer 2005, Vol. 40, Nr. 2. S. 3-8.

Bock, Andreas (2017): Islamistischer Terrorismus: Die konstruierte Bedrohung. In: Zeitschrift für Außen- und Sicherheitspolitik. Vol. 10, S. 245–265.

Böhmer, Wolfgang, Christoph Brandt und Jan Friso Groote (2009): Evaluation of a business continuity plan using process algebra and modal logic. In: Computer Science Reports. Vol. 912.

Boland, Brodie, Aaron De Smet, Rob Palter und Aditya Sanghvi (2020): Reimagining the office and work life after COVID-19. Zuletzt aufgerufen online am 24.02.2021 unter: https://www.health-revolution.org/uploads/1/0/6/7/106777763/reimagining-the-office-and-work-life-after-covid-19-final__1_.pdf

Bomsel, Olivier und Gilles Le Blanc (2004): Digitalisation, innovation, and industrial organisation: the pivotal case of the auto industry. In: International Journal of Electronic Business, Vol. 2, Nr. 2, 2004. S. 193 – 204.

Bonafede, Concetto, Paola Cerchiello und Paolo Giudici (2007): Statistical models for business continuity Management. In: Journal of Operational Risk, Vol. 2, Nr.4 2007. S. 79 – 96.

Bonner, Lance (2012): Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches. In: , 40 Washington University Journal of Law & Policy. Vol 40, 2012. S. 257 – 277.

Borges, Georg, Jörg Schwenk, Carl-Friedrich Stuckenberg und Christoph Wegener (2011): Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte. Springer-Verlag Berlin Heidelberg 2011.

Bornholdt und K. Sneppen (2014): Do Bitcoins make the world go round? On the dynamics of competing crypto-currencies. Zuletzt aufgerufen online am 27.06.2017 unter: https://arxiv.org/pdf/1403.6378.pdf

Boscarino, Joseph A., Richard E. Adams, Charles R. Figley, Sandro Galea und Edna B. Foa (2006): Fear of Terrorism and Preparedness in New York City 2 Years After the Attacks: Implications for Disaster Planning and Research. In: Public Health Manag Pract. 2006 ; 12(6): S. 505–513.

Boutellier, Roman, Eric Montagne, Berthold Barodte und Michael Hausding (2007): Hightech Projekte und deren Risiken. Abhängigkeiten von technischen und Geschäftsrisiken im Projektmanagement. In: Zeitschrift für Risk, Fraud und Compliance. Vol. 3. S. 131-135.

Bradbury, Judith (1989): The Policy Implications of Differing Concepts of Risk. In: Science, Technology & Human Values. Vol. 14 No. 4, Autumn 1989. S. 380 – 399.

Braes, Bruce und David Brooks (2010): Organisational Resilience: A Propositional Study to Understand and Identify the Essential Concepts. Confernce Paper, 3rd Australian Security and Intelligence Conference, Perth 30. Nov. 2010.

Bram, Jason, James Orr, and Carol Rapaport (2002): Measuring the Effects of the September 11 Attack on New York City. In: Economic Policy Review, Nov. 2002. S. 5 – 20.

Brand, Murray, Craig Valli und Andrew Woodward (2011): A Threat to Cyber Resilience: A Malware Rebirthing Botnet. Conference paper International Cyber Resilience Conference, Perth 1.–2. Aug. 2011.

Brandt, Christoph, Frank Hermann und Jan Friso Groote (2011): Generation and Evaluation of Business Continuity Processes using Algebraic Graph Transformation and the mCRL2 Process Algebra. In: Journal of Research and Practice in Information Technology, Vol. 43, No. 1, February 2011.

Bratton, Benjamin H. (2015): The Stack. On Software and Sovereignty. MIT Press.

Braubach, Angela (2011): Vulnerabilität der Kritischen Infrastruktur Wasserversorgung gegenüber Naturkatastrophen. Auswirkungen des Augusthochwassers 2002 auf die Wasserversorgung und das Infektionsgeschehen der Bevölkerung in Sachsen und Sachsen-Anhalt. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Bonn.

Browning, Christopher und Matt McDonald (2011): The future of critical security studies: Ethics and the politics of security. In: European Journal of International Relations. Nr. 19, Vol. 2. S. 235 –255.

Brunsdon, Dave und Erica Dalziell (2005): Making Organisations Resilient: Understanding the Reality of the Challenge. Resilient Infrastructure Conference. Rotorua, 8. August 2005. S. 27 - 34.

Bryce, Cormac, Patrick Ring , Simon Ashby und Jamie Wardman (2020): Resilience in the face of uncertainty: early lessons from the COVID-19 pandemic. In: Journal of Risk Research, Vol. 23 Nr. 7-8. S. 880-887.

Brzoska Michael, Götz Neuneck und Jürgen Scheffran (2021): Corona-Pandemie: Implikationen für die Sicherheitspolitik. In: Policy Brief. Corona-Pandemie: Implikationen für die Sicherheitspolitik. Vol. 2. S. 1-8.

Buchholz, Birgit und Leo Wangler (2016): Digitalisierung und neue Geschäftsmodelle. In: Volker Wittpahl (Hrsg.). Digitalisierung. Bildung.Technik. Innovation. Springer. Berlin, 2016. S. 177 – 183.

Buhr, Daniel (2015): Industrie 4.0. Neue Aufgaben für die Innovationspolitik. Friedrich-Ebert-Stiftung, Bonn. 2015.

Bund, Jakob und Ann-Sophie Leonard (2020): Informationskrieg: Impfstoffe. Zuletzt aufgerufen am 06.03.2020 unter: https://doi.org/10.3929/ethz-b-000432770.

Burstedde, Alexander, Susanne Seyda, Lydia Malin, Paula Risius, Anika Jansen, Regina Flake und Dirk Werner (2020): ‚Versorgungsrelevante' Berufe in der Corona-Krise. Fachkräftesituation und Fachkräftepotenziale in kritischen Infrastrukturen. Institut der deutschen Wirtschaft. Köln.

Busse, Matthias und Carsten Hefeker (2005): Political Risk, Institutions and Foreign Direct Investment. In: European Journal of Political Economy. Vol. 23, Nr.2. S. 397-415.

Buzan, Barry, Ole Waever und Jaap de Wilde (1998): Security. A new framework for analysis. Lynne Rienner Publishers, Boulder. 1998.

Carvalho e Silva, Hedwio, Rita de Cassia Cordeiro de Castro, Marcos Jose Negreiros Gomes, und Anilton Salles Garcia (2012): Well-Founded IT Architecture Ontology: An Approach from a Service Continuity Perspective. In: R. Benlamri (Hrsg.): NDT 2012, Part II, CCIS 294. S. 136–150.

Carr, Madeline (2016): Public Private Partnerships in National Cyber-security Strategies, International Affairs. Nr. 92, Vol. 1. S. 43–62.

Castells, Manuel (2010): The Rise of the Network Society. Blackwell Publishing, 2. Ausgabe.

Cavelty, Myriam Dunn und Manuel Suter (2009): Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. In: International Journal of Critical Infrastructure Protection (2009). S. 1-9.

Cavelty, Myriam Dunn (2013): From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. In: International Studies Review (2013) Vol. 15, S. 105 – 122.

Caves, Richard (2000): The Multinational Enterprise as an Economic Organization. In: Jeffry Frieden und David Lake (Hrsg.): International Political Economy. Perspectives On Global Power and Wealth. Routledge, London. S. 145-155.

Cerullo, Virginia und Michael J. Cerullo (2004): Business Continuity Planning: A comprehensive approach. In: ISM Journal. Vol. 2 2004. S. 70 – 78.

Chamorel, Patrick (2019): Macron Versus the Yellow Vests. In: Journal of Democracy. Vol. 30, Nr. 4. S. 48-62.

Chandler, David (2014): Beyond neoliberalism: Resilience, the new art of governing complexity. In: David Chandler (Hrsg.): Resilience. International Policies, Practices and Discourses. Vol. 1, Nr. 2. S. 47-63.

Chigada, Joel und Rujeko Madzinga (2021): Cyberattacks and threats during COVID-19: A systematic literature review. In: South African Journal of Information Management, Nr. 23. S. 1-11.

Christensen, Kristoffer und Karen Petersen (2017): Public-private Partnerships on Cyber Security: A Practice of Loyalty. In: International Affairs, Nr. 93 Vol. 6. S. 1435–1452.

Chongvilaivan, Aekapol (2012): Thailand's 2011 flooding: Its impact on direct exports and global supply chains. In: ARTNeT Working Paper Series, No. 113. S. 1-35.

Choo, Kim-Kwang Raymond, Russell G Smith and Rob McCusker (2007): The future of technology-enabled crime in Australia. In: Trends & issues in crime and criminal justice series: No 341 2007 Canberra. S. 1-6.

Choras, Michal, Rafal Kozik, Maria Pilar Torres Bruna, Artsiom Yautsiukhin, Andrew Churchill, Iwona Maciejewska, Irene Eguinoa und Adel Jomni (2015): Comprehensive Approach to Increase Cyber Security and Resilience, 10. International Conference on Availability, Reliability and Security (ARES), 2015. S. 686 - 692.

Chou, Te-Chun (2013): Security threats on cloud computing vulnerabilities. In: International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3. S. 79 – 88.

Church, Richard, Maria P. Scaparra und Richard Middleton (2004): Identifying Critical Infrastructure: The Median and Covering Facility Interdiction Problems. In: Annals of the Association of American Geographers, 94(3), 2004, S. 491 – 502.

Church, Richard und M. Paola Scaparra (2007): Analysis of Facility Systems' Reliability when Subject To Attack or a Natural Disaster. In: Alan T. Murray und Tony H. Grubesic (Hrsg.): Critical Infrastructure. Reliability and Vulnerability. Springer, Berlin 2007. S. 221 – 242.

Ciuk, Sylwia, Juliette Koning und Monika Kostera (2018): Organizational Ethnographies. In: Catherine Cassell, Ann Cunliffe und Gina Grandy (Hrsg.): The Sage Handbook of Qualitative Business and Management Research Methods. SAGE Publications Ltd, 2018. S. 270-185.

Clapton, William (2009): Risk and hierarchy in international society. In: Global Change, Peace & Security, Vol. 21, 1. S. 19-35.

Clapton, William (2011): Risk in International Relations. In: International Relations 2011, 25 (3). S. 280-295.

Connor, Steven (2004): Topologies: Michel Serres and the Shapes of Thought. In: Anglistik, 15 (2004): S. 105-117.

Conway, Paul (2010): Preservation in the Age of Google: Digitization, Digital Preservation, and Dilemmas. In: Library Quarterly, vol. 80, no. 1, pp. 61-79.

Cook, David M. (2010): Mitigating Cyber-Threats Through Public-Private Partnerships: Low Cost Governance with High-Impact Returns. Conference paper International Cyber Resilience Conference, Perth 23. Aug. 2010. S. 22 – 30.

Cortis, Dominic, Jeremy Debattista, Johann Debono und Mark Farrell (2019): InsurTech. In: Theo Lynn, John G. Mooney, Pierangelo Rosati und Mark Cummins (Hrsg.): Disrupting Finance FinTech and Strategy in the 21st Century- Palgrave, Dublin. S. 73-84.

Cutler, Claire, Virginia Haufler und Tony Porter (1999): Private Authority and International Affairs. State University of New York Press, Albany.

Daase, Christopher und Oliver Kessler (2007): Knowns and Unknowns in the `War on Terror': Uncertainty and the Political Construction of Danger. In: Security Dialogue Vol. 38, Nr. 4. S. 411-434.

Davidshofer, Stephan, Julien Jeandesboz und Francesco Ragazzi (2016): Technology and security practices: Situating the technological imperative. In: International Political Sociology, Tranversal Lines in International Relations. Routledge, London. S. 205-227.

Delios, Andrews und Witold Henisz (2003): Research notes and commentaries. Political hazards, experience, and sequential entry strategies: the international expansion of Japanese firms.1980–1998. Strategic Management, 24. S.1153-1164.

Demary, Vera (2022): Wie der russische Cyberkrieg deutsche Unternehmen bedroht. In: IW-Kurzbericht 2022, Nr. 15. S. 1-3.

Deppermann, Arnulf (2000): Ethnographische Gesprächsanalyse: Zu Nutzen und Notwendigkeit von Ethnographie für die Konversationsanalyse. In: Gesprächsforschung - Online-Zeitschrift zur verbalen Interaktion. Nr. 1. S. 96-124.

Dierkes, Stefan, Elmar Gerum, Murat Ayaz und Nils Stieglitz (2005): Strategische Kontrolle als Element des Risikomanagements. In: IT-Security 2005. S. 38-51.

Dochow, Carsten (2022): Cybersicherheitsrecht im Gesundheitswesen. In: Medizinrecht (2022). Nr. 40. S. 100–110.

Doelitzscher, Frank, Anthony Sulistio, Christoph Reich, Hendrik Kuijs und David Wolf (2011): Private cloud for collaboration and e-Learning services: from IaaS to SaaSIn: Computing (2011) 91, S. 23–42.

Dolan, Catherine, Christina Garsten und Dinah Rajak (2011): Ethnographies of corporate ethicizing. In: Focaal—Journal of Global and Historical Anthropology. Vol. 60. S. 3–8.

Douglas, Mary (1992): Risk and Blame: Essays in Cultural Theory. Routledge, London.

Dreißigacker, Arne, Bennet von Skarczinski und Gina Rosa Wollinger (2020): Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. In: Christian Grafl, Monika Stempkowski, Katharina Beclin und Isabel Haider (Hrsg.): Sag, wie hast du's mit der Kriminologie? Die Kriminologie im Gespräch mit ihren Nachbardisziplinen. Forum Verlag Godesberg, Mönchengladbach. S. 933-952.

Dreyfus, Pablo (1999): When All the Evils Come Together. Cocaine, Corruption, and Shining Path in Peru's Upper Huallaga Valley, 1980 to 1995. In: Journal of Contemporary Criminal Justice, Vol. 15 No. 4, November 1999 370-396.

Dullien, Sebastian; Alexander Herzog-Stein, Peter Hohlfeld, Sven Schreiber und Silke Tober (2020): Schneller Ausstieg oder bedachte Lockerung? Zur Zukunft von Kontaktbeschränkungen in der Covid-19-Krise. In: IMK Policy Brief., Nr. 88.

Dwertmann, Anne und Markus Schürholz (2016): Digitalisierung in der Gesundheit. In: Volker Wittpahl (Hrsg.). Digitalisierung. Bildung.Technik. Innovation. Springer. Berlin, 2016. S. 165 - 172.

Eckert, Claudia (2008): IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg Verlag, München, 5. Auflage.

Eckert, Claudia (2014): IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg Verlag, München, 9. Auflage.

Eden, Lorraine (1991): Bringing the Firm Back In: Multinationals in International Political Economy. In: Millennium - Journal of International Studies, Nr. 20. S. 197-224.

Eichhorst, Werner, Holger Hinte, Ulf Rinne und Verena Tobsch (2016): Digitalisierung und Arbeitsmarkt: Aktuelle Entwicklungen und sozialpolitische Herausforderungen. In: IZA Standpunkte Nr. 85, Juli 2016.

Elbe, Stefan (2005): HIV/AIDS: The International Security Dimensions. In: Elke Krahmann (Hrsg.): New Threats and New Actors in International Security. New York 2005. S. 111-130.

Elliott, Dominic, Steve Letza, Martina McGuinness und Clive Smallman (2000): Governance, Control and Operational Risk: The Turnbull Effect. In: Risk Management, Vol. 2, No. 3. S. 47-59.

Engels, Barbara (2020): Corona: Stresstest für die Digitalisierung in Deutschland. In: IW-Kurzbericht, Nr. 23. Institut der deutschen Wirtschaft (IW), Köln.

Erdogmus, Nesli und Sébastien Marcel (2014): Spoofing attacks to 2D face recognition systems with 3D masks. In: IEEE Transactions on Information Forensics and Security. Vol. 9, Nr. 7. S. 1084-1097.

Eriksson, Johan und Giampiero Giacomello (2006): The Information Revolution, Security, and International Relations: (IR)relevant Theory. In: International Political Science Review. Vol. 27, Nr. 3. S. 221–244.

Ernest, M. und J. M. Nisavic (2007): Adding value to the IT organization with the Component Business Model. In: IBM Systems Journal. Vol 46, Nr. 3, 2007. S. 387 – 403.

Erskine, Toni und Madeline Carr (2016): Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace In: Anna-Maria Osula und Henry Rõigas (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications, Tallinn 2016. S. 87-109.

Ewald, Francois (1991): Die Versicherungs-Gesellschaft. In: Beck, Ulrich (1991) (Hrsg): Politik in der Risikogesellschaft. Essays und Analysen. Frankfurt am Main, 1991. S. 288-302.

Faulkner, Phil, Alberto Feduzi, Charles McCann Jr. und Jochen Runde (2021): F. H. Knight's Risk, Uncertainty, and Profit and J. M. Keynes' Treatise on Probability after 100 years. In: Cambridge Journal of Economics, Vol. 45, Nr. 5. S. 857–882.

Fekete, Alexander, Christiane Grinda und Celia Norf (2016): Resilienz in der Risiko- und Katastrophenforschung: Perspektiven für disziplinübergreifende Arbeitsfelder. In: Rüdiger

Wink (Hrsg.): Multidisziplinäre Perspektiven der Resilienzforschung. Springer, Wiesbaden 2016. S. 215-232.

Felt, Adrienne Porter, Matthew Finifter, Erika Chin, David Wagner. (2011): A Survey of Mobile Malware in the Wild. ACM Workshop on Security and Privacy in Mobile Devices (SPSM), ACM, 17, October, 2011. S. 1-12.

Ferguson, Neil, Derek Cummings, Christophe Fraser, James Cajka, Philip Cooley und Donald Burke (2006): Strategies for mitigating an influenza pandemic. In: Nature 422, S. 448-452.

Fieldhouse, David (2000): A New Imperial System"? The Role of the Multinational Corporations Reconsidered. In: Jeffry Frieden und David Lake (Hrsg.): International Political Economy. Perspectives On Global Power and Wealth. Routledge, London. S. 167-179.

Fineberg, Harvey (2014): Pandemic Preparedness and Response - Lessons from the H1N1 Influenza of 2009. In: The New England Journal of Medicine. 370 (14). S. 1335 – 1342.

Finlay, Brett, Raymond See und Robert Brunham (2004): Rapid response research to emerging infectious diseases: lessons from SARS. In: Nature Reviews Microbiology, Vol. 2. Nr. 7. S. 602-607.

Fischer, Wolfgang (2007): Analyse und Simulation strategischer Angriffe auf die kritische Infrastruktur Internet. Schriften des Forschungszentrums Jülich Reihe Informationstechnik / Information Technology, Vol. 14. Jülich 2007.

Fisher, John (2013): Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach. In: William & Mary Business Law Review. Vol. 4, Nr. 1. S. 215-239.

Flynn, Stephen E. (2008): America the Resilient. Defying Terrorism and Mitigating Natural Disasters. In: Foreign Affairs. Vol. 87, Nr. 2. Mar. /Apr. 2008. S. 2 – 8.

Flüter-Hoffmann, Christiane, Andrea Hammermann und Oliver Stettes (2018): Individuelle und organisationale Resilienz: Theoretische Konzeption und empirische Analyse auf Basis eines kombinierten Beschäftigten-Betriebsdatensatzes, IW-Analysen, Nr. 127. Institut der deutschen Wirtschaft (IW). Köln.

Foucault, Michel (2005): Analytik der Macht. Suhrkamp, Frankfurt am Main 2005. 7. Auflage.

Foucault, Michel (2006): Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I. In: Michel Senellart (Hrsg.): Vorlesungen am Collège de France 1977-1978. Frankfurt am Main 2006.

Foss, Nicolai (2020): The Impact of the Covid-19 Pandemic on Firms' Organizational Designs. In: Journal of Management Studies. 2020 Oct. Zuletzt online aufgerufen am 28.02.2021 unter: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7675467/

Frewer, Lynn (2004): The public and effective risk communication. In: Toxicology Letters 149. S. 391–397.

Fries, Jan Ludwig, Niklas Garnadt, Jens Herold, Florian Kirsch, Franziska Lembcke, Pia Molitor, Lukas Nöh, Malte Preuß, Wolf Reuter, Felix Rutkowski, Milena Schwarz, Sebastian Weiske und Mustafa Yeter (2020): Nachfrage- und angebotsseitige Einschränkungen der wirtschaftlichen Aktivität in Deutschland infolge der Corona-Pandemie. Arbeitspapier, Nr. 02/2020, Sachverständigenrat zur Begutachtung der Gesamtwirtschaftlichen Entwicklung, Wiesbaden

G-M

Gaycken, Sandro und Michael Karger (2011): Entnetzung statt Vernetzung. Paradigmenwechsel bei der IT-Sicherheit. In: Multimedia und Recht 23 (1) /2011 S. 3-8.

Geiges, Lars (2018): Wie die AfD im Kontext der „Flüchtlingskrise" mobilisierte. Eine empirisch-qualitative Untersuchung der „Herbstoffensive 2015". In: Z Politikwissenchaft. Vol. 28. S.: 49–69.

Genz, Carolin und Aylin Tschoepe (2021): Ethnographie als Methodologie. In: Anna Heinrich**,** Séverine Marguin, Angela Million und Jög Stollmann (Hrsg.): Handbuch qualitative und visuelle Methoden der Raumforschung. Bielefeld, Transcript Verlag, 2021. S. 225-236.

Gereffi, Gary, Pavida Pananond und Torben Pedersen (2022): Resilience Decoded: The Role of Firms, Global Value Chains, and the State in COVID-19 Medical Supplies. In: California Management Review. Vol. 64, Nr. 2. S. 46-70.

Gerrard, Simon und Judith Petts (1998): Isolation or Integration? The Relationship Between Risk Assessment and Risk Management. In: University of Illinois Law Review, 1996, 1, 163. 1998. S. 1-19.

Gewald, Heiko und Jens Dibbern (2007): Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. In: Information & Management. Mai 2009. S. 249-257.

Ghanchi Ali (2020): Adaptation of the National Plan for the Prevention and Fight Against Pandemic Influenza to the 2020 COVID-19 Epidemic in France. Zuletzt am 24.06.2021 online aufgerufen unter: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/52E7FE3C85DEC1C5CB097CF3297D2E3D/S1935789320000828a.pdf/adaptation_of_the_national_plan_for_the_prevention_and_fight_against_pandemic_influenza_to_the_2020_covid19_epidemic_in_france.pdf

Ghodeswar, Bhimrao und Janardan Vaidyanathan (2008): Business process outsourcing: an approach to gain access to world-class capabilities. In: Business Process Management Journal. February 2008. S. 23-38.

Gigerenzer, Gerd, Kirsten Schlegel-Matthies und Gert G. Wagner (2016): Digitale Welt und Gesundheit. eHealth und mHealth – Chancen und Risiken der Digitalisierung im Gesundheitsbereich. SVRV, Berlin. 2016.

Goh, Mark, Joseph Lim und Fanwen Meng (2007): Production, Manufacturing and Logistics. A stochastic model for risk management in global supply chain networks. In: European Journal of Operational Research. 2007 Nr. 182. S. 164–173.

Goldstein, Daniel (2010): Toward a Critical Anthropology of Security. In: Current Anthropology. Vol. 51, Nr. 4. S. 487-517.

Goldstone, Jack, Robert Bates, David Epstein, Ted Robert Gurr, Michael Lustik, Monty Marshall George, Jay Ulfelder und Mark Woodward (2010): A Global Model for Forecasting Political Instability. In: *American Journal of Political Science*, Vol. 54, No. 1. S. 190–208.

Gomez, Miguel und Christophe Whyte (2021): Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threat. In: International Studies Quarterly. Vol. 65, Nr. 4. S. 1-29.

Grant, Vaughan (2018): Critical Infrastructure Public-Private Partnerships: When is the Responsibility for Leadership Exchanged? In: Security Challenges, Vol. 14, Nr. 1 (2018). S. 40-52.

Greitzer, Frank (2014): Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In: 2014 IEEE Security and Privacy Workshops. S. 236 – 250.

Grossman, Gene und Elhanan Helpman (2005): Outsourcing in a Global Economy. In: Rev Econ Studies 72 (1) Jan. S. 135–159.

Günther, Lars, Georg Ruhrmann und Jutta Milde (2011): Pandemie: Wahrnehmung der gesundheitlichen Risiken durch die Bevölkerung und Konsequenzen für die Risiko- und Krisenkommunikation. Forschungsforum Öffentliche Sicherheit Schriftenreihe Sicherheit Nr. 7, Juni 2011, FU Berlin.

Graz, Jean-Christophe, Oliver Kessler und Rahel Kunz (2020): International Political Economy (IPE) meets International Political Sociology (IPS). In: International Relations. Vol. 33, Nr. 4. S. 586–619.

Hanson, Rebecca (2018): Ethnographies of Security: Pushing Security Studies Beyond the Bounds of International Relations. In: Qualitative Sociology, Vol. 41. S. 135–144.

Hammermann, Andrea und Hans-Peter Klös (2016): Digitalisierung und Arbeitsmarkt. Stellungnahme für die Enquetekommission „Zukunft von Handwerk und Mittelstand in NRW“ des Landtages NRW. IdW, Köln, 2016.

Hanft, Anke, Wolfgang Müskens und Petra Muckel (2004): Zertifizierung und Nachweis von IT-Kompetenzen. QUEM, Berlin 2004.

Hart, Keith und Horacio Ortiz (2014): The Anthropology of Money and Finance: Between Ethnography and World History. In: Annual Review of Anthropology. Vol. 43. S. 465-482.

Hashim, Ahmed, Lucie Jean-Gilles, Michala Hegermann-Lindencrone, Ian Shaw, Caroline Brown und Jonathan Nguyen-Van-Tam (2012): Did pandemic preparedness aid the response to pandemic (H1N1) 2009? A qualitative analysis in seven countries within the WHO European Region. In: Journal of Infection and Public Health. Vol. 5. S. 286-296.

Haucap, Justus, Ferdinand Pavel, Rafael Aigner, Michael Arnold, Moritz Hottenrott und Christiane Kehder (2015) : Chancen der Digitalisierung auf Märkten für urbane Mobilität: Das Beispiel Uber, DICE Ordnungspolitische Perspektiven, No. 73. S. 1 – 45.

Haucap, Justus (2020): Plattformökonomie: neue Wettbewerbsregeln – Renaissance der Missbrauchsaufsicht. In: Wirtschaftsdienst 2020. Vol. 100. S. 20-29.

Heineman, Ben und Fritz Heimann (2006): The Long War Against Corruption. In: Foreign Affairs. Vol. 85, Nr. 3. S. 75-86.

Heinrich, Anett, Heiko Kempa, Jochen Kerbusch und Eike-Christian Spitzner (2016): Datenökonomie und digitale Effizienz – Die Reduktion und Abstraktion von Daten in der vernetzten Welt. In: Volker Wittpahl (Hrsg.): Digitalisierung. Bildung.Technik. Innovation. Springer. Berlin, 2016. S. 51 – 59.

Hejase, Hussin, Hasan Fayyad-Kazan, Ale Hejase und Imad Moukadem (2021): Cyber Security amid COVID-19. In: Computer and Information Science. Vol. 14, Nr.. 2; S. 10-25.

Henisz, Witold und Bennet Zelner (2003): The strategic organization of political risks and opportunities. In: Strategic Organization, Vol 1(4). S. 451–460.

Hernes, Tor und Tore Bakken (2003): Implications of Self-Reference: Niklas Luhmann's Autopoiesis and Organization Theory. In: Organization Studies. Vol. 24, Nr. 9. S. 1511–1535.

Hessel, Stefan und Andreas Rebman (2021): Gesetzliche Verpflichtungen zur IT-Sicherheit für Unternehmen in Deutschland. In: Jusletter IT. Mai 2021. S. 263-270.

Hettich, Erwin, Markus Schimmer und Günter Müller-Stewens (2015): Die Wiedergeburt der Diversifikation. In: Harvard Business Manager. Jan. 2015. S. 55 – 61.

Hill, Jennifer, Randolph Ford und Ingrid Farreras (2015): Real conversations with artificial intelligence: A comparison between human–human online conversations and human–chatbot conversations. In: Computers in Human Behavior, 49 (2015). S. 245–250.

Hindmarsh, Richard (2013): Nuclear Disaster at Fukushima Daiichi. Introducing the Terrain. In: Richard Hindmarsh (Hrsg.): Nuclear Disaster at Fukushima Daiichi: Social, Political and Environmental Issues. Routledge, 2013. S. 1 -21.

Hitzler, Ronald (2000): Die Erkundung des Feldes und die Deutung der Daten. Annäherungen an die (lebensweltliche) Ethnographie. In: Werner Lindner (Hrsg.): Ethnographische Methoden in der Jugendarbeit. VS Verlag für Sozialwissenschaften, Wiesbaden. S. 17-31.

Hitzler, Ronald und Miriam Gothe (2015): Methodologisch-methodische Aspekte ethnographischer Forschungsprojekte. In: Ronald Hitzler und Miriam Gothe (Hrsg.): Ethnographische Erkundungen, Erlebniswelten. Springer Fachmedien Wiesbaden 2015. S. 9-16.

Ho, Jung-Chun, Shu-Fen Kao, Jung-Der Wang, Chien-Tien Su, Chiao-Tzu Patricia Lee, Ruey-yu Chen, Hung-Lun Chang, Marco Ieong und PeterWushou Chang (2013): Risk perception, trust, and factors related to a planned new nuclear power plant in Taiwan after the 2011 Fukushima disaster. In: Journal of Radiological Protection. Vol. 33 2013. S. 773 – 789.

Hobsbawm, Eric (1952): The Machine Breakers. In: Past and Present. No 1. Feb 1952. S. 57-70.

Holmes, Douglas (2009): Experimental identities (after Maastricht). In: Jeffrey Checkel und Peter Katzenstein (Hrsg.): European Identity. Cambridge University Press, Cambridge. S. 52-80.

Holmes, Douglas und George Marcus (2012): Collaborative Imperatives: A Manifesto, of Sorts, for the Reimagination of the Classic Scene of Fieldwork Encounter. In: Monica Konrad (Hrsg.): Collaborators Collaborating Counterparts in Anthropological Knowledge and International Research Relations. Berghahn Books. S. 126-144.

Holmes, Douglas (2019): Markets are a function of language: Notes on a narrative economics. In: Economics Discussion Papers. Nr. 2019-18. S. 1-16.

Holmgren, Åke (2007): A Framework for Vulnerability Assessment of Electric Power Systems. In: Alan T. Murray und Tony H. Grubesic (Hrsg.): Critical Infrastructure. Reliability and Vulnerability. Springer, Berlin 2007. S. 31 – 56.

Homeland Security Council (2007): National Strategy for Pandemic Influenza. Implementation Plan. One Year Summary. Zuletzt aufgerufen online am 07.02.2018 unter: https://www.cdc.gov/flu/pandemic-resources/pdf/pandemic-influenza-implementation.pdf

Hong, Jason (2012): The Current State of Phishing Attacks. In: Communications of the ACM, Vol. 55, Nr. 1, S. 74-81.

Hood, John und Shahid Nawaz (2004): Political Risk Exposure and Management in Multi-National Companies: Is There a Role for the Corporate Risk Manager? In: Risk Management, Vol. 6, No. 1 (2004). S. 7-18.

Horst, Sven-Ove (2012): Risikomanagement im Krankenhaus. Eine postmoderne Perspektive. Eichstätt-Ingolstadt : Universitätsbibliothek der Katholischen Universität Eichstätt-Ingolstadt.

Hoffmann, E.T. A. (1816): Der Sandmann. Reclam, Ditzingen, 2015.

Huang, Keman, Stuart Madnick, Nazli Choucri und Fang Zhang (2021): A Systematic Framework to Understand Transnational Governance for Cybersecurity Risks from Digital Trade. In: Global Policy. Vol. 12, Nr. 5. S. 625-638.

Huber, Markus, Stewart Kowalskiy, Marcus Nohlbergz und Simon Tjoa (2009): Towards Automating Social Engineering. Using Social Networking Sites. In: Computational Science and Engineering, 29.-31. Aug. 2009. S. 117-124.

Ivanov, Dmitry und Alexandre Dolgui (2020): Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. In: International Journal of Production Research, Taylor & Francis, 2020, Vol. 58, Nr. 10. S. 2904-2915.

Jadeja, Yashpalsinh und Kirit Modi (2012): Cloud Computing - Concepts, Architecture and Challenges. In: 2012 Intenational Conference on Computing, Electronics and Electrical Technologies [ICCEET]. S. 877-880.

Järveläinen, Jonna (2012): IT incidents and business impacts: Validating a framework for continuity management in information systems. In: International Journal of Information Management Vol. 33. S. 583–590.

Jarvis, Darryl. (2000): International Relations and the Challenge of Postmodernism. Defending the Discipline. Columbia.

Jarvis, Darryl (2007): Risk, Globalisation and the State: A Critical Appraisal of Ulrich Beck and the World Risk Society Thesis. In: Global Society, Vol. 21, No. 1, January, 2007. S. 23-47.

Jarvis, Darryl (2008): Conceptualizing, Analyzing and Measuring Political Risk: The Evolution of Theory and Method. National University of Singapore, 2008. S. 1-78.

Jarvis, Darryl (2011): Theorising Risk and Uncertainty in International Relations: The Contributions of Frank Knight. In: International Relations, 25(3). S. 296– 312.

Jokobsen, Jo (2012): Political Risk and the Multinational Company. Concepts, Theories and Evidence. Trondheim, 2012.

Jonen, Andreas und Volker Lingnau (2004) : Basel II und die Folgen für das Controlling von kreditnehmenden Unternehmen. In: Beiträge zur Controlling-Forschung, No. 1.

Jung, Hans und Patricia Kraft (2017): Digital vernetzt. Transformation der Wertschöpfung: Szenarien, Optionen und Erfolgsmodelle für smarte Geschäftsmodelle, Produkte und Services. Carl Hanser Verlag, München.

Jüttner, Uta (2005): Supply chain risk management Understanding the business requirements from a practitioner perspective. In: The International Journal of Logistics Management. Vol. 16 Nr. 1, 2005. S. 120 – 141.

Kahan, Jerome, Andrew C. Allen und Justin K. George (2009): An Operational Framework for Resilience. In: Journal of Homeland Security and Emergency Management. Vol. 6, Nr. 1 2009. S. 1 – 48.

Kahl, Martin (2011): Introduction: Dealing with Transnational Risks of Violence. In: Martin Kahl (Hrsg.): The Transnationalisation of Risks in Violence. 2011, Baden-Baden. S. 7-16.

Kahler, Miles (2018): Countering Illicit Financial Flows: Expanding Agenda, Fragmented Governance. In: Kahler, Miles Maya Forstater, Michael G. Findley, Jodi Vittori, Erica Westenberg und Yaya Fanusie (Hrsg.): Global Governance to Combat Illicit Financial Flows. Council on Foreign Relations, New York. S. 1-11.

Kaldor, Mary (2018): Global Security Cultures. Polity Press, Medford.

Kaplan, Stanley und John Garrick 1981: On the Quantitative Definition of Risk. In: Risk Analysis, Vol. I, No. I, 1981. S. 11-27.

Karim, Akram Jalal (2011): Business Disaster Preparedness: An Empirical Study for measuring the Factors of Business Continuity to face Business Disaster. In: International Journal of Business and Social Science. Vol. 2, Nr. 18. S. 183 – 192.

Kasperson, Roger, Ortwin Renn, Paul Slovic, Halina Brown, Jacque Emel, Robert Goble, Jeanne Kasperson, und Samuel Ratic (1988): The Social Amplification of Risk A Conceptual Framework. In: Risk Analysis, Vol. 8, No. 2, 1988. S. 177-187.

Kaufmann, Mareile (2013): Emergent self-organisation in emergencies: Resilience rationales in interconnected societies. In: International Policies, Practices and Discourses. Vol. 1, Nr. 1. S. 53–68.

Kaufmann, Mareile (2015): Resilience governance and ecosystemic space: A critical perspective on the EU approach to Internet security. In: Environment and Planning D: Society and Space. Vol. 33. S. 512– 527.

Kaufmann, Stefan und Sabine Blum (2011): Governing (In)Security. The Rise of Resilience. In: Helmuth Gander, Walter Perron, Ralf Poscher, Gisela Riescher und Thomas Würtenberger (Hrsg.): Resilienz in der offenen Gesellschaft. Symposium des Centre for Security and Society. Nomos, Baden-Baden 2011. S. 235-257.

Khan, Omera und Daniel A. Sepúlveda Estay (2015): Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. In: Technology Innovation Management Review. Apr. 2015. S. 6 – 12.

Kharraz, Amin, William Robertson, Davide Balzarotti, Leyla Bilge, und Engin Kirda (2015): Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: *Proceedings of the International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) Mailand. Juli 2015. S. 1-20.*

Kianpour, Mazaher, Stewart Kowalski und Harald Øverby (2022): Advancing the concept of cybersecurity as a public good. In: Simulation Modelling Practice and Theory. Vol. 116. S. 1-16.

Kilger, Christoph (2008): Computer Assembly. In: Stadtler, Hartmut und Christoph Kilger (Hrsg.): Supply Chain Management and Advanced Planning. Concepts, Models, Software, and Case Studies. Springer, Berlin 2008. S. 381 – 398.

Kirk, Jessica und Matt McDonald (2021): The Politics of Exceptionalism: Securitization and COVID-19. In: Global Studies Quarterly, Nr. 1. S. 1–12.

Klick, Heiko und Olga Andruschak (2014): Verwundbarkeit an der Schnittstelle von Informationstechnologie und anwendendem Personal. In: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2014): Stromausfall. Grundlagen und Methoden zur Reduzierung des Ausfallrisikos der Stromversorgung. BBK, Bonn. S. 90 - 94.

Klinke, Andreas und Ortwin Renn (2002): A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. In: Risk Analysis Vol. 22 (6). S. 1071–1094.

Knight, Frank (1921): Risk, Uncertainty, and Profit. Kelly New York.

Knoblauch, Hubert (2001): Fokussierte Ethnographie: Soziologie, Ethnologie und die neue Welle der Ethnographie. In: Sozialer Sinn, Vol. 2, Nr. 1. S. 123-141.

Koch, Martin (2017): Internationale Organisationen in der Weltgesellschaft. Campus Verlag, Frankfurt/New York, 2017.

Kocher, Martin und Klaus Weyerstraß (2020): Coronavirus stellt nationale und internationale Wirtschaftspolitik vor große Herausforderungen. In: ÖGfE Policy Brief 11, 2020.

Kolvart, Merit, Margus Poola und Addi Rull (2016): Smart Contracts. In: Tanel Kerikmäe und Addi Rull (Hrsg.): The Future of Law and eTechnologies. Springer Verlag. S. 133 – 148.

Kotter, John (2008): A Sense of Urgency. Harvard Business School Publishing. Boston.

Krabel, Stefan (2016): Arbeitsmarkt und Digitalisierung – Wie man benötigte digitale Fähigkeiten am Arbeitsmarkt messen kann. In: Volker Wittpahl (Hrsg.). Digitalisierung. Bildung.Technik. Innovation. Springer. Berlin, 2016. S. 99 - 107.

Krahmann, Elke (2005): From State to Non-State Actors: The Emergence f Security Governance. In: Krahmann, Elke (Hrsg.): New Threats and New Actors in International Security. New York 2005. S. 3-22.

Krahmann, Elke (2007): Risk Markets: The Commodification of Security and the Risk Society. Paper for: 6th Pan-European International Relations Conference Turin, 12-15 September 2007.

Krotofil, Marina und Alvaro A. Cárdenas (2013): Resilience of Process Control Systems to Cyber-Physical Attacks. In: Hanne Riis Nielson and Dieter Gollmann (Hrsg.): Secure IT Systems. NordSec 2013, S. 166 – 182.

Krüger, Wolfgang (2016): Was bedeuten Digitalisierung und Industrie 4.0 für den Mittelstand? In: Krüger, Wolfgang (Hrsg.): Digitalisierung und Industrie 4.0 – Herausforderungen für den Mittelstand. Schriftenreihe der FHM, Bielefeld, Nr. 8. S. 5 – 12.

Kuerbis, Brenden und Farzaneh Badiei (2017): Mapping the Cybersecurity Institutional Landscape. In: Digital Policy, Regulation and Governance. Nr. 19, Vol. 6. S. 466–492.

Kulatilaka, Nalin (2001): Strategic Options in the Digital Era. In: Business Strategy Review, Volume 12, No. 4, 2001.

Kundur, Deepa, Xianyong Feng, Shan Liu, Takis Zourntos und Karen Butler-Purry (2010): Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. In: IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids. 29 - 31 November 2010, Aalborg.

Lallie, Harjinder Singh, Lynsay Shepherd, Jason Nurse, Arnau Erola, Gregory Epiphaniou Carsten Maple und Xavier Bellekens (2021): Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. In: Computers & Security. Vol. 105. June 2021.

Lam, Wing (2002): Ensuring Business Continuity. In: IT Pro. Jun. 2002. S. 19 – 25.

Lansdall-Welfare, Thomas, Saatviga Sudhahar, Giuseppe A. Veltriy und Nello Cristianini (2014): On the Coverage of Science in the Media: A Big Data Study on the Impact of the

Fukushima Disaster. Conference Paper: International Conference on Big Data, 27. – 30. Okt 2014, Washington DC.

Langheinrich, Marc und Friedemann Mattern (2003): Digitalisierung des Alltags. Was ist Pervasive Computing? In: Aus Politik und Zeitgeschichte (B 42/2003), 13. Oktober 2003.

Langwald, Katharina (2021): Multidisciplinary Approaches to Security: The Paris School and Ontological Security. Zuletzt aufgerufen am 27.05.2022 unter: https://www.e-ir.info/2021/07/13/multidisciplinary-approaches-to-security-the-paris-school-and-ontological-security/

Lansdall-Welfare, Thomas, Saatviga Sudhahar, Giuseppe A. Veltriy und Nello Cristianini (2014): On the Coverage of Science in the Media: A Big Data Study on the Impact of the Fukushima Disaster. Conference Paper: International Conference on Big Data, 27. – 30. Okt 2014, Washington DC.

LaPorte, Todd (2007): Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise. In: Journal of Contingencies and Crisis Management. Volume 15 Number 1 March 2007. S. 60-64.

Leander, Anna (2005): The Market for Force and Public Security: The Destabilizing Consequences of Prrivate Military Companies. In: Journal of Peace Research. Vol. 42, Nr. 5. S. 605–622.

Lee, C.K.M, Yu Ching Yeung und Zhen Hong, (2012): An integrated framework for outsourcing risk management. In: Industrial Management & Data Systems, Vol. 112 Nr. 4, S. 541 – 558.

Lemke, Thomas (2000): Foucault, Governmentality, and Critique. In: Rethinking Marxism Conference, University of Amherst (MA), September 21-24, 2000. S.1-17.

Lepping, Joachim und Matthias Palzkil (2016): Die Chance der digitalen Souveränität. In: Volker Wittpahl (Hrsg.). Digitalisierung. Bildung. Technik. Innovation. Springer. Berlin, 2016. S. 17 – 26.

Lieberman, Gary (2015): Preparing for a Cyberattack by Extending BCM Into the C-suite. In: ISACA Journal Vol. 5. S.

Liebetrau, Tobias; Christensen, Kristoffer Kjærgaard (2020): The Ontological Politics of Cyber Security. Emerging Agencies, Actors, Sites and Spaces. In: European Journal of International Security. Zuletzt online aufgerufen am 24.02.2021 unter: https://doi.org/10.1017/eis.2020.10

Linkov, Igor, Daniel A. Eisenberg, Kenton Plourde, Thomas P. Seager, Julia Allen und Alex Kott (2013): Resilience metrics for cyber systems. In: Environment Systems and Decisions. Vol. 33, Nr. 4, 2013. S. 471 476.

Luhmann, Niklas (1984): Soziale Systeme. Grundriß einer allgemeinen Theorie, Frankfurt: Suhrkamp 1984.

Luhmann, Niklas (1986): The autopoiesis of social systems. In: Felix Geyer und Johannes van der Zouwen (Hrsg.): Sociocybernetic Paradoxes. Sage Publications, London, 1986, S. 172-192.

Luhmann, Niklas (1991): Soziologie des Risikos. Berlin, New York 1991.

Luhmann, Niklas (1996): Das Risiko der Versicherung gegen Gefahren. In: Soziale Welt. 47, (3). S. 273-283.

Luhmann, Niklas (2000): Organisation und Entscheidung. Wiesbaden 2000.

Luisi, Pier (2003): Autopoiesis: a review and a reappraisal. In: Naturwissenschaften. Nr. 90. S. 49–59.

Lupton, Deborah (2006): Sociology and risk. In: Gabe Mythen und Sandra Walklate (Hrsg.), Beyond the Risk Society: Critical Reflections on Risk and Human Security. Maidenhead: Open University Press, S.11—24.

Majinge, Charles (2020): Can Multinational Corporations Help Secure Human Rights and the Rule of Law? The Case of Sudan. In: Law and Politics in Africa, Asia and Latin America. Vol. 44, Nr. 1. S. 7-31.

Manzei, Alexandra (2009): Neue betriebswirtschaftliche Steuerungsformen im Krankenhaus: wie durch die Digitalisierung der Medizin ökonomische Sachzwänge in der Pflegepraxis entstehen. In: Pflege und Gesellschaft 14 (2009), 1, S. 38-53.

Marom, Shaike und Robert N. Lussier (2020): Corporate Social Responsibility during the Coronavirus Pandemic: An Interim Overview. In: Business and Economic Research, Vol. 10, Nr. 2. S. 250-269.

Marshall, Tim (2017): Die Macht der Geographie. Dtv, Köln. 5. Auflage.

Maturana, Humberto und Francisco Varela (1980): Autopoiesis and Cognition: The Realization of the Living, Reidel, Dordrecht.

McGuire, Cheri (2015): The Expanding Cybersecurity Threat. In: Technology Innovation Management Review TIM Lecture Series. Mar. 2015. S. 46 – 48.

McLean, Craig, Alan Patterson und John Williams (2009): Risk assessment, policy-making and the limits of knowledge: the precautionary principle and international relations. In International Relations, 23 (4). S. 548-566.

Mendonça, David und William Alan Wallace (2006): Impacts of the 2001 World Trade Center Attack on New York City Critical Infrastructures. In: Journal of Infrastructure Systems. Dec. 2006. S. 260 -270.

Meredith, Lisa, Lisa Shugarman, Anita Chandra, Stephanie Taylor, Stefanie Stern, Ellen Burke Beckjord, Andrew Parker und Terri Tanielian (2008): Analysis of Risk Communication Strategies and Approaches with At- Risk Populations to Enhance Emergency Preparedness, Response, and Recovery. In: RAND Health working paper series. December 2008.

Menzel, Ulrich (2021): Corona und die gefesselte Globalisierung. In: Berliner Journal für Soziologie. Nr. 7. S. 1-30.

Mishna, Faye, Elizabeth Milne, Marion Bogo und Luana Pereira (2021): Responding to COVID-19: New Trends in Social Workers' Use of Information and Communication Technology. In: Clinical Social Work Journal (2021) Vol. 49. S. 484–494.

Miller, Kent (1992): A Framework for Integrated Risk Management in International Business. In: Journal of International Business Studies, Vol. 23, 2. S. 311-331.

Mingers, John (1989): An Introduction to Autopoiesism. Implications and Applications. In: Systems Practice. Vol. 2. Nr. 2. S. 159-180.

Ministr, Jan, Martin Ńtevko und Josef Fiala (2009): The it service continuity management principles implementation by method A2. In: IDIMT Conference, Prag, Juli 2009. S. 131 – 140.

Mohler, G, M. Short, Sean Malinowski, Mark Johnson, G. Tita, Andrea Bertozzik und P. J. Brantingham (2015): Randomized Controlled Field Trials of Predictive Policing. In: Journal of the American Statistical Association, 110(512). S. 1-43.

Momani, Naill (2010): Business Continuity Planning: Are We Prepared for Future Disasters. In: American Journal of Economics and Business Administration 2 (3). S. 272-279.

Moser, Andreas, Christopher Kruegel and Engin Kirda (2007): Exploring Multiple Execution Paths for Malware Analysis. In: Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washington, 20. – 23. Mai 2007. S. 231-245.

Mosin, Hasan, Nilesh Prajapati und Safvan Vohara (2010): Case study on social engineering techniques for persuasion. In: International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC). Vol. 2, Nr. 2, June 2010. S. 17 – 23.

Mounier-Jack, Sandra und Richard Coker (2006): How prepared is Europe for Pandemic Influenza? An Analysis of National Plans.Zuletzt online aufgerufen am 24.06.2021 unter: https://www.espace-ethique.org/sites/default/files/44._london_school_evaluation.pdf

Müller, Klaus (2011): Verordnete Sicherheit – das Schutzprofil für das Smart Metering Gateway. Eine Bewertung des neuen Schutzprofils. In: Datenschutz und Datensicherheit (8) 2011. S. 547 – 551.

Murray, Alan und Tony Grubesic (2007): Overview of Reliability and Vulnerability in Critical Infrastructure. In: Alan T. Murray und Tony H. Grubesic (Hrsg.): Critical Infrastructure. Reliability and Vulnerability. Springer, Berlin 2007. S. 1 – 8.

Mythen, Gabe (2004): Ulrich Beck. A critical introduction to the Risk Society. London, 2004.

N-Q

Nasiri, Mina, Juhani Ukko, Minna Saunila und Tero Rant (2020): Managing the digital supply chain: The role of smart technologies. In: Technovation. Vol. 96–97, August–September 2020.

Neumann, Kirsten, Rainer Moorfeld, Kerstin Reulke (2016): Die Digitalisierung der Energiewende - vom Smart Grid zur intelligenten Energieversorgung In: Volker Wittpahl (Hrsg.). Digitalisierung. Bildung.Technik. Innovation. Springer. Berlin, 2016. S. 141 - 150.

Nicoll, Scott und Russell Owens (2013): Emergency Response and Business Continuity. The Next Generation in Planning. In: Professional Safety. Sept. 2013. S. 50 – 55.

Nijaz, Bajgoric und Young Moon (2009): Enhancing systems integration by incorporating business continuity drivers. In: Industrial Management & Data Systems Vol. 109 Nr. 1. S. 74-97.

Ng, Kwan-Hoong und Mei-Li Lean (2012): The Fukushima nuclear crisis reemphasizes the need for improved risk communication and better use of social media. In: Health physics. Sept. 2012. S. 307 – 310.

Norio, Okada, Tao Ye, Yoshio Kajitani, Peijun Shi, und Hirokazu Tatano (2011): The 2011 Eastern Japan Great Earthquake Disaster: Overview and Comments. In: Interantional Journal of Disaster Risk Science. 2011 Vol. 2, Nr. 1. S. 34 – 42.

Olaniyan, Azeez (2011): Unorthodox peacekeepers and responses in Africa. In: Sabelo Gumedz (Hrsg.): From market for force to market for peace Private military and security companies in peacekeeping operations. ISS Monograph Number 183. Pretoria, 2011. S. 5-16.

Omar, Adnan, David Alijani, und Roosevelt Mason (2011): Information technology disaster recovery plan: case study. In: Academy of Strategic Management Journal. Vol. 10, Nr. 2, 2011. S. 127-142.

Orebaugh, Angela (2012): Social Media Malware. In: IA Newsletter. Vol. 15, Nr. 2, 2012. S. 4 – 6.

Ortiz, Horacio (2009): Investors and efficient markets: The everyday imaginaries of investment management. In: Economic sociology. The European electronic newsletter. Vol. 11, Nr. 1. S. 34-40.

Ortiz, Horacio (2013): Financial value. Economic, moral, political, global. In: HAU: Journal of Ethnographic Theory Vol. 3, Nr. 1. S. 64–79.

Ortiz, Horacio (2021): A political anthropology of finance: Studying the distribution of money in the financial industry as a political process. In: Anthropological Theory. Vol. 21, Nr. 1. S. 3–27.

Ortiz, Isabel, Sara Burke, Mohamed Berrada und Hernán Saenz Cortés (2022): World Protests A Study of Key Protest Issues in the 21st Century. Friedrich-Ebert-Stiftung New York.

Osterhammel, Jürgen (2010): Die Verwandlung der Welt. Eine Geschichte des 19. Jahrhunderts. BpB, Bonn.

Osterholm, Michael (2005): Preparing for the Next Pandemic. In: Foreign Affairs. Vol. 84, No. 4. S. 24 – 37.

Owen, Louise (2009): Performing 'risk': Neoliberalization and contemporary performance. Queen Mary, University of London. Zuletzt aufgerufen am 08.02.2018: https://qmro.qmul.ac.uk/xmlui/bitstream/handle/123456789/489/OWENPerformingRisk2010.pdf?sequence=1

Pauli, Manfred, Michael Schermann und Helmut Krcmar (2010): The Risk-Aware Enterprise Architecture: Towards a Transparent Inventory of IT Risk Management Artifacts. In: Klaus-

Peter Fähnrich und Bogdan Franczyk (Hrsg.): Informatik 2010 Service Science – Neue Perspektiven für die Informatik. Band 2. Leipzig 2010. S. 259 – 264.

Pathak, P.B. (2016): A Dangerous Trend of Cybercrime: Ransomware Growing Challenge. In: International Journal of Advanced Research in Computer Engineering & Technology Vol. 5 Nr. 2, Feb. 2016. S. 371 – 373.

Perrow, Charles (2011): Fukushima and the inevitability of accidents. In: Bulletin of the Atomic Scientists. Nov. 2011 67. S. 44 - 52.

Petersen, Karen (2017): Risk and Security. In: Myriam Dunn Cavelty und Thierry Balzacq (Hrsg.): Routledge Handbook on Security Studies. Routledge, New York, 2017. S. 117-125.

Pfeifer, Dietmar (2006): Risikomanagement und Solvency II bei Versicherungsunternehmen. Ergebnisse der Marktstudie. Wissenschaftliche Marktstudie der Carl von Ossietzky Universität Oldenburg.

Pike, Andy, Stuart Dawley und John Tomaney (2010): Resilience, adaption and adaptability. In: Cambridge Journal of Regions, Economy and Society 2010, 3, S. 59-70.

Power, Michael (2005): The invention of operational risk, Review of International Political Economy, Vol. 12, 4. S. 577-599.

Power, Michael, Tobias Scheytt, Kim Soin und Kerstin Sahlin (2009): Reputational Risk as a Logic of Organizing in Late Modernity. In: Organization Studies 30. S. 301–324.

Provos, Dean, Niels McNamee, Panayiotis Mavrommatis, Ke Wang and Nagendra Modadugu (2007): The Ghost in the Browser. Analysis of Web-based Malware. In: HotBots'07 Proceedings of the first conference on Hot Topics in Understanding Botnets. S. 1-9. Zuletzt aufgerufen am 09.11.2017: http://web2.airmail.net/jripley/Ghost%20in%20the%20Browser.pdf.

R-Z

Racz, Nicolas, Edgar Weippl und Andreas Seufert (2010): Questioning the need for separate IT risk management frameworks. In: Klaus-Peter Fähnrich und Bogdan Franczyk (Hrsg.): Informatik 2010 Service Science – Neue Perspektiven für die Informatik. Band 2. Leipzig 2010. S. 245 – 252.

Rahim, Robbi, Heri Nurdiyanto, Ansari Saleh, Dahlan Abdullah, Dedy Hartama und Darmawan Napitupulu (2018): Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm. In: Journal of Physics: Conference Series 954 (2018). S. 1-5.

Rasmussen, Jens (1997): Risk Management in a dynamic society: A modelling problem. In: Safety Science Vol. 27, No. 2/3. S. 183-213.

Renn, Ortwin and Andreas Klinke (2004): Systemic risks: a new challenge for risk management. In: EMBO reports; Vol. 5. S. 41-46.

Rieger, Oya (2008): Preservation in the Age of Large-Scale Digitization. A White Paper. Council on Library and Information Resources. Washington D.C. 2008.

Riekmann, Johannes und Martina Kraus (2015): Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe, DIW-Wochenbericht, Vol. 82, Nr. 12, S. 295-301.

Roark, Brian, Murat Saraclar und Michael Collins (2008): Discriminative n-gram language modeling. In: Computer Speech and Language 21 (2007) 373–392.

Robert Koch Institut (2007): Nationaler Pandemieplan Teil III. Berlin.

Rodríguez, Eduardo und Juan Carlos García-Palomares (2014): Measuring the vulnerability of public transport networks. In: Journal of Transport Geography. Feb. 2014. S. 50 – 63.

Rodrik, Dani (2001): The Global Governance of Trade. As if Development really mattered. Working Paper for United Nations Development Programme, 2001.

Roitsch, Mario und Herbert Meyr (2008): Oil Industry. In: Stadtler, Hartmut und Christoph Kilger (Hrsg.): Supply Chain Management and Advanced Planning. Concepts, Models, Software, and Case Studies. Springer, Berlin 2008. S. 399 – 414.

Rose, Adam (2004): Defining and measuring economic resilience to disasters. In: Disaster Prevention and Management. Vol. 14, Nr. 4. S. 307-314

Rose, Adam (2011): Resilience and Sustainability in the Face of Disasters. In: Environmental Innovation and Societal Transitions. Vol. 1. S. 96 – 100.

Rüegsegger, Adrian (2016): Messung von Körperdaten an der Schnittstelle zwischen Lifestyle und Medizin. In: ARS Medici. Nr. 24, 2016. S. 1149 -1152.

Ruiz-Albacete, Virginia, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez, Javier Galbally, Julian Fierrez und Javier Ortega-Garcia (2008): Direct attacks using fake images in iris verification. In: Schouten B., Juul N.C., Drygajlo A., Tistarelli M. (Hrsg.): Biometrics and Identity Management. Lecture Notes in Computer Science, Vol. 5372. Springer, Heidelberg.

Sahebjamnia, Navid, S.A. Torabi und Afshin Mansouri (2015): Integrated business continuity and disaster recovery planning: Towards organizational resilience. In: European Journal of Operational Research · April 2015. S. 261 – 273.

Sako, Mari (2006): Outsourcing and Offshoring: Implications for Productivity of Business Services. In: Oxford Review of Economic Policy · December 2006. S. 499-512.

Salvi, Harshada und Ravindra V. Kerkar (2015): Ransomware: A Cyber Extortion. In: Asian Journal of Convergence in Technology Volume II Issue III (2015). S. 1 – 6.

Sarewitz, Daniel et. al. (2003): Vulnerability and Risk: Some Thaughts from a Political and Policy Perspective. In: Risk Analysis, Vol. 23, No. 4, 2003. S. 805 – 810.

Scaife, Nolen, Henry Carter, Patrick Traynor and Kevin R.B. Butler (2016): CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In: 2016 IEEE 36th International Conference on Distributed Computing Systems. S. 303 – 312.

Schäfer, Dorothea (2021): Wirecard-Skandal: Wirtschaftsprüfung am Scheideweg. In: DIW Wochenbericht. Deutsches Institut für Wirtschaftsforschung. Vol. 88, Nr. 18. S. 320-321.

Scheer, Dirk, Stefan Gold, Christina Benighaus, Ludger Benighaus, Julia Ortleb und Ortwin Renn (2010): Kommunikation von Risiko und Gefährdungspotenzial aus Sicht verschiedener Stakeholder. Bundesinstitut für Risikobewertung, Berlin.

Scherrer, Yvonne (2018): Organisationale Resilienz und Antifragilität in Einsatzorganisationen. In: Eva-Maria Kern, Richter, Gregor Richter, Johannes C. Müller, Fritz-Helge Voß (Hrsg.): Einsatzorganisationen. Erfolgreiches Handeln in Hochrisikosituationen. Springer Fachmedien. Wiesbaden. S. 79-101.

Schermann, Michael, und Helmut Krcmar (2010): Risk Management, Compliance und Governance für widerstandsfähige Informationssysteme. In: Klaus-Peter Fähnrich und Bogdan Franczyk (Hrsg.): Informatik 2010 Service Science – Neue Perspektiven für die Informatik. Band 2. Leipzig 2010. S. 227 – 228.

Schintler, Laurie Anne, Sean Gorman, Rajendra Kulkarni und Roger Stough (2007): Moving from Protection to Resiliency: A Path to Securing Critical Infrastructure. In: Alan T. Murray und Tony H. Grubesic (Hrsg.): Critical Infrastructure. Reliability and Vulnerability. Springer, Berlin 2007. S. 291 – 308.

Schulze, Matthias (2021): Ransomware: technische, nationale und multilaterale Gegenmaßnahmen. In: SWP-Aktuell. Nr. 56. S. 1-8.

Schumpeter, Joseph A. (1942): Capitalism, Socialism and Democracy. Harper and Broher. New York.

Schwering, Benjamin (2010): Die Relevanz von IT-Compliance Prüfungsstandards bei IT-Auslagerungen im deutschen Bankensektor. In: Klaus-Peter Fähnrich und Bogdan Franczyk (Hrsg.): Informatik 2010 Service Science – Neue Perspektiven für die Informatik. Band 2. Leipzig 2010. S. 231 – 238.

Seidl, David und Hannah Mormann (2015): Niklas Luhmann as Organization Theorist. In: Paul Adler (Hrsg.): Oxford Handbook of Sociology, Social Theory and Organization Studies: Contemporary Currents. Oxford: Oxford University Press. S. 125-157.

Serres, Michel (1994): Atlas. Julliard. Paris.

Serres, Michel (1995): Genesis. University of Michigan Press, Ann Arbor.

Sheth, Jagdish, Can Uslay und Rajendra Sisodia (2021): Globalization of Competition: The Global Rule of Three and the New Triad Power. In: Bala Balachandran (Hrsg.): GLIM Management Review and Transformation. Great Lakes Institute of Management, Gurgaon. S. 11-29.

Singer, Andrew (2007): Potential Risks Associated with the Proposed Widespread Use of Tamiflu. In: Environmental Health Perspectives. Vol. 115. S. 102-106.

Sittig, Dean und Hardeep Singh (2016): A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. In: Applied Clinical Informatics 2016; 7: 624–632.

Shaw, Gregory (2004): The competencies required for executive level business crisis and continuity managers. George Washington University 2004.

Smit, Naomi (2005): Business Continuitz Management. A maturity model. Erasmus University Rotterdam. Informatics & Economics.

Smith, David (2003): Business continuity and crisis management. In: Management quarterly. Jan. 2003. S. 27 – 33.

Strange, Susan (2000): States, Firms, And Diplomacy. In: Jeffry Frieden und David Lake (Hrsg.): International Political Economy. Perspectives On Global Power and Wealth. Routledge, London. S. 60-68.

Stoeckli, Emanuel, Christian Dremel und Falk Uebernickel (2018): Exploring characteristics and transformational capabilities of InsurTech innovations to understand insurance value creation in a digital world. In: Electronic Markets. Vol. 28, S. 287-305.

Stowasser Sascha und Anika Peschl 2019: Arbeitswelt im Wandel: Qualifizierung zu resilienzfördernder Führung. In: Anika Peschl, (Hrsg.): Arbeitswelt im Wandel – Maßnahmen zur Unterstützung resilienzfördernder Führung. Leistung & Entgelt. S. 3-45.

Talaulicar, Till (2009): Global retailers and their corporate codes of ethics: the case of Wal-Mart in Germany. In: The Service Industries Journal. Vol. 29, Nr. 1. S. 47 –58.

Tierney, Kathleen und Michel Bruneau (2007): Conceptualizing and Measuring Resilience. A Key to Disaster Loss Reduction. In: TR News Vol. 250. Nr. 5. S. 14 – 17.

Thomas, Kurt und David Nicol (2010): The Koobface Botnet and the Rise of Social Malware. In: Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software, Malware 2010.

Todo, Yasuyuki, Kentaro Nakajima und Petr Matous (2014): How do supply chain networks affect the resilience of firms to natural disasters? Evidence from the great East Japan earthquake. In: Journal of regional science. Vol. 55, Nr. 2. Mar. 2015. S. 209 – 229.

Torabi, S.A., H. Rezaei Soufi und Navid Sahebjamnia (2014): A new framework for business impact analysis in business continuity management (with a case study). In: Safety Science. S. 309 – 323.

TU Berlin (2012): Energie- und Kraftstoffversorgung von Tankstellen und Notstromaggregaten bei Stromausfall (TankNotStrom). TOTAL Deutschland GmbH, Berlin.

Tuan, Tong Anh, Hoang Viet Long, Le Hoang Son, Raghvendra Kumar, Ishaani Priyadarshini und Nguyen Thi Kim Son (2020): Performance evaluation of Botnet DDoS attack detection using machine learning. In: Evolutionary Intelligence. Vol. 13. S. 283–294.

Utz, Sonja, Friederike Schultz und Sandra Glocka (2012): Crisis communication online: How medium, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster. In: Public Relations Review. March 2013. S. 40 – 46.

Vanderstraeten, Raf (2000): Autopoiesis and socialization: on Luhmann's reconceptualization of communication and socialization. In: British Journal of Sociology. Vol.. 51 Nr. 3. S. 581–598.

Vassilaki, Irini (2015): Computer- und Internet-Strafrecht. Universität Oldenburg, Center für lebenslanges Lernen C3L. Oldenburg.

Velte, Anthony, Toby Velte und Robert Elsenpeter (2010): Cloud Computing: A Practical Approach. McGraw-Hill Companies, New York.

Vieten, Ulrike (2020): The "New Normal" and "Pandemic Populism": The COVID-19 Crisis and Anti-Hygienic Mobilisation of the Far-Right. In: Social Sciences Vol. 9 Nr. 9. Zuletzt online aufgerufen am 29.06.2021 unter: https://www.mdpi.com/2076-0760/9/9/165

Vorndran, Ingeborg (2010): Unfallstatistik. Verkehrsmittel im Risikovergleich. In: Statistisches Bundesamt. Wirtschaft und Statistik 12/2010. S. 1083 – 1088.

Voss, Martin und Cordula Dittmer (2016): Resilienz aus katastrophensoziologischer Perspektive. In: Rüdiger Wink (Hrsg.): Multidisziplinäre Perspektiven der Resilienzforschung. Springer, Wiesbaden 2016. S. 179-198.

Waever, Ole (1995): Securitization and Desecuritization. In: Ronnie Lipschutz (Hrsg.): On Security. Columbia University Press, New York, 1995. S. 46-86.

Walter, Gregor (2008): Internetkriminalität: Eine Schattenseite der Globalisierung. Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. Berlin, 2008.

Walser, Konrad und Reinhard Riedl (2010): Unternehmensarchitekturmanagement als Mittler zwischen IT-Governance und IT-Management. In: Klaus-Peter Fähnrich und Bogdan Franczyk (Hrsg.): Informatik 2010 Service Science – Neue Perspektiven für die Informatik. Band 2. Leipzig 2010. S. 253 – 258.

Wang, Bin, Yukun Liu, Jing Qian und Sharon Parker (2021): Achieving Effective Remote Working During the COVID-19 Pandemic: A Work Design Perspective. In: Applied Psychology. Vol. 70. Nr. 1. S. 16 – 59.

Ward, Stephen (2003): Approaches to Integrated Risk Management: A Multi-Dimensional Framework. In: Risk Management, Vol. 5, No. 4 (2003) S. 7-23.

Weber, Stefan (2016): IT-Sicherheit und Nutzer: Chancen und Risiken in der Digitalisierung. In: Volker Wittpahl (Hrsg.). Digitalisierung. Bildung. Technik. Innovation. Springer. Berlin, 2016. S. 27 – 34.

Wentland, Alexander und Nina Klimburg-Witjes (2021): „Die Benutzer sind das Problem, nicht das System. Verantwortung". Vertrauen und Vulnerabilität in IT-Sicherheitsdiskursen. In: Kathrin Braun und Cordula Kropp (Hrsg.): In digitaler Gesellschaft. Neukonfiguration zwischen Robotern, Algorithmen und Usern. Transcript Verlag, Bielefeld. S. 167-188.

Welzbacher, Christian, Walter Pirk, Anne Ostheimer, Karen Bartelt, Jens Bille und Markus Klemmt (2015): Digitalisierung der Wertschöpfungs- und Marktprozesse – Herausforderungen und Chancen für das Handwerk. Hannover, 2015.

Wijnia, Ype und Igor Nikolic (2007): Assessing Business Continuity risks in IT. In: IEEE International Conference on Systems, Man and Cybernetics. 7-10 Oktober 2007, S. 3547 – 3553.

Willems, Diana (2013): Neue Kriminalisierungsrisiken? Zur Bedeutung des Internets für die Kriminalitätsprävention. In: Forum Kriminalprävention Nr. 3, 2013. S. 3-8.

Williams, Michael (2003): Words, Images, Enemies: Securitization and International Politics. In: International Studies Quarterly. Nr. 47. S. 511–531.

Wittpahl, Volker (2016), (Hrsg.): Digitalisierung. Bildung. Technik. Innovation. Springer. Berlin.

Wüllenweber, Kim, Stefanie Jahner und Helmut Krcmar, (2008): Relational Risk Mitigation: The Relationship Approach to Mitigating Risks in Business Process Outsourcing. In: Hawaii International Conference on System Sciences HICSS-41; Big Island, Hawaii, USA.

Wolf, Patrick und Matthias Goeken (2010): Integration von IT- und unternehmensweitem Risikomanagement auf Konzeptebene. In: Klaus-Peter Fähnrich und Bogdan Franczyk (Hrsg.): Informatik 2010 Service Science – Neue Perspektiven für die Informatik. Band 2. Leipzig 2010. S. 239 – 244.

World Health Organization (2009): Pandemic Influenza Preparedness and Response. WHO Press, Genf 2009.

Xue, Ling, Cheng Zhang, Hong Ling, Xia Zhao (2013): Risk-Mitigation in Supply Chain Digitization: A Study of System Modularity and IT Governance. In: Journal of Management Information Systems. Vol. 30. Nr. 1. S. 325 – 352.

Zschoche, Miriam (2015): Performance Effects of Divesting Foreign Production Affiliates: A Network Perspective. In: Long Range Planning. S. 1-11.

Zsidisn, G., S. Melnyk und G. Ragatz (2005): An institutional theory perspective of business continuity planning for purchasing and supply management. In: International Journal of Production Research. Vol. 43. No. 16, Aug. 2005. S. 3401 – 3420.

Onlinequellen:

AGCS (2012): Managing disruptions. Supply chain risk: an insurer's perspective. Zuletzt aufgerufen am 16.02.2017 unter: http://www.agcs.allianz.com/assets/PDFs/white%20papers/AGCS%20Managing%20disruptions%20Nov2012.pdf

AGCS (2013): Allianz Risk Pulse. Focus: Business Risks. Zuletzt aufgerufen am 16.02.2017 unter: http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-RP-Risk%20Barometer%20Jan2013.pdf

AGCS (2018): Allianz Risk Barometer 2018. Zuletzt aufgerufen am 16.12.2018 unter: https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/migration/media/press/document/2018-01-16_AGCS-Medienmitteilung-Risk-Barometer-2018.pdf

AGCS (2020): Allianz Risk Barometer 2020. Zuletzt aufgerufen am 05.05.2021 unter: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html

AGCS (2020a): Coronavirus: business interruption and supply chain impact. Zuletzt aufgerufen am 05.05.2021 unter: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/coronavirus-bi.html

AGCS (2022): Allianz Risk Barometer. Zuletzt aufgerufen am 03.07.2022 unter: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

AT&T (2013): AT&T Business Continuity Study. U.S. National Results. Zuletzt aufgerufen am 02.02.2017 unter: https://www.att.com/Common/about_us/pdf/2013_business_continuity_study.pdf

BaFin (2022): Neue VAIT: BaFin-Rundschreiben tritt in Kraft. Zuletzt aufgerufen am 11.12.2022 unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2022/meldung_2022_03_03_Aktualisierung_VAIT.html

Bain & Company (2013): Versicherungen: Die digitale Herausforderung. Zuletzt aufgerufen am 21.07.2017 unter: http://www.bain.de/Images/BainBrief_Versicherungen_Die-digitale-Herausforderung_FINAL.pdf

BCBS - Basel Committee on Banking Supervision (2012): Principles for the supervision of financial conglomerates. Aufgerufen online zuletzt am 11.02.2018 unter: https://www.bis.org/publ/joint27.pdf

BCM Academy (2016): Das BCM-Barometer. 2015 / 2016 –Jahresumfrage BCM Academy GmbH. Zuletzt aufgerufen am 15.07.2017 unter: http://www.bcmacademy.de/media/bcma.de/Abbildungen/Survey%20BCM%20Barometer/Bericht_2015_2016.pdf. Zuletzt aufgerufen m 30.12.2016.

BDSG - Bundesdatenschutzgesetz. Zuletzt aufgerufen am 04.12.2016 unter https://dejure.org/gesetze/BDSG.

Booz and Company (2008): Bringing Back Best Practices in Risk Management. Banks' Three Lines of Defense. Zuletzt aufgerufen am 09.05.2016 unter: https://www.strategyand.pwc.com/media/file/Bringing-Back-Best-Practices-in-Risk-Management.pdf

Bundesamt für Sicherheit in der Informationstechnologie (BSI) (2019): Die Lage der IT-Sicherheit in Deutschland 2019. Zuletzt aufgerufen am 20.07.2020 unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7

Bundesamt für Sicherheit in der Informationstechnologie (BSI) (2020): Die Lage der IT-Sicherheit in Deutschland 2020. Zuletzt aufgerufen am 05.05.2021 unter:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnologie (BSI) (2022): Cyber-Sicherheitslage im Zusammenhang mit dem russischen Angriff auf die Ukraine. Zuletzt aufgerufen am 19.06.2022 unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Ukraine-Krise/ukraine-krise_node.html

Bundesministerium für Gesundheit (2017): Das E-Health Gesetz. Zuletzt aufgerufen am 20.02.2017 unter: https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/e-health-gesetz/e-health.html

Bundesministerium für Wirtschaft (2017): Den digitalen Wandel gestalten. Zuletzt aufgerufen am 20.02.2017 unter: http://www.bmwi.de/Redaktion/DE/Dossier/digitalisierung.html

Continuity Insights und KPMG (2008) Business Continuity Benchmarking Report. A Study of the Factors Influencing Business Continuity Management Programs. Zuletzt aufgerufen am 16.06.2016 unter: http://www.rbzaneadvisors.com/pdf/CI-KPMG08-FinalResults.pdf

Deloitte (2022): Digital Operational Resilience Act (DORA): Widerstandsfähigkeit für Versicherer. Zuletzt aufgerufen am 11.12.2022 unter: https://www2.deloitte.com/de/de/pages/risk/articles/digital-operational-resilience-act-dora.html

Dohnen, Caspar (2018): Digitale Währung Bitcoin. Ende könnte schon 2022 kommen. Deutschlandfunk. Zuletzt aufgerufen am 11.01.2017 unter: http://www.deutschlandfunk.de/digitale-waehrung-bitcoin-ende-koennte-schon-2022-kommen.769.de.html?dram:article_id=407422

EU-DORA (2022): Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations. Zuletzt aufgerufen am 11.12.2022 unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

EU-DSGVO (2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Zuletzt aufgerufen am 21.11.2018 unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679

Heise Security (2006): Exploits für alle. Dunkle Künste. Aufgerufen zuletzt am 29.06.2017 unter: https://www.heise.de/security/artikel/Dunkle-Kuenste-271410.html

IAEA - International Atomic Energy Agency (2015): The Fukushima Daiichi Accident 2015 Zuletzt aufgerufen am 06.01.2017 unter: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1710-ReportByTheDG-Web.pdf

IFAA – Institut für angewandte Arbeitswissenschaften (2020): Business Continuity Management (BCM). Krisenfestigkeit durch organisationale Resilienz. Zuletzt aufgerufen am 06.12.2022 unter: https://www.arbeitswissenschaft.net/fileadmin/Downloads/Angebote_und_Produkte/Zahlen_Daten_Fakten/ifaa_Zahlen_Daten_Fakten_BCM_2020-05-26.pdf

Kassenärztliche Bundesvereinigung (2017): Positionen der KBV zur elektronischen Patientenakte. Zuletzt aufgerufen am 10.02.2018 unter: http://www.kbv.de/html/31190.php

McAfee (2018): Most Dangerous Celebrity 2018. Zuletzt aufgerufen am 21.12.2018 unter: https://www.mcafee.com/enterprise/de-de/about/newsroom/press-releases/2018/20181002-01.html

McKinsey Global Institute (2011): Big data: The next frontier for innovation, competition, and productivity. Zuletzt aufgerufen online am 15.01.2016 unter: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation

PWC (2009) Exploring ermerging risks. Zuletzt aufgerufen am 01.02.2018 unter: https://globenewswire.com/news-release/2009/06/15/399199/167215/en/PricewaterhouseCoopers-Webcast-Explores-Emerging-Risks-in-a-Global-Environment.html

Ransomletter (2022): Lösegeldzahlungen bei Ransomware-Angriffen: ein geostrategisches Risiko. Zuletzt aufgerufen am 11.12.2022 unter: https://ransomletter.github.io/

Richter, Christoph (2017): Struktur-Rückbau in den Regionen. Wenn das Krankenhaus schließt. Deutschlandfunk. Zuletzt aufgerufen am 31.12.2017 unter: http://www.deutschlandfunk.de/struktur-rueckbau-in-den-regionen-wenn-das-krankenhaus.724.de.html?dram:article_id=406405.

Statista (2018): Anzahl der monatlich aktiven Facebook Nutzer weltweit vom 3. Quartal 2008 bis zum 4. Quartal 2017 (in Millionen). Zuletzt aufgerufen am 11.02.2018 unter: https://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/

Statista (2018a): Polizeilich erfasste Fälle von Cyberkriminalität im engeren Sinne in Deutschland von 2004 bis 2017. Zuletzt aufgerufen am 12.01.2018 unter: https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/

Statista (2018b): Prognose zum Volumen der jährlich generierten digitalen Datenmenge weltweit in den Jahren 2016 und 2025 (in Zettabyte). Zuletzt aufgerufen am 10.01.2018 unter: https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/

Statista (2018c): Vergleich der Anzahl der Filme und Serien im US-Netflix-Katalog in den Jahren 2014 und 2016. Zuletzt aufgerufen am 10.01.2018 unter:

https://de.statista.com/statistik/daten/studie/652040/umfrage/anzahl-der-filme-und-serien-im-us-netflix-angebot/

Statista (2019): Börsenwert der größten Internetunternehmen weltweit im Juni 2019. Zuletzt aufgerufen am 11.12.2022 unter: https://de.statista.com/statistik/daten/studie/217485/umfrage/marktwert-der-groessten-internet-firmen-weltweit/

Statista (2022): Marktkapitalisierung von Google, Apple, Facebook, Amazon und Microsoft in den Jahren 2013 bis 2022. Zuletzt aufgerufen am 14.08.2022 unter: https://de.statista.com/statistik/daten/studie/1187049/umfrage/marktkapitalisierung-gafam/

Statista (2022a): Polizeilich erfasste Fälle von Cyberkriminalität im engeren Sinne[1] in Deutschland von 2007 bis 2021. Zuletzt aufgerufen am 09.12.2022 unter: https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/

Statista (2022b): Umsatz von Google weltweit in den Jahren 2013 bis 2021. Zuletzt aufgerufen am 11.12.2022 unter: https://de.statista.com/statistik/daten/studie/541785/umfrage/umsatz-von-google-weltweit/#:~:text=Im%20Jahr%202021%20belief%20sich,von%20Google%20finden%20Sie%20hier.

Statistisches Bundesamtes (2014): Verkehr. Verkehrsunfälle. Fachserie 8 – Reihe 7 Zuletzt aufgerufen am 15.11.2016 unter: https://www.destatis.de/DE/Publikationen/Thematisch/TransportVerkehr/Verkehrsunfaelle/VerkehrsunfaelleMonat/VerkehrsunfaelleM2080700151094.pdf?__blob=publicationFile.

Tagesschau (2021): Unternehmen wollen selbst impfen. Zuletzt aufgerufen am 15.11.2016 unter: https://www.tagesschau.de/wirtschaft/unternehmen/wirtschaft-impfungen-101.html

---

Zeitschriften:

BBC (2018): BA investigation into website hack reveals more victims. Zuletzt aufgerufen am 05.11.2018 unter: https://www.bbc.com/news/technology-45953237

Beuth, Patrick (2017): Ransomware. Microsoft ist Opfer des eigenen Erfolgs. In Zeit Online. Zuletzt aufgerufen am 14.05.2017 unter: http://www.zeit.de/digital/datenschutz/2017-05/ransomware-wannacry-windows-xp-microsoft-hackerattacke-malware

Guardian (2022): US-Canada bridge blockade risks huge economic damage, governments warn. Zuletzt aufgerufen am 30.11.2022 unter: https://www.theguardian.com/world/2022/feb/09/us-auto-plants-face-shortages-shutdowns-layoffs-protesters-block-canada-bridge

Handelsblatt (2014): Tamiflu-Kritik und starker Franken setzen Roche unter Druck. Zuletzt aufgerufen am 15.12.2015 unter:

http://www.handelsblatt.com/unternehmen/industrie/pharmakonzern-tamiflu-kritik-und-starker-franken-setzen-roche-unter-druck/9764560.html

Handelsblatt (2019): Cyberangriff auf Politiker. Zuletzt aufgerufen am 06.01.2018 unter: https://www.handelsblatt.com/politik/deutschland/datenklau-cyberangriff-auf-politiker-hier-herrscht-voellige-ratlosigkeit/23828688.html

Handelsblatt (2021): Ford muss kurzfristig Produktion stoppen. Zuletzt aufgerufen am 05.05.2021 unter: https://www.handelsblatt.com/unternehmen/industrie/chipmangel-ford-muss-kurzfristig-produktion-stoppen/27097026.html

Handelsblatt (2021a): Millionen aus der Maskenaffäre: Das haben die Unions-Politiker mit ihren Corona-Provisionen gemacht. Zuletzt aufgerufen am 02.06.2021 unter: https://www.handelsblatt.com/politik/deutschland/pandemie-profiteure-millionen-aus-der-maskenaffaere-das-haben-die-unions-politiker-mit-ihren-corona-provisionen-gemacht/27200534.html?ticket=ST-1347960-4Ajm3MBYs3yq9gIAZx92-ap2

Krüger-Brand, Heike und Falk Osterloh (2017): Elektronische Patientenakte. Viele Modelle – noch keine Strategie. In: Deutsches Ärzteblatt, 114, Nr. 43. S. 1658-1662.

Mühlbauer, Peter (2018): OpenSchufa will Bonitätsauskunft-Algorithmus herausfinden. Zuletzt aufgerufen am 19.06.2018 unter: https://www.heise.de/tp/features/OpenSchufa-will-Bonitaetsauskunft-Algorithmus-herausfinden-3975166.html.

Neuerer, Dietmar (2017): Behörde verbietet spionagetaugliche Puppe - Firma wehrt sich. Handelsblatt. Zuletzt aufgerufen am 20. Februar 2017 unter: http://www.handelsblatt.com/politik/deutschland/my-friend-cayla-behoerde-verbietet-spionagetaugliche-puppe-firma-wehrt-sich/19407840.html

Sachsinger, Christian (2017): Microsofts andauernder Einfluss auf Wirtschaft und Gesellschaft. Online verfügbar, zuletzt aufgerufen am 19.05.2017 unter: http://www.br.de/radio/bayern2/programmkalender/ausstrahlung-958362.html

Spiegel Online (2017): Missbrauch von Marktmacht. Zuletzt aufgerufen am 27.06.2017 unter: http://www.spiegel.de/netzwelt/netzpolitik/google-vs-eu-kommission-eu-verhaengt-rekordstrafe-von-2-42-milliarden-a-1154605.html

Spiegel Online (2017): Banker in Frankfurt. Frust, Angst - und super Gehälter. Zuletzt aufgerufen am 11.01.2017 unter: http://www.spiegel.de/wirtschaft/unternehmen/banker-in-frankfurt-veraengstlicht-demotiviert-gut-bezahlt-a-1186876.html

Spiegel Online (2022): Hacker veröffentlichen Gesundheitsdaten von Millionen Australiern. Zuletzt aufgerufen am 29.11.2022 unter: https://www.spiegel.de/netzwelt/web/australien-krankenkasse-medibank-gehackt-taeter-veroeffentlichen-gesundheitsdaten-von-millionen-a-6995839c-68dd-4f2a-93da-4af1f885367d

The Telegraph (2018): British Airways: Reports of delays and cancellations at Heathrow as airline reports 'systems issue'. Zuletzt aufgerufen online am 03.12.2018 unter: https://www.telegraph.co.uk/news/2018/07/18/british-airways-reports-delays-cancellations-heathrow-airline/

Zeit Online (2015): Internetkriminalität. Hacker stehlen Daten von zweitgrößtem US-Krankenversicherer. Zuletzt aufgerufen am 19.05.2017 unter: http://www.zeit.de/digital/2015-02/hacker-usa-krankenversicherung-anthem