ZHAW School of Management and Law
Studiengang Master Wirtschaftsinformatik

School of Management and Law

Masterarbeit

Vergleichende empirische Untersuchung der Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche

Autor: Reto Nüesch Erismann
Auftraggeber: Dr. Tim Geppert, ZHAW
Erstgutachter: Dr. Tim Geppert, ZHAW
Zweitgutachter: Dr. Nico Ebert, ZHAW
Ort, Datum: Winterthur, 09.10.2023

Vorwort

Nach rund 20 Jahren Berufstätigkeit als Ingenieur in der Logistikbranche habe ich mich 2021 für eine Auszeit entschieden und mit Mitte 40 ein Masterstudium in Wirtschaftsinformatik begonnen. Ein halbes Jahr später nahm ich parallel zum Teilzeitstudium eine neue berufliche Herausforderung als Leiter Technik und Applikationen bei Cargologic an. Seitdem verantworte ich u.a. die IT des Unternehmens. Angesichts der akuten Bedrohungslage durch Cyberattacken war die Themenwahl für die Masterarbeit ein Glücksfall für mich. So konnte ich mich intensiv mit der Thematik «Cybersicherheit» auseinandersetzen, wofür ich rückblickend sehr dankbar bin.

An dieser Stelle möchte ich allen, die zu dieser Arbeit beigetragen haben, meinen herzlichen Dank und meine Anerkennung aussprechen. Ein besonderer Dank gilt meinem Betreuer Tim Geppert, dessen fachliche und methodische Unterstützung es mir ermöglicht hat, das Forschungsthema zu strukturieren und mich thematisch weiterzuentwickeln. Seine konstruktiven Ratschläge und sein wertvolles Feedback haben mir geholfen, diese Arbeit zu verfeinern und zu verbessern. Ein weiterer Dank geht an Arne Dreißigacker und Anna Isenhardt für die unkomplizierte Bereitstellung ihrer Forschungsdaten. Dadurch konnte ich meine Ergebnisse mit solchen aus Deutschland und der Schweiz vergleichen. Des Weiteren danke ich den Branchenverbänden Spedlogswiss, vertreten durch Thomas Schwarzenbach, und GS1 Switzerland, vertreten durch Jan Eberle, für die freundliche Unterstützung und Bereitstellung ihrer Mitgliederregister für den Versand der Einladung zur Online-Umfrage. Ihr Netzwerk in der Speditions- und Logistikbranche hat dazu beigetragen, dass die Online-Befragung überhaupt stattfinden konnte. Ein weiterer Dank gilt der Expertin und den Experten, die am Fachgespräch teilgenommen und ihre wertvollen Erkenntnisse und Perspektiven mit mir geteilt haben. Ihre Erfahrungen haben wesentlich dazu beigetragen, die Ergebnisse dieser Arbeit zu reflektieren. Schliesslich danke ich meiner Frau Astrid Erismann ganz herzlich für die Durchsicht der Arbeit und ihre wertvollen Anregungen während des gesamten Schreibprozesses. Ihre Unterstützung hat massgeblich zur Qualität dieser Arbeit beigetragen.

Winterthur, Mai 2023 Reto Nüesch Erismann

Zusammenfassung

Anlässlich der akuten Bedrohungslage durch Cyberattacken weltweit widmet sich die vorliegende Masterarbeit der Frage, wie sich die aktuelle Situation bezüglich Cyberangriffen und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche[1] im Vergleich zur Schweizer Maschinen-, Elektro- und Metallindustrie[2] sowie zur deutschen Logistik- und MEM-Branche darstellt.

Nach einer Literaturanalyse, welche die Bedrohungslage, den Forschungsstand sowie Trends bei technischen und organisatorischen IT-Sicherheitsmassnahmen ermittelte, wurde eine quantitative Querschnittsanalyse in Form einer Online-Befragung durchgeführt. Die in der Schweizer Logistikbranche erhobenen Daten wurden anschliessend ausgewertet und mit bestehenden Daten zur deutschen Logistik- und MEM-Branche sowie zur Schweizer MEM-Branche verglichen. Die gewonnenen Erkenntnisse wurden zudem in einem Fachgespräch diskutiert.

Es zeigte sich, dass die Unternehmen der Schweizer Logistikbranche technisch und organisatorisch auf einem ähnlich hohen Niveau auf Cyberangriffe vorbereitet sind wie die Unternehmen der Schweizer MEM-Branche. Zudem haben die angegriffenen Unternehmen der Schweizer Logistikbranche ihre IT-Sicherheitsmassnahmen nach den Angriffen nochmals deutlich verbessert. Abschliessend wird empfohlen, das Thema Cybersicherheit auf Geschäftsleitungsebene in einem zentralen Risikomanagement zu verankern und dem Faktor Mensch künftig noch mehr Beachtung zu schenken. Insbesondere auf künstlicher Intelligenz basierende Cyberangriffe sind immer schwieriger zu erkennen und entsprechende Sensibilisierungsmassnahmen der Mitarbeitenden für die Cybersicherheit von Unternehmen deshalb von grösster Bedeutung.

[1] Die Bezeichnung «Schweizer Speditions- und Logistikbranche» wird nachfolgend verkürzt als «Schweizer Logistikbranche» verwendet.

[2] Die Bezeichnung «Schweizer Maschinen-, Elektro- und Metallindustrie» wird nachfolgend verkürzt als «Schweizer MEM-Branche» verwendet.

Inhaltsverzeichnis

1. Einführung

Russlands Krieg in der Ukraine führt seit Februar 2022 dazu, dass Aktivitäten von Hackern und der Einsatz von Malware zunehmen. Es zeigt sich eine verstärkte Zusammenarbeit zwischen cyberkriminellen Gruppen und Trickbot-Banden, die es auf ukrainische Organisationen abgesehen haben (Hammond et al., 2022). Dabei kann es zu Kollateralschäden kommen, da die Cyberangriffe teilweise nur schlecht kontrolliert werden können und dies zu sogenannten «Spillover-Effekten» führt (NCSC, 2022). Laut World Economic Forum (2023) belegt das Risiko «weitverbreiteter Cyberkriminalität und Cybersicherheitslücken», nach Schweregrad und auf zwei und zehn Jahre hinaus betrachtet, den Platz 8 von 32 der grössten globalen Risiken. In einer aktuellen Umfrage von Cisco geben fast 60% der Teilnehmenden an, dass sie in den letzten 12 Monaten einen Vorfall im Bereich der Cybersicherheit erlebt haben (Cisco, 2023). IBM zeigt im «IBM Security X-Force Threat Intelligence Index 2023» auf, dass die häufigste Angriffsart auf Unternehmen mit 27% der Fälle im Jahr 2022 die Erpressung war. Die Angriffe ereigneten sich zu 25 % in der Fertigungsindustrie, zu 9% im Handel und zu 4% in der Transportindustrie. Dabei war «Phishing» der führende Angriffsvektor, der in 41% der Fälle identifiziert werden konnte. Cyberangriffe v.a. mit Erpressungen sind so präsent wie noch nie und die Schwachstelle oft die Mitarbeitenden (Worley et al., 2023).

Während kommerzielle Organisationen, wie z.B. Anbieter von IT-Sicherheitsmassnahmen, regelmässig Berichte publizieren, gibt es im deutschsprachigen Raum auch zunehmend akademische Literatur zur Betroffenheit von Unternehmen (Dreißigacker et al., 2020). Diese zeichnet sich jedoch durch eine grosse Heterogenität aus und ist nur bedingt auf die Schweiz anwendbar. In Deutschland wurden umfangreiche Querschnittstudien (Barth et al., 2020; Dreißigacker et al., 2020, 2021) zur Betroffenheit der Unternehmen von Cyberangriffen durchgeführt. In der Schweiz wurden nur wenige vergleichbare Studien durchgeführt, so in der MEM-Industrie (Isenhardt et al., 2022), für Organisationen im Sozialbereich (Baier et al., 2022) und zu den Themen Digitalisierung, Home-Office und Cyber-Sicherheit in KMU (Peter et al., 2020). Barth et al. (2020) zeigt, dass die höchsten durchschnittlichen Schadenssummen je Unternehmen absteigend in den Branchen Chemie & Pharma, Maschinenbau und Automobil verursacht wurden. Sarder & Haschak (2019) stuft die Betroffenheit der Fertigungsindustrie, des Handels und des Logistiksektors tiefer ein als jene des Finanzsektors, jedoch höher als jene des

Bildungswesens. Cyberangriffe bedrohen Betriebe weltweit und sind unterdessen zu einem beträchtlichen Risikofaktor auch für die Schweizer Logistikbranche geworden. Die Betroffenheit von Cyberangriffen wurde jedoch in dieser Branche bisher in der Schweiz nicht systematisch untersucht.

Viele Speditions- und Logistikunternehmen haben bereits wirkungsvolle IT-Sicherheitsmassnahmen umgesetzt. Doch wie ist die Branche als Ganzes und insbesondere im Vergleich zur MEM-Branche aufgestellt? Daraus abgeleitet stellen sich im Rahmen dieser Arbeit folgende Forschungsfragen:

a) *Wie stellt sich die aktuelle Situation in Bezug auf Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche im Vergleich zur MEM-Branche dar?*

b) *Auf welche Cyberangriffsarten mussten Unternehmen der Schweizer Speditions- und Logistikbranche in den letzten 24 Monaten reagieren?*

c) *Welche IT-Sicherheitsmassnahmen wurden in Unternehmen der Schweizer Speditions- und Logistikbranche getroffen?*

In Anlehnung an Dreißigacker et al. (2020, 2021) und Isenhardt et al. (2022) wurde im Zeitraum Februar bis März 2023 eine quantitative Querschnittanalyse in Form einer Online-Umfrage zur Cyberkriminalität und IT-Sicherheitsmassnahmen in der Schweizer Logistikbranche durchgeführt. Die Stichprobe ist aufgrund der geringen Anzahl Teilnehmenden zwar nicht repräsentativ, dennoch zeigt das Resultat eine gute Momentaufnahme der Branche.

Vorliegende Arbeit beginnt mit einer Analyse der jüngsten Literatur, stellt dann die Ergebnisse der vorgenommenen Online-Umfrage in der Logistikbranche vor und vergleicht diese anschliessend mit den Daten der Umfrage von Dreißigacker et al. (2021) zur deutschen Logistik- und MEM-Branche sowie der Umfrage von Isenhardt et al. (2022), zur Schweizer MEM-Branche. Die daraus gewonnenen Erkenntnisse werden in einem Fachgespräch mit einer Expertin und mehreren Experten reflektiert und anschliessend Empfehlungen für die Logistikbrache formuliert.

2. Related Work

2.1 Literaturrecherche

Die Methodik der Literaturrecherche wird in Kapitel 3.1 beschrieben.

2.1.1 Definition des Themenbereichs

Hauptforschungsfragen

a) *Wie stellt sich die aktuelle Situation in Bezug auf Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche im Vergleich zur MEM-Branche dar?*

b) *Auf welche Cyberangriffsarten mussten Unternehmen der Schweizer Speditions- und Logistikbranche in den letzten 24 Monaten reagieren?*

c) *Welche IT-Sicherheitsmassnahmen wurden in Unternehmen der Schweizer Speditions- und Logistikbranche getroffen?*

Nebenforschungsfragen

- *Gibt es Unterschiede in Bezug auf Cyberangriffsarten und IT-Sicherheitsmassnahmen zwischen…*
  - *der deutschen Logistik- und MEM-Branche?*
  - *der Schweizer und der deutschen MEM-Branche?*
  - *der Schweizer und der deutschen Logistikbranche?*
  - *der Schweizer Logistik- und MEM-Branche?*

2.1.2 Konzeptualisierung des Themas

In Anlehnung an Cooper (1988) wurde die Literaturrecherche in Tabelle 1 charakterisiert, wobei die Zielgruppe dieser Arbeit allgemeine Wissenschaftler:innen und Praktiker:innen sind. Mit diesem Fokus wurde der nächste Schritt geplant und durchgeführt.

Nr.	Charakteristik	Kategorien			
1	**Fokus**	Forschungsergebnisse	Forschungsmethoden	Theorien	Anwendungen
2	**Ziel**	Integration	Kritik	Zentrale Fragen	
3	**Organisation**	historisch	konzeptuell	methodologisch	
4	**Perspektive**	neutrale Darstellung	Befürwortung der Position		
5	**Zielgruppe**	Spezialisierte Wissenschaftler	Allgemeine Wissenschaftler:innen	Praktiker:innen, Politiker:innen	Öffentlichkeit
6	**Abdeckung**	vollständig	umfassend & ausgewählt	repräsentativ	zentral

Tabelle 1: Taxonomie der Literaturrecherche (Cooper, 1988)

2.1.3 Datenbanksuche

Zur Vorbereitung der Literaturrecherche wurden die relevanten Fachbegriffe in Deutsch und Englisch mit Hilfe einer Wortfeldanalyse eruiert (Perathoner & Burch, 2021) und in Tabelle 2 dargestellt.

Kernbegriff	cyber crime	cyber security	survey	company
Synonyme	online crime, *Internetkriminalität*	it security, *IT Sicherheit, Cyber Sicherheit*	investigation, *Umfrage, Studie*	enterprise, firm, *Firma, Unternehmen*
Oberbegriffe	cyber war	risk management	research, *Forschung*	corporate
Unterbegriffe	ransom ware, malware, hacker	firewall, backup	quantitative, qualitative	
Verwandte Begriffe	cyber threat, cyber attack, *Internetangriff*	cyber defence, *Gegenmassnahme*, *Cyber Verteidigung*, cyber resilience, *Resilienz*		

Tabelle 2: Wortfeld (Perathoner & Burch, 2021)

Für die Datenbanksuche wurden die Datenbanken Business Source Premier, ProQuest / EconLit, Clarivate / Web of Science und Swisscovery verwendet. Es wurden viele englische Suchbegriffe verwendet, da Publikationen in diesem Themenbereich primär auf Englisch verfasst sind. Am 28.01.2023 ergab die Vorwärtssuche 70 Artikel, die weiter analysiert wurden (siehe Tabelle 3).

		Anzahl Suchresultate am 28.01.2023			
	Datenbanken	**Business Source Premier**	**ProQuest / EconLit**	**Clarivate / Web of Science**	**Swisscovery**
	Allgemeine Filter	Academic Journals	Wissenschaftliche Zeitschriften	Highly Cited Papers	Artikel: Online verfügbar; Thema: Cybersecurity; Sprache: Englisch, Deutsch
Suchbegriffe 1 *	cyber crime OR online crime OR Internetkriminalität OR cyber threat OR cyber attack OR Internetangriff	4'209	186	229	2'222
Suchbegriffe 2 *	cyber security OR it security OR IT Sicherheit OR cyber defence OR Cyber Verteidigung	14'156	15'560	1'467	4'158
Suchbegriffe 3 *	survey OR investigation OR research OR Umfrage OR Forschung	1'219'579	269'664	147'410	2'652
Suchbegriffe 4 *	company OR enterprise OR firm OR Firma OR Unternehmen	544'149	269'991	13'043	552
Schnittmenge 1	1 AND 2	1'830	90	165	2'220
Schnittmenge 2	1 AND 2 AND 3	603	23	141	1'617
Schnittmenge 3	1 AND 2 AND 3 AND 4	124	5	4	225
Publikationstyp	Peer-Reviewed Journals	122	5	31	190
Zeitraum	2018-2023	60	3	4	149
	2020-2023	43	1	2	116
	2022-2023	23	1	1	45
* Alle Felder	**ohne Duplikate** (Export in Zotero)	20	3	4	43
		80	Betrachtungsumfang	**70**	total untersuchte Artikel

Tabelle 3: Datenbanksuche

Die Rückwärtssuche basierte auf der aktuellen Studie von Isenhardt (2022) und Artikel die im Internet zum Thema gefunden wurden. So konnten weitere 27 Artikel mit einer Relevanz für die bevorstehende Online-Umfrage identifiziert und zur Analyse hinzugefügt werden[3].

2.1.4 Analyse und Synthese

Die Literatur konnte hinsichtlich der Autoren- und Herausgeberschaften in folgende drei Kategorien eingeteilt werden (Dreißigacker et al., 2021):

a) *behördliche, politiknahe und andere nicht-kommerzielle Institutionen*

b) *kommerzielle bzw. unternehmerische Organisationen*

c) *akademische Forschungseinrichtungen*

Die eigentliche Literaturanalyse und -synthese folgt in den Kapiteln 2.2 bis Kapitel 2.5.

[3] In der Datei «20230430 Literaturrecherche.xlsx» ist eine Übersicht aller Artikel (mit Kommentaren und einer Klassifizierung) zu finden.

2.1.5 Forschungsagenda und Forschungsstand

Die Literaturrecherche zeigte, welche Schwerpunkte die Online-Umfrage haben soll und welche Fragen aktuell relevant sind. Es wurden die allgemeine Bedrohungslage sowie die technischen und organisatorischen Schwerpunkte der Forschung in den letzten 12 Monaten untersucht. Ziel dieser Analyse war es, einen Überblick zu gewinnen, um die Fragekataloge der Umfragen von Dreißigacker et al. (2021) und Isenhardt et al. (2022) für die eigene empirische Befragung einzugrenzen, zu aktualisieren oder zu modifizieren.

Der Stand der Literatur zum Thema «Cyberangriffe gegen Unternehmen» ist sehr dynamisch: Einerseits ist das Thema hoch aktuell, andererseits ändert sich die Bedrohungslage andauernd. So weisen die empirischen quantitativen Studien eine grosse Heterogenität in Bezug auf ihren Forschungsschwerpunkt auf und unterscheiden sich stark in den Bereichen Methodik, Stichprobe, Operationalisierung und Ergebnisdarstellung, sodass eine Gegenüberstellung der Forschungsresultate nur sehr eingeschränkt möglich ist (Dreißigacker et al., 2020). Die empirischen Untersuchungen in Deutschland und der Schweiz fokussieren stark auf die Betroffenheit der Unternehmen und deren IT-Sicherheitsmassnahmen.

2.2 Allgemeine Bedrohungslage

2.2.1 Häufigkeit von Cyberangriffen und Risikoeinschätzung

Eine repräsentative Studie aus dem Jahre 2005 (Rantala, 2005) zeigte bereits, dass über alle Branchen und Angriffsarten 67% der befragten Unternehmen 2005 mindestens einmal Opfer von Cyberangriffen geworden sind. Dacorogna (2022) stuft das aktuelle Cyberrisiko aufgrund der COVID-19 Pandemie und dem Krieg in der Ukraine so hoch ein wie noch nie in den letzten 30 Jahren.

Das britische Versicherungsunternehmen Hiscox meldete 2021 eine Zunahme von Unternehmen, die in den letzten 12 Monaten eine Cyberattacke gemeldet haben, von 38% auf 43% (Hiscox, 2021) und 2022 eine Zunahme in der gleichen Kategorie von 43% auf 48% (Hiscox, 2022b). Inwiefern die Angriffe auch erfolgreich gewesen sind, beantworten diese beiden Studien nicht. Bitcom berichtete, dass 2019 in Deutschland mindestens 75% aller Unternehmen in den letzten 24 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren. Die gleiche Umfrage ergab 2015 einen Wert von lediglich

51%. Der Anteil digitaler Angriffe war 2017 erst 43% und 2019 bereits 70% (Barth et al., 2020).

Das World Economic Forum befragte im Zeitraum vom 07.09.2022 bis 05.10.2022 über 1'200 Expertinnen und Experten aus Wissenschaft, Wirtschaft, Regierung, internationaler Gemeinschaft und Zivilgesellschaft zu ihrer Wahrnehmung globaler Risiken. Dabei wurden 32 globale Risiken nach ihren wahrscheinlichen Auswirkungen (Schweregrad) über einen Zeitraum von 2 und 10 Jahren eingeschätzt. Das Risiko «weitverbreiteter Cyberkriminalität und Cybersicherheitslücken», belegte in beiden Betrachtungszeiträumen den achten Platz (World Economic Forum, 2023).

2.2.2 Geografische Unterschiede

IBM berichtet (Worley et al., 2023), dass 2022 der asiatisch-pazifische Raum bereits zum zweiten Jahr in Folge, die am häufigsten angegriffene Region ist. Auf sie entfallen 31% der Vorfälle, die durch IBM registriert werden konnten. Europa folgt mit 28% und Nordamerika mit 25% der Vorfälle. Im Vergleich zu 2021 sind die Regionen Asien-Pazifik und Europa um fünf bzw. vier Prozentpunkte gestiegen. Gleichzeitig sank der Anteil in der Region Naher Osten von 14 % auf 4 %. In der Region Asien-Pazifik war das verarbeitende Gewerbe mit 48 % der Fälle der am häufigsten angegriffene Wirtschaftszweig. In Europa war das Vereinigte Königreich mit 43 % der Fälle das am häufigsten angegriffene Land. In Nordamerika waren Energieunternehmen mit 20 % der Fälle die am häufigsten angegriffenen Unternehmen. In Lateinamerika entfielen 67 % der registrierten Angriffe auf Brasilien. Der häufigste Angriff im Nahen Osten und Afrika war mit 27 % der Fälle der Einsatz von Backdoors.

2.2.3 Einfluss des Krieges in der Ukraine

Der militärische Angriff Russlands auf die Ukraine im Februar 2022 wurde von Cyberangriffen auf kritische Infrastrukturen begleitet. So wurden in den ersten Tagen des Konflikts sechs verschiedene Malware-Stränge gegen kritische Infrastruktur in der Ukraine eingesetzt, die das Ziel verfolgten, die Daten zu löschen. Diese hochentwickelten Angriffe wurden staatlichen Akteuren zugeschrieben (NCSC, 2022). Als Reaktion auf die Cyberangriffe hat die ukrainische Regierung die «IT Army of Ukraine» ausgerufen, die u.a. mit (D)DoS-Angriffen russische Online-Ressourcen angriff (NCSC, 2022). Der Krieg in der Ukraine hat in der ganzen Welt Ressourcen mobilisiert, die sich gegen

Russland gerichtet haben. So deklarierte z.B. das internationale Hackerkollektiv Anonymous am 24.02.2022, dass es sich nun offiziell im Cyber-Krieg gegen die russische Regierung befindet (Milmo, 2022). Es wurde festgestellt, dass russische Cyberattacken oft in enger Abstimmung mit Militäraktionen durchgeführt wurden (Lella et al., 2022). Bei allen Angriffen kann es zu Kollateralschäden kommen, da die Cyberangriffe teilweise nur schlecht kontrolliert werden können und dies zu sogenannten «Spillover-Effekten» führt (NCSC, 2022). Trotzdem sind grossflächige und schwere Angriffe, wie sie von westlichen Regierungen befürchtet worden waren, bisher ausgeblieben (Worley et al., 2023).

2.2.4 Unternehmensbereiche und Wirtschaftszweige

Die Angriffe werden oft nicht als zielgerichtet eingeschätzt (Dreißigacker et al., 2020). Verschiedene Unternehmensbereiche und Wirtschaftszweige sind unterschiedlich betroffen. Folgende Unternehmensbereiche wurden 2019 in Deutschland in absteigender Häufigkeit Opfer von Sabotage, Spionage und Datendiebstahl (Barth et al., 2020):

- *Marketing und Vertrieb 33%*
- *Lager und Logistik 28%*
- *Personalwesen und Human Resources 27%*
- *IT (Administration oder Service) 27%*
- *Geschäftsführung und Management 26%*
- *Produktion und Fertigung 25%*
- *Finanz- und Rechnungswesen 23%*
- *Einkauf 16%*
- *Forschung und Entwicklung 15%*
- *Weiss nicht / Keine Angabe 11%*

Die Betroffenheit der Wirtschaftszweige zeigte 2022, dass sich 25 % in der Fertigungsindustrie, 9% im Handel und 4% der Angriffe in der Transportindustrie ereigneten. Im Jahr 2018 ereigneten sich in der Fertigungsindustrie 10 %, im Handel 11% und in der Transportindustrie 13% der Angriffe. Die Fertigungsindustrie registrierte somit eine Steigerung von 15% auf 25 %, während Handel und Transportindustrie 2022 weniger

angegriffen wurden als vier Jahre zuvor. Diese von IBM X-Force im Transportsektor erfassten Vorfälle werden folgendermassen in beschrieben:

> *Down from seventh place in 2021, transportation returned to its 2020 ranking of ninth place. However, the industry still comprised roughly the same percentage of incidents to which X-Force responded. Phishing was the most common initial access vector in 51% of cases - evenly split between links, attachments and spear phishing as a service. Abuse of valid local accounts made up 33% of initial access vectors, with valid cloud accounts serving as the entry point for 17% of cases. The top actions on objectives were server access and deployment of remote access tools at 25% each, followed by spam campaigns, ransomware, backdoors and defacement in 13% of cases each. Data theft was most common in 50% of cases, with extortion and impacts to brand reputation at 25% each. European transportation entities were the most targeted group, comprising 62% of cases, with Asia-Pacific in second place at just over 37%. (Worley et al., 2023, S. 51)*

Sarder & Haschak (2019) stuften die Betroffenheit der Fertigungsindustrie, des Handels und des Logistiksektors tiefer ein als jene des Finanzsektors, jedoch höher als jene des Bildungswesens, der Kommunikation und der Gastronomie. Die Wirtschaftsbereiche Maschinenbau, Industrie und Pharma wurden 2020 in Bezug auf Wirtschaftsspionage als «hoch gefährdet» eingestuft, während Handel, Verkehr & Lagerei als «durchschnittlich» bis «sehr gering» eingestuft werden (Zwahlen et al., 2020).

2.2.5 Fokus auf kleinere und mittlere Unternehmen (KMU)

Von kleineren und mittleren Unternehmen (KMU) spricht man in der Schweiz, wenn ein Unternehmen weniger als 250 Arbeitskräfte beschäftigt. In der Schweiz sind das 99.7% aller Unternehmen (NCSC, 2023). In Deutschland werden 99.4% der Unternehmen als KMU klassifiziert (Statistisches Bundesamt, 2023). Das Nationale Zentrum für Cybersicherheit (NCSC) fokussierte deshalb im letzten Halbjahresbericht explizit auf die Situation der KMU (NCSC, 2023) und wies darauf hin, dass KMU oft nicht die Möglichkeiten haben, eigene Sicherheitsabteilungen aufzubauen und auch in den

Unternehmensleitungen nicht ausreichend Wissen vorhanden ist. Eine Einbindung der der Cyberrisiken in ein zentrales Risikomanagement wird generell empfohlen. Kleinunternehmen (10-99 Mitarbeitende) sind besonders gefährdet, angegriffen zu werden, da sie oft in Lieferketten von Grossunternehmen eingebunden sind und entweder über Spezialwissen verfügen oder als Einfallstore für die Grossunternehmen gesehen werden. Die Angriffe stiegen in dieser Unternehmensgrössenklasse von 2015 (47%) bis 2019 (75%) um 28% an (Barth et al., 2020).

2.2.6 Angriffsarten

Verma & Shri (2022) untersuchten 324 Artikel zwischen 2011 und 2021 und kamen zum Schluss, dass die am häufigsten auftretenden Cyberangriffe in Unternehmen «Malware», «Phishing», «(D)DoS-Angriffe», «IoT-Angriffe» und neu erkannte «SQL-Angriffe» waren. Laut Worley et al. (2023) war 2022 Erpressung mit 27% der Fälle die häufigste Angriffsart auf Unternehmen. Dabei war «Phishing» der führende Angriffsvektor, der in 41% der Fälle identifiziert werden konnte. Die Versicherung Hiscox stuft sogar 62% der Angriffsvektoren als «Phishing E-Mails» ein und meldet, dass nur 59 % der Unternehmen, die ein Lösegeld gezahlt haben, alle Daten wiederherstellen konnten (Hiscox, 2022a). Die Studie von Dreißigacker (2020), eine CATI-Befragung von 5’000 Unternehmen mit mindestens zehn Beschäftigten und mit Sitz in Deutschland, zeigte ein ähnliches Bild:

- *Phishing 22%*
- *Sonstige Schadsoftware 21.3%*
- *Ransomware 12.5%*
- *Spyware 11.3%*
- *CEO-Fraud 8.1%*
- *(D)DoS-Angriffe 6.4%*
- *Defacing-Angriffe 3.1%*
- *Manuelles Hacking 2.8%*

Es ist anzumerken, dass der Angriffsvektor «Phishing» z.B. zur Erpressung durch Ransomware oder Spionageaktivitäten mittels «Spyware» führen kann und immer in

Kombination zu betrachten ist. Die Untersuchung der Schweizer MEM-Industrie (Isenhardt et al., 2022) zeigt ein ähnliches Bild in Bezug auf Angriffe in den letzten 12 Monaten, wobei «CEO-Fraud» die Aufzählung der Angriffsarten vor «Phishing» anführt:

- *CEO-Fraud 49.8%*
- *Phishing 43.1%*
- *Sonstige Schadsoftware 20.7%*
- *Hackerangriff 17.1%*
- *Sonstiges Social Engineering 16.2%*
- *(D)DoS-Attacke 11.5%*
- *Ransomware-Angriffe 11.3%*
- *Abhören oder Abfangen digitaler Kommunikation 8.4%.*

2.3 Technische Schwerpunkte

2.3.1 Einsatz künstlicher Intelligenz

In diesem Kapitel wird aufgezeigt, wie mit Hilfe künstlicher Intelligenz die IT-Sicherheitsmassnahmen verbessert werden können. Auf die Tatsache, dass auch Angreifer diese Technologie nutzen, um ihre Attacken effektiver zu machen (Korolov, 2022), wird hier nicht näher eingegangen.

Anomalie-Detektion

Cyberangriffe gegen Unternehmen können auch sich auch gegen die Infrastruktur auf Steuerungsebene richten. Mit zunehmender Verbreitung von Internet-of-Things-Technologien (IoT) und vernetzter Sensoren und Aktoren werden industrielle speicherprogrammierbare Steuerungen (SPS) in Unternehmen angreifbar. Dabei ist die kritische Infrastruktur sowie die Energie- und Wasserversorgung speziell schützenswert. Unternehmen kritischer Branchen haben zunehmend ein Notfallmanagement etabliert (Barth et al., 2020), stehen jedoch im Fokus der Angreifenden. Um Unregelmässigkeiten auf Steuerungsebene festzustellen, was aufgrund der proprietären Architektur der SPS schwierig ist, wird künstliche Intelligenz eingesetzt. So zeigte der Einsatz eines neuronalen Netzwerkes mit Ein-Klassen-Klassifizierung, dass sich diese Technik eignet, um Unregelmässigkeiten in SPS zu ermitteln (Aboah Boateng et al., 2022).

Machine Learning kann auch dazu eingesetzt werden, (D)DoS-Attacken in cyber-physischen Produktionssystemen zu detektieren. Saghezchi et al. (2022) verwendeten dabei «semi-supervised», «unsupervised», und «supervised» Lernalgorithmen, wobei die «supervised» Lernalgorithmen «Decision Tree», «Random Forest» und «K-Nearest Neigbour» mit 99.9% Genauigkeit die besten Resultate zeigen. Die zwei «unsupervised» Lernalgorithmen «K-Means» und «Erwartungs-Maximierung» zeigten jedoch auch eine Genauigkeit von 95%, was für zukünftige Anwendungen sehr interessant sein kann, da kein vorgängiges Labeling der Daten vorgenommen werden muss.

Detektion von Malware

Deep-Learning-Techniken können genutzt werden, um Malware-Code zu erkennen und zu klassifizieren. Dazu wird der Code der ausführbaren exe-Dateien in 8-bit Graustufenbilder umgewandelt und diese mittels Techniken zur Datenerweiterung bearbeitet (z.B. Drehen von Bildern mit verschiedenen Winkeln, horizontales und vertikales Spiegeln und Zoomen). Diese Bilder können dann in eine mehrstufiges Deep-Learning-Modell eingespeist werden («Convolutional Neural Network», Typ VGG-16), um in der ersten Stufe zu erkennen, ob es sich dabei um Malware handelt und um sie in einer zweiten Stufe noch in Kategorien zu klassifizieren (Alzahrani et al., 2022).

Auch Yadav et al. (2022) bestätigen mit ihrem Vergleich von 26 vortrainierten Convolutional Neural Network-Modellen zur Erkennung von gepackter und ungepackter Android-Malware, dass diese Technik zuverlässig funktioniert.

Erkennung bösartiger Websites oder Chatbots

Bösartige Websites, die z.B. Zugangsdaten sammeln, können oft nicht einfach von ihren gutartigen Gegenstücken unterschieden werden. Chaiban at al. (2022) untersuchten, wie maschinelles Lernen die Merkmale von Websites auswerten kann, um zu erkennen, ob die Seite bösartig ist. Sie verwendeten dazu neuronale Netze des Typs Transformer und stellten fest, dass die URL-Einbettung für das «XGBoost-Model» das Merkmal mit dem grössten Einfluss ist. Erstaunlicherweise waren inhaltsbezogene Merkmale wie HTLM oder JavaScript nicht unter den Top 10-Merkmalen.

Die Bekämpfung von Social Engineering als Bestandteil von Cyberattacken hat unterschiedliche Aspekte (Washo, 2021), wobei das Chat-basierte Social-Engineering (CSE) durch Einsatz von maschinellem Lernen erkannt werden kann. Tsinganos et al. (2022) zeigten, dass mit einem vortrainierten BERT-Modell persistentes Verhalten, als

Auslöser für erfolgreiche Chat-basierte Social-Engineering-Angriffe, erkannt werden kann.

2.3.2 Cyber Threat Intelligence

Asymmetrie zwischen Täter und Opfer

Es besteht eine Asymmetrie zwischen Unternehmen, die die Best-Practice-Cybersicherheitsstandards der Branche vollständig einhalten und organisierten Einheiten, wie Verbrechersyndikate und paramilitärische Kräfte, die die Cyberangriffe ausführen. Die Unternehmen können, mit den ihnen zur Verfügung stehenden Ressourcen, solchen Cyberangriffen im militärischen Stil nicht standhalten. Ein Weg, dieser immer grösser werdenden Asymmetrie zu begegnen, ist der Austausch von Cyber-Bedrohungsdaten, die sogenannte «Cyber Threat Intelligence» (CTI), um die Cyber-Abwehr besser zu steuern (Kotsias et al., 2022).

Datenaustausch

Unternehmen, die von Cyberattacken getroffen wurden, kommunizieren dies oft gar nicht und falls doch, verwenden sie oft Standardformulierungen zur Beschreibung des Vorfalls. Die Allgemeinheit erfährt also keinen Erkenntnisgewinn. Eine Befragung von Geschäftsführer:innen Schweizer KMU hat schon 2017 aufgezeigt, dass eine Mehrheit eine gesetzliche Meldepflicht befürwortet, sofern sie einfach durchführbar wäre, die Anonymität der Unternehmen gewahrt würde und ein Mehrwert für die KMU im Sinne erhöhter Cybersicherheit entstünde (Mändli & Repic, 2017). Unterdessen hat die U.S. Securities and Exchange Commission (SEC) Vorschriften und Richtlinien angepasst (Peng & Chang-Wei Li, 2022). Auch in der Schweiz wurde Ende 2022 eine Botschaft verabschiedet, um zumindest Unternehmen mit kritischer Infrastruktur dazu zu verpflichten, ihre Cyberangriffe zu melden (Botschaft zur Änderung des Informationssicherheitsgesetzes, 2022). Ziel ist es, Informationen zu generieren, welche vom NCSC genutzt werden können. Datenaustausch und Meldepflicht erleichtern es sowohl staatlichen Stellen, als auch Unternehmen, die Cyberangriffe besser zu verstehen und sich koordiniert dagegen zu schützen. Gleichzeitig ermöglicht der Datenaustausch der Versicherungsbranche die Risiken zu verstehen und zu kalkulieren (Cremer et al., 2022), aber auch die Angriffe dahingehend quantitativ auszuwerten, um Anreize für Unternehmen zu schaffen, sich besser zu schützen (Palsson et al., 2020). Aufgrund der

Aktualität des Themas, wurde die Frage nach dem Einsatz von Cyber Threat Intelligence, und inwiefern die Vorfälle gemeldet wurden, in die Online-Umfrage für diese Masterarbeit aufgenommen (vgl. Kapitel 2.5.3).

2.3.3 Integrität der Lieferkette

Nachfolgendes Zitat von ICTswitzerland gibt einen guten Überblick zum Thema Integrität der Lieferkette:

> *Bei einem Angriff über die Lieferkette werden Komponenten bereits vor der Lieferung an den Endabnehmer kompromittiert oder manipuliert. Dies kann bereits im Design und bei der Entwicklung von Chips, bei der Herstellung oder Integration von Komponenten oder während dem Transport zum Endabnehmer geschehen. Die Manipulation während des Betriebs, z.B. durch Lieferung einer kompromittierten Firmware, muss ebenfalls berücksichtigt werden. Die Integrität digitaler Lieferobjekte ist insbesondere durch nicht dokumentierte Zugänge und Backdoors oder implantierte Fehlfunktionen gefährdet. (Frei et al., 2019, S. 11)*

Integrität der Hardware

Heutige ICT-Hardware wird global und kostengünstig von unzähligen Unternehmen hergestellt, was es einem Unternehmen erschwert, die ganze Supply Chain zu überwachen und aufgrund der komplexen Technologie fast verunmöglicht, die Komponenten vor dem Gebrauch auf ihre Integrität zu überprüfen. Das «National Institute of Standards and Technology» (NIST) hat dazu eine umfassende Publikation veröffentlicht (Boyens et al., 2022), in der die Initiative zur Verbesserung des Cyber Supply Chain Risk Management (C-SCRM) vorgestellt wird. Es wird ein Ansatz präsentiert, wie die Original-Geräte-Hersteller (OEM) jedem Gerät ein Artefakt mitgeben können, das die Attribute des Gerätes mit der Identität des Gerätes verbindet, sodass die Anwendenden vor dem Einsatz der Hardware einerseits die Quelle und Authentizität des Artefakts überprüfen und andererseits die im Artefakt gespeicherten Attribute mit den tatsächlichen Attributen des Geräts abgleichen kann. Diese Überprüfung soll dann auch im laufenden Betrieb durchgeführt werden können, um die Integrität der Hardware über die ganze Betriebsdauer hinweg sicherzustellen.

Integrität der Software

Software-Supply-Chains sind komplex und oft wissen die Unternehmen nur beschränkt, welche Software-Komponenten in ihrer Software verbaut sind. Ende 2020 wurde entdeckt, dass das Netzwerkverwaltungssystem Orion von SolarWinds kompromittiert wurde. Angreifer haben sich Zugang zum Netzwerk von SolarWinds verschafft und über längere Zeit Informationen sammeln können. Anschliessend wurde eine Schadprogramm in den Erstellungsprozess von Orion eingeschleust. Die kompromittierte Software wurde dann von den Kunden heruntergeladen und installiert (Lella et al., 2021). Die EU bezweckt mit dem «Cyber Resilience Act» (CSA), die Transparenz zu erhöhen, indem u.a. die Softwarelieferanten eine Software-Inventarliste («Software Bill of Materials», SBOM) erstellen und zu Verfügung stellen müssen, damit Unternehmen bei einem Vorfall abschätzen können, welche Softwareteile betroffen sind. Eine SBOM sollte den Unternehmen auch ermöglichen, ihre Supply-Chain-Risiken besser einzuschätzen (European Commission, 2022).

2.4 Organisatorische Schwerpunkte

Gartners «Top Trends in Cybersecurity» empfehlen zwei Jahre in Folge (Firstbrook et al., 2022; Addiscott et al., 2023), dass dem Faktor Mensch besondere Aufmerksamkeit geschenkt werden sollte, um die Cybersicherheit der Unternehmen zu erhöhen.

2.4.1 Bedrohungen durch Insider

Bedrohungen durch «Insider Threats» stellen eine immanente und in Unternehmen oft nicht ausreichend beachtete Bedrohung der Cybersicherheit dar (Georgiadou et al., 2022). Bedrohungen für die Cybersicherheit nehmen zu, wobei eine Mehrheit von Insidern ausgehen. Diese befinden sich oft hinter den Sicherheitsschutzmechanismen der Unternehmen und haben oft privilegierten Zugang zum Netzwerk. Machine Learning kann Muster im Verhalten erkennen und Hinweise auf Bedrohungen geben (Liu et al., 2018). Mitarbeitende, die sich persönlich für Cybersicherheit einsetzen, sind weniger anfällig für Cybersecurity-Fehlverhalten. Deshalb kann das Management einer Unternehmung Rahmenbedingungen schaffen, die dieses Verhalten fördern und so die Bedrohung durch Insider reduzieren (Silaule et al., 2022).

2.4.2 Nutzen von Präventionskampagnen

Es besteht ein deutliches Forschungsdefizit in Bezug auf die Wirksamkeit politischer Initiativen und Präventionskampagnen zur Verhütung von Internetkriminalität (Brewer et al., 2019). In Grossbritannien wurde allerdings untersucht, ob es wahrscheinlicher ist, dass Unternehmen, die über die Kampagnen der britischen Regierung zur Cybersicherheit informiert sind, die empfohlenen Cybersicherheitsmassnahmen umsetzen und ob Unternehmen, die die von der britischen Regierung empfohlenen Sicherheitsmassnahmen umgesetzt haben, seltener Opfer von Cyberkriminalität werden. Dabei wurde festgestellt, dass das Bewusstsein der Cybersicherheitsmassnahmen bei Unternehmen zu einer Umsetzung der Cybersicherheitsmassnahmen führt, dies jedoch keinen nachweisbaren Einfluss auf die Wahrscheinlichkeit hat, Opfer eines Cyberangriffes zu werden bzw. negative Konsequenzen daraus zu erleiden (Kemp, 2023).

2.4.3 Rolle des Managements

Cybersicherheit ist aufgrund der fortschreitenden Digitalisierung ein strategisch relevantes Thema für Unternehmensleitungen. Die Cybersicherheitsbereitschaft ist jedoch unterschiedlich. Cisco schätzt, dass nur 15% der Unternehmen weltweit gut auf Sicherheitsrisiken vorbereitet sind. Gleichzeitig äussern 82% der dafür Verantwortlichen, dass Vorfälle im Bereich der Cybersicherheit ihr Unternehmen in den nächsten 12 bis 24 Monaten wahrscheinlich beeinträchtigen werden (Cisco, 2023). 40% der Top-Führungskräfte geben an, nicht beurteilen zu können, wie stark die Cyberabwehr ihres Unternehmens ist und wie auf Cyberangriffe reagiert werden soll (Sweeney, 2016). Der Leitgedanke «Cybersicherheit ist Chefsache» wird von den Unternehmen nur ungenügend umgesetzt (Pawlowska & Scherer, 2021).

In Anbetracht dessen, dass Unternehmensleitungen oft mit Mitarbeitenden höheren Alters besetzt sind, ist die Untersuchung von Geil et al. (2018) aufschlussreich, in der eine Bewertung der Cybersicherheitspraktiken im Agrarsektor der Vereinigten Staaten vorgenommen wurde. Es konnte festgestellt werden, dass die wahrgenommene Anfälligkeit auf Cyberangriffe und der wahrgenommene Nutzen von IT-Sicherheitsmassnahmen wichtige Faktoren für deren Einführung sind. Es wurde untersucht, ob Alter, Geschlecht und Bildung einen Einfluss auf die wahrgenommene Gefährdung durch Cyberangriffe haben. Es konnte aufgezeigt werden, dass lediglich das Alter einen Einfluss auf die Wahrnehmung hat.

Nicht nur Grossunternehmen sind betroffen, sondern auch KMU. Die Unternehmensleitungen sollten sich mit dem Thema auseinandersetzen, tun es aber nur ungenügend. Die Untersuchung dieses Phänomens bei Schweizer KMU zeigte, dass das Management einer Organisation ein Bewusstsein für Cybersicherheit haben muss, denn die Geschäftsleitung befindet schlussendlich über die Umsetzung der Massnahmen zur Stärkung der Cybersicherheit (Schellinger et al., 2020). Auch wenn der Einsatz von Sicherheitsstandards (z. B. ISO 2700x, NIST Cybersecurity Framework, IT-Grundschutz des BSI, etc.) den KMU helfen würde, die Cybersicherheit zu erhöhen, nutzt sie nur eine Minderheit der KMU (Hirschi & Portmann, 2017). Yigit Ozkan & Spruit (2022) erstellten deshalb ein anpassungsfähiges Framework für die Bewertung und Standardisierung des Reifegrads der Cybersicherheit, um die Lücke zwischen den spezifischen Anforderungen und Rollen von KMU im digitalen Ökosystem, den existierenden Reifegradbewertungsmodellen und den Standards zur Bewertung und Verbesserung der Cybersicherheit-Fähigkeiten zu schliessen (ASMAS: Adaptable Security Maturity Assessment and Standardization framework). KMU haben oft nicht die Ressourcen und Fähigkeiten, um eine Cybersicherheitsstruktur zu schaffen und sollten deshalb die von externen Sicherheitsdienstleistern angebotenen Services nutzen (Ullah & Nab, 2022). Schlussendlich ist für die Cybersicherheit entscheidend, dass die Mitarbeitenden für dieses Thema sensibilisiert werden, was vom Management zuerst erkannt und danach gezielt gefördert werden muss.

2.4.4 Sensibilisierung und Schulung des Personals

Die meisten Cyberangriffe starten anfänglich mit «Phishing» als Zugangsvektor, wie z.B. die Studie von IBM bei 41 % der Vorfälle zeigt (Worley et al., 2023). Doch auch bei «CEO-Fraud» und anderen «Social Engineering-Angriffen» ist der Mensch und sein Urteilsvermögen das zentrale Element. Um das Bewusstsein für die Cybersicherheit zu schaffen und die Mitarbeitenden für die Gefahren zu sensibilisieren, haben Chowdhury et al. (2022) ein didaktisches Konzept entworfen und evaluiert, das sich auf die sogenannte «personalisierte Lerntheorie» (PLT) abstützt. Diese besagt, dass die Schulungsinhalte auf die Person, basierend auf ihren Lernzielen, dem Profil des Lernenden und ihren allgemeinen Lernpräferenzen, zugeschnitten sein sollten. Text- und spielbasierte Schulungsformate eignen sich besonders gut, um Verhaltensänderungen bei Mitarbeitenden herbeizuführen. Inwiefern sich Mitarbeitende sogar selbständig

weiterbilden oder an Programmen zur Sensibilisierung für Informationssicherheit teilnehmen, hängt ebenfalls von der Vermittlungsstrategie ab. Es ist wichtig, dass diese Programme die Einstellung der Mitarbeitenden positiv beeinflussen und sie motivieren, Sicherheitspraktiken in ihre täglichen Aktivitäten einzubeziehen (Alkhazi et al., 2022). Sogar die Scrum-Methode wurde im Kontext von Cybersicherheitskursen erfolgreich eingesetzt (Nyemkova et al., 2022). Ausserdem wurde nachgewiesen, dass das Bewusstsein für Cybersicherheit die Motivation der Mitarbeitenden, sich schützend zu verhalten, positiv beeinflusst (Wong et al., 2022).

2.4.5 COVID-19 & Homeoffice

Die COVID-19-Pandemie führte weltweit zu einer verstärkten Nutzung von Homeoffice-Arbeitsplätzen. Dreißigacker et al. (2021) berichten, dass im ersten Quartal 2020 in Deutschland 68% der Unternehmen die Möglichkeiten für Homeoffice geschaffen haben. Der Anteil privat genutzter Soft- / Hardware stieg auf 31% an, dass sich in 13% der Unternehmen die wahrgenommene IT-Sicherheit verschlechterte. So trafen 20% der Unternehmen zusätzliche IT-Sicherheitsmassnahmen zur Vorkehrung. In den Schweizer KMU hat sich im ersten Lockdown (März / April 2020) die Anzahl der Mitarbeitenden, die von zu Hause arbeiteten, fast vervierfacht (Anstieg von 10% auf 38%). Nach Aufhebung der Homeoffice-Pflicht hat sich die Homeoffice-Nutzung auf hohem Niveau (Dauerhafter Anstieg von 10% auf 16%) stabilisiert (Peter et al., 2020). Die Unternehmen mussten ihre IT-Infrastruktur, IT-Sicherheitskonzepte und Richtlinien rasch der Situation anpassen. Pawlowska & Scherer (2021) haben die IT-Sicherheit im Homeoffice unter besonderer Berücksichtigung der COVID-19 Situation in Deutschland untersucht. So erhöhten 11% der Unternehmen den prozentualen Anteil ihres IT-Budget für Cybersicherheit. Auch Cyber-Kriminelle passten sich an die Pandemie-Situation an. Es traten z.B. «Phishing-E-Mails» mit vermeintlichen Corona-Informationen in Erscheinung. Die Pandemie wurde von den 32% der Kleinst- und von 67% der Grossunternehmen als Beschleuniger für ihre Digitalisierungsprojekte wahrgenommen. Dabei ist vor allem die Nutzung von Video-Konferenzsystemen stark angestiegen. Bei der Einführung neuer Systeme gaben jedoch nur 51% der Unternehmen an, die Cybersicherheit von Anfang an mitzuberücksichtigen. Wie in Kapitel 2.4.4 erwähnt, sind die Mitarbeitenden ein zentrales Element im IT-Sicherheitskonzept jedes Unternehmens. Hijji & Alam (2022) entwickelten deshalb ein Konzept, um die Cybersecurity Awareness

Trainings dem Umstand der vermehrten Homeoffice-Tätigkeit anzupassen. Dieses stellt sicher, dass die Mitarbeitenden für die jüngsten, auf «Social Engineering» basierenden Cyberangriffe und -bedrohungen sensibilisiert werden.

2.5 Empirische Studien zu Cyberangriffen gegen Unternehmen

2.5.1 Deutschland

Dreißigacker et al. (2020, 2021) untersuchten Cyberangriffe gegen Unternehmen und die dagegen getroffenen IT-Sicherheitsmassnahmen im Rahmen der Initiative «IT-Sicherheit in der Wirtschaft», die von Dezember 2017 bis März 2021 dauerte. So untersuchten sie 2020 mittels einer CATI-Befragung 5'000 Unternehmen mit mindestens zehn Beschäftigten sowie Sitz in Deutschland. Alle 687 Unternehmen, die 2020 einwilligten, an einer Folgebefragung teilzunehmen, wurden 2021 zu einer Online-Befragung eingeladen. Beide Befragungen basieren auf einer disproportional geschichteten Zufallsstichprobe. Auf Anfrage hin stellte Arne Dreißigacker die Umfragedaten dieser zwei Studien, unter Einhaltung der im Datennutzungsvertrag[4] festgehaltenen Bedingungen, für die vorliegende Masterarbeit zur Verfügung.

Seine Studien kommen zum Schluss, dass die Unternehmen vermehrt Cyberangriffe abzuwehren haben (Anstieg von Angriffen in den letzten 12 Monaten vor den Befragungen von 41.1% auf 59,6%). Dieser Anstieg ist auf die Zunahme der Prävalenzrate von «Phishing» zurückzuführen. Weiter wird festgehalten, dass die grundlegenden IT-Sicherheitsmassnahmen weit verbreitet sind, jedoch in Umfang und Reifegrad eine grosse Varianz aufweisen.

Barth et al. (2020) untersuchten im Auftrag des Digitalverbands Bitkom e.V. (wie auch bereits 2015 und 2017) den Wirtschaftsschutz Deutscher Unternehmen und erstellten einen Studienbericht, auf den in den vorhergehenden Kapitel bereits mehrmals referenziert wurde. Die repräsentative Untersuchung zeigte, dass 75% aller befragten Unternehmen in den letzten 24 Monaten vor der Befragung Opfer von Datendiebstahl, Industriespionage oder Sabotage wurden.

[4] Der Datennutzungsvertrag ist im Anhang einsehbar.

2.5.2 Schweiz

In der Schweiz registriert das NCSC sämtliche gemeldeten Vorfälle, wobei dies auch Meldungen aus der Bevölkerung sein können. Im ersten Halbjahresbericht 2022 (NCSC, 2022) wird von einem Anstieg der Meldungen von 70% (Anstieg zur Vorhalbjahresperiode von 10’234 auf 17'186 Meldungen) berichtet. Die Anzahl Meldungen im zweiten Halbjahr 2022 blieb jedoch praktisch gleich (NCSC, 2023). Dabei ist zu bedenken, dass nur erkannte Vorfälle gemeldet wurden und nicht jeder erkannte Vorfall gemeldet wird. Gemäss Isenhardt (2022) dürfte die tatsächliche Anzahl der Cyberangriffe jedoch deutlich höher liegen, da im Bereich Cybercrime davon ausgegangen wird, dass der Anteil Straftaten, die den Behörden nicht gemeldet werden, sehr gross ist. Oft wollen die Verantwortlichen einen Reputationsschaden vermeiden. Eine knappe Mehrheit (52%) der Geschäftsführer:innen von Schweizer KMU gaben 2017 auch an, Cyberangriffe aus Angst vor Reputationsschäden nicht melden zu wollen (Mändli & Repic, 2017).

Eine Untersuchung zur Cyberkriminalität gegen Organisationen im Sozialbereich (Baier et al., 2022) zeigte, dass auch hier 62.2% der befragten Institutionen in den letzten 12 Monaten vor der Befragung einen Cyberangriff erlebt haben. In Bezug auf die IT-Sicherheitsmassnahmen lautet das Fazit der Autoren:

> *Die Befunde lassen sehr allgemein ausgedrückt die Folgerung zu, dass die Organisationen hier noch aktiver werden können, insofern sie im Vergleich mit Wirtschaftsunternehmen etwas schlechter abschneiden. (Baier et al., 2022, S. 27)*

Eine Studie, die im Auftrag von Swissmem (Verband der Schweizer Maschinen-, Elektro- und Metallindustrie) durch das Institut für Strafrecht und Kriminologie der Universität Bern durchgeführt wurde (Isenhardt et al., 2022), kommt zum Schluss, dass 70.4% der befragten Unternehmen in den letzten 24 Monaten vor der Befragung mindestens einen Cyberangriff erlebt haben. Auch in der MEM-Branche war die häufigste Angriffsart «Phishing». In Bezug auf die IT-Sicherheitsmassnahmen haben die befragten Unternehmen mindestens vier und durchschnittlich 25 der 35 abgefragten Massnahmen umgesetzt. Über ein Drittel der Unternehmen gibt sogar an 26 bis 30 (und ein Viertel mehr als 30) Massnahmen umgesetzt zu haben.

Die Studie von Baier et al. (2022), wie auch die Studie von Isenhardt (2022) basieren auf einer Gelegenheitsstichprobe, wurden weder vollständig noch systematisch erstellt und sind daher nicht repräsentativ. Dies erschwert es, die Schweizer Studien mit denjenigen von Dreißigacker et al. (2020, 2021) zu vergleichen.

2.5.3 Fragebogenentwicklung[5]

Auf Basis der Studien von Dreißigacker et al. (2020, 2021), Isenhardt (2022) und der Erkenntnisse aus der Literaturrecherche wurden die Fragen für die Online-Befragung der Schweizer Logistikbranche entwickelt. Initial wurden die Fragen aus den Studien extrahiert, in tabellarischer Form gegenübergestellt (Ausschnitt dargestellt in Tabelle 4) und anschliessend die Fragen für die Online-Befragung definiert. Dreißigacker et al. (2021) erweiterten die Angriffsarten und IT-Sicherheitsmassnahmen in ihrer Folgebefragung, weshalb nur diese (Forschungsbericht Nr. 162) für die Definition der Fragen bzw. Antwortmöglichkeiten berücksichtigt wurde.

Kapitel	Forschungsbericht Nr. 152 2018/2019	Forschungsbericht Nr. 162 2020	Swissmem-Umfrage 2022	Umfrage Logistikbranche 2023
A Einstieg				
		A00 Haben Sie persönlich bereits in der ersten Befragung für ihr Unternehmen teilgenommen? (Ja;Nein; Weiss nicht; Keine Angabe)		
	A01 In welchem Bereich sind Sie in Ihrem Unternehmen tätig? (Geschäftsführung/ Vorstand; IT & Informationssicherheit; Datenschutz; Werkssicherheit; Revision/ Prüfung; Externer Dienstleister; Sonstiges [mit Freitext]; Weiss nicht; Keine Angabe [Mehrfachantworten möglich])	**A01 In welchem Bereich sind Sie in Ihrem Unternehmen tätig?** (Geschäftsführung/ Vorstand; IT, IT-Sicherheit oder Informationssicherheit; Governance & Datenschutz; Sonstiges; Weiss nicht; Keine Angabe [Mehrfachantworten möglich])		**A01 In welchem Bereich sind Sie in Ihrem Unternehmen tätig?** (Geschäftsführung/ Vorstand; IT, IT-Sicherheit oder Informationssicherheit; Governance & Datenschutz; Sonstiges; Weiss nicht; Keine Angabe [Mehrfachantworten möglich])
				A02 In welchem Wirtschaftszweig / welcher Branche ist Ihr Unternehmen tätig? NOGA => 2. Stufe
		D09 Wie viele Mitarbeiter hat Ihr Unternehmen? Wenn Sie es nicht genau wissen, geben Sie bitte einen Schätzwert an.	**17 Wie viele Mitarbeitende hat Ihr unternehmen?**	**A03 Wie viele Mitarbeitende hat Ihr unternehmen?**
		(Anzahl [nummerische Angabe]	1 – 49 / 50 – 249 / 250 – 999 / über 1000 (4)	1 – 9 10-49 50 – 249 >250
	D06 Wie viele Beschäftigten Ihres Unternehmens investieren den überwiegenden Teil ihrer Arbeitszeit in ... (... den Betrieb der IT insg.?; davon speziell in den Betrieb von IT- und Informationssicherheit?), Antwortmöglichkeiten: (nummerische Angabe; Weiss nicht; Keine Angabe)			**A04 Wieviele Mitarbeitende davon sind hauptsächlich mit IT und speziell mit der IT - & Informationssicherheit beschäftigt?** Anzahl angeben
	D07 Hat Ihr Unternehmen IT-Funktionen ausgelagert? (Email & Kommunikation; Netzwerk-Administration & Wartung; Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale); Cloud-Software & Cloud-Speicher; ITSecurity (z.B. Incident Detection, SIEM, Threat Intelligence); Sonstiges; Keine IT-Funktionen ausgelagert [Mehrfachantworten möglich]), Antwortmöglichkeiten: (Ja; Nein; Weiss nicht; Keine Angabe)	**D07 Welche IT-Funktionen werden von einem externen Dienstleister erbracht (Outsourcing)?** (Keine IT-Funktionen ausgelagert; Email & Kommunikation; Netzwerk-Administration & Wartung; Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale); Cloud-Software & Cloud-Speicher; IT-Security (z.B. Incident Detection, SIEM, Threat Intelligence); Sonstiges [mit Freitext]; Weiss nicht; Keine Angabe [Mehrfachantworten möglich])		**A05 Hat Ihr Unternehmen IT-Funktionen an einem externen Dienstleister vergeben (Outsourcing)?** **Wenn ja, welche IT-Funktionen?** Keine IT-Funktionen ausgelagert Email & Kommunikation Netzwerk-Administration & Wartung Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale) Cloud-Software & Cloud-Speicher IT-Security (z.B. Incident Detection, SIEM, SOC, Threat Intelligence) Sonstiges [mit Freitext] Weiss nicht Keine Angabe [Mehrfachantworten möglich]

Tabelle 4: Gegenüberstellung der Fragekataloge (Ausschnitt)

[5] Die Fragebogenentwicklung ist in der Datei «20230430 Entwicklung des Fragenkataloges.xlsx» dokumentiert.

Angriffsarten

Forschungsbericht Nr. 162 2020	Swissmem-Umfrage 2022	Umfrage Logistikbranche 2023
Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware	Hackerangriff (manuelles Hacking) auf IT-Systeme und Firmengeräte, d.h. die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware
Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Erfolgreicher Angriff mit Ransomware, bei dem Unternehmensdaten verschlüsselt wurden	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln
Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen	Abhören oder Abfangen digitaler Kommunikation, z.B. E-Mails, Telefonate, Besprechungen	Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen
Sonstige Schadsoftware – z.B. Viren, Würmer oder Trojaner	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner
Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten
Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern		Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern
Phishing, wobei Mitarbeiter mit echt aussehenden E-Mails oder Webseiten getäuscht wurden, um z.B. sensible Unternehmensdaten zu erlangen	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden
CEO-Fraud, wobei eine Führungspersönlichkeit des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitern zu bewirken	«CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung	«CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung
	Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen	Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen
Sonstiger Cyberangriff	andere Angriffsart (Bitte angeben, um welche Art von Angriff es sich handelte)	andere Angriffsart (Bitte angeben, um welche Art von Angriff es sich handelte)
	Nicht verwendet	
	Diebstahl von Informationsmedien, z.B. Smartphones, Handy, PC, Laptop, Festplatten, Unterlagen, Mustern, Maschinenteilen durch einen Einbruch in Firmengebäude	Diebstahl von Informationsmedien, z.B. Smartphones, Handy, PC, Laptop, Festplatten, Unterlagen, Mustern, Maschinenteilen durch einen Einbruch in Firmengebäude
	Diebstahl von Informationsmedien, z.B. Smartphones, Handy, PC, Laptop, Festplatten durch Personen, die Zugang zum Firmengelände haben/hatten, wie z.B. Mitarbeitende, Besucher u.ä.	Diebstahl von Informationsmedien, z.B. Smartphones, Handy, PC, Laptop, Festplatten durch Personen, die Zugang zum Firmengelände haben/hatten, wie z.B. Mitarbeitende, Besucher u.ä.
	Diebstahl von sensiblen digitalen Daten bzw. Informationen durch eigene Mitarbeitende	Diebstahl von sensiblen digitalen Daten bzw. Informationen durch eigene Mitarbeitende
	Physischer Diebstahl von sensiblen physischen Dokumenten, z.B. Unterlagen, Mustern, Maschinen, Bauteilen durch eigene Mitarbeitende	Physischer Diebstahl von sensiblen physischen Dokumenten, z.B. Unterlagen, Mustern, Maschinen, Bauteilen durch eigene Mitarbeitende
	Unrechtmässiger Abfluss von Daten durch Dritte, z.B. Zulieferer, Dienstleister, bei Kundenanlagen	Unrechtmässiger Abfluss von Daten durch Dritte, z.B. Zulieferer, Dienstleister, bei Kundenanlagen
	Digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen	Digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen
	Physische Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen	Physische Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen
		Angriff auf IoT-Infrastruktur

Tabelle 5: Gegenüberstellung der Angriffsarten

Um die Befragung nicht zu umfangreich werden zu lassen und damit einen Abbruch der Teilnahme zu riskieren, wurde die Anzahl der Angriffsarten auf zehn Auswahlmöglichkeiten begrenzt. So wurde z.B. komplett darauf verzichtet, physische Angriffe, Sabotage und IoT-Angriffe abzufragen.

IT-Sicherheitsmassnahmen

Forschungsbericht Nr. 162 2020	SwissMEM Umfrage 2022	Umfrage Logistikbranche 2023
Informationssicherheitsmanagementsystem (ISMS)	Einführung eines Informationssicherheits-Managementsystems (ISMS)	Einführung eines Informationssicherheits-Managementsystems (ISMS)
Security Information and Event Management (SIEM)		Security Information and Event Management (SIEM)
Security Operation Center (SOC)	Kontinuierliches Monitoring sämtlicher Log-Daten in der Unternehmens ICT	Security Operation Center (SOC)
Antivirensoftware	Aktuelle Antivirensoftware	Antivirensoftware
Schutz der IT-Systeme mit einer Firewall	Schutz der ICT-Systeme mit einer Firewall	Schutz der IT-Systeme mit einer Firewall
	Intrusion Detection System (IDS)	Intrusion Detection System (IDS)
Austausch von Bedrohungsdaten (z.B. Threat Intelligence)		Cyber Threat Intelligence (Austausch von Bedrohungsdaten)
Künstliche Intelligenz basierte Maßnahmen		Künstliche Intelligenz basierte Maßnahmen
	Trennung der ICT-Netzwerke der Firma, wie z. B. ein vom Internet getrenntes Netzwerk	Netzwerksegmentierung
Regelmäßige Backups	Regelmässige Backups/Datensicherungen	Regelmäßige Backups
	Physisch getrennte Aufbewahrung von Backups	
Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme	Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme	Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme
Risiko- und Schwachstellenanalysen (auch Pentest)	Regelmässige Risiko- und Schwachstellenanalysen	Regelmässige Risiko- und Schwachstellenanalysen
Aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates	Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches	Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches
Verschlüsselung von Kommunikation	Verschlüsselung von E-Mails	Verschlüsselung von E-Mails
Verschlüsselung von sensiblen Daten	Verschlüsselung von Festplatten	Verschlüsselung von Festplatten
	Schulungen zur ICT-Sicherheit für Mitarbeitende	Cyber Awareness Trainings für Mitarbeitende
Schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit	Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit	Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit
Schriftliche Richtlinien zum Notfallmanagement	Schriftlich fixierte Richtlinien zum Notfallmanagement	Schriftlich fixierte Richtlinien zum Notfallmanagement
Mindestanforderungen für Passwörter	Mindestanforderungen für Passwörter	Mindestanforderungen für Passwörter
Zwei-Faktor Authentifizierung	Multifaktor-Authentifikation	Multifaktor-Authentifikation
Individuelle Vergabe von Zugangs- und Nutzerrechten	Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe	Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe
	Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk	Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk
Verstärkte physische Sicherheit	Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen	Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen
	Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern	Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern
	Weitere Massnahmen (bitte eintragen)	Weitere Massnahmen (bitte eintragen)
	Nicht verwendet	
Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001 o. VdS 3473)		
Test der Datenwiederherstellung (Restoring)		Test der Datenwiederherstellung (Restoring)
	Physisch getrennte Aufbewahrung von Backups	
		Spezielle Cyber Awareness Trainings für Mitarbeitende im Homeoffice > weglassen
	Background-Checks von Geschäftspartnern (Lieferanten, Dienstleister, Berater etc.)	Background-Checks von Geschäftspartnern (Lieferanten, Dienstleister, Berater etc.)
		Einsatz von Virtual Private Network (VPN) für Mitarbeitende ausserhalb des Unternehmens
		Einsatz des Zero Trust Konzeptes
	Alle Fernzugriffe (für Wartung und Administration) auf Leitstelle und Steuerungsanlagen sind mit starker Authentisierung abgesichert	Alle Fernzugriffe (für Wartung und Administration) auf Leitstelle und Steuerungsanlagen sind mit starker Authentisierung abgesichert
	Klare Regelungen für den Umgang mit vertraulichen Informationen (Informationssicherheitskonzept)	Klare Regelungen für den Umgang mit vertraulichen Informationen (Informationssicherheitskonzept)
	Eindeutige Klassifizierung/Kennzeichnung von Betriebsgeheimnissen	Eindeutige Klassifizierung/Kennzeichnung von Betriebsgeheimnissen
	Geheimhaltungsverpflichtungen für Mitarbeitende	Geheimhaltungsverpflichtungen für Mitarbeitende
	Geheimhaltungsverpflichtungen für Geschäftspartner	Geheimhaltungsverpflichtungen für Geschäftspartner
	Weisungen für die Mitnahme von vertraulichen Informationen bei Auslandsreisen	Weisungen für die Mitnahme von vertraulichen Informationen bei Auslandsreisen
	Weisungen für das Verhalten bei Messen und Ausstellungen	Weisungen für das Verhalten bei Messen und Ausstellungen
	Besuchermanagement/Zutrittskontrollen	Besuchermanagement/Zutrittskontrollen
	Clean-Desk-Policy	Clean-Desk-Policy
	Regelmässige Kontrollen (der Arbeitsplätze, der Mitarbeitenden etc.) in Bezug auf die Einhaltung von Vorschriften	Regelmässige Kontrollen (der Arbeitsplätze, der Mitarbeitenden etc.) in Bezug auf die Einhaltung von Vorschriften
	Physische Sicherheitsmassnahmen, z.B. Kameras, Alarme, Badge-Schliesssysteme	Physische Sicherheitsmassnahmen, z.B. Kameras, Alarme, Badge-Schliesssysteme
	Kontrolle der veröffentlichten Informationen, z.B. auf Homepage /durch Mitarbeitende in den sozialen Medien	Kontrolle der veröffentlichten Informationen, z.B. auf Homepage /durch Mitarbeitende in den sozialen Medien

Tabelle 6: Gegenüberstellung der IT-Sicherheitsmassnahmen

Die Fragen zu den IT-Sicherheitsmassnahmen wurden in technische und organisatorische Massnahmen unterteilt und aus oben genannten Gründen auf total 25 Einträge begrenzt.

2.6 Zwischenresümee

Die Literaturrecherche zeigt klar auf, dass Cyberangriffe gegen Unternehmen häufiger werden, die häufigste initiale Angriffsart «Phishing» ist und deshalb der Faktor Mensch äusserst relevant für die Cybersicherheit der Unternehmen ist. Die Schweizer Logistikbranche setzt sich vorwiegend aus den Wirtschaftszweigen «Handel» sowie «Verkehr und Lagerei» zusammen. Der Handel gehört zu den Branchen mit dem höchsten Reifegrad bei der Cybersicherheitsbereitschaft, wohingegen das Transportwesen zu jenen Branchen zählt, die erst am Anfang ihrer Entwicklung in diesem Bereich stehen (Cisco, 2023).

Künstliche Intelligenz (KI) spielt in der Abwehr von Cyberangriffen, wie auch in der Erkennung von Verhaltensmustern eigener Mitarbeitenden, eine immer wichtigere Rolle. Die Verwendung von auf «künstlicher Intelligenz basierenden» IT-Sicherheitsmassnahmen wird deshalb in der Online-Umfrage explizit abgefragt.

Die Awareness und Schulung des Managements und der Mitarbeitenden werden in der Literatur als entscheidende Faktoren genannt. Deshalb wurden nachfolgende Aussagen zur Einschätzung in die Umfrage aufgenommen:

- *Die Geschäftsführung ist sich der IT-Risiken bewusst und hält die Vorgaben ein*
- *Alle Beschäftigten absolvieren mindestens jährlich ein «Cyber Awareness Training»*
- *Ausgewählte Mitarbeitende absolvieren mindestens jährlich ein «Cyber Awareness Training»*
- *Mitarbeitende, die regelmässig im Homeoffice arbeiten, absolvieren mindestens jährlich ein spezielles «Cyber Awareness Training»*
- *Es gibt verschiedene «Cyber Awareness Trainings» für verschiedene Zielgruppen im Unternehmen*
- *Es existieren Massnahmen zur Erfolgskontrolle/Vertiefung der Schulungen*
- *«Cyber Awareness Trainings» werden in verschiedenen Sprachen angeboten*

Um den Maturitätsgrad der Cybersicherheit im Unternehmen zu erfahren, wurde (trotz zunehmender Komplexität der Umfrage) eine Einschätzung aller vorhandenen IT-Sicherheitsmassnahmen in die Umfrage aufgenommen:

- *Bitte schätzen Sie den Reifegrad und die Verbreitung bzw. den Geltungsbereich der vorhandenen IT-Sicherheitsmassnahmen im Unternehmen ein.*

Um die Vergleichbarkeit der Umfrageergebnisse von Dreißigacker et al. (2020, 2021), Isenhardt (2022) und der Online-Umfrage in der Schweizer Logistikbranche sicherzustellen, wurden die Formulierungen der Fragen soweit möglich aus den vorhergehenden Studien für die Online-Umfrage übernommen.

3. Methode

3.1 Literaturrecherche

Um relevante Artikel zur Forschungsfrage zu finden, die die vorhandenen Studien (Dreißigacker et al., 2020, 2021; Isenhardt et al., 2022) ergänzen können, wurde die Forschungsmethode einer systematischen Literaturrecherche angewendet. Um dabei die Nachvollziehbarkeit zu gewährleisten, wurde in Kapitel 2.1 die Systematik nach (Brocke et al., 2009) genutzt.

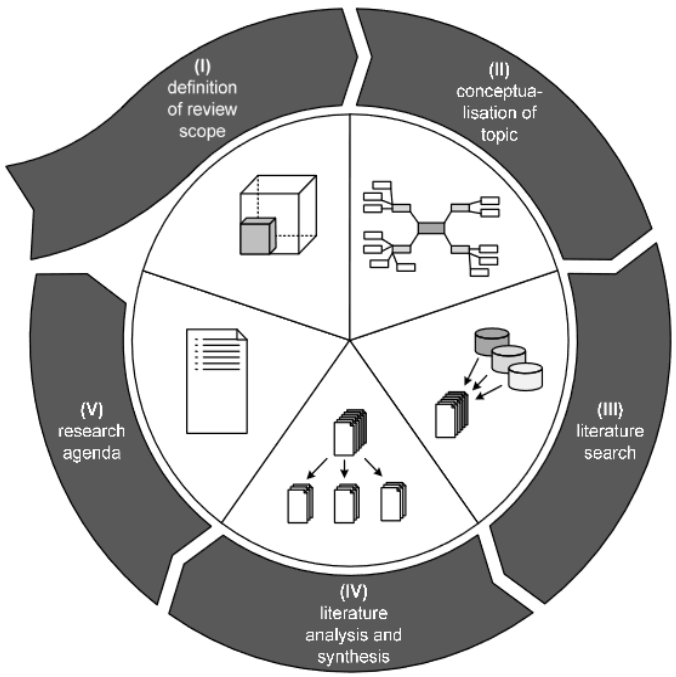


Abbildung 1: Framework für die Literaturrecherche nach Broke et al. (2009)

3.2 Online-Umfrage

Die anschiessend durchgeführte Befragung setzt als empirische Forschungsmethode die quantitativen Querschnittanalyse ein (Wilde & Hess, 2006, 2007), um eine Momentaufnahme der Betroffenheit von Cyberangriffen und des Einsatzes von IT-Sicherheitsmassnahmen in der Schweizer Logistikbranche zu erheben.

Der Fragekatalog wurde einerseits aus den Befragungen von Dreißigacker (2020, 2021) und Isenhardt (2022) abgeleitet, andererseits ergänzt mit Erkenntnissen aus der Literaturrecherche (z.B. mit der Frage nach der Ausbildung von Mitarbeitenden im Thema «Cyber Awareness Training»).

Zur Datenerhebung wurde eine quantitative Befragung nach der Methode von Snijkers und Meyermann (2017) durchgeführt.

3.2.1 Planung der Umfrage

Üblicherweise lassen sich aus einer quantitativen Querschnittanalyse Rückschlüsse auf die Grundgesamtheit schliessen (Wilde & Hess, 2006). Die Logistikbranche besteht nach der Definition von Wohlers (2015) aus den nachfolgenden Wirtschaftsbereichen (Bundesamt für Statistik, 2008a, 2008b, 2013):

- *Wasserversorgung und Abfallentsorgung (E, Codes 36-39)*
- *Handel, Instandhaltung und Reparatur von Motorfahrzeugen (G, Codes 45-47)*
- *Verkehr und Lagerei (H, Codes 49-53)*

Eine repräsentative Stichprobe müsste bei 12’077 registrierten Unternehmen der Logistikbranche im Jahre 2020 (Bundesamt für Statistik, 2022b, 2022a) und einem Konfidenzniveau von 95% und einer Fehlerspanne von 5% rund 373 Antworten von Unternehmen beinhalten (Stocker & Steinke, 2022). In der vorliegenden Arbeit wurde die Stichprobe jedoch nicht zufällig aus der Grundgesamtheit ausgewählt. Sie basiert auf den Mitgliederregistern von Spedlogswiss (450 E-Mail-Adressen), des GS1 Logistik Leiter Clubs (456 E-Mail-Adressen), des GS1 Club de Logisticiens de Suisse Romande (146 E-Mail-Adressen) und einer Anzahl Teilnehmenden, die über LinkedIn auf die Befragung aufmerksam wurden. Dies bedeutet, dass bereits eine Stichprobenverzerrung vorliegt und unabhängig vom Rücklauf und der daraus resultierenden der Stichprobengrösse, nur bedingt Rückschlüsse auf die Grundgesamtheit gezogen werden

können. Dennoch ergibt die Umfrage eine Momentaufnahme der Situation in der Logistikbranche.

3.2.2 Operationalisierung der Umfrage

Der Fragebogen wurde aus einer Gegenüberstellung jener von Dreißigacker (2020, 2021) und Isenhardt (2022) abgeleitet. Ferner wurden die Erkenntnisse aus dem Kapitel 2 in die Fragestellungen und insbesondere deren Antwortmöglichkeiten eingearbeitet. Die Fragen wurden geschlossen formuliert. Als Antwortmöglichkeiten standen die abgestufte Zustimmung bzw. Einschätzung, die Eingabe von Zahlenwerten oder die Auswahl von vorgegebenen Punkten zur Verfügung. Es wurde darauf geachtet, dass Aufzählungen noch mit einem Freitextfeld ergänzt werden konnten, falls etwas nicht aufgeführt war. Sämtliche Elemente der Umfrage wurden in Deutsch, Französisch und Englisch zur Verfügung gestellt, um sie allen Teilnehmenden in der Schweizer Logistikbranche zugänglich zu machen.

Die Branchenverbände Spedlogswiss und GS1 Switzerland haben sich dankenswerterweise dazu bereit erklärt, den Umfragelink an ihre Mitglieder zu senden. Die zu diesem Zweck formulierten Anschreiben, sind im Anhang zu finden. Weiter wurde die Umfrage im LinkedIn-Profil des Autors mit der Aufforderung zur Teilnahme publiziert. Um die drei unterschiedlichen Zielgruppen und deren Rücklaufquote beurteilen zu können, wurde die Online-Umfrage in drei gleichwertige Kopien aufgeteilt und die Umfrage-Links den Zielgruppen entsprechend zur Verfügung gestellt.

Um eine möglichst hohe Teilnahmebereitschaft zu erzielen, wurden folgende Punkte umgesetzt (Snijkers und Meyermann, 2017):

- *Den Verbänden wurde ein individuelles Anschreiben in Deutsch, Französisch und Englisch für die verbandsinterne Kommunikation zur Verfügung gestellt.*
- *Im Anschreiben wurde auf die Branchenverbände als prominente Unterstützer der Umfrage hingewiesen.*
- *Als Anreiz wurde auf die Verlosung einer Betriebsführung inkl. Verpflegung unter den Teilnehmenden hingewiesen.*
- *Für Rückfragen wurde eine Telefonnummer und E-Mail-Adresse kommuniziert.*

- *Nicht alle Fragen waren als obligatorisch gekennzeichnet, um die Teilnehmenden nicht zu frustrieren und um die Anzahl eingereichter Fragebogen zu erhöhen.*

Vor der Publikation der Online-Befragung musste die Vollständigkeit, Rechtschreibung, Logik und Funktionsweise getestet werden. Dieses Pre-Testing fand in allen drei Sprachen mit acht Probanden im In- und Ausland auf Windows und MacOS und iOS Betriebssystemen statt. Es wurden dabei die Internetbrowser Chrome, Safari und Firefox verwendet. Nach der Fehlerbehebung wurden voneinander unabhängige Umfragevarianten für die drei Zielgruppen (GS1, Spedlogswiss, LinkedIn) erstellt. Anschliessend wurden Testantworten in die Statistiksoftware SPSS exportiert, um sicherzustellen, dass die Umfrageergebnisse auch verarbeitet werden konnten.

3.2.3 Feldarbeit und Datenverarbeitung

Die eigentliche Datenerhebung bzw. die Online-Befragung wurde zwischen dem 24.02.2023 und dem 24.03.2023 in Deutsch, Französisch und Englisch mit Hilfe der Umfragesoftware LimeSurvey[6] auf der Plattform der ZHAW durchgeführt. Anschliessend wurden die Ergebnisse bereinigt, plausibilisiert und nach Branche gefiltert, dass schlussendlich nur noch vollständige Antwortsätze aus der Schweizer Logistikbranche vorhanden waren.

3.2.4 Datenübernahme aus anderen Studien

Um die Ergebnisse der Befragung mit den Forschungsergebnissen in Deutschland (Dreißigacker et al., 2020, 2021) vergleichen zu können, wurden vom Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) die bereinigten Datensätze in Form eines SPSS-Datensatzes zur Verfügung gestellt. Auch die Forschungsergebnisse zur Schweizer MEM-Branche (Isenhardt et al., 2022), wurden von der Universität Bern in Form eines bereinigten SPSS-Datensatzes zur Verfügung gestellt. Die dazugehörenden Datennutzungsverträge sind im Anhang zu finden.

[6] Version 3.14.8+180829

3.2.5 Datenanalyse

Als Analyse-Software wurde «IBM Statistical Package for Social Science» (SPSS, Version 28) für deskriptive Statistik, vergleichende Analysen, statistische Auswertung und teilweise für die die Darstellung der Daten verwendet. Microsoft Excel diente mehrheitlich der Plausibilisierung der Ergebnisse und wurde v.a. für die Erstellung der Grafiken eingesetzt.

3.3 Qualitative Befragung

Als Ergänzung zur Online-Umfrage wurde am 11.05.2023 von 09:00 bis 10:00 Uhr ein Fachgespräch durchgeführt. Die Teilnehmenden vertraten einen internationalen Verein für Logistikstandards, einen grossen Schweizer Branchenverband und mehrere internationale Transport- und Logistikunternehmen. Es wurde vorgängig ein Gesprächsleitfaden versendet, der die wichtigsten Erkenntnisse der vorliegenden Arbeit und die Fragen dazu enthielt. Das Fachgespräch wurde als semi-strukturiertes Interview geführt. Dabei konnte aufgrund der zeitlichen Limite nicht auf jede Frage eingegangen werden. Die Liste der Teilnehmenden, der Gesprächsleitfaden sowie der zusammengefasste Gesprächsverlauf ist im Anhang dieser Masterarbeit zu finden. Das Gespräch wurde via Microsoft Teams durchgeführt und aufgezeichnet. Zitate und Inhalte wurden mit einer Zeitangabe auf die Aufzeichnung referenziert.

4. Resultate

4.1 Ergebnisse der Umfrage in der Schweizer Logistikbranche

4.1.1 Erhebungszeitraum

Die Umfragen starteten leicht zeitversetzt und waren rund einen Monat lang online. Das Versenden einer Erinnerung am 07.03.2023 führte erwartungsgemäss zu einer zweiten Welle von Teilnehmenden.

Umfrage	Startdatum	Enddatum	Dauer in Tagen
GS1	27.02.2023	24.03.2023	25
SPEDLOGSWISS	24.02.2023	24.03.2023	28
LinkedIn	27.02.2023	24.03.2023	25

Tabelle 7: Erhebungszeitraum der Online-Umfragen

Das ursprünglich angekündigte Ende der Umfrage (12.03.2023) wurde absichtlich überschritten. So konnten die später eingereichten Antworten mitberücksichtigt werden.

4.1.2 Datenbereinigung, Rücklaufquote und Sprache

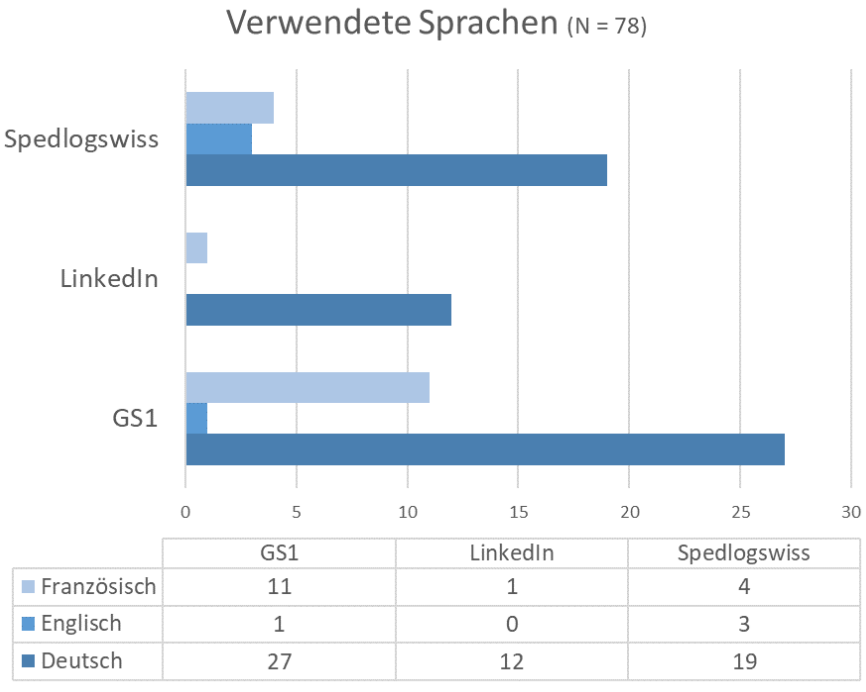
Die drei Umfragen wurden von insgesamt 144 Teilnehmenden (100%) begonnen, wobei 97 Teilnehmende mehr als zwei Umfrageseiten ausfüllten (69%). Bereinigt konnten schliesslich 78 Teilnehmende (55%) bzw. Datensätze mit mindestens «einem berichteten Cyberangriff» oder «einer Rangfolge möglicher Folgen eines Cyberangriffes» für die Analyse übernommen werden.

Die Rücklaufquoten bei GS1 (6.5%) und Spedlogswiss (5.8%) waren eher tief im Vergleich zur Umfrage von Isenhardt (2022) mit einem Rücklauf von 22.6%.

Umfrage	Kontaktierte Personen	Nutzbare Datensätze	Rücklaufquote
GS1	602	39	6.5%
SPEDLOGSWISS	450	26	5.8%
LinkedIn	n.v.	13	n.v.

Tabelle 8: Rücklaufquote der Online-Umfragen

Die Antworten teilten sich in alle drei angebotenen Sprachen auf, wobei Deutsch erwartungsgemäss am häufigsten verwendet wurde.



	GS1	LinkedIn	Spedlogswiss
Französisch	11	1	4
Englisch	1	0	3
Deutsch	27	12	19

Abbildung 2: Verwendete Sprachen bei der Beantwortung der Online-Umfrage

4.1.3 Abgrenzung Logistikbranche und angewandte Betriebe

Die Definition der Logistikbranche (vgl. Kapitel 3.2.1) sieht vor, dass die 78 auswertbaren Antworten der Online-Umfrage[7] auf die Wirtschaftszweige E, G und H eingeschränkt werden, wobei keine Antwort aus dem Wirtschaftszweig E eingegangen ist. Diese 45 Antworten werden in den nachfolgenden Kapiteln mit «LOG» bezeichnet (in Tabelle 9 blau umrandet). Da die antwortenden Personen über die Verteiler der Logistik-Branchenverbände Spedlogswiss und GS1 angeschrieben wurden, werden weitere 28 Antworten, die nicht von Betrieben aus den Wirtschaftszweigen G und H stammen, mit «LOG+» bezeichnet. Die einzige Ausnahme bilden die fünf Antworten, die über LinkedIn eingegangen sind und nicht den Wirtschaftszweigen G oder H angehören (in Tabelle 9 rot gepunktet umrandet). Werden diese weggelassen, ergeben sich 73 Antworten[8], die für die folgenden Analysen als Logistikbranche (LOG & LOG+) verwendet werden können.

In welchem Wirtschaftszweig / in welcher Branche ist Ihr Unternehmen tätig bzw. das Unternehmen, das Sie als ICT-Dienstleister vertreten? * survey Kreuztabelle

Anzahl

		survey			
		GS1	LinkedIn	Spedlogswiss	Gesamt
In welchem Wirtschaftszweig / in welcher Branche ist Ihr Unternehmen tätig bzw. das Unternehmen, das Sie als ICT-Dienstleister vertreten?	C: Verarbeitendes Gewerbe/Herstellung von Waren	10	3	0	13
	F: Baugewerbe/Bau	1	0	1	2
	G: Handel; Instandhaltung und Reparatur von Motorfahrzeuge	6	7	0	13
	H: Verkehr und Lagerei	10	1	21	32
	I: Gastgewerbe/Beherbergung und Gastronomie	1	0	0	1
	J: Information und Kommunikation	1	0	0	1
	L: Grundstücks- und Wohnungswesen	0	1	0	1
	M: Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen	1	0	0	1
	N: Erbringung von sonstigen wirtschaftlichen Dienstleistungen	4	1	0	5
	P: Erziehung und Unterricht	1	0	0	1
	Q: Gesundheits- und Sozialwesen	1	0	0	1
	S: Erbringung von sonstigen Dienstleistungen	3	0	4	7
Gesamt		39	13	26	78

Tabelle 9: Logistikbranche und nicht berücksichtigte Antworten (A02)

[7] In den Abbildungs- und Tabellenbeschreibungen werden jeweils am Ende in Klammern die Fragennummer aus der Online-Umfrage referenziert.

[8] LOG: N = 45; LOG+: N = 28

4.1.4 Teilnehmende Personen und Unternehmen

Ein guter Drittel der teilnehmenden Personen waren Mitglieder einer Geschäftsleitung oder eines Vorstandes (39%). Ein weiterer Drittel der Teilnehmenden beschäftigte sich beruflich mit IT / ICT, IT-Sicherheit / Informationssicherheit oder Governance & Datenschutz (35%). Ein Rest von 26% ordnete sich einer «sonstigen» Rolle zu.

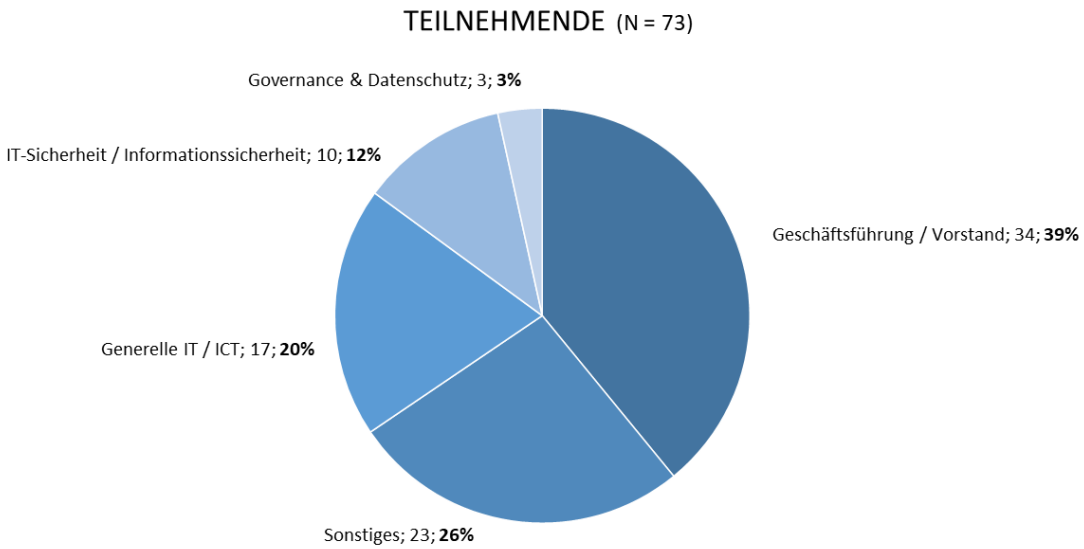


Abbildung 3: Rollen der Teilnehmenden (A01)

Wie viele Mitarbeitende hat Ihr Unternehmen bzw. das Unternehmen, das Sie als ICT-Dienstleister vertreten?

		Unternehmen	Anteil
LOG	1 bis 9 Beschäftigte (Microunternehmen)	5	6.8%
	10 bis 49 Beschäftigte (Kleine Unternehmen)	10	13.7%
	50 bis 249 Beschäftigte (Mittlere Unternehmen)	10	13.7%
	ab 250 Beschäftigte (Grosse Unternehmen)	20	27.4%
		45	61.6%
LOG+	1 bis 9 Beschäftigte (Microunternehmen)	3	4.1%
	10 bis 49 Beschäftigte (Kleine Unternehmen)	5	6.8%
	50 bis 249 Beschäftigte (Mittlere Unternehmen)	11	15.1%
	ab 250 Beschäftigte (Grosse Unternehmen)	9	12.3%
		28	38.4%
Total	1 bis 9 Beschäftigte (Microunternehmen)	8	11.0%
	10 bis 49 Beschäftigte (Kleine Unternehmen)	15	20.5%
	50 bis 249 Beschäftigte (Mittlere Unternehmen)	21	28.8%
	ab 250 Beschäftigte (Grosse Unternehmen)	29	39.7%
		73	100.0%

Tabelle 10: Teilnehmende pro Unternehmensgrössenklasse (A03)

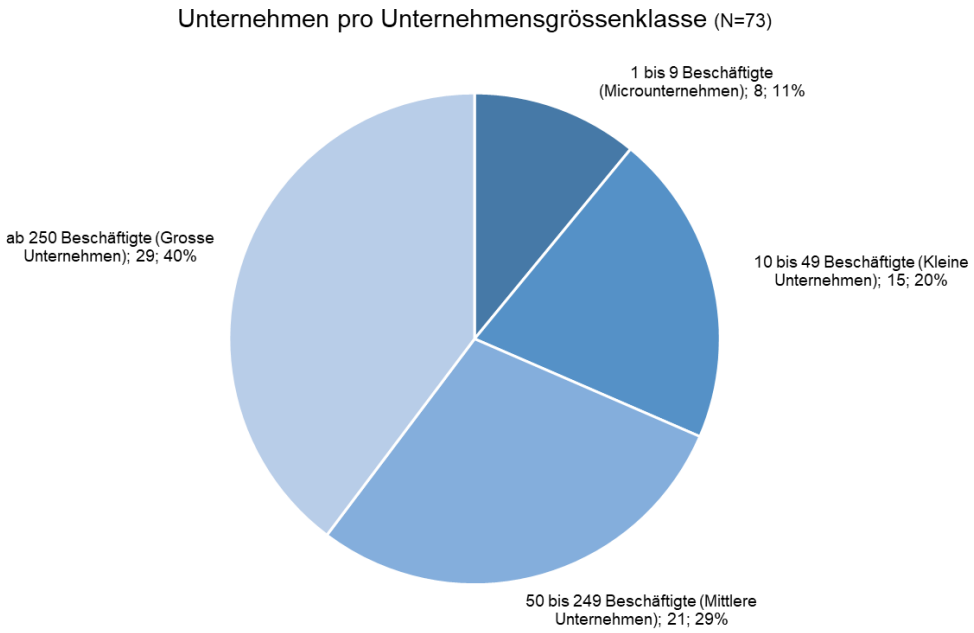


Abbildung 4: Teilnehmende pro Unternehmensgrössenklasse total (A03)

Bei Betrachtung der Verteilung der Teilnehmenden in Bezug auf die Unternehmensgrösse sind die Unternehmen ab 250 Mitarbeitenden mit 40% im Vergleich zu mittleren (29%), kleinen (20%) und sehr kleinen (11%) Unternehmen überproportional vertreten. Aufgrund der Tatsache, dass eine kleine Gelegenheitsstichprobe vorliegt, wird auf eine Gewichtung der Antworten zur Berücksichtigung aller Grössenklassen verzichtet.

Die Anzahl der Mitarbeitenden, die sich hauptsächlich mit «genereller IT / ICT» beschäftigten (Frage A04, N=68) variierte zwischen 0 und 700 Personen. Der Mittelwert lag bei 31 und der Median bei 3 Mitarbeitenden. Der Mittelwert für Personen die sich vorwiegend mit «IT-Sicherheit / Informationssicherheit» beschäftigten (N=66) lag bei 3.1 und der Median bei 1.

4.1.5 Outsourcing der ICT

Durchschnittlich gaben 35% der befragten Unternehmen an, ICT-Services ausgelagert zu haben. Unter «Sonstiges» wurde Folgendes genannt: Alarmserver, Betreuung ABACUS, CISO, ERP (3x), ERP/TMS, gewisse Services teils als Managed Services ausgelagert (z.B. Datacenter, Server bis Layer 2, Administration dann wieder inhouse), Mutterhaus in DE, Print Service, Kassen, Logistiksysteme und Saas.

Hat Ihr Unternehmen IT-Funktionen an einen externen Dienstleister vergeben (Outsourcing)? Wenn ja, welche IT-Funktionen?

	LOG (N=45)		LOG+ (N=28)		Total (N=73)	
Keine IT-Funktionen ausgelagert	4	8.9%	4	14.3%	8	11.0%
Email & Kommunikation	20	44.4%	10	35.7%	30	41.1%
Netzwerk-Administration & Wartung	22	48.9%	11	39.3%	33	45.2%
Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale)	18	40.0%	12	42.9%	30	41.1%
Cloud-Software & Cloud-Speicher	28	62.2%	10	35.7%	38	52.1%
IT-Security (z.B. Incident Detection, SIEM, SOC, Threat Intelligence)	19	42.2%	10	35.7%	29	39.7%
Sonstiges	8	17.8%	3	10.7%	11	15.1%

Tabelle 11: Outsourcing von ICT-Services (A05)

4.1.6 Risikoeinschätzung der Unternehmen

Erstaunlicherweise schätzten 50.7% der befragten Unternehmen das Risiko, in den nächsten 12 Monaten Opfer eines gezielten Cyberangriffes zu werden, als «eher gering» ein. Auch ein breit gestreuter Cyberangriff wird von 45.2% der Unternehmen als «eher gering» eingestuft.

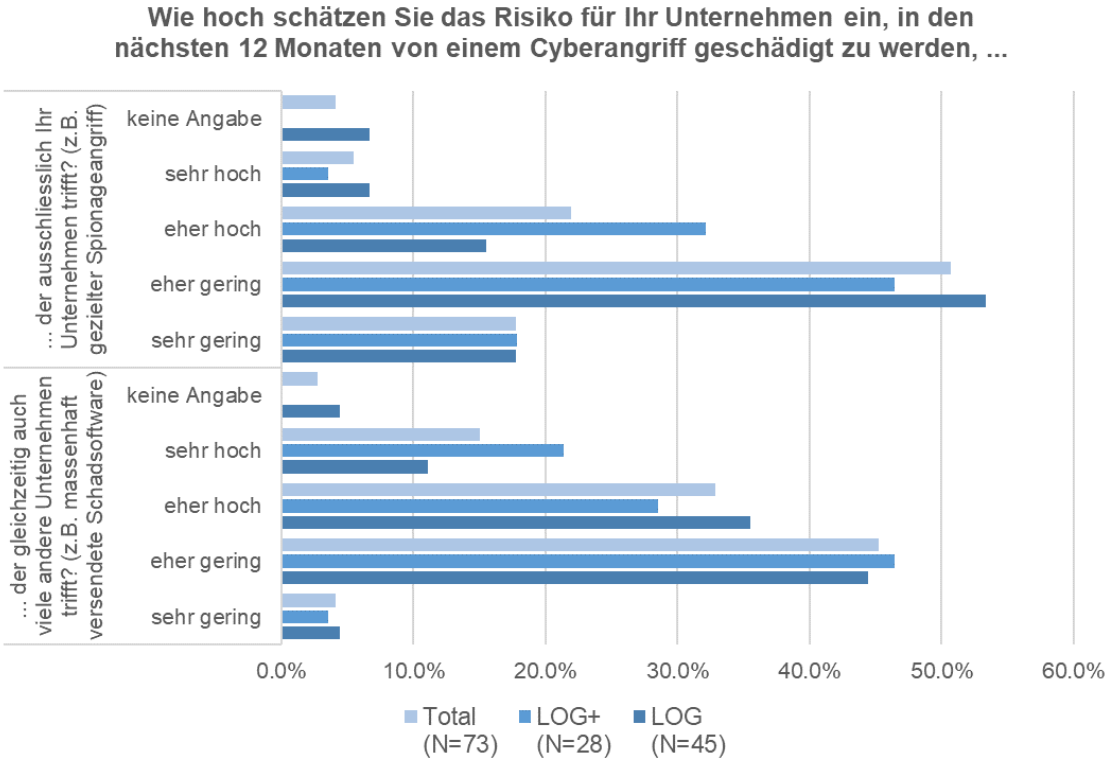


Abbildung 5: Risikoeinschätzung zu Angriff in den nächsten 12 Monaten (A06)

Die Unternehmen nehmen zu 53.4% an, dass sie aufgrund ihrer Reputation oder ihrem Kundenkreis angegriffen würden. 13.7% der Unternehmen nehmen an, dass sie aufgrund ihrer besonderen Produkte, Herstellungsverfahren oder Dienstleistungen angegriffen würden.

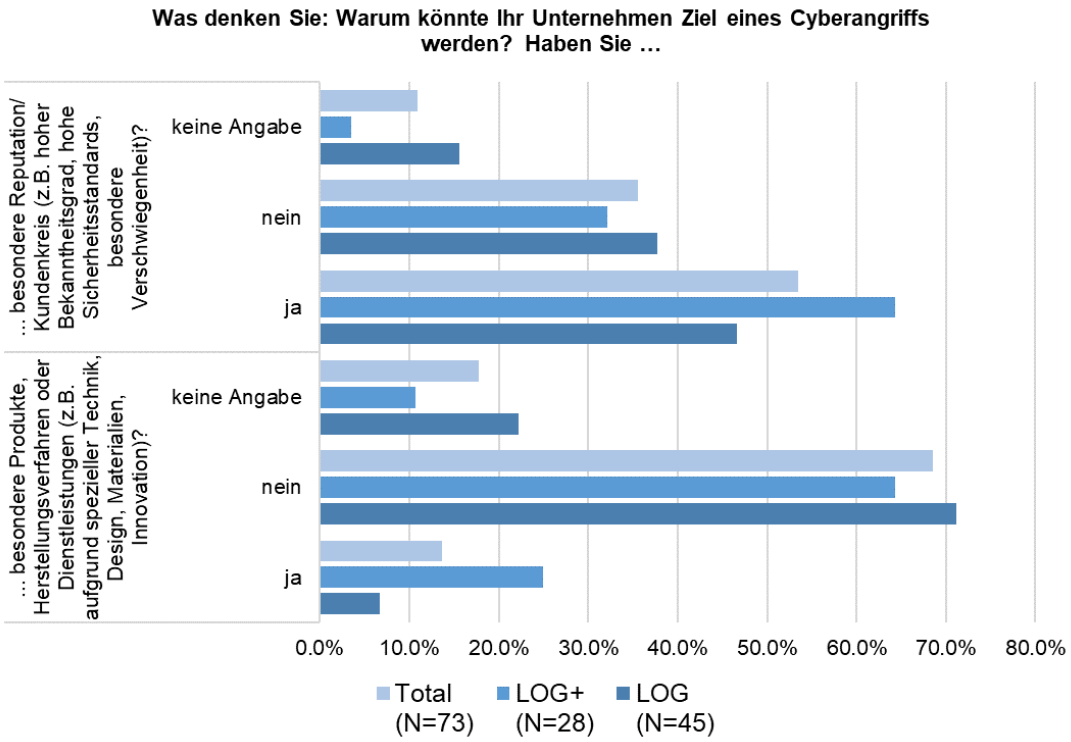


Abbildung 6: Gründe für potenziellen Cyberangriff (A07)

4.1.7 Von Cyberangriffen betroffene Unternehmen

Angriffe generell und in den letzten 24 Monaten vor der Befragung

Von den teilnehmenden Unternehmen gaben 64% (47 von 73) an, bereits einmal oder mehrmals von einem Cyberangriff betroffen gewesen zu sein.

In den letzten 24 Monaten waren 45.2% (33 von 73) der Unternehmen von mindestens einem Angriff betroffen. Am häufigsten waren «Phishing-Angriffe» mit 39.9% aller Angriffe, gefolgt von «sonstigem Social Engineering» mit 19.4% und «CEO-Fraud» mit 17.1%.

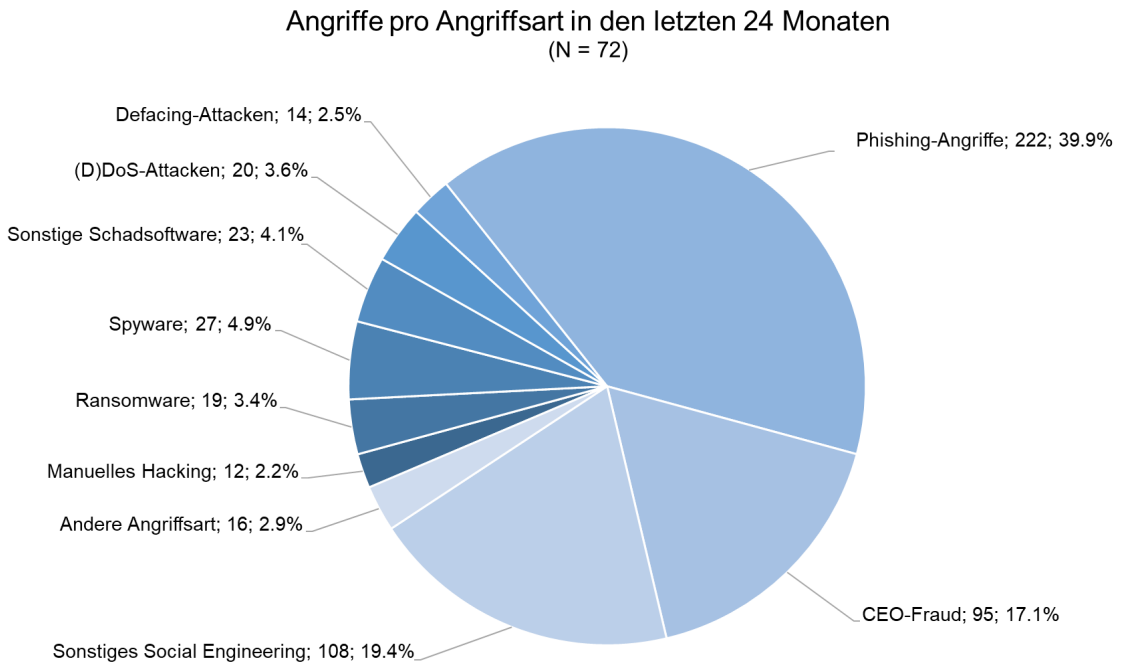


Abbildung 7: Summe aller Cyberangriffe nach Angriffsart (B01)

Die Angaben, wie oft ein Angriff in den letzten 24 Monaten vor der Befragung stattgefunden hat, wurden gruppiert und in Tabelle 12 dargestellt. Beim Betrachten der gruppierten Häufigkeit zeigt sich, dass z.B. die 95 registrierten «CEO-Fraud-Angriffe» 24.7% der Unternehmen betraf und 75.3% keinen solchen Angriff verzeichneten. Von den angegriffenen Unternehmen erlebten 15.1% ein bis zwei solche Angriffe innerhalb der letzten 24 Monate.

	LOG CH & LOG+ CH						
	In den letzten 24 Monaten vor der Befragung						
Häufigkeit der Betroffenheit durch einzelne Angriffsarten (in Prozent)	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	73	87.7%	9.6%		2.7%		
Spyware-Angriff (um zur Daten auszuspähen)	73	89.0%	6.8%		1.4%	1.4%	1.4%
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	73	87.7%	9.6%	1.4%	1.4%		
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	73	95.9%	2.7%		1.4%		
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	73	89.0%	8.2%	1.4%	1.4%		
Defacing-Attacke (um Inhalte von Websites zu verändern)	73	94.5%	4.1%		1.4%		
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	73	75.3%	15.1%	2.7%	1.4%	2.7%	2.7%
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	73	68.5%	11.0%	8.2%	4.1%	4.1%	4.1%
Sonstiges "Social Engineering" (gezielte Täuschung von Mitarbeitenden)	73	86.3%	8.2%		2.7%		2.7%
Andere Angriffsart	73	95.9%	1.4%		2.7%		

Tabelle 12: Häufigkeit der Cyberangriffe (gruppiert) (B02)

Nachfolgende Abbildung 8 zeigt, wie die Unternehmen[9] von unterschiedlichen Angriffsarten in unterschiedlicher Intensität betroffen waren. Dazu wurde pro Unternehmen die Anzahl unterschiedlicher Angriffsarten gezählt und diese gruppiert (x-Ache) und die jeweilige Anzahl Angriffe pro Gruppe summiert (y-Achse). So erlebten die Unternehmen am häufigsten die Kombination von drei unterschiedlichen Angriffsarten.

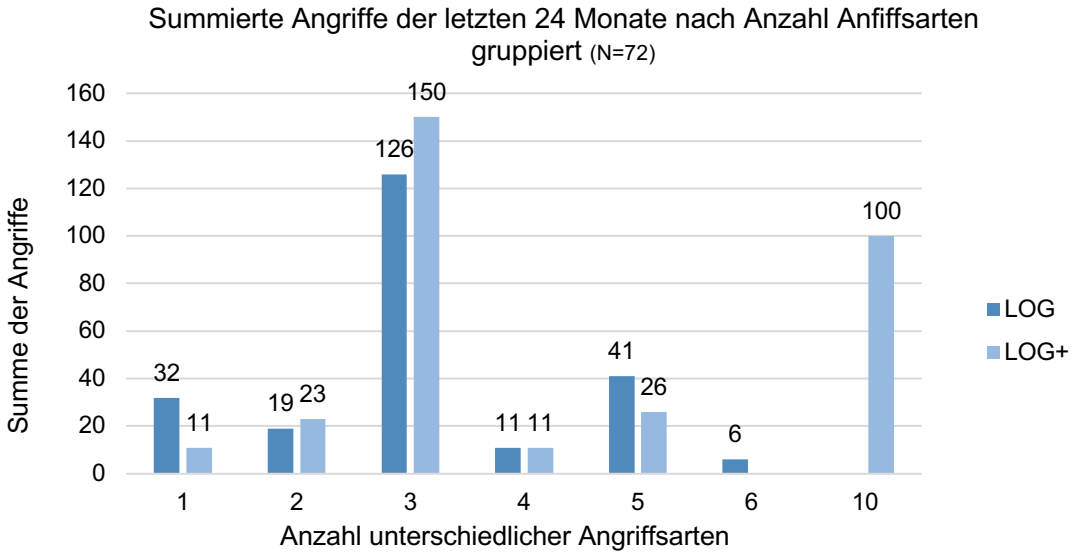


Abbildung 8: Unterschiedliche Angriffsarten und ihre Intensität (B02)

«Schwerwiegendster Cyberangriff»

«Phishing-Angriffe» wurden von 19.2% der Unternehmen als die «schwerwiegendsten Angriffe» wahrgenommen, direkt gefolgt von «CEO-Fraud» 12.3% und «Ransomware» 8.2%. Da die Stichprobengrösse klein ist, lassen sich keine weiteren Aussagen zu den Untergruppen LOG und LOG+ machen.

Die Summe aller genannten Angriffe (=44) übersteigt die Anzahl angegriffener Unternehmen (=33), da drei Unternehmen Mehrfachnennungen angegeben haben, bei denen die Angriffe zusammen aufgetreten sind (siehe Frage B04 im Anhang).

[9] Es wurde ein Ausreisser-Datensatz entfernt, der als Platzhalter sehr hohe Zahlen eingegeben hat (9'999'999) und den Hinweis «Für mich praktisch nicht ausfüllbar war der Abschnitt mit den Fragen wieviel Phishing- / Malware-Angriffe stattfanden. Woher sollte man das denn wissen, bzw. wie messen?».

Sie haben für die unten aufgeführten Angriffsarten angegeben, dass Ihr Unternehmen in den letzten 24 Monaten von diesen betroffen war. Welcher dieser Angriffe war aus Ihrer Sicht der schwerwiegendste?

Wirtschaftszweig Gruppe	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohn Nutzung spezieller Schadsoftware	Denial of Service (D)DoS-Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern	«CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitende zu bewirken, z.B. Geldüberweisung	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Andere Angriffsart	Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen
LOG CH (N = 45)	2	2	1	0	4	1	7	7	0	0
	4.4%	4.4%	2.2%	0.0%	8.9%	2.2%	15.6%	15.6%	0.0%	0.0%
LOG+ CH (N = 28)	4	1	1	1	1	1	2	7	1	1
	14.3%	3.6%	3.6%	3.6%	3.6%	3.6%	7.1%	25.0%	3.6%	3.6%
LOG CH & LOG+ CH (N = 73)	6	3	2	1	5	2	9	14	1	1
	8.2%	4.1%	2.7%	1.4%	6.8%	2.7%	12.3%	19.2%	1.4%	1.4%

Abbildung 9: Schwerwiegendster Cyberangriff (LOG CH & LOG+ CH) (B04)

Initialer Angriffspunkt und Motivation der Täterschaft

Von den 33 Unternehmen, die einen «schwerwiegenden Angriff» erlebt haben, gaben 40% auf die Frage nach dem ursprünglichen Angriffspunkt «Niederlassung im Inland» als Ursprung des Angriffs an. Nur 10% nannten die «Niederlassung im Ausland». 33% machten keine Angabe.

Initialer Angriffspunkt	**LOG** (N=19)	**LOG+** (N=11)	**Total** (N=33)	
Niederlassung im Inland	7	5	**12**	**40%**
Niederlassung im Ausland	2	1	**3**	**10%**
Lieferanten	4	1	**5**	**17%**
Keine Angabe	6	4	**10**	**33%**
Gesamtergebnis	**19**	**11**	**30**	**100%**

Tabelle 13: Initialer Angriffspunkt (B05)

Die Einschätzung, weshalb ihr Unternehmen Opfer eines Angriffes wurde, beantworteten 32 von 33 Unternehmen. 69% der Unternehmen gehen dabei von einem «nicht zielgerichteten» Angriff aus, 13% gehen von einem «zielgerichteten» Angriff aus. 19% machten keine Angabe.

Motivation der Täterschaft	**LOG** (N=21)	**LOG+** (N=11)	**Total** (N=32)	
Das Unternehmen wurde beim schwerwiegendsten Angriff als ein Unternehmen von vielen anderen attackiert (z.B. bei massenhaft versendeter Schadsoftware, Ransomware-Angriffen oder dem Ausnützen von technischen Schwachstellen).	14	8	**22**	**69%**
Das Unternehmen wurde beim schwerwiegendsten Angriff zielgerichtet attackiert/ausgewählt (z.B. gezielter Spionageangriff).	3	1	**4**	**13%**
keine Angabe	4	2	**6**	**19%**
Gesamtergebnis	**21**	**11**	**32**	**100%**

Tabelle 14: Motivation der Täterschaft (B06)

Folgen für das Unternehmen

Von 33 betroffenen Unternehmen beantworteten 32 diese Frage, wobei für 15 Unternehmen der Angriff «keine Folgen» hatte. Am häufigsten wurden Kostenfolgen für die Wiederherstellung von Daten und IT-Infrastruktur genannt.

	LOG (N=21)	LOG+ (N=11)	**Total (N=32)**
Keine Folge	10	5	**15**
Kosten für Sofortmassnahmen zur Abwehr und Aufklärung	6	4	**10**
Kosten für Wiederherstellung von Daten oder IT-Infrastruktur (Hardware und Software)	6	2	**8**
Kosten für externe Beratung	5	2	**7**
Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen	4	2	**6**
Erhöhung des Zusammenhalts unter den Mitarbeitenden	2	3	**5**
Ausfall der Informatik	3	1	**4**
Positive Reaktionen (z.B. von Kundinnen und Kunden) auf den raschen und resilienten Umgang mit dem Angriff	2	2	**4**
Betriebsunterbrechung (d.h. vollständiger oder teilweiser Ausfall der Produktion und Administration)	1	2	**3**
Interne Reorganisationskosten	3		**3**
Erpressung mit den verschlüsselten Daten	1	1	**2**
Kosten aufgrund von Lösegeldzahlungen		1	**1**
Negative Auswirkung auf die Geschäftsentwicklung		1	**1**
Reputationsverluste/Negative Presse		1	**1**
Diebstahl oder Schädigung von IT- oder Kommunikationsgeräten			
Erpressung mit entwendeten Daten			
Kosten für Rechtsstreitigkeiten, Schadensersatz, Strafen			
Kundenverluste/Auftragsverluste			
Verlust von personenbezogenen Daten, z.B. Kundendaten, Daten von Mitarbeitenden			
Entlassung von Mitarbeitenden			
Höhere Mitarbeitendenfluktuation, z.B. Verlust von kompetenten Arbeitskräften			
Keine Angabe	1	1	**2**

Tabelle 15: Folgen des schwerwiegendsten Angriffes auf das Unternehmen (B07)

Lösegeldforderungen

Lediglich zwei Unternehmen gaben an nach dem «schwerwiegendsten Angriff» mit einer Lösegeldforderung konfrontiert gewesen zu sein, welcher sie beide nicht nachgekommen sind (Frage B08: N=6, Frage B09: N=2).

Folgen für die IT-Systeme

Durch den «schwerwiegendsten Angriff» war am häufigsten der Standard-Arbeitsplatz und die Office-IT (42%), gefolgt von E-Mail und Kommunikation (39%) betroffen.

Aufgrund der kleinen Stichprobe können keine verallgemeinernden Schlüsse aus diesen Zahlen gezogen werden.

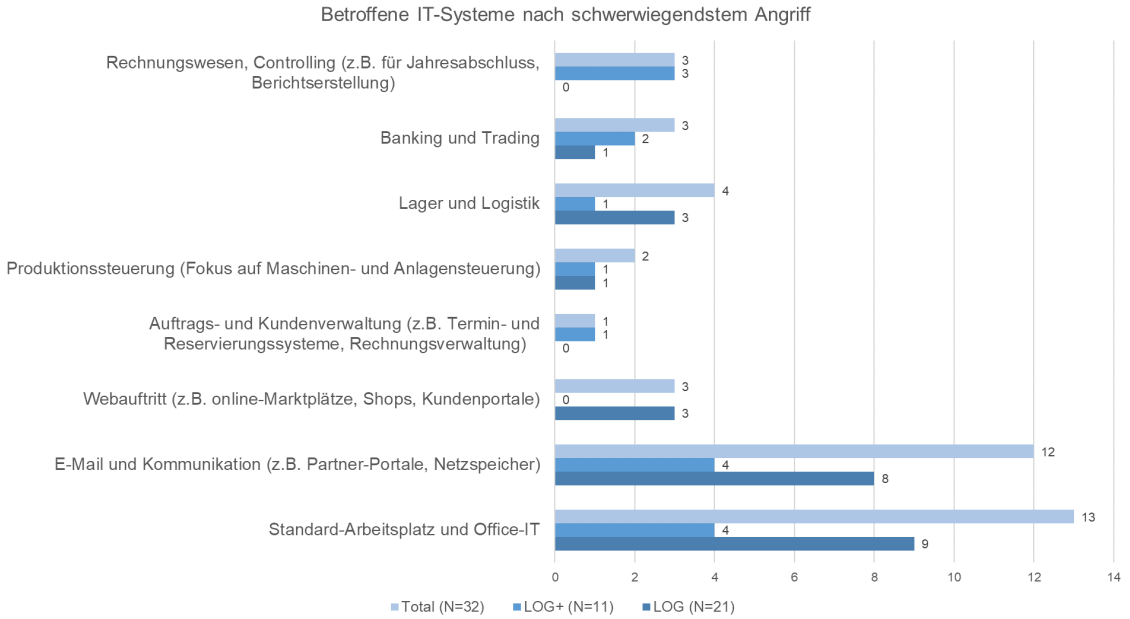


Abbildung 10: Betroffene IT-Systeme nach schwerwiegendstem Angriff (B11)

Kostenfolge des Angriffes

Die Kosten, die durch den «schwerwiegendsten Angriff» entstanden sind, weisen eine sehr hohe Spannweite auf, wobei der maximale Betrag von CHF1 Mrd. angezweifelt werden muss. Bei 31 Unternehmen liegt der Median der Kostenfolge bei CHF 1'000.

Bitte geben Sie an, welche Kosten durch den von Ihnen angegebenen schwerwiegendsten Angriff in CHF entstanden sind.

Wirtschaftszweig Gruppe			
	LOG CH (N = 45)	Antworten	21
		Mittelwert	37'227
		Median	524
		Std.-Abweichung	85'935
		Spannweite	300'000
		Minimum	-
		Maximum	300'000
	LOG+ CH (N = 28)	Antworten	10
		Mittelwert	100'112'350
		Median	1'250
		Std.-Abweichung	316'188'443
		Spannweite	1'000'000'000
		Minimum	-
		Maximum	1'000'000'000
	LOG CH & LOG+ CH (N = 73)	Antworten	31
		Mittelwert	32'319'525
		Median	1'000
		Std.-Abweichung	179'593'994
		Spannweite	1'000'000'000
		Minimum	-
		Maximum	1'000'000'000

Tabelle 16: Kostenfolge nach schwerwiegendstem Angriff (B12)

Folgen des Angriffes

Von den 32 Unternehmen schätzte lediglich ein Unternehmen die Folgen des «schwerwiegendsten Angriffes» als «existenzgefährdend» ein. Zwei Drittel gaben an, dass der Angriff «kurzfristig behebbar und leicht verdaubar» war. Für einen Drittel zog der Angriff «keine Einschränkungen» nach sich.

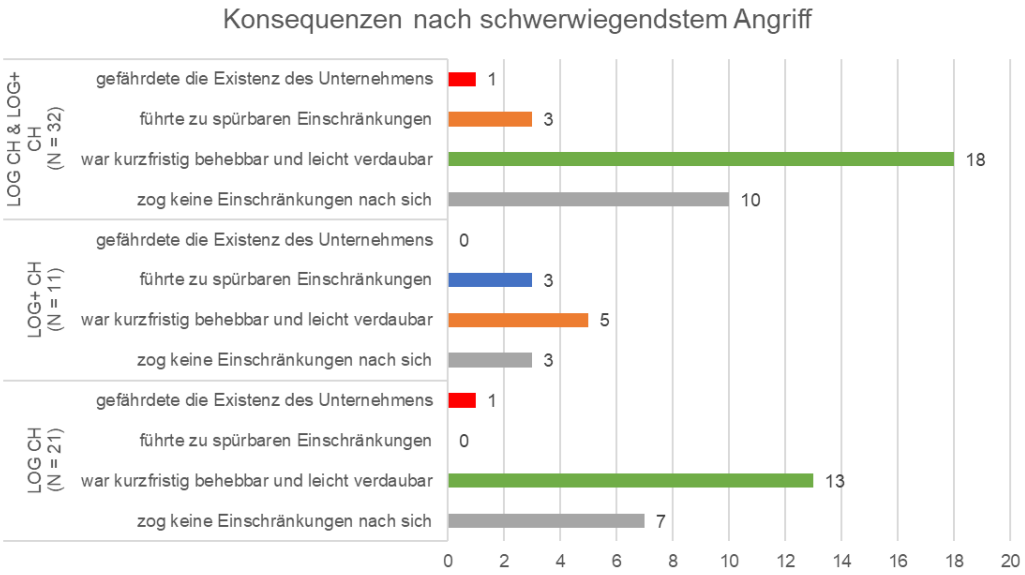


Abbildung 11: Konsequenzen nach schwerwiegendstem Angriff (B16)

Betroffene Daten

Alle Daten-Kategorien waren gleichermassen betroffen, kunden- und personenbezogene Daten mit 12.5% etwas häufiger. Es ist zu beachten, dass die sehr kleine Stichprobe keine verallgemeinernden Aussagen zulässt.

In Tabelle 17 ist zu beachten, dass aufgrund der geringen Anzahl Antworten nicht jede Antwortmöglichkeit (ja, sie wurden gelöscht /gestohlen / manipuliert / verschlüsselt oder blockiert) für jede Datenkategorie existiert.

Waren bei dem genannten schwerwiegendsten Angriff die folgenden Daten betroffen? Wurden diese gelöscht, manipuliert, gestohlen oder verschlüsselt?

		Kunden- und personenbezogene Daten		Betriebs-wirtschaftliche Daten		Produktions- und Prozessdaten		Produkt und F&E Daten		Andere Daten	
Wirtschaftszweig Gruppe		Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent
LOG CH	ja, sie wurden gelöscht	1	4.8								
	ja, sie wurden verschlüsselt oder blockiert	1	4.8	1	4.8	1	4.8	1	4.8	1	4.8
	ja (total)	**2**	**9.5**	**1**	**4.8**	**1**	**4.8**	**1**	**4.8**	**1**	**4.8**
	nein	18	85.7	19	90.5	19	90.5	19	90.5	19	90.5
	keine Angabe	1	4.8	1	4.8	1	4.8	1	4.8	1	4.8
	N	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**
LOG+ CH	ja, sie wurden gestohlen			1	3.6					1	3.6
	ja, sie wurden manipuliert	1	3.6								
	ja, sie wurden verschlüsselt oder blockiert	1	3.6	1	3.6	2	7.1	2	7.1	1	3.6
	ja (total)	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**
	nein	7	25.0	7	25.0	7	25.0	7	25.0	7	25.0
	keine Angabe	2	7.1	2	7.1	2	7.1	2	7.1	2	7.1
	N	**28**	**100.0**	**11**	**100.0**	**11**	**100.0**	**11**	**100.0**	**11**	**100.0**
LOG CH & LOG+ CH	ja, sie wurden gelöscht	1	3.1								
	ja, sie wurden gestohlen			1	3.1					1	3.1
	ja, sie wurden manipuliert	1	3.1								
	ja, sie wurden verschlüsselt oder blockiert	2	6.3	2	6.3	3	9.4	3	9.4	2	6.3
	ja (total)	**4**	**12.5**	**3**	**9.4**	**3**	**9.4**	**3**	**9.4**	**3**	**9.4**
	nein	25	78.1	26	81.3	26	81.3	26	81.3	26	81.3
	keine Angabe	3	9.4	3	9.4	3	9.4	3	9.4	3	9.4
	N	**49**	**100.0**	**32**	**100.0**	**32**	**100.0**	**32**	**100.0**	**32**	**100.0**

Tabelle 17: Betroffene Daten (B13)

Kommunikation nach dem Angriff

Zwei Drittel der 33 betroffenen Unternehmen informierten nach einem Cyberangriff die Eigentümerschaft des Unternehmens. An zweiter Stelle folgten die Geschäftspartner. Die Kunden und die Öffentlichkeit wurden am wenigsten oft informiert.

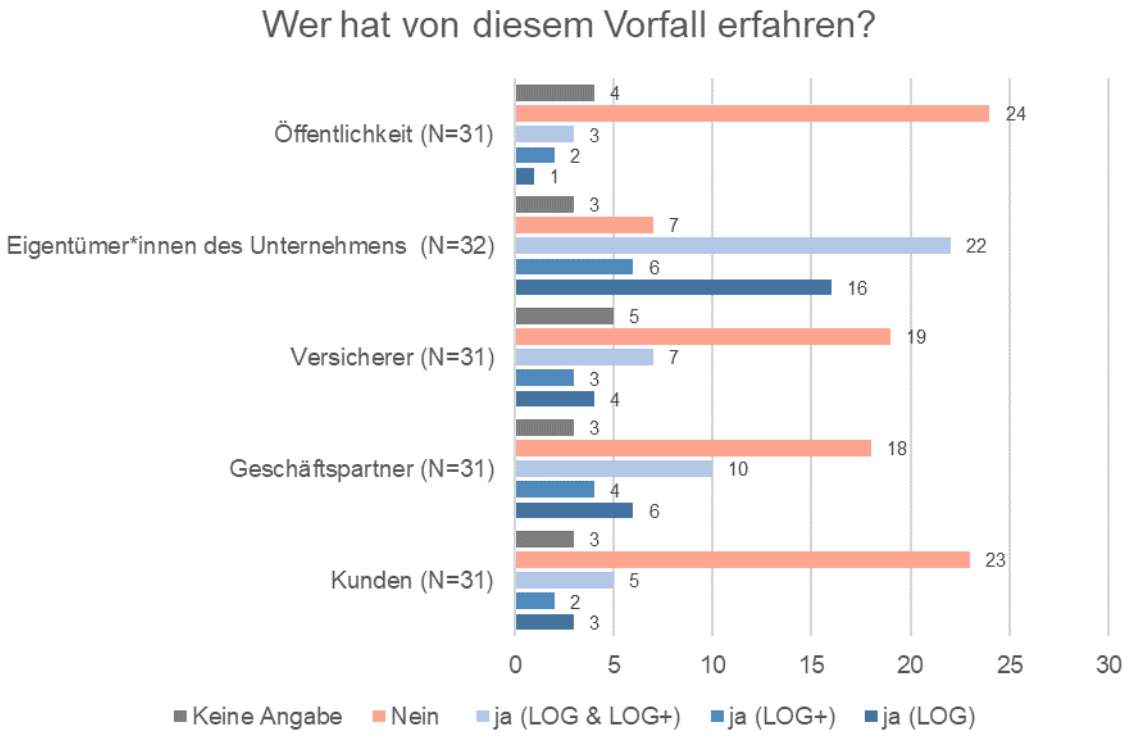


Abbildung 12: Information der Stakeholder nach dem Angriff (B14)

Kontaktaufnahme nach dem Angriff

44% der Unternehmen kontaktierten nach dem «schwerwiegendsten Angriff» einen «spezialisierten Dienstleister». 19% informierte die «Polizei» und 22% das «Nationale Zentrum für Cybersicherheit NCSC».

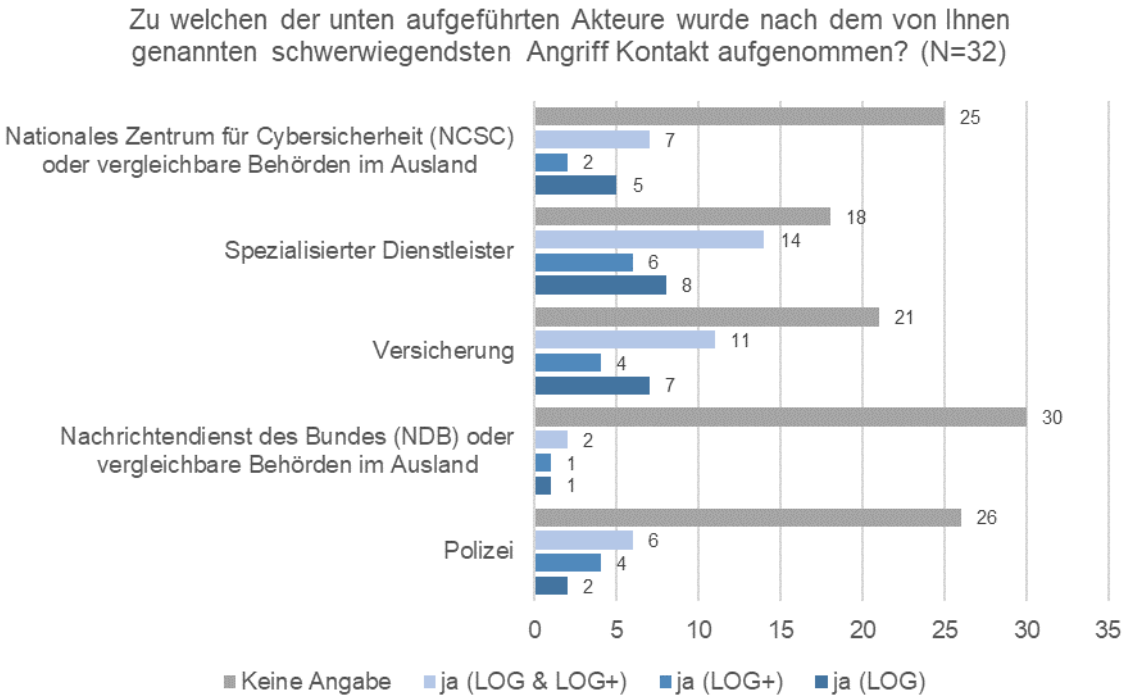


Abbildung 13: Kontaktaufnahme nach dem Angriff (B15)

IT-Sicherheitsmassnahmen

Technische IT-Sicherheitsmassnahmen

Bereits vor dem «schwerwiegendsten Angriff» erreichte ein Drittel der abgefragten Massnahmen einen Umsetzungsgrad von über 75%. Auffällig war, dass der Umsetzungsgrad des «Security Information and Event Management (SIEM)» mit 25.0%, der «Informationssicherheitsmanagementsysteme (ISMS)» mit 28.6% und die «Zwei-Faktor Authentifizierung» mit 53.6% nach den erfolgten Angriffen die grössten Steigerungen verzeichneten.

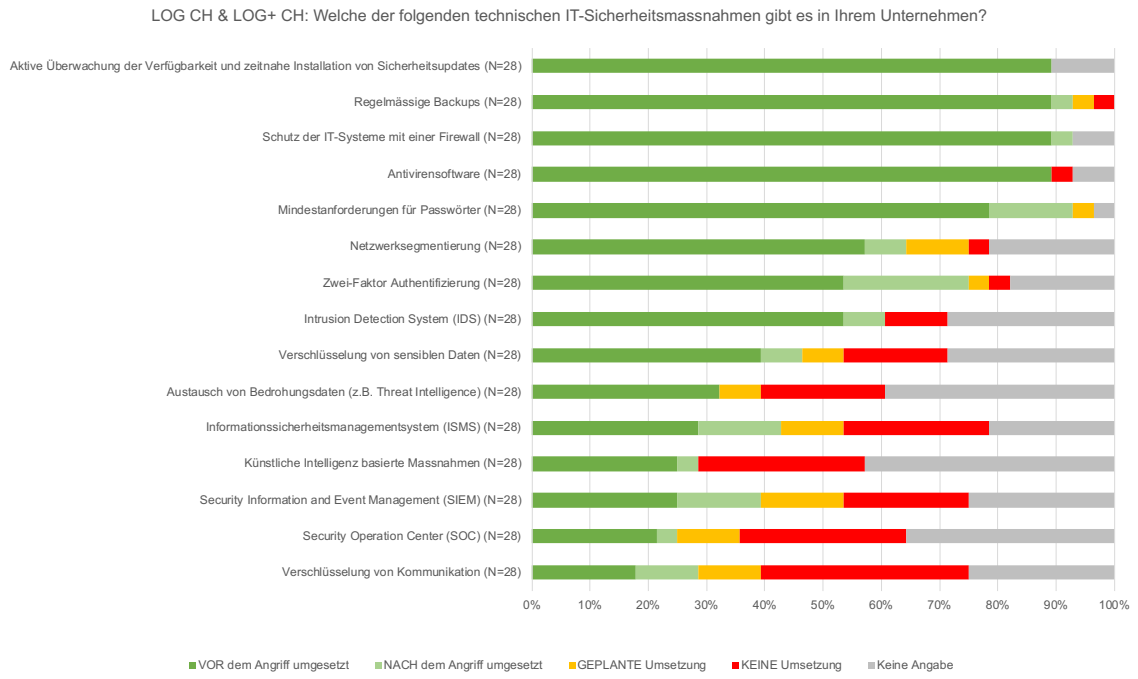


Abbildung 14: Technische IT-Sicherheitsmassnahmen (C0101)

Es gibt auch Unternehmen, die ihren IT-Grundschutz vernachlässigen und keine Umsetzung von «Zwei-Faktor Authentifizierung», «Netzwerksegmentierungen» «Antivirensoftware» oder «Regelmässigen Backups» planen.

Beteiligung an der Entdeckung des Angriffes

Die Frage, welche technische IT-Sicherheitsmassnahme beim «schwerwiegendsten Angriff» zur Entdeckung des Vorfalls beigetragen hat, zeigt, dass «Antivirensoftware», «Schutz der IT-Systeme mit einer Firewall» und «Intrusion Detection System» die ersten drei Plätze belegen.

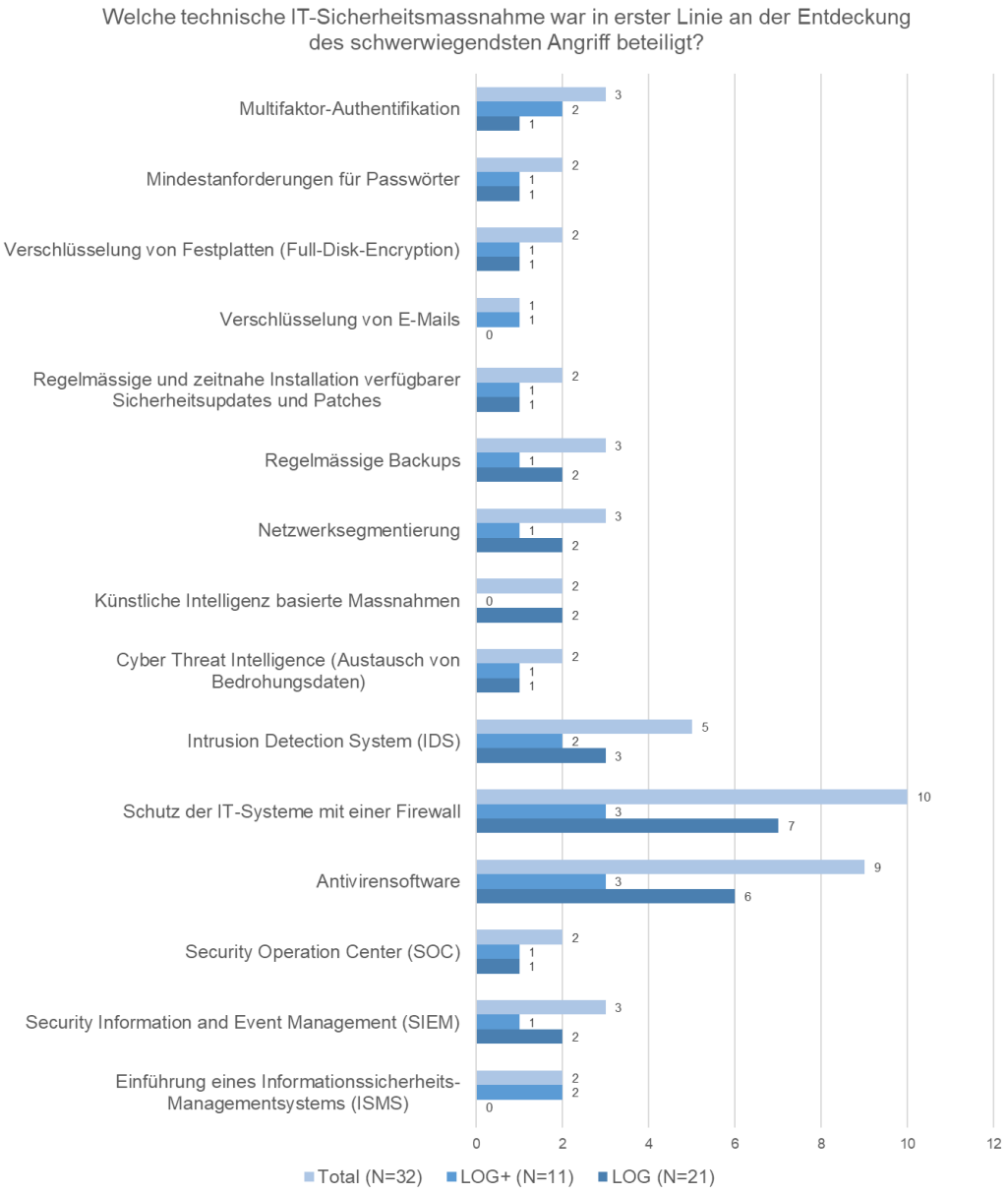


Abbildung 15: Beteiligte Massnahmen bei Entdeckung des Angriffes (C02)

Organisatorische IT-Sicherheitsmassnahmen

Die organisatorischen IT-Sicherheitsmassnahmen erreichen keine so hohen Umsetzungsgrade, wie die technischen Massnahmen, weisen jedoch eine höhere minimale Umsetzung auf. Auffällig ist, dass die Unternehmen angaben, nach dem Angriff folgende organisatorischen IT-Sicherheitsmassnahmen umgesetzt zu haben: «Risiko- und Schwachstellenanalysen (auch Pentest)» (plus 18.5%), «Schulungen zur ICT-Sicherheit für Mitarbeitende» (plus 14.8%), «Schriftliche Richtlinien zum Notfallmanagement» (plus 11.1%).

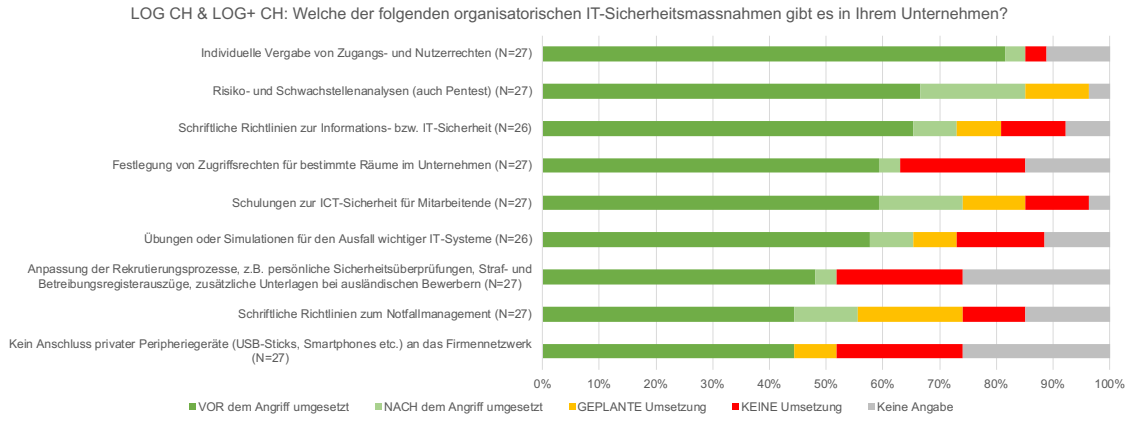


Abbildung 16: Organisatorische IT-Sicherheitsmassnahmen (C0102)

Durchschnittlicher Umsetzungsgrad der IT-Sicherheitsmassnahmen

Trotz der unterschiedlichen Umsetzungsgrade der technischen und organisatorischen IT-Sicherheitsmassnahmen, zeigen sich sehr vergleichbare Durchschnittswerte in den einzelnen Kategorien.

Durchschnittlicher Umsetzungsgrad der IT-Sicherheitsmassnahmen

	VOR dem Angriff	**NACH** dem Angriff	**Nach** Umsetzung der geplanten Massnahmen	**KEINE** Umsetzung	Keine Angabe
Technische IT-Sicherheitsmassnahmen (N=28)	59.7%	67.2%	72.7%	11.0%	16.2%
Organisatorische IT-Sicherheitsmassnahmen (N=27)	58.5%	66.4%	73.5%	13.3%	13.2%

Tabelle 18: Durchschnittlicher Umsetzungsgrad der Massnahmen (C0101, C0102)

Reifegrad und Verbreitung der IT-Sicherheitsmassnahmen

Die 33 angegriffenen Unternehmen konnten die «vor oder nach einem Angriff» eingesetzten sowie «die geplanten IT-Sicherheitsmassnahmen» in Bezug auf Reife und Verbreitung bewerten. Die Reifegradskala[10] hatte vier Stufen, die Verbreitungsskala[11] drei Stufen. Pro IT-Sicherheitsmassnahme wurde die Anzahl Nennungen einer Stufe mit dem Wert dieser Stufe multipliziert und alle Stufen-Produkte einer IT-Sicherheitsmassnahme addiert (Summenprodukt). Dies ergab den globalen Reifegrad einer IT-Sicherheitsmassnahme. Die Verbreitung wurde analog berechnet.

Bei der Betrachtung des Reife- und Verbreitungsgrades der IT-Sicherheitsmassnahmen ist festzustellen, dass diese mehrheitlich korrelieren.

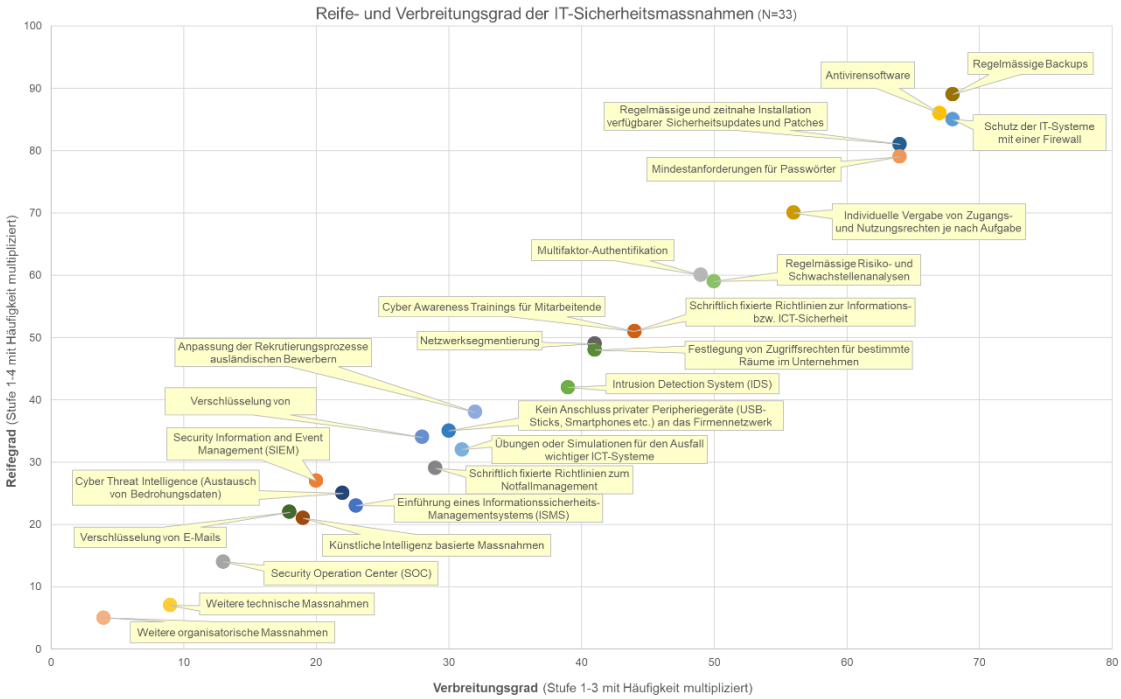


Abbildung 17: Reife-/Verbreitungsgrad der Massn. (m. Angriff) (C0501, C0502)

[10] 1 (Grundfunktionalität/-umfang); 2 (Erweiterte Funktionalität/Umfang); 3 (Grundfunktionalität und regelmässige Überprüfung/Optimierung); 4 (Erweiterte Funktionalität und regelmässige Überprüfung/Optimierung)

[11] 1 (stark begrenzte Verbreitung im Unternehmen); 2 (teilweise verbreitet im Unternehmen); 3 (weitgehende Verbreitung im Unternehmen)

4.1.8 Von Cyberangriffen nicht betroffene Unternehmen

Rangfolge der «schwerwiegendsten Folgen»

Von den 40 Unternehmen, die bis zur Umfrage noch nicht Opfer eines Angriffes geworden waren, erstellten 22 eine Rangfolge der «schwerwiegendsten Folgen» und stuften dabei die «Betriebsunterbrechung» als «schwerwiegendste Folge» ein.

Welches wären die schwerwiegendsten Folgen für Ihr Unternehmen, falls es Opfer eines Cyberangriffes würde? Bitte wählen Sie die 5 schwerwiegendsten Folgen aus und bringen Sie diese in eine Rangfolge. (N=22)

Rang	Folge
1	Betriebsunterbrechung (d.h. vollständiger oder teilweiser Ausfall der Produktion und Administration)
2	Ausfall der Informatik
	Kosten für Sofortmassnahmen zur Abwehr und Aufklärung
3	Negative Auswirkung auf die Geschäftsentwicklung
	Reputationsverluste/Negative Presse
4	Kosten für Wiederherstellung von Daten oder IT-Infrastruktur (Hardware und Software)
5	Kundenverluste/Auftragsverluste
	Verlust von personenbezogenen Daten, z.B. Kundendaten, Daten von Mitarbeitenden

Abbildung 18: Rangfolge der schwerwiegendsten Folgen (B03)

Existierende technische IT-Sicherheitsmassnahmen

Die existierenden technischen IT-Sicherheitsmassnahmen zeigen ein anderes Bild als in Kapitel 4.1.7. So haben die nicht betroffenen Unternehmen zu 96.7% ein «regelmässiges Backup», sind zu 90% von einer «Firewall» und «Antivirensoftware» geschützt und spielen zu 83.3% «regelmässig Sicherheitsupdates und Patches» ein. Als weitere Massnahmen wurden noch je einmal «Webproxy» und «VPN» genannt. Erstaunlicherweise gibt es Unternehmen, die noch keine technischen IT-Sicherheitsmassnahmen umgesetzt haben.

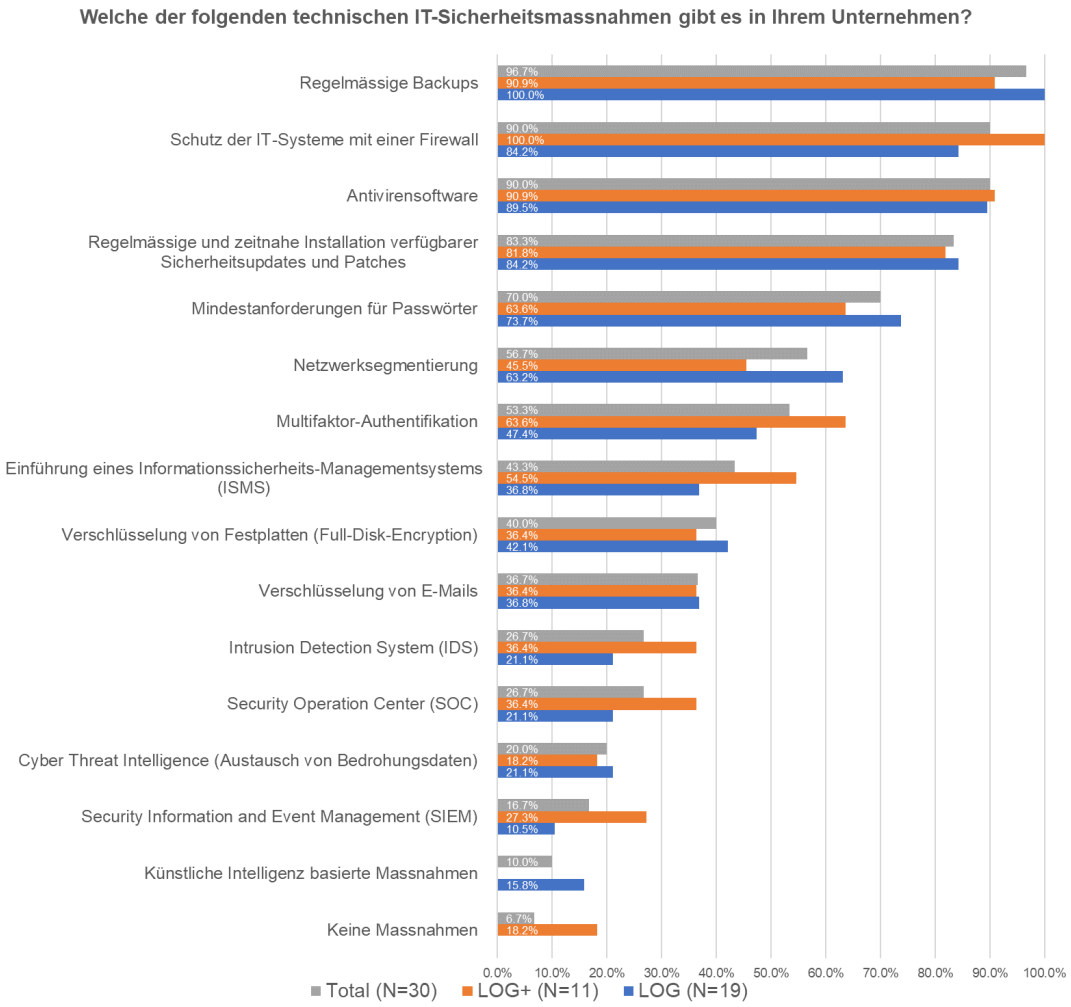


Abbildung 19: Existierende technische IT-Sicherheitsmassnahmen (C0301)

Geschätzter Nutzen der technischen IT-Sicherheitsmassnahmen

Der geschätzte Nutzen der sieben meistangewandten IT-Sicherheitsmassnahmen entspricht dem Umsetzungsgrad dieser Massnahmen. Den Nutzen von «Antivirensoftware» stufen erstaunlicherweise 10% als «eher klein» ein.

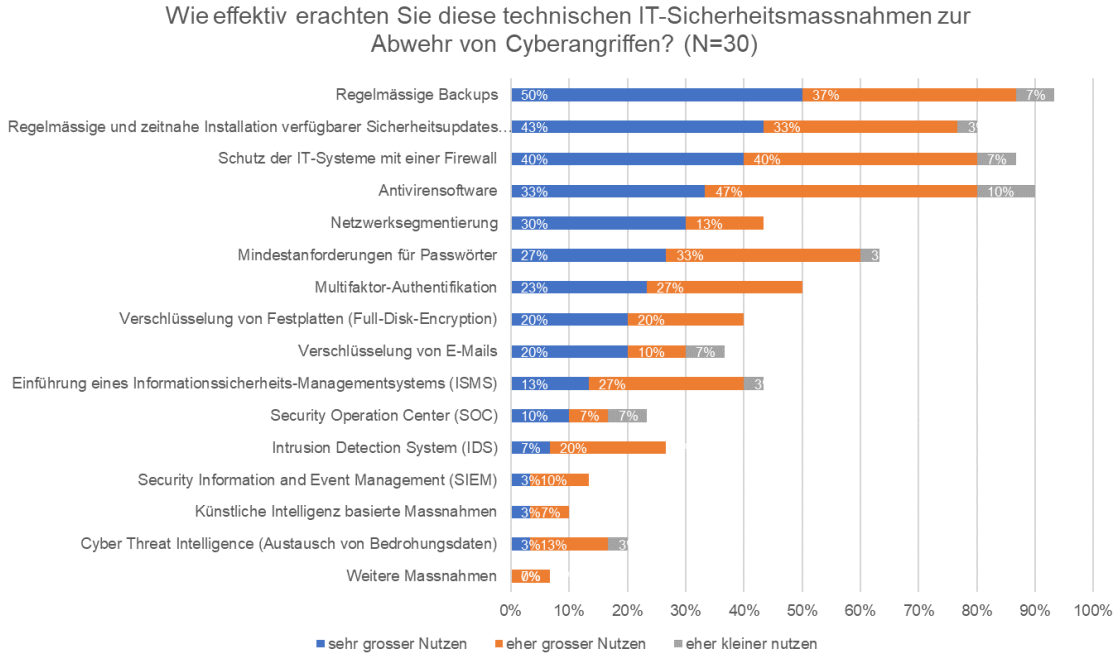


Abbildung 20: Geschätzter Nutzen der technischen IT-Sicherheitsmassnahmen (C04)

Existierende organisatorische IT-Sicherheitsmassnahmen

Zwei Drittel der nicht betroffenen Unternehmen führen «Cyber Awareness Trainings für Mitarbeitende» durch. Angegriffene Unternehmen hatten vor dem Angriff lediglich einen Wert von 59.3% erreicht. Als weitere Massnahmen wurden noch je einmal «Krisenmanagement» und «Versand von Test-Phishing E-Mails» genannt. Erstaunlicherweise gibt es Unternehmen, die noch keine organisatorischen IT-Sicherheitsmassnahmen umgesetzt haben.

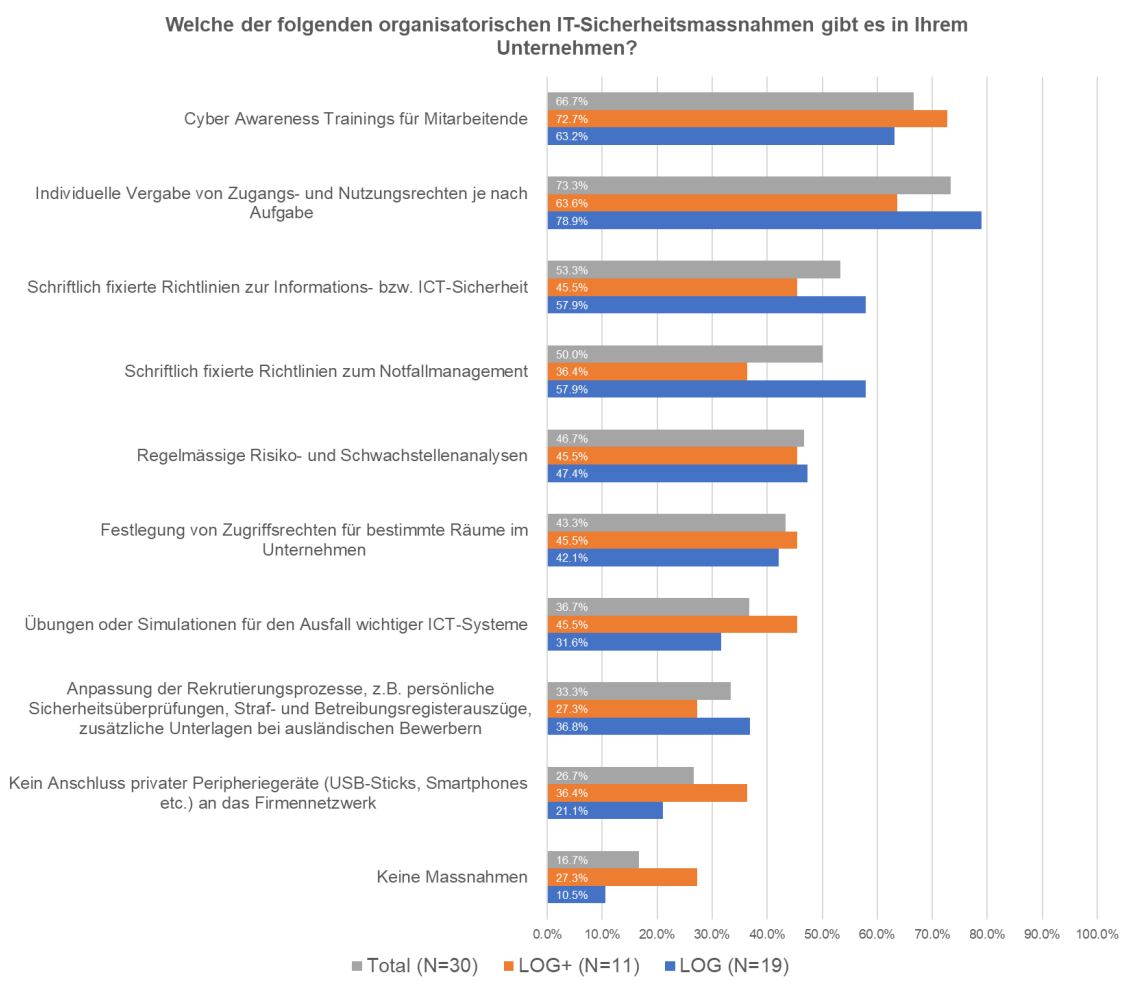


Abbildung 21: Existierende organisatorische IT-Sicherheitsmassnahmen (C0302)

Korrelation zwischen Betroffenheit und IT-Schutzmassnahmen

Eine Korrelation zwischen Betroffenheit und IT-Schutzmassnahmen lassen die vorliegenden Daten nicht nachweisen.

Beim qualitativen Vergleich der betroffenen und nicht betroffenen Unternehmen zeigt sich jedoch, dass die betroffenen Unternehmen vor dem Angriff aus technischer Sicht 18.8% seltener eine «verschlüsselte Kommunikation» verwendet und 14.8% seltener ein «Informationssicherheitsmanagementsystem (ISMS)» eingesetzt haben. Aus organisatorischer Sicht haben die nicht betroffenen Unternehmen 7.4% öfters «Schulungen zur ICT-Sicherheit für Mitarbeitende» durchgeführt und 5.6% öfters «schriftliche Richtlinien zum Notfallmanagement» ungesetzt.

LOG CH & LOG+ CH	Umsetzungsgrad angegriffener Unternehmen (N = 28)	Umsetzungsgrad **NICHT** angegriffener Unternehmen (N = 30)	Differenz
Verschlüsselung von Kommunikation	17.9%	36.7%	-18.8%
Informationssicherheitsmanagementsystem (ISMS)	28.6%	43.3%	-14.8%
Regelmässige Backups	89.3%	96.7%	-7.4%
Security Operation Center (SOC)	21.4%	26.7%	-5.2%
Verschlüsselung von sensiblen Daten	39.3%	40.0%	-0.7%
Antivirensoftware	89.3%	90.0%	-0.7%
Schutz der IT-Systeme mit einer Firewall	89.3%	90.0%	-0.7%
Zwei-Faktor Authentifizierung	53.6%	53.3%	0.2%
Netzwerksegmentierung	57.1%	56.7%	0.5%
Aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates	89.3%	83.3%	6.0%
Security Information and Event Management (SIEM)	25.0%	16.7%	8.3%
Mindestanforderungen für Passwörter	78.6%	70.0%	8.6%
Intrusion Detection System (IDS)	53.6%	26.7%	26.9%

Tabelle 19: Vergleich umgesetzte techn. Massnahmen m./o. Angriff (C0101, C0301)

LOG CH & LOG+ CH	Umsetzungsgrad angegriffener Unternehmen (N = 28)	Umsetzungsgrad **NICHT** angegriffener Unternehmen (N = 30)	Differenz
Schulungen zur ICT-Sicherheit für Mitarbeitende	59.3%	66.7%	-7.4%
Schriftliche Richtlinien zum Notfallmanagement	44.4%	50.0%	-5.6%
Individuelle Vergabe von Zugangs- und Nutzerrechten	81.5%	73.3%	8.1%
Schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit	65.4%	53.3%	12.1%
Anpassung der Rekrutierungsprozesse (z.B. persönliche Sicherheitsüberprüfungen)	48.1%	33.3%	14.8%
Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen	59.3%	43.3%	15.9%
Kein Anschluss privater Peripheriegeräte (z.B. USB-Sticks) an das Firmennetzwerk	44.4%	26.7%	17.8%
Risiko- und Schwachstellenanalysen (auch Pentest)	66.7%	46.7%	20.0%
Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme	57.7%	36.7%	21.0%

Tabelle 20: Vergleich umgesetzte org. Massnahmen m./o. Angriff (C0101, C0301)

Reifegrad und Verbreitung der existierenden IT-Sicherheitsmassnahmen

Die nicht angegriffenen Unternehmen konnten die «vorhandenen IT-Sicherheitsmassnahmen» in Bezug auf Reife und Verbreitung bewerten. Die Reifegradskala[12] hatte vier Stufen, die Verbreitungsskala[13] drei Stufen. Pro IT-Sicherheitsmassnahme wurde die Anzahl Nennungen einer Stufe mit dem Wert dieser Stufe multipliziert und alle Stufen-Produkte einer IT-Sicherheitsmassnahme addiert (Summenprodukt). Dies ergab den globalen Reifegrad einer IT-Sicherheitsmassnahme. Die Verbreitung wurde analog berechnet.

Bei der Betrachtung des Reife- und Verbreitungsgrades der existierenden IT-Sicherheitsmassnahmen bei nicht angegriffenen Unternehmen konnte festgestellt werden, dass diese mehrheitlich korrelieren.

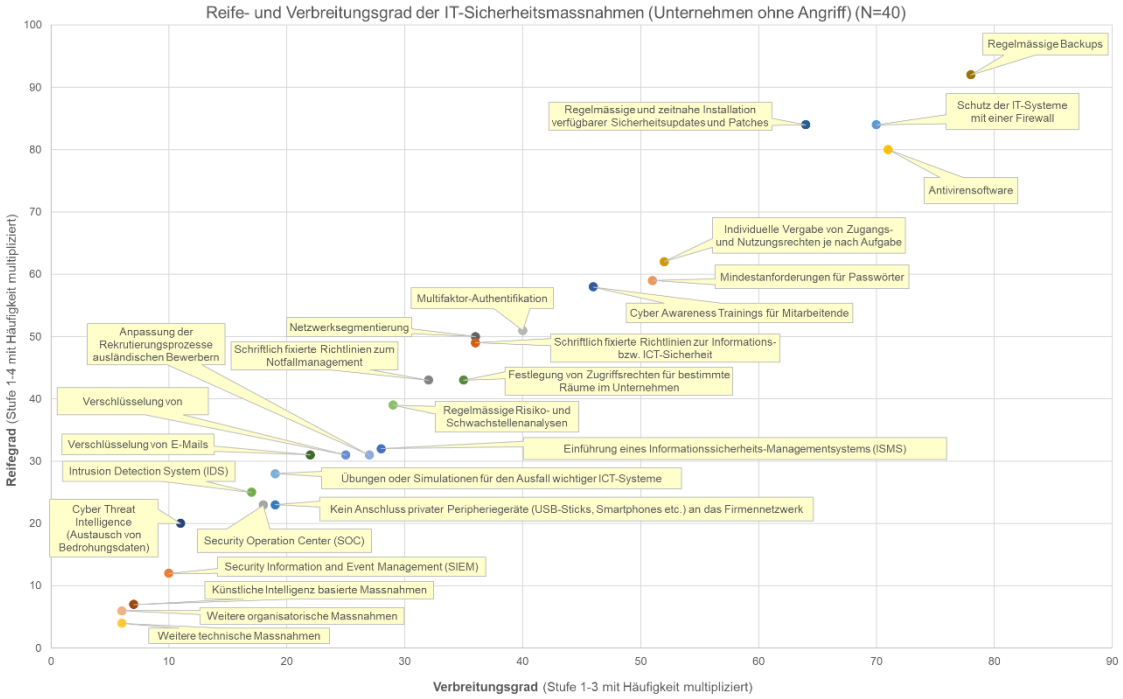


Abbildung 22: Reife-/Verbreitungsgrad der Massnahmen (o. Angriff)

[12] 1 (Grundfunktionalität/-umfang); 2 (Erweiterte Funktionalität/Umfang); 3 (Grundfunktionalität und regelmässige Überprüfung/Optimierung); 4 (Erweiterte Funktionalität und regelmässige Überprüfung/Optimierung)

[13] 1 (stark begrenzte Verbreitung im Unternehmen); 2 (teilweise verbreitet im Unternehmen); 3 (weitgehende Verbreitung im Unternehmen)

4.1.9 Cyberversicherung

22 Unternehmen gaben an, über eine Cyberversicherung zu verfügen und 10 davon mussten bestimmte IT-Sicherheitsstandards nachweisen, um die Versicherung abzuschliessen. Fünf Unternehmen, die keine Versicherung abgeschlossen haben, gaben als Grund das Preis-Leistungs-Verhältnis an. Da die Stichprobengrösse sehr klein ist, können hier keine verallgemeinernden Schlüsse gezogen werden.

<table>
<tr><td colspan="5">Haben Sie eine Versicherung gegen Informationssicherheitsverletzungen (Cyberversicherung)? (N = 56)</td></tr>
<tr><td colspan="2">ja = 22</td><td colspan="2">nein = 11</td><td rowspan="3">keine Angabe = 23</td></tr>
<tr><td colspan="2">Mussten zum Abschluss der Cyberversicherungen bestimmte IT-Sicherheitsstandards nachgewiesen werden?</td><td colspan="2">Warum hat Ihr Unternehmen keine Cyberversicherung?</td></tr>
<tr><td>ja = 10</td><td>nein = 3</td><td>Wir haben uns damit noch nicht beschäftigt
1</td><td>Das Preis-Leistungs-Verhältnis stimmt nicht
5</td><td>Sonstiger Grund
4</td></tr>
</table>

Tabelle 21: Verbreitung von Cyberversicherungen (C07, C08, C09)

4.1.10 Einschätzung des Risikobewusstseins

Das Risikobewusstsein der Belegschaft wird mehrheitlich positiv wahrgenommen. Insbesondere den Geschäftsführenden wird klar attestiert, dass sie sich «der Risiken bewusst sind und sich an die Vorgaben halten».

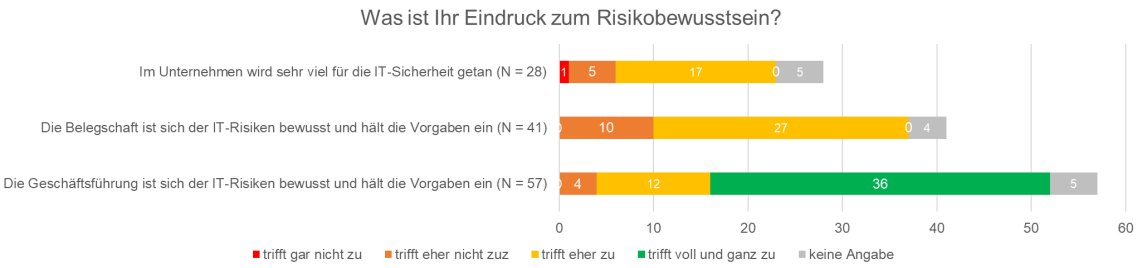


Abbildung 23: Einschätzungen zum Risikobewusstsein (C10)

4.1.11 IT-Sicherheitsschulungen

Die organisatorische IT-Sicherheitsmassnahme «Cyber Awareness Trainings» wurde bei angegriffenen (74,1%[14]), wie auch nicht angegriffenen (66.7%) Unternehmen umgesetzt. Die weiterführenden Fragen zu den Schulungsangeboten zeigen jedoch, dass ein beträchtlicher Teil der Antworten auf der negativen Seite liegen und keine der Fragen Zustimmung in der Kategorie «trifft voll und ganz zu» erhalten hat.

[14] inkl. der nach dem Angriff umgesetzte Massnahmen

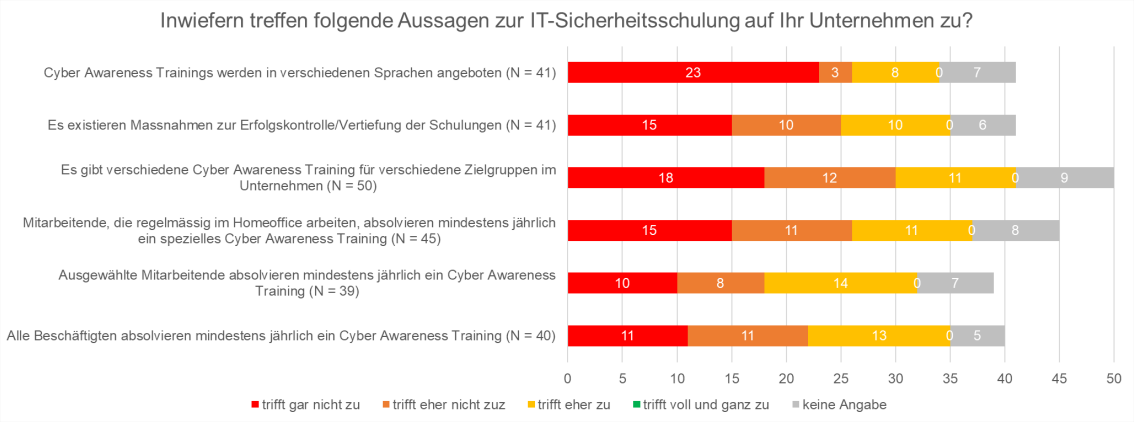


Abbildung 24: Einschätzungen zum Thema IT-Sicherheitsschulungen (C11)

4.2 Vergleich der Ergebnisse mit Studien aus Deutschland und der Schweiz

Es muss an dieser Stelle darauf hingewiesen werden, dass die nachfolgenden Analysen auf sehr kleinen Stichproben basieren und die verglichenen Zeiträume der Studien versetzt sind, die in den Fragen betrachteten Zeiträume unterschiedlich weit zurückreichen und vor, in oder nach der COVID-19-Pandemie liegen (siehe Abbildung 25).

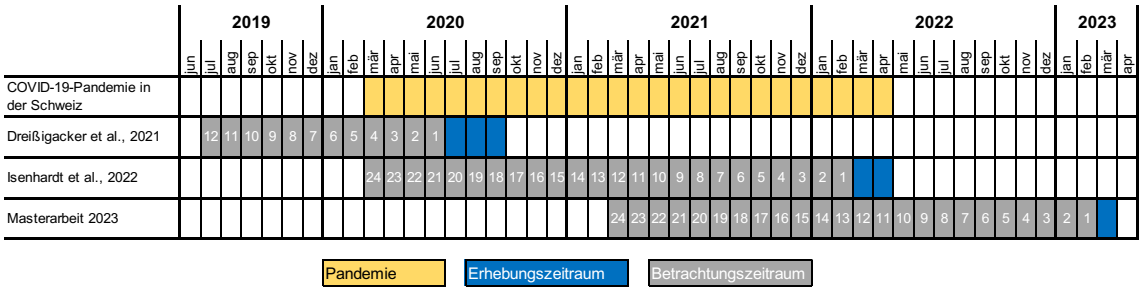


Abbildung 25: Zeitliche Abfolge der verschiedenen Studien

Ferner ist zu beachten, dass die im Rahmen dieser Arbeit durchgeführte Online-Umfrage, wie auch diejenige von Isenhardt et al. (2022), auf Gelegenheitsstichproben basieren, während die Umfragen von Dreißigacker et al. (2020, 2021) Zufallsstichproben nutzten. Es muss davon ausgegangen werden, dass die Motivation eines Unternehmens an einer Online-Umfrage teilzunehmen, mit der individuellen Erfahrung im Themengebiet Cybersecurity/-crime eine Rolle spielt. Die gemachten Aussagen können deshalb nur bedingt verallgemeinert werden.

4.2.1 Vorgehensweise

Für die vergleichenden Analysen wurden zuerst die Daten von Dreißigacker et al. (2021) für die MEM- und Logistikbranche aufbereitet (Abbildung 26, Schritt 1 und 2). Anschliessend wurden die Branchen anhand der in Kapitel 4.2.2 dargestellten vergleichbaren Fragestellungen miteinander verglichen (Abbildung 26, Schritt 3). Um zu ermitteln, ob sich die Situation in Deutschland zu derjenigen in der Schweiz unterscheidet, wurden anschliessend die MEM- und die Logistikbranchen beider Länder anhand dieser Fragestellungen verglichen (Abbildung 26, Schritt 4 und 5). Um auch beurteilen zu können, inwiefern sich die die MEM- und die Logistikbranchen in der Schweiz unterscheiden, wurden auch diese Branchen anhand vergleichbarer Fragestellungen verglichen (Abbildung 26, Schritt 6).

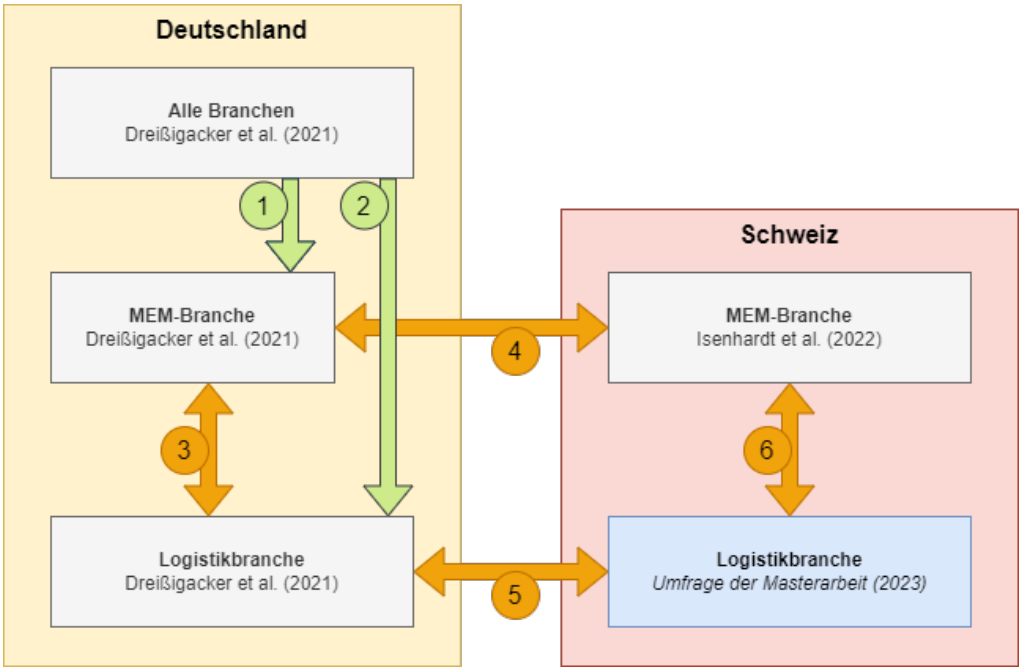


Abbildung 26: Übersicht der Schritte der vergleichenden Analysen

4.2.2 Vergleichbare Fragestellungen

Die über alle drei Umfragen[15] hinweg vergleichbaren Fragestellungen werden nachfolgend aufgeführt und in Kapitel 4.2 weiter analysiert. Die exakten Fragestellungen mit den dazugehörenden Antwortoptionen können dem Fragebogen im Anhang entnommen werden.

Fragen zu Cyberangriffen

- *B01) War Ihr Unternehmen jemals von einem oder mehreren der unten aufgeführten Cyberangriffe betroffen? …*
- *B02) Wenn ja, wie häufig in den letzten 24 Monaten vor der Befragung?*
- *B04) Welcher dieser Angriffe war aus Ihrer Sicht der «schwerwiegendste»?*
- *B07) Gab es bei diesem «schwerwiegendsten Angriff» eine Lösegeldforderung?*
- *B12) Bitte geben Sie an, welche Kosten durch den von Ihnen angegebenen «schwerwiegendsten Angriff» entstanden sind.*
- *B13) Waren bei dem genannten «schwerwiegendsten Angriff» die folgenden Daten betroffen? …*
- *B16) Bitte ergänzen Sie: Der durch den «schwerwiegendsten Angriff» erfolgte Schaden...*

Fragen zu IT-Sicherheitsmassnahmen

- *C0101) Welche der folgenden technischen IT-Sicherheitsmassnahmen gibt es in Ihrem Unternehmen? Geben Sie bitte gegebenenfalls an, ob die Massnahme erst nach dem «schwerwiegendsten Angriff» der letzten 24 Monate eingeführt wurde.*
- *C0102) Welche der folgenden organisatorischen IT-Sicherheitsmassnahmen gibt es in Ihrem Unternehmen? Geben Sie bitte gegebenenfalls an, ob die Massnahme erst nach dem «schwerwiegendsten Angriff» der letzten 24 Monate eingeführt wurde.*

[15] Dreißigacker et al. (2021), Isenhardt et al. (2022), Online-Umfrage dieser Masterarbeit

4.2.3 Nutzbare Datensätze der deutschen Studie

Von den 601 Antworten der Folgebefragung (Dreißigacker et al., 2021) konnten 97 der MEM-[16] und 95 der Logistikbranche[17] zugeordnet werden.

Wirtschaftszweig Gruppe

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	MEM	97	16.1	50.5	50.5
	LOG	95	15.8	49.5	100.0
	Gesamt	192	31.9	100.0	
Fehlend	System	409	68.1		
Gesamt		601	100.0		

Tabelle 22: Nutzbare Datensätze von Dreißigacker et al. (2021)

Branchencode (WZ 2008 - Adresssample) * Wirtschaftszweig Gruppe Kreuztabelle

Anzahl

		Wirtschaftszweig Gruppe MEM	LOG	Gesamt
Branchencode (WZ 2008 - Adresssample)	Metallerzeugung u.-bearbeitung	2	0	2
	H.v.Metallerzeugnissen	26	0	26
	H.v.DV-Gerät.,elektron. u. opt.Erzeugn.	14	0	14
	H.v.elektr.Ausrüstg.	12	0	12
	Maschinenbau	36	0	36
	H.v.Kraftwagen u. Kraftwagenteilen	5	0	5
	Sonstiger Fahrzeugbau	2	0	2
	Wasserversorgung	0	2	2
	Abwasserentsorgung	0	3	3
	Sammlung,Abfallbeseiti-gung,Rückgewinnung	0	6	6
	Kfz-Handel;Instandh.u. Rep.v.Kfz	0	6	6
	Großhandel (oh.Kfz)	0	40	40
	Eh.(oh.Handel m.Kfz)	0	10	10
	Landverkehr;Transport i. Rohrleitungen	0	17	17
	Schifffahrt	0	2	2
	Lagerei;sonst.Dienst-leistg.f.d.Verkehr	0	8	8
	Post-,Kurier-u. Expressdienste	0	1	1
Gesamt		97	95	192

Tabelle 23: Wirtschaftszweig Gruppen von Dreißigacker et al. (2021)

[16] Wirtschaftszweige: 24, 25, 26, 27, 28, 29, 30, 33. Dies entspricht der Definition von Nicolas Stephan, Ressortleiter Volkswirtschaft, Swissmem vom 09.01.2023. Der Bereich 325 wurde ausgeschlossen, da nicht dieser im vorliegenden Datensatz nicht selektierbar ist.

[17] Wirtschaftszweige: 36, 37, 38, 39, 45, 46, 47, 49, 50, 51, 52, 53

4.2.4 Vergleich der deutschen MEM- und Logistikbranche

Betroffenheit

Die Unternehmen der MEM- und Logistikbranche zeigten eine ähnliche Betroffenheit von Cyberangriffen, wobei auffällig war, dass die MEM-Branche mit 47.4% «Phishing-Angriffen» häufiger angegriffen wurde als die Logistikbranche mit 40.0%. Die Angriffe mit «Ransomware» fanden in der MEM-Branche mit 23.7% ebenfalls öfter statt als in der Logistikbranche mit 14.7%. Die Logistikbranche hingegen war mit 12.6% öfter von «(D)DoS-Attacken» betroffen als die MEM-Branche mit 3.1%.

Bezogen auf die letzten 12 Monate:
Von welchen Angriffsarten war Ihr Unternehmen betroffen und musste aktiv reagieren?

Wirtschaftszweig Gruppe	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen	Sonstige Schadsoftware - z.B. Viren, Würmer, Trojaner	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware)	((D)DoS) Attacke, die auf eine Überlastung von Web- oder E-Mail-Server zielte	Defacing-Attacke, die das Ziel hatte, unbefugt Webinhalte des Unternehmens zu verändern	CEO-Fraud, wobei eine Führungspersönlichkeit des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitern zu bewirken	Phishing, wobei Mitarbeiter mit echt aussehenden E-Mails oder Webseiten getäuscht wurden, um z.B. sensible Unternehmensdaten zu erlangen	Sonstiger Cyberangriff
MEM DE (N = 97)	23	17	35	2	3	0	23	46	0
	23.7%	17.5%	36.1%	2.1%	3.1%	0.0%	23.7%	47.4%	0.0%
LOG DE (N = 95)	14	16	31	1	12	4	20	38	1
	14.7%	16.8%	32.6%	1.1%	12.6%	4.2%	21.1%	40.0%	1.1%

Tabelle 24: Betroffenheit durch Cyberangriffe (MEM DE, LOG DE)

Häufigkeit

Die Häufigkeit der Angriffe entspricht dem Bild der Betroffenheit. So waren «Phishing-Angriffe», gefolgt von «Angriffen mit sonstiger Schadsoftware» und «Spyware-Angriffen», die häufigsten drei Angriffsarten in beiden Branchen.

Häufigkeit der Betroffenheit durch einzelne Angriffsarten (Anzahl)	MEM DE							LOG DE						
	In den letzten 12 Monaten vor der Befragung							In den letzten 12 Monaten vor der Befragung						
	N =	0 mal oder leer	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	97	74	19	3			1	95	83	8	3			1
Spyware-Angriff (um zur Daten auszuspähen)	97	81	4	2	2	3	5	95	83	4	2	1	1	4
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	97	66	9	4	4	4	10	95	67	9	6	3	3	7
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	97	95	1		1			95	94	1				
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	97	94	1	2				95	84	5		1	3	2
Defacing-Attacke (um Inhalte von Websites zu verändern)	97	97						95	91	3				1
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	97	74	13	4	3	2	1	95	76	11	4	1	1	2
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	97	55	5	2	9	9	17	95	61	7	4	5	4	14

Tabelle 25: Häufigkeit der Angriffe absolut (MEM DE, LOG DE)

Häufigkeit der Betroffenheit durch einzelne Angriffsarten (in Prozent)	MEM DE							LOG DE						
	In den letzten 12 Monaten vor der Befragung							In den letzten 12 Monaten vor der Befragung						
	N =	0 mal oder leer	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	97	76.3%	19.6%	3.1%			1.0%	95	87.4%	8.4%	3.2%			1.1%
Spyware-Angriff (um zur Daten auszuspähen)	97	83.5%	4.1%	2.1%	2.1%	3.1%	5.2%	95	87.4%	4.2%	2.1%	1.1%	1.1%	4.2%
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	97	68.0%	9.3%	4.1%	4.1%	4.1%	10.3%	95	70.5%	9.5%	6.3%	3.2%	3.2%	7.4%
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	97	97.9%	1.0%		1.0%			95	98.9%	1.1%				
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	97	96.9%	1.0%	2.1%				95	88.4%	5.3%		1.1%	3.2%	2.1%
Defacing-Attacke (um Inhalte von Websites zu verändern)	97	100.0%						95	95.8%	3.2%				1.1%
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	97	76.3%	13.4%	4.1%	3.1%	2.1%	1.0%	95	80.0%	11.6%	4.2%	1.1%	1.1%	2.1%
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	97	56.7%	5.2%	2.1%	9.3%	9.3%	17.5%	95	64.2%	7.4%	4.2%	5.3%	4.2%	14.7%

Tabelle 26: Häufigkeit der Angriffe in Prozent (MEM DE, LOG DE)

«Schwerwiegendster Angriff»

Als «schwerwiegendste Cyberangriffe» wurden in beiden Branchen «Phishing» genannt (MEM: 16.5%, LOG 10.5%). In der MEM-Branche folgen dann Angriffe mit «Ransomware» (10.3%) und «CEO-Fraud» (6.2%) und in der Logistikbranche Angriffe mit «sonstiger Schadsoftware» (7.4%), «Ransomware» (6.3%) und «CEO-Fraud» (6.3%).

Welcher Cyberangriff der letzten 12 Monate war der schwerwiegendste?
(Mehrfachantwort bei einer Kombination von mehreren Angriffsarten möglich)

Wirtschaftszweig Gruppe	Ransomware-Angriff (um Daten zu verschlüsseln)	Spyware-Angriff (um zur Daten auszuspähen)	Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	Manuelles Hacking (um Soft- und Hardware zu manipulieren)	(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	Defacing-Attacke (um Inhalte von Websites zu verändern)	CEO-Fraud (Vortäuschung einer Führungspersönlichkeit)	Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	Sonstiger Cyberangriff	Weiss nicht	Keine Angabe
MEM DE (N = 97)	10	2	3	2	0	0	6	16	0	7	6
	10.3%	2.1%	3.1%	2.1%	0.0%	0.0%	6.2%	16.5%	0.0%	7.2%	6.2%
LOG DE (N = 95)	6	3	7	0	2	1	6	10	0	7	7
	6.3%	3.2%	7.4%	0.0%	2.1%	1.1%	6.3%	10.5%	0.0%	7.4%	7.4%

Tabelle 27: Schwerwiegendster Cyberangriff (MEM DE, LOG DE)

Lösegeldforderung

Cyberangriffe, die zu einer Erpressung mit Lösegeldforderung führten, traten in beiden Branchen sehr selten auf. Die mit «Ja» beantworteten Fälle lagen bei etwa 5%, wobei die Stichprobengrösse sehr klein ist und keine weiteren Rückschlüsse zulässt.

Gab es bei diesem Angriff eine Lösegeld-Forderung?

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
MEM DE (N = 97)	Ja	4	4.1%
	Nein	42	43.3%
	Weiss nicht	3	3.1%
	Keine Angabe	48	49.5%
LOG DE (N= 95)	Ja	5	5.3%
	Nein	38	40.0%
	Weiss nicht	2	2.1%
	Keine Angabe	50	52.6%

Tabelle 28: Lösegeldforderungen (MEM DE, LOG DE)

Durch Angriff verursachte Kosten

Bei der Angabe, welche Kosten durch den «schwerwiegendsten Angriff» entstanden sind, unterscheiden sich die Branchen stark beim Mittelwert und Median der Kosten.

Wie hoch waren die materiellen Schäden (schätzungsweise) für diese Position in Euro?

Wirtschaftszweig Gruppe			
	MEM DE (N = 97)	Antworten	26
		Mittelwert	155'555
		Median	1'775
		Std.-Abweichung	743'604
		Spannweite	3'799'999
		Minimum	1
		Maximum	3'800'000
	LOG DE (N = 95)	Antworten	23
		Mittelwert	4'561
		Median	1'000
		Std.-Abweichung	10'513
		Spannweite	44'950
		Minimum	50
		Maximum	45'000

Tabelle 29: Durch Angriffe verursachte Kosten (MEM DE, LOG DE)

Bei genauerer Betrachtung der hohen Kosten in der MEM-Branche fällt auf, dass dies auf einzelne Ereignisse zurückzuführen ist. So flossen in einem Fall in der MEM-Branche sehr hohe Gelder ab (€ 3.8 Mio.). Bereinigt um dieses Ereignis ist der Mittelwert in der

MEM-Branche (€ 9'777.64) immer noch um Faktor 2.1 höher als in der Logistikbranche (€ 4'560.87).

Bei Betrachtung der Mittelwerte und Mediane der einzelnen Positionen fällt auf, dass diese (mit Ausnahme der bereits diskutierten abgeflossenen Gelder) in sehr ähnlichem Rahmen liegen.

Wie hoch waren die materiellen Schäden

		Wirtschaftszweig Gruppe	
		MEM DE (N = 97)	LOG DE (N = 95)
Kosten durch Externe Beratung (z.B. IT-Dienstleister, Rechtsberatung)	Antworten	10	11
	Summe	75'000	28'950
	Mittelwert	7'500	2'895
	Median	1'750	1'000
	Minimum	300	50
	Maximum	50'000	20'000
Abgeflossene Gelder	Antworten	3	2
	Summe	3'881'000	41'000
	Mittelwert	1'293'667	20'500
	Median	80'000	20'500
	Minimum	1'000	1'000
	Maximum	3'800'000	40'000
Wiederbeschaffung/ Wiederherstellung von Soft- oder Hardware (keine Personalkosten)	Antworten	2	6
	Summe	3'090	7'050
	Mittelwert	1'545	1'410
	Median	1'545	1'500
	Minimum	90	350
	Maximum	3'000	2'500
Personalkosten für die Behebung des Problems (Abwehr & Aufklärung)	Antworten	22	17
	Summe	65'550	23'350
	Mittelwert	3'278	1'374
	Median	500	500
	Minimum	200	150
	Maximum	20'000	8'000
Betriebsunterbrechung/ Umsatzverlust (z.B. durch Mitarbeiter, die nicht arbeiten konnten)	Antworten	5	5
	Summe	19'800	4'550
	Mittelwert	4'950	910
	Median	4'500	1'000
	Minimum	800	50
	Maximum	10'000	2'000

Tabelle 30: Durch Cyberangriff verursachte Einzelkosten (MEM DE, LOG DE)

Betroffene Daten

Die durch den «schwerwiegendsten Angriff» betroffen Daten sind im Bereich der Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes etc.) in der MEM-Branche mit 17.8% stärker betroffen als in der Logistikbranche mit 10.0%.

Waren durch den Angriff folgende Daten betroffen?

Wirtschaftszweig Gruppe		Personenbezogene Daten		Strategie-, Vertriebs- und Finanzinformationen (z.B. Preislisten, Sanierungspläne, Akquisitionen, Finanz- und Rechnungswesendaten)		Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes etc.)		Sonstige wichtige Daten	
		Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent
MEM DE	Ja	6	13.3	5	11.4	8	17.8	-	-
	Nein	39	86.7	39	88.6	37	82.2	40	100.0
	N	**45**	**100.0**	**44**	**100.0**	**45**	**100.0**	**40**	**100.0**
LOG DE	Ja	4	10.0	3	7.5	4	10.0	2	5.7
	Nein	36	90.0	37	92.5	36	90.0	33	94.3
	N	**40**	**100.0**	**40**	**100.0**	**40**	**100.0**	**35**	**100.0**

Tabelle 31: Betroffene Daten (MEM DE, LOG DE)

Folgen des «schwerwiegendsten Angriffes»

Die Folgen des «schwerwiegendsten Angriffs» zeigen in beiden Branchen eine unterschiedliche Verteilung. In der Logistikbranche traten 23.8% «kurz- und mittelfristig» behebbare Schäden auf, in der MEM-Branche hingegen lediglich 8.3%. Die Mehrheit in der MEM-Branche verzeichnete mit 89.6% «keinen derartigen Schaden». In der Logistikbranche waren dies 76.2%.

Wie schwerwiegend schätzen Sie die verursachten Schäden dieses Angriffes insgesamt ein? - Nicht-materieller Schaden (z.B. Reputationsverlust oder Wettbewerbsnachteil)

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
MEM DE (N = 48)	Kein derartiger Schaden	43	89.6%
	Kurzfristig / gering	4	8.3%
	Mittelfristig/ deutlich spürbar	0	0.0%
	Bestandsgefährdend	1	2.1%
LOG DE (N = 42)	Kein derartiger Schaden	32	76.2%
	Kurzfristig / gering	9	21.4%
	Mittelfristig/ deutlich spürbar	1	2.4%
	Bestandsgefährdend	0	0.0%

Tabelle 32: Nicht-materieller Schaden (MEM DE, LOG DE)

Technische IT-Sicherheitsmassnahmen

Bei den eingesetzten technischen IT-Sicherheitsmassnahmen zeigen beide Branchen eine ähnliche Verteilung. «Regelmässige Backups», «Schutz der IT-Systeme mit einer Firewall» und «Antivirensoftware» wurden als technische IT-Sicherheitsmassnahmen in beiden Branchen konsequent eingesetzt.

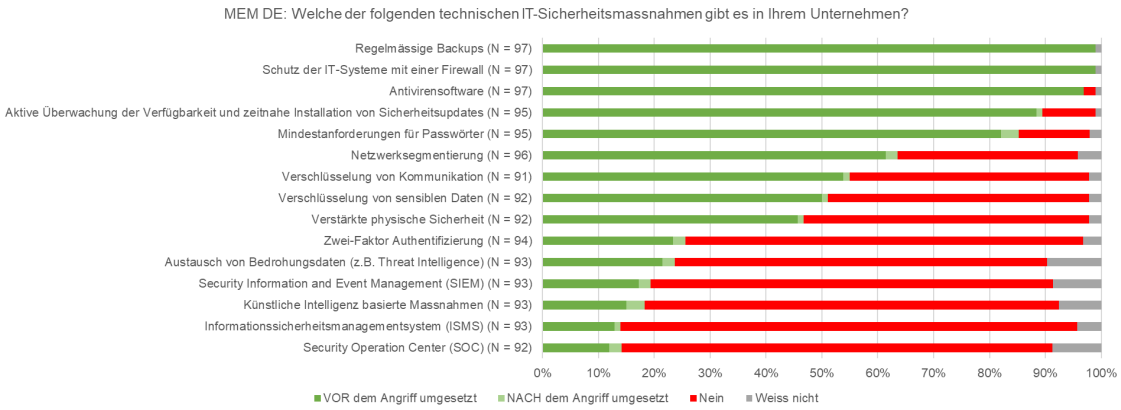


Abbildung 27: Technische IT-Sicherheitsmassnahmen (MEM DE)

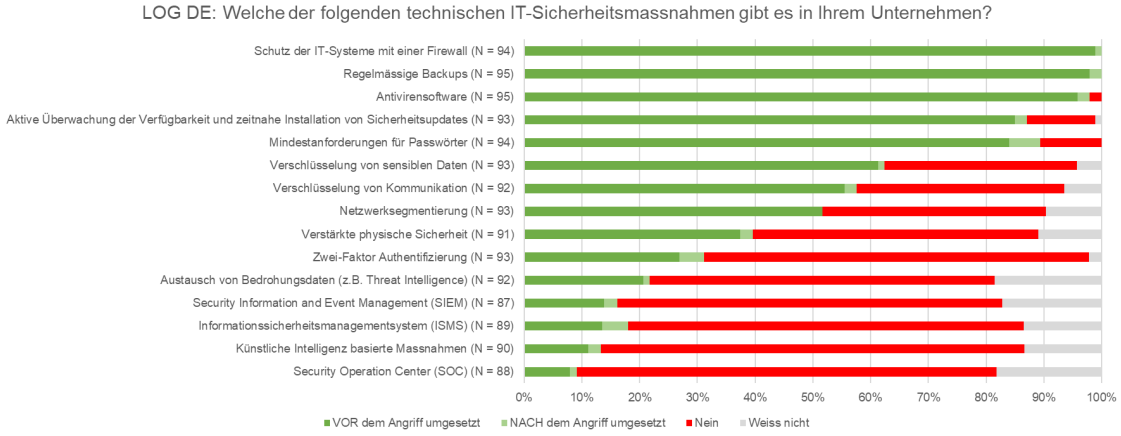


Abbildung 28: Technische IT-Sicherheitsmassnahmen (LOG DE)

Inklusive der nach dem «schwerwiegendsten Angriff» implementierten Massnahmen, wurde die «Netzwerksegmentierung» in der MEM-Branche häufiger eingesetzt als in der Logistikbranche (Differenz: 11.9%). Dafür setzte die Logistikbranche die «Verschlüsselung sensibler Daten» häufiger ein (Differenz: 11.3%).

Organisatorische IT-Sicherheitsmassnahmen

Bei den eingesetzten organisatorischen IT-Sicherheitsmassnahmen zeigen beide Branchen eine ähnliche Verteilung. Bei der Betrachtung der eingesetzten Massnahmen nach dem «schwerwiegendsten Angriff», waren in der MEM-Branche sowohl die «schriftlichen Richtlinien zur Informations- bzw. IT-Sicherheit» (Differenz: 13.2%) als auch die «Tests der Datenwiederherstellung (Restoring)» (Differenz 19.1%) verbreiteter als in der Logistikbranche. Weiter fällt auf, dass «Penetration-Tests» in der Logistikbranche (zumindest vor dem «schwerwiegendsten Angriff») weniger häufig gewesen waren. Nach dem «schwerwiegendsten Angriff» verblieb eine Differenz von 9% zu Gunsten der MEM-Branche.

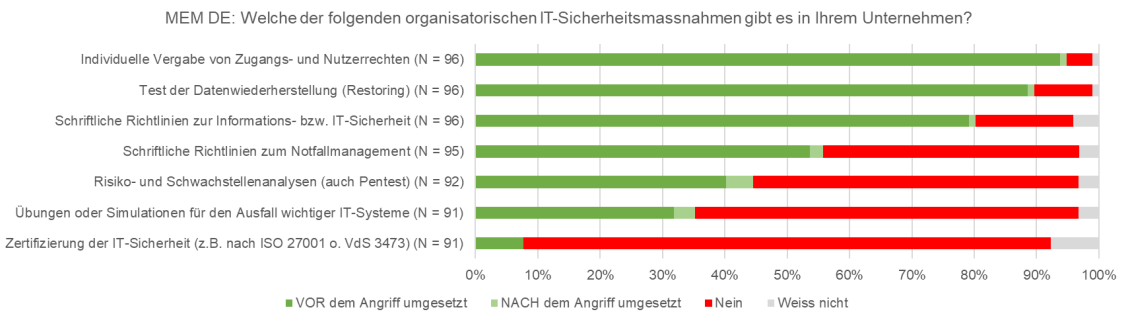


Abbildung 29: Organisatorische IT-Sicherheitsmassnahmen (MEM DE)

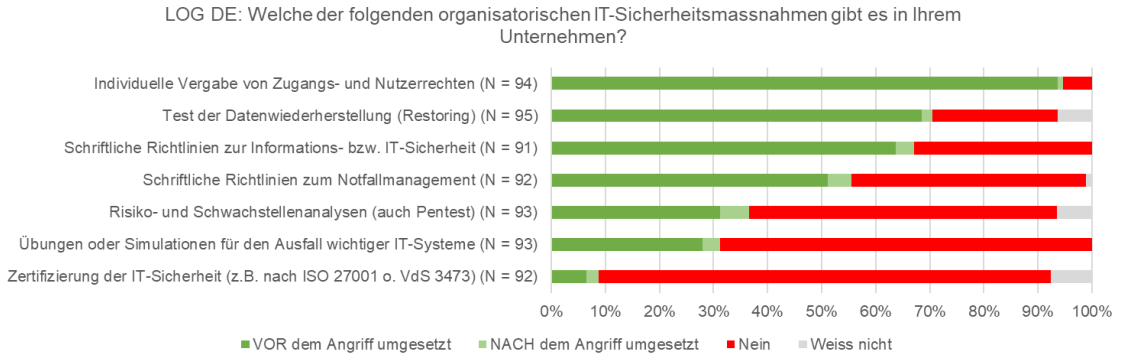


Abbildung 30: Organisatorische IT-Sicherheitsmassnahmen (LOG DE)

Zusammenfassung

Der abschliessende Vergleich der MEM- mit der Logistikbranche in Deutschland zeigt, dass beide in Bezug auf Art und Häufigkeit sehr ähnlich von Cyberangriffen betroffen waren. In der MEM-Branche waren aufgrund der Unternehmensstrukturen häufiger Produktionsdaten betroffen als in der Logistikbranche. In der Logistikbranche traten häufiger «kurz- und mittelfristig» behebbare Schäden auf, die Folgekosten waren hingegen tiefer als in der MEM-Branche.

4.2.5 Vergleich der deutschen und der Schweizer MEM-Branche

Nachfolgend wird die deutsche mit der Schweizer MEM-Branche verglichen, um herauszufinden, ob sich die Cyberangriffe und IT-Sicherheitsmassnahmen auf unterschiedlichem Niveau bewegen. Die Umfrageergebnisse werden direkt miteinander verglichen. Es gilt zu beachten, dass der Zeitraum zur Ermittlung der Betroffenheit und des «schwerwiegendsten Angriffes» in der deutschen 12 Monate (Dreißigacker et al., 2021), in der Schweizer Studie (Isenhardt et al., 2022) hingegen 24 Monate beträgt, dass die Studien zeitlich versetzt und mit unterschiedlichen Stichprobenarten durchgeführt wurden.

Betroffenheit

Die MEM-Branche in Deutschland war öfter durch «Phishing-Angriffe» betroffen (Differenz: 6.1%). Die Schweizer MEM-Branche hingegen wird öfter durch «CEO-Fraud» angegriffen als die deutsche MEM-Branche (Differenz: 23.5%). Angriffe mit «sonstiger Schadsoftware» wurden in der deutschen MEM-Branche häufiger genannt als in der Schweiz (Differenz: 16.2%). Währenddessen «Angriffe mittels manuellem Hacking» in der Schweiz verbreiteter waren (Differenz: 14.5 %).

Bezogen auf die letzten 12 Monate:
Von welchen Angriffsarten war Ihr Unternehmen betroffen und musste aktiv reagieren?

Wirtschaftszweig Gruppe	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen	Sonstige Schadsoftware - z.B. Viren, Würmer, Trojaner	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware)	(D)DoS-Attacke, die auf eine Überlastung von Web- oder E-Mail-Server zielte	CEO-Fraud, wobei eine Führungspersönlichkeit des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitern zu bewirken	Phishing, wobei Mitarbeiter mit echt aussehenden E-Mails oder Webseiten getäuscht wurden, um z.B. sensible Unternehmensdaten zu erlangen		Sonstiger Cyberangriff
MEM DE (N = 97)	23	17	35	2	3	23	46		0
	23.7%	17.5%	36.1%	2.1%	3.1%	23.7%	47.4%		0.0%

Tabelle 33: Betroffenheit durch Cyberangriffe (MEM DE)

Wirtschaftszweig Gruppe	Erfolgreicher Angriff mit Ransomware, bei dem Unternehmensdaten verschlüsselt wurden	Abhören oder Abfangen digitaler Kommunikation, z.B. E-Mails, Telefonate, Besprechungen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Hackerangriff (manuelles Hacking) auf IT-Systeme und Firmengeräte, d.h. die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware	Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	"CEO-Fraud", wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitende zu bewirken, z.B. Geldüberweisung	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E Mails oder Websites erfolgreich getäuscht wurden und z.B. sensibl Unternehmensdaten erlangt wurden	Sonstiges "Social Engineering", bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messer oder sonstigen Veranstaltungen	andere Angriffsart
MEM CH (N = 271)	30	22	54	45	30	128	112	42	9
	11.1%	8.1%	19.9%	16.6%	11.1%	47.2%	41.3%	15.5%	3.3%

Tabelle 34: Betroffenheit durch Cyberangriffe (MEM CH)

Häufigkeit

Bei der Betrachtung der Angriffshäufigkeit fällt auf, dass in der deutschen MEM-Branche 43.3% und in der Schweizer MEM-Branche 43.4% der Unternehmen mindestens einmal in 12 bzw. 24 Monaten einem «Phishing-Angriff» ausgesetzt waren, also fast gleich oft. «CEO-Fraud» trat in den Schweizer MEM-Unternehmen jedoch häufiger auf als in deutschen MEM-Unternehmen (Differenz: 26.1%). Weiter fällt auf, dass durch «manuelles Hacking» in der Schweizer MEM-Branche mehr Unternehmen betroffen sind als in der deutschem MEM-Branche (Differenz: 15.0%). Diese ist wiederum um öfter von «Ransomware-Angriffen» betroffen (Differenz: 12.4%).

	MEM DE							MEM CH						
	In den letzten 12 Monaten vor der Befragung							In den letzten 24 Monaten vor der Befragung						
Häufigkeit der Betroffenheit durch einzelne Angriffsarten (Anzahl)	N =	0 mal oder leer	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	97	74	19	3			1	266	236	28	2			
Spyware-Angriff (um zur Daten auszuspähen)	97	81	4	2	2	3	5	263	241	17	2		1	2
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	97	66	9	4	4	4	10	261	207	32	14	3	1	4
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	97	95	1		1			263	218	29	8	4		4
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	97	94	1	2				262	232	20	3	4		3
Defacing-Attacke (um Inhalte von Websites zu verändern)	97	97												
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	97	74	13	4	3	2	1	257	129	68	27	13	5	15
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	97	55	5	2	9	9	17	260	148	46	17	11	3	35
Sonstiges "Social Engineering" (gezielte Täuschung von Mitarbeitenden)								260	218	18	11	5		8
Andere Angriffsart								245	236	5	2			2

Tabelle 35: Häufigkeit der Angriffe absolut (MEM DE, MEM CH)

	MEM DE							MEM CH						
	In den letzten 12 Monaten vor der Befragung							In den letzten 24 Monaten vor der Befragung						
Häufigkeit der Betroffenheit durch einzelne Angriffsarten (in Prozent)	N =	0 mal oder leer	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	97	76.3%	19.6%	3.1%			1.0%	266	88.7%	10.5%	0.8%			
Spyware-Angriff (um zur Daten auszuspähen)	97	83.5%	4.1%	2.1%	2.1%	3.1%	5.2%	263	91.6%	6.5%	0.8%		0.4%	0.8%
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	97	68.0%	9.3%	4.1%	4.1%	4.1%	10.3%	261	79.3%	12.3%	5.4%	1.1%	0.4%	1.5%
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	97	97.9%	1.0%		1.0%			263	82.9%	11.0%	3.0%	1.5%		1.5%
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	97	96.9%	1.0%	2.1%				262	88.5%	7.6%	1.1%	1.5%		1.1%
Defacing-Attacke (um Inhalte von Websites zu verändern)	97	100.0%												
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	97	76.3%	13.4%	4.1%	3.1%	2.1%	1.0%	257	50.2%	26.5%	10.5%	5.1%	1.9%	5.8%
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	97	56.7%	5.2%	2.1%	9.3%	9.3%	17.5%	260	56.9%	17.7%	6.5%	4.2%	1.2%	13.5%
Sonstiges "Social Engineering" (gezielte Täuschung von Mitarbeitenden)								260	83.8%	6.9%	4.2%	1.9%		3.1%
Andere Angriffsart								245	96.3%	2.0%	0.8%			0.8%

Tabelle 36: Häufigkeit der Angriffe in Prozent (MEM DE, MEM CH)

«Schwerwiegendster Angriff»

Als «schwerwiegendster Angriff» wurde in der Schweizer MEM-Branche «Phishing-Angriffe» mit 24.4% am häufigsten genannt. In der deutschen MEM-Branche nannten dies lediglich 16.5% der Unternehmen (Differenz: 7.9%). Darauf folgte in der Schweizer MEM-Branche der «CEO-Fraud» mit 18.8%, der in der deutschen MEM-Branche nur von 6.2% genannt wurde (Differenz: 12.6%). In der Schweizer MEM-Branche wurden

auch «Hacker-Angriffe» als «schwerwiegendster Angriff» öfter genannt als in der deutschen MEM-Branche (Differenz: 6.1%).

Welcher Cyberangriff der letzten 12 Monate war der schwerwiegendste? (Mehrfachantwort bei einer Kombination von mehreren Angriffsarten möglich)

Wirtschaftszweig Gruppe	Ransomware-Angriff (um Daten zu verschlüsseln)	Spyware-Angriff (um zur Daten auszuspähen)	Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	Manuelles Hacking (um Soft- und Hardware zu manipulieren)	(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	CEO-Fraud (Vortäuschung einer Führungspersönlichkeit)	Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	Sonstiger Cyberangriff		Defacing-Attacke (um Inhalte von Websites zu verändern)	Weiss nicht	Keine Angabe
MEM DE (N = 97)	10	2	3	2	0	6	16	0		0	7	6
	10.3%	2.1%	3.1%	2.1%	0.0%	6.2%	16.5%	0.0%		0.0%	7.2%	6.2%

Tabelle 37: Schwerwiegendster Cyberangriff (MEM DE)

Sie haben angegeben, dass Ihr Unternehmen in den letzten 24 Monaten angegriffen wurde. Welcher dieser Angriffe war aus Ihrer Sicht der schwerwiegendste?

Wirtschaftszweig Gruppe	Erfolgreicher Angriff mit Ransomware, bei dem Unternehmensdaten verschlüsselt wurden	Abhören oder Abfangen digitaler Kommunikation, z.B. E-Mails, Telefonate, Besprechungen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Hackerangriff (manuelles Hacking) auf IT-Systeme und Firmengeräte, d.h. die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware	Denial of Service (D)DoS-Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	"CEO-Fraud", wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Anderer, bei der vorherigen Frage genannter Angriff	Sonstiges "Social Engineering", bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden			
MEM CH (N = 271)	20	10	18	22	9	51	66	3	10			
	7.4%	3.7%	6.6%	8.1%	3.3%	18.8%	24.4%	1.1%	3.7%			

Abbildung 31: Schwerwiegendster Cyberangriff (MEM CH)

Lösegeldforderung

Cyberangriffe, die zu einer Erpressung mit Lösegeldforderung führten, waren in beiden MEM-Branchen sehr selten (MEM DE: 4.1%, MEM CH 3.7%). Die fehlenden Antworten (keine Angabe) der Schweizer MEM-Branche lassen sich mit der Tatsache erklären, dass nur 20 Unternehmen der Stichprobe von einem Ransom-Angriff betroffen waren und elf davon die Frage mit «ja» oder «nein» beantworteten. Somit entsprechen die verbleibenden Fälle in der Schweiz dem Nein-Stimmen-Anteil der Befragten in der deutschen MEM-Branche. Die Situation der MEM-Branchen ist also vergleichbar.

Gab es bei diesem Angriff eine Lösegeld-Forderung?

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
MEM DE (N = 97)	Ja	4	4.1%
	Nein	42	43.3%
	Weiss nicht	3	3.1%
	Keine Angabe	48	49.5%

Erpressung mit entwendeten oder verschlüsselten Daten: Lösegeldforderung?

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
MEM CH (N = 271)	Ja	10	3.7%
	Nein	1	0.4%
	Weiss nicht	2	0.7%
	Keine Angabe	258	95.2%

Tabelle 38: Lösegeldforderungen (MEM DE, MEM CH)

Durch Angriff verursachte Kosten

Wie hoch waren die materiellen Schäden (schätzungsweise) für diese Position in Euro?

Wirtschaftszweig Gruppe			
MEM DE (N = 97)	Antworten	25
	Mittelwert	161’762
	Median	2’000
	Std.-Abweichung	758’250
	Spannweite	3’799’999
	Minimum	1
	Maximum	3’800’000

Wie hoch war die Schadenhöhe in CHF?

Wirtschaftszweig Gruppe			
MEM CH (N = 271)	Antworten	77
	Mittelwert	205’143
	Median	30’000
	Std.-Abweichung	463’194
	Spannweite	2’000’000
	Minimum	-
	Maximum	2’000’000

Tabelle 39: Durch Angriffe verursachte Kosten (MEM DE, MEM CH)

Die Folgekosten eines Cyberangriffes waren in der deutschen MEM-Branche tiefer in Bezug auf den Mittelwert und insbesondere in Bezug auf den Median. Der Median der Folgekosten lag in der Schweizer MEM-Branche (CHF 30'000.-) fünfzehnmal höher[18] als in der deutschen MEM-Branche (€ 2'000.-). In Tabelle 40 sind die Folgekosten in Bezug auf die Unternehmensgrösse (=Anzahl Mitarbeitende) dargestellt. Auffällig ist der unerklärbare Rückgang des Medians in unterschiedlichen Grössenklassen: In der deutschen MEM-Branche liegt der Rückgang bei Unternehmen mit 100-249

[18] Aufgrund der aktuellen Währungsparität wird vereinfachend ein Umrechnungskurs von 1:1 angenommen.

Mitarbeitenden, in der Schweizer MEM-Branche liegt der Rückgang bei Unternehmen mit 250-999 Mitarbeitenden. Generell steigen in den MEM-Branchen die Folgekosten mit zunehmender Unternehmensgrösse.

Wie hoch waren die materiellen Schäden (schätzungsweise) für diese Position in Euro?

		Mitarbeitende	Anzahl	Mittelwert	Median	Maximum	Minimum	Std.-Abweichung
MEM DE	Mitarbeiterzahl (Adresssample)	10-49	10					
		50-99	24	6'450	3'800	20'000	200	7'621
		100-249	25	2'709	445	19'500	1	5'963
		250-499	28	17'108	2'100	86'000	200	34'040
		500+	10	969'000	37'500	3'800'000	1'000	1'887'545

Höhe des Schadens

		Mitarbeitende	Anzahl	Mittelwert	Median	Maximum	Minimum	Std.-Abweichung
MEM CH	Unternehmens-grösse	1 - 49	102	76'207	5'000	1'500'000	-	279'916
		50 - 249	69	121'250	50'000	1'000'000	1'000	223'985
		250 - 999	30	325'714	30'000	2'000'000	-	739'726
		über 1000	41	483'389	150'000	2'000'000	1'000	672'635

Tabelle 40: Folgekosten nach Unternehmensgrösse (MEM DE, MEM CH)

Betroffene Daten

Waren durch den Angriff folgende Daten betroffen?

Wirtschaftszweig Gruppe		Personenbezogene Daten		Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes etc.)				Strategie-, Vertriebs- und Finanzinformationen (z.B. Preislisten, Sanierungspläne, Akquisitionen, Finanz- und Rechnungswesendaten)		Sonstige wichtige Daten	
		Häufigkeit	Prozent	Häufigkeit	Prozent			Häufigkeit	Prozent	Häufigkeit	Prozent
MEM DE	**Ja**	6	13.3	8	17.8			5	11.4		-
	Nein	39	86.7	37	82.2			39	88.6	40	100.0
	N	**45**	**100.0**	**45**	**100.0**			**44**	**100.0**	**40**	**100.0**

Waren durch den Angriff folgende Daten betroffen?

Wirtschaftszweig Gruppe		Kunden- und personenbezogene Daten		Produktions- und Prozessdaten		Produkt und F & E Daten		Betriebswirtschaftliche Daten		andere Daten	
		Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent
MEM CH	**ja**	31	18.9	20	12.2	17	10.4	25	15.2	15	9.1
	nein	116	70.7	130	79.3	129	78.7	124	75.6	111	67.7
	weiss	13	7.9	10	6.1	11	6.7	10	6.1	18	11.0
	N	**164**	**100.0**	**164**	**100.0**	**164**	**100.0**	**164**	**100.0**	**164**	**100.0**

Tabelle 41: Betroffene Daten (MEM DE, MEM CH)

In der deutschen MEM-Branche war die Datenkategorie «Produktdaten» mit 17.8% am häufigsten betroffen. Wenn in der Schweizer MEM-Branche die Datenkategorien «Produktions- und Prozessdaten» mit den «Produkt und F & E Daten» zusammengefasst betrachtet werden, sind diese mit 22.6% ebenfalls am häufigsten betroffen. In beiden Branchen folgen anschliessend die Datenkategorien «Personenbezogene Daten» und «Betriebswirtschaftliche Daten». Die Situation in der MEM-Branche beider Länder ist also sehr vergleichbar.

Folgen des «schwerwiegendsten Angriffes»

In beiden Branchen waren nur 2% der «schwerwiegendsten Angriffe» «existenzgefährdend». Die Kategorien «kurzfristig behebbaren Angriffe» und «Angriffe ohne Folgen» unterscheiden sich in der deutschen MEM-Branche stark von der Schweizer MEM-Branche. So gaben in der deutschen Studie 89% der antwortenden Unternehmen an, keine Folgen aufgrund eines Cyberangriffes zu haben und in der Schweizer Studie lediglich 4.8%. Hier muss jedoch beachtet werden, dass «MEM DE» auf einer Zufalls- und «MEM CH» auf einer Gelegenheitsstichprobe basiert und die Schweizer Fallzahlen sehr gering sind.

Wie schwerwiegend schätzen Sie die verursachten Schäden dieses Angriffes insgesamt ein?

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
MEM DE (N = 48)	Kein derartiger Schaden	43	89.6%
	Kurzfristig / gering	4	8.3%
	Mittelfristig/ deutlich spürbar	0	0.0%
	Bestandsgefährdend	1	2.1%

Nähere Angaben zum Schaden - Bitte ergänzen Sie: Der durch den schwerwiegendsten Angriff erfolgte Schaden...

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
MEM CH (N = 95)	zog keine Einschränkungen nach sich	13	13.7%
	war kurzfristig behebbar und leicht verdaubar	65	68.4%
	führte zu spürbaren Einschränkungen	15	15.8%
	gefährdete die Existenz des Unternehmens	2	2.1%

Tabelle 42: Nicht-materieller Schaden (MEM DE, MEM CH)

Technische IT-Sicherheitsmassnahmen

«Schutz der IT-Systeme mit einer Firewall», «regelmässige Backups» und «Antivirensoftware» wurden als technische IT-Sicherheitsmassnahmen in den MEM-Branchen beider Länder konsequent eingesetzt. Bei Betrachtung der «IT-

Sicherheitsmassnahmen vor dem «schwerwiegendsten Angriff» lag der grösste Unterschied im Einsatz eines «Security Information and Event Management» (SIEM). Die Schweizer MEM-Branche (49.0%) war der deutschen MEM-Branche (17.2%) bei dieser Massnahme voraus (Differenz: 31.8%). In der Schweiz wurde auch der Einsatz eines «Informationssicherheitsmanagementsystem» (ISMS) öfter angegeben (Differenz: 11.9%).

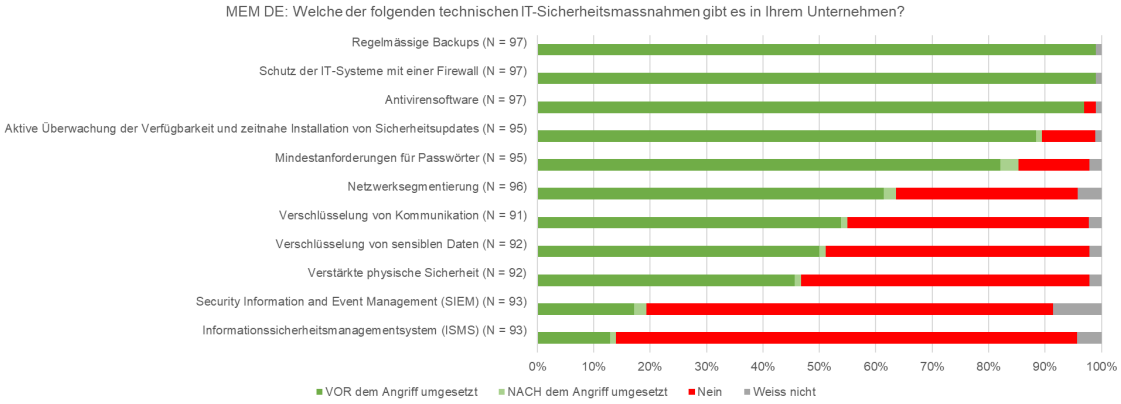


Abbildung 32: Technische IT-Sicherheitsmassnahmen (MEM DE)

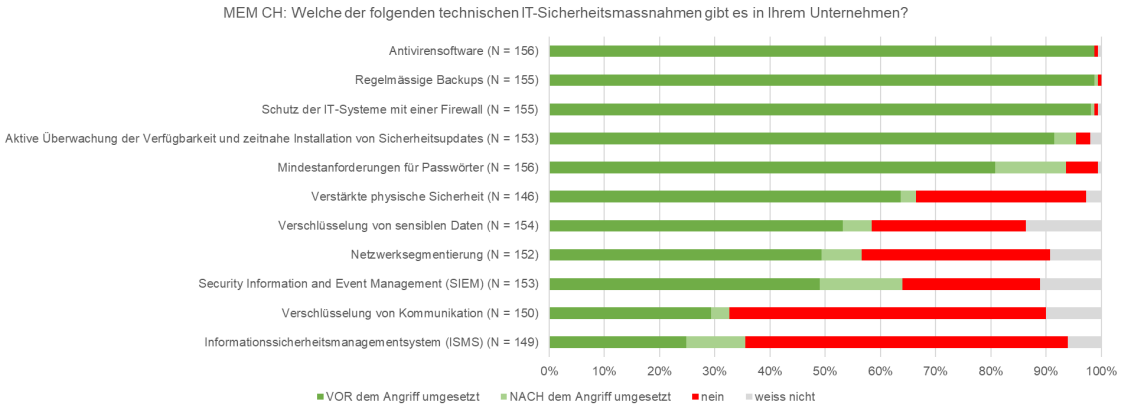


Abbildung 33: Technische IT-Sicherheitsmassnahmen (MEM CH)

«Verstärkte Physische Sicherheit» wird in der Schweizer MEM-Branche öfter eingesetzt als in der deutschen MEM-Branche (Differenz: 18%). Beim Einsatz «verschlüsselter Kommunikation» ist die deutsche MEM-Branche (53.8%) der Schweizer MEM-Branche (29.3%) voraus (Differenz: 24.5%). Vor dem «schwerwiegendsten Angriff» lag der Einsatz von «Mindestanforderungen für Passwörter» in beiden Ländern bei rund 80% (DE: 82.1%, CH: 80.8%). Nach dem Angriff haben in der deutschen MEM-Branche lediglich 3.2% der Unternehmen diese Massnahme ergänzt, während in der Schweizer MEM-Branche 12.8% der Unternehmen nachgerüstet haben.

Organisatorische IT-Sicherheitsmassnahmen

Der grösste Unterschied bei den organisatorischen IT-Sicherheitsmassnahmen vor dem «schwerwiegendsten Angriff» lässt sich im Branchenvergleich in der Durchführung von «Risiko- und Schwachstellenanalysen (auch Pentest)» finden. Die Schweizer MEM-Branche lag bei 55.2% und die deutsche MEM-Branche bei 40.2% (Differenz: 15%).

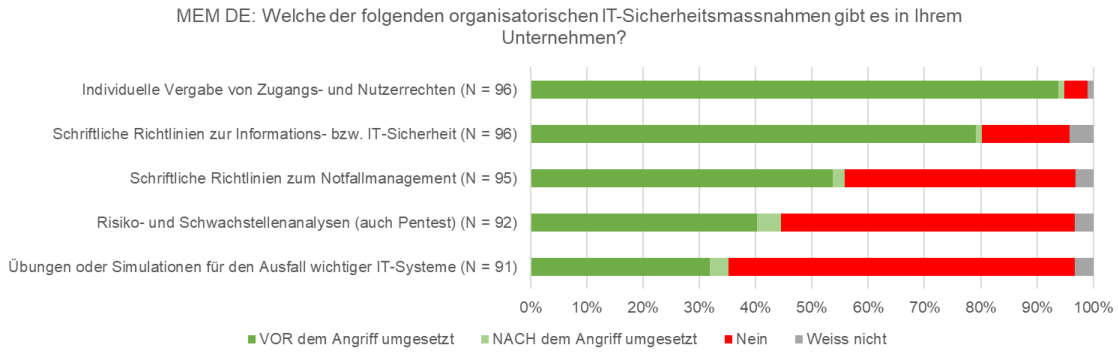


Abbildung 34: Organisatorische IT-Sicherheitsmassnahmen (MEM DE)

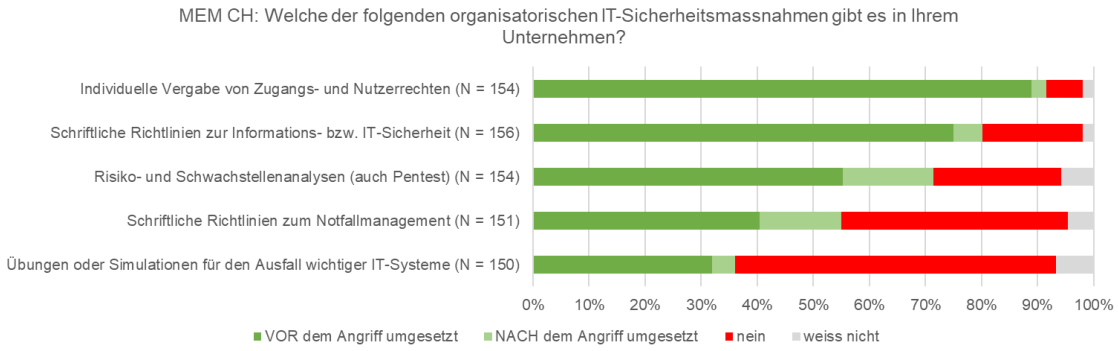


Abbildung 35: Organisatorische IT-Sicherheitsmassnahmen (MEM CH)

Umgekehrt verhält es sich bei der Erstellung von «schriftlichen Richtlinien zum Notfallmanagement», wo die deutsche MEM-Branche mit 53.7% Umsetzungsgrad der Schweizer MEM-Branche mit 40.4% voraus war (Differenz: 13.3%). Bei der Betrachtung des Umsetzungsgrades nach dem «schwerwiegendsten Angriff» schliesst sich die Lücke bei den «schriftlichen Richtlinien zum Notfallmanagement», nicht aber bei den «Risiko- und Schwachstellenanalysen (auch Pentest)», wo eine Differenz von 11.9% bestehen bleibt.

Zusammenfassung

Bei einem Ländervergleich der MEM-Branchen fällt in Bezug auf die Cyberangriffe auf, dass «CEO-Fraud» in der Schweiz häufiger aufgetreten ist. In beiden Ländern wurde «Phishing», neben dem erwähnten «CEO-Fraud» in der Schweiz, als «schwerwiegendster

Angriff» genannt. Die Branchen unterscheiden sich hauptsächlich durch die Folgekosten, die durch die Cyberangriffe entstanden sind. So liegt der Schaden-Median mit CHF 30'000.- in der Schweiz fünfzehnmal höher als in Deutschland. In Bezug auf die IT-Sicherheitsmassnahmen waren «Security Information and Event Management (SIEM)», «Informationssicherheitsmanagementsysteme (ISMS)» und «verstärkte Physische Sicherheit» in der Schweiz verbreiteter. In Deutschland wurde dafür mehr auf den Einsatz «verschlüsselter Kommunikation» gesetzt.

Auch wenn der Vergleich der beiden Branchen auf den ersten Blick eine ähnliche Verteilung zeigt, fällt bei genauerer Betrachtung der Ergebnisse auf, dass in der Schweizer MEM-Branche 77.1% einen «schwerwiegenden Angriff» nannten, in der deutschen MEM-Branche hingegen nur 53.6%. In Anbetracht dessen, dass die Schweizer Studie auf einer Gelegenheitsstichprobe basiert und über einen längeren Zeitraum zurückblickt, kann dieser Unterschied erklärt werden.

4.2.6 Vergleich der deutschen und der Schweizer Logistikbranche

Wie in Kapitel 4.1.3 erläutert, wird die Schweizer Logistikbranche mit den Daten bzw. Antworten der Gruppen LOG und LOG+ dargestellt. Die Umfrageergebnisse der deutschen und der Schweizer Studie werden direkt miteinander verglichen. Es gilt zu beachten, dass der Zeitraum zur Ermittlung der Betroffenheit und des «schwerwiegendsten Angriffes» in der deutschen 12 Monate (Dreißigacker et al., 2021), in der Schweizer Studie 24 Monate beträgt (Isenhardt et al., 2022), dass die Studien zeitlich versetzt und mit unterschiedlichen Stichprobenarten durchgeführt wurden.

Betroffenheit

In der deutschen und in der Schweizer Logistikbranche wurden «Phishing-Angriffe» am meisten und auch fast gleich häufig als «schwerwiegendster Angriff» genannt (Differenz 0.3%). Auffällig ist jedoch der Unterschied bei «CEO-Fraud», wo die Schweizer Logistikbranche eine höhere Betroffenheit ausgewiesen hat als in Deutschland (Differenz: 11.8%). In der Schweiz werden auch öfter «(D)DoS-Angriffe» (Differenz: 12.2%) und «Ransomware-Angriffe» (Differenz: 11.3%) registriert. Nur Angriffe mit «sonstiger Schadsoftware» wurden in der deutschen Logistikbranche öfter genannt (Differenz: 9.3%).

Bezogen auf die letzten 12 Monate: Von welchen Angriffsarten war Ihr Unternehmen betroffen und musste aktiv reagieren?

Wirtschaftszweig Gruppe	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Spyware, die das Ziel hatte, Nützeraktivitäten oder sonstige Daten auszuspähen	Sonstige Schadsoftware - z.B. Viren, Würmer, Trojaner	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware)	Defacing-Attacke, die das Ziel hatte, unbefugt Webinhalte des Unternehmens zu verändern	Denial of Service ((D)DoS) Attacke, die auf eine Überlastung von Web- oder E-Mail-Server zielte	CEO-Fraud, wobei eine Führungspersönlichkeit des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbe	Phishing, wobei Mitarbeiter mit echt aussehenden E-Mails oder Webseiten getäuscht wurden, um z.B. sensible Unternehmens	Sonstiger Cyberangriff	
LOG DE (N = 95)	14	16	31	1	12	4	20	38	1	
	14.7%	16.8%	32.6%	1.1%	12.6%	4.2%	21.1%	40.0%	1.1%	

Tabelle 43: Betroffenheit durch Cyberangriffe (LOG DE)

War Ihr Unternehmen in den letzten 24 Monaten von einem oder mehreren der unten aufgeführten Cyberangriffe betroffen?

Wirtschaftszweig Gruppe	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware	Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern	Denial of Service (D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	«CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Andere Angriffsart	Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen
LOG CH (N = 45)	12	8	11	3	2	8	15	16	3	9
	26.7%	17.8%	24.4%	6.7%	4.4%	17.8%	33.3%	35.6%		20.0%
LOG+ CH (N = 28)	7	4	6	4	3	4	9	13	1	5
	25.0%	14.3%	21.4%	14.3%	10.7%	14.3%	32.1%	46.4%		17.9%
LOG CH & LOG+ CH (N = 73)	19	12	17	7	5	12	24	29	4	14
	26.0%	16.4%	23.3%	9.6%	6.8%	16.4%	32.9%	39.7%	5.5%	19.2%

Tabelle 44: Betroffenheit durch Cyberangriffe (LOG CH & LOG+ CH)

Häufigkeit

Die Angriffe mittels «CEO-Fraud» traten in der Schweizer Logistikbranche häufiger auf (Differenz: 8.9%). In Deutschland waren hingegen häufiger «sonstige Angriffe mit Schadsoftware (Viren, Würmer, Trojaner)» (Differenz: 18.4%) und «Phishing-Angriffe» (Differenz: 9.1%) anzutreffen.

Häufigkeit der Betroffenheit durch einzelne Angriffsarten (Anzahl)	LOG DE (In den letzten 12 Monaten vor der Befragung)							LOG CH & LOG+ CH (In den letzten 24 Monaten vor der Befragung)						
	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	95	83	8	3			1	73	64	7		2		
Spyware-Angriff (um zur Daten auszuspähen)	95	83	4	2	1	1	4	73	65	5		1	1	1
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	95	67	9	6	3	3	7	73	64	7	1	1		
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	95	94	1					73	70	2		1		
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	95	84	5		1	3	2	73	65	6	1	1		
Defacing-Attacke (um Inhalte von Websites zu verändern)	95	91	3				1	73	69	3		1		
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	95	76	11	4	1	1	2	73	55	11	2	1	2	2
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	95	61	7	4	5	4	14	73	50	8	6	3	3	3
Sonstiges "Social Engineering" (gezielte Täuschung von Mitarbeitenden)								73	63	6		2		2
Andere Angriffsart								73	70	1		2		

Tabelle 45: Häufigkeit der Angriffe absolut (LOG DE, LOG CH & LOG+ CH)

Häufigkeit der Betroffenheit durch einzelne Angriffsarten (in Prozent)	LOG DE (In den letzten 12 Monaten vor der Befragung)							LOG CH & LOG+ CH (In den letzten 24 Monaten vor der Befragung)						
	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	95	87.4%	8.4%	3.2%			1.1%	73	87.7%	9.6%		2.7%		
Spyware-Angriff (um zur Daten auszuspähen)	95	87.4%	4.2%	2.1%	1.1%	1.1%	4.2%	73	89.0%	6.8%		1.4%	1.4%	1.4%
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	95	70.5%	9.5%	6.3%	3.2%	3.2%	7.4%	73	87.7%	9.6%	1.4%	1.4%		
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	95	98.9%	1.1%					73	95.9%	2.7%		1.4%		
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	95	88.4%	5.3%		1.1%	3.2%	2.1%	73	89.0%	8.2%	1.4%	1.4%		
Defacing-Attacke (um Inhalte von Websites zu verändern)	95	95.8%	3.2%				1.1%	73	94.5%	4.1%		1.4%		
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	95	80.0%	11.6%	4.2%	1.1%	1.1%	2.1%	73	75.3%	15.1%	2.7%	1.4%	2.7%	2.7%
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	95	64.2%	7.4%	4.2%	5.3%	4.2%	14.7%	73	68.5%	11.0%	8.2%	4.1%	4.1%	4.1%
Sonstiges "Social Engineering" (gezielte Täuschung von Mitarbeitenden)								73	86.3%	8.2%		2.7%		2.7%
Andere Angriffsart								73	95.9%	1.4%		2.7%		

Tabelle 46: Häufigkeit der Angriffe in Prozent (LOG DE, LOG CH & LOG+ CH)

«Schwerwiegendster Angriff»

In der Schweizer Logistikbranche wurden mehr «Phishing-Angriffe» als «schwerwiegendste Angriffe» registriert als in der deutschen Logistikbranche (Differenz: 8.7%).

Welcher Cyberangriff der letzten 12 Monate war der schwerwiegendste? (Mehrfachantwort bei einer Kombination von mehreren Angriffsarten möglich)

Wirtschaftszweig Gruppe	Ransomware-Angriff (um Daten zu verschlüsseln)	Spyware-Angriff (um zur Daten auszuspähen)	Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	Manuelles Hacking (um Soft- und Hardware zu manipulieren)	(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	Defacing-Attacke (um Inhalte von Websites zu verändern)	CEO-Fraud (Vortäuschung einer Führungspersönlichkeit)	Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	Sonstiger Cyberangriff	Weiss nicht	Keine Angabe	
LOG DE (N = 95)	6	3	7	0	2	1	6	10	0	7	7	
	6.3%	3.2%	7.4%	0.0%	2.1%	1.1%	6.3%	10.5%	0.0%	7.4%	7.4%	

Tabelle 47: Schwerwiegendster Cyberangriff (LOG DE)

Sie haben für die unten aufgeführten Angriffsarten angegeben, dass Ihr Unternehmen in den letzten 24 Monaten von diesen betroffen war. Welcher dieser Angriffe war aus Ihrer Sicht der schwerwiegendste?

Wirtschaftszweig Gruppe	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohn Nutzung spezieller Schadsoftware	Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern	«CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitende zu bewirken, z.B. Geldüberweisung	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Andere Angriffsart			Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen
LOG CH (N = 45)	2	2	1	0	4	1	7	7	0			0
	4.4%	4.4%	2.2%	0.0%	8.9%	2.2%	15.6%	15.6%	0.0%			0.0%
LOG+ CH (N = 28)	4	1	1	1	1	1	2	7	1			1
	14.3%	3.6%	3.6%	3.6%	3.6%	3.6%	7.1%	25.0%	3.6%			3.6%
LOG CH & LOG+ CH (N = 73)	6	3	2	1	5	2	9	14	1			1
	8.2%	4.1%	2.7%	1.4%	6.8%	2.7%	12.3%	19.2%	1.4%			1.4%

Abbildung 36: Schwerwiegendster Cyberangriff (LOG CH & LOG+ CH)

Auch traten in der Schweizer Logistikbranche häufiger «CEO-Fraud» (Differenz: 6%) und «(D)DoS-Attacken» (Differenz: 4.7%) auf. Aufgrund der kleinen Fallzahlen darf dieser Unterschied jedoch nicht verallgemeinert werden.

Lösegeldforderung

Der Anteil der Lösegeldforderungen liegt in Deutschland etwas höher. Auch dieser Unterschied kann aber aufgrund der kleinen Fallzahlen nicht weiter interpretiert werden.

Gab es bei diesem Angriff eine Lösegeld-Forderung?

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
LOG DE (N= 95)	Ja	5	5.3%
	Nein	38	40.0%
	Weiss nicht	2	2.1%
	Keine Angabe	50	52.6%

Gab es bei diesem schwerwiegendsten Angriff eine Lösegeldforderung?

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
LOG CH (N = 45)	Nein	2	4.4%
	Keine Angabe	43	95.6%
LOG+ CH (N = 28)	Ja	2	7.1%
	Nein	1	3.6%
	Keine Angabe	25	89.3%
LOG CH & LOG+ CH (N = 73)	Ja	2	2.7%
	Nein	3	4.1%
	Keine Angabe	68	93.2%

Tabelle 48: Lösegeldforderungen (LOG DE, LOG CH & LOG+ CH)

Durch Angriff verursachte Kosten

Cyberangriffe verursachten in der deutschen Logistikbranche bei Betrachtung des Medians gleich hohe Kosten als in der Schweizer Logistikbranche. Einzelne Ausreisser (bis zu CHF 1 Mrd.) führten zu einer sehr starken Streuung der Antworten. Die Frage, ob betroffene Unternehmen bei einer Gelegenheitsstichprobe tendenziell eher an einer Umfrage dieser Art teilnehmen, müsste weiter untersucht werden.

Wie hoch waren die materiellen Schäden (schätzungsweise) für diese Position in Euro?

Wirtschaftszweig Gruppe	LOG DE (N = 95)	Antworten	23
		Mittelwert	4'561
		Median	1'000
		Std.-Abweichung	10'513
		Spannweite	44'950
		Minimum	50
		Maximum	45'000

Bitte geben Sie an, welche Kosten durch den von Ihnen angegebenen schwerwiegendsten Angriff in CHF entstanden sind.

Wirtschaftszweig Gruppe	LOG CH (N = 45)	Antworten	21
		Mittelwert	37'227
		Median	524
		Std.-Abweichung	85'935
		Spannweite	300'000
		Minimum	-
		Maximum	300'000
	LOG+ CH (N = 28)	Antworten	10
		Mittelwert	100'112'350
		Median	1'250
		Std.-Abweichung	316'188'443
		Spannweite	1'000'000'000
		Minimum	-
		Maximum	1'000'000'000
	LOG CH & LOG+ CH (N = 73)	Antworten	31
		Mittelwert	32'319'525
		Median	1'000
		Std.-Abweichung	179'593'994
		Spannweite	1'000'000'000
		Minimum	-
		Maximum	1'000'000'000

Tabelle 49: Durch Angriffe verursachte Kosten (LOG DE, LOG CH & LOG+ CH)

Betroffene Daten

Die betroffenen Datenkategorien verteilen sich sowohl in der deutschen als auch in der Schweizer Logistikbranche gleichmässig auf alle Kategorien, wobei die Stichprobe sehr klein ist und keine verallgemeinernden Rückschlüsse zulässt.

		Waren durch den Angriff folgende Daten betroffen?									
		Personenbezogene Daten		Strategie-, Vertriebs- und Finanzinformationen (z.B. Preislisten, Sanierungspläne, Akquisitionen, Finanz- und Rechnungswesendaten)		Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes etc.)				Sonstige wichtige Daten	
Wirtschaftszweig	Gruppe	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent			Häufigkeit	Prozent
LOG DE	**Ja**	**4**	**10.0**	**3**	**7.5**	**4**	**10.0**			**2**	**5.7**
	Nein	36	90.0	37	92.5	36	90.0			33	94.3
	N	**40**	**100.0**	**40**	**100.0**	**40**	**100.0**			**35**	**100.0**

Tabelle 50: Betroffene Daten (LOG DE)

		Waren bei dem genannten schwerwiegendsten Angriff die folgenden Daten betroffen? Wurden diese gelöscht, manipuliert, gestohlen oder verschlüsselt?									
		Kunden- und personenbezogene Daten		Betriebswirtschaftliche Daten		Produktions- und Prozessdaten		Produkt und F&E Daten		Andere Daten	
Wirtschaftszweig	Gruppe	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent
LOG CH	ja, sie wurden gelöscht	1	4.8								
	ja, sie wurden verschlüsselt oder blockiert	1	4.8	1	4.8	1	4.8	1	4.8	1	4.8
	ja (total)	**2**	**9.5**	**1**	**4.8**	**1**	**4.8**	**1**	**4.8**	**1**	**4.8**
	nein	18	85.7	19	90.5	19	90.5	19	90.5	19	90.5
	keine Angabe	1	4.8	1	4.8	1	4.8	1	4.8	1	4.8
	N	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**
LOG+ CH	ja, sie wurden gestohlen			1	3.6					1	3.6
	ja, sie wurden manipuliert	1	3.6								
	ja, sie wurden verschlüsselt oder blockiert	1	3.6	1	3.6	2	7.1	2	7.1	1	3.6
	ja (total)	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**
	nein	7	25.0	7	25.0	7	25.0	7	25.0	7	25.0
	keine Angabe	2	7.1	2	7.1	2	7.1	2	7.1	2	7.1
	N	**28**	**100.0**	**11**	**100.0**	**11**	**100.0**	**11**	**100.0**	**11**	**100.0**
LOG CH & LOG+ CH	ja, sie wurden gelöscht	1	3.1								
	ja, sie wurden gestohlen			1	3.1					1	3.1
	ja, sie wurden manipuliert	1	3.1								
	ja, sie wurden verschlüsselt oder blockiert	2	6.3	2	6.3	3	9.4	3	9.4	2	6.3
	ja (total)	**4**	**12.5**	**3**	**9.4**	**3**	**9.4**	**3**	**9.4**	**3**	**9.4**
	nein	25	78.1	26	81.3	26	81.3	26	81.3	26	81.3
	keine Angabe	3	9.4	3	9.4	3	9.4	3	9.4	3	9.4
	N	**49**	**100.0**	**32**	**100.0**	**32**	**100.0**	**32**	**100.0**	**32**	**100.0**

Tabelle 51: Betroffene Daten (LOG CH & LOG+ CH)

Folgen des «schwerwiegendsten Angriffes»

Die Unternehmen der Logistikbranche schätzen in Deutschland den nicht-materiellen Schaden des «schwerwiegendsten Angriffes» weniger dramatisch ein als in der Schweiz. Die Stichprobengrösse und -art gilt es auch hier zu berücksichtigen.

Wie schwerwiegend schätzen Sie die verursachten Schäden dieses Angriffes insgesamt ein? - Nicht-materieller Schaden (z.B. Reputationsverlust oder Wettbewerbsnachteil)

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
LOG DE (N = 42)	Kein derartiger Schaden	32	76.2%
	Kurzfristig / gering	9	21.4%
	Mittelfristig/ deutlich spürbar	1	2.4%
	Bestandsgefährdend	0	0.0%

Tabelle 52: Nicht-materieller Schaden (LOG DE)

Bitte ergänzen Sie: Der durch den schwerwiegendsten Angriff erfolgte Schaden...

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
LOG CH (N = 21)	zog keine Einschränkungen nach sich	7	33.3%
	war kurzfristig behebbar und leicht verdaubar	13	61.9%
	führte zu spürbaren Einschränkungen	0	0.0%
	gefährdete die Existenz des Unternehmens	1	4.8%
LOG+ CH (N = 11)	zog keine Einschränkungen nach sich	3	27.3%
	war kurzfristig behebbar und leicht verdaubar	5	45.5%
	führte zu spürbaren Einschränkungen	3	27.3%
	gefährdete die Existenz des Unternehmens	0	0.0%
LOG CH & LOG+ CH (N = 32)	zog keine Einschränkungen nach sich	10	31.3%
	war kurzfristig behebbar und leicht verdaubar	18	56.3%
	führte zu spürbaren Einschränkungen	3	9.4%
	gefährdete die Existenz des Unternehmens	1	3.1%

Tabelle 53: Nicht-materieller Schaden (LOG CH & LOG+ CH)

Technische IT-Sicherheitsmassnahmen

Der Umsetzungsgrad der 14 technischen IT-Sicherheitsmassnahmen liegt in der deutschen Logistikbranche bei 51.7%, in der Schweizer Logistikbranche bei vergleichbaren 52.6%. Wenn die «nach dem Angriff umgesetzten» Massnahmen mitberücksichtigt werden, zeigt sich ein anderes Bild. Die Schweizer Logistikbranche erreicht bei dieser Betrachtung mit einem Vorsprung von 6.0% einen Umsetzungsgrad von 59.9%. Nicht berücksichtigt sind die noch geplanten 5.9% IT-Sicherheitsmassnahmen.

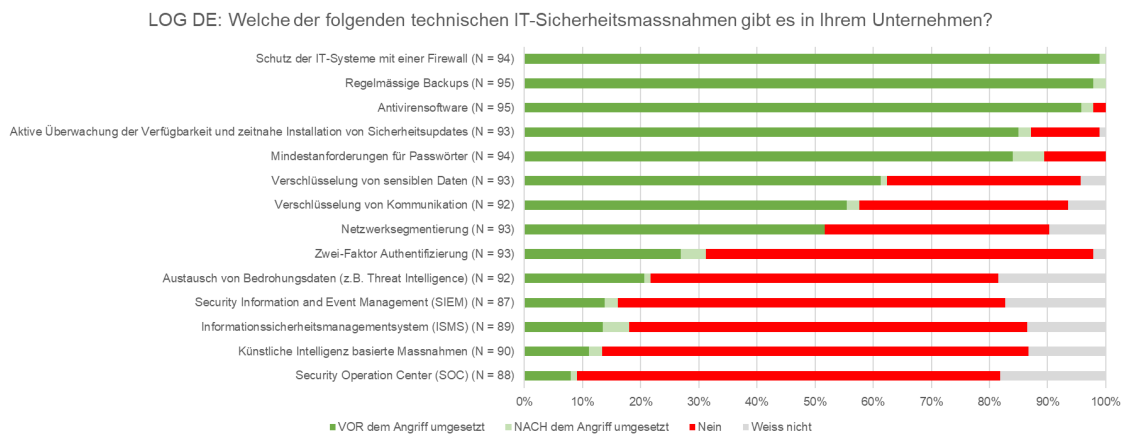


Abbildung 37: Technische IT-Sicherheitsmassnahmen (LOG DE)

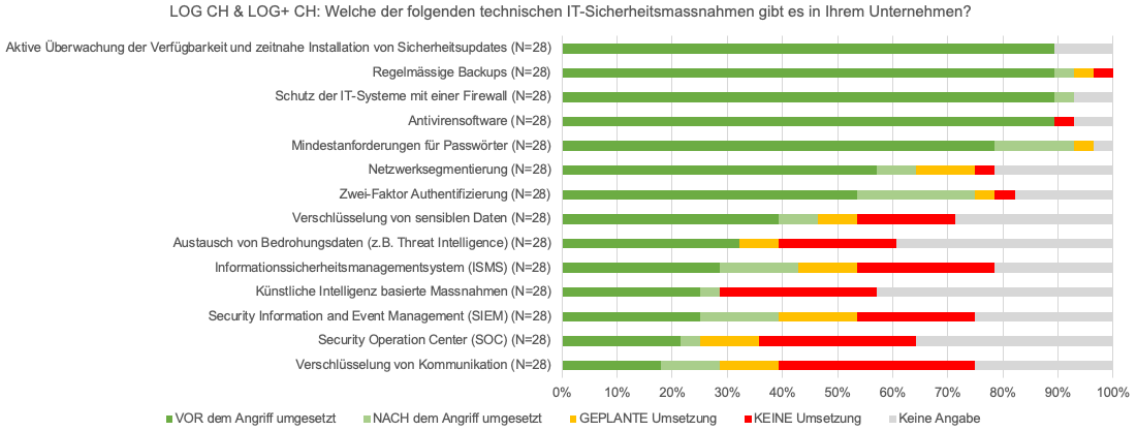


Abbildung 38: Technische IT-Sicherheitsmassnahmen (LOG CH & LOG+ CH)

Organisatorische IT-Sicherheitsmassnahmen

Die organisatorischen IT-Sicherheitsmassnahmen zeigen ein ähnliches Bild. Die Schweizer Logistikbranche erreicht bei den «vor dem Angriff umgesetzten» einen Umsetzungsgrad von 63.1% und bei den «nach dem Angriff umgesetzten» einen von 72.9%. Die deutschen Vergleichswerte liegen bei 53.5% bzw. 57.0%. Weiter zeigt sich, dass betreffend «nach dem Angriff umgesetzt» lediglich die «individuelle Vergabe von Zugangs- und Nutzerrechten» in Deutschland verbreiteter sind (Differenz: 9.5%) und die Schweizer Logistikbranche öfter auf «Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme» setzt (Differenz: 28.8%).

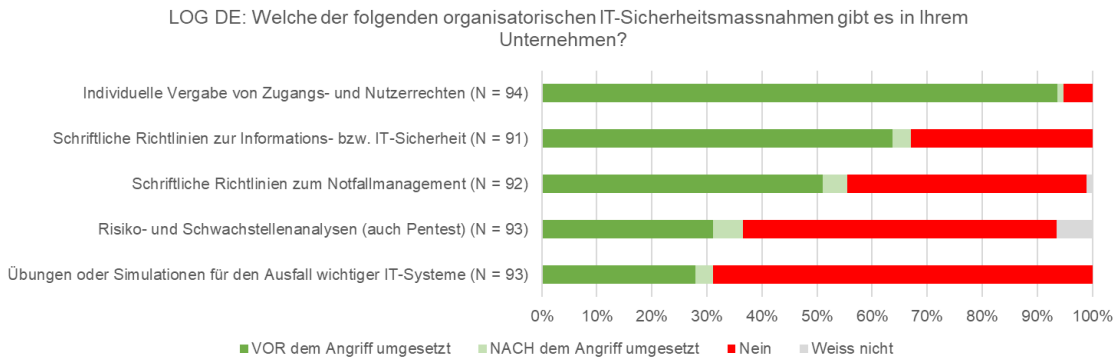


Abbildung 39: Organisatorische IT-Sicherheitsmassnahmen (LOG DE)

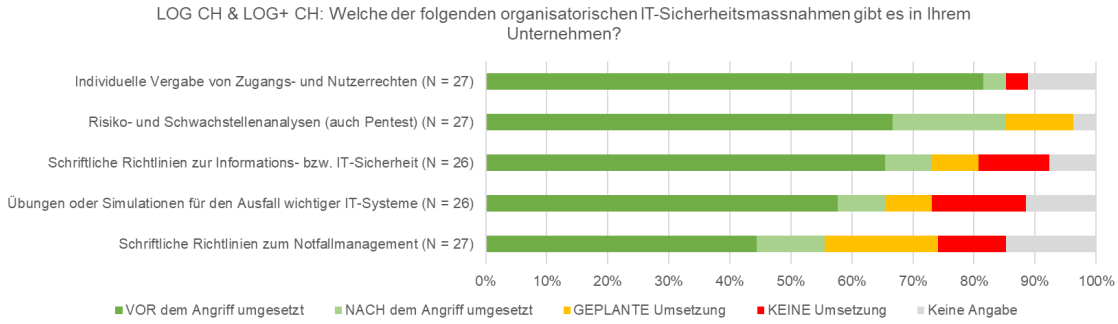


Abbildung 40: Organisatorische IT-Sicherheitsmassnahmen (LOG CH & LOG+ CH)

Zusammenfassung

Die Logistikbranchen der Schweiz und Deutschland sind ähnlich betroffen. In der Schweiz traten die Angriffsarten «CEO-Fraud», «Ransomware» und «(D)DoS-Attacken» häufiger auf, während in Deutschland Angriffe mit «sonstiger Schadsoftware» und «Phishing-Angriffe» öfter auftraten. «Phishing» war in beiden Ländern der meistgenannte «schwerwiegendste Angriff». Der Median der Folgekosten war vergleichbar und lag in beiden Ländern bei CHF 1'000.- bzw. € 1'000.-. Der nicht-materielle Schaden wurde sehr unterschiedlich eingeschätzt, was vermutlich auf die unterschiedliche Art der Stichproben zurückzuführen ist.

Im Vergleich der MEM-Branchen in Deutschland und der Schweiz (Kapitel 4.2.5) wurde ersichtlich, dass die Quote der genannten «schwerwiegendsten Angriffe» in der Schweiz um 23.5% höher liegt. Dieses Muster lässt sich jedoch im Vergleich der Logistikbranchen in Deutschland und der Schweiz nicht erkennen. In der Schweizer Logistikbranche war diese Quote sogar 5.2% tiefer.

4.2.7 Vergleich der Schweizer MEM- und Logistikbranche

In diesem letzten der vier vergleichenden Kapitel wird ein Branchenvergleich zwischen der MEM- und Logistikbranche in der Schweiz angestellt. Beide verwendeten Studien basieren auf einer Gelegenheitsstichprobe.

Betroffenheit

In der MEM-Branche war «CEO-Fraud» (47.2%) die häufigste Angriffsart, die mit 14.4% auch die grösste Differenz zur Logistikbranche (32.9%) aufwies. «Phishing-Angriffe» waren in der Logistikbranche (39.7%) und in der MEM-Branche (41.3%) mit einer Differenz von 1.6% fast gleicht verbreitet. In der Logistikbranche waren «Ransomware» (26.0%) mit 15.0% Differenz und «Spyware» (16.4%) mit 8.3% Differenz zur MEM-Branche häufiger.

War Ihr Unternehmen in den letzten 24 Monaten von einem oder mehreren der unten aufgeführten Cyberangriffe betroffen?

Wirtschaftszweig Gruppe	Erfolgreicher Angriff mit Ransomware, bei dem Unternehmensdaten verschlüsselt wurden	Abhören oder Abfangen digitaler Kommunikation, z.B. E-Mails, Telefonate, Besprechungen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Hackerangriff (manuelles Hacking) auf IT-Systeme und Firmengeräte, d.h. die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware	Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielen	"CEO-Fraud", wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitende zu bewirken, z.B. Geldüberweisung	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Sonstiges "Social Engineering", bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messer oder sonstigen Veranstaltungen	andere Angriffsart
MEM CH (N = 271)	30	22	54	45	30	128	112	42	9
	11.1%	8.1%	19.9%	16.6%	11.1%	47.2%	41.3%	15.5%	3.3%

Tabelle 54: Betroffenheit durch Cyberangriffe (MEM CH)

War Ihr Unternehmen in den letzten 24 Monaten von einem oder mehreren der unten aufgeführten Cyberangriffe betroffen?

Wirtschaftszweig Gruppe	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohn Nutzung spezieller Schadsoftware	Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	«CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitende zu bewirken, z.B. Geldüberweisung	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen	Andere Angriffsart	Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern
LOG (N = 45)	12	8	11	3	8	15	16	9	3	2
	26.7%	17.8%	24.4%	6.7%	17.8%	33.3%	35.6%	20.0%		4.4%
LOG+ (N = 28)	7	4	6	4	4	9	13	5	1	3
	25.0%	14.3%	21.4%	14.3%	14.3%	32.1%	46.4%	17.9%		10.7%
LOG CH & LOG+ CH (N = 73)	19	12	17	7	12	24	29	14	4	5
	26.0%	16.4%	23.3%	9.6%	16.4%	32.9%	39.7%	19.2%	5.5%	6.8%

Tabelle 55: Betroffenheit durch Cyberangriffe (LOG CH & LOG+ CH)

Häufigkeit

Auch die Häufigkeit der Cyberangriffe «CEO-Fraud», «manuelles Hacking» und «Phishing» war in den in der MEM-Branche analog der Betroffenheit höher als in der Logistikbranche.

Häufigkeit der Betroffenheit durch einzelne Angriffsarten (Anzahl)	MEM CH							LOG CH & LOG+ CH						
	In den letzten 24 Monaten vor der Befragung							In den letzten 24 Monaten vor der Befragung						
	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	266	236	28	2				73	64	7		2		
Spyware-Angriff (um zur Daten auszuspähen)	263	241	17	2		1	2	73	65	5		1	1	1
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	261	207	32	14	3	1	4	73	64	7	1	1		
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	263	218	29	8	4		4	73	70	2		1		
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	262	232	20	3	4		3	73	65	6	1	1		
Defacing-Attacke (um Inhalte von Websites zu verändern)								73	69	3		1		
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	257	129	68	27	13	5	15	73	55	11	2	1	2	2
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	260	148	46	17	11	3	35	73	50	8	6	3	3	3
Sonstiges "Social Engineering" (gezielte Täuschung von Mitarbeitenden)	260	218	18	11	5		8	73	63	6		2		2
Andere Angriffsart	245	236	5	2			2	73	70	1		2		

Tabelle 56: Häufigkeit der Angriffe absolut (MEM CH, LOG CH & LOG+ CH)

Häufigkeit der Betroffenheit durch einzelne Angriffsarten (in Prozent)	MEM CH							LOG CH & LOG+ CH						
	In den letzten 24 Monaten vor der Befragung							In den letzten 24 Monaten vor der Befragung						
	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal	N =	0 mal	1-2 mal	3-5 mal	6-10 mal	11-20 mal	mehr als 20 mal
Ransomware-Angriff (um Daten zu verschlüsseln)	266	88.7%	10.5%	0.8%				73	87.7%	9.6%		2.7%		
Spyware-Angriff (um zur Daten auszuspähen)	263	91.6%	6.5%	0.8%		0.4%	0.8%	73	89.0%	6.8%		1.4%	1.4%	1.4%
Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner)	261	79.3%	12.3%	5.4%	1.1%	0.4%	1.5%	73	87.7%	9.6%	1.4%	1.4%		
Manuelles Hacking (um Soft- und Hardware zu manipulieren)	263	82.9%	11.0%	3.0%	1.5%		1.5%	73	95.9%	2.7%		1.4%		
(D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten)	262	88.5%	7.6%	1.1%	1.5%		1.1%	73	89.0%	8.2%	1.4%	1.4%		
Defacing-Attacke (um Inhalte von Websites zu verändern)								73	94.5%	4.1%		1.4%		
"CEO-Fraud" (Vortäuschung einer Führungspersönlichkeit)	257	50.2%	26.5%	10.5%	5.1%	1.9%	5.8%	73	75.3%	15.1%	2.7%	1.4%	2.7%	2.7%
Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten)	260	56.9%	17.7%	6.5%	4.2%	1.2%	13.5%	73	68.5%	11.0%	8.2%	4.1%	4.1%	4.1%
Sonstiges "Social Engineering" (gezielte Täuschung von Mitarbeitenden)	260	83.8%	6.9%	4.2%	1.9%		3.1%	73	86.3%	8.2%		2.7%		2.7%
Andere Angriffsart	245	96.3%	2.0%	0.8%			0.8%	73	95.9%	1.4%		2.7%		

Tabelle 57: Häufigkeit der Angriffe in Prozent (MEM CH, LOG CH & LOG+ CH)

«Schwerwiegendster Angriff»

In der MEM-Branche wurden im Vergleich zur Logistikbranche öfter «Phishing-Angriffe» (Differenz: 5.2%), «CEO-Fraud» (Differenz: 6.5%) und «manuelles Hacking» (Differenz: 6.7%) als «schwerwiegendste Angriffe» genannt.

Die Logistikbranche verzeichnete einzig mehr «(D)DoS-Angriffe» als die MEM-Branche (Differenz: 3.5%). Die Stichprobengrösse lässt jedoch keine verallgemeinernden Rückschlüsse zu.

Sie haben angegeben, dass Ihr Unternehmen in den letzten 24 Monaten angegriffen wurde. Welcher dieser Angriffe war aus Ihrer Sicht der schwerwiegendste?

Wirtschaftszweig Gruppe	Erfolgreicher Angriff mit Ransomware, bei dem Unternehmensdaten verschlüsselt wurden	Abhören oder Abfangen digitaler Kommunikation, z.B. E-Mails, Telefonate, Besprechungen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Hackerangriff (manuelles Hacking) auf IT-Systeme un Firmengeräte, d.h. die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware	Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten		"CEO-Fraud", wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Sonstiges "Social Engineering", bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden	Anderer, bei der vorherigen Frage genannter Angriff
MEM CH (N = 271)	20	10	18	22	9		51	66	10	3
	7.4%	3.7%	6.6%	8.1%	3.3%		18.8%	24.4%	3.7%	1.1%

Abbildung 41: Schwerwiegendster Cyberangriff (MEM CH)

Sie haben für die unten aufgeführten Angriffsarten angegeben, dass Ihr Unternehmen in den letzten 24 Monaten von diesen betroffen war. Welcher dieser Angriffe war aus Ihrer Sicht der schwerwiegendste?

Wirtschaftszweig Gruppe	Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen	Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner	Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware	Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten	Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern	«CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung	Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden	Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen	Andere Angriffsart
LOG CH (N = 45)	2	2	1	0	4	1	7	7	0	0
	4.4%	4.4%	2.2%	0.0%	8.9%	2.2%	15.6%	15.6%	0.0%	0.0%
LOG+ CH (N = 28)	4	1	1	1	1	1	2	7	1	1
	14.3%	3.6%	3.6%	3.6%	3.6%	3.6%	7.1%	25.0%	3.6%	3.6%
LOG CH & LOG+ CH (N = 73)	6	3	2	1	5	2	9	14	1	1
	8.2%	4.1%	2.7%	1.4%	6.8%	2.7%	12.3%	19.2%	1.4%	1.4%

Tabelle 58: Schwerwiegendster Cyberangriff (LOG CH & LOG+ CH)

Lösegeldforderung

In beiden Branchen wurden ähnlich wenig Fälle gemeldet, wo ein Lösegeld bezahlt worden ist. Aufgrund der kleinen Stichprobengrösse lassen sich aber keine verallgemeinernden Schlüsse daraus ziehen.

Erpressung mit entwendeten oder verschlüsselten Daten: Lösegeldforderung?

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
MEM CH (N = 271)	Ja	10	3.7%
	Nein	1	0.4%
	Weiss nicht	2	0.7%
	Keine Angabe	258	95.2%

Gab es bei diesem schwerwiegendsten Angriff eine Lösegeldforderung?

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
LOG CH (N = 45)	nein	2	4.4%
	Keine Angabe	43	95.6%
LOG+ CH (N = 28)	Ja	2	7.1%
	Nein	1	3.6%
	Keine Angabe	25	89.3%
LOG CH & LOG+ CH (N = 73)	Ja	2	2.7%
	Nein	3	4.1%
	Keine Angabe	68	93.2%

Tabelle 59: Lösegeldforderungen (MEM CH, LOG CH & LOG+ CH)

Durch Angriff verursachte Kosten

Die Schadenhöhe in der MEM-Branche fällt bei Vergleich des Medians dreissigmal höher aus als in der Logistikbranche. Welche Art von Kosten angefallen waren, wurde nicht untersucht.

Wie hoch war die Schadenhöhe in CHF?

Wirtschaftszweig Gruppe	MEM CH (N = 271)	Antworten	77
		Mittelwert	205'143
		Median	30'000
		Std.-Abweichung	463'194
		Spannweite	2'000'000
		Minimum	-
		Maximum	2'000'000

Bitte geben Sie an, welche Kosten durch den von Ihnen angegebenen schwerwiegendsten Angriff in CHF entstanden sind.

Wirtschaftszweig Gruppe	LOG CH (N = 45)	Antworten	21
		Mittelwert	37'227
		Median	524
		Std.-Abweichung	85'935
		Spannweite	300'000
		Minimum	-
		Maximum	300'000
	LOG+ CH (N = 28)	Antworten	10
		Mittelwert	100'112'350
		Median	1'250
		Std.-Abweichung	316'188'443
		Spannweite	1'000'000'000
		Minimum	-
		Maximum	1'000'000'000
	LOG CH & LOG+ CH (N = 73)	Antworten	31
		Mittelwert	32'319'525
		Median	1'000
		Std.-Abweichung	179'593'994
		Spannweite	1'000'000'000
		Minimum	-
		Maximum	1'000'000'000

Tabelle 60: Durch Angriffe verursachte Kosten (MEM CH, LOG CH & LOG+ CH)

Betroffene Daten

Die betroffenen Datenkategorien verteilen sich in beiden Branchen auf alle Kategorien. «Kunden- und Personenbezogene Daten» scheinen in der MEM-Branche etwas öfter betroffen zu sein, wobei die Stichprobe sehr klein ist und keine verallgemeinernden Rückschlüsse zulässt.

Waren durch den Angriff folgende Daten betroffen?

Wirtschaftszweig Gruppe		Kunden- und personenbezogene Daten		Betriebswirtschaftliche Daten		Produktions- und Prozessdaten		Produkt und F & E Daten		andere Daten	
		Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent
MEM CH	ja, sie wurden gelöscht	1	0.6	3	1.8	3	1.8	1	0.6	2	1.2
	ja, sie wurden manipuliert	9	5.5	7	4.3	3	1.8	2	1.2	3	1.8
	ja, sie wurden gestohlen	11	6.7	4	2.4	4	2.4	5	3.0	4	2.4
	ja, sie wurden verschlüsselt oder blockiert	10	6.1	11	6.7	10	6.1	9	5.5	6	3.7
	ja (total)	31	18.9	25	15.2	20	12.2	17	10.4	15	9.1
	nein	116	70.7	124	75.6	130	79.3	129	78.7	111	67.7
	weiss nicht	13	7.9	10	6.1	10	6.1	11	6.7	18	11.0
	N	**164**	**100.0**	**164**	**100.0**	**164**	**100.0**	**164**	**100.0**	**164**	**100.0**

Waren bei dem genannten schwerwiegendsten Angriff die folgenden Daten betroffen? Wurden diese gelöscht, manipuliert, gestohlen oder verschlüsselt?

Wirtschaftszweig Gruppe		Kunden- und personenbezogene Daten		Betriebswirtschaftliche Daten		Produktions- und Prozessdaten		Produkt und F&E Daten		Andere Daten	
		Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent	Häufigkeit	Prozent
LOG CH	ja, sie wurden gelöscht	1	4.8								
	ja, sie wurden verschlüsselt oder blockiert	1	4.8	1	4.8	1	4.8	1	4.8	1	4.8
	ja (total)	**2**	**9.5**	**1**	**4.8**	**1**	**4.8**	**1**	**4.8**	**1**	**4.8**
	nein	18	85.7	19	90.5	19	90.5	19	90.5	19	90.5
	keine Angabe	1	4.8	1	4.8	1	4.8	1	4.8	1	4.8
	N	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**	**21**	**100.0**
LOG+ CH	ja, sie wurden gestohlen			1	3.6					1	3.6
	ja, sie wurden manipuliert	1	3.6								
	ja, sie wurden verschlüsselt oder blockiert	1	3.6	1	3.6	2	7.1	2	7.1	1	3.6
	ja (total)	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**	**2**	**7.1**
	nein	7	25.0	7	25.0	7	25.0	7	25.0	7	25.0
	keine Angabe	2	7.1	2	7.1	2	7.1	2	7.1	2	7.1
	N	**28**	**100.0**	**11**	**100.0**	**11**	**100.0**	**11**	**100.0**	**11**	**100.0**
LOG CH & LOG+ CH	ja, sie wurden gelöscht	1	3.1								
	ja, sie wurden gestohlen			1	3.1					1	3.1
	ja, sie wurden manipuliert	1	3.1								
	ja, sie wurden verschlüsselt oder blockiert	2	6.3	2	6.3	3	9.4	3	9.4	2	6.3
	ja (total)	**4**	**12.5**	**3**	**9.4**	**3**	**9.4**	**3**	**9.4**	**3**	**9.4**
	nein	25	78.1	26	81.3	26	81.3	26	81.3	26	81.3
	keine Angabe	3	9.4	3	9.4	3	9.4	3	9.4	3	9.4
	N	**49**	**100.0**	**32**	**100.0**	**32**	**100.0**	**32**	**100.0**	**32**	**100.0**

Tabelle 61: Betroffene Daten (MEM CH, LOG CH & LOG+ CH)

Folgen des «schwerwiegendsten Angriffes»

Beide Branchen zeigen eine ähnliche Verteilung der Folgen. Die Logistikbranche schätzt die Folgen leicht gravierender ein als die MEM-Branche. Die Stichprobengrösse und -art gilt es auch hier zu berücksichtigen.

Nähere Angaben zum Schaden - Bitte ergänzen Sie: Der durch den schwerwiegendsten Angriff erfolgte Schaden...

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
MEM CH (N = 95)	zog keine Einschränkungen nach sich	13	13.7%
	war kurzfristig behebbar und leicht verdaubar	65	68.4%
	führte zu spürbaren Einschränkungen	15	15.8%
	gefährdete die Existenz des Unternehmens	2	2.1%

Abbildung 42: Nicht-materieller Schaden (LOG CH & LOG+ CH)

Bitte ergänzen Sie: Der durch den schwerwiegendsten Angriff erfolgte Schaden...

Wirtschaftszweig Gruppe		Häufigkeit	Prozent
LOG CH (N = 21)	zog keine Einschränkungen nach sich	7	33.3%
	war kurzfristig behebbar und leicht verdaubar	13	61.9%
	führte zu spürbaren Einschränkungen	0	0.0%
	gefährdete die Existenz des Unternehmens	1	4.8%
LOG+ CH (N = 11)	zog keine Einschränkungen nach sich	3	27.3%
	war kurzfristig behebbar und leicht verdaubar	5	45.5%
	führte zu spürbaren Einschränkungen	3	27.3%
	gefährdete die Existenz des Unternehmens	0	0.0%
LOG CH & LOG+ CH (N = 32)	zog keine Einschränkungen nach sich	10	31.3%
	war kurzfristig behebbar und leicht verdaubar	18	56.3%
	führte zu spürbaren Einschränkungen	3	9.4%
	gefährdete die Existenz des Unternehmens	1	3.1%

Tabelle 62: Nicht-materieller Schaden (LOG CH & LOG+ CH)

Technische IT-Sicherheitsmassnahmen

Der Umsetzungsgrad der 11 technischen IT-Sicherheitsmassnahmen liegt in der MEM-Branche (inkl. der «nach dem Angriff umgesetzten») bei 71.4%, was ein höherer Durchschnittswert darstellt als in der Logistikbranche mit 67.2% (Differenz: 4.2%). Bei Betrachtung des Umsetzungsgrades (inkl. der «nach dem Angriff» umgesetzten Massnahmen) fällt auf, dass Unternehmen der MEM-Branche technologisch einen Vorsprung auf die Logistikbranche haben. Folgende technischen IT-Sicherheitsmassnahmen sind in der MEM-Branche ausgeprägter im Einsatz:

- *«Informationssicherheitsmanagementsystem (ISMS)» (Differenz: 17.6%)*
- *«Mindestanforderungen für Passwörter» (Differenz: 9.4%)*
- *«Netzwerksegmentierung» (Differenz: 9.4%)*
- *«Aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates» (Differenz: 9.1%)*

Die Logistikbranche hat allerdings geplant, den Umsetzungsgrad der technischen IT-Sicherheitsmassnahmen durchschnittlich um 5.5% zu erhöhen.

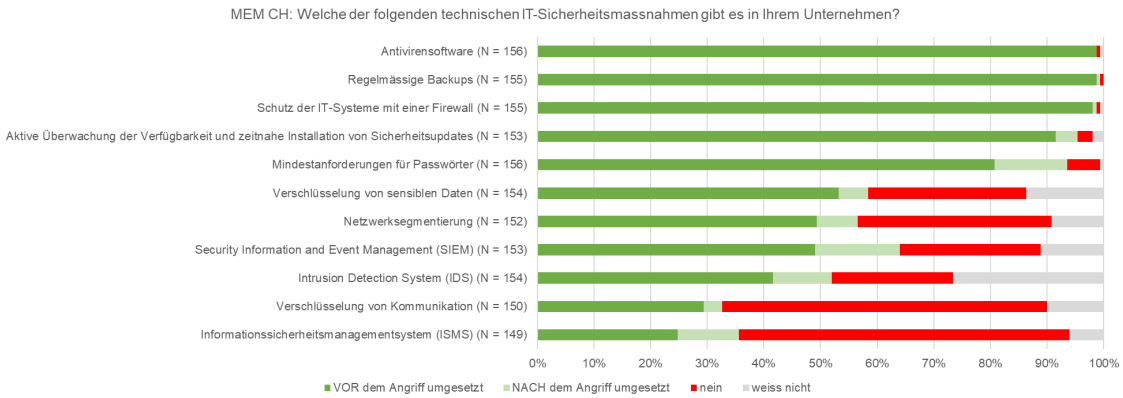


Abbildung 43: Technische IT-Sicherheitsmassnahmen (MEM CH)

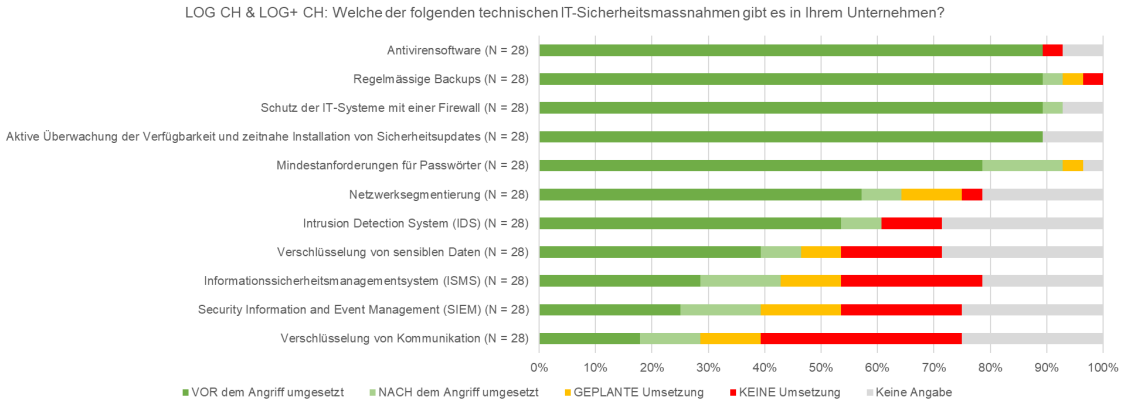


Abbildung 44: Technische IT-Sicherheitsmassnahmen (LOG CH & LOG+ CH)

Organisatorische IT-Sicherheitsmassnahmen

Die Logistikbranche ist der MEM-Branche beim Umsetzungsgrad der neun organisatorischen IT-Sicherheitsmassnahmen (inkl. der «nach dem Angriff umgesetzten») einen Schritt voraus (Differenz: 4.7%).

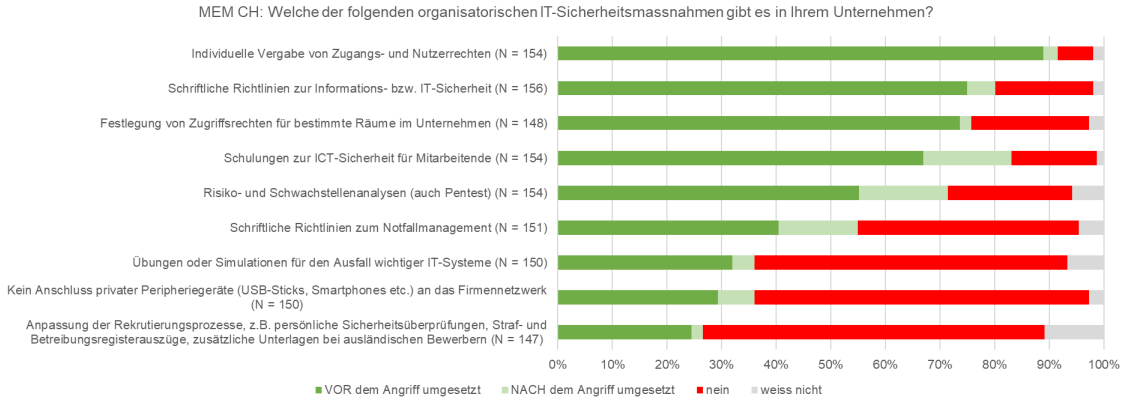


Abbildung 45: Organisatorische IT-Sicherheitsmassnahmen (MEM CH)

Nachfolgende organisatorischen IT-Sicherheitsmassnahmen machen den Unterschied:

- *«Schriftliche Richtlinien zum Notfallmanagement» (Differenz: 19.6%)*
- *«Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk» (Differenz: 17.9%)*
- *«Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern» (Differenz: 15.9%)*

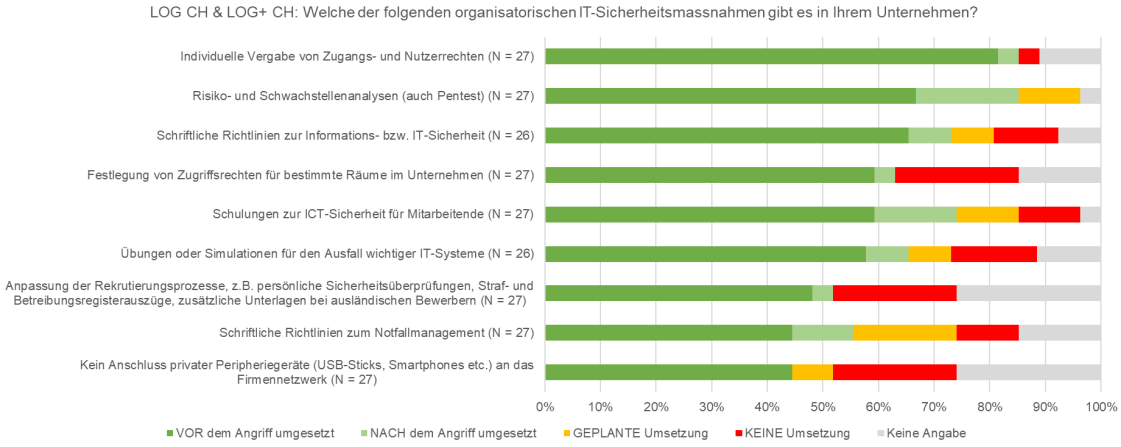


Abbildung 46: Organisatorische IT-Sicherheitsmassnahmen (LOG CH & LOG+ CH)

Die MEM-Branche hingegen hat die «Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen» häufiger umgesetzt, wie die Logistikbranche (Differenz: 20.2%).

Zusammenfassung

In Bezug auf die registrierten Cyberangriffe ist die MEM-Branche häufiger von «CEO-Fraud» und «manuellem Hacking» betroffen als die Logistikbranche. So wird «CEO-Fraud» in der MEM-Branche auch häufigsten als «schwerwiegendster Angriff» aufgeführt, während in der Logistikbranche «Phishing» diesen Platz einnimmt.

Der durch Angriffe verursachte Kosten-Median liegt in der MEM-Branche auf einem dreissigmal höheren Niveau als in der Logistikbranche. Generell hat die MEM-Branche bei den technischen IT-Sicherheitsmassnahmen einen höheren Umsetzungsgrad erreicht als die Logistikbranche. Diese kann bei den organisatorischen Massnahmen einen Vorsprung für sich beanspruchen.

4.3 Fachgespräch

Die Resultate der bisherigen Kapitel wurden im Rahmen eines Fachgesprächs diskutiert. Folgende Expertin und Experten nahmen an dieser Diskussionsrunde teil, die über Microsoft Teams durchgeführt und aufgezeichnet wurde.

Teilnehmende	Funktion	Organisation
Experte 1	Head of Industry Engagement Transport and Logistics	Internationaler Verein zur Standardisierung von Logistikprozessen
Experte 2	Geschäftsleiter Industrie 2025	Schweizer Branchenverband
Experte 3	Chief Information Officer (CIO)	Internationales Transport- und Logistikunternehmen
Experte 4	Leiter Logistik und Europaverkehre	Internationales Transport- und Logistikunternehmen
Expertin 5	Chief Information Security Manager (CISO)	Internationales Transport- und Logistikunternehmen

Tabelle 63: Teilnehmende am Fachgespräch

Die nachfolgende Zusammenfassung gibt einen Überblick, wie die Branchenvertreter:innen zu den einzelnen Themen stehen. Die Teilnehmenden des Gesprächs und der zusammengefasste Gesprächsverlauf sind im Anhang zu finden

Stellenwert der Mitarbeitenden

Der Faktor Mensch wird im Kontext der Cyberabwehr als äusserst relevant erachtet. Die technischen IT-Sicherheitsmassnahmen dürfen dabei aber nicht vernachlässigt werden, da diese die Grundlage jeder Cyberabwehr bilden und zwingend umfassend umgesetzt werden müssen. «Cyber Awareness Trainings» für alle Mitarbeitenden sind insbesondere bei KMU nicht üblich. Viel eher werden Informationsveranstaltungen den eigentlichen Schulungen vorgezogen. Dies wird mit dem Argument begründet, dass es sehr lange dauern kann, bis eine Schulungs-Kultur etabliert ist und dafür oft aufgrund der Kosten grosse Überzeugungsarbeit beim Management geleistet werden muss. Gleichzeitig ist die Bereitschaft, technische IT-Sicherheitsmassnahmen umzusetzen sehr gross, da dies auch oft in der alleinigen Verantwortung der IT-Abteilung liegt. Die Fachpersonen waren sich einig, dass sich E-Learning v.a. für die initiale Sensibilisierung der Mitarbeitenden gut eignet. Im Anschluss an solche Einführungen sollten jedoch stets noch individuell an die Firma sowie den Tätigkeits- und Verantwortungsbereich angepasste Schulungen vor Ort durchgeführt werden. Basis für diese individuellen Trainings sind die zuvor eruierten Risiken in den jeweiligen Bereichen. Auch eine anschliessende Überprüfung des Verhaltens und eine Begleitung derjenigen, die etwas länger benötigen, um das Thema aufzunehmen, wurde im Gespräch empfohlen.

Wahrnehmung der Risiken

Cyberrisiken werden aus Sicht der Fachpersonen oft nicht wahrgenommen und v.a. Geschäftsleitungen von KMU wiegen sich oft in falscher Sicherheit, da das Thema Cybersicherheit an die IT-Leitung, einen externen Dienstleister oder eine Versicherung delegiert wurde. Für eine Risikoeinschätzung muss beim Management ein Grundwissen vorhanden sein, damit die Risiken korrekt antizipieren werden können. Es wird empfohlen, die Cyberrisiken in das zentrale und fortlaufend neu beurteilte Risikomanagement zu integrieren. Generell wird das Risiko, Opfer eines Cyberangriffs zu werden, als sehr hoch eingestuft.

Kommunikation der Cyberangriffe

Die Logistikbranche tut sich schwer damit, einen Angriff proaktiv an die Kundschaft zu kommunizieren, da diese in der Folge die benötigte Logistikdienstleistung möglicherweise schnell und vermutlich dauerhaft bei einem anderen Dienstleister beziehen würde. Es wurde diskutiert, dass es den angegriffenen Unternehmen vermutlich nicht bewusst war, dass sie eine Meldung an das NCSC hätten erstatten sollten, zudem hätten Unternehmen nach einem Cyberangriff oft andere Probleme zu bewältigen. Es bestand im Gespräch Konsens darüber, dass eine Meldung ans NCSC in anonymisierter Form für alle vorteilhaft wäre. Es wird ferner empfohlen, dass alle Unternehmen ein Kommunikationskonzept ausarbeiten, wie auf unterschiedlich schwere Angriffe zu reagieren ist.

Anwendung von IT-Sicherheitsmassnahmen

Die MEM-Branche ist traditionell in KMU organisiert und technisch geprägt. Dies führt dazu, dass die technischen IT-Sicherheitsmassnahmen Priorität haben. Zudem sind organisatorische Massnahmen schwieriger umzusetzen und haben oft auch eine kulturelle Dimension. Aktuell findet noch keine Diskussion statt, inwiefern künstliche Intelligenz eine Veränderung der Cyber-Bedrohungslage zur Folge haben könnte. Es wird jedoch davon ausgegangen, dass v.a. «Phishing-Angriffe» immer schwieriger als solche zu erkennen sind und dass sich die Frequenz noch einmal erhöhen wird.

Bedrohung durch Cyberangriffe

Es wurde einerseits eine Zunahme der Cyberangriffe festgestellt, andererseits standen bisher im Jahre 2023, aufgrund der geopolitischen Situation (Krieg in der Ukraine, Energiepreise, Inflation, etc.), andere Themen im medialen Fokus. Einen direkten Anstieg der Cyberangriffe konnte von niemandem festgestellt werden. Die in der Schweiz überdurchschnittliche Häufigkeit des «CEO-Fraud» wurde mit der flachen Hierarchie in der KMU-dominierten Schweiz in Verbindung gebracht. Für Mitarbeitende ist ein CEO eher greifbar als in einem Unternehmen in Deutschland.

5. Diskussion

In diesem Kapitel wird die Hauptforschungsfrage «Wie stellt sich die aktuelle Situation in Bezug auf Cyberangriffe und IT-Sicherheitsmassnahmen in der Logistikbranche im Vergleich zur MEM-Branche dar?» diskutiert. Es werden dazu die Literatur, die Daten der Online-Umfrage und die die Vergleiche zur Schweizer MEM- sowie zur deutschen Logistikbranche herangezogen. Weiter werden die Aussagen aus dem Fachgespräch aufgegriffen. Die Zeitangaben der Zitate beziehen sich auf die Aufzeichnung des Fachgespräches.

Ausbildung des Personals steht im Mittelpunkt

Die durchgeführten Umfragen bestätigten, dass die Logistik-, wie auch die MEM-Branche in der Schweiz und Deutschland, am meisten durch «Phishing-Angriffe» bedroht werden. Es entspricht auch der Aussage im «IBM Security X-Force Threat Intelligence Index 2023», dass «Phishing» der Hauptangriffsvektor ist, der in 41% der Fälle identifiziert werden konnte (Worley et al., 2023). Ferner sind beim weit verbreiteten «CEO-Fraud» und «sonstigem Social Engineering» die Mitarbeitenden und ihr Urteilsvermögen das zentrale Element und müssen mit besonderer Aufmerksamkeit bedacht werden (Firstbrook et al., 2022). Dies wird auch von NCSC im aktuellen Halbjahresbericht (NCSC, 2023) und im Rahmen des Fachgespräches bestätigt:

«Der Faktor Mensch macht 70-80% der Verteidigungsschiene aus.»

Expertin 5 (12:33)

Die Angriffsart «CEO-Fraud», von der die Schweizer MEM-Branche beim «schwerwiegendsten Angriff» mit 18.8% auffällig oft betroffen war, zeigte auch in der Schweizer Logistikbranche mit 12.3% einen erhöhten Wert. In Deutschland verzeichnete die Logistikbranche lediglich 6.3% und die MEM-Branche 6.2% «schwerwiegendste Angriffe» mit «CEO-Fraud». Die Häufigkeit von «CEO-Fraud» scheint ein Schweizer Phänomen zu sein. Im Fachgespräch wurde die Hypothese diskutiert, dass in der Schweiz KMU mit flachen Hierarchien weit verbreitet sind und deshalb der/die CEO für die Mitarbeitenden greifbarer ist als in einer vergleichbaren Situation in Deutschland.

«In der Schweiz ist die Wahrscheinlichkeit viel höher, dass die Mitarbeitenden Kontakt mit den CEO haben. In einer KMU-Struktur mit flacher Hierarchie ist ein CEO greifbarer. Dies könnte ein Grund sein, weshalb «CEO-Fraud» in der Schweiz besser funktioniert und deshalb auch häufiger auftritt.» Experte 4 (59:20)

Die Umfrage in der Schweizer Logistikbranche bestätige einerseits, dass Schulungen für Mitarbeitende als organisatorische IT-Sicherheitsmassnahme bei Unternehmen, die von einem Angriff betroffen waren, nach dem Angriff zu 74.1% und bei nicht angegriffenen Unternehmen zu 66.7% umgesetzt waren, andererseits zeigten die Fragen nach der Ausgestaltung der Trainings ein differenzierteres Bild. Zwei Drittel der Unternehmen führen die «Cyber Awareness Trainings» nicht in verschiedenen Sprachen und an die Zielgruppe angepasst durch. Es fehlt auch an Erfolgskontrollen und spezifischen Trainings für Mitarbeitende, die im Homeoffice arbeiten. Auch die regelmässige Wiederholung ist nicht sichergestellt. Doch genau diese Elemente werden von Chowdhury et al. (2022), Alkhazi et at. (2022) und Hijji & Alam (2022) in ihren Konzepten empfohlen, um die Mitarbeitenden einerseits zu sensibilisieren, andererseits zu involvieren und um die Cybersicherheit zu erhöhen (Wong et al., 2022). Nachfolgendes Zitat aus dem Fachgespräch bestätigt die Wichtigkeit von Erfolgskontrollen:

«Es erwies sich auch als zielführend, dass nach «Awareness Trainings» eine Überprüfung gemacht wurde, um einzelne Mitarbeitende, die bei der Überprüfung nicht erfolgreich waren, noch einmal zu informieren und ihnen das Ganze noch einmal zu erklären.» Experte 3 (17:38)

In der deutschen Logistikbranche wurde die organisatorische IT-Sicherheitsmassnahme der Schulung nicht erhoben. In der Schweizer MEM-Branche zeigte sich jedoch, dass die organisatorische IT-Sicherheitsmassnahme «Schulungen zur ICT-Sicherheit für Mitarbeitende» bei Unternehmen, die von einem «schwerwiegendsten Angriff» betroffen waren, vor dem Angriff bei 67% und nach dem Angriff bei 83.1% lag. Dies war eine Massnahme mit der grössten durch einen Angriff hervorgerufenen Steigerung von 16.2% (Isenhardt et al., 2022). Die Schweizer Logistikbranche steigerte sich durch die erlebten Angriffe in dieser Massnahme um 14.8%. Es besteht also in beiden Branchen Verbesserungspotential. Dies wurde im Schlussbericht der MEM-Umfrage (Initiative «Industrie 2025», 2023) jedoch nicht sehr prominent ausgewiesen. Das Fachgespräch ergab, dass Schulungen für die Mitarbeitenden in der Schweizer MEM-Branche nicht im Zentrum stehen, da lieber in technische IT-Sicherheitsmassnahmen investiert wird. Vor allem KMUs sehen die Notwendigkeit von Schulungen oft nicht ein und es bedarf grösserer Überzeugungsarbeit seitens IT / CISO, um flächendeckende Schulungen durchführen zu können. Der Faktor Mensch wird allgemein als sehr wichtig erachtet, die technischen IT-Sicherheitsmassnahmen müssen aber dennoch als Grundvoraussetzung alle umgesetzt werden. E-Learning wird als geeignetes Mittel zur Sensibilisierung der Mitarbeitenden gesehen, muss aber noch mit individualisierten Trainings vor Ort (inkl. Erfolgskontrolle) ergänzt werden.

> *«KMU haben oft das Gefühl, alles selbst machen zu müssen. Doch genau in dem Thema gibt es unterdessen sehr gute Dienstleister auf dem Markt, die «Cyber Awareness Trainings» anbieten. Da sollte der Beizug externer Hilfe unbedingt in Betracht gezogen werden.»*
> *Experte 2 (16:44)*

Im Fachgespräch wurde betont, dass Training sehr gut durch externe Dienstleister vorbereitet werden können. Dies entspricht der Empfehlung von Ullah und Nab (2022), angebotene Services von externen Sicherheitsdienstleistern zu nutzen. Die Online-Umfrage zeigte auch, dass bereits über 40% der Unternehmen IT-Funktionen, wie «E-Mail & Kommunikation», «Netzwerk-Administration & Wartung», den Webauftritt und «Cloud-Software & Cloud-Speicher» sowie die «IT-Security» ausgelagert haben. Die Expertin und Experten waren sich auch einig, wie wichtig es ist, dass eine Anpassung der Trainingsinhalte an die lokalen Gegebenheiten (Gebäude, Prozess, Tätigkeiten, etc.) stattfindet, damit sich die Mitarbeitenden damit identifizieren können.

Wahrnehmung der Risiken in der Geschäftsleitung

Die Unternehmen der Schweizer Logistikbranche schätzen die Wahrscheinlichkeit, in den nächsten 12 Monaten von einem Cyberangriff geschädigt zu werden, der gleichzeitig auch viele andere Unternehmen trifft, zu 49% als «sehr/eher gering» und zu 48% als «eher/sehr hoch» ein. Diese ausgewogene Risikoeinschätzung widerspricht einerseits dem aktuellen «Cisco Cybersecurity Readiness Index», der von 82% der Verantwortlichen berichtet, die eine Beeinträchtigung durch einen Cyberangriff in den nächsten 12-24 Monaten als wahrscheinlich erachten (Cisco, 2023)und andererseits den Umfrageergebnissen aus der deutschen MEM- und Logistik-Branche (Dreißigacker et al., 2021), die diese Frage mit 39% bzw. 40% als «sehr/eher gering» und mit 57% % als «eher/sehr hoch» einstufen.

Es kann davon ausgegangen werden, dass Personen in der Rolle als Geschäftsführende oder Vorstandsmitglieder aufgrund der notwendigen Berufserfahrung tendenziell älter sind. Geil et al. (2018) zeigten, dass das Alter einen Einfluss auf die Wahrnehmung von Cyberrisiken hat. Es muss davon ausgegangen werden, dass die an der Online-Umfrage teilnehmenden, insbesondere die 39% geschäftsführende Personen oder Vorstandsmitglieder, das Risiko als zu tief einstufen. Dies haben bereits Pawlowska und Scherrer (2021) festgestellt und auch das Fachgespräch bestätigt:

> *«Das Risiko eines Cyberangriffes ist so hoch, dass gesagt werden kann, dass heute zu wenig getan wird» Experte 4 (34:04)*

Die MEM-Branche thematisierte dieses Thema in der Umfrage nicht. Das Fachgespräch ergab, dass sich speziell Geschäftsleitungen von KMU in der MEM-Branche oft in falscher Sicherheit wiegen, wenn das Thema an die IT-Verantwortlichen abgegeben oder an eine Versicherung delegiert wurde. Generell wurde festgestellt, dass ein zentrales Risikomanagement (inkl. der Cyberrisiken) aufgebaut und regelmässig begutachtet werden muss. Es muss in der Geschäftsleitung verankert sein und durch den CIO sichergestellt werden, dass sich die Geschäftsleitung der Cyberrisiken bewusst ist und die Rahmenbedingungen schaffen kann, die auch Bedrohungen durch Insider reduzieren (Silaule et al., 2022). Der Beizug externer Dienstleister wurde im Fachgespräch mehrmals genannt, um speziell KMU ohne eigene Abteilung für Informationssicherheit, zu stärken. Dies entspricht auch der aktuellen Empfehlung des NCSC, dass die Zuweisung von

Ressourcen an Cybersicherheitsmassnahmen im Rahmen des Risikomanagements entschieden werden muss (NCSC, 2023).

Kommunikation von Cyberangriffen

Es wurde festgestellt, dass die gemeldeten Lösegeldforderungen (MEM CH 3.7%, LOG CH 2.7%) bei weitem nicht den 27% der Fälle entsprachen, die IBM nannte (Worley et al., 2023). Dies lässt vermuten, dass eine Mehrheit der Geschäftsführenden aufgrund eines potenziellen Reputationsschadens Cyberangriffe immer noch nicht kommunizieren wollen (Mändli & Repic, 2017). Wie aktuell diese Befürchtung ist, zeigt nachfolgendes Zitat aus dem Fachgespräch:

> *Bevor einem Kunden proaktiv kommuniziert wird, dass man Opfer eines Cyberangriff wurde und für eine unbestimmte Zeit handlungsunfähig ist, wird versucht, dem Kunden irgendeine Geschichte zu erzählen, um Zeit zu gewinnen.» Experte 4 (40:50)*

Der tiefe Umsetzungsgrad der technischen IT-Sicherheitsmassnahme «Cyber Threat Intelligence» (Austausch von Bedrohungsdaten) von 20% bei nicht angegriffenen Unternehmen stützt diese Vermutung. Betroffene Unternehmen erreichen vor dem «schwerwiegendsten Angriff» einen Umsetzungsgrad von 54%. Nach dem Angriff steigerte sich der Umsetzungsgrad dieser Sicherheitsmassnahme am meisten von allen technischen Massnahmen auf 75%. Die Logistikbranche zeigt hier eine erfreuliche Lernkurve, hat aber diesbezüglich noch grosses Potential. Die betroffenen Unternehmen gaben nach dem «schwerwiegendsten Angriff» zu 44% an, einen spezialisierten Dienstleiter kontaktiert zu haben. Nur 22% meldeten sich beim NCSC und 19% bei der Polizei. In der Schweizer MEM-Branche meldeten sich nach dem «schwerwiegendsten Angriff» lediglich 12% beim NCSC, was vermuten lässt, dass die Verschwiegenheit in dieser Branche noch grösser ist als in der Logistikbranche. Isenhardt et al. (2022) zeigten klar auf, dass hier noch Verbesserungspotential in der Schweizer MEM-Branche besteht. Das Fachgespräch ergab, dass dieser tiefe Wert nicht erklärbar ist, zumal «Cyber Intelligence» als wichtiges Instrument zur Erhöhung der Cybersicherheit erachtet wird, was der Empfehlung von Kostinas (2022) entspricht. Aus diesem Grund versucht auch die Politik aktuell, eine Cyberangriff-Meldepflicht für kritische Infrastruktur einzuführen (Botschaft zur Änderung des Informationssicherheitsgesetzes, 2022). Es zeigte sich im

Gespräch auch, dass nicht allen bewusst war, dass nach einem Cyberangriff dem NCSC eine Meldung erstattet werden sollte.

«Jedes Unternehmen sollte eine Kommunikationsstrategie haben. Dies abhängig vom Vorfall, um adäquat kommunizieren zu können. Auch hier sollte externe Hilfe beigezogen werden.» Experte 2 (39:50)

Es wurde angeregt, dass sich Unternehmen vor einem «schwerwiegenden Cyberangriff» ein Kommunikationskonzept erarbeiten, das verschieden starke Cyberangriffen vorsieht und auch die Information des NCSC vorsieht.

Anwendung der IT-Sicherheitsmassnahmen

Der durchschnittliche Umsetzungsgrad der IT-Sicherheitsmassnahmen lag bei den befragten Unternehmen der Schweizer Logistikbranche, die einen «schwerwiegendsten Angriff» erlebten, im Vergleich zur Schweizer MEM-Branche bei den technischen Massnahmen -4% tiefer und bei den organisatorischen Massnahmen +5% höher. Aufgrund der kleinen Stichprobe kann keine verallgemeinernde Aussage daraus abgeleitet werden, doch die Daten legen den Schluss nahe, dass die MEM-Branche öfter in «Informationssicherheitsmanagementsysteme (ISMS)» investiert und die Logistikbranche bessere «schriftliche Richtlinien zum Notfallmanagement» ausgearbeitet hat. Der globale «Cisco Cybersecurity Readiness Index» (Cisco, 2023) stuft 16% der Unternehmen der Transportbranche über alle Kriterien hinweg in die «Beginner» Kategorie ein, während die Fertigungsindustrie in Bezug auf ihr Device-Management sogar in die höchste Kategorie «ausgereift» eingestuft wird. Dieser Unterschied der Branchen lässt sich aufgrund der Umfragen für die Schweiz nicht bestätigen.

Generell lässt sich feststellen, dass diejenigen Unternehmen, die an den Umfragen teilgenommen haben, die Grundlagen der Cybersicherheit gut umgesetzt haben und speziell diejenigen, die Opfer eines Cyberangriffes wurden, ihre IT-Sicherheitsmassnahmen auf technischer, wie auch auf organisatorischer Ebene verbessert haben.

«Die technischen IT-Sicherheitsmassnahmen sind einfacher umzusetzen als diejenigen mit den Mitarbeitenden. Deshalb wurden in der Logistik vermutlich bereits viele technische Massnahmen

umgesetzt, während das Thema noch nicht in der Unternehmenskultur verankert ist.» Experte 1(47:43)

Eine Korrelation zwischen Betroffenheit und IT-Schutzmassnahmen lassen die vorliegenden Daten nicht quantitativ nachweisen. Doch beim qualitativen Vergleich der betroffenen und nicht betroffenen Unternehmen zeigt sich, dass die betroffenen Unternehmen vor dem Angriff weniger oft über eine «Firewall», «Antivirensoftware» und ein «Backup» verfügten und auch die «aktuellen Sicherheitspatches» nicht installiert hatten. Was klar für den Nutzen dieser grundlegenden IT-Sicherheitsmassnahmen spricht. Es wird vermutet, dass die Logistikbranche diese technischen Grundlagen noch nicht konsequent umgesetzt hat.

Die Umsetzung der in der Literaturrecherche (Kapitel 2.3 und 2.4) ausgeführten technischen und organisatorischen Schwerpunkte können aufgrund der vorhandenen Datenlage nicht umfassend beurteilt werden. Einzig die Frage nach dem Umsetzungsgrad der auf «künstlicher Intelligenz basierten Massnahmen» wurde in der Online-Umfrage gestellt und ergab, dass nach dem «schwerwiegendsten Angriff» bereits 46% der Unternehmen solche Massnahmen im Einsatz haben und weitere 7.1% der Unternehmen eine Umsetzung geplant haben. Die nicht angegriffenen Unternehmen wiesen bei auf «künstlicher Intelligenz basierten Massnahmen» lediglich einen Umsetzungsgrad von 10% auf, was sich mit den vorliegenden Daten nicht erklärt lässt. In der deutschen Logistikbranche setzen bereits 52% der Unternehmen auf «künstliche Intelligenz basierende Massnahmen» ein. Die MEM-Branche thematisierte das Thema der künstlichen Intelligenz in der Umfrage nicht, das Fachgespräch ergab jedoch anhand des Beispiels ChatGPT, dass aktuell in beiden Branchen die Diskussion geführt wird, wie künstliche Intelligenz die Cyberbedrohungslage verändern wird und wie die IT-Sicherheitsmassnahmen angepasst werden müssen.

«Da heute Content so schnell und auch automatisiert hergestellt werden kann, wird es immer leichter, erfolgreiche «Phishing-Angriffe» zu machen. Durch die Automatisierung der Angriffe wird mit einer noch höheren Frequenz gerechnet, die aufgrund der höheren Qualität auch zu mehr erfolgreichen Angriffen führen wird.» Experte 4 (51:20)

Es wird vielmehr vermutet, dass sich die Unternehmen nicht ausreichend bewusst sind, dass ihre Mitarbeitenden bereits ChatGPT in der Firma nutzen. Allgemein wird von einer Zunahme qualitativ immer besser werdenden «Phishing-Attacken» und «sonstigem Sozial Engineering» ausgegangen.

> *Aktuell steht die Faszination von ChatGPT im Vordergrund und die Risiken sind noch nicht fassbar. Es braucht noch mehr Zeit, bis das Risikobewusstsein bezüglich AI/KI vorhanden ist.» Experte 1 (50:45)*

Hier muss jedoch angemerkt werden, dass die Gelegenheitsstichprobe beider hier verwendeten Schweizer Umfragen keine repräsentative Aussage erlauben und weiterführende Forschung notwendig ist, um den generellen Stand der IT-Sicherheitsmassnahmen und insbesondere der Einsatz von auf «künstlicher Intelligenz basierten Massnahmen» in der Logistik- und MEM-Branche Branchen zu erheben.

Aktuelle Bedrohung durch Cyberangriffe

Die Rate der Unternehmen, die in den letzten 12 bzw. 24 Monaten angegriffen wurden, unterscheidet sich in den vorliegenden drei Datensätzen markant. So waren in der deutschen Logistikbranche 32 von 95 Unternehmen (34%), in der Schweizer MEM-Branche 167[19] von 271 (62%) und in der Schweizer Logistikbranche 33 von 73 (45%) von einem «schwerwiegendsten Angriff» betroffen. Die höheren Werte in der Schweiz lassen sich mit der Art der Stichprobe (Gelegenheits- vs. Zufallsstichprobe) und der Länge des Betrachtungszeitraumes (24 statt 12 Monate) begründen. Inwiefern angegriffene Unternehmen eher an einer Umfrage dieser Art teilnehmen, kann nicht beurteilt werden. Die Grössenordnung hingegen erstaunt nicht. Auch im «Cisco Cybersecurity Readiness Index» (Cisco, 2023) wird berichtet , dass fast 60 % der Befragten in den letzten 12 Monaten einen Vorfall im Bereich der Cybersicherheit erlebt haben. Auch die Versicherung Hiscox berichtete eine Zunahme der betroffenen Unternehmen innerhalb der letzten 12 Monate auf 48% (Hiscox, 2022b). Das

[19] Im Bericht von Isenhardt et al. (2022) werden 173 Unternehmen genannt, die mindestens einen Angriff innerhalb der letzten 24 Monaten verzeichnet haben. Der Unterschied zu den in dieser Arbeit ausgewiesenen 167 Unternehmen liegt in den gezählten Angriffsarten. In dieser Arbeit wurden die nachfolgenden Angriffe nicht mitgezählt: digitalen Daten bzw. Informationen durch eigene Mitarbeitende, Physischer Diebstahl von sensiblen physischen Dokumenten, Unrechtmässiger Abfluss von Daten durch Dritte und Digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen

Fachgespräch zeigte ebenfalls, dass ein deutlicher Anstieg An Cyberangriffen festgestellt werden konnte.

> *«Über die Rechtsberatung des Branchenverbands[20] konnte ein deutlicher Anstieg von Cyberangriffen registriert werden [und zwar] durch Firmen, die in der Aufbereitung der Vorfälle die Rechtsberatung in Anspruch genommen haben.» Experte 2 (55:12)*

Weiter zeigte sich, dass die Median-Kosten eines Cyberangriffes in der Schweizer MEM-Branche dreissigmal so hoch waren wie in der deutschen MEM-Branche und fünfzehnmal so hoch waren wie in der Schweizer und deutschen Logistikbranche. Gründe für diesen Umstand wurden keine erhoben. Diese Tatsache deckt sich aber mit der Aussage von Barth et al. (2020), dass die höchsten durchschnittlichen Schadenssummen je Unternehmen in den Branchen Chemie & Pharma, Maschinenbau und Automobil (in dieser Reihenfolge) festgestellt wurden.

Im Kontext des Krieges in der Ukraine, blieben grossflächige und schwere Angriffe, wie sie von westlichen Regierungen befürchtet worden waren, bisher aus (Worley et al., 2023). Weder im Fachgespräch noch in der Umfrage, konnten Hinweise auf vermehrte Cyberangriffe aus Russland identifiziert werden. Die befürchteten «Spillover-Effekte» (NCSC, 2022) konnten nicht nachgewiesen werden.

Fazit, Limitierungen und zukünftige Forschung

Die Untersuchung der Schweizer Logistikbranche zeigt ein mit der Schweizer MEM-Branche vergleichbares Bild. Beide Branchen wurden mittels einer Gelegenheitsstichprobe über die Branchenvereinigungen angefragt und beteiligten sich mit unterschiedlichem Rücklauf[21] an den Umfragen. Die eingangs gestellten Forschungsfragen[22] konnten im Rahmen dieser Arbeit alle diskutiert werden. Dabei zeigte sich, dass in der Logistikbranche noch Verbesserungspotential vorhanden ist.

---

[20] Der Name des Branchenverbandes wurde durch den Autor anonymisiert.

[21] MEM: 22.6%; LOG: 6.2%

[22] Wie stellt sich die aktuelle Situation in Bezug auf Cyberangriffe und IT-Sicherheitsmassnahmen in der Speditions- und Logistikbranche im Vergleich zur MEM-Branche dar? Auf welche Cyberangriffsarten mussten Unternehmen der Schweizer Speditions- und Logistikbranche in den letzten 24 Monaten reagieren? Welche IT-Sicherheitsmassnahmen wurden in Unternehmen der Schweizer Speditions- und Logistikbranche getroffen?

Da die Gelegenheitsstichprobe beider hier verwendeten Schweizer Umfragen keine repräsentative Aussagen erlauben, ist weiterführende Forschung notwendig. Insbesondere die Korrelation zwischen technischen und organisatorischen IT-Sicherheitsmassnahmen, ihrem Reifegrad und der Häufigkeit von erfolgreichen Angriffen sollte weiter untersucht werden. Dazu müsste für alle untersuchten Branchen eine repräsentative Stichprobe über einen längeren Zeitraum hinweg gezogen und die Ergebnisse gewichtet ausgewertet werden.

6. Empfehlungen

Zusammenfassend lassen sich folgende Empfehlungen für die Schweizer Logistikbranche ableiten:

1. Bewusstsein für Cyberrisiken in den Geschäftsleitungen schaffen

Geschäftsleitungen gestalten die Rahmenbedingungen und sprechen die Budgets, damit sich eine Cyber- und Informationssicherheitskultur etablieren kann. Dazu sollten alle Mitglieder dieses Führungsgremiums über aktuelles Wissen zum Thema Cybersicherheit verfügen, um die sich stetig ändernde Bedrohungslage beurteilen zu können. Letztere sollte regelmässig an Geschäftsleitungssitzungen traktandiert werden. Dazu sollten auch jüngere Mitarbeitende im Unternehmen und externe Dienstleistungsunternehmen beigezogen werden.

2. Integriertes Risikomanagement in den Geschäftsleitungen etablieren

Geschäftsleitungen beurteilen regelmässig die Unternehmensrisiken, indem sie ein Risikomanagementsystem bewirtschaften. Dabei sollten die Cyberrisiken unbedingt eingeschlossen und in kürzeren Zyklen überprüft werden als eher statische Risiken. Diese Aufgabe sollte nicht an den CIO oder ein externes Dienstleistungsunternehmen delegiert werden.

3. Nutzung externer Ressourcen

Oft verfügen kleinere und mittlere Unternehmen nicht über die notwendigen Ressourcen, um eine eigene IT-Sicherheitsabteilung zu betreiben. Es ist indes nicht sinnvoll, das Thema Cybersicherheit intern an jemanden im Nebenamt zu delegieren. Vielmehr sollten KMU professionelle Dienstleistungsunternehmen mit der Aufgabe betrauen bzw. fest einbinden, um die Cybersicherheit zu gewährleisten. Spezialisierte Dienstleister sind auch in der Lage, die Systeme rund um die Uhr zu überwachen, was für die Cybersicherheit entscheidend ist.

4. Risikobasierte und individualisierte «Cyber Awareness Trainings»

Das richtige Verhalten der Mitarbeitenden ist elementar in der Cyberabwehr. Und die Cybersicherheit immer nur so gut, wie das schwächste Einfallstor. Um alle Mitarbeitenden nachhaltig ausbilden zu können, sollten die Vorgesetzten gemeinsam mit den IT-Verantwortlichen das Arbeitsumfeld nach möglichen Cyberrisiken analysieren und daraus individuelle und gegebenenfalls mehrsprachige «Cyber Awareness Trainings» erstellen (z.B. Mitarbeitende der Buchhaltung in der Abwehr von «CEO-Fraud-Angriffen» ausbilden). Dabei sollte ein Augenmerk auf die Vermittlung der Inhalte gelegt werden, denn die Mitarbeitenden sind aufnahmefähiger, wenn das Training abwechslungsreich ist, Spass macht und sich die Teilnehmenden einbringen können.

5. Cyberangriffe ins «Business Contingency Planning» integrieren

Es sollte ein nach Schweregrad von Cyberangriffen abgestuftes Notfallkonzept erarbeitet werden (Krisenorganisation, aktueller Kundenstamm, externe Partner, Checklisten, Telefonlisten, Kommunikationskonzept, Ersatzgeräte, etc.). Die vorgesehenen externen Dienstleister sollten bei der Erstellung des Konzeptes bereits involviert werden. So kann sichergestellt werden, dass die Zusammenarbeit im Ernstfall funktioniert. Wichtig ist ferner, dass im Kommunikationskonzept eine Meldung an das NCSC vorgesehen ist. Es wird empfohlen, dass die Notfallszenarien nicht nur auf technischer, sondern auch auf organisatorischer Ebene regelmässig überprüft, angepasst und trainiert werden, um im Krisenfall angemessen und rasch reagieren zu können.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Aboah Boateng, E., Bruce, J. W., & Talbert, D. A. (2022). Anomaly Detection for a Water Treatment System Based on One-Class Neural Network. *IEEE access*, *10*, 115179–115191. https://doi.org/10.1109/ACCESS.2022.3218624

Addiscott, R., Michaels, A., D'Hoinne, J., Neubauer, L., Teixeira, H., Watts, J., Candrick, W., & Voster, W. (2023). *Top Trends in Cybersecurity 2023* (Nr. G00782545; Initiatives: Cyber Risk). Gartner.

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE access*, *10*, 32–43. https://doi.org/10.1109/ACCESS.2022.3230286

Alzahrani, A. I. A., Ayadi, M., Asiri, M. M., Al-Rasheed, A., & Ksibi, A. (2022). Detecting the Presence of Malware and Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques. *Electronics (Basel)*, *11*(22). https://doi.org/10.3390/electronics11223665

Baier, D., Biberstein, L., Girschik, K., & Wardak, S. (2022). *Cyberkriminalität gegen Organisationen im Sozialbereich. Ergebnisse einer Onlinebefragung im Kanton Zürich*. ZHAW, Soziale Arbeit.

Barth, M., Hellemann, N., Kob, T., Krösmann, C., Morgenstern, U., Tschersich, T., Ritter, T., Schulmann, H., Trapp, D., & Wintergerst, R. (2020). *Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt* (Studienbericht Nr. 2020). Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

Boyens, J., Brown, C., Deane, C., Diamond, T., Grayson, N., Hurlburt, J., Paulsen, C., Polk, W., Regenscheid, A., Scarfone, K., & Souppaya, M. (2022). *Supply Chain Assurance: Validating the Integrity of Computing Devices*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-34

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime Prevention: Theory and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-030-31069-1

Brocke, J. vom, Simons, A., Niehaves, B., Reimer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. *ECIS 2009 Proceedings*, *161*. https://aisel.aisnet.org/ecis2009/161

Bundesamt für Statistik. (2008a). *NOGA 2008 − Allgemeine Systematik der Wirtschaftszweige − Einführung*. https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-ienstleistungen/nomenklaturen/noga.assetdetail.344513.html

Bundesamt für Statistik. (2008b). *NOGA 2008 − Allgemeine Systematik der Wirtschaftszweige − Erläuterungen*. https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-ienstleistungen/nomenklaturen/noga.assetdetail.344101.html

Bundesamt für Statistik. (2013). *NOGA 2008 − Titel*. https://www.bfs.admin.ch/asset/de/262590

Bundesamt für Statistik. (2022a). *Anzahl Unternehmen, Beschäftigte und Umsatz von Unternehmensgruppen nach Art der Gruppe und Branchen (BFS50)*. https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/stagre.assetdetail.23647290.html

Bundesamt für Statistik. (2022b). *Statistik der Unternehmensgruppen (STAGRE)*. https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/erhebungen/inquiry-stagre.assetdetail.23329167.html

Botschaft zur Änderung des Informationssicherheitsgesetzes, BBl 2023 84 (2022). https://www.fedlex.admin.ch/eli/fga/2023/84/de

Chaiban, A., Sovilj, D., Soliman, H., Salmon, G., & Lin, X. (2022). Investigating the Influence of Feature Sources for Malicious Website Detection. *Applied sciences*, *12*(6). https://doi.org/10.3390/app12062806

Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, *113*.

Cisco. (2023). *Cisco Cybersecurity Readiness Index − Resilience in a Hybrid World*. Cisco. https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*(1). https://doi.org/10.1007/BF03177550

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *Geneva papers on risk and insurance. Issues and practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dacorogna, M., & Kratz, M. (2022). Special Issue «Cyber Risk and Security». *Risks*, *10*(6).

Dreißigacker, A., Skarczinski, B. von, & Wollinger, G. R. (2021). *Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer Folgebefragung 2020*. Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN). https://kfn.de/wp-content/uploads/Forschungsberichte/FB_162.pdf

Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019*. Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN). https://kfn.de/wp-content/uploads/Forschungsberichte /FB_152.pdf

European Commission. (2022). *Proposal for a regulation of the european parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*. https://ec.europa.eu/newsroom/dae/redirection/document/89543

Firstbrook, P., Olyaei, S., Shoard, P., Thielemann, K., Ruddy, M., Gaehtgens, F., Addiscott, R., & Candrick, W. (2022). *Top Trends in Cybersecurity 2022* (Nr. G00760806; Initiatives: Cyber Risk).

Frei, S., Jungo, C., Busch, D., & Reischuk, R. (2019). *Supply Chain Security − Analyse & Massnahmen zur Sicherung der digitalen Lieferkette*. Arbeitsgruppe Supply Chain Security der Kommission Cybersecurity von ICTswitzerland.

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber Security on the Farm: An Assessment of Cyber Security Practices in the United States Agriculture Industry. *International Food and Agribusiness Management Review*, *21*(3), 317–334.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting Insider Threat via a Cyber-Security Culture Framework. *Journal of Computer Information Systems*, *62*(4), 706–716.

Hammond, C., Villadsen, O., & Mühr, G. (2022, Mai 19). ITG23 Crypters Highlight Cooperation Between Cybercriminal Groups. *Security Intelligence*. https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cyber criminal-groups/

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors (Basel, Switzerland)*, *22*(22). https://doi.org/10.3390/s22228663

Hirschi, O., & Portmann, A. (2017). *Nationale Studie zur Informationssicherheit in Schweizer KMU*. Hochschule Luzern.

Hiscox. (2021). *Hiscox Cyber Readiness Report 2021*. Hiscox Ltd. https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2021.pdf

Hiscox. (2022a). *Cyber Readiness Report 2022 − Ransomware Update*. Hiscox Ltd. https://www.hiscox.de/wp-content/uploads/2022/11/Hiscox-Cyber-Readiness-Ransomware-Update-2022_EN.pdf

Hiscox. (2022b). *Hiscox Cyber Readiness Report 2022*. Hiscox Ltd. https://info.hiscox.de/hubfs/Dokumente/Hiscox%20Cyber%20Readiness%20Report%202022.pdf?_hsmi=206879730&_hsenc=p2ANqtz-8o8xMm4QoqXh8G-M5Hw_tBymRlJtc-hBTjdvUx-2zjagJDuYl-3ukiJDaGkeYI7ZrcY0HO9BtYcldZ-LmDpxyuBtuqnFZ7n5Gf4QRKupdU-C3NV-c

Initiative «Industrie 2025». (2023). *Cybersicherheit − Umfrage zur Bedrohungslage mit Empfehlungen für die Praxis*. Swissmem. https://industrie2025.us13.list-manage.com/track/click?u=c81e8205e609107bbc59b9343&id=0c517d7587&e=fbf0776d55

Isenhardt, A., Frey, L. E., & Hostettler, U. (2022). *Befragung zur Sicherheit in Unternehmen bezüglich digitaler und physischer Angriffe: Auswertungsbericht zuhanden des Verbands Swissmem*. Universität Bern – Institut für Strafrecht und Kriminologie. https://doi.org/10.48350/172496

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers & security*, *127*. https://doi.org/10.1016/j.cose.2022.103089

Korolov, M. (2022, Juni 13). *9 ways hackers will use machine learning to launch attacks*. CSO Online. https://www.csoonline.com/article/3250144/6-ways-hackers-will-use-machine-learning-to-launch-attacks.html

Kotsias, J., Ahmad, A., & Scheepers, R. (2022). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, *32*(1). 35-51.

Lella, I., Theocharidou, M., Tsekmezoglou, E., Malatras, A., Garcia, S., & Valeros, V. (2021). *ENISA-Bericht zur Bedrohungslage − Lieferkettenangriffe*. European Network and Information Security Agency. https://doi.org/10.2824/168593

Lella, I., Tsekmezoglou, E., Svetozarov Naydenov, R., Ciobanu, C., Malatras, A., & Theocharidou, M. (2022). *ENISA threat landscape 2022: July 2021 to July 2022*. European Union Agency for Cybersecurity. https://doi.org/10.2824/764318

Liu, L., De Vel, O., Han, Q., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE COMMUNICATIONS SURVEYS AND TUTORIALS*, *20*(2). https://doi.org/10.1109/COMST.2018.2800740

Mändli, K., & Repic, A. (2017). *Cyberrisiken in Schweizer KMUs − Befragung von GeschäftsführerInnen Schweizer KMUs*. gfs-zürich, Markt- und Sozialforschung.

Milmo, D. (2022, Februar 27). Anonymous: The hacker collective that has declared cyberwar on Russia. *The Guardian*. https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

NCSC. (2022). *Informationssicherung − Lage in der Schweiz und International* (Halbjahresbericht Nr. 2022/1). Nationales Zentrum für Cybersicherheit. https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2022-1.html

NCSC. (2023). *Informationssicherung − Lage in der Schweiz und International* (Halbjahresbericht Nr. 2022/2). Nationales Zentrum für Cybersicherheit. https://www.newsd.admin.ch/newsd/message/attachments/78227.pdf

Nyemkova, E., Justice, C., Liaskovska, S., & Lakh, Y. (2022). Methods of Current Knowledge Teaching on the Cybersecurity Example. *Education sciences*, *12*(11). https://doi.org/10.3390/educsci12110732

Palsson, K., Gudmundsson, S., & Shetty, S. (2020). Analysis of the Impact of Cyber Events for Cyber Insurance. *Geneva Papers on Risk and Insurance: Issues and Practice*, *45*(4), 564–579. https://doi.org/10.1057/s41288-020-00171-w

Pawlowska, A., & Scherer, B. (2021). *IT-Sicherheit im Home-Office unter besonderer Berücksichtigung der COVID-19 Situation. Ergebniskurzbericht einer repräsentativen Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI)*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Umfrage-Home-Office/umfrage_home-office-2020.pdf?__blob=publicationFile&v=3

Peng, J. & Chang-Wei Li. (2022). Security breaches and modifications on cybersecurity disclosures. *Accounting & Management Information Systems / Contabilitate si Informatica de Gestiune*, *21*(3), 452–470.

Perathoner, Y., & Burch, C. (2021, Dezember 17). *Recherchestrategien für die Projekt-, Semester-, Seminar- oder Abschlussarbeit*. Beyond Books. https://blog.zhaw.ch/hochschulbibliothek/2021/12/17/recherchestrategien-fuer-die-projekt-semester-seminar-oder-abschlussarbeit/

Peter, M. K., Hölzli, A., Kaelin, A. W., Lerch, K. M., Vifian, P., & Wettstein, N. (2020). *Digitalisierung, Home-Office und Cyber-Sicherheit in KMU*. FHNW Hochschule für Wirtschaft.

Rantala, R. R. (2005). *Cybercrime Against Businesses, 2005*. U.S. Departement of Justice, Office of Justice Programms. https://www.google.ch/books/edition/Cybercrime_Against_Businesses_2005/Kd5ot9kMdB0C?hl=de&gbpv=0

Saghezchi, F. B., Mantas, G., Violas, M. A., de Oliveira Duarte, A. M., & Rodriguez, J. (2022). Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs. *Electronics (Basel)*, *11*(4). https://doi.org/10.3390/electronics11040602

Sarder, M. D., & Haschak, M. (2019). Cyber security and its implication on material handling and logistics. *College-Industry Council on Material Handling Education*, 1–18.

Schellinger, J., Tokarski, K. O., & Kissling-Näf, I. (Hrsg.). (2020). *Digitale Transformation und Unternehmensführung: Trends und Perspektiven für die Praxis*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-26960-9

Silaule, C. B., Makhubele, L. M., & Mamorobela, S. P. (2022). A model to reduce insider cybersecurity threats in a South African telecommunications company. *South African journal of information management*, *24*(1). https://doi.org/10.4102/sajim.v24i1.1573

Snijkers, G., & Meyermann, A. (2017). Betriebs- und Unternehmenssurveys: Der Surveyprozess und Surveyqualität. In S. Liebig, W. Matiaske, & S. Rosenbohm (Hrsg.), *Handbuch Empirische Organisationsforschung*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-08580-3_11-1

Statistisches Bundesamt. (2023, Mai 13). *Kleine und mittlere Unternehmen*. Statistisches Bundesamt. https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/_inhalt.html

Stocker, T. C., & Steinke, I. (2022). *Statistik − Grundlagen und Methodik* (2. Aufl.). De Gruyter. https://doi.org/10.1515/9783110744194-202

Sweeney, B. (2016, September 13). Cybersecurity Is Every Executive's Job. *Harvard Business Review*. https://hbr.org/2016/09/cybersecurity-is-every-executives-job

Tsinganos, N., Fouliras, P., & Mavridis, I. (2022). Applying BERT for Early-Stage Recognition of Persistence in Chat-Based Social Engineering Attacks. *Applied sciences*, *12*(23). https://doi.org/10.3390/app122312353

Ullah, B., & Nab, S. I. (2022). Developing cyber security strategies for business organization to prevent data breaches. *KASBIT Business Journal*, *15*(4), 71–88.

Verma, A., & Shri, C. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision.* https://doi.org/10.1177/09722629221074760

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*, 100126. https://doi.org/10.1016/j.chbr.2021.100126

Wilde, T., & Hess, T. (2006). Methodenspektrum der Wirtschaftsinformatik. *Institut für Wirtschaftsinformatik und Neue Medien*, *Arbeitsbericht Nr. 2/2006*. https://www.dmm. bwl.uni-muenchen.de/download/epub/ab_2006_02.pdf

Wilde, T., & Hess, T. (2007). Forschungsmethoden der Wirtschaftsinformatik. *WIRTSCHAFTSINFORMATIK*, *49*(4), 280–287. https://doi.org/10.1007/s11576-007-0064-z

Wohlers, E. (2015). *Logistik – ein wichtiger Wirtschaftsbereich in Deutschland* (Nr. 92; HWWI Policy Paper). Hamburgisches WeltWirtschaftsInstitut (HWWI). https://www.hwwi.org/fileadmin/hwwi/Publikationen/Policy/HWWI_Policy_Paper_92.pdf

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*.

World Economic Forum. (2023). *WEF_Global_Risks_Report_2023.pdf* (Global Risks Report Nr. 2023). https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Worley, M., Caridi, C., Alvarez, M., Bakken, K., Bedard, Y., Brancati, M., Bedell, C., Chung, J., Craig, S., DiRe, J., Dwyer, J., Hammond, C., Henson, K., Jourdan, G.-V., Onut, V., Mayne, M., McMillen, D., Metrick, K., Moore, S., … Zorabedian, J. (2023). *IBM Security X-Force Threat Intelligence Index 2023*. IBM Corporation.

Yadav, P., Menon, N., Ravi, V., Vishvanathan, S., & Pham, T. D. (2022). EfficientNet convolutional neural networks-based Android malware detection. *Computers & security*, *115*. https://doi.org/10.1016/j.cose.2022.102622

Yigit Ozkan, B., & Spruit, M. (2022). Adaptable Security Maturity Assessment and Standardization for Digital SMEs. *The Journal of computer information systems*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1080/08874417.2022.2119442

Zwahlen, F., Marti, I., Richter, M., Konopatsch, C., & Hostettler, U. (2020). *Wirtschaftsspionage in der Schweiz – Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB)*. Universität Bern – Institut für Strafrecht und Kriminologie.

Eigenständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit respektive die von mir ausgewiesene Leistung selbständig, ohne Mithilfe Dritter und nur unter Ausnützung der angegebenen Quellen verfasst respektive erbracht habe.

Ort, Datum: Winterthur, 9. Oktober 2023

Unterschrift:

Anhang

Übersicht der häufigsten Methoden von Cyberangriffen

Ausschnitt aus der Swissmem-Publikation (Initiative «Industrie 2025», 2023, S. 15)

» Hackerangriff

Als Hackerangriff werden Aktivitäten bezeichnet, welche die Manipulation von Computern, Smartphones, Tablets oder ganzer Netzwerke zum Ziel haben. Diese allgemeine Bedeutung lässt sich auf manuelles Hacking eingrenzen – die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware. Dabei haben Hacker nicht zwingend kriminelle Absichten. Häufig geht es ihnen auch nur darum, Schwachstellen in IT-Systemen aufzudecken.

» Phishing

Als Phishing werden Versuche bezeichnet, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben. Ziel ist es, an Daten des Internet-Nutzers zu gelangen oder ihn zur Ausführung einer bestimmten Aktion zu bewegen. In der Folge wird zum Beispiel eine Schadsoftware installiert oder es werden Finanzmittel gestohlen.

» Social Engineering

Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, Personen zum Beispiel zur Preisgabe von vertraulichen Informationen oder zur Freigabe von Finanzmitteln zu bewegen. Dabei kommen oftmals Phising-Methoden zum Einsatz.

» CEO-Fraud

CEO-Fraud ist eine der häufigsten Formen von Social Engineering in der gegen Unternehmen gerichteten Cyberkriminalität. Meist werden im Namen des CEO E-Mails verfasst, in denen Mitarbeitenden gebeten werden, eine Zahlung zu veranlassen.

» Schadsoftware

Schadsoftware (engl. Malware) bezeichnet Programme wie Viren, Trojaner und Würmer, die schädliche Funktionen ausführen – sei es das Löschen oder Übermitteln von Dateien oder die Kompromittierung der Sicherheitssoftware. Die Schadfunktionen sind gewöhnlich getarnt oder die Software läuft unbemerkt im Hintergrund ab.

» Ransomware

Ransomware ist eine Form von Schadsoftware, die auf Lösegeldforderungen abzielt. Dabei werden Daten verschlüsselt oder Zugänge gesperrt. Die Betroffenen werden darauf zu einer Lösegeldzahlung aufgefordert, um wieder Zugriff auf die Dateien zu erhalten.

» (D)DoS-Attacke

Eine DoS-Attacke hat eine Überlastung der IT-Infrastruktur zum Ziel. Das Kürzel DoS steht für «Denial of Service», auf Deutsch «Verweigerung des Dienstes». Dabei wird eine Website oder ein E-Mail-Server mit so vielen Anfragen bombardiert, dass das System seine Dienste wegen Überlastung nicht mehr erbringen kann. Bei einem Distributed Denial-of Service (DDoS) werden die Angriffe auf mehrere Systeme verteilt.

Übersicht der eingesetzten IT-Sicherheitsmassnahmen

Welche der folgenden IT-Sicherheitsmassnahmen gibt es in Ihrem Unternehmen?			Studie	Dreissigacker								Isenhardt					Nüesch Erismann											
			WZ-Gruppe	MEM DE				LOG DE				MEM CH					LOG CH					LOG+ CH				LOG CH & LOG+ CH		
Typ	Massnahme	Kategorie		VOR dem Angriff umgesetzt	NACH dem Angriff umgesetzt	Nein	Weiss nicht	Gesamt	VOR dem Angriff umgesetzt	NACH dem Angriff umgesetzt	Nein	Weiss nicht	Gesamt	VOR dem Angriff umgesetzt	NACH dem Angriff umgesetzt	Nein	Weiss nicht	Gesamt	VOR dem Angriff umgesetzt	NACH dem Angriff umgesetzt	GEPLANTE Umsetzung	KEINE Umsetzung	Keine Angabe	Gesamt	VOR dem Angriff umgesetzt	NACH dem Angriff umgesetzt	GEPLANTE Umsetzung	KEINE Umsetzung	Keine Angabe	Gesamt
Technisch	Intrusion Detection System (IDS)	Häufigkeit							64	16	33	41	154	9	1	3	6	19	6	1		2	9	15	2		3	8	28
Technisch	Informationssicherheitsmanagementsystem (ISMS)	Häufigkeit	12	1	76	4	93	12	4	61	12	89	37	16	87	9	149	4	3	2	5	5	19	4	1	1	2	1	9	8	4	3	7	6	28
Technisch	Security Information and Event Management (SIEM)	Häufigkeit	16	2	67	8	93	12	2	58	15	87	75	23	38	17	153	4	3	4	3	5	19	3	1		3	2	9	7	4	4	6	7	28
Technisch	Security Operation Center (SOC)	Häufigkeit	11	2	71	8	92	7	1	64	16	88			4	1	3	3	8	19	2		5	2	9	6	1	3	8	10	28
Technisch	Antivirensoftware	Häufigkeit	94		2	1	97	91	2	2		95	154		1	1	156	17	1		1	1	19	8			1	9	25	1			1	2	28
Technisch	Schutz der IT-Systeme mit einer Firewall	Häufigkeit	96			1	97	93	1			94	152	1	1	1	155	17	1			1	19	8			1	9	25	1			2	28
Technisch	Austausch von Bedrohungsdaten (z.B. Threat Intelligence)	Häufigkeit	20	2	62	9	93	19	1	55	17	92					7				4	8	19	2		2	2	3	9	9		2	6	11	28
Technisch	Auf künstliche Intelligenz basierte Massnahmen	Häufigkeit	14	3	69	7	93	10	2	66	12	90					5	1			4	9	19	2		4	3	9	7	1		8	12	28
Technisch	Netzwerksegmentierung	Häufigkeit	59	2	31	4	96	48		36	9	93	75	11	52	14	152	9	2	3	1	4	19	7			2	9	16	2	3	1	6	28
Technisch	Regelmässige Backups	Häufigkeit	96			1	97	93	2			95	153	1		1	155	16	1	1	1		19	9				9	25	1	1	1		28
Technisch	Physisch getrennte Aufbewahrung von Backups	Häufigkeit											140	7	2	5	154																
Technisch	Aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates	Häufigkeit	84	1	9	1	95	79	2	11	1	93	140	6	4	3	153	17				2	19	8			1	9	25				3	28
Technisch	Verschlüsselung von Kommunikation	Häufigkeit	49	1	39	2	91	51	2	33	6	92	44	5	86	15	150	4	2	1	7	5	19	1	1	2	3	2	9	5	3	10	7	28
Technisch	Verschlüsselung von sensiblen Daten	Häufigkeit	46	1	43	2	92	57	1	31	4	93	82	8	43	21	154	7		1	5	6	19	4	2	1		2	9	11	2	2	5	8	28
Technisch	Mindestanforderungen für Passwörter	Häufigkeit	78	3	12	2	95	79	5	10		94	126	20	9	1	156	16	2		1	1	19	6	2	1			9	22	4	1		1	28
Technisch	Zwei-Faktor-Authentifizierung	Häufigkeit	22	2	67	3	94	25	4	62	2	93					8	5	1	1	4	1	19	7	1			1	9	15	6	1	1	5	28
Technisch	Verstärkte physische Sicherheit	Häufigkeit	42	1	47	2	92	34	2	45	10	91	93	4	45	4	146																	
Technisch	Alle Fernzugriffe (für Wartung und Administration) auf Leitstelle und Steuerungsanlagen sind mit starker Authentisierung abgesichert	Häufigkeit										112	11	17	14	154																	
Organisatorisch	Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk	Häufigkeit										44	10	92	4	150	9		2	3	5	19	3			3	2	8	12		2	6	7	27
Organisatorisch	Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme	Häufigkeit	29	3	56	3	91	26	3	64		93	48	6	86	10	150	9	1	2	3	3	18	6	1		1	8	15	2	2	4	3	26
Organisatorisch	Risiko- und Schwachstellenanalysen (auch Pentest)	Häufigkeit	37	4	48	3	92	29	5	53	6	93	85	25	35	9	154	11	5	2	1	1	19	7		1		8	18	5	3		1	27
Organisatorisch	Schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit	Häufigkeit	76	1	15	4	96	58	3	30		91	117	8	28	3	156	10	2	2	3	2	19	7				7	17	2	2	3	2	26
Organisatorisch	Schriftliche Richtlinien zum Notfallmanagement	Häufigkeit	51	2	39	3	95	47	4	40	1	92	61	22	61	7	151	9	3	2	2	3	19	3	3	1	1	8	12	3	5	3	4	27
Organisatorisch	Individuelle Vergabe von Zugangs- und Nutzerrechten	Häufigkeit	90	1	4	1	96	88	1	5		94	137	4	10	3	154	16			1	2	19	6	1			1	8	22	1		1	3	27
Organisatorisch	Schulungen zur ICT-Sicherheit für Mitarbeitende	Häufigkeit											103	25	24	2	154	12	2	1	3	1	19	4	2	2			8	16	4	3	3	1	27
Organisatorisch	Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbenden	Häufigkeit											36	3	92	16	147	9	1		4	5	19	4			2	2	8	13	1		6	7	27
Organisatorisch	Test der Datenwiederherstellung (Restoring)	Häufigkeit	85	1	9	1	96	65	2	22	6	95																						
Organisatorisch	Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001 o. VdS 3473)	Häufigkeit	7		77	7	91	6	2	77	7	92																						
Organisatorisch	Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen	Häufigkeit											109	3	32	4	148	12			4	3	19	4	1		2	1	8	16	1		6	4	27
Organisatorisch	Klare Regelungen für den Umgang mit vertraulichen Informationen (Informationssicherheitskonzept)	Häufigkeit											88	11	47	4	150																
Organisatorisch	Eindeutige Klassifizierung/Kennzeichnung von Betriebsgeheimnissen	Häufigkeit											63	5	74	6	148																
Organisatorisch	Geheimhaltungsverpflichtungen für Mitarbeitende	Häufigkeit											125	2	17	4	148																
Organisatorisch	Geheimhaltungsverpflichtungen für Geschäftspartner	Häufigkeit											118	1	22	6	147																
Organisatorisch	Weisungen für die Mitnahme von vertraulichen Informationen bei Auslandsreisen	Häufigkeit											39	4	95	11	149																
Organisatorisch	Weisungen für das Verhalten an Messen und Ausstellungen	Häufigkeit											51	1	81	15	148																
Organisatorisch	Besuchermanagement/Zutrittskontrollen	Häufigkeit											109	3	33	4	149																
Organisatorisch	Background-Checks von Geschäftspartnern (Lieferanten, Dienstleister, Berater etc.)	Häufigkeit											48	4	81	15	148																
Organisatorisch	Clean-Desk-Policy	Häufigkeit											33	4	100	11	148																
Organisatorisch	Regelmässige Kontrollen (der Arbeitsplätze, der Mitarbeitenden etc.) in Bezug auf die Einhaltung von Vorschriften	Häufigkeit											23	3	113	7	146																
Organisatorisch	Kontrolle der veröffentlichten Informationen, z.B. auf Homepage / durch Mitarbeitende in den sozialen Medien	Häufigkeit											59	5	79	5	148																

Fachgespräch

Rahmenbedingungen

Datum

Donnerstag, 11.05.2023, 09:00-10:00 Uhr

Ort

Microsoft Teams mit Aufzeichnung

Teilnehmende

Name	Funktion	Organisation
Experte 1	Head of Industry Engagement Transport and Logistics	Internationaler Verein zur Standardisierung von Logistikprozessen
Experte 2	Geschäftsleiter Industrie 2025	Schweizer Branchenverband
Experte 3	Chief Information Officer (CIO)	Internationales Transport- und Logistikunternehmen
Experte 4	Leiter Logistik und Europaverkehre	Internationales Transport- und Logistikunternehmen
Expertin 5	Chief Information Security Officer (CISO)	Internationales Transport- und Logistikunternehmen

Ziel

Das Gespräch soll als kurze Zusammenfassung der Kernaussagen bzw. als Input von Branchenvertreter:innen ein Teil der Masterarbeit werden.

Vertraulichkeit

Das Gespräch wird aufgezeichnet, weil auf ein exaktes Transkribieren des Gesprochenen verzichtet wird. So können die Aussagen mittels Zeitangabe referenziert werden. Wenn Aussagen in der Masterarbeit nicht erwähnt werden dürfen, so kann dies jederzeit im Gespräch angemerkt werden.

Gesprächstyp

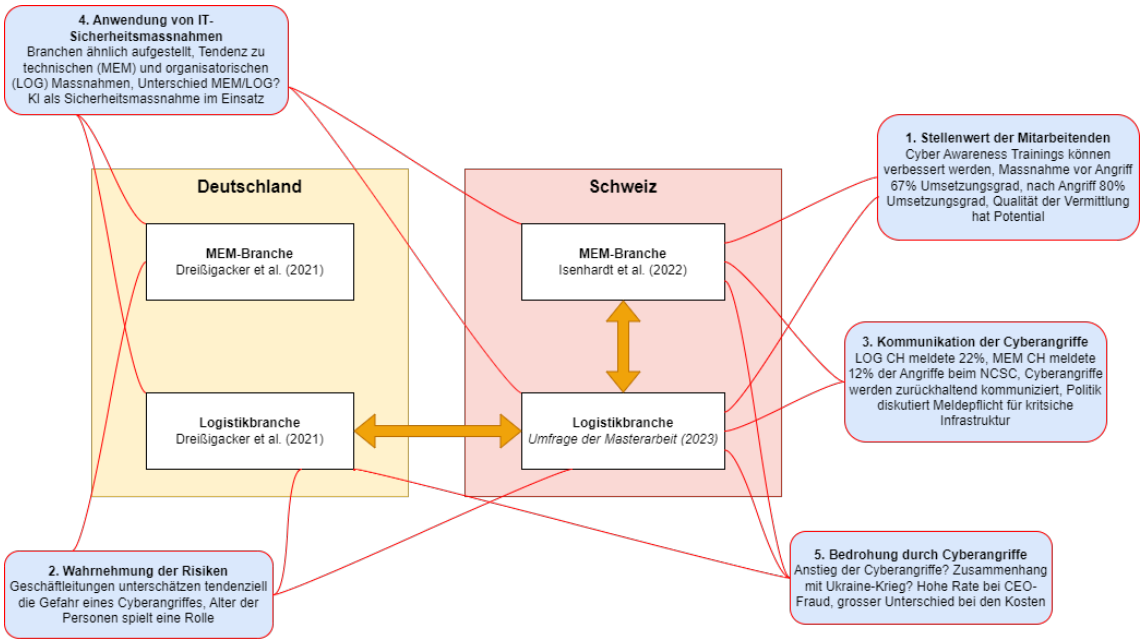
Semi-strukturiertes Interview

Gesprächsleitfaden

Der nachfolgende Gesprächsleitfaden wurde vorgängig an die Teilnehmenden des Fachgespräches versendet und enthält die wichtigsten Erkenntnisse der vorliegenden Arbeit sowie Fragen, die als Diskussionsgrundlage im Fachgespräch (semi-strukturiertes Interview) verwendet werden konnten.

Fachgespräch mit Vertreter:innen der Schweizer Logistik- und MEM-Branche

Hauptforschungsfrage: «Wie stellt sich die aktuelle Situation in Bezug auf Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche im Vergleich zur Schweizer MEM-Branche dar?»



1. Stellenwert der Mitarbeitenden

Die Untersuchung zeigte, dass sowohl die Logistik-, als auch die MEM-Branche in der Schweiz und Deutschland am meisten durch «Phishing-Angriffe» bedroht werden. Auch beim weit verbreiteten «CEO-Fraud» und «sonstigem Social Engineering» sind die Mitarbeitenden und ihr Urteilsvermögen das zentrale Element und müssen mit besonderer Aufmerksamkeit bedacht werden. Die Umfrage in der Schweizer Logistikbranche bestätigte einerseits, dass Schulungen für Mitarbeitende als organisatorische IT-Sicherheitsmassnahme bei Unternehmen, die von einem Angriff betroffen waren, nach dem Angriff zu 74% und bei nicht angegriffenen Unternehmen zu 67% umgesetzt waren, andererseits zeigten die Fragen nach der Ausgestaltung der Trainings ein differenzierteres Bild. Zwei Drittel der Unternehmen führen die «Cyber Awareness Trainings» nicht in

verschiedenen Sprachen und an die Zielgruppe angepasst durch. Es fehlt auch an Erfolgskontrollen und spezifischen Trainings für Mitarbeitende, die im Homeoffice arbeiten. Auch die regelmässige Wiederholung der Trainings ist nicht sichergestellt.

Vergleich: In der Schweizer MEM-Branche zeigte sich jedoch, dass die organisatorische IT-Sicherheitsmassnahme «Schulungen zur ICT-Sicherheit für Mitarbeitende» bei Unternehmen, die von einem «schwerwiegendsten Angriff» betroffen waren, vor dem Angriff bei 67% und nach dem Angriff bei 83% lag. Dies war die Massnahme mit der grössten durch einen Angriff hervorgerufenen Steigerung von 16%. Die Schweizer Logistikbranche steigerte sich durch die erlebten Angriffe in dieser Massnahmen um 15%. Es besteht also in beiden Branchen Verbesserungspotential. Im Swissmem-Schlussbericht Cybersicherheit - Umfrage zur Bedrohungslage mit Empfehlungen für die Praxis wurde dieser Umstand erwähnt, jedoch wurde nicht näher darauf eingegangen.

Diskussion

a) Welchen Stellenwert haben «Cyber Awareness Trainings»?

b) Wie kann sichergestellt werden, dass die Vermittlung didaktisch optimal gestaltet wird?

2. Wahrnehmung der Risiken

Die Unternehmen der Schweizer Logistikbranche schätzen die Wahrscheinlichkeit, in den nächsten 12 Monaten von einem Cyberangriff geschädigt zu werden, der gleichzeitig auch viele andere Unternehmen trifft, zu 49% als «sehr/eher gering» ein und zu 48% als «eher/sehr hoch» ein. Dieser ausgewogenen Risikoeinschätzung wiederspricht der aktuelle Cisco Cybersecurity Readiness Index, der von 82% der Verantwortlichen berichtet, die eine Beeinträchtigung durch einen Cyberangriff in den nächsten 12-24 Monaten als wahrscheinlich erachten. In der deutschen MEM- und Logistik-Branche wurde diese Frage mit 40% als «sehr/eher gering» und mit 57% % als «eher/sehr hoch» eingestuft. Die Umfrage in der Schweizer MEM-Branche untersuchte dies nicht. An der durchgeführten Online-Umfrage haben 39% Geschäftsführende oder Vorstandsmitglieder teilgenommen und es wird davon ausgegangen, dass Geschäftsführende oder Vorstandsmitglieder aufgrund der notwendigen Berufserfahrung tendenziell älter sind. Das Alter hat nachgewiesenermassen einen Einfluss auf die Wahrnehmung von Cyberrisiken. Es besteht der Eindruck, dass die Wahrnehmung der Risiken aufgrund dieser Tatsache als zu tief eingestuft wird.

Diskussion

a) Wie wird das Risiko, in den nächsten 12 Monaten von einem Cyberangriff geschädigt zu werden, eingestuft?

b) Wird die Auffassung geteilt, dass das Risiko eines Cyberangriffes von Geschäftsleitungen in der Speditions- und Logistikbranche tendenziell zu tief eingeschätzt wird?

3. Kommunikation der Cyberangriffe

Es wurde festgestellt, dass die gemeldeten Lösegeldforderungen (MEM CH 3.7%, LOG CH 2.7%) bei weitem nicht den 27% der Fälle entsprachen, die im IBM Security X-Force Threat Intelligence Index 2023 erwähnt wurden. 2017 wurde bei Schweizer KMU erforscht, dass eine Mehrheit der Geschäftsführenden aufgrund eines potenziellen Reputationsschadens Cyberangriffe nicht kommunizieren wollen. Der tiefe Umsetzungsgrad der technischen IT-Sicherheitsmassnahme «Cyber Threat Intelligence» (Austausch von Bedrohungsdaten) stützt diese Vermutung. Betroffene Unternehmen erreichen vor dem «schwerwiegendsten Angriff» einen Umsetzungsgrad von 54%. Nach dem Angriff steigerte sich der Umsetzungsgrad dieser Sicherheitsmassnahme am meisten von allen technischen Massnahmen, auf 75%. Die Logistikbranche zeigt hier eine erfreuliche Lernkurve. Die betroffenen Unternehmen gaben nach dem «schwerwiegendsten Angriff» zu 44% an, einen spezialisierten Dienstleiter kontaktiert zu haben. Nur 22% meldeten sich beim Nationalen Zentrum für Cybersicherheit (NCSC) und 19% bei der Polizei. In der Schweizer MEM-Branche meldeten sich nach dem «schwerwiegendsten Angriff» lediglich 12% beim NCSC, was vermuten lässt, dass die Verschwiegenheit in dieser Branche noch grösser ist als in der Logistikbranche. Die Swissmem-Studie zeigte auf, dass hier noch Verbesserungspotential in der Branche besteht. Aus diesen Gründen ist die Politik aktuell bestrebt, eine Cyberangriff-Meldepflicht für kritische Infrastruktur einzuführen.

Diskussion

a) Sollten Cyberangriffe öffentlich kommuniziert werden?

b) Wird der «Austausch von Bedrohungsdaten» mit spezialisierten Dienstleistenden und/oder dem NCSC als ein aktuelles Thema wahrgenommen?

c) Wie lässt sich der Unterschied zwischen der Schweizer MEM- und Logistikbranche in Bezug auf die gemeldeten Fälle beim NCSC erklären?

d) Wird eine generelle Meldepflicht befürwortet?

4. Anwendung von IT-Sicherheitsmassnahmen

Der durchschnittliche Umsetzungsgrad der IT-Sicherheitsmassnahmen lag bei den befragten Unternehmen der Schweizer Logistikbranche, die einen «schwerwiegendsten Angriff» erlebten, im Vergleich zur Schweizer MEM-Branche etwa gleich hoch. Aufgrund der kleinen Stichprobe darf keine verallgemeinernde Aussage daraus abgeleitet werden, doch die Daten legen den Schluss nahe, dass die MEM-Branche öfter in «technische IT-Sicherheitsmassnahmen» und die Logistikbranche eher in «organisatorische IT-Sicherheitsmassnahmen» investiert. In der Literatur lassen sich Hinweise finden, dass die Transportbranche einen sehr tiefen und die Fertigungsindustrie einen sehr hohen Grad an «Cyber Readiness» aufweist. Der Unterschied zwischen den Branchen lässt sich aufgrund der Schweizer Umfragen nicht bestätigen. Generell lässt sich feststellen, dass diejenigen Unternehmen, die an den Umfragen teilgenommen haben, die Grundlagen der Cybersicherheit gut umgesetzt haben und speziell diejenigen, die Opfer eines Cyberangriffes wurden, ihre IT-Sicherheitsmassnahmen auf technischer sowie auf organisatorischer Ebene verbessert haben. In der Literatur wird berichtet, dass die Unternehmen aufgrund der Pandemie und der damit verbundenen Verlagerung von Arbeitsplätzen ins Homeoffice, die IT-Sicherheitsmassnahmen angepasst und die IT-Budgets erhöht wurden. Der Umsetzungsgrad der auf «künstlicher Intelligenz basierten Massnahmen» wurde in der Online-Umfrage gestellt und ergab, dass nach dem «schwerwiegendsten Angriff» bereits 46% der Unternehmen solche Massnahmen im Einsatz haben und weitere 7.1% dies geplant haben umzusetzen. In der deutschen Logistikbranche setzen diese Massnahme bereits 52% der Unternehmen ein. Die Schweizer MEM-Branche thematisierte in der Umfrage das Thema der künstlichen Intelligenz nicht.

Diskussion

a) *Wie wird das unterschiedliche Anwenden von technischen und organisatorischen IT-Sicherheitsmassnahmen in der Schweizer MEM- und Logistikbranche interpretiert?*
b) *Kann ein Unterschied der «Cyber Readiness» zwischen der MEM- und Logistikbranche im Alltag festgestellt werden?*
c) *Konnte im beruflichen Umfeld eine Anpassung der IT-Sicherheitsmassnahmen aufgrund der Pandemie beobachtet werden?*
d) *Wie wird der Einfluss künstlicher Intelligenz auf die Cybersicherheit eingestuft?*

5. Bedrohung durch Cyberangriffe

Die Rate der Unternehmen, die in den letzten 12 bzw. 24 Monaten angegriffen wurden, unterscheidet sich in den vorliegenden drei Datensätzen markant. So waren in der deutschen Logistikbranche 32 von 95 Unternehmen (34%), in der Schweizer MEM-Branche 173 von 271 (64%) und in der Schweizer Logistikbranche 33 von 73 (45%) von einem «schwerwiegendsten Angriff» betroffen. Die höheren Werte in der Schweiz liegen an der Art der Stichprobe. Die deutsche Zufallsstichprobe weist einen tieferen Wert auf als die Gelegenheitsstichprobe. Betroffene Unternehmen neigen infolgedessen dazu, an Umfragen zur Cybersicherheit teilzunehmen. Die Grössenordnung hingegen erstaunt nicht. Auch im Cisco Cybersecurity Readiness Index wird berichtet, dass fast 60 % der Befragten in den letzten 12 Monaten einen Vorfall im Bereich der Cybersicherheit erlebt haben.

Die Angriffsart «CEO-Fraud», von der die Schweizer MEM-Branche beim «schwerwiegendsten Angriff» mit 18.8% auffällig oft betroffen war, zeigte auch in der Schweizer Logistikbranche mit 12.3% einen erhöhten Wert. In Deutschland verzeichnete die Logistikbranche lediglich und 6.3%, die MEM-Branche 6.2% «schwerwiegendste Angriffe» mit «CEO-Fraud». Die Häufigkeit von «CEO-Fraud» scheint ein Schweizer Phänomen zu sein.

Weiter zeigte sich, dass die Median-Kosten eines Cyberangriffes in der Schweizer MEM-Branche dreissigmal so hoch waren wie in der deutschen MEM-Branche und fünfzehnmal so hoch wie in der Schweizer und deutschen Logistikbranche. Gründe für diesen Umstand wurden keine erhoben.

Diskussion

a) Wurde im Umfeld im letzten Jahr ein Anstieg von Cyberangriffen festgestellt?

b) Konnten im Kontext der kriegerischen Aktivitäten in der Ukraine ein Anstieg von Cyberangriffen festgestellt werden?

c) Weshalb ist «CEO-Fraud» in der Schweizer MEM- und Logistikbranche verbreiteter als in Deutschland?

d) Wie lassen sich die viel höheren Folgekosten in der MEM-Branche im Vergleich zur Logistikbranche erklären?

Gesprächsverlauf

Der Gesprächsleitfaden wurde den Teilnehmenden des Fachgespräches am 08.05.2023 zur Vorbereitung und vor allem zur Orientierung per E-Mail zugestellt. Das Gespräch am 11.05.2023 konnte aufgrund der zeitlichen Begrenztheit nicht auf alle Fragen gleichermassen eingehen. Nachfolgend wird der Gesprächsverlauf zusammenfassend wiedergegeben. Generell werden Aussagen mittels Zeitangabe auf die Teams-Aufzeichnung[23] referenziert.

Stellenwert der Mitarbeitenden

Welchen Stellenwert haben «Cyber Awareness Trainings» und wie wird sichergestellt, dass diese in guter Qualität durchgeführt werden?

- *Experte 2 (09:57): KMU investieren lieber in technische Sicherheitsmassnahmen als in Schulungen. Die Schulung der Mitarbeitenden ist der grösste Hebel, wird von den KMU aber eher als ungewohnt und als Hürde wahrgenommen.*
- *Experte 1 (10:55): Die effektive Schulung der Mitarbeitenden ist oft mit einem kulturellen Change verbunden. Meist wird lediglich eine Infoveranstaltung durchgeführt. Anschliessend werden die Mitarbeitenden zu wenig begleitet. Die Angriffsfläche, die die Mitarbeitenden darstellen, ist massiv grösser als man sich das bewusst ist. So kommt es, dass z.B. im Zug oft sehr nachlässig mit dem Notebook gearbeitet wird. Dies sind sich die Firmen oft nicht bewusst.*
- *Expertin 5 (12:33): Faktor Mensch ist wichtig, doch die technischen Hausaufgaben müssen erledigt werden (Patch-Management, Rechte-Management, SOC) und sind gesetzt, da führt kein Weg daran vorbei. Der Faktor Mensch macht 70-80% der Verteidigungsschiene aus. Manager sind sich der Risiken bewusst. Der Zertifizierung-Scope [im Unternehmen der Expertin 5] bezieht sich auf die 300 Mitarbeitenden der Corporate IT. Die weiteren 8'100 Mitarbeitenden werden jetzt dann mit einem E-Learning-Kurs geschult. Dies erfolgt nach jahrelanger, massiver Überzeugungsarbeit, dass dies ein Thema für alle Mitarbeitenden ist. Spannend sind die nicht so IT-affinen Leute in einer Niederlassung, die nicht täglich am Computer arbeiten und noch nicht viel von Datenschutz und Informationssicherheit gehört*

[23] Cybersecurity _ Diskussion der Umfrageergebnisse-20230511_090059-Besprechungsaufzeichnung.mp4

haben. E-Learning ist effizient, weil schnell viele Leute in vielen Sprachen erreicht werden können. Das Einzige, was jedoch wirklich funktioniert, ist die Leute face-to-face auszubilden und ihnen zu erklären, was Cybersicherheit bedeutet, z.B. dass sie ihre Daten auch privat nicht ohne darüber nachzudenken teilen sollten. Theoretischem zu Datenschutz und sicheren Passwörtern pflichten alle bei, doch es bedarf mehr, dass sich wirklich eine Änderung im Handeln der Mitarbeitenden ergibt.

- *Experte 4 (15:03): Onlineschulungen sind wichtig, die unterschiedlichen Abteilungen müssen aber individuell geschult werden. So ist ein Kundencenter viel häufiger externer Kommunikation ausgesetzt als ein Umschlagsmitarbeiter. Auch eine Buchhaltung hat mit Bankinformationen auf andere Themen zu achten als ein Zolldeklarant. Eine Interpretation der möglichen Risiken muss stattfinden und die Schulungen der Mitarbeitenden müssen individuell angepasst werden.*
- *Experte 2 (16:44): KMU haben oft das Gefühl, alles selbst machen zu müssen. Doch genau bei diesen Thema gibt es unterdessen sehr gute Dienstleister auf dem Markt, die «Cyber Awareness Trainings» anbieten. Da sollte der Beizug externer Expertise unbedingt in Betracht gezogen werden.*
- *Experte 3 (17:38): Das ISMS beinhaltet je nach Scope «Cyber Awareness Trainings». Es ist sicherlich gut, die Mitarbeitenden live zu schulen, doch mit Online-Schulungen beginnt man die Leute zu sensibilisieren. Solche Schulungen müssen auch nicht selbst gemacht werden, da gibt es gute externe Dienstleister die Trainings customizen können. Schlussendlich beginnt das Thema zu leben. Die Logistik ist eine Datenverarbeitungsmaschinerie und wenn alle Mitarbeitenden realisieren, dass nicht nur Güter verschoben werden, beginnt es, dank gemeinsamem Engagement zu funktionieren. Es erwies sich auch als zielführend, dass nach «Cyber Awareness Trainings» eine Überprüfung gemacht wurde, um einzelne Mitarbeitende, die nicht erfolgreich waren, noch einmal informieren zu können und ihnen das Ganze noch einmal zu erklären.*
- *Expertin 5 (19:42): Es werden viele externe Ressourcen, im Umfang von bis zu drei Vollzeitstellen, beigezogen. Dies unter anderem, um Schulungen zu konzipieren. Die Berater können Inputs liefern, die aber noch an die Firma angepasst werden müssen. So wurden die Schulungen über die Jahre hinweg immer besser. Praxisbeispiele sind in jedem Unternehmen sehr wichtig, um den Bezug herzustellen.*

- *Experte 3 (20:37): Eine Anpassung auf die Gegebenheiten, Gebäude und Tätigkeiten der Firma sind wichtig, dass sich die Mitarbeitenden damit identifizieren können.*

Wahrnehmung der Risiken

Wird die Auffassung geteilt, dass das Risiko eines Cyberangriffs von Geschäftsleitungen in der Speditions- und Logistikbranche tendenziell zu tief eingeschätzt wird?

- *Experte 4 (22:58): Risiko wird sicherlich zu einem Teil wahrgenommen. Aus der Perspektive eines Bereichsleiters, der einer Länderorganisation unterstellt ist, fehlen zwei Sachen: Erstens die Einstufung der Cyberrisiken zwischen allen anderen Risken (z.B. Zoll). Die Cyberrisiken werden abhängig davon, wie die Medien darüber berichten, wahrgenommen (Risikovolatilität). Zweitens fehlt dem Management das Verständnis für Cybergefahren, um antizipieren zu können, wie reagiert werden muss.*
- *Expertin 5 (25:23): Es gibt regen Austausch mit der Führungsebene respektive mit einem der vier Geschäftsführenden, dem IT-Leiter. Der Schulterschluss mit der operativen Einheit ist nicht vorhanden. Es fehlt ein zentrales Risikomanagement (Finanz-, Prozess, Informationsrisiken). Themen werden oft aufgrund aktueller Cyberangriffe priorisiert (z.B. Krisenmanagement).*
- *Experte 1 (27:28): Im klassischen KMU-Bereich nimmt man die Gefahr auf strategische Ebene wahr, hat aber noch viele weitere Risiken zu beurteilen. Das führt zu einem Optimismus, dass nichts geschehen wird. Es werden dann Massnahmen eingeleitet und gehofft, dass diese ausreichend sind. Das Thema Cybersicherheit ist bei KMU auf strategischer Ebene zu wenig verankert. Allenfalls sieht die Situation bei grösseren Unternehmen besser aus. Eine langfristige Perspektive fehlt.*
- *Experte 2 (28:38): Das Management von KMUs wiegt sich oft in falscher Sicherheit. Das Thema liegt beim IT-Leiter oder es wurde eine Versicherung abgeschlossen. Wenn die Cybersicherheit zusätzlich noch an einen externen Dienstleister ausgelagert wurde, verstärkt sich das trügerische Gefühl von Sicherheit.*
- *Experte 3 (30:44): Die strategische Verankerung des Themas Cybersecurity ist relevant. Es hilft, in einer Geschäftsleitung aktuelle Fälle, wie z.B. der Ausfall des ERP bei Marktbegleitern für vier Wochen, zu besprechen. Ebenfalls muss auf Stufe Geschäftsleitung das Bewusstsein geschärft werden, dass die Angreifer 7/24 im*

Einsatz sind und mit gewissen Massnahmen angefangen werden muss, um sich Schritt für Schritt zu verbessern.

Wie wird das Risiko, in den nächsten 12 Monaten von einem Cyberangriff geschädigt zu werden, eingestuft?

- *Experte 3 (30:25): Studien berichten von Angriffsraten von über 90%, deshalb wird ein Cyberangriff als sehr wahrscheinlich erachtet.*
- *Experte 1 (32:25): Angriffe finden jeden Tag statt. Jedes «Phishing-Mail» ist ein Angriff. Auf der technischen Seite ist die Wahrscheinlichkeit eher kein, da alle Massnahmen ergriffen wurden. Es wird ein Angriffsrisiko von 1-2% geschätzt. Viel grösser ist das Risiko übers Personal angegriffen zu werden (Notebook wurde nicht gesperrt oder «Phishing-Mail» wurde nach erfolgter Schulung geöffnet). Beim Verein[24] wurden nach einer Schulung «Fake-Phishing-Mails» versendet und die «gefährlichen» Links mit einer Quote von 80% geöffnet. In diesem Bereich wird deshalb das Risiko, von einem Angriff betroffen zu sein, mit 50% eingeschätzt.*
- *Experte 4 (34:04): Die Gefahr von Anrufen mit gekaperten Telefonnummern stellt ein Problem dar, da Angreifer Telefonnummern von bekannten Personen aus dem Adressbuch vorgeben. So finden Angriffe auf unterschiedlichsten Ebenen statt. Im Bereich der KMU gibt es interessante Unternehmen zum Angreifen, da sie wenig Ressourcen in die IT-Sicherheit investieren können, andererseits solid kapitalisiert sind und eine Struktur haben, die schlecht auf eine Attacke reagieren kann – mit fatalen Folgen. Ein Ausfall des Transport Management Systems hätte enorme Folgen für ein Transportunternehmen. Das Risiko eines Cyberangriffs ist so hoch, dass gesagt werden kann, dass heute zu wenig getan wird.*

Kommunikation der Cyberangriffe

Weshalb werden Cyberangriffe nur in wenigen Fällen dem Nationalen Zentrum für Cybersicherheit (NCSC) gemeldet?

- *Experte 2 (39:50): Nach einem Angriff haben die Unternehmen andere Probleme, als den Angriff zu melden. Es ist nicht erklärbar, weshalb die Melderate der MEM-*

[24] Der Name des Vereins wurde durch den Autor anonymisiert.

Branche beim NCSC so tief ist, denn dies ist ein ganz wichtiges Instrument, um Cyberangriffe zu bekämpfen. Eine Meldung in anonymisierter Form sollte erfolgen. Jedes Unternehmen sollte eine Kommunikationsstrategie haben. Dies abhängig vom Vorfall, um adäquat kommunizieren zu können. Auch hier sollte externe Hilfe beigezogen werden.

- *Experte 4 (40:50): Angriffe werden aufgrund des Reputationsschadens und dem Verlust der Transportaufträge lieber nicht gemeldet, da die Kunden eines Transportunternehmens keine Möglichkeit haben, dem angegriffenen Unternehmen Zeit zur Erholung einzuräumen und die Sendungen sofort einem anderen Transportunternehmen anvertrauen. Solche Sendungen kommen möglicherweise nie mehr zurück, da die Kunden oft mehrere Dienstleister parallel nutzen. Bevor einem Kunden proaktiv kommuniziert wird, dass man Opfer eines Cyberangriff wurde und für eine unbestimmte Zeit handlungsunfähig ist, wird versucht, dem Kunden irgendeine Geschichte zu erzählen, um Zeit zu gewinnen. Um eine Meldung bei NCSC zu machen, müsste zuerst das Bewusstsein vorhanden sein, dass eine Meldung erfolgen sollte.*

- *Experte 1 (43:51): Vielen ist das Thema zu wenig präsent und viele wissen vermutlich nicht, dass es diese Meldestelle gibt, wo in anonymisierter Form eine Meldung abgesetzt werden kann, die einen Nutzen für alle generiert.*

- *Experte 3 (44:46): Ein Kommunikationskonzept und entsprechende Checklisten (Telefonlisten, aktueller Kundenstamm, etc.) sollten vorbereitet werden. Da sollte auch die Meldung ans NCSC inkludiert sein. Dies bedingt Ressourcen und eine Strategie. Im KMU-Bereich ist man sich dessen vermutlich zu wenig bewusst oder es fehlt die Stelle, die sich darüber Gedanken macht und das Ganze organisiert.*

Anwendung von IT-Sicherheitsmassnahmen

Wie wird das unterschiedliche Anwenden von technischen und organisatorischen IT-Sicherheitsmassnahmen in der Schweizer MEM- und Logistikbranche interpretiert?

- *Experte 2 (47:20): Die Unternehmen der MEM-Branche sind technisch geprägt. Das Thema Cybersecurity landet oft beim IT-Verantwortlichen, der in der Tendenz eher die technischen IT-Sicherheitsmassnahmen umsetzt.*

- *Experte 1 (47:43): Die technischen IT-Sicherheitsmassnahmen sind einfacher umzusetzen als diejenigen mit den Mitarbeitenden. Deshalb wurden in der Logistik vermutlich bereits viele technische Massnahmen umgesetzt, während das Thema noch nicht in der Unternehmenskultur verankert ist.*

Findet aktuell eine Diskussion über technische IT-Sicherheitsmassnahmen statt, die allenfalls durch die mediale Präsenz von ChatGPT angefacht wurde?

- *Experte 3 (49:05): Die Möglichkeiten in der AI-/KI-Welt sind endlos. «Phishing-Angriffe» können bisher oft aufgrund sprachlicher Fehler erkannt werden. Die Sprachqualität wird sich jedoch stark verbessern. Neu können z.B. auch ausländische Angreifer:innen fehlerfreies Deutsch schreiben und die «Phishing-Angriffe» automatisieren. Dazu kommen die Angriffe mit Fake-Stimmen, bei denen eine Stimme so tönt wie die einer bekannten Person. Das eröffnet neue Möglichkeiten für «Social Engineering-Angriffe». Inwiefern AI/KI heute in den Firmen bereits ein grosses Thema im Bereich Cybersicherheit ist, kann nicht beurteilt werden. Es wird jedoch bezweifelt. Oft wissen die verantwortlichen Personen nicht einmal, dass ihre Belegschaft mit ChatGPT arbeitet.*
- *Experte 1 (50:45): Aktuell steht die Faszination von ChatGPT im Vordergrund und die Risiken sind noch nicht fassbar. Es braucht noch mehr Zeit, bis das Risikobewusstsein bezüglich AI/KI vorhanden ist.*
- *Experte 4 (51:20): Heute sind breit abgestützte «Phishing-Angriff» aufwendig zu konstruieren (Website, Content, E-Mailadressen, Links, Produktdarstellungen, etc.). Da heute Content so schnell und auch automatisiert hergestellt werden kann, wird es immer leichter, erfolgreiche «Phishing-Angriffe» zu machen. Durch die Automatisierung der Angriffe wird mit einer noch höheren Frequenz gerechnet, die aufgrund der höheren Qualität auch zu mehr erfolgreichen Angriffen führen wird.*

Bedrohung durch Cyberangriffe

Wurde im Umfeld im letzten Jahr ein Anstieg von Cyberangriffen festgestellt?

- *Experte 1 (53:54): Vor drei Jahren war noch kein Fall eines Angriffs bekannt, vor zwei Jahren berichteten die ersten Firmen von konkreten Cyberangriffen und letztes Jahr war noch einmal ein kleiner Anstieg festzustellen. Es wird sich zeigen, ob die IT-Sicherheitsmassnahmen dies nun eindämmen.*

- *Experte 2 (55:12): Über die Rechtsberatung des Branchenverbands[25] konnte ein deutlicher Anstieg von Cyberangriffen registriert werden, durch Firmen, die in der Aufbereitung der Vorfälle die Rechtsberatung in Anspruch genommen haben.*
- *Experte 4 (55:58): In der Pandemie war ein Anstieg feststellbar (2020<2021<2022). Im Jahr 2023 ist es eher ruhig. Andere Themen standen im Vordergrund (Inflation, Energiepreise, Wahlbeeinflussung, Krieg, etc.).*

Konnten im Kontext der kriegerischen Aktivitäten in der Ukraine ein Anstieg von Cyberangriffen festgestellt werden?

- *Experte 1 (57:34): Es wurde keine spürbare Veränderung wahrgenommen.*

Weshalb ist «CEO-Fraud» in der Schweizer MEM- und Logistikbranche verbreiteter als in Deutschland?

- *Experte 2 (58:41): Der Branchenverband[25] war nach Auswertung der Umfrage [Isenhardt et al. (2022)] über diese Tatsache ebenfalls verwundert. Das Bewusstsein, dass «CEO-Fraud» in Deutschland generell weniger oft registriert wird, war nicht vorhanden bei der Diskussion der Studienergebnisse 2022. Diese konzentrierte sich vielmehr auf die Massnahmen, die daraus abgeleitet werden konnten. Vielleicht sind die Schweizer gutgläubiger oder es gibt mehr zu holen.*
- *Experte 4 (59:20): In der Schweiz ist die Wahrscheinlichkeit viel höher, dass die Mitarbeitenden Kontakt mit den CEO haben. In einer KMU-Struktur mit flacher Hierarchie ist ein CEO greifbarer. Dies könnte ein Grund sein, weshalb «CEO-Fraud» in der Schweiz besser funktioniert und deshalb auch häufiger auftritt.*
- *Experte 1 (1:00:04): Es ist unbekannt, welches Land welche Priorität hat. Der starke Finanzplatz Schweiz könnte eine anziehende Wirkung haben.*

[25] Der Name des Branchenverbandes wurde durch den Autor anonymisiert.

Online-Umfrage

Anschreiben[26]

Spedlogswiss

Versendet am Donnerstag, 23. Februar 2023

Umfrage zur Cybersicherheit in der Logistik

Sehr geehrte Damen und Herren

Cyberangriffe bedrohen Betriebe weltweit und sind unterdessen zu einem beträchtlichen Risikofaktor auch für die Schweizer Speditions- und Logistikbranche geworden. Viele Speditions- und Logistikunternehmen haben bereits wirkungsvolle IT-Sicherheitsmassnahmen umgesetzt. Doch wie ist die Branche als Ganzes aufgestellt?

Reto Nüesch Erismann (Leiter Technik & Applikationen, Cargologic) führt im Rahmen seiner Masterarbeit (Wirtschaftsinformatik, ZHAW) eine diesbezügliche Standortbestimmung in der Logistikbranche durch und vergleicht diese mit der Maschinen-, Elektro- und Metallindustrie (MEM-Industrie). SPEDLOGSWISS und GS1 unterstützen ihn dabei, weil sie an einer aussagekräftigen Umfrage zu diesem Thema interessiert sind.

Helfen auch Sie mit und nehmen Sie bis am 12. März 2023 an der anonymen Online-Umfrage teil. Allen Teilnehmenden stehen die Ergebnisse ab Mitte 2023 zur Verfügung und es gibt eine exklusive Führung bei Cargologic (Flughafen Zürich) zum Thema Luftfracht und Elektromobilität inkl. Mittagessen im Circle zu gewinnen, sofern eine E-Mail-Adresse am Schluss der Umfrage angegeben wird.

Hier kommen Sie direkt zur Umfrage:
Deutsch
Französisch
Englisch

Herzlichen Dank für Ihre Teilnahme!

Mit freundlichen Grüssen
SPEDLOGSWISS
Verband schweizerischer Speditions- und Logistikunternehmen
Vorname Name
Funktion

[26] Es wird nur die deutsche Version angefügt.

GS1 Switzerland

Versendet am Montag, 27. Februar 2023

Umfrage zur Cybersicherheit in der Logistik

Sehr geehrte Damen und Herren

Cyberangriffe bedrohen Betriebe weltweit und sind unterdessen zu einem beträchtlichen Risikofaktor auch für die Schweizer Speditions- und Logistikbranche geworden. Viele Speditions- und Logistikunternehmen haben bereits wirkungsvolle IT-Sicherheitsmassnahmen umgesetzt. Doch wie ist die Branche als Ganzes aufgestellt?

Reto Nüesch Erismann (Leiter Technik & Applikationen, Cargologic) führt im Rahmen seiner Masterarbeit (Wirtschaftsinformatik, ZHAW) eine diesbezügliche Standortbestimmung in der Logistikbranche durch und vergleicht diese mit der Maschinen-, Elektro- und Metallindustrie (MEM-Industrie). GS1 Switzerland, LCS, LSR und SPEDLOGSWISS unterstützen ihn dabei, weil sie an einer aussagekräftigen Umfrage zu diesem Thema interessiert sind.

Die Zielgruppe der Umfrage sind die Speditions- und Logistikunternehmen in der Schweiz. Dies beinhaltet jedoch nicht nur die klassischen Logistikdienstleister, Transport- und Speditionsunternehmen, sondern auch den Gross- und Detailhandel sowie die die Entsorgung von Gütern.

Helfen auch Sie mit und nehmen Sie bis am 12. März 2023 an der anonymen Online-Umfrage teil. Allen Teilnehmenden stehen die Ergebnisse ab Mitte 2023 zur Verfügung und es gibt eine exklusive Führung bei Cargologic (Flughafen Zürich) zum Thema Luftfracht und Elektromobilität inkl. Mittagessen im Circle zu gewinnen, sofern eine E-Mail-Adresse am Schluss der Umfrage angegeben wird.

Hier kommen Sie direkt zur Umfrage:
Deutsch
Französisch
Englisch

Herzlichen Dank für Ihre Teilnahme!

Mit freundlichen Grüssen
GS1 Switzerland
Logistik Leiter Club
Club de Logisticiens de Suisse Romande
Vorname Name
Funktion

LinkedIn

Veröffentlicht am Montag, 27. Februar 2023

Erinnerungsschreiben

Spedlogswiss

Gesendet am Dienstag, 7. März 2023

Umfrage zur Cybersicherheit in der Logistik

Sehr geehrte Damen und Herren

Seit dem 23. Februar 2023 haben Sie die Möglichkeit, an der "Untersuchung der Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche" teilzunehmen.

Falls Sie noch nicht teilgenommen haben, bitte ich Sie, bis am 12.03.2023 den Fragebogen vollständig auszufüllen. Sie leisten damit einen wertvollen Beitrag, um eine Standortbestimmung unserer Branche vorzunehmen.

Da es sich eher um technische Fragen handelt, bitte ich Sie, den Fragebogen allenfalls an die IT-Verantwortlichen in Ihrem Unternehmen weiterzuleiten. Hat Ihr Unternehmen die IT-Funktionen an einen externen Dienstleister vergeben, bitte ich Sie, die Umfrage an Ihn weiterzuleiten.

Allen Teilnehmenden stehen die Ergebnisse ab Mitte 2023 zur Verfügung und es gibt eine exklusive Führung bei Cargologic (Flughafen Zürich) zum Thema Luftfracht und Elektromobilität inkl. Mittagessen im Circle zu gewinnen, sofern eine E-Mail-Adresse am Schluss der Umfrage angegeben wird.

Hier kommen Sie direkt zur Umfrage:
Deutsch
Französisch
Englisch

Herzlichen Dank für Ihre Teilnahme!

Mit freundlichen Grüssen
SPEDLOGSWISS
Verband schweizerischer Speditions- und Logistikunternehmen
Vorname Name
Funktion

GS1 Switzerland

Gesendet am Dienstag, 7. März 2023

Umfrage zur Cybersicherheit in der Logistik

Sehr geehrte Damen und Herren

Seit dem 27. Februar 2023 haben Sie die Möglichkeit, an der "Untersuchung der Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche" teilzunehmen.

Falls Sie noch nicht teilgenommen haben, bitte ich Sie, bis am 12.03.2023 den Fragebogen vollständig auszufüllen. Sie leisten damit einen wertvollen Beitrag, um eine Standortbestimmung unserer Branche vorzunehmen.

Da es sich eher um technische Fragen handelt, bitte ich Sie, den Fragebogen allenfalls an die IT-Verantwortlichen in Ihrem Unternehmen weiterzuleiten. Hat Ihr Unternehmen die IT-Funktionen an einen externen Dienstleister vergeben, bitte ich Sie, die Umfrage an Ihn weiterzuleiten.

Allen Teilnehmenden stehen die Ergebnisse ab Mitte 2023 zur Verfügung und es gibt eine exklusive Führung bei Cargologic (Flughafen Zürich) zum Thema Luftfracht und Elektromobilität inkl. Mittagessen im Circle zu gewinnen, sofern eine E-Mail-Adresse am Schluss der Umfrage angegeben wird.

Hier kommen Sie direkt zur Umfrage:
Deutsch
Französisch
Englisch

Herzlichen Dank für Ihre Teilnahme!

Mit freundlichen Grüssen
GS1 Switzerland
Logistik Leiter Club
Club de Logisticiens de Suisse Romande
Vorname Name
Funktion

Fragebogen[27]

[Einleitung] Untersuchung der Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche

Sehr geehrte Damen und Herren

Unterstützt von GS1 Switzerland, Logistikleiterclub Schweiz, Club de Logisticiens de Suisse Romande, SPEDLOGSWISS und ZHAW führe ich im Rahmen meiner Masterarbeit eine «Umfrage zu Cyberangriffen und IT-Sicherheitsmassnahmen in der Schweizer Logistikbranche» durch. Es soll untersucht werden, wie es um die Cybersicherheit steht: Werden Unternehmen gezielt angegriffen? Welche IT-Sicherheitsmassnahmen wurden umgesetzt? Welchen Stellenwert haben die Mitarbeitenden?

Da es sich eher um technische Fragen handelt, bitte ich Sie, den Fragebogen allenfalls an die IT-Verantwortlichen in Ihrem Unternehmen weiterzuleiten. Hat Ihr Unternehmen die IT-Funktionen an einen externen Dienstleister vergeben, bitte ich Sie, die Umfrage an ihn weiterzuleiten.

Die Umfrage wird anonym durchgeführt. Die Ergebnisse werden allen Teilnehmenden Mitte 2023 zur Verfügung gestellt und es wird eine exklusive Führung bei **Cargologic** (Flughafen Zürich) zum Thema Luftfracht und Elektromobilität inkl. Mittagessen im Circle verlost, sofern eine E-Mail-Adresse am Schluss der Umfrage angegeben wird.

Mit Ihrer Teilnahme bis am 12. März 2023 helfen Sie mit, Erkenntnisse zu gewinnen, um die Cybersicherheit in der Logistikbranche zu erhöhen.

Falls Sie Fragen zur Umfrage oder zu einzelnen Fragen haben sollten oder technischen Support in Anspruch nehmen möchten, erreichen Sie mich unter: nueesret@students.zhaw.ch oder +41 77 453 38 32.

Der Fragebogen wird ca. 20 Minuten Bearbeitungszeit in Anspruch nehmen.

Klicken Sie nun bitte auf «Weiter», um die Umfrage zu starten.

Herzlichen Dank für Ihre Teilnahme!

Reto Nüesch Erismann
Master-Student Wirtschaftsinformatik, ZHAW
Leiter Technik und Applikationen / Mitglied der Geschäftsleitung, Cargologic

[A01] In welchem Bereich sind Sie in Ihrem Unternehmen tätig? *
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *Geschäftsführung / Vorstand*
- ☐ *Generelle IT / ICT*
- ☐ *IT-Sicherheit / Informationssicherheit*
- ☐ *Governance & Datenschutz*
- ☐ *Sonstiges*
- ☐ *Keine Angabe*

[A02] In welchem Wirtschaftszweig / in welcher Branche ist Ihr Unternehmen tätig bzw. das Unternehmen, das Sie als ICT-Dienstleister vertreten? *
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ☐ *A: Land- und Forstwirtschaft, Fischerei*
- ☐ *B: Bergbau und Gewinnung von Steinen und Erden*
- ☐ *C: Verarbeitendes Gewerbe/Herstellung von Waren*
- ☐ *D: Energieversorgung*

[27] Version Spedlogswiss, Deutsch (* = Pflichtfelder)

- ☐ *E: Wasserversorgung; Abwasser- und Abfallentsorgung und Beseitigung von Umweltverschmutzungen*
- ☐ *F: Baugewerbe/Bau*
- ☐ *G: Handel; Instandhaltung und Reparatur von Motorfahrzeuge*
- ☐ *H: Verkehr und Lagerei*
- ☐ *I: Gastgewerbe / Beherbergung und Gastronomie*
- ☐ *J: Information und Kommunikation*
- ☐ *K: Erbringung von Finanz- und Versicherungsdienstleistungen*
- ☐ *L: Grundstücks- und Wohnungswesen*
- ☐ *M: Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen*
- ☐ *N: Erbringung von sonstigen wirtschaftlichen Dienstleistungen*
- ☐ *O: Öffentliche Verwaltung, Verteidigung; Sozialversicherung*
- ☐ *P: Erziehung und Unterricht*
- ☐ *Q: Gesundheits- und Sozialwesen*
- ☐ *R: Kunst, Unterhaltung und Erholung*
- ☐ *S: Erbringung von sonstigen Dienstleistungen*
- ☐ *T: Private Haushalte mit Hauspersonal; Herstellung von Waren und Erbringung von Dienstleistungen durch private Haushalte für den Eigenbedarf ohne*
- ☐ *U: Exterritoriale Organisationen und Körperschaften*

(NOGA 2008)

[A02C] Bitte spezifizieren Sie den Wirtschaftszweig / die Branche noch etwas genauer...
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage A02 war «C: Verarbeitendes Gewerbe/Herstellung von Waren»
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *10: Herstellung von Nahrungs- und Futtermitteln*
- ☐ *11: Getränkeherstellung*
- ☐ *12: Tabakverarbeitung*
- ☐ *13: Herstellung von Textilien*
- ☐ *14: Herstellung von Bekleidung*
- ☐ *15: Herstellung von Leder, Lederwaren und Schuhen*
- ☐ *16: Herstellung von Holz-, Flecht-, Korb- und Korkwaren (ohne Möbel)*
- ☐ *17: Herstellung von Papier, Pappe und Waren daraus*
- ☐ *18: Herstellung von Druckerzeugnissen; Vervielfältigung von bespielten Ton-, Bild- und Datenträgern*
- ☐ *19: Kokerei und Mineralölverarbeitung*
- ☐ *20: Herstellung von chemischen Erzeugnissen*
- ☐ *21: Herstellung von pharmazeutischen Erzeugnissen*
- ☐ *22: Herstellung von Gummi- und Kunststoffwaren*
- ☐ *23: Herstellung von Glas und Glaswaren, Keramik, Verarbeitung von Steinen und Erden*
- ☐ *24: Metallerzeugung und -bearbeitung*
- ☐ *25: Herstellung von Metallerzeugnissen*

- ☐ *26: Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen*
- ☐ *27: Herstellung von elektrischen Ausrüstungen*
- ☐ *28: Maschinenbau*
- ☐ *29: Herstellung von Automobilen und Automobilteilen*
- ☐ *30: Sonstiger Fahrzeugbau*
- ☐ *31: Herstellung von Möbeln*
- ☐ *32: Herstellung von sonstigen Waren*
- ☐ *325: Herstellung von medizinischen und zahnmedizinischen Apparaten und Materialien*
- ☐ *33: Reparatur und Installation von Maschinen und Ausrüstungen*

[A02E] Bitte spezifizieren Sie den Wirtschaftszweig / die Branche noch etwas genauer...
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage A02 war «E: Wasserversorgung; Abwasser- und Abfallentsorgung und Beseitigung von Umweltverschmutzungen»
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *36: Wasserversorgung*
- ☐ *37: Abwasserentsorgung*
- ☐ *38: Sammlung, Behandlung und Beseitigung von Abfällen; Rückgewinnung*
- ☐ *39: Beseitigung von Umweltverschmutzungen und sonstige Entsorgung*

[A02G] Bitte spezifizieren Sie den Wirtschaftszweig / die Branche noch etwas genauer...
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage A02 war «G: Handel; Instandhaltung und Reparatur von Motorfahrzeuge»
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *45: Handel mit Motorfahrzeugen; Instandhaltung und Reparatur von Motorfahrzeugen*
- ☐ *46: Grosshandel (ohne Handel mit Motorfahrzeugen)*
- ☐ *47: Detailhandel (ohne Handel mit Motorfahrzeugen)*

[A02H] Bitte spezifizieren Sie den Wirtschaftszweig / die Branche noch etwas genauer...
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage A02 war «H: Verkehr und Lagerei»
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *49: Landverkehr und Transport in Rohrfernleitungen*
- ☐ *50: Schifffahrt*
- ☐ *51: Luftfahrt*
- ☐ *52: Lagerei sowie Erbringung von sonstigen Dienstleistungen für den Verkehr*
- ☐ *53: Post-, Kurier- und Expressdienste*

[A03] Wie viele Mitarbeitende hat Ihr Unternehmen bzw. das Unternehmen, das Sie als ICT-Dienstleister vertreten? *
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ☐ *1 bis 9 Beschäftigte (Microunternehmen)*
- ☐ *10 bis 49 Beschäftigte (Kleine Unternehmen)*
- ☐ *50 bis 249 Beschäftigte (Mittlere Unternehmen)*
- ☐ *ab 250 Beschäftigte (Grosse Unternehmen)*

[A04] Wie viele Mitarbeitende davon arbeiten hauptsächlich im Bereich ...
Nur Zahlen dürfen in diese Felder eingegeben werden.
Bitte geben Sie Ihre Antwort(en) hier ein:

- ☐ *Generelle IT / ICT? _____*
- ☐ *IT-Sicherheit / Informationssicherheit? _____*

[A05] Hat Ihr Unternehmen IT-Funktionen an einen externen Dienstleister vergeben (Outsourcing)? Wenn ja, welche IT-Funktionen?
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *Keine IT-Funktionen ausgelagert*
- ☐ *E-Mail & Kommunikation*
- ☐ *Netzwerk-Administration & Wartung*
- ☐ *Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale)*
- ☐ *Cloud-Software & Cloud-Speicher*
- ☐ *IT-Security (z.B. Incident Detection, SIEM, SOC, Threat Intelligence)*
- ☐ *Sonstiges (bitte eintragen): _____*

[A06] Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, in den nächsten 12 Monaten von einem Cyberangriff geschädigt zu werden, ...
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	sehr gering	eher gering	eher hoch	sehr hoch	keine Angabe
... der gleichzeitig auch viele andere Unternehmen trifft? (z.B. massenhaft versendete Schadsoftware)					
... der ausschliesslich Ihr Unternehmen trifft? (z.B. gezielter Spionageangriff)					

[A07] Was denken Sie: Warum könnte Ihr Unternehmen Ziel eines Cyberangriffs werden? Haben Sie ...?
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	ja	nein	keine Angabe
... besondere Produkte, Herstellungsverfahren oder Dienstleistungen (z.B. aufgrund spezieller Technik, Design, Materialien, Innovation)			
... besondere Reputation / Kundenkreis (z.B. hoher Bekanntheitsgrad, hohe Sicherheitsstandards, besondere Verschwiegenheit)			

[B01] War Ihr Unternehmen jemals von einem oder mehreren der unten aufgeführten Cyberangriffe betroffen? *
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	ja	nein	keine Angabe
Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware			

	ja	nein	keine Angabe
Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln			
Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen			
Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner			
Denial of Service (D)DoS-Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten			
Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern			
Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden			
«CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung			
Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken / Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen			
Andere Angriffsart			

[B0101] Bitte beschreiben Sie den Cyberangriff "Andere Angriffsart".
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage B01 war «ja» bei Option «Andere Angriffsart»
Bitte geben Sie Ihre Antwort hier ein: _____

[B02] Wenn ja, wie häufig in den letzten 24 Monaten vor der Befragung? *
Tragen Sie bitte «Null» ein, wenn in den letzten 24 Monaten kein Angriff erfolgte.
Es werden nur in Frage B01 mit «ja» beantwortete Cyberangriffe aufgeführt.
Bitte geben Sie Ihre Antwort(en) hier ein:

- ☐ *Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware _____*
- ☐ *Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln _____*
- ☐ *Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen _____*
- ☐ *Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner _____*
- ☐ *Denial of Service (D)DoS-Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten _____*
- ☐ *Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern _____*
- ☐ *Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden _____*

- ☐ *CEO-Fraud, wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung _____*
- ☐ *Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken / Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen _____*
- ☐ *Andere Angriffsart _____*

[B03] Welches wären die schwerwiegendsten Folgen für Ihr Unternehmen, falls es Opfer eines Cyberangriffes würde?
Bitte wählen sie die 5 schwerwiegendsten Folgen aus und bringen Sie diese in eine Rangfolge.
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antworten auf Frage B01 waren ausschliesslich «nein»
Bitte wählen Sie maximal 5 Antworten. Bitte nummerieren Sie jede Box in der Reihenfolge Ihrer Präferenz.

- ☐ *Ausfall der Informatik*
- ☐ *Diebstahl oder Schädigung von IT- oder Kommunikationsgeräten*
- ☐ *Betriebsunterbrechung (d.h. vollständiger oder teilweiser Ausfall der Produktion und Administration)*
- ☐ *Erpressung mit den verschlüsselten Daten*
- ☐ *Erpressung mit entwendeten Daten*
- ☐ *Kosten für Sofortmassnahmen zur Abwehr und Aufklärung*
- ☐ *Kosten aufgrund von Lösegeldzahlungen*
- ☐ *Kosten für Wiederherstellung von Daten oder IT-Infrastruktur (Hardware und Software)*
- ☐ *Kosten für externe Beratung*
- ☐ *Kosten für Rechtsstreitigkeiten, Schadensersatz, Strafen*
- ☐ *Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen*
- ☐ *Negative Auswirkung auf die Geschäftsentwicklung*
- ☐ *Kundenverluste / Auftragsverluste*
- ☐ *Verlust von personenbezogenen Daten, z.B. Kundendaten, Daten von Mitarbeitenden*
- ☐ *Reputationsverluste / Negative Presse*
- ☐ *Interne Reorganisationskosten*
- ☐ *Entlassung von Mitarbeitenden*
- ☐ *Höhere Mitarbeitenden Fluktuation, z.B. Verlust von kompetenten Arbeitskräften*
- ☐ *Positive Reaktionen (z.B. von Kundinnen und Kunden) auf den raschen und resilienten Umgang mit dem Angriff*
- ☐ *Erhöhung des Zusammenhalts unter den Mitarbeitenden*
- ☐ *Andere*

[B0301] Bitte beschreiben Sie "andere" Folge eines Cyberangriffes.
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage B03 war «ja» bei Option «Andere»
Bitte geben Sie Ihre Antwort hier ein: _____

[B04] Sie haben für die unten aufgeführten Angriffsarten angegeben, dass Ihr Unternehmen in den letzten 24 Monaten von diesen betroffen war. Welcher dieser Angriffe war aus Ihrer Sicht der schwerwiegendste? *
Es werden nur in Frage B02 mit > 0 beantwortete Cyberangriffe aufgeführt.
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware*
- ☐ *Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln*
- ☐ *Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen*
- ☐ *Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner*
- ☐ *Denial of Service (D)DoS-Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten*
- ☐ *Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern*
- ☐ *Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden*
- ☐ *CEO-Fraud, wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung*
- ☐ *Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen*
- ☐ *Andere Angriffsart*

Sie können mehrere Angriffsarten auswählen, wenn mehrere Angriffsarten zusammen aufgetreten sind.

[B05] Wo war der initiale Angriffspunkt des von Ihnen angegebenen «schwerwiegendsten Angriffs»?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ☐ *Niederlassung im Inland*
- ☐ *Niederlassung im Ausland*
- ☐ *Subunternehmer*
- ☐ *Lieferanten*
- ☐ *Kundschaft*
- ☐ *Dienstleister, z.B. Cloudanbieter*
- ☐ *Keine Angabe*
- ☐ *Anderer Ort oder Teilnehmer der Supply Chain (bitte eintragen)*

[B06] Was denken Sie: Wurde Ihr Unternehmen bei dem von Ihnen angegebenen «schwerwiegendsten Angriff» bzw. den zusammengehörigen Angriffen...
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ☐ *zielgerichtet attackiert / ausgewählt (z.B. gezielter Spionageangriff)?*
- ☐ *als ein Unternehmen von vielen anderen attackiert (z.B. bei massenhaft versendeter Schadsoftware, Ransomware-Angriffen oder dem Ausnützen von technischen Schwachstellen)?*
- ☐ *keine Angabe*

[B07] Zu welchen Folgen hat der genannte schwerwiegendste Angriff bzw. die zusammengehörigen Angriffe geführt?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.

Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *Ausfall der Informatik*
- ☐ *Diebstahl oder Schädigung von IT- oder Kommunikationsgeräten*
- ☐ *Betriebsunterbrechung (d.h. vollständiger oder teilweiser Ausfall der Produktion und Administration)*
- ☐ *Erpressung mit den verschlüsselten Daten*
- ☐ *Erpressung mit entwendeten Daten*
- ☐ *Kosten für Sofortmassnahmen zur Abwehr und Aufklärung*
- ☐ *Kosten aufgrund von Lösegeldzahlungen*
- ☐ *Kosten für Wiederherstellung von Daten oder IT-Infrastruktur (Hardware und Software)*
- ☐ *Kosten für externe Beratung*
- ☐ *Kosten für Rechtsstreitigkeiten, Schadensersatz, Strafen*
- ☐ *Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen*
- ☐ *Negative Auswirkung auf die Geschäftsentwicklung*
- ☐ *Kundenverluste/Auftragsverluste*
- ☐ *Verlust von personenbezogenen Daten, z.B. Kundendaten, Daten von Mitarbeitenden*
- ☐ *Reputationsverluste/Negative Presse*
- ☐ *Interne Reorganisationskosten*
- ☐ *Entlassung von Mitarbeitenden*
- ☐ *Höhere Mitarbeitenden Fluktuation, z.B. Verlust von kompetenten Arbeitskräften*
- ☐ *Positive Reaktionen (z.B. von Kundinnen und Kunden) auf den raschen und resilienten Umgang mit dem Angriff*
- ☐ *Erhöhung des Zusammenhalts unter den Mitarbeitenden*
- ☐ *Keine Angabe*
- ☐ *Keine Folge*
- ☐ *Andere (bitte eintragen): _____*

[B08] Gab es bei diesem «schwerwiegendsten Angriff» eine Lösegeldforderung?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ☐ *ja*
- ☐ *nein*
- ☐ *keine Angabe*

[B09] Ist Ihr Unternehmen der Lösegeldforderung nachgekommen?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Frage B08 wurde mit «ja» beantwortet.
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ☐ *ja*
- ☐ *nein*
- ☐ *keine Angabe*

[B10] Sind die Angreifer ihren Versprechungen (Daten-Entschlüsselung oder Stoppen des Angriffs) nachgekommen?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Frage B09 wurde mit «ja» beantwortet.
Bitte wählen Sie nur eine der folgenden Antworten aus:

☐ *ja*

☐ *nein*

☐ *keine Angabe*

[B11] Waren folgende IT-Systeme vom schwersten Angriff betroffen?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	ja	nein	keine Angabe
Standard-Arbeitsplatz und Office IT			
E-Mail und Kommunikation (z.B. Partner-Portale, Netzspeicher)			
Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale)			
Auftrags- und Kundenverwaltung (z.B. Termin- und Reservierungssysteme, Rechnungsverwaltung)			
Produktionssteuerung (Fokus auf Maschinen- und Anlagensteuerung)			
Lager und Logistik			
Banking und Trading			
Rechnungswesen, Controlling (z.B. für Jahresabschluss, Berichtserstellung)			
IT-Sicherheitssysteme (z.B. Firewalls, SIEM)			
Sonstige Systeme (z.B. Projektplanung, CAD, Berechnungen von Statik)			

[B12] Bitte geben Sie an, welche Kosten durch den von Ihnen angegebenen «schwerwiegendsten Angriff» entstanden sind.
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
In diesem Feld darf nur ein ganzzahliger Wert > 0 eingetragen werden. Bitte schätzen Sie, falls die Kosten nicht genau beziffert werden können.

☐ *Bitte geben Sie Ihre Antwort hier ein: CHF _____*

[B13] Waren bei dem genannten «schwerwiegendsten Angriff» die folgenden Daten betroffen? Wurden diese gelöscht, manipuliert, gestohlen oder verschlüsselt?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	ja, sie wurden gelöscht	ja, sie wurden manipuliert	ja, sie wurden gestohlen	ja, sie wurden verschlüsselt oder blockiert	nein	keine Angabe
Kunden- und personenbezogene Daten						
Produktions- und Prozessdaten						

	ja, sie wurden gelöscht	ja, sie wurden manipuliert	ja, sie wurden gestohlen	ja, sie wurden verschlüsselt oder blockiert	nein	keine Angabe
Produkt und F&E Daten						
Betriebswirtschaftliche Daten						
Andere Daten						

[B14] Wer hat von diesem Vorfall erfahren?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	ja	nein	keine Angabe
Kunden			
Geschäftspartner			
Versicherer			
Eigentümer*innen des Unternehmens			
Öffentlichkeit			

[B15] Zu welchen der unten aufgeführten Akteure wurde nach dem von Ihnen genannten «schwerwiegendsten Angriff» Kontakt aufgenommen?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie alle zutreffenden Antworten aus:

☐ *Polizei*

☐ *Nachrichtendienst des Bundes (NDB) oder vergleichbare Behörden im Ausland*

☐ *Versicherung*

☐ *Spezialisierter Dienstleister*

☐ *Nationales Zentrum für Cybersicherheit (NCSC) oder vergleichbare Behörden im Ausland*

☐ *Andere (bitte eintragen): _____*

[B16] Bitte ergänzen Sie: Der durch den «schwerwiegendsten Angriff» erfolgte Schaden...
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie nur eine der folgenden Antworten aus:

☐ *war kurzfristig behebbar und leicht verdaubar*

☐ *führte zu spürbaren Einschränkungen*

☐ *gefährdete die Existenz des Unternehmens*

☐ *zog keine Einschränkungen nach sich*

☐ *Anderer Schaden (bitte eintragen): _____*

[C0101] Welche der folgenden technischen IT-Sicherheitsmassnahmen gibt es in Ihrem Unternehmen?
Geben Sie bitte an, ob die Massnahme VOR oder NACH dem «schwerwiegendsten Angriff» der letzten 24 Monate eingeführt wurde bzw. ob die Einführung geplant ist.
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	VOR dem Angriff umgesetzt	NACH dem Angriff umgesetzt	GEPLANTE Umsetzung	KEINE Umsetzung	Keine Angabe
Einführung eines Informationssicherheits-Managementsystems (ISMS)					
Security Information and Event Management (SIEM)					
Security Operation Center (SOC)					
Antivirensoftware					
Schutz der IT-Systeme mit einer Firewall					
Intrusion Detection System (IDS)					
Cyber Threat Intelligence (Austausch von Bedrohungsdaten)					
Künstliche Intelligenz basierte Massnahmen					
Netzwerksegmentierung					
Regelmässige Backups					
Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches					
Verschlüsselung von E-Mails					
Verschlüsselung von Festplatten (Full-Disk-Encryption)					
Mindestanforderungen für Passwörter					
Multifaktor-Authentifikation					
Weitere technische Massnahmen					

[C010101] Bitte beschreiben Sie «Weitere technische Massnahmen».
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage C0101 war «ja» bei Option «Weitere technische Massnahmen»
Bitte geben Sie Ihre Antwort hier ein: _____

[C0102] Welche der folgenden <u>organisatorischen</u> IT-Sicherheitsmassnahmen gibt es in Ihrem Unternehmen?
Geben Sie bitte an, ob die Massnahme VOR oder NACH dem «schwerwiegendsten Angriff» der letzten 24 Monate eingeführt wurde bzw. ob die Einführung geplant ist.
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Eine Antwort auf Frage B04 wurde mit «ja» beantwortet.
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	VOR dem Angriff umgesetzt	NACH dem Angriff umgesetzt	GEPLANTE Umsetzung	KEINE Umsetzung	Keine Angabe
Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme					

	VOR dem Angriff umgesetzt	NACH dem Angriff umgesetzt	GEPLANTE Umsetzung	KEINE Umsetzung	Keine Angabe
Regelmässige Risiko- und Schwachstellenanalysen					
Cyber Awareness Trainings für Mitarbeitende					
Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit					
Schriftlich fixierte Richtlinien zum Notfallmanagement					
Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe					
Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk					
Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen					
Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern					
Weitere organisatorische Massnahmen					

[C010102] Bitte beschreiben Sie «Weitere organisatorische Massnahmen».
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage C0102 war «ja» bei Option «Weitere organisatorische Massnahmen»
Bitte geben Sie Ihre Antwort hier ein: _____

[C02] Welche technische IT-Sicherheitsmassnahme war in erster Linie an der Entdeckung des «schwerwiegendsten Angriff» beteiligt?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage C0102 war «VOR dem Angriff umgesetzt».
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *Einführung eines Informationssicherheits-Managementsystems (ISMS)*
- ☐ *Security Information and Event Management (SIEM)*
- ☐ *Security Operation Center (SOC)*
- ☐ *Antivirensoftware*
- ☐ *Schutz der IT-Systeme mit einer Firewall*
- ☐ *Intrusion Detection System (IDS)*
- ☐ *Cyber Threat Intelligence (Austausch von Bedrohungsdaten)*
- ☐ *Künstliche Intelligenz basierte Massnahmen*
- ☐ *Netzwerksegmentierung*

- ☐ *Regelmässige Backups*
- ☐ *Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches*
- ☐ *Verschlüsselung von E-Mails*
- ☐ *Verschlüsselung von Festplatten (Full-Disk-Encryption)*
- ☐ *Mindestanforderungen für Passwörter*
- ☐ *Multifaktor-Authentifikation*
- ☐ *Weitere Massnahmen*

[C0301] Welche der folgenden technischen IT-Sicherheitsmassnahmen gibt es in Ihrem Unternehmen?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antworten auf Frage B01 waren ausschliesslich «nein»
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *Einführung eines Informationssicherheits-Managementsystems (ISMS)*
- ☐ *Security Information and Event Management (SIEM)*
- ☐ *Security Operation Center (SOC)*
- ☐ *Antivirensoftware*
- ☐ *Schutz der IT-Systeme mit einer Firewall*
- ☐ *Intrusion Detection System (IDS)*
- ☐ *Cyber Threat Intelligence (Austausch von Bedrohungsdaten)*
- ☐ *Künstliche Intelligenz basierte Massnahmen*
- ☐ *Netzwerksegmentierung*
- ☐ *Regelmässige Backups*
- ☐ *Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches*
- ☐ *Verschlüsselung von E-Mails*
- ☐ *Verschlüsselung von Festplatten (Full-Disk-Encryption)*
- ☐ *Mindestanforderungen für Passwörter*
- ☐ *Multifaktor-Authentifikation*
- ☐ *Weitere technische Massnahmen*
- ☐ *Keine Massnahmen*

[C030101] Bitte beschreiben Sie «Weitere technische Massnahmen».
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage C0301 war «ja» bei Option «Weitere technische Massnahmen»
Bitte geben Sie Ihre Antwort hier ein: _____

[C0302] Welche der folgenden organisatorischen IT-Sicherheitsmassnahmen gibt es in Ihrem Unternehmen?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antworten auf Frage B01 waren ausschliesslich «nein»
Bitte wählen Sie alle zutreffenden Antworten aus:

- ☐ *Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme*
- ☐ *Regelmässige Risiko- und Schwachstellenanalysen*
- ☐ *Cyber Awareness Trainings für Mitarbeitende*
- ☐ *Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit*

- ☐ *Schriftlich fixierte Richtlinien zum Notfallmanagement*
- ☐ *Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe*
- ☐ *Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk*
- ☐ *Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen*
- ☐ *Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern*
- ☐ *Weitere organisatorische Massnahmen*
- ☐ *Keine Massnahmen*

[C030201] Bitte beschreiben Sie «Weitere organisatorische Massnahmen».
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage C0302 war «ja» bei Option «Weitere organisatorische Massnahmen»
Bitte geben Sie Ihre Antwort hier ein: _____

[C04] Wie effektiv erachten Sie diese technischen IT-Sicherheitsmassnahmen zur Abwehr von Cyberangriffen?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Es werden nur in Frage C0301 mit «ja» beantwortete IT-Sicherheitsmassnahmen aufgeführt.
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	sehr grosser Nutzen	eher grosser Nutzen	eher kleiner Nutzen	sehr kleiner Nutzen	keine Angabe
Einführung eines Informationssicherheits-Managementsystems (ISMS)					
Security Information and Event Management (SIEM)					
Security Operation Center (SOC)					
Antivirensoftware					
Schutz der IT-Systeme mit einer Firewall					
Intrusion Detection System (IDS)					
Cyber Threat Intelligence (Austausch von Bedrohungsdaten)					
Künstliche Intelligenz basierte Massnahmen					
Netzwerksegmentierung					
Regelmässige Backups					
Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches					
Verschlüsselung von E-Mails					
Verschlüsselung von Festplatten (Full-Disk-Encryption)					
Mindestanforderungen für Passwörter					
Multifaktor-Authentifikation					
Weitere Massnahmen					

[C0501] Bitte schätzen Sie den Reifegrad der vorhandenen IT-Sicherheitsmassnahmen im Unternehmen ein.
Geben Sie bitte an, was am ehesten für Ihr Unternehmen zutrifft.
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage C0101 oder C0102 war «VOR dem Angriff umgesetzt» oder «NACH dem Angriff umgesetzt» oder «GEPLANTE Umsetzung».
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	Reifegradskala 1: Grundfunktionalität / -umfang	Reifegradskala 2: Erweiterte Funktionalität / Umfang	Reifegradskala 3: Grundfunktionalität und regelmässige Überprüfung / Optimierung	Reifegradskala 4: Erweiterte Funktionalität und regelmässige Überprüfung / Optimierung
Einführung eines Informationssicherheits-Managementsystems (ISMS)				
Security Information and Event Management (SIEM)				
Security Operation Center (SOC)				
Antivirensoftware				
Schutz der IT-Systeme mit einer Firewall				
Intrusion Detection System (IDS)				
Cyber Threat Intelligence (Austausch von Bedrohungsdaten)				
Künstliche Intelligenz basierte Massnahmen				
Netzwerksegmentierung				
Regelmässige Backups				
Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches				
Verschlüsselung von E-Mails				
Verschlüsselung von Festplatten (Full-Disk-Encryption)				
Mindestanforderungen für Passwörter				
Multifaktor-Authentifikation				
Weitere technische Massnahmen				
Übungen oder Simulationen für den				

	Reifegradskala 1: Grundfunktionalität / -umfang	Reifegradskala 2: Erweiterte Funktionalität / Umfang	Reifegradskala 3: Grundfunktionalität und regelmässige Überprüfung / Optimierung	Reifegradskala 4: Erweiterte Funktionalität und regelmässige Überprüfung / Optimierung
Ausfall wichtiger ICT-Systeme				
Regelmässige Risiko- und Schwachstellenanalysen				
Cyber Awareness Trainings für Mitarbeitende				
Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit				
Schriftlich fixierte Richtlinien zum Notfallmanagement				
Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe				
Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk				
Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen				
Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern				
Weitere organisatorische Massnahmen				

[C0502] Bitte schätzen Sie die Verbreitung bzw. den Geltungsbereich der vorhandenen IT-Sicherheitsmassnahmen im Unternehmen ein.
Geben Sie bitte an, was am ehesten für Ihr Unternehmen zutrifft.
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort auf Frage C0101 oder C0102 war «VOR dem Angriff umgesetzt» oder «NACH dem Angriff umgesetzt» oder «GEPLANTE Umsetzung».
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	Verbreitung im Unternehmen 1: stark begrenzt	Verbreitung im Unternehmen 2: teilweise	Verbreitung im Unternehmen 3: weitgehend
Einführung eines Informationssicherheits-Managementsystems (ISMS)			
Security Information and Event Management (SIEM)			
Security Operation Center (SOC)			
Antivirensoftware			
Schutz der IT-Systeme mit einer Firewall			
Intrusion Detection System (IDS)			
Cyber Threat Intelligence (Austausch von Bedrohungsdaten)			
Künstliche Intelligenz basierte Massnahmen			
Netzwerksegmentierung			
Regelmässige Backups			
Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches			
Verschlüsselung von E-Mails			
Verschlüsselung von Festplatten (Full-Disk-Encryption)			
Mindestanforderungen für Passwörter			
Multifaktor-Authentifikation			
Weitere technische Massnahmen			
Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme			
Regelmässige Risiko- und Schwachstellenanalysen			
Cyber Awareness Trainings für Mitarbeitende			
Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit			
Schriftlich fixierte Richtlinien zum Notfallmanagement			
Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe			
Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk			

	Verbreitung im Unternehmen 1: stark begrenzt	Verbreitung im Unternehmen 2: teilweise	Verbreitung im Unternehmen 3: weitgehend
Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen			
Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern			
Weitere organisatorische Massnahmen			

[C0601] Bitte schätzen Sie den Reifegrad der vorhandenen IT-Sicherheitsmassnahmen im Unternehmen ein.
Geben Sie bitte an, was am ehesten für Ihr Unternehmen zutrifft.
Es werden nur IT-Sicherheitsmassnahmen aufgeführt, die in Frage C0301 oder C0302 mit «ja» beantwortet wurden.
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	Reifegradskala 1: Grundfunktionalität / -umfang	Reifegradskala 2: Erweiterte Funktionalität / Umfang	Reifegradskala 3: Grundfunktionalität und regelmässige Überprüfung / Optimierung	Reifegradskala 4: Erweiterte Funktionalität und regelmässige Überprüfung / Optimierung
Einführung eines Informationssicherheits-Managementsystems (ISMS)				
Security Information and Event Management (SIEM)				
Security Operation Center (SOC)				
Antivirensoftware				
Schutz der IT-Systeme mit einer Firewall				
Intrusion Detection System (IDS)				
Cyber Threat Intelligence (Austausch von Bedrohungsdaten)				
Künstliche Intelligenz basierte Massnahmen				
Netzwerksegmentierung				
Regelmässige Backups				
Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches				

	Reifegradskala 1: Grundfunktionalität / -umfang	Reifegradskala 2: Erweiterte Funktionalität / Umfang	Reifegradskala 3: Grundfunktionalität und regelmässige Überprüfung / Optimierung	Reifegradskala 4: Erweiterte Funktionalität und regelmässige Überprüfung / Optimierung
Verschlüsselung von E-Mails				
Verschlüsselung von Festplatten (Full-Disk-Encryption)				
Mindestanforderungen für Passwörter				
Multifaktor-Authentifikation				
Weitere technische Massnahmen				
Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme				
Regelmässige Risiko- und Schwachstellenanalysen				
Cyber Awareness Trainings für Mitarbeitende				
Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit				
Schriftlich fixierte Richtlinien zum Notfallmanagement				
Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe				
Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk				
Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen				
Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern				

	Reifegradskala 1: Grundfunktionalität / -umfang	Reifegradskala 2: Erweiterte Funktionalität / Umfang	Reifegradskala 3: Grundfunktionalität und regelmässige Überprüfung / Optimierung	Reifegradskala 4: Erweiterte Funktionalität und regelmässige Überprüfung / Optimierung
Weitere organisatorische Massnahmen				

[C0602] Bitte schätzen Sie die Verbreitung bzw. den Geltungsbereich der vorhandenen IT-Sicherheitsmassnahmen im Unternehmen ein.
Geben Sie bitte an, was am ehesten für Ihr Unternehmen zutrifft.
Es werden nur IT-Sicherheitsmassnahmen aufgeführt, die in Frage C0301 oder C0302 mit «ja» beantwortet wurden.
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	Verbreitung im Unternehmen 1: stark begrenzt	Verbreitung im Unternehmen 2: teilweise	Verbreitung im Unternehmen 3: weitgehend
Einführung eines Informationssicherheits-Managementsystems (ISMS)			
Security Information and Event Management (SIEM)			
Security Operation Center (SOC)			
Antivirensoftware			
Schutz der IT-Systeme mit einer Firewall			
Intrusion Detection System (IDS)			
Cyber Threat Intelligence (Austausch von Bedrohungsdaten)			
Künstliche Intelligenz basierte Massnahmen			
Netzwerksegmentierung			
Regelmässige Backups			
Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches			
Verschlüsselung von E-Mails			
Verschlüsselung von Festplatten (Full-Disk-Encryption)			
Mindestanforderungen für Passwörter			
Multifaktor-Authentifikation			
Weitere technische Massnahmen			
Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme			
Regelmässige Risiko- und Schwachstellenanalysen			
Cyber Awareness Trainings für Mitarbeitende			

	Verbreitung im Unternehmen 1: stark begrenzt	Verbreitung im Unternehmen 2: teilweise	Verbreitung im Unternehmen 3: weitgehend
Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit			
Schriftlich fixierte Richtlinien zum Notfallmanagement			
Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe			
Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk			
Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen			
Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern			
Weitere organisatorische Massnahmen			

[C07] Haben Sie eine Versicherung gegen Informationssicherheitsverletzungen (Cyberversicherung)?
Bitte wählen Sie nur eine der folgenden Antworten aus:

☐ *ja*

☐ *nein*

☐ *keine Angabe*

[C08] Musste zum Abschluss der Cyberversicherungen bestimmte IT-Sicherheitsstandards nachgewiesen werden?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind: Frage C07 wurde mit «ja» beantwortet.
Bitte wählen Sie nur eine der folgenden Antworten aus:

☐ *ja*

☐ *nein*

☐ *keine Angabe*

[C09] Warum hat Ihr Unternehmen keine Cyberversicherung?
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind: Frage C07 wurde mit «nein» beantwortet.
Bitte wählen Sie alle zutreffenden Antworten aus:

☐ *Wir haben uns damit noch nicht beschäftigt*

☐ *Das Preis-Leistungs-Verhältnis stimmt nicht*

☐ *Wir konnten keine Versicherung finden, die uns versichert*

☐ *Sonstiger Grund*

☐ *Keine Angabe*

[C10] Was ist Ihr Eindruck zum Risikobewusstsein?
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	trifft gar nicht zu	trifft eher nicht zu	trifft eher zu	trifft voll und ganz zu	keine Angabe
Die Geschäftsführung ist sich der IT-Risiken bewusst und hält die Vorgaben ein					
Die Belegschaft ist sich der IT-Risiken bewusst und hält die Vorgaben ein					
Im Unternehmen wird sehr viel für die IT-Sicherheit getan					

[C11] Inwiefern treffen folgende Aussagen zur IT-Sicherheitsschulung für Ihr Unternehmen zu?
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	Trifft gar nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft voll und ganz zu	Keine Angabe
Alle Beschäftigten absolvieren mindestens jährlich ein Cyber Awareness Training					
Ausgewählte Mitarbeitende absolvieren mindestens jährlich ein Cyber Awareness Training					
Mitarbeitende, die regelmässig im Homeoffice arbeiten, absolvieren mindestens jährlich ein spezielles Cyber Awareness Training					
Es gibt verschiedene Cyber Awareness Training für verschiedene Zielgruppen im Unternehmen					
Es existieren Massnahmen zur Erfolgskontrolle/Vertiefung der Schulungen					
Cyber Awareness Trainings werden in verschiedenen Sprachen angeboten					

[D01] An dieser Stelle können Sie Rückmeldungen, Anregungen und Kommentare zur Umfrage erfassen. Fragen senden Sie bitte direkt an: nueesret@students.zhaw.ch
Bitte geben Sie Ihre Antwort hier ein: _____

Vielen Dank für Ihre Teilnahme!
Die Ergebnisse der Studie werden allen Teilnehmenden Mitte Jahr zur Verfügung gestellt.

[D02] Weiter wird eine exklusive Führung bei Cargologic (Flughafen Zürich) zum Thema Luftfracht und Elektromobilität inkl. Mittagessen im Circle verlost.
Bitte wählen Sie alle zutreffenden Antworten aus:

☐ *Ja, ich möchte die Ergebnisse erhalten*

☐ *Ja, ich möchte an der Verlosung teilnehmen*

☐ *Kein Interesse*

[D03] Die Umfrage wurde anonym durchgeführt. Ihre E-Mail-Adresse wird lediglich für das Zusenden der Studienresultate und für die Teilnahme an der Verlosung verwendet.
Bitte geben Sie Ihre E-Mail-Adresse ein. *
Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Frage D02 wurde mit «Ja, ich möchte die Ergebnisse erhalten» und / oder «Ja, ich möchte an der Verlosung teilnehmen» beantwortet.
Bitte geben Sie Ihre Antwort hier ein: _____

[Abschluss] Vielen Dank für Ihre Teilnahme an der Umfrage zu Cyberangriffen und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikbranche!

Beste Grüsse
Reto Nüesch Erismann
Master-Student Wirtschaftsinformatik, ZHAW
Leiter Technik und Applikationen / Mitglied der Geschäftsleitung, Cargologic

Datennutzungsvertrag Kriminologisches Forschungsinstitut Niedersachsen e. V.

KRIMINOLOGISCHES
FORSCHUNGSINSTITUT
NIEDERSACHSEN E.V.

Vertrag über die Nutzung von Daten
zwischen

dem Kriminologischen Forschungsinstitut Niedersachsen (KFN), vertreten durch den Direktor Prof. Dr. Thomas Bliesener,

und
Reto Nüesch Erismann (Zürcher Hochschule für Angewandte Wissenschaften), nachfolgend: „Datennehmer“

§ 1 Einleitung

Der Vertrag regelt die Rechte und Pflichten zwischen dem KFN und der Datennehmer*in bezüglich der Nutzung von Daten des Projektes „Cyberangriffe gegen Unternehmen“. In diesem Projekt wurde eine CATI-Befragung von 5.000 Unternehmen sowie eine Folgebefragung mittels Online-Fragebogen durchgeführt und ein zusammengefasster Datensatz erstellt. Auf diesen Datensatz beziehen sich die nachfolgenden vertraglichen Regelungen.

§ 2 Vertragsgegenstand

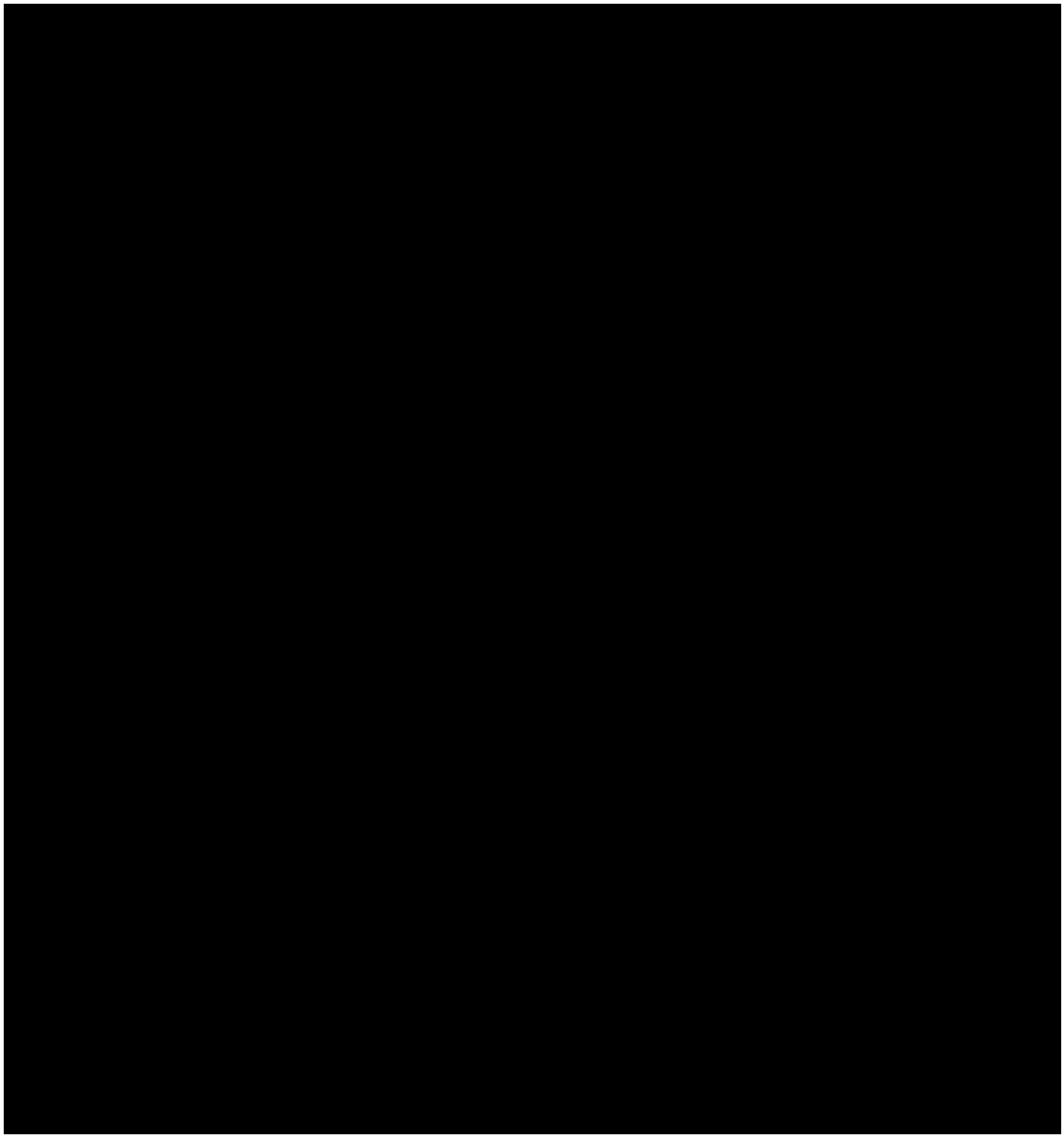
(1) Der Datennehmer erhält eine Kopie des Datensatzes über Nextcloud. Er ist berechtigt, im Rahmen seiner Abschlussarbeit „Vergleichende empirische Untersuchung von Schweizer Unternehmen der Logistikbranche in Bezug auf die Cybersecurity“ (Arbeitstitel der Masterarbeit) die Daten zu sichten, Fragestellungen zu entwerfen und diese mit dem Datensatz zu prüfen.

(2) Der zur Verfügung gestellte Datensatz darf nur vom Datennehmer zu dem Zweck der Bearbeitung der Abschlussarbeit verwendet werden. Die Verwendung hat stets in der unter § 3 beschriebenen Weise in Abstimmung mit dem KFN zu geschehen.

(3) Es dürfen keine Kopien des oben genannten Datensatzes angefertigt werden. Der Datensatz darf, auch in Auszügen, nicht an dritte Personen weitergegeben werden. Die Daten sind stets für Dritte unzugänglich aufzubewahren. Die Wahrung sämtlicher datenschutzrechtlicher Anforderungen im Umgang mit dem kopierten Datensatz obliegt dem Datennehmer.

§ 3 Einbeziehung des KFN

(1) Um Qualifikationsarbeiten von Beschäftigten/Praktikant*innen des KFN vor Konkurrenzarbeiten zu schützen und Doppelbearbeitungen zu vermeiden, bedarf die Bearbeitung jeder einzelnen Fragestellung der schriftlichen Zustimmung des KFN. Die Datennehmer*in teilt dem KFN daher das konkret in Aussicht genommene Thema per E-Mail mit. Im Anschluss entscheidet das KFN – regelmäßig binnen vier Wochen – über die Erteilung beziehungsweise



Datennutzungsvertrag Universität Bern

UNIVERSITÄT BERN

Vertrag über die Nutzung von Daten
zwischen

der Universität Bern, Vertreten durch Prof. (FH) Dr. habil. Ueli Hostettler

und

Reto Nüesch Erismann (Zürcher Hochschule für Angewandte Wissenschaften),
nachfolgend: „Datennehmer“

§ 1 Einleitung

Der Vertrag regelt die Rechte und Pflichten zwischen der Universität Bern und dem Datennehmer bezüglich der Nutzung von Daten der im Auftrag von Swissmem durchgeführten Studie „Befragung zur Sicherheit in Unternehmen bezüglich digitaler und physischer Angriffe“. Im Rahmen der Studie wurden 271 Firmen aus der MEM-Industrie befragt, die Mitglied bei Swissmem sind. Auf diesen Datensatz beziehen sich die nachfolgenden vertraglichen Regelungen.

§ 2 Vertragsgegenstand

(1) Der Datennehmer erhält eine Kopie des Datensatzes. Er ist berechtigt, im Rahmen seiner Abschlussarbeit „Vergleichende empirische Untersuchung von Schweizer Unternehmen der Logistikbranche in Bezug auf die Cybersecurity“ (Arbeitstitel der Masterarbeit) die Daten zu sichten, Fragestellungen zu entwerfen und diese mit dem Datensatz zu prüfen.

(2) Der zur Verfügung gestellte Datensatz darf nur vom Datennehmer zu dem Zweck der Bearbeitung der Abschlussarbeit verwendet werden. Die Verwendung hat stets in der unter § 3 beschriebenen Weise in Abstimmung mit der Universität Bern zu geschehen.

(3) Es dürfen keine Kopien des oben genannten Datensatzes angefertigt werden. Der Datensatz darf, auch in Auszügen, nicht an dritte Personen weitergegeben werden. Die Daten sind stets für Dritte unzugänglich aufzubewahren. Die Wahrung sämtlicher datenschutzrechtlicher Anforderungen im Umgang mit dem kopierten Datensatz obliegt dem Datennehmer.