Beispielsweise ist absehbar, dass sich mit einer zunehmenden Vernetzung im „Internet der Dinge“ erhebliche Datenschutzherausforderungen ergeben oder dass die „Data Leakage“-Problematik im Rahmen von Globalisierung und Arbeitsteilung in Outsourcing-Verhältnissen deutlich an Gewicht gewinnt.

Die Umsetzung

Während heute viele Unternehmen über eine Geschäftsstrategie verfügen, sieht es bei der IT-Strategie deutlich schlechter aus. Diese liegt nur selten als niedergeschriebenes Dokument vor. Eine IT-Sicherheitsstrategie ist in Unternehmen kaum zu finden, hier ist die öffentliche Hand aufgrund gesetzlicher Vorschriften schon weiter. Doch auch in diesem Bereich geschieht es häufig, dass eine IT-Sicherheitsstrategie zwar auf dem Papier steht, aber in der Praxis nicht umgesetzt wird. Dies liegt meist an unklaren Verantwortlichkeiten oder am fehlenden Budget. Generell sollte eine IT-Sicherheitsstrategie immer mit einer eigenen Jahresplanung mit Budgetierung im Rahmen der unternehmensinternen Planungsprozesse verankert sein.

Zudem ist die Festlegung klarer Verantwortlichkeiten nötig. Hier gilt es, alle Zielgruppen und Akteure einer IT-Sicherheitsstrategie zu berücksichtigen. Dazu gehören IT-Security-Mitarbeiter und IT-Architekten, Mitarbeiter von Fachabteilungen, Vorstand und Geschäftsführung sowie interne und externe Prüfer. Auch Dienstleister wie Lieferanten, Outsourcing-Provider, Forschungsstellen oder Informationsanbieter sowie Kunden sind bei Bedarf in die IT-Sicherheitsstrategie einzubinden. Denn der Sicherheitsansatz ist schließlich so stark wie die schwächste Stelle. Und nur mit klaren Verantwortlichkeiten und Budgets ist die Verbindlichkeit der IT-Sicherheitsstrategie gewährleistet.

Trends und Tendenzen im IT-Markt

Mit einer IT-Sicherheitsstrategie kommen Unternehmen von der Reaktion zur Aktion. Dazu sind Prognosen wichtig, um durch einen Blick in die Zukunft auf Trends und Tendenzen vorbereitet zu sein. Dies wird immer wichtiger, wie verschiedene Entwicklungen zeigen. Eine davon ist die aktuelle Datenexplosion. Bereits 2014 wurden gemäß Fraunhofer-Institut 4,4 Zettabytes an Daten erzeugt, das ist eine 4 mit 21 Nullen. Bis 2020 wird sich diese Anzahl verzehnfachen. Die Datenmenge verdoppelt sich dabei alle zwei Jahre. Im Jahr 2020 werden 32 Milliarden Devices wie Smartphones, Tablets, Sensoren, Steuerungen oder Fahrzeuge meist mobil Daten übertragen. Dabei nimmt die technische und organisatorische Komplexität der Datenflüsse, etwa für Governance und Steuerung, auch durch IT-Outsourcing an externe Cloud-Provider sowie die parallele Verwendung alter und neuer IT-Systeme kontinuierlich zu. Dies führt zu mehr Sicherheitslücken, die zum Beispiel durch DDoS-Attacken ausgenutzt werden. Bereits 2013 gab es gemäß Ponemon Institute 1,4 erfolgreiche Angriffe pro Woche und Unternehmen. Die Kosten betrugen im Schnitt 7,56 Millionen US-Dollar pro Unternehmen und Jahr in Deutschland.

Fehlende Intuition der Mitarbeiter bei Sicherheitsbedrohungen führt zu mangelnder Aufmerksamkeit. So steigt etwa die Gefahr durch Phishing-Mails oder Social Engineering permanent. Die Mitarbeiter verwenden auch zunehmend Social-Media-Angebote wie Facebook, XING oder Twitter sowohl privat als auch am Arbeitsplatz. Dabei nehmen sie die damit verbundenen Risiken kaum wahr, ebenso wenig wie bei der Nutzung ihrer privaten Mobilgeräte am Arbeitsplatz. Selbst wenn firmeneigene Smartphones und Tablets angeschafft werden, erfolgt dies häufig ohne begleitendes Sicherheitskonzept oder Mobile-Device-Management. Dies liegt nicht nur an mangelnder Zeit oder fehlenden Budgets, sondern auch am Fachkräftemangel. Dabei sind Unternehmen heute extrem abhängig von der IT und den entsprechenden Skills.

Neben diesen Gefahren steigen auch die externen Anforderungen an die Unternehmen. Dazu gehören vor allem die zunehmenden Regularien und gesetzlichen Vorschriften, die Einfluss auf die IT-Struktur nehmen. Allen voran zählt hierzu das geplante IT-Sicherheitsgesetz, das für branchenweite Sicherheitsstandards in Unternehmen aus den Bereichen Energiewirtschaft, Informationstechnik, Logistik, Gesundheitswesen, Wasserversorgung, Lebensmittelwirtschaft und Finanzwesen sorgen soll. Dazu gehört auch eine Pflicht zur Meldung von Cyberattacken an das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Mindestanforderungen an das Risikomanagement (MaRisk) stellen die deutschen Kreditinstitute ebenfalls vor immer neue Herausforderungen.

Weitere Anforderungen an die IT-Sicherheit ergeben sich aus der Sourcing-Strategie. So ist beim Outsourcing nicht nur festzulegen, welche Prozesse und Daten an Externe herausgegeben werden dürfen, sondern auch der Querbezug zur eigenen IT-Strategie zu beachten.

Die IT-Sicherheitsstrategie sollte zu diesen Tendenzen und Risiken sowie deren Bedeutung für das Unternehmen und seine Ziele Stellung beziehen und daraus Prioritäten ableiten. Dazu gehört auch die Einordnung von Sicherheitsarchitekturen und -technologien, etwa für Data Loss Prevention (DLP), Identifizierungs- und Authentifizierungsmanagement (IAM) sowie Security Information and Event Management (SIEM), in den Unternehmenskontext.

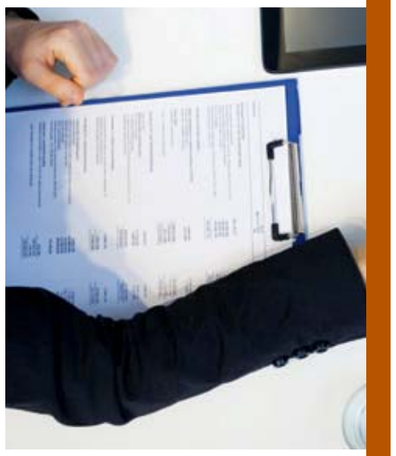
Fazit

Anhand dieser zehn Elemente können Unternehmen eine individuelle und umfassende IT-Sicherheitsstrategie entwickeln. Damit sind sie nicht nur aufgrund der Vollständigkeit des Ansatzes besser geschützt, sondern auch, weil sie Gefahren proaktiv statt reaktiv begegnen. Und wenn sie damit auch nur einen einzigen großen Sicherheitsvorfall vermeiden, hat sich der Aufwand finanziell und durch den gewahrten Ruf mehr als gelohnt. «

Dr. Gerald Spiegel
ist Senior Manager
Information Security Solutions
bei Sopra Steria Consulting.

IT-SICHERHE T: ÖKONO ISCH PLANEN UND BE VERTEN

Heutige Ansätze zur Planung und E tung von IT-Sicherheitsmaßnahmen basieren oftmals auf Methoden der Investitionsrech oder es kommen allgemeine Frameworks zum IT-Service-Management zum Einsatz. Bessere ichkeiten bietet die „Resource-based View“ (RBV).



© Minerva Studio/iStock/Thinkstock/Getty Images

» Cyberangriffe auf Firmen, öffentliche Ein gen und Privatpersonen haben in jüngster Zei isch zugenommen, wie Angaben des Bitkom un un- desministeriums für Bildung und Forschu BF) belegen. Angriffe auf IT-Systeme und ins lere Cyberangriffe können die Betroffenen auf di ten schädigen:

» Im industriellen Umfeld können Unterb gen von Produktionsprozessen zu ökonomis hä- den in Form von Produktivitätseinbußen, ge- nem Gewinn und der Nichteinhaltung vor bar- ten Lieferterminen führen.

» Bei einer Cyberattacke auf den zweitg US- Krankenversicherer Anthem Inc. im Jahr 2 ang Angreifern der Zugriff auf persönliche Da me, Geburtsdatum, Adresse und Sozialvers gs- nummer) von ungefähr 80 Millionen Pers wei Monate später meldete der US-Kranken erer Premera Blue Cross sogar den unautorisie griff auf medizinische Daten von über 11 Millio den. In solchen Fällen greift das US-amerikanis AA-

Gesetz (Health Insurance Portability and Accountability Act), das die Sicherheit von Patienteninformationen regelt und im Fall von Anthem Zivilklagen ermöglicht, da Sozialversicherungsnummern und Geburtstage unverschlüsselt gespeichert wurden.

Unternehmen reagieren auf wachsende Cybergefahren durch hohe Investitionen in technologische, organisatorische und personelle Sicherheitsmaßnahmen. 2014 wuchsen nach Angaben von Gartner die weltweiten Ausgaben für IT-Sicherheit um 7,9 Prozent im Vergleich zum Vorjahr auf 71,1 Milliarden US-Dollar. Damit versuchen Unternehmen nicht nur ökonomischem Schaden vorzubeugen, sondern sie müssen auch rechtliche und regulatorische Vorgaben implementieren (z.B. Sarbanes-Oxley Act und HIPAA im US-amerikanischen Raum, Basel III/Capital Requirements Directive im europäischen Raum).

Unternehmen sehen sich heute vielfältigen technologischen Cybergefahren ausgesetzt, deren Abwehr durch IT-Sicherheitsmaßnahmen im ökonomischen, organisatorischen und rechtlichen Kontext betrachtet und

gemanagt werden muss. Das IT-Sicherheitsmanagement muss dabei sowohl planerische Anforderungen einschließlich des Risikomanagements („Ex ante"-Perspektive) als auch evaluationsbezogene Anforderungen („Ex post"-Perspektive) umsetzen. Diese Anforderungen lassen sich in folgende zentrale Fragen kondensieren:

» Welche Assets einer Organisation bedürfen welchen Schutzes?

» Welche technischen, organisatorischen und personellen Maßnahmen ermöglichen diesen Schutz?

» Welche Investitionssumme sollte mit welcher Maßnahme verbunden werden?

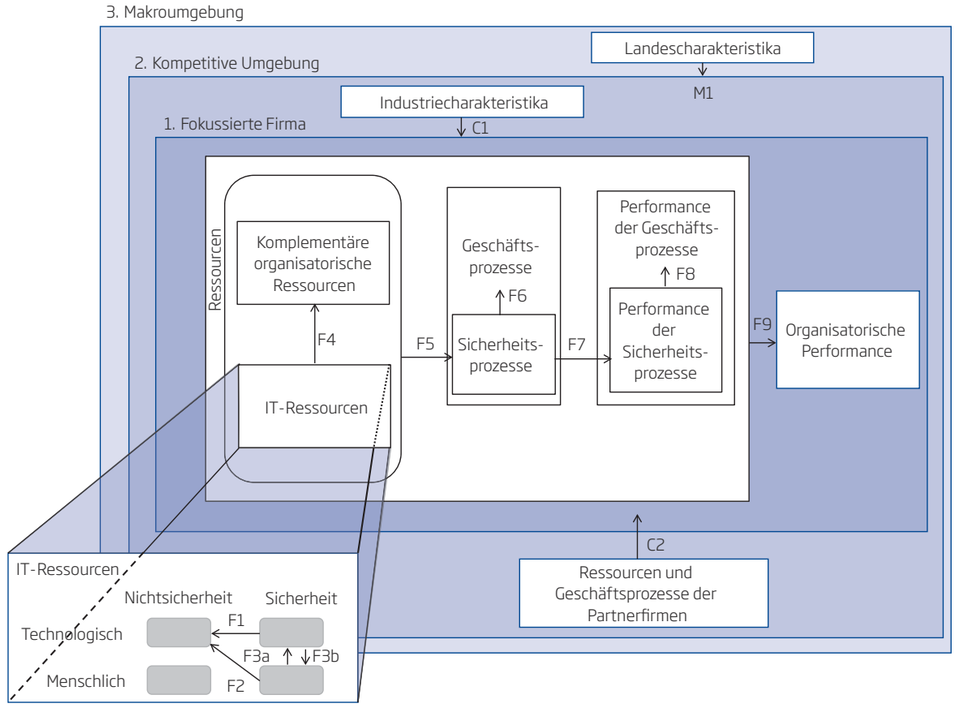
» Inwiefern waren IT-Sicherheitsinvestitionen effektiv und effizient?

Heutige Ansätze zur Planung und Bewertung von IT-Sicherheitsmaßnahmen basieren oftmals auf Methoden der Investitionsrechnung, z.B. Return on Security Investment (ROSI). Darüber hinaus kommen allgemeine Frameworks zum IT-Servicemanagement wie z.B. COBIT und ITIL zum Einsatz. Diese Maßnahmen zur Operationalisierung der Nutzenbewertung von IT-Sicherheitsmaßnahmen sind nur begrenzt geeignet, Unternehmen bei der Beantwortung der obengenannten Fragen zu helfen. Ihre begrenzte Nützlichkeit besteht u.a. darin, dass

» nicht nur die Kosten, sondern auch der Nutzen in Form von vermiedenem Schaden (Opportunitätsleistung) berücksichtigt werden müssen und

» auch nichtquantifizierbarer Nutzen wie zum Beispiel Wettbewerbsvorteile und Reputation beachtet werden müssen.

EINE RESSOURCENBASIERTE PERSPEKTIVE (RBV) AUF IT-SICHERHEITSINVESTITIONEN



Quelle: Weishäupl, E., Yasasin, E. und Schryen, G., (2015), IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review. Proceedings der 23rd European Conference on Information Systems (ECIS), Münster, 26. – 29. Mai 2015

Eine ressourcenbasierte Perspektive auf IT-Sicherheit

Betrachtet man Angriffe auf IT-Systeme eines Unternehmens als Angriffe auf seine Ressourcen, so bietet sich zur Konzeptualisierung von IT-Sicherheit und ihrer unternehmensweiten Auswirkungen die bereits in anderen ökonomischen Kontexten angewendete „Resource-based View" (RBV) an. Ihre Anwendung gestattet es zum einen, angreifbare IT-Ressourcen sowohl im Kontext ihrer Wechselwirkungen mit anderen Ressourcen als auch in ihrer Bedeutung für Unternehmensprozesse und -performance zu betrachten. Zum anderen öffnet sie den Blick nicht nur auf diese unternehmensfokussierte Sicht, sondern auch auf Anforderungen aus der Wettbewerbs- und Makroumgebung, die – wie oben geschildert – Einfluss auf IT-Sicherheit(sinvestitionen) nehmen.

Innerhalb des Unternehmens lassen sich Ressourcen differenzieren in organisatorische Ressourcen und IT-Ressourcen, die sich ihrerseits in zwei Dimensionen und vier Typen untergliedern lassen. Es bestehen vielfache Wechselwirkungen zwischen den Ressourcentypen (Pfeile F1–F3b in der Grafik), beispielsweise können (Investitionen in) IT-Sicherheitsschulungen von Mitarbeitern mit Fokus auf Passwortsicherheit (Wahl eines sicheren Passwortes, regelmäßiges Ändern des Passwortes) Auswirkungen auf den Schutz von CRM- und ERP-Systemen und ihren Daten haben (Pfeil F2).

Des Weiteren können Investitionen in sicherheitsbezogene IT-Ressourcen auch Auswirkungen auf organisatorische Ressourcen haben, so wirkt sich zum Beispiel eine Investition in ein biometrisches Authentifikationssystem, das den Zugang zu einem Firmengebäude kontrolliert, auf die Sicherheit der Büroräume, Akten, Daten und auch der Mitarbeiter aus (Pfeil F4). Diese Investition gestattet Mitarbeitern durch einen Fingerabdruck oder Irisscan einen schnelleren und sicheren Zugang zum Firmengebäude als bei der Verwendung von Schlüsseln, Passwörtern oder Smartcards (Pfeile F5 und F7). Dies erhöht die Effizienz von Geschäftsprozessen, da Mitarbeiter schneller am Arbeitsplatz sind und weniger Unberechtigte einen Zugang zur Firma erhalten (Pfeile F6 und F8).

Die höhere „Performance" der Sicherheitsprozesse lässt sich dabei z.B. mittels der Klassifikationsfehler („false positives" und „false negatives") erfassen, die der Geschäftsprozesse durch Produktivitätsmaße. Eine höhere Performance von Prozessen wirkt letztendlich auch auf eine höhere organisatorische Performance des Unternehmens, zum Beispiel bezüglich Gewinn, Shareholdervalue, Wettbewerbsfähigkeit und Reputation (Pfeil F9).

Anforderungen und Einflüsse auf IT-Sicherheitsinvestitionen bestehen nicht nur aus unternehmensinterner Sicht, sondern können auch aus der Wettbewerbs- und aus der Makroumgebung resultieren. Beispielsweise ergeben sich aus dem Regelwerk Basel III des Baseler Ausschusses für Bankenaufsicht sowie aus den US-amerikanischen Gesetzen Sarbanes-Oxley Act und HIPAA mittelbare und unmittelbare Anforderungen an die IT-Sicherheit(sinvestitionen) von Unternehmen (Pfeile C1 und M1). Auch Kooperationen mit Partnerfirmen können IT-Sicherheitsmaßnahmen beeinflussen, wenn beispielsweise im Rahmen von interorganisationalen Wertschöpfungsketten gemeinsame IT-Ressourcen und Daten genutzt werden und geschützt werden müssen (Pfeil C2).

Operationalisierung der RBV als Herausforderung

Die ressourcenbasierte Perspektive bietet sich sowohl als Entscheidungsgrundlage als auch für die Evaluierung von IT-Sicherheitsmaßnahmen an. Zur Operationalisierung im unternehmerischen Kontext müssen jedoch noch einige Herausforderungen gemeistert werden. Zentrale Fragestellungen sind dabei die folgenden:

» Welche Metriken sind geeignet, um die Auswirkungen von IT-Sicherheitsmaßnahmen zu messen?

» Welche Daten zur Anwendung der Metriken sind erforderlich/verfügbar oder müssen verfügbar gemacht werden?

» Wie können die potenziell unterschiedlichen Sichtweisen mehrerer Stakeholder und organisatorischer Untereinheiten innerhalb eines Unternehmens in die Planung und Bewertung von IT-Sicherheitsmaßnahmen einbezogen werden?

» Wie können Managementprozesse zur Planung und Bewertung von IT-Sicherheitsmaßnahmen etabliert werden, die eine kontinuierliche Verbesserung der IT-Sicherheit gestatten, indem Evaluationsergebnisse bei der (nächsten) Planung berücksichtigt werden?

Zusammenfassend lässt sich festhalten, dass die ressourcenbasierte Perspektive ein integriertes und ganzheitliches Management von IT-Sicherheit(sinvestitionen) gestattet, dessen Operationalisierbarkeit jedoch noch gemeinsamer Forschungsaktivitäten von Wissenschaftlern und Unternehmen bedarf. «

Prof. Dr. Guido Schryen
ist Professor für Wirtschaftsinformatik an der Universität Regensburg und ist Co-Sprecher des Bayerischen Forschungsverbundes „FORSEC – Sicherheit hochgradig vernetzter IT-Systeme".

Eva Weishäupl
ist Wissenschaftliche Mitarbeiterin an der Professur für Wirtschaftsinformatik der Universität Regensburg.