IWI Diskussionsbeiträge
 # Nr. 85 (4. Dezember 2018)[1]

ISSN 1612-3646

Cyber-Risiko – Aktuelle Bedrohungslage und mögliche Lösungsansätze

Levin Rühmann[2], Oliver Werth[3], Nadine Guhr[4]
und **Michael H. Breitner [5]**

[1] Kopien oder eine PDF-Datei sind auf Anfrage erhältlich: Institut für Wirtschaftsinformatik, Leibniz Universität Hannover, Königsworther Platz 1, 30167 Hannover (www.iwi.uni-hannover.de).
[2] Student der Wirtschaftswissenschaften an der Leibniz Universität Hannover
[3] Wissenschaftlicher Mitarbeiter und Doktorand, Institut für Wirtschaftsinformatik, (werth@iwi.uni-hannover.de)
[4] Akademische Rätin, Dr. rer. pol., Institut für Wirtschaftsinformatik (guhr@iwi.uni-hannover.de)
[5] Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre und Direktor des Instituts für Wirtschaftsinformatik (breitner@iwi.uni-hannover.de)

Abstrakt

Cyber-Risiken stellen eine zunehmende Bedrohung und Herausforderung für Staat, Wirtschaft und Gesellschaft dar. Trotz einer steigenden Zahl an cyber-kriminellen Übergriffen werden die erforderlichen Schutzmaßnahmen in vielen Unternehmen bisher jedoch nur unzureichend umgesetzt. Vor diesem Hintergrund ist es das Ziel dieses Diskussionsbeitrages geeignete Lösungsansätze für die Erhöhung der Cyber-Sicherheit zu erarbeiten und zu präsentieren. Auf Basis einer literarischen Auswertung wurde der Versuch unternommen, eine ganzheitliche Cyber-Sicherheitsstrategie auf Unternehmensebene zu entwickeln bzw. wesentliche Phasen und Faktoren im Entwicklungsprozess einer Cyber-Sicherheitsstrategie herauszuarbeiten. In diesem Zusammenhang werden schließlich drei grundlegende Entwicklungsschritte aus der Literatur hergeleitet und ausführlich erläutert sowie einige der wichtigsten Maßnahmen beleuchtet. Dabei stellte sich in einer abschließenden, kritischen Betrachtung heraus, dass eine universelle Cyber-Sicherheitsstrategie unter den vorherrschenden Umständen kaum zu realisieren ist, da jede Organisation in ihren personellen, finanziellen, physischen und organisatorischen Ressourcen, Abläufen und Strukturen ein einzigartiges Konstrukt bildet. Dennoch können die im Rahmen dieses Diskussionspapieres herausgestellten Aspekte als Orientierungsrahmen und Handlungsempfehlung für die Entwicklung und Umsetzung einer Cyber-Sicherheitsstrategie herangezogen werden.

Schlagwörter: Cyber-Sicherheit, Cyber-Risiko, Strategie, Maßnahmen, Handlungsempfehlungen

1. Einleitung

Die Informations-und Kommunikationstechnologie (IuK-Technologie) hat in den letzten Jahren in zunehmendem Maße sämtliche Lebens-und Arbeitsbereiche durchdrungen und im Rahmen der Digitalisierung zu einem grundlegenden Wandel im staatlichen, wirtschaftlichen und gesellschaftlichen Bereich beigetragen. Sichere und leistungsfähige Informations-und Kommunikationssysteme sind zum Rückgrat der Gesellschaft und Wirtschaft herangewachsen. Insbesondere das Internet hat sich in diesem Zusammenhang zu einem wesentlichen Treiber in diesem Prozess der Digitalisierung herausgebildet und den Weg für viele neue Geschäftsmodelle geebnet, sich als Basis für die internationale Wertschöpfung etabliert sowie allgemein einen wichtigen Beitrag zur Veränderung und Beschleunigung der Geschäftsprozesse geleistet[1].Neben den zahlreichen Chancen und Errungenschaften der informations-und kommunikationstechnischen Entwicklungen der letzten Jahre, die den Begriff der Digitalisierung geformt und die Gesellschaft und Wirtschaft geprägt haben, bergen die Veränderungen und Fortschritte auch eine Vielzahl an Risiken. So zeigt sich derzeit inter-national eine steigende Aktivität krimineller Akteure gegen die IuK-Technologie von Wirtschaftsunternehmen oder staatlichen Einrichtungen. Beispiele, wie der Cyber-An-griff auf das deutsche Außenministerium und andere Bundesbehörden, verdeutlichen diesen Trend und unterstreichen zugleich das enorme Schadenspotential. Die Täter agieren dabei grundsätzlich anonym im Verborgenen und nutzen nahezu jede Schwachstelle, die sich ihnen bietet. Während das Entdeckungsrisiko für die Angreifer äußerst gering ist, sind die Gefahren für Wirtschafts-und Finanzunternehmen sowie für staatliche Einrichtungen, aber auch für die Bürger, äußerst groß und allgegenwärtig[2] [3].
Die unternehmensinternen Informations-und Kommunikationssysteme sind somit zu einem Schlüsselfaktor herangewachsen, den es mit sämtlichen, zur Verfügung stehenden Mitteln zu schützen gilt. Für alle betroffenen Parteien sollte es daher oberste Priorität haben, sowohl auf technischer als auch auf organisatorischer Ebene entsprechende Maßnahmen zu ergreifen, um eine zuverlässige Funktionsweise zu gewährleisten und sich gegen derartige Risiken zu schützen. In diesem Zusammenhang sind Unternehmen und staatliche Einrichtungen dazu aufgefordert, umfangreiche Sicherheitsstrategien zu entwerfen, um ihre Prozesse, Systeme, Daten und Informationen vor dem unbefugten Zugriff durch Dritte zu schützen. Vor dem Hintergrund einer immer komplexer und dynamischer werdenden Umwelt und einer zunehmenden Vernetzung der Informationssysteme ist dies eine große Herausforderung für alle Beteiligten. Die Auseinandersetzung mit den neuen Gefahren und die Schaffung nachhaltiger und sicherer Lösungen ist jedoch unabdingbar, zumal die informationsverarbeiten-den Systeme und Prozesse heutzutage einen grundlegenden Faktor in Hinblick auf die Sicherstellung des allgemeinen Geschäftsbetriebs und die Erreichung der Geschäfts-ziele darstellen[4]. Wie bereits angesprochen, stellen die Digitalisierung und der Fortschritt in der IuK-Technologie den

[1] BMI (2016), S. 4; Fraunhofer (2014), S. 9; Ziercke, J. (2016), S. 230
[2] Aus Gründen der Lesbarkeit, wird im gesamten Diskussionspapier die männliche Form stellvertretend für Personen beiderlei Geschlechts verwendet.
[3] Ziercke, J. (2016), S. 230-231; Sauerbrey, A. et al. (2018)
[4] Bartsch, M. / Frey, S. (2017), S. 10-11; BSI (2016b), S. 69; BSI (2014a), S. 7

Staat, die Wirtschaft und die Gesellschaft vor eine zunehmend größer werdende Herausforderung. Vor allem Unternehmen sehen sich immer stärker durch verschiedene, ihre Systeme und Daten bedrohende Gefahren konfrontiert. Lange Zeit haben wirtschaftliche und staatliche Akteure die Sicherheit ihrer Informationssysteme und damit die Sicherheit sensibler Daten und Informationen lediglich als nachrangiges Ziel betrachtet und diese folglich leichtfertig aufs Spiel gesetzt[5].

Die Aktualität und Brisanz rund um das Thema Cyber-Risiken ist enorm und macht es zu einem der meist diskutierten Bereiche der heutigen Zeit. Wie sich gezeigt hat, ist die Bedrohungslage besonders vor dem Hintergrund des Digitalisierungsprozesses und einer sich stetig verändernden technischen Umwelt von einer zunehmenden Komplexität und Professionalität geprägt. Insbesondere der starke Anstieg der zu speichernden und zu verarbeitenden Daten, die sich im Zusammenhang der Digitalisierung und globalen Vernetzung ergeben, veranschaulicht das große Risikopotential für Wirtschaft und Gesellschaft. So ist davon auszugehen, dass es bis zum Jahr 2020 zu einer Verfünffachung des Datenvolumens gegenüber dem Jahr 2015 kommen wird. Der Schutz der sensiblen Unternehmensdaten vor cyber-kriminellen Aktivitäten, wie Spionage, Sabotage oder Manipulation, wird damit einhergehend ein weiterhin ernstzunehmender Faktor sein, um auf lange Sicht die Existenz eines Unternehmens zu sichern[6].

Vor diesem Hintergrund und einer sich ständig verändernden technischen und organisatorischen Umwelt wie auch den sich daraus ergebenden internen und externen Problemstellungen ist es das Ziel dieses Diskussionspapieres, Lösungsansätze zu erarbeiten und Handlungsempfehlungen vorzustellen, welche im Kontext einer ganzheitlichen Cyber-Sicherheitsstrategie auf Unternehmensebene implementiert und, den individuellen Strukturen, Ressourcen und Abläufen entsprechend, zum Schutz der internen IT-Infrastrukturen, Daten und Informationen umgesetzt werden können. Aus dieser übergeordneten Zielsetzung kann schließlich die allgemeine Forschungsfrage hergeleitete werden:

„Warum sollten sich Unternehmen mit der Entwicklung geeigneter Strategien im Bereich der Cyber-Sicherheit auseinandersetzen und wie könnten entsprechende Schritte in diesem Prozess aussehen?"

Für ein fundiertes Verständnis der Zusammenhänge wird zu Beginn dieses Diskussionspapieres zunächst eine Einführung in die Thematik gegeben. Dazu zählt, neben der Definition und Abgrenzung des Cyber-Begriffs, vor allem ein Überblick über aktuelle Cyber-Risiken, ihr Bedrohungspotential und die dahinterstehenden Täter und Motive. Ausgewählte Studien geben darüber hinaus einen Einblick in die Reichweite und Relevanz der Thematik. Im Anschluss wird dann Bezug zur Cyber-Sicherheit genommen und hier die wichtigsten Aspekte beleuchtet. Im Mittelpunkt dieses Abschnitts steht eine eingehende Betrachtung der staatlichen Bemühungen hinsichtlich der Gewährleistung von Cyber-Sicherheit. Neben gesetzlichen Rahmenbedingungen wird an dieser Stelle auch auf weitere Initiativen, insbesondere unter der Schirmherrschaft des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), eingegangen. Daran anknüpfend wird im dritten Kapitel der Blick auf die

[5] BSI (2014b), S. 8; Fraunhofer (2014), S. 11

[6] Hungerland, F. et al. (2016), S. 15-16

Konzeptionierung einer Cyber-Sicherheitsstrategie gelenkt. Nach einer anfänglichen Definition des Strategiebegriffs wird sich dann mit der Herleitung und der anschließenden Erläuterung der wichtigsten Schritte im Strategieentwicklungsprozess beschäftigt. Im weiteren Verlauf werden einige der wichtigsten präventiven, reaktiven und stabilisierenden Maßnahmen in Bezug auf die Erhöhung der Cyber-Sicherheit vorgestellt. Es folgt schließlich eine kritische Betrachtung der herausgearbeiteten Aspekte, ehe ein kurzes Fazit dieses Diskussionspapieres abschließt.

2. Theoretischer Hintergrund

2.1. Cyber-Risiko

Cyber-Risiko ist in der Literatur ein häufig diskutierter, bisher jedoch nicht einheitlich definierter Begriff. Oft werden unter dieser Kategorie Risiken zusammengefasst, die mit der Nutzung des Internets einhergehen[7]. Im Rahmen einer in den letzten Jahren zunehmenden Bedeutung dieser Risikoklasse, ist eine derart eng gefasste Definition jedoch nicht mehr zeitgemäß. Andere Ansätze, wie die von Mukhopadhyay et al. (2005, 2013), sind in ihrer Ausführung ebenfalls zu begrenzt. So definieren diese Autoren Cyber-Risiken als bösartige elektronische Vorfälle, deren Eintreten zu einer Unterbrechung des unternehmerischen Geschäftsbetriebes führen und folglich finanzielle Einbußen verursachen kann[8]. In der Literatur lassen sich jedoch auch weitere Ansätze und Bemühungen hinsichtlich einer Definition finden, die eine weiter gefasste Perspektive einnehmen. Dazu zählen bspw. Böhme und Katarina (2006), welche Cyber-Risiken als zentrale Bedrohung für die Sicherheit von Informationssystemen beschreiben und in diesem Zusammenhang auch auf das daraus resultierende Schadensausmaß aufmerksam machen[9]. Eine abschließende Definition erweist sich vor dem Hintergrund zahlreicher Ansätze als Herausforderung. Nach Auswertung und Begutachtung zahlreicher Definitionsbemühungen soll sich in diesem Diskussionspapier vor allem auf den Ansatz von Refsdal et al. (2015) und Aussagen des BSI bezogen werden. Demnach beschreibt der Begriff eine Vielzahl möglicher Risikoszenarien, die sich in Hinblick auf den Cyber-Raum, d.h. mit dem Internet oder ähnlichen Netzen in Verbindung stehende Informationstechnik, ergeben. Dies umfasst letztlich auch die darauf fußende Kommunikation, Anwendungen und Prozesse sowie dort verarbeitete und gespeicherte Daten und Information[10]. Als zentrale Bedrohungsformen im Bereich des Cyber-Risikos können exemplarisch Malware [11] (Viren, Würmer Trojaner, Ransomsoftware), Distributed-Denial-of-Service (DDoS) [12] und Botnetze [13], Social

[7] ISO (2012), S. 4 und 10
[8] Mukhopadhyay, A. et al. (2013), S. 1;Mukhopadhyay, A. et al. (2005), S. 156
[9] Böhme, R. / Kataria, G. (2006), S. 3
[10] Refsdal, A. et al. (2015), S. 29 und 33;BSI (2018c)
[11] BSI (2017), S. 22
[12] Yu, S. (2014), S. 1-2
[13] Yu, S. (2014), S. 3-4; Gu, G. et al. (2008), S. 139

Engeneering [14], und Man-in-the-Middle-Angriffe [15] genannt werden, welche es zu berücksichtigen gilt.

2.2. Cyber-Sicherheit

Der Begriff Cyber-Sicherheit bzw. Cyber-Security wird oft als Synonym für IT-Sicherheit oder Informationssicherheit gebraucht. Während sich im Fachjargon mehr und mehr der Begriff Informationssicherheit anstelle des ursprünglich genutzten Begriffs IT-Sicherheit verfestigt, tritt in der Gesellschaft und Politik nun zunehmend der in der Vergangenheit eher selten gebrauchte Begriff Cyber-Sicherheit in den Vordergrund. Sicherheit beschreibt grundsätzlich eine Ausgangssituation ohne jegliche Gefahr, sodass die Begriffe Cyber-, IT-und Informationssicherheit als völlig gefahrenlose Zustände im Cyber-Raum, der IT oder der Informationen zu betrachten sind [16]. Informationssicherheit ist in diesem Zusammenhang generell breiter gefasst als der Begriff IT-Sicherheit, welcher sich auf die Sicherheit und Verfügbarkeit der IT an sich beschränkt. Im Wesentlichen ist die IT-Sicherheit ein Teil der Informationssicherheit, welche nicht nur die technologische Komponente, sondern auch die nicht-technologische Form von Informationen umfasst und die Sicherheit und Verfügbarkeit der Informationen an sich in den Mittelpunkt stellt. Die Informationssicherheit zielt somit darauf ab, neben den Informationen an sich, auch Systeme und Prozesse zu schützen, welche mit der Speicherung, Verarbeitung oder Bereitstellung dieser Informationen beauftragt sind[17] [18]. Es besteht darüber hinaus eine Schnittmenge zwischen den Begriffen Cyber-Risiko, IT-Risiko und Informationssicherheitsrisiko, sodass schließlich auch die Informationssicherheit und folglich die IT-Sicherheit als eine Untereinheit der Cyber-Sicherheit betrachtet werden können.
Im Kontext des Risikomanagementprozesses wird unter Cyber-Sicherheit jede Art von Maßnahme verstanden, die zur Minimierung der Cyber-Risiken und letztlich zum Schutz der mit dem Cyber-Raum in Verbindung stehenden bzw. darauf basierenden Risikoobjekte beiträgt. Diese Cyber-Risikoobjekte umfassen unter anderem entsprechende Informationsinfrastrukturen, Personen und Nutzer, Geschäftsprozesse, Anwendungen, Dienste und Telekommunikationssysteme sowie die hier verarbeiteten, gespeicherten und übermittelten Daten und Informationen. Die Maßnahmen zum Schutz dieser digitalen Umgebung und der Risikoobjekte sind vielfältig. Ihre Gesamtheit setzt sich aus verschiedenen Strategien, Leitlinien, Schulungen, Sicherheitskonzepten, Risikomanagementverfahren, Technologien und Sicherheitsmechanismen zusammen[19]. Es zeigt sich, dass sich der Begriff Cyber-Sicherheit vor allem auf die Sicherheit im Cyber-Raum, d.h. auf jede Form einer internetbasierten oder auf ähnlichen Netzwerken fußenden IuK-Technologie sowie entsprechende Anwendungen und Prozesse bzw. dort verarbeitete Informationen und Daten, bezieht. Im Mittelpunkt

[14] Mouton, F. et al. (2014), S. 269; Dreo Rodosek, G. / Golling, M. (2013), S. 188-189; Wiedemer, A. / Hochenrieder, M. (2015), S. 685
[15] Dreo Rodosek, G. / Golling, M. (2013), S. 188; Callegati, F. et al. (2009), S. 78-79; BSI (2016b), S. 1254
[16] Klipper, S. (2015a), S. 10
[17] Königs, H.-P. (2017), S. 161-162
[18] In diesem Diskussionspapier werden die Begriffe IT-Sicherheit und Informationssicherheit synonym verwendet
[19] Königs, H.-P. (2017), S. 408; Hochkommissariat für nationale Sicherheit (2016)

steht daher der Schutz in einer digitalen Umgebung bzw. die Sicherheit bei der Speicherung, Verarbeitung und Bereitstellung von digitalen Daten und Informationen. Allerdings betrifft Cyber-Sicherheit nicht ausschließlich den Cyber-Raum, sondern umfasst zusätzlich auch Aspekte in Hinblick auf die Gewährleistung der allgemeinen Sicherheit in der IuK-Technologie[20]. In diesem Zusammenhang kommt der Erreichung und Bewahrung bestimmter Schutzziele eine besondere Bedeutung zu. Ein weiterer wichtiger, bereits angesprochener Faktor ist zudem, dass in der heutigen Zeit der Großteil der Daten und Informationen nicht mehr physisch, sondern digital gespeichert und verarbeitet wird, sodass eine synonyme Verwendung der Begriffe Informationssicherheit und Cyber-Sicherheit durchaus zulässig ist und auch im Rahmen dieses Diskussionspapieres vorgenommen wird.
Eine besondere Bedeutung in Bezug auf die Cyber-bzw. Informationssicherheit kommt den sogenannten Schutzzielen oder Grundwerten zu. Dabei handelt es sich um die bereits in der „herkömmlichen" IT-Sicherheit verfolgten Systemziele Vertraulichkeit, Verfügbarkeit und Integrität. Die Gewährleistung dieser Ziele wird insbesondere durch die Verschmelzung der digitalen und physischen Umgebung zu einer immer komplexer werdenden Aufgabe.

3. Konzeptionierung einer Cyber-Sicherheitsstrategie

3.1. Entwicklungsprozess einer Cyber-Sicherheitsstrategie

Trotz eines Bedeutungsgewinns im Rahmen einer zunehmenden politischen, wirtschaftlichen und gesellschaftlichen Diskussion lassen sich weiterhin viele Unternehmen, speziell im klein-und mittelständischen Bereich, Zeit, entsprechende Bemühungen und Maßnahmen voranzutreiben und eine ganzheitlich Cyber-Sicherheitsarchitektur zu etablieren. Vor diesem Hintergrund soll sich im Folgenden explizit mit der Entwicklung einer, die strategischen Unternehmensziele berücksichtigenden, Cyber-Sicherheitsstrategie, als eine Teilstrategie der maßgeblichen Unternehmensstrategie, beschäftigt werden[21]. Im Kontext der Cyber-Sicherheitsstrategie, die einen Teil der übergeordneten Unternehmensstrategie darstellt und somit auch von diesbezüglichen strategischen Entscheidungen tangiert wird, sehen sich Verantwortliche mit der Bewältigung verschiedener Anforderungen in unterschiedlichen Bereichen konfrontiert. Der Konzeptionierungsprozess einer Cyber-Sicherheitsstrategie ist eine komplexe Aufgabe, bei der idealerweise drei grundlegende und ineinander-greifende Stufen durchlaufen werden (siehe Abbildung 1). Am Anfang steht im Normalfall die Analyse der unternehmerischen Ausgangslage und der damit zusammenhängenden externen und internen Umwelt. Unmittelbar darauf folgt die Festlegung der strategischen Cyber-Ziele, ehe auf Basis der gewonnenen Erkenntnisse und festgelegten Ziele unter anderem die Zuweisung von Verantwortlichkeiten und die Definition von Handlungsfeldern und Meilensteinen stattfindet. Im letzten Schritt sollte die Erstellung eines detaillierten Umsetzungsplans für die Maßnahmen und Vorhaben zur Erhöhung der Cyber-Sicherheit erfolgen. Bei dem gesamten Strategieentwicklungsprozess sowie der anschließenden Durchführung der ausführlich geplanten Maßnahmen sind darüber hinaus unterstützende Monitoring-Strukturen zu schaffen, die eine umfassende

[20] BSI (2018c)
[21] Bartsch, M. / Frey, S. (2017), S. 75-76

Überprüfung und Kontrolle ermöglichen und bei der Identifikation von Abweichungen entsprechende Rückmeldungen geben. Auf diese Weise kann bspw. ein Ab-gleich von bereits durchgeführten Maßnahmen mit vorgegebenen Zielen sichergestellt und im Bedarfsfall eine Korrektur eingeleitet werden[22][23].

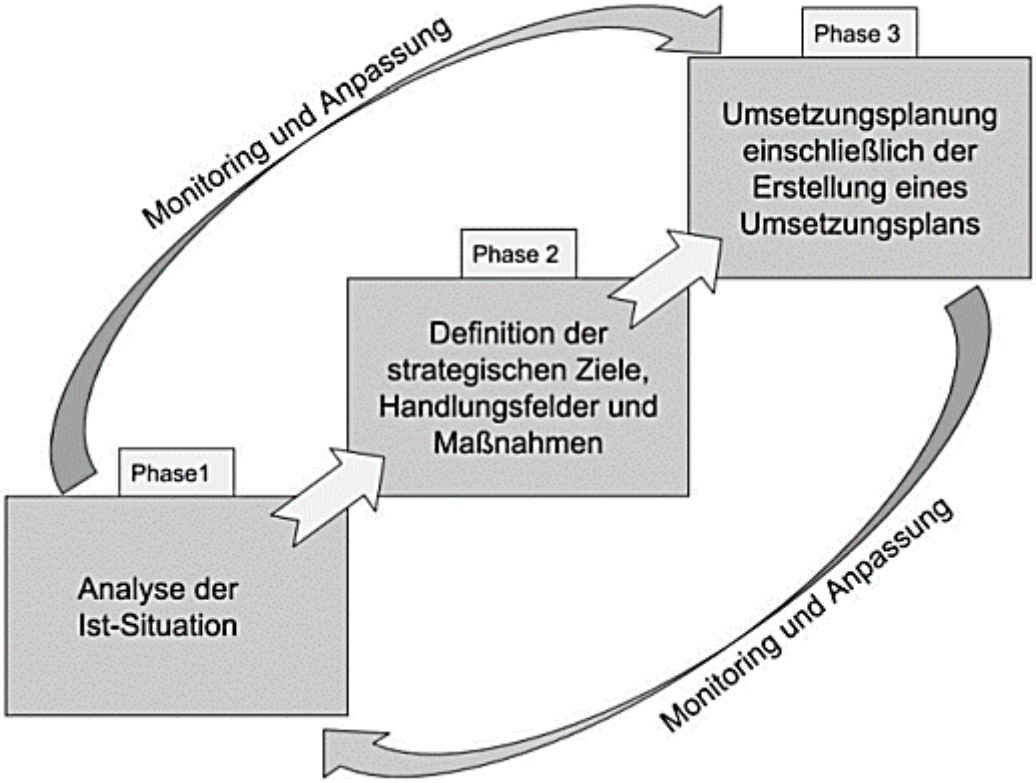

Abbildung 1: Wichtige Entwicklungsphasen einer Cyber-Sicherheitsstrategie (in Anlehnung an Bartsch, M. / Frey, S. (2017), S. 77)

Um eine erfolgreiche unternehmensweite Cyber-Sicherheitsstrategie zu etablieren, ist es, wie bereits erläutert, im ersten Schritt notwendig, die eigene Ausganglage in Hinblick auf verschiedene, die Cyber-Sicherheit betreffende Aspekte zu analysieren und zu bewerten. Es geht um ähnliche Abschätzungen und Fragestellungen, wie sie bereits auf Gesamtunternehmensebene gestellt wurden. Im Mittelpunkt stehen die Gegenüber-stellung der Stärken, Schwächen, Risiken und Chancen sowie der Erkenntnisgewinn in Bezug auf die eigene Verwundbarkeit, die Herausforderungen im Unternehmens-umfeld und die internen Fähigkeiten und Ressourcen. In diesem, häufig unter dem Oberbegriff Risiko-Assessment zusammengefassten Prozess geht es in erster Linie um den Durchlauf der drei grundlegenden Phasen Risikoidentifikation, Risikoanalyse und Risikobewertung bzw. Risikopriorisierung. Der erste wichtige Schritt bei der Analyse der Ist-Situation ist die Risikoidentifikation. Dabei spielt nicht nur die Identifikation der Risiken eine Rolle, sondern eine Vielzahl weiterer, für die Entwicklung der Cyber-Sicherheitsstrategie bedeutender Aspekte. So ist an erster Stelle zu klären,

[22] Bartsch, M. / Frey, S. (2017), S. 49-50 und 75-76
[23] Eine eingehendere Betrachtung der einzelnen Stufen im Entwicklungsprozess einer Cyber-Sicherheitsstrategie erfolgt im weiteren Verlauf dieses Diskussionspapieres

welche Objekte oder Assets grundsätzlich zu schützen sind und mit welchen Anforderungen dies verbunden ist. Eine entsprechende Liste sollte idealerweise umfassende Informationen zu den ermittelten Assets bereitstellen. Dazu zählt, neben der Auflistung aller identifizierten Risikoobjekte, die im Rahmen des Risikomanagements überprüft und gesteuert werden sollen, vor allem die Zuordnung der damit verbundenen Zuständigkeiten. An dieser Stelle sollte sich die Frage gestellt werden, welche Systeme, Informationen und Einrichtungen besonders gefährdet sind und bei einer konkreten Cyber-Attacke Schaden nehmen können. Des Weiteren sollten bei der Risikoidentifikation die Abhängigkeiten zwischen den Assets herausgestellt werden. Hier stehen Fragestellungen im Mittelpunkt, welche die Zusammenfassung einzelner Risikoobjekte zu größeren Assets und insbesondere auch die Unterscheidung zwischen primären und unterstützenden Assets betreffen[24]. Als primäre Assets gelten alle Geschäftsprozesse, die notwendig sind, um die Unternehmensziele zu erreichen, gesetzliche und vertragliche Vorgaben einzuhalten sowie jene Vorgänge, die sensible, geheime Prozesse oder Teilprozesse beinhalten. Aber auch Informationen, die einen unabdingbaren Beitrag zur Erreichung unternehmerischer Ziele leisten, datenschutzrechtliche Relevanz haben, einen strategischen Wert aufweisen oder bei ihrer Beschaffung, Verarbeitung und Speicherung mit hohen Kosten verbunden sind, gehören zu der Kategorie der primären Assets.
Nachdem sich im Zuge der Risikoidentifikation ein Überblick über die zentralen Assets, Bedrohungen, Maßnahmen, Schwachstellen und Schadensfolgen verschafft wurde, geht es auf der nächsten Stufe, der Risikoanalyse, zuvorderst um das tiefere Verständnis und die Schätzung von Wahrscheinlichkeiten in Hinblick auf Bedrohungen, mit denen sich ein Unternehmen tatsächlich konfrontiert sieht. Unterschieden wird in erster Linie zwischen qualitativen und quantitativen Methoden. Bei qualitativen Techniken wird auf konkrete Zahlenwerte verzichtet und der Schaden bzw. die Häufigkeit stattdessen mithilfe von Ordnungsbegriffen in geeigneten Skalensystemen dargestellt. Gängige Ordnungsbegriffe sind bspw. „gering", „mittel" und „hoch". Die Anwendung dieser Methode eignet sich besonders bei neuartigen Risiken. Sie kann allerdings auch dann erfolgen, wenn die Ermittlung konkreter Zahlen nicht gewährleistet wird bzw. mit zu großem Aufwand oder zu hohen Kosten verbunden ist. Die quantitativen Analysemethoden hingegen stützen sich auf konkrete Zahlen (z. B. Kosten in Euro) und Wahrscheinlichkeiten. Unsicherheit entsteht vor allem aufgrund dessen, dass es meist aus der Vergangenheit stammende Werte sind, welche die Entscheidungsgrundlage bilden. Die Unsicherheit über zukünftige Ereignisse sollte schließlich auch in der Analyse Berücksichtigung finden[25]. Den letzten Schritt der Risikoanalyse bildet die Erstellung eines Risiko-Levels für jedes Bedrohungsszenario. Als Basis dienen die zuvor vorgenommenen Einschätzungen hinsichtlich der Auswirkungen und Wahrscheinlichkeiten. Um für jedes Bedrohungsszenario einen Vektor zu erhalten, der im Folgenden zur Bewertung und Priorisierung der Risiken herangezogen werden kann, werden meist komplexe Verfahren eingesetzt, bei denen die generierten Größen kombiniert und in einen Zusammenhang gesetzt werden. Das abschließende Ergebnis der Risikoanalyse sollte somit optimaler Weise eine Liste sein, die eine ausführliche Einschätzung und Klassifizierung der aktuellen Bedrohungsszenarien beinhaltet[26]. In

[24] Königs, H.-P. (2017), S. 413; Klipper, S. (2015b), S. 66-68
[25] Königs, H.-P. (2017), S. 56-57; Klipper, S. (2015b), S. 34 und 72-73
[26] Klipper, S. (2015b), S. 72-74

der letzten Phase geht es schlussendlich um die Risikobewertung und -priorisierung. In erster Linie sollte hier aus Sicht des Unternehmens eine Abwägung und Entscheidung über die Wichtigkeit bzw. Gefahr der identifizierten Risiken stattfinden. Dabei sind die Risiken nicht mehr isoliert zu betrachten, sondern vielmehr mit dem übergeordneten Kontext der Organisation zu verknüpfen. In diesem Zusammenhang ist es notwendig, dass die Bedrohungsszenarien in Bezug zu den individuellen unternehmerischen Basiskriterien gesetzt und daraufhin mittels einer Skala bewertet werden. Die Bewertung des Problems ist primär von der Beziehung zu übergeordneten Zielen und dem Einfluss auf das Prozessergebnis abhängig. Des Weiteren spielt die Dringlichkeit der Problembeseitigung bzw. die zeitliche Komponente eine wichtige Rolle. Nur durch diesen Vergleichsprozess ist es möglich, eine abschließende Einschätzung bzgl. der Bedeutung für das Unternehmen zu erreichen und eine Rangfolge zu erstellen, die letztlich den Ausgangspunkt für weiterführende Schritte und die abschließende Behandlung der Risiken darstellt[27]. Um im Rahmen der Risikoidentifikation, -analyse und -bewertung den Ist-Zustand der unternehmerischen Cyber-Sicherheit zu ermitteln, Schwachstellen aufzuspüren und daraus Optimierungspotentiale abzuleiten, kann auf eine Vielzahl verschiedener Instrumente zurückgegriffen werden. Speziell Checklisten sind ein gutes Mittel in Bezug auf die Identifikation von Sicherheitslücken und Missständen. Hierbei können über die strukturierte Abfrage sicherheitsrelevanter Themen, Schwachstellen schnell und effizient identifiziert werden. Vorgaben und Muster für derartige Checklisten lassen sich unter anderem in den ISO-Standards und den Grundschutzkatalogen des BSI finden[28]. Um im weiteren Verlauf die konkreten Maßnahmen und ihre Umsetzung zur Behebung vorhandener Sicherheitslücken zu planen und zu initiieren, sollte sich, ausgehend von den Ergebnissen des bereits durchgeführten Risiko-Assessments, im nächsten Schritt zunächst mit der Definition unternehmensspezifischer, strategischer Ziele beschäftigt werden. Hierbei handelt es sich um messbare, langfristig angestrebte Zustände, die einer Organisation einen klaren Orientierungsrahmen für die Zukunft bieten, dabei jedoch idealerweise einen gewissen Grad an Flexibilität, insbesondere hinsichtlich möglicher Maßnahmen zur Erreichung eines Ziels, zulassen. Ein allgemeines Beispiel für ein strategisches Ziel im Bereich Cyber-Sicherheit kann unter anderem die Optimierung der Sicherheitsarchitektur zur Vermeidung von Cyber-Angriffen sein. Neben der Schaffung eines geeigneten Rahmens zur Orientierung und Kontrolle tragen strategische Ziele auch zu einer stärkeren Identifikation und Motivation seitens der Beteiligten bei. Um ein klares Verständnis bei den Mitarbeitern zu erzielen, ist es daher notwendig, dass die Ziele einfach, aber dennoch detailliert formuliert werden. Des Weiteren sollte der Fokus auf ein bestimmtes bzw. nur wenige strategische Ziele gelegt werden, um einen richtungsweisenden Fokus zu ermöglichen. Aus übergeordneter Unternehmenssicht ist die Formulierung derartiger Ziele ein adäquates Mittel zur Setzung langfristiger Prioritäten. Es geht primär um den Einsatz von finanziellen Mitteln und zeitlichen Ressourcen sowie um die Frage, ob diesbezüglich eine externe Unterstützung in Anspruch genommen werden sollte. Im besten Fall sollten strategische Ziele dauerhaft stabil und unabhängig sein. Dennoch sind sie nicht als statisch zu betrachten, da sie im Zuge der Veränderung der Unternehmensumwelt und der allgemeinen Rahmenbedingungen auch Anpassungen und Modifizierungen unterzogen

[27] Kersten, H. et al. (2013), S. 31-32; Klipper, S. (2015b), S. 75; Wolf, E. et al. (2013), S. 211-212
[28] Wolf, E. et al. (2013), S. 211-212; Klipper, S. (2015b), S. 118

werden können. Dieser Anpassungsfähigkeit sind jedoch gewisse Grenzen geboten. So ist die Reduzierung der Risiken bzw. die Stärkung der Sicherheit bei einer falschen Zieldefinition im Rahmen einer Cyber-Strategie nur schwer zu erreichen[29].
Im Anschluss an die ausführliche und erfolgreiche Identifikation, Analyse und Bewertung der unternehmenseigenen Cyber-Sicherheitsarchitektur und der daran anknüpfenden Festlegung strategischer Ziele, kann im nächsten Schritt mit der sogenannten Risiko-Behandlung bzw. Risiko-Steuerung begonnen werden. Dazu zählt zuvorderst die Entscheidung über mögliche Behandlungsoptionen und die Definition, Konzeption und Planung von sicherheitsrelevanten, die definierten Anforderungen erfüllenden Maßnahmen für jedes Einzelrisiko. Die Grundvoraussetzung, um die Risikolage des Unternehmens erfolgreich zu verbessern, ist vor allem, dass nicht nur eine vorübergehende Kompensation der Cyber-Sicherheitsrisiken angestrebt wird, sondern die Ri-siko-Behandlung nachhaltig und unter Berücksichtigung der übergeordneten Unternehmensziele erfolgt[30]. Bei der unmittelbaren Behandlung wird grundsätzlich zwischen den folgenden vier Handlungsmöglichkeiten bzw. Risikostrategien unterschieden. Dies sind die Risikovermeidung, die Risikoreduktion, der Risikotransfer und die Risikoakzeptanz. Die Entscheidung, ob ein Risiko vermieden, reduziert, akzeptiert oder transferiert bzw. geteilt wird, sollte auf Basis der Ergebnisse des Risiko-Assessments vorgenommen und für jedes Risiko individuell getroffen werden. Besonders wichtig bei der Auswahl einer Risikostrategie und der damit einhergehenden Aktivitäten und Vorgänge ist die Berücksichtigung der Wirksamkeit und des Kosten-Nutzen-Verhältnisses, wobei unter Umständen auch ökonomisch nicht begründbare Entscheidungen notwendig sein können. Im Idealfall sollen die Behandlungsmöglichkeiten die Risiken nachweislich mindern, vermeiden oder bei der Inanspruchnahme einer Versicherung vom Unternehmen fernhalten. Eine Gewährleistung von absoluter Sicherheit ist in diesem Zusammenhang jedoch nicht möglich. Risiken aufgrund mangelnder Ressourcen oder einer zu geringen Sachkenntnis gänzlich zu ignorieren, ist ebenfalls keine nachhaltige Option. Darüber hinaus sollten die vier möglichen Risikostrategien und die daraus hervorgehenden Behandlungsansätze nicht zwangsweise isoliert betrachtet und umgesetzt werden, sondern vielmehr im Rahmen einer gezielten Kombination Anwendung finden, um eventuell einen stärkeren Beitrag zur Risikobehandlung leisten zu können. Eine bereichsübergreifende Betrachtung ist vor allem deswegen sinnvoll, da sich der Wirkungsraum einzelner Optionen oder Maßnahmen in vielen Fällen nicht nur auf das ursprünglich zu bewältigende Risiko beschränkt. So ist es bspw. möglich, dass eine Aktion auf die Reduzierung eines bestimmten Risikos abzielt, gleichzeigt aber ein weiteres Bedrohungspotenzial unvorhergesehen vermindert und daher unter Umständen weitergehende, ursprünglich in diesem Bereich geplante Maßnahmen hinfällig werden lässt. Auf diese Weise lässt sich ggf. auch das Kosten-Nutzen Verhältnis positiv beeinflussen. Um die Übersicht bzgl. dieser Wechselwirkungen zu wahren und einzelne Risiken nicht in Vergessenheit geraten zu lassen, ist eine umfassende Dokumentation der Risikoobjekte und der dazugehörigen Maßnahmen von Nöten[31]. Grundsätzlich sollte sich das zuständige Unternehmen somit zunächst mit der Wirksamkeit und Umsetzbarkeit sowie den Kosten einzelner Optionen und Maßnahmen auseinandersetzen. Bei einer

[29] Sternad, D. (2015), S. 31-32; Bartsch, M. / Frey, S. (2017), S. 78-79
[30] Königs, H.-P. (2017), S. 69-71
[31] Knoll, M. (2017), S. 15-16; Klipper, S. (2015b), S. 79-80

Entwicklung und Etablierung Cyber-Sicherheitsstrategie sollten, und folglich auch bei der Planung und Umsetzung einzelner Schritte zur Behebung und Bewältigung priorisierter Cyber-Risiken nicht nur die technische Dimension berücksichtigt werden, sondern eine ganzheitliche Sicht auf die Prozesse und Strukturen erfolgen. So bezieht sich das Cyber-Problem nicht nur auf die informationstechnische, sondern auch auf die organisatorische, physische und personelle Ebene. Risiken können in all diesen Bereichen auftreten und das Ziel der Cyber-Sicherheit gefährden. Daraus entsteht schließlich der Anspruch, in all diesen Handlungsfeldern tätig zu werden und, je nach Erfordernis, entsprechende Maßnahmen zu entwickeln und umzusetzen, um einen unternehmensweiten Schutz gegen Cyber-Angriffe zu gewährleisten. Für die Festlegung von risikomindernden Schritten ist es wichtig, die Konzentration zunächst auf jene Teilrisiken zu lenken, die zu der stärksten Verringerung des Gesamtrisikos im Bereich der Cyber-Sicherheit beitragen. Dabei gibt es keinen vorgeschriebenen Weg Cyber-Sicherheit zu realisieren, sondern jedes Unternehmen ist dazu angehalten, seiner Risikolage entsprechend, eine individuelle Definition von Handlungsfeldern und Maßnahmen vorzunehmen[32].

Um im Anschluss an die Ausarbeitung eines Soll-Konzepts und der damit einhergehenden Festlegung eines Orientierungsrahmens eine Optimierung und Verbesserung der Prozesse zu erreichen, ist eine ausführliche Planung und Strukturierung der Implementierung notwendig. Dieser Schritt der Umsetzungsplanung ist ebenso wichtig wie die Auswahl der Maßnahmen und Handlungsfelder. Dazu zählt auch die Berücksichtigung organisatorischer und sozialer Rahmenbedingungen. Im Wesentlichen erfolgt in diesem Schritt die systematische, projektartige Überführung des zuvor festgelegten Soll-Konzepts in den praktischen Betrieb und somit die technische und organisatorische Etablierung, unter Einbindung und Information aller maßgeblich beteiligten Stellen. Oft ist es jedoch genau diese entscheidende Phase der Prozessoptimierung, die Projekte scheitern lässt[33]. Der Umsetzungs-und Optimierungsprozess erfolgt meist in Form eines oder mehrerer Projekte. Dazu wird im Rahmen des Projektmanagements in vielen Fällen auf bereits bewährte Methoden zurückgegriffen, welche die damit verbundene Planung und Organisation der Maßnahmen beschreiben und steuern. Von besonderer Bedeutung ist an dieser Stelle die Auswahl der Umsetzungsform, die den Grundstein für die Ableitung bestimmter Gestaltungsmerkmale, insbesondere in Hinblick auf personelle und zeitliche Erfolgsfaktoren des Umsetzungsprozesses, bildet[34]. Welche dieser Alternativen sich für den Umsetzungsprozess am ehesten eignet, wird in erster Linie durch die individuellen unternehmerischen Rahmenbedingungen beeinflusst[35]. Es lassen sich grundsätzlich fünf Bereiche ausmachen, welche die Wahl der Umsetzungsform beeinflussen und hinsichtlich des Erfolgs eines Projekts berücksichtig werden sollten. Dies sind vor allem wirtschaftliche Rahmenbedingungen. So spielt das vorgegebene Budget zur Realisierung des Projekts eine maßgebliche Rolle. Bei der Implementierung kommt es aber mehrheitlich auch zu organisatorischen Veränderungen, besonders im Bereich der Aufbauorganisation. Dabei geht es um die Zuweisung und Neuordnung von Rollen und Aufgaben unter Berücksichtigung der entsprechenden Ressourcen. Technische Rahmenbedingungen sind ein weiterer ausschlaggebender Faktor in Bezug auf die Umsetzung. So sind

[32] Bartsch, M. / Frey, S. (2017), S. 53
[33] Hagenloch, E. et al. (2013), S. 226
[34] Hagenloch, E. et al. (2013), S. 229
[35] Hagenloch, E. et al. (2013), S. 229

insbesondere technische Maßnahmen, bspw. neue oder veränderte IT-Anwendungen und Systeme, ein häufig gewähltes Mittel zur Reduzierung von Cyber-Risiken. In diesem Zusammenhang gilt es auch, diesbezügliche Begrenzungen, wie zu geringe IT-Kapazitäten, zu berücksichtigen. Ebenso bedeutend ist die Beachtung von soziologischen und kulturellen Einflüssen. Die Veränderungsbereitschaft der Unternehmenskultur ist hier ein wichtiger Faktor, der die Umsetzung beeinflussen kann. Neben wirtschaftlichen, organisatorischen, technischen und soziokulturellen Rahmenbedingungen sind aber auch persönliche Erfahrungen ein zu berücksichtigender Einflussfaktor bei der Umsetzungsplanung. Es besteht die Möglichkeit, dass sich beteiligte Parteien entweder positiv zum Realisierungsprozess äußern und aktiv daran beteiligen oder sich aber gegen geplante Programme und deren Einführung stellen und dahingehend Widerstand leisten. All diese Gegebenheiten sollten letztlich bei der Übertragung des Soll-Konzepts in den Regelbetrieb Berücksichtigung finden. Der Umsetzungsprozess, der hauptsächlich in den Aufgabenbereich des oberen Managements fällt, kann daher nur erfolgreich sein, wenn er von den beteiligten Parteien akzeptiert wird und zugleich finanzielle, personelle und zeitliche Ressourcen und Rahmenbedingungen berücksichtigt[36]. Die Basis für den Umsetzungsplan stellt, wie bereits erwähnt, das Soll-Konzept und die strategischen Ziele dar. Die dort festgelegten Schwerpunkte, Handlungsfelder und Initiativen bilden letztendlich den Ausgangspunkt für die Planung der Implementierung und die Ableitung passender Meilensteine. Letztere dienen dem Abgleich von messbaren Zwischenergebnissen mit vorher gesetzten Zielen und sollten stets Bestandteil eines Umsetzungsplans sein. Ein Meilenstein ist erst erreicht, wenn die hierzu im Voraus definierten Arbeitspakete vollständig abgeschlossen sind. Besonders wichtig ist es, dass die zugrundeliegenden Arbeitspakete, die grundsätzlich in Abhängigkeit ihrer Wichtigkeit und Relevanz strukturiert sind, im Rahmen der zeitlichen Planung mit einem Start-und Endtermin versehen werden, um die Messbarkeit und Vergleichbarkeit zu gewährleisten. Verzögerungen besonders wichtiger und dringender Tätigkeiten sollten vermieden werden, da dies zu einer Verschiebung des gesamten Zeit-und Umsetzungsplans führen kann. Die zeitliche Planung, einschließlich der Definition einzelner Arbeitspakete und Meilensteine zur Kontrolle des Fortschritts und der Festlegung von Berichterstattungs-und Ergebnispräsentationsterminen, ist als ein maßgeblicher Erfolgsfaktor bei der Umsetzungsplanung einzuordnen. Insbesondere in den ersten Monaten des Planungshorizonts sollte der Detaillierungsgrad der angestrebten Maßnahmen hoch sein. In den Folgejahren hingegen reicht zunächst die Angabe von Tendenzen[37].

3.2. Maßnahmen zur Erhöhung der Cyber-Sicherheit

Nachdem sich im vorangegangenen Abschnitt im Wesentlichen mit dem Vorgehen hinsichtlich der Entwicklung einer geeigneten Cyber-Sicherheitsstrategie beschäftigt wurde und entsprechende Eckpunkte, Handlungsfelder und Umsetzungsformen abgeleitet und herausgearbeitet wurden, soll in diesem Abschnitt auf einige der wichtigsten Ansätze zur Erhöhung der Cyber-Sicherheit eingegangen werden. Um die Übersichtlichkeit zu wahren, wird eine Unterscheidung zwischen präventiven sowie reaktiven,

[36] Hagenloch, E. et al. (2013), S. 227-228
[37] Hagenloch, E. et al. (2013), S. 228-229 und 231; Pöchtrager, S. / Wagner, W. (2018), S. 181-183

stabilisierenden Maßnahmen vorgenommen. Allerdings ist eine einwandfreie Zuordnung zu einer dieser Kategorien nicht immer möglich, da bestimmte Instrumente in mehreren Bereichen Auswirkungen haben können. Maßnahmen im Bereich der Cyber-Sicherheit sollten durch die Reduzierung der Eintrittswahrscheinlichkeit im besten Fall zu einer Modifizierung der Risikohöhe bzw. zu einer Verringerung des Schadensausmaßes beitragen[38]. Welche Methoden und Techniken sich am ehesten eignen, hängt von der individuellen Risikolage und den finanziellen, zeitlichen und personellen Ressourcen eines Unternehmens ab. Wie bereits erläutert, sollten Entscheidungen über die Maßnahmenauswahl im Prozess der Strategieentwicklung getroffen werden. Dazu zählt schließlich auch die detaillierte Umsetzungsplanung.
Neben einigen bereits beschriebenen Methoden, wie Checklisten, die unmittelbar im Rahmen der Analyse der Ist-Situation und der Identifikation von Schwachstellen angewendet werden, gibt es zahlreiche weitere Maßnahmen, die ein Unternehmen präventiv, d.h. vorbeugend, implementieren kann, um Cyber-Risiken frühzeitig zu erkennen, im Ernstfall besser und effektiver auf Cyber-Angriffe reagieren zu können und Risiken und Schäden zu mindern oder gänzlich zu vermeiden. Zu dieser Gruppe von Maßnahmen zählen in erster Linie Schulungen und Sensibilisierungstrainings, aber auch Cyber-Versicherungen sowie weitere technische und organisatorische Ansätze zur Erhöhung der Cyber-Sicherheit.
Insbesondere Schulungen und Trainings sind ein wichtiger Baustein zur Erhöhung der unternehmerischen Cyber-Sicherheit. Diese sicherheitserhöhenden Programme können allerdings nur dann erfolgreich sein und Wirkung zeigen, wenn sich die Mitarbeiter eines Unternehmens ihrer Rolle und Bedeutung in diesem Prozess bewusst sind und entsprechende Entscheidungen und Initiativen unterstützen. Die Basis bietet die Etablierung und Pflege einer umfassenden Sicherheitskultur und eines gesunden Sicherheitsbewusstseins (engl. Awareness). So sind es gerade Mitarbeiter, die in dem Fokus von Cyber-Kriminellen stehen und vor allem im Kontext von umfassenden und sich stetig verändernden Social Engineering Attacken zum Türöffner zu sensiblen Bereichen und Systemen instrumentalisiert werden[39].
Seit einiger Zeit besteht für Unternehmen die Möglichkeit, Cyber-Risiken bzw. Schäden, die durch einen konkreten Cyber-Angriff oder andere informationstechnische Vorfälle verursacht werden, bei Versicherungsunternehmen in Rückdeckung zu geben. Diese sogenannten Cyber-Versicherungen, teilweise auch als Hacker-Versicherung oder Datenschutz-Versicherung bezeichnet, sind eine verhältnismäßig neue Produktgruppe im Angebotsportfolio der Versicherer. Kommt es zu einem konkreten Cyber-Angriff, z. B. im Kontext des Diebstahls, Verlusts oder Missbrauchs von sensiblen, digital gespeicherten Daten und Information, sowie damit einhergehend zu einer Verletzung der Cyber-Sicherheit, kann das betroffene Unternehmen, je nach vertraglicher Ausgestaltung, von einer Vielzahl an Ersatz-und Unterstützungsleistungen des entsprechenden Versicherungsunternehmens profitieren. Da sich auf Dauer nicht ausschließen lässt, dass gewisse Angriffsformen die Sicherheitshürden überwinden, ist es umso wichtiger, Maßnahmen zu implementieren, die den Tätern zumindest den unmittelbaren Zugang zu besonders schützenswerten und sensiblen Systemen und Daten erschweren[40].

[38] Klipper, S. (2015a), S. 25
[39] Wiedemer, A. / Hochenrieder, M. (2015), S. 686; BSI (2016b), S. 153
[40] Wiedemer, A. / Hochenrieder, M. (2015), S. 688

Eine dieser Möglichkeiten auf der ersten Verteidigungslinie ist die Verschlüsselung bestimmter Emails, Daten, Informationen, Systeme oder Netzwerke. Eine weitere, weitverbreitete Möglichkeit Tätern den Zugriff auf unternehmensinterne Systeme, Anwendungen und Daten zu erschweren, ist der Einsatz von Sicherheitsgateways, im allgemeinen Sprachgebrauch auch als Firewall bezeichnet. Hierbei handelt es sich um eine aus hard-und softwaretechnischen Elementen bestehende Sicherheitsvorrichtung für Netzwerke, die, unter Berücksichtigung definierter Sicherheits-richtlinien, IP-Netze koppelt und die Kommunikation überwacht. Es geht im Wesentlichen um die Kontrolle bzw. Zulassung oder Blockade des ein-und ausgehenden Datenverkehrs. Um die Sicherheit der Systeme, Daten und Anwendungen zu gewährleisten, ist ein umfassendes Kontroll-und Berechtigungssystem hinsichtlich der zugreifenden Parteien zu implementieren. Eine derartige Festlegung von Zugriffsregelungen und Berechtigungskonzepten ist notwendig, da in der heutigen Zeit Unternehmen immer mehr zu virtuellen Institutionen heranwachsen, in denen verschiedene Partner und Organisationseinheiten online und unternehmensübergreifend an gemeinsamen Projekten zusammenarbeiten[41].

Während in dem vorangegangenen Abschnitt präventive Lösungsansätze beleuchtet wurden, die hauptsächlich mit dem Ziel verbunden sind, Cyber-Angriffen vorzubeugen bzw. den Tätern den Zugang zu wichtigen Systemen und Daten zu erschweren, sollen nun sowohl reaktive als auch stabilisierende Aktivitäten im Vordergrund stehen. Dazu zählen vor allem Maßnahmen und Initiativen, wie die IT-Forensik oder IT-Notfallpläne, die im unmittelbaren Zusammenhang zu einem konkreten und ggf. erfolgreich durchgeführten Cyber-Angriff zum Einsatz kommen und, je nach Problemstellung und Sachlage, eine optimale Reaktion bieten sowie das Unternehmen zum geregelten Geschäftsbetrieb zurückführen sollen.

Die IT-Forensik, teilweise auch als Computer-Forensik bezeichnet, beschäftigt sich mit der Untersuchung von verdächtigen bzw. tatsächlich rechtswidrigen und kriminellen Vorfällen im Bereich der IuK-Technologie. Im Rahmen von Cyber-Angriffen geht es generell darum, digitale Spuren der Täter zu identifizieren, zu analysieren, auszuwerten und anschließend zu einem Gesamtbild zusammenzufügen. Es handelt sich dementsprechend in erster Linie um ein Werkzeug zur Ursachenforschung und Aufklärung von cyber-kriminellen Straftaten[42]. Laut BSI beschränkt sich die IT-Forensik allerdings nicht nur auf diese kriminelle Dimension, sondern schließt zusätzlich auch die allgemeinen Einsatzmöglichkeiten aus Sicht des Anlagenbetreibers mit ein. Dazu zählt die Untersuchung von Vorfällen, die keinen kriminellen Hintergrund aufweisen, wie Hard- oder Softwareversagen oder andere Probleme, die auf ein Fehlverhalten der Nutzer zurückzuführen sind[43].

Da Cyber-Angriffe oder anderweitige informationstechnische Ausfälle und Fehlfunktionen eine erhebliche Beeinträchtigung der Geschäftsprozesse und demnach auch Umsatzeinbußen und andere Schäden zur Folge haben können, ist es unabdingbar ein Notfallmanagement, häufig auch als betriebliches Kontinuitätsmanagement bezeichnet, zu implementieren. Dadurch wird gewährleistet, dass im Ernstfall eine zielgerichtete Reaktion erfolgen kann. Nur durch die präventive Etablierung einer derartigen Institution können Schäden minimiert und eine optimale

[41] Herwig, V. / Schlabitz, L. (2004), S. 289
[42] Dolle, W. (2009), S. 183; BSI (2016b), S. 5010
[43] BSI (2011), S. 8

Notfallversorgung und -bewältigung, in Form einer schnellen und strukturierten Rückkehr zum geregelten Betrieb, sichergestellt werden. Das Notfallmanagement wird dann aktiv, wenn ein Notfall bzw. Schadensereignis die Kontinuität und Verfügbarkeit bestimmter Prozesse und Ressourcen einschränkt und infolgedessen den allgemeinen Geschäftsbetrieb beeinträchtigt[44]. Die Wahl der zu ergreifenden Maßnahmen beruht im Wesentlichen auf der Beurteilung des Schadens und seiner voraussichtlichen Entwicklung. Je nach Ausmaß sollten daher bestimmte Eskalationsstufen mit zugehörigen Methoden, Kriterien und Vorgehensplänen definiert werden. So ist es möglich, dass sich ein Notfall schnell zu einer bedrohlichen Krise ausweitet, was eine erhebliche Gefährdung der Fortführung des Geschäftsbetriebs bedeuten und in der Folge eine Bedrohung für die Existenz der Unternehmung sein kann[45].

4. Kritische Würdigung

Im Rahmen der Bearbeitung der Thematik wird deutlich, dass Cyber-Sicherheit einen immer wichtigeren Stellenwert in der Gesellschaft, Wirtschaft und Politik einnimmt und auch dringend einnehmen sollte. So sind die Gefahren aus dem Cyber-Raum vielfältiger und komplexer denn je und es kommen täglich neue Angriffs-und Bedrohungsformen hinzu. Inzwischen fällt es schwer, einen genauen und vor allem aktuellen Überblick über die Täter und Ausgestaltungsmöglichkeiten entsprechender Angriffe zu erhalten. Auf die bedeutendsten und in der Mehrzahl der Fälle Anwendung findenden Vorgehensweisen wurde zwar in diesem Diskussionspapier hingewiesen, allerdings ist da-von auszugehen, dass im Laufe der Zeit bereits neue Arten oder Abwandlungen bestehender Formen hinzugekommen sind. Diese steigende Komplexität und Dynamik der Cyber-Risiken, aber auch der Fortschritt in der Technologie stellt eine der größten Herausforderungen und Risiken für die Erarbeitung und Bereitstellung von cyberrelevanten Lösungsansätzen dar. Um Zugang zu wichtigen Systemen, Daten und Informationen zu erlangen, entwickeln die Täter kontinuierlich neue Strategien. Da sich Unternehmen immer wieder mit diesen, bisher unbekannten und stetig an Komplexität dazugewinnenden Cyber-Angriffen konfrontiert sehen, ist das Thema Cyber-Sicherheit als eine dauerhafte Aufgabe einzuordnen, die einer fortwährenden Beobachtung bedarf.
Die in diesem Diskussionspapier aus der Literatur hergeleiteten Entwicklungsphasen einer Cyber-Sicherheitsstrategie, von der Analyse, über die Festlegung strategischer Ziele, Handlungsfelder und Maßnahmen, bis hin zur Umsetzungsplanung, sind daher nicht als einmalige Tätigkeit anzusehen, sondern erfordern eine stetige Kontrolle und Anpassung[46]. Cyber-Sicherheit ist folglich eine ganzheitliche, sich über alle Abteilungen und Fachgebiete im Unternehmen erstreckende Disziplin, die in der Praxis, ähnlich einem Kreislauf, ständig weiterzuentwickeln ist.
In Bezug auf diese dynamischen Prozesse lässt sich schlussfolgern, dass selbst bei minimalen technischen Veränderungen der IT-Architektur oder auch bei organisatorischen Anpassungen, wie der Neueinstellung von Mitarbeitern, die bisherige Strategie überprüft und ggf. modifiziert werden sollte. Dazu zählen schließlich sowohl die Anpassung des Maßnahmenkatalogs als auch der Methoden und Instrumente an

[44] BSI (2008), S. 1; BSI (2016b), S. 120
[45] BSI (2016b), S. 120; Königs, H.-P. (2017), S. 329
[46] Klipper, S. (2015b), S. 92; BMI (2016), S. 7 und 45; Bartsch, M. / Frey, S. (2017), S. 76

sich. So sollte z. B. bei der Einstellung eines neuen Mitarbeiters eine genaue Befragung hinsichtlich seines Kenntnis-und Wissensstands sowie seiner Qualifikation und Erfahrung bzgl. cyber-relevanter Themen erfolgen, um abschätzen zu können, inwieweit und in welchem Umfang Personalentwicklungs-oder Sensibilisierungsmaßnahmen notwendig sind. In jedem Falle sollte aber vor der Aufnahme der Tätigkeit eine genaue Aufklärung über unternehmensinterne Sicherheitsrichtlinien und Regelungen stattfinden. Dazu zählt, neben der Einweisung und Bekanntmachung mit unternehmensspezifischen informationstechnischen Abläufen, Vorgehensweise und Pflichten, auch die präzise Zuweisung von Zugriffs-und Zutrittsberechtigungen, um von Beginn an Missverständnisse zu vermeiden[47]. Unter Umständen ist es darüber hinaus möglich, dass neue Mitarbeiter selbst ein gewisses Know-how, das sie sich bspw. während der Ausübung einer früheren Tätigkeit angeeignet haben, in die Organisation transferieren und somit einen positiven Beitrag zur Weiterentwicklung der internen Cyber-Sicherheitskultur leisten. Des Weiteren kann jedoch auch die Beendigung oder Änderung eines Arbeitsverhältnisses mit ernstzunehmenden, cyber-relevanten Aufgaben verbunden sein. So sollten insbesondere bisher durch diese Mitarbeiter genutzte Informationswerte, wie physische oder logische Schlüssel, Authentisierungsmittel oder auch Computer, dem Unternehmen zurückgeben werden, um zu vermeiden, dass jene im Nachhinein zu kriminellen Zwecken verwendet werden. Aber auch die Zugangsberechtigungen zu bestimmten Systemen und Anwendungen sollten gelöscht bzw. an den neuen Aufgabenbereich angepasst werden. Als besonders kritisch könnte sich in diesem Zusammen-hang die dienstliche Nutzung privater mobiler Geräte erweisen, da der Einfluss des Unternehmens auf hier verarbeitete und gespeicherte Daten äußerst begrenzt ist. Bei der Auflösung des Arbeitsverhältnisses oder dem Arbeitsplatzwechsel könnte es daher geschehen, dass wichtige, anwenderspezifische und sensible Unternehmensdaten weiterhin genutzt bzw. nicht gelöscht werden [48] . Diese Bedrohungen sind häufig nicht auf den ersten Blick sichtbar, können einer Organisation jedoch auf lange Sicht großen Schaden zufügen. So könnte der Fall eintreten, dass ein ehemaliger Mitarbeiter ein mobiles Gerät, z. B. ein Notebook, nicht ausreichend durch geeignete Maßnahmen, wie eine Firewall oder ein Virenschutzprogramm, sichert und in der Konsequenz als leichtes Ziel für potentielle Cyber-Angriffe gilt. Es ist auch möglich, dass ein Mitarbeiter nach dem Wechsel des Arbeitgebers dazu instrumentalisiert wird, wichtige Daten an Dritte weiterzugeben oder selbst Daten zu manipulieren, Zugänge zu blockieren oder andere cyber-kriminelle Straftaten zu begehen. Einmal mehr wird deutlich, dass Mitarbeiter einen äußerst bedeutenden Faktor darstellen, wenn es um die Umsetzung von Cyber-Sicherheit geht. Deshalb sollten entsprechende Maßnahmen einen überaus hohen Stellenwert einnehmen. In Hinblick auf den dynamischen Digitalisierungsprozess und den stetigen Fortschritt in der Technologie stellt sich die Frage, wie diese Schulungsprojekte für Mitarbeiter ausgestaltet sein sollten. Die reine Wissensvermittlung cyber-relevanter Themen scheint hier zwar als unmittelbarer, reaktiver Ansatz sinnvoll zu sein, allerdings ist davon auszugehen, dass anwenderspezifische Schulungen, bspw. im Rahmen eines Einzeltrainings, langfristig die stärksten Auswirkungen auf die unternehmensinterne Sicherheitskultur haben. Das könnte damit begründet werden, dass die Mitarbeiter in

[47] Kersten, H. et al. (2013), S. 166-171
[48] Kersten, H. et al. (2013), S. 171-172

diesem Fall direkt mit dem Problem konfrontiert werden und durch eine individuelle Betreuung mit der Lösung bzw. Vorgehensweise zur Vermeidung der Bedrohung vertraut gemacht werden. Diese Option dürfte allerdings vor allem für Unternehmen mit einer großen Mitarbeiterschaft schwer umzusetzen sein, da sie vermutlich mit einem hohen zeitlichen Aufwand verbunden ist.
Um eine grundsätzliche Sensibilisierung für die Bedeutung der Cyber-Thematik zu erreichen, sollten geeignete Initiativen ggf. schon viel früher ansetzen. So schlägt auch das BMI in der Cyber-Sicherheitsstrategie für Deutschland vor, bereits in der schulischen Ausbildung mit der Vermittlung von digitalem Wissen und digitalen Kompetenzen zu beginnen und dies kontinuierlich über die verschiedenen Stufen des Bildungsprozesses und des beruflichen Werdegangs bis in das Erwachsenenalter fortzuführen. Durch die schon früh beginnende Wissensvermittlung und Sensibilisierung bzgl. des verantwortungsvollen Auftretens und Verhaltens im Cyber-Raum wie auch des bedachten Einsatzes der IT kann schließlich ein Grundverständnis bei der Verwendung von entsprechenden Technologien in der Bevölkerung bewirkt und als Folge dessen die Anzahl der erfolgreichen Cyber-Angriffe in Deutschland reduziert werden[49]. Dieser Ansatz, der sich ursprünglich auf Privatanwender bezieht, könnte Unternehmen auf lange Sicht viel Arbeit ersparen, da Mitarbeitern nun nicht mehr in vollem Umfang Grundlagenwissen zu vermittelt ist. Das wiederum würde zu erheblichen finanziellen und zeitlichen Ersparnissen für die Beteiligten führen. Allerdings sollte ein derartiges Vorgehen nicht bedeuten, dass vollkommen auf Trainings-und Sensibilisierungsmaßnahmen verzichtet werden kann. Da es sich um eine dynamische Disziplin handelt und jedes Unternehmen über individuelle Strukturen verfügt, lassen sich Weiterbildungen und Schulungen auf Dauer nicht vermeiden.
Es zeigt sich, dass sich das Thema Cyber-Sicherheit nicht nur, wie häufig angenommen, auf eine rein technische Ebene bezieht, sondern deutlich weitreichender ist. So begehen viele Unternehmen den Fehler, Cyber-Sicherheit vollkommen mit der Sicherheit der informationstechnischen Systeme gleichzusetzen und bei der Konzeptionierung einer Cyber-Sicherheitsstrategie ausschließlich in diesem Bereich aktiv zu werden. Allerdings geht Cyber-Sicherheit deutlich über die technische Betrachtungsweise hinaus und beinhaltet zudem auch physische, organisatorische und personelle Aspekte[50]. Während die Unternehmen auf der technischen Ebene bis zu einem gewissen Grad von den Zulieferern und Herstellern abhängig sind, können sie auf der organisatorischen, physischen und personellen Ebene die Grundlagen für die Erhöhung der Cyber-Sicherheit größtenteils eigenständig schaffen. Allgemein stellt sich jedoch die Frage, inwiefern und ob es überhaupt möglich ist, eine Cyber-Sicherheitsstrategie zu entwickeln, die unternehmensübergreifend Anwendung finden kann. Da jedes Unternehmen in seiner Struktur, seinen Abläufen und seiner grundsätzlichen Organisation ein individuelles Konstrukt ist, für das es einer spezifischen Planung bedarf, würde ein einheitliches Konzept vermutlich scheitern. Mit Blick auf die einzelnen Planungsphasen lässt sich sagen, dass es sich bei den in diesem Diskussionspapier hergeleiteten Entwicklungsschritten und Inhalten einer Cyber-Strategie um einen beispielhaften Leitfaden zur Orientierung in der komplexen Umwelt handelt, der grobe Ansatzpunkte zur Verfügung stellt, wie ein generelles Vorgehen zur Erhöhung der Cyber-Sicherheit aussehen könnte. Vor allem die Wahl bzw. die Ausgestaltung der zu

[49] BMI (2016), S. 14
[50] Bartsch, M. / Frey, S. (2017), S. 49

ergreifenden Maßnahmen ist stark von der unternehmensspezifischen Struktur und Risikosituation abhängig. Insbesondere die individuelle Ressourcenausstattung ist ein wichtiger Aspekt in Bezug auf die Cyber-Sicherheitsstrategie. So hängt die Detailtiefe einzelner Planungsschritte und Aktivitäten in hohem Maße von den finanziellen Mitteln und besonders von dem verfügbaren Personal eines Unternehmens ab. Aufgrund der unmittelbaren Bedrohungslage und der hohen Schadenssummen sollten sich sowohl klein-und mittelständische Unternehmen als auch internationale Großkonzerne eingehend mit der Implementierung einer eigenen Cyber-Sicherheitsabteilung bzw. der Entwicklung einer Cyber-Sicherheitsstrategie beschäftigen. Verschiedene Studien zeigen, dass die Zahl der Cyber-Angriffe in den letzten Jahren stark angestiegen ist. Laut Bitkom waren in den Jahren 2015 und 2016 mehr als die Hälfte aller befragten Unternehmen von einem Cyber-Angriff betroffen. Besonders Großunternehmen scheinen gefährdet[51]. Eine Studie des Prüfungs-und Beratungsunternehmens Deloitte zeigt, dass ca. 83 Prozent der befragten Großunternehmen mit mehr als 1000 Mitarbeitern mehrmals monatlich mit Cyber-Attacken konfrontiert werden[52]. Im Kontext des technischen Fortschritts und der Digitalisierung sollten sich aber auch kleine Unternehmen nicht dem Veränderungsprozess entziehen bzw. auf die Implementierung von cyber-relevanten Maßnahmen verzichten. Hier stellt sich in erster Linie die Frage, ob oder in welchem Umfang sich diese Organisationen mit der Entwicklung einer eigenen Cyber-Sicherheitsstrategie beschäftigen können und welch Instru-mente grundsätzlich zur Auswahl stehen. Insbesondere die begrenzten Ressourcen sind an dieser Stelle ein wichtiger Aspekt, den es zu beachten gilt. Speziell kleine Unternehmen können sich nicht in dem Umfang mit dem Thema auseinandersetzen und dahingehende Kapazitäten zur Verfügung stellen, wie große Unternehmen dazu in der Lage sind[53]. Derartige entwicklungstechnische Vorgänge und der anschließende Realisierungsprozess sind aus finanziellen und personellen Gesichtspunkten eine große Herausforderung. So besteht die Voraussetzung, dass die benötigten Kompetenzen dafür im Unternehmen vorhanden sind und das Personal zur Bearbeitung dieser Aufgaben verfügbar ist. Die Bereitstellung der erforderlichen Ressourcen kann wiederum zu einer starken finanziellen Belastung führen. Um diesen großen organisatorischen und personellen Aufwand zu vermeiden, kann möglicherweise auf anderweitige Lösungsansätze zurückgegriffen werden. Eine Alternative könnte die Inanspruchnahme von Beratungsdienstleistungen externer Firmen sein. Auf diese Weise kann der Druck vom eigenen Unternehmen genommen werden und darüber hinaus vom Know-how spezialisierter Firmen profitiert werden, welche z. B. ein maßgeschneidertes Konzept zur Erhöhung der Cyber-Sicherheit zusammenstellen, interne Abläufe analysieren, Schwachstellen aufspüren, Handlungspläne erarbeiten oder in konkreten Notfallsituationen reaktive und unterstützende Services bereitstellen. Unter Umständen arbeiten diese Unternehmen wiederum mit weiteren Kooperationspartnern zusammen, sodass im Folgenden auf schnellem und effektivem Wege die Maßnahmenumsetzung eingeleitet werden können[54]. Besonders für kleine Unternehmen mit wenigen Mitarbeitern könnten diese Lösungsansätze Vorteile bieten, da somit vom Spezialwissen der Experten profitiert und zugleich die internen, personellen Ressourcen geschont werden können. Hier stellt sich dennoch die Frage, ob dies auf lange Sicht finanziell tragbar

[51] Bitkom (2017), S. 2
[52] DTTL (2017), S. 8
[53] DTTL (2017), S. 9
[54] HiSolutions AG (2018); PwC (2018); DTTL (2018)

ist, zumal die Strategien und Programme regelmäßige Anpassungen und Kontrollen erfordern.
Eine andere, ggf. wirtschaftlichere und daher eher geeignete Möglichkeit ist der Abschluss einer Cyber-Versicherung. Durch die individuelle Bausteinauswahl gemäß der eigenen Risikolage, kann sich im Schadensfall besser abgesichert werden. Eine Versicherung gegen Schäden aus einem Cyber-Angriff könnte jedoch von gewissen Unternehmen als Ersatz für schadensvorbeugende und präventive Maßnahmen angesehen werden. Ein solcher Gedankengang sollte vermieden werden, da auch der Deckungsrahmen einer Cyber-Versicherung, je nach gewählten Bausteinen, begrenzt ist. Vor allem indirekte Kosten und Schäden, wie Reputations-oder Marktwertverluste, lassen sich nur schwer bemessen und könnten langfristig hohe Kosten verursachen. In vielen Tarifen können die Versicherten allerdings mittlerweile auch verschiedene Assistance-Leistungen in Anspruch nehmen. Dazu zählen nicht nur reaktive Ansätze, wie die Vermittlung von IT-Forensik-Experten, Rechtberatern oder PR-Spezialisten, sondern auch präventive und beratende Services[55]. Auch wenn sich ein Unternehmen entschließt, die Entwicklung einer Cyber-Sicherheitsstrategie und damit einhergehende technische, organisatorische, physische und personelle Aspekte eigenständig zu strukturieren und zu planen, stehen hierfür ausreichend Anhaltspunkte und Leitlinien zur Verfügung, um diesen Prozess bestmöglich zu unterstützen. Speziell das BSI engagiert sich stark für die Bereitstellung von umfangreichen Informationsangeboten zum Thema Cyber-Sicherheit und die Schaffung von passenden Rahmenbedingungen. Dabei richtet sich das BSI an verschiedene Zielgruppen. Neben Informationen für Bürger, die bspw. im Rahmen der Initiative „BSI für Bürger" online abrufbar sind, bietet das BSI auch weitreichende Beteiligungsmöglichkeiten, Leitlinien und Handlungsempfehlung für die Wirtschaft an[56].
Insbesondere die öffentlich zugänglichen IT-Grundschutz-Kataloge, die auf Grundlage der internationalen Zertifizierungsnorm für Informationssicherheitsmanagementsysteme (ISO/IEC 27001) entwickelt und abgestimmt wurden, sind ein äußerst hilfreiches Mittel, um Cyber-Sicherheitskonzepte unternehmensweit zu etablieren. Grundsätzlich handelt es sich hierbei um einen anerkannten Sicherheitsleitfaden, der eine Sammlung aus organisatorischen, personellen, infrastrukturellen und technischen Standard-Maßnahmen enthält, die für alle gängigen Geschäftsprozesse, Anwendungen und Systeme geeignet sind und, je nach Kombination, einen ganzheitlichen und angemessenen Basisschutz bieten[57]. Die Gesamtheit oder zumindest Teile der in den Sicherheitsleitlinien beschriebenen Standards und Empfehlungen können schließlich einen unter-stützenden Beitrag zu der Entwicklung einer individuellen Sicherheitskultur und zum Aufbau einer unternehmenseigenen Standardisierung leisten[58]. Die Orientierung an bestimmten Standard-Regelwerken kann darüber hinaus aber auch ein wichtiger Faktor sein, um eine Zertifizierung, z. B. nach ISO-Standards, zu erhalten und in diesem Zusammenhang gewisse Kundenanforderungen zu erfüllen. In diesem Fall steht hauptsächlich der Anspruch der Unternehmensleitung im Vordergrund, eine möglichst gute Außendarstellung zu erreichen und die eigene Position am Markt zu stärken. Die

[55] Biener, C. et al. (2015), S. 54; Mukhopadhyay, A. et al. (2005), S. 157; KPMG AG (2017), S. 20; GDV (2017); Allianz Deutschland AG (2016)
[56] BSI (2017), S. 49 und 69
[57] BSI (2016b), S. 71-72; BSI (2018b)
[58] Königs, H.-P. (2017), S. 194

Schaffung einer Zertifizierungsmöglichkeit, deren Bescheinigung durchaus mit hohen qualitativen Anforderungen verbunden ist, könnte letztlich einen Anreiz für viele Unternehmen darstellen, sich stärker mit dem Thema Cyber-Sicherheit auseinanderzusetzen und die geforderten Sicherheitsstandards durch die Entwicklung und Implementierung einer Cyber-Sicherheitsstrategie in die eigene Sicherheitsarchitektur zu integrieren. Allgemein könnte die unternehmensübergreifende Einführung einer gesetzlichen Zertifizierung oder Sicherheitsampel eine gewisse Vergleichbarkeit gewährleisten und gleichzeitig dafür Sorge tragen, dass die Sicherheit des Wirtschaftsstandorts Deutschland in erheblichem Maß positiv beeinflusst wird. Der Rückgriff auf ein Standard-Regelwerk könnte ggf. auch vor dem Hintergrund der Erfüllung gesetzlicher und regulatorischer Anforderungen erfolgen[59]. So erhalten Unternehmen in letzter Zeit nicht nur Druck seitens der Kunden und Partner, sondern auch vom Gesetzgeber, der den Handlungsbedarf in diesem Bereich in zunehmendem Maße wahrnimmt und versucht durch geeignete Maßnahmen Abhilfe zu schaffen. Mit verschiedenen Richtlinien und gesetzlichen Regelungen, wie dem IT-Sicherheitsgesetzt, der EU-Datenschutzgrundverordnung und der NIS-Richtlinie, wird von staatlicher Seite aus versucht, die Unternehmen dazu zu drängen, in dem Bereich der Informationssicherheit tätig zu werden und sich gegen Gefahren aus dem Cyber-Raum zu schützen[60]. Die Schaffung entsprechender Rahmenbedingungen kann schließlich einen entscheidenden Beitrag dazu leisten, den deutschen und europäischen Wirtschaftsraum sicherer zu gestalten und besonders die Konsumenten zu schützen. Es ist zu erwarten, dass diese Regelungen dazu führen, dass sich Unternehmen zukünftig stärker mit dem Schutz ihrer Systeme, Anwendungen, Daten und Web-Services auseinandersetzen werden, zumal im Falle der fehlenden Berücksichtigung dieser Vorschriften unter Umständen hohe Strafen drohen[61]. Theoretisch sind Gesetze in diesem Bereich eine gute Möglichkeit, um alle Beteiligten für Cyber-Sicherheit und den Datenschutz zu sensibilisieren sowie zum Aufbau und der Integration geeigneter Strukturen und Programme zu drängen. Allerdings setzt dies wiederum gewisse Kontroll-und Überprüfungsmechanismen voraus, um die Einhaltung und Anpassung der Standards sicherzustellen. Vor dem Hintergrund der fortschreitenden Digitalisierung, einer sich ständig verändernden technischen und organisatorischen Umwelt wie auch unternehmensspezifischer Infrastrukturen und Prozesse ist es nur schwer vorstellbar, wie zukünftig gewährleistet werden soll, dass entsprechende Gesetze branchenübergreifend durchgesetzt werden. Als erschwerender Faktor kommt hinzu, dass häufig verschiedene Parteien an der Entwicklung und Umsetzung von Cyber-Sicherheitskonzepten beteiligt sind, sodass sich die Schuldzuweisung im Schadensfall zu einer äußerst komplexen Herausforderung erweisen kann. Auch wenn ggf. eine explizite Zuweisung und Definition von Verantwortlichkeiten im Rahmen einer Cyber-Sicherheitsstrategie stattgefunden hat, kann es unter Umständen sein, dass sich aufgrund der vielschichtigen Strukturen und Überschneidungen der Bereiche nur schwer herausfinden lässt, wo ein Fehler begangen wurde und welcher Partei er zugeschrieben werden kann. Besonders bei der Integration externer Partner und Experten zur Prüfung der Systeme und Beratung hinsichtlich der Cyber-Sicherheit können sich Schwierigkeiten ergeben[62]. Mit Blick auf die sehr dynamischen

[59] Königs, H.-P. (2017), S. 241; BSI (2018b), BSI (2014a), S. 37-38
[60] BMWi (2018); BSI (2016a), S. 5; BSI (2018a)
[61] Verlag Dierichs GmbH & Co KG (2018)
[62] DTTL (2014), S. 6

Entwicklungen der letzten Jahre lässt sich sagen, dass speziell in Bezug auf die zunehmende Nutzung innovativer Technologien, wie der Cloud-Technologie, neue gesetzliche Regelungen benötigt werden, um sichere Rahmenbedingungen zu schaffen und Daten und Informationen zu schützen.
Aber nicht nur der Gesetzgeber steht hier in der Pflicht, sondern auch die Unternehmen sind dazu angehalten, ihre strategischen Konzepte in Hinblick auf die Cyber-Sicherheit zu überdenken und anzupassen. So sollte vor allem im Zuge der zunehmenden Smartphone-Nutzung zu beruflichen Zwecken eine Modifizierung der Cyber-Sicherheitsstrategien erfolgen. Da Smartphones immer stärker in die unternehmensinternen Strukturen integriert werden, dabei jedoch zugleich auch den Privatgebrauch unterstützen und den Anwender nicht zu stark einschränken sollten, stellt die Entwicklung entsprechender Sicherheitskonzepte eine enorme Herausforderung dar. Eine große Gefahr ergibt sich an dieser Stelle primär durch den unachtsamen Gebrauch. Wird ein Gerät bspw. gestohlen, kann dies eine unmittelbare Bedrohung darstellen, denn unter Umständen können sich darauf sensible Unternehmensdaten befinden, die auf diesem Wege in fremde Hände gelangen und in der Folge den Einflussbereich des Unternehmens verlassen. Aber auch durch das Herunterladen bestimmter Applikationen können schädliche Programme das Smartphone infizieren und im Hintergrund ggf. Nachrichten mitlesen und auf wichtige Daten und Informationen zugreifen, ohne dass es der Benutzer bemerkt. Bei der Entwicklung einer unternehmensweiten Cyber-Sicherheitsstrategie sollten die Beteiligten daher das Blickfeld erweitern und jegliche Bedrohungsquellen in den Planungsprozess einbeziehen. Denn je mehr Technologie genutzt wird, desto größer ist letztendlich die Gefahr, Opfer eines Cyber-Angriffs zu werden. Ein umfassendes „Mobile Device Management" zur zentralen Verwaltung der verwendeten mobilen Geräte und Aktivitäten sollte demnach in der heutigen Zeit ein wichtiger Bestandteil einer Cyber-Sicherheitsstrategie sein[63].
Das Beispiel des Smartphones zeigt erneut, welche Dimensionen das Thema Cyber-Sicherheit einnimmt und welche fundamentalen Entscheidungen damit zusammenhängen. Dazu zählt schließlich auch, dass sich bereits bei der Auswahl der zugrundeliegenden Systemkomponenten, Applikationen oder Tools mit sicherheitstechnischen Details auseinandergesetzt wird und nicht erst bei Eintritt eines Schadensfalls. Eine der wichtigsten Entscheidungen bezieht sich auf den Einsatz von Standard-oder Individualsoftware. Je nach gewählter Option entscheidet sich, welche Sicherheitsmaßnahmen zu ergreifen sind bzw. in welchem Ausmaß und welcher Intensität sie eingesetzt werden sollten. Beide Alternativen haben grundsätzlich zahlreiche Vor-und Nachteile, die im weiteren Unternehmensgeschehen eine maßgebliche Rolle spielen können. Standardsoftware bietet sich in erster Linie aufgrund ihrer vergleichsmäßig geringen Implementierungs-und Anpassungskosten wie auch einer schnellen Verfügbarkeit an. Zudem kann ein Unternehmen durch die Einführung von Standardsoftware von einem Know-how-Transfer sowie einem dauerhaften Support und umfangreichen Schulungsangeboten durch den Hersteller profitieren. Allerdings ist die technische Anpassungsfähigkeit im Vergleich zu Individualsoftware, deren Struktur und Organisation sich vollkommen auf interne Prozesse anpassen lässt, sehr begrenzt. Individualsoftware gilt hingegen nach der sehr ressourcenvereinnahmenden Einführung als eher unausgereift und fehlerbehaftet. Durch die unmittelbare Einflussnahme auf den Ent-

[63] Li, Q. / Clark, G. (2013), S. 78-79; Wiedemer, A. / Hochenrieder, M. (2015), S. 684-685

wicklungsprozess einer Individualsoftware können jedoch bereits sehr früh individuelle Sicherheitsbausteine und ggf. andere cyber-relevante Faktoren in das Programm einfließen. Zugleich wird durch die Entwicklung und Implementierung einer Individualsoftware kein Abhängigkeitsverhältnis zum Softwarehersteller und den damit einhergehenden Dienstleistungen aufgebaut[64]. Daraus wird ersichtlich, dass sich Unternehmen bereits bei der fundamentalen Planung, Entwicklung und Integration entsprechender informationstechnischer Strukturen damit auseinanderzusetzen haben, auf welche Art und Weise mit dem Thema Cyber-Sicherheit umgegangen werden soll und welche Faktoren hier eine ausschlaggebende Rolle spielen sollen. So entscheidet sich schon bei der Wahl der Software, ob bestimmte Kooperationen und damit einhergehende sicherheitsrelevante Abhängigkeiten eingegangen werden oder die Entwicklung von Sicherheitsmechanismen und die anschließende Integration in die Konzepte eigenständig geschehen.
Cyber-Sicherheit beginnt somit bereits bei der Konzeptionierung der grundlegendsten Entscheidungen und Prozesse. Diese werden nicht nur durch die übergeordnete Unternehmensstrategie beeinflusst, sondern sie wirken im Gegenzug, insbesondere durch die Nutzung der eingesetzten Technologien und Methoden, auch auf diese zurück. So wird die strategische Planung von Umweltveränderungen und folglich auch von Veränderungen der IT beeinflusst. Da hier grundsätzlich auch sicherheitsrelevante Aspekte im Vordergrund stehen, wird deutlich, dass die Cyber-Sicherheitsstrategie nicht als isoliertes Objekt betrachtet, sondern in den Gesamtkontext des Unternehmens eingeordnet werden sollte[65]. Eines der größten Probleme bei der Gewährleistung der Sicherheit auf technischer Ebene ist derzeit jedoch noch die starke Abhängigkeit von den Herstellern und Anbietern, die nur teilweise für die Sicherheit ihrer IT-Lösungen die Verantwortung übernehmen. Um an dieser Stelle mehr Vertrauen und Transparenz zu schaffen, bräuchte es eine Herstellerverantwortung, welche diese dazu drängt, für die Sicherheit der angebotenen Komponenten, Systeme und Services zu haften. Vorbild könnte die Automobilbranche sein, in der die Hersteller mehrheitlich für die Sicherheit ihrer Produkte einstehen und als Ansprechpartner verfügbar sind, um bei den ersten Anzeichen von Problemen, bspw. im Rahmen von Rückrufaktionen, die Fehler zu beseitigen und auf diese Weise das Vertrauen der Kunden langfristig sicherzustellen. Derartige Strukturen bestehen im IT-Bereich bisher nicht. Eine Gesamtverantwortung übernimmt hier kaum ein Hersteller, obwohl dies zu einer deutlichen Reduzierung der existierenden Sicherheitsprobleme, einer besseren Abstimmung der Software und Hardware sowie einer effizienteren Fehlersuche und -korrektur führen würde. Das IT-Sicherheitsgesetz hat durch die Verantwortungs-und Pflichtzuweisung der Webseiten-Betreiber bereits einen wichtigen Beitrag geleistet, um die Nutzer zu schützen. Für die Zukunft sind je-doch weitere, internationale Anstrengung notwendig, um die Cyber-Sicherheit auf technischer Ebene voranzubringen und die Internetnutzung sicherer zu gestalten[66].
Die Bereitstellung vertrauenswürdiger Informationstechnik sollte in der Konsequenz ein wesentlicher Bestandteil zukünftiger politischer Anstrengungen sein. Dazu zählt auch, ausländische Anbieter hierzulande durch geeignete Ansätze in die Pflicht zu nehmen, die Vertraulichkeit ihrer Produkte zu gewährleisten und gewisse Standards zu erfüllen.

[64] Mertens, P. et al. (2017), S. 136
[65] Krcmar, H. (2015), S. 92-93
[66] Pohlmann, N. (2016), S. 40

Hier könnte, wie bereits erwähnt, die Implementierung von standardisierten Sicherheitskriterien, unterstützt durch entsprechende Sicherheitszertifikate, ein adäquates Mittel sein, um diesbezüglich eine höhere Transparenz sicherzustellen und gleichzeitig eine Differenzierungsmöglichkeit auf dem Markt zu etablieren. Dabei gilt es, das Blickfeld zu erweitern und auch aufstrebende Technologien, besonders im Bereich der mobilen Nutzung, einzubeziehen[67]. Allgemein zeigt sich, dass es aufgrund der zahlreichen Herausforderungen, Angriffsformen und Strategien kein Patentrezept zur Gewährleistung von Cyber-Sicherheit geben kann. Die vernetzte Sicherheit kann jedoch ein wichtiger Faktor auf nationaler und internationaler Ebene sein, um den Bedrohungen gemeinsam zu begegnen. So gibt es heutzutage bereits viele Netzwerke zwischen wirtschaftlichen, staatlichen und gesellschaftlichen Akteuren, die deutschlandweit, in Europa oder global zusammenarbeiten. Diese kooperativen Konzepte können einen entscheidenden Beitrag dazu leisten, den Austausch von Informationen zu vereinfachen und das Verantwortungsbewusstsein und Vertrauen zwischen den beteiligten Parteien zu stärken. In Deutschland nimmt unter anderem das Cyber-Abwehrzentrum unter der Oberaufsicht des BSI eine wichtige Rolle im Kampf gegen Cyber-Kriminalität ein. Hier sind die zentralen Sicherheitsbehörden miteinander vernetzt. Der Fokus der Initiative, welcher derzeit nur auf der IT-Sicherheit liegt, sollte allerdings zu einem umfassenderen, vor allem die Kriminalitätsbekämpfung einschließenden Ansatz erweitert werden. Es ist daher geeignete Strukturen zu schaffen, um nicht nur den Informationsaustausch und die präventiven Maßnahmen zur Cyber-Abwehr zu fördern, sondern zukünftig auch das Krisenmanagement und die anschließende Strafverfolgung in das Konzept einzubeziehen. In diesem Zusammenhang sollte auch die Zusammenarbeit zwischen verschiedensten Akteuren aus Wirtschaft und Wissenschaft sowie aus Strafverfolgungsbehörden systematisch ausgebaut werden, um das entsprechende Know-how bereichsübergreifend nutzen und die sich ergebenden Potentiale dieser Netzwerke vollständig wahrnehmen zu können. Nur durch die kontinuierliche, bereichsübergreifende und internationale Zusammenarbeit kann eine frühzeitige und umfassende Sensibilisierung erfolgen und ein ganzheitlicher Schutz gegen Cyber-Risiken, durch die Schaffung verschiedener Einflussmöglichkeiten und Initiativen zur Früherkennung und Verfolgung cyberrelevanter Straftaten, sichergestellt werden[68]. Unabhängig davon sollten die eigenverantwortliche Gewährleistung der Sicherheit auf Unternehmensebene und der diesbezügliche Schutz sensibler Daten und Informationen stets an erster Stelle stehen. Damit sollte idealerweise auch der Anspruch einhergehen, präventive Maßnahmen zu realisieren. Eine Studie der Beratungsgesellschaft PricewaterhouseCoopers (PwC) aus dem Jahr 2017 zeigt allerdings, dass im mittelständischen Bereich die Einführung geeigneter präventiver Sicherheitskonzepte, trotz verbesserter Zahlen im Vergleich zu den Vorjahren, weiterhin stockend verläuft[69]. Viel zu selten ist es der Ansatz einer frühzeitigen Vorsorge, der die Unternehmen antreibt geeignete Sicherheitskonzepte zu entwickeln und zu etablieren. In vielen Unternehmen werden derzeit lediglich reaktiv Sicherheitslücken geschlossen. So ist es häufig die unmittelbare Konfrontation mit einer erfolgreich durchgeführten Cyber-Attacke, die Unternehmen in diesem Bereich tätig werden lässt. Mit der Höhe des entstandenen Schadens steigt meist auch die

[67] BSI (2014a), S. 37
[68] Ziercke, J. (2016), S. 235-237
[69] PwC (2017), S. 4-11; Ziercke, J. (2016), S. 238

Motivation sich für Cyber-Sicherheitsmaßnahmen stark zu machen und dahingehende Anstrengungen zu unternehmen, um sich künftig gegen diese Vorfälle zu schützen. In vielen Fällen kann auch die Einführung von staatlichen Auflagen und Regulierungen, wie der Erlass der NIS-Richtlinie oder die Verabschiedung des IT-Sicherheitsgesetzes, den ausschlaggebenden Anstoß für den Aufbau einer Cyber-Sicherheitsarchitektur geben[70]. Eine weitere Problematik ist außerdem die mangelhafte Strafverfolgung in diesem Bereich. Um eine Verbesserung hinsichtlich der derzeit noch geringen Aufklärungsquote zu erreichen und die hohe Dunkelziffer von nicht gemeldeten Cyber-Angriffen zu verringern, sollten die Unternehmen zukünftig stärker in die Pflicht genommen werden, Cyber-Angriffe bei staatlichen Stellen und Strafverfolgungsbehörden zur Anzeige zu bringen. Viele Unternehmen verweigern sich diesem Schritt zurzeit noch, da sie einen Reputationsverlust befürchten oder ohnehin einen Ermittlungserfolg der zuständigen Behörden ausschließen. Dieser Trugschluss führt jedoch dazu, dass die Täter ungehindert weitere Straftaten begehen können, ohne dafür zur Rechenschaft gezogen zu werden. Zugleich wird durch die fehlende Anzeige von gescheiterten oder erfolgreich durchgeführten Cyber-Angriffen die Diskrepanz zu den tatsächlich gemeldeten Straftaten immer größer. Dies stellt wiederum eine große Problematik dar, denn um eine effektive Bekämpfung zu gewährleisten, gilt eine möglichst realitätsnahe Einschätzung der Bedrohungslage als Grundvoraussetzung[71]. Allgemein zeigt sich somit, dass das Thema Cyber-Sicherheit vor dem Hintergrund einer immer dynamischer und komplexer werdenden internen und externen Umwelt, eine äußerst umfangreiche Aufgabe ist, bei der verschiedenen Parteien eine Schlüsselrolle zukommt. Zudem wird deutlich, dass das Cyber-Risiko nicht isoliert zu betrachtet ist. Auch wenn Privatanwender in diesem Diskussionspapier nicht im Vordergrund stehen, sollte ein allumfassender Lösungsansatz bereits auf dieser Ebene mit geeigneten Maßnahmen ansetzen und im weiteren Verlauf staatliche Initiativen, Behörden, Wirtschaftsunternehmen wie auch die Wissenschaft und Gesellschaft im Rahmen einer bereichsübergreifenden Zusammenarbeit miteinbeziehen. Um ganzheitliche Cyber-Sicherheit zu gewährleisten sind besonders auf staatlicher Ebene passende Schritte zu entwickeln und umzusetzen. So kann eine Cyber-Sicherheitsstrategie auf Unternehmensebene nur erfolgreich sein, wenn der Staat ausreichende und sichere Rahmenbedingungen für die grundlegenden Netz-und Kommunikationsstrukturen schafft. Auf Unternehmensebene zeigt sich dabei, dass der Entwicklungsprozess einer Cyber-Strategie möglicherweise nicht so gradlinig verläuft, wie in der Theorie dargelegt. Es ist durchaus möglich, dass einzelne Entwicklungsschritte und Maßnahmen mehrmals durchzuführen oder an die sich verändernde Umwelt anzupassen sind. Der Strategieentwicklungsprozess ist demzufolge als Kreislauf zu betrachten, der in Hinblick auf immer komplexer werdende Technologien und Bedrohungsformen ständig verbessert und weiterentwickelt werden sollte. Ob und in welchem Ausmaß ein Unternehmen in der Lage ist, entsprechende Strategien und Methoden zu entwickeln und umzusetzen, hängt unter anderem in hohem Maß von der individuellen Ressourcenausstattung im finanziellen, technischen, physischen, organisatorischen und personellen Bereich ab. Grundsätzlich gibt es demnach lediglich Handlungsempfehlungen, jedoch keinen universellen Lösungsweg, der bereichs-und unternehmensübergreifend Anwendung finden kann, denn jedes

[70] Bartsch, M. / Frey, S. (2017), S. 77-78
[71] Ziercke, J. (2016), S. 238

Unternehmen ist in seinen Strukturen, Abläufen und Ressourcen ein einzigartiges Konstrukt. Bei der Entwicklung und Implementierung einer umfassenden Cyber-Sicherheitsstrategie sollten diese individuellen Gegebenheiten berücksichtigt werden.

5. Fazit und Ausblick

Das vorliegende Diskussionspapier zeigt, dass der Cyber-Sicherheit vor dem Hintergrund der Digitalisierung und dem stetigen Fortschritt in der IuK-Technologie eine immer größere Bedeutung zukommt. Im Rahmen einer Einführung in die Thematik wurde dabei zunächst ein Überblick über die aktuellen Bedrohungsformen, Täter und Motive gegeben sowie, durch die Bezugnahme zu aktuellen Studien, sowie die Bedrohungslage bzgl. der Cyber-Risiken abgeschätzt. Hier zeigte sich, dass nicht nur Cyber-Angriffe an sich, sondern auch die Täterstrukturen immer komplexer werden und somit eine zunehmende Bedrohung für Staat, Wirtschaft und Gesellschaft, aber auch Privatanwender darstellen. So sieht sich auch Deutschland mit einer steigenden Zahl an Cyber-Angriffen konfrontiert. Verschiedene Studien belegen, dass hierzulande bereits ein Großteil der Unternehmen Ziel eines entsprechenden Angriffs war. Trotz dieser Entwicklung bleibt die Implementierung von Sicherheitsmaßnahmen in vielen Fällen hinter den Erwartungen zurück. In diesem Zusammenhang wurde der Fokus anschließend auf das Thema Cyber-Sicherheit gelenkt. An dieser Stelle wurde nach einer anfänglichen Definition des Sicherheitsbegriffs und einer Erläuterung der Schutzziele speziell auf die staatlichen Maßnahmen zur Erhöhung der Cyber-Sicherheit eingegangen. Es wurde deutlich, dass der Gesetzgeber seit einiger Zeit verstärkt darauf drängt, geeignete Rahmenbedingungen zu schaffen. Darüber hinaus wird sich durch die Etablierung verschiedener Initiativen und Informationsangebote immer mehr dafür eingesetzt, Lösungsansätze und Hilfestellungen für Wirtschaft und Gesellschaft bereitzustellen. Besonders dem BSI kommt hier eine maßgebliche Bedeutung zu. Im weiteren Verlauf des Diskussionspapieres wurde schließlich die Konzeptionierung einer Cyber-Sicherheitsstrategie auf Unternehmensebene dargestellt. Dazu wurden drei wesentliche Schritte des Strategieentwicklungsprozesses herausgearbeitet. So sollte zu Beginn idealerweise eine genaue Analyse der unternehmensinternen Strukturen und Abläufe stattfinden. Auf Basis der identifizierten Schwachstellen und der definierten strategischen Ziele sollten im Folgenden die Handlungsfelder und Meilensteine bestimmt werden und im Zuge der Umsetzungsplanung eine Festlegung und Strukturierung der zu ergreifenden Maßnahmen und Ressourcen erfolgen. In diesem Zusammenhang wurden im Anschluss einige der wichtigsten Ansätze zur Erhöhung der Cyber-Sicherheit erläutert. Vor allem präventiv können Unternehmen eine Vielzahl von Möglichkeiten wahrnehmen, um Cyber-Attacken zu verhindern, das Schadenspotential zu senken oder im Ernstfall schneller und effektiver zu reagieren. Im Kontext der abschließenden Diskussion zeigte sich insbesondere, dass die Lösungsansätze und Strategien stark von der unternehmensinternen Ressourcenausstattung abhängen. Die in diesem Diskussionspapier herausgestellten Aspekte sind dabei als eine grundsätzliche Handlungsempfehlung zu betrachten, deren detaillierte Umsetzung schlussendlich im Ermessen des zuständigen Unternehmens liegt. Neben technischen, organisatorischen und finanziellen Aspekten haben hauptsächlich Mitarbeiter durch ihr Verhalten und die Wahl ihrer Handlungen einen großen Einfluss auf die interne Cyber-Sicherheit. Aber auch staatlichen Initiativen kommt eine große Verantwortung zu. So sollten geeignete Rahmenbedingungen geschaffen und ausgebaut werden, um die

Sicherheit der Kommunikations-und Netzstrukturen zu fördern. Ob und in welcher Weise dies gelingen wird, hängt in erster Linie auch von bereichsübergreifenden, kooperativen Programmen auf nationaler und internationaler Ebene ab. Allgemein sollten alle Beteiligten im Kampf gegen Cyber-Bedrohungen zukünftig stärker zusammenarbeiten, um in diesem dynamischen Prozess einer sich ständig verändernden Umwelt, einer zunehmenden Vernetzung und immer komplexer werdender Angriffsformen, die Verarbeitung, Speicherung und Übermittlung digitaler Informationen und Daten sicherer zu gestalten und Systeme, Anwendungen und Prozesse zu schützen. Vor allem die zunehmende Einbindung neuartiger Technologien, wie die Nutzung von Cloud-Diensten, dürfte neue Fragen hinsichtlich der Cyber-Sicherheit aufwerfen und die Verantwortlichen bei der Entwicklung und Implementierung entsprechender Konzepte vor große Herausforderung stellen. Hier sollten letztlich auch die Hersteller und Anbieter der Technologien stärker in die Pflicht genommen werden.

6. Literaturverzeichnis

Allianz Deutschland AG (Hrsg.) (2016): Rote Karte für Hacker, URL: https://www.allianzdeutschland.de/cyberschutz-/id_78393612/index, letztmalig aufgerufen am 14.11.2018.

Bartsch, M. / Frey, S. (2017): Cyberstrategien für Unternehmen und Behörden - Maßnahmen zur Erhöhung der Cyberresilienz, Wiesbaden.

Biener, C. / Eling, M. / Matt, A. / Wirfs, J.H. (2015): Cyber Risk: Risikomanagement und Versicherbarkeit, in: Institut für Versicherungswirtschaft der Universität St. Gallen (Hrsg.), IVW-HSG-Schriftenreihe, 54. Auflage, St. Gallen.

Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Hrsg.) (2017): Wirtschaftsschutz in der digitalen Welt, URL: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf, letztmalig aufgerufen am 14.11.2018.

BMI - Bundesministerium des Innern, für Bau und Heimat (Hrsg.) (2016): Cyber-Sicherheitsstrategie für Deutschland 2016, URL: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStra-tegie.pdf, letztmalig aufgerufen am 14.11.2018.

BMWi - Bundesministerium für Wirtschaft und Energie (Hrsg.) (2018): Europäische Datenschutz-Grundverordnung, URL: https://www.bmwi.de/Re-daktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverord-nung.html, letztmalig aufgerufen am 14.11.2018.

Böhme, R. / Kataria, G. (2006): Models and Measures for Correlation in Cyber-insurance, Proceedings of the Workshop on the Economics of Information Security (WEIS), Cambridge.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2008): BSI-Standard 100-4 – Notfallmanagement, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=1, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2011): Leitfaden „IT-Forensik" - Version 1.0.1 (März 2011), URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2014a): Die Lage der IT-Sicherheit in Deutschland 2014, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2014b): Leitfaden Cyber-Sicherheits-Check, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden-Cyber-Sicherheits-Check.pdf?__blob=publicationFile&v=2, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2016a): Das IT-Sicherheitsgesetz, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=7, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2016b): IT-Grundschutz-Kataloge: 15. Ergänzungslieferung - 2016, URL: https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2017): Die Lage der IT-Sicherheit in Deutschland 2017, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=3, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2018a): Gesetz zur Umsetzung der NIS-Richtlinie, URL: https://www.bsi.bund.de/DE/Das-BSI/NIS-Richtlinie/NIS_Richtlinie_node.html, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2018b): ISO 27001 Zertifizierung auf Basis von IT-Grundschutz, URL: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html, letztmalig aufgerufen am 14.11.2018.

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2018c): Cyber-Sicherheit, URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html, letztmalig aufgerufen am 14.11.2018.

Callegati, F. / Cerroni, W. / Ramilli, M. (2009): Man-in-the-Middle Attack to the HTTPS Protocol, in: IEEE Security & Privacy, 7. Jg., Heft 1, S. 78-81.

Dolle, W. (2009): Computer-Forensik in der Praxis - Mit Open-Source-Werkzeugen die Aufklärung von Computerkriminalität unterstützen, in: Datenschutz und Datensicherheit, 33. Jg., Heft 3, S. 183-188.

Dreo Rodosek, G. / Golling, M. (2013): Cyber Security: Challenges and Application Areas, in: Essig, M. / Hülsmann, M. / Kern, E.-M. / Klein-Schmeink, S. (Hrsg.), Supply Chain Safety Management - Security and Robustness in Logistics, 1. Auflage, Berlin, Heidelberg, S. 179-197.

DTTL - Deloitte Touche Tohmatsu Limited (Hrsg.) (2014): Rüstzeug für das Topmanagement - Aufbau eines effektiven Cyber-Security-Programms, URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/audit/Cyber-Broschuere-Ruestzeug-fuer-Topmanagement.pdf, letztmalig aufgerufen am 14.11.2018.

DTTL - Deloitte Touche Tohmatsu Limited (Hrsg.) (2018): Cyber Risk Services, URL: https://www2.deloitte.com/de/de/pages/risk/solutions/cyberrisk.html#, letztmalig aufgerufen am 14.11.2018.

Fraunhofer - Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. (Hrsg.) (2014): Strategie- und Positionspapier Cyber-Sicherheit 2020: Herausforderungen für die IT-Sicherheitsforschung, URL: https://www.iese.fraunhofer.de/content/dam/iese/de/dokumente/Fraunhofer-Strategie-und_Positionspapier_Cyber-Sicherheit2020.pdf, letztmalig aufgerufen am 14.11.2018.

GDV - Gesamtverband der Deutschen Versicherungswirtschaft e. V. (Hrsg.) (2017): So funktioniert die Cyberversicherung für den Mittelstand, URL: https://www.gdv.de/de/themen/news/so-funktioniert-die-cyberversicherung-fuer-den-mittelstand-4706, letztmalig aufgerufen am 14.11.2018.

Gu, G. / Perdisci, R. / Zhang, J. / Lee, W. (2008): BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection, in: 17th Usenix Security Symposium, San Jose, S. 139-154.

Hagenloch, E. / Müller, S. / Scherber, M. (2013): Organisatorische Umsetzung, in: Bayer, F. / Kühn, H. (Hrsg.), Prozessmanagement für Experten, Berlin, Heidelberg, S. 225-247.

Herwig, V. / Schlabitz, L. (2004): Unternehmensweites Berechtigungsmanagement, in: Wirtschaftsinformatik, 46. Jg., Heft 4, S. 289-294.

HiSolutions AG (Hrsg.) (2018): Security Consulting, URL: https://www.hisolutions.com/security-consulting/, letztmalig aufgerufen am 14.11.2018.

Hochkommissariat für nationale Sicherheit (Hrsg.) (2016): Definition der Cyber-Sicherheit, URL: https://www.infocrise.lu/de/web/guest/cyber-definition-cyber-sicherheit, letztmalig aufgerufen am 14.11.2018.

Hungerland, F. / Pflüger, W. / Funken, J. / Vöpel, H. (2016): Sicherheit, in: Hamburgisches WeltWirtschaftsInstitut und Berenberg (Hrsg.), Strategie 2030 - Vermögen und Leben in der nächsten Generation, 22. Auflage, Hamburg.

ISO - International Organization for Standardization (Hrsg.) (2012): ISO/IEC 27032:2012, Information technology - Security techniques - Guidelines for cybersecurity, Genf.

Kersten, H. / Reuter, J. / Schröder, K.-W. (2013): IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz - Der Weg zur Zertifizierung, 4. Auflage, Wiesbaden.

Klipper, S. (2015a): Cyber Security - Ein Einblick für Wirtschaftswissenschaftler, Wiesbaden.

Klipper, S. (2015b): Information Security Risk Management - Risikomanagement mit ISO/IEC 27001, 27005 und 31010, 2. Auflage, Wiesbaden.

Knoll, M. (2017): IT-Risikomanagement im Zeitalter der Digitalisierung, in: HMD Praxis der Wirtschaftsinformatik, 54. Jg., Heft 1, S. 4-20.

Königs, H.-P. (2017): IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken, 5. Auflage, Wiesbaden.

KPMG AG (Hrsg.) (2017): Neues Denken, Neues Handeln: Insurance Thinking Ahead - Versicherungen im Zeitalter von Digitalisierung und Cyber. Studienteil B: Cyber, URL: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-cyber-de.pdf, letztmalig aufgerufen am 14.11.2018.

Krcmar, H. (2015): Informationsmanagement, 6. Auflage, Berlin, Heidelberg.

Li, Q. / Clark, G. (2013): Mobile Security: A Look Ahead, in: IEEE Security & Privacy, 11. Jg., Heft 1, S. 78-81.

Mertens, P. / Bodendorf, F. / König, W. / Schumann, M. / Hess, T. / Buxmann, P. (2017): Grundzüge der Wirtschaftsinformatik, 12. Auflage, Berlin.

Mouton, F. / Leenen, L. / Venter, H.S. (2016): Social Engineering Attack Examples, Templates and Scenarios, in: Computers & Security, 59. Jg., Heft C, S. 186-209.

Mukhopadhyay, A. / Saha, D. / Mahanti, A. / Chakrabarti, B.B. / Podder, A. (2005): Insurance for Cyber-Risk: A Utility Model, in: Decision, 32. Jg., Heft 1, S. 153-169.

Mukhopadhyay, A. / Chatterjee, S. / Saha, D. / Mahanti, A. / Sadhukan, S.K. (2013): Cyberrisk Decision Models: To insure IT or not? in: Decision Support Systems, 56. Jg., Heft 1, S. 11-26.

Pöchtrager, S. / Wagner, W. (2018): Von der Idee zum Businessplan - Geschäftsideen in der Agrar- und Ernährungswirtschaft erfolgreich umsetzen mit Beispielen aus Österreich, Wiesbaden.

Pohlmann, N. (2016): Zur Entwicklung einer IT-Sicherheitskultur - Wie das IT-Sicherheitsgesetz den gesellschaftlichen Umgang mit IT-Risiken fördern kann, in: Datenschutz und Datensicherheit, 40. Jg., Heft 1, S. 38-42.

PwC - PricewaterhouseCoopers AG (Hrsg.) (2017): Im Visier der Cyber-Gangster - So gefährdet ist die Informationssicherheit im deutschen Mittel-tand, URL: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf, letztmalig aufgerufen am 14.11.2018.

Refsdal, A. / Solhaug, B. / Stolen, K. (2015): Cyber-Risk Management, Cham, Heidelberg.

Sauerbrey, A. / Jansen, F. / Salzen, C. von / Alvarez, S. / Voss, O. (2018): Cyber-Angriff: Unter russischer Beobachtung, URL: https://www.tagesspiegel.de/politik/cyber-angriff-unter-russischer-beobachtung/21021564.html, letztmalig aufgerufen am 14.11.2018.

Sternad, D. (2015): Strategieentwicklung kompakt - Eine praxisorientierte Einführung, Wiesbaden.

Verlag Dierichs GmbH & Co KG (Hrsg.) (2018): Die neue Datenschutz Grund-verordnung (DSGVO) - Das müssen Sie wissen, URL: https://www.hna.de/netzwelt/eu-datenschutz-grundverordnung-dsgvo-muessen-sie-wissen-9828468.html, letztmalig aufgerufen am 14.11.2018.

Wiedemer, A. / Hochenrieder, M. (2015): Mehr Transparenz – höheres Risiko: Sicherheit für Unternehmen im Web, in: Linnhoff-Popien, C. / Zaddach, M. / Grahl, A. (Hrsg.), Marktplätze im Umbruch - Digitale Strategien für Services im Mobilen Internet, Berlin, Heidelberg, S. 679-689.

Wolf, E. / Appelhans, L. / Klose, R. (2013): Organisatorische Prozessoptimierung, in: Bayer, F. / Kühn, H. (Hrsg.), Prozessmanagement für Experten - Impulse für aktuelle und wiederkehrende Themen, Berlin, Heidelberg, S. 203-221.

Yu, S. (2014): Distributed Denial of Service Attack and Defense, New York.

Ziercke, J. (2016): Cybercrime als Herausforderung für die Internetgesellschaft, in: Bär, C. / Fischer, A. / Gulden, H. (Hrsg.), Informationstechnologien als Wegbereiter für den steuerberatenden Berufsstand, Berlin, Heidelberg, S. 229-241.

IWI Discussion Paper Series/Diskussionsbeiträge
ISSN 1612-3646

Michael H. Breitner, Rufus Philip Isaacs and the Early Years of Differential Games, 36 S., #1, 22. Januar 2003.

Gabriela Hoppe und Michael H. Breitner, Classification and Sustainability Analysis of e-Learning Applications, 26 S., #2, 13. Februar 2003.

Tobias Brüggemann und Michael H. Breitner, Preisvergleichsdienste: Alternative Konzepte und Geschäftsmodelle, 22 S., #3, 14. Februar 2003.

Patrick Bartels und Michael H. Breitner, Automatic Extraction of Derivative Prices from Webpages using a Software Agent, 32 S., #4, 20. Mai 2003.

Michael H. Breitner und Oliver Kubertin, WARRANT-PRO-2: A GUI-Software for Easy Evaluation, Design and Visualization of European Double-Barrier Options, 35 S., #5, 12. September 2003.

Dorothée Bott, Gabriela Hoppe und Michael H. Breitner, Nutzenanalyse im Rahmen der Evaluation von E-Learning Szenarien, 14 S., #6, 21. Oktober 2003.

Gabriela Hoppe und Michael H. Breitner, Sustainable Business Models for E-Learning, 20 S., #7, 05. Januar 2004.

Heiko Genath, Tobias Brüggemann und Michael H. Breitner, Preisvergleichsdienste im internationalen Vergleich, 40 S.,#8, 21. Juni 2004.

Dennis Bode und Michael H. Breitner, Neues digitales BOS-Netz für Deutschland: Analyse der Probleme und mögliche Betriebskonzepte, 21 S. #9, 05. Juli 2004.

Caroline Neufert und Michael H. Breitner, Mit Zertifizierungen in eine sicherere Informationsgesellschaft, 19 S., #10, 05. Juli 2004.

Marcel Heese, Günter Wohlers und Michael H. Breitner, Privacy Protection against RFID Spying: Challenges and Countermeasures, 22 S., #11, 05. Juli 2004.

Liina Stotz, Gabriela Hoppe und Michael H. Breitner, Interaktives Mobile(M)-Learning auf kleinen Endgeräten wie PDAs and Smartphones, 31 S., #12, 18. August 2004.

Frank Köller und Michael H. Breitner, Optimierung von Warteschlangensystemen in Call Centern auf Basis von Kennzahlenapproximationen, 24 S., #13, 10. Januar 2005.

Phillip Maske, Patrick Bartels und Michael H. Breitner, Interactive M(obile)-Learning with UbiLearn 0.2, 21 S., #14, 20. April 2005.

Robert Pomes und Michael H. Breitner, Strategic Management of Information Security in State-run Organizations, 18 S., #15, 05. Mai 2005.

Simon König, Frank Köller und Michael H. Breitner, FAUN 1.1 User Manual, 134 S., #16, 04. August 2005.

Christian von Spreckelsen, Patrick Bartels und Michael H. Breitner, Geschäftsprozessorientierte Analyse und Bewertung der Potentiale des Nomadic Computing, 38 S., #17, 14. Dezember 2006.

Stefan Hoyer, Robert Pomes, Günter Wohlers und Michael H. Breitner, Kritische Erfolgsfaktoren für ein Computer Emergency Response Team (CERT) am Beispiel CERT-Niedersachsen, 56 S., #18, 14. Dezember 2006.

Christian Zietz, Karsten Sohns und Michael H. Breitner, Konvergenz von Lern-, Wissens-und Personalmanagementssystemen: Anforderungen an Instrumente für integrierte Systeme, 15 S., #19, 14. Dezember 2006.

Christian Zietz und Michael H. Breitner, Expertenbefragung „Portalbasiertes Wissensmanagement“: Ausgewählte Ergebnisse, 30 S., #20, 05. Februar 2008.

Harald Schömburg und Michael H. Breitner, Elektronische Rechnungsstellung: Prozesse, Einsparpotentiale und kritische Erfolgsfaktoren, 36 S., #21, 05. Februar 2008.

Halyna Zakhariya, Frank Köller und Michael H. Breitner, Personaleinsatzplanung im Echtzeitbetrieb in Call Centern mit Künstlichen Neuronalen Netzen, 35 S., #22, 05. Februar 2008.

Jörg Uffen, Robert Pomes, Claudia M. König und Michael H. Breitner, Entwicklung von Security Awareness Konzepten unter Berücksichtigung ausgewählter Menschenbilder, 14 S., #23, 05. Mai 2008.

Johanna Mählmann, Michael H. Breitner und Klaus-Werner Hartmann, Konzept eines Centers der Informationslogistik im Kontext der Industrialisierung von Finanzdienstleistungen, 19 S., #24, 05. Mai 2008.

Jon Sprenger, Christian Zietz und Michael H. Breitner, Kritische Erfolgsfaktoren für die Einführung und Nutzung von Portalen zum Wissensmanagement, 44 S., #25, 20. August 2008.

Finn Breuer und Michael H. Breitner, „Aufzeichnung und Podcasting akademischer Veranstaltungen in der Region D-A-CH": Ausgewählte Ergebnisse und Benchmark einer Expertenbefragung, 30 S., #26, 20. August 2008.

Harald Schömburg, Gerrit Hoppen und Michael H. Breitner, Expertenbefragung zur Rechnungseingangsbearbeitung: Status quo und Akzeptanz der elektronischen Rechnung, 40 S., #27, 15. Oktober 2008.

Hans-Jörg von Mettenheim, Matthias Paul und Michael H. Breitner, Akzeptanz von Sicherheitsmaßnahmen: Modellierung, Numerische Simulation und Optimierung, 30 S., #28, 16. Oktober 2008.

Markus Neumann, Bernd Hohler und Michael H. Breitner, Bestimmung der IT-Effektivität und IT-Effizienz serviceorientierten IT-Managements, 20 S., #29, 30. November 2008.

Matthias Kehlenbeck und Michael H. Breitner, Strukturierte Literaturrecherche und -klassifizierung zu den Forschungsgebieten Business Intelligence und Data Warehousing, 10 S., #30, 19. Dezember 2009.

Michael H. Breitner, Matthias Kehlenbeck, Marc Klages, Harald Schömburg, Jon Sprenger, Jos Töller und Halyna Zakhariya, Aspekte der Wirtschaftsinformatikforschung 2008, 128 S., #31, 12. Februar 2009.

Sebastian Schmidt, Hans-Jörg v. Mettenheim und Michael H. Breitner, Entwicklung des Hannoveraner Referenzmodels für Sicherheit und Evaluation an Fallbeispielen, 30 S., #32, 18. Februar 2009.

Sissi Eklu-Natey, Karsten Sohns und Michael H. Breitner, Buildung-up Human Capital in Senegal -E-Learning for School drop-outs, Possibilities of Lifelong Learning Vision, 39 S., #33, 01. Juli 2009.

Horst-Oliver Hofmann, Hans-Jörg von Mettenheim und Michael H. Breitner, Prognose und Handel von Derivaten auf Strom mit Künstlichen Neuronalen Netzen, 34 S., #34, 11. September 2009.

Christoph Polus, Hans-Jörg von Mettenheim und Michael H. Breitner, Prognose und Handel von Öl-Future-Spreads durch Multi-Layer-Perceptrons und High-Order-Neuronalnetze mit Faun 1.1 , 55 S., #35, 18. September 2009

Jörg Uffen und Michael H. Breitner, Stärkung des IT-Sicherheitsbewusstseins unter Berücksichtigung psychologischer und pädagogischer Merkmale, 37 S., #36, 24. Oktober 2009.

Christian Fischer und Michael H. Breitner, MaschinenMenschen – reine Science Fiction oder bald Realität? 36 S., #37, 13. Dezember 2009.

Tim Rickenberg, Hans-Jörg von Mettenheim und Michael H. Breitner, Plattformunabhängiges Softwareengineering eines Transportmodells zur ganzheitlichen Disposition von Strecken-und Flächenverkehren, 38 S., #38, 11. Januar 2010.

Björn Semmelhaack, Jon Sprenger und Michael H. Breitner, Ein ganzheitliches Konzept für Informationssicherheit unter besonderer Berücksichtigung des Schwachpunktes Mensch, 56 S., #39, 03. Februar 2009.

Markus Neumann, Achim Plückebaum, Jörg Uffen und Michael H. Breitner, Aspekte der Wirtschaftsinformatikforschung 2009, 70 S., #40, 12. Februar 2010.

Markus Neumann, Bernd Hohler und Michael H. Breitner, Wertbeitrag interner IT – Theoretische Einordnung und empirische Ergebnisse, 38 S., #41, 31. Mai 2010.

Daniel Wenzel, Karsten Sohns und Michael H. Breitner, Open Innovation 2.5: Trendforschung mit Social Network Analysis, 46 S., #42, 01. Juni 2010.

Naum Neuhaus, Karsten Sohns und Michael H. Breitner, Analyse der Potenziale betrieblicher Anwendungen des Web Content Mining, 44 S., #43, 08. Juni 2010.

IWI Discussion Paper Series/Diskussionsbeiträge
ISSN 1612-3646

Ina Friedrich, Jon Sprenger und Michael H. Breitner, Discussion of a CRM System Selection Approach wih Experts: Selected Results from an Empirical Study, 22 S., #44, 15. November 2010.

Jan Bührig, Angelica Cuylen, Britta Ebeling, Christian Fischer, Nadine Guhr, Eva Hagenmeier, Stefan Hoyer, Cornelius Köpp, Lubov Lechtchinskaia, Johanna Mählmann und Michael H. Breitner, Aspekte der Wirtschaftsinformatikforschung 2010, 202 S., #45, 03. Januar 2011.

Philipp Maske und Michael H. Breitner, Expertenbefragung: Integrierte, interdisziplinäre Entwicklung von M(obile)-Learning Applikationen, 42 S., #46, 28. Februar 2011.

Christian Zietz, Jon Sprenger und Michael H. Breitner, Critical Success Factors of Portal-Based Knowledge Management, 18 S., #47, 04. Mai 2011.

Hans-Jörg von Mettenheim, Cornelius Köpp, Hannes Munzel und Michael H. Breitner, Integrierte Projekt-und Risikomanagementunterstützung der Projektfinanzierung von Offshore-Windparks, 18 S., #48, 22. September 2011.

Christoph Meyer, Jörg Uffen und Michael H. Breitner, Discussion of an IT-Governance Implementation Project Model Using COBIT and Val IT, 18 S., #49, 22. September 2011.

Michael H. Breitner, Beiträge zur Transformation des Energiesystems 2012, 31 S., #50, 12. Februar 2012.

Angelica Cuylen und Michael H. Breitner, Anforderungen und Herausforderungen der elektronischen Rechnungsabwicklung: Expertenbefragung und Handlungsempfehlungen, 50 S., #51, 05. Mai 2012

Helge Holzmann, Kim Lana Köhler, Sören C. Meyer, Marvin Osterwold, Maria-Isabella Eickenjäger und Michael H. Breitner, Plinc. Facilitates linking. – Ein Accenture Campus Challenge 2012 Projekt, 98 S., #52, 20. August 2012.

André Koukal und Michael H. Breitner, Projektfinanzierung und Risikomanagement Projektfinanzierung und Risikomanagement von Offshore-Windparks in Deutschland, 40 S., #53, 31. August 2012.

Halyna Zakhariya, Lubov Kosch und Michael H. Breitner, Concept for a Multi-Criteria Decision Support Framework for Customer Relationship Management System Selection, 14 S., #55, 22. Juli 2013.

Tamara Rebecca Simon, Nadine Guhr und Michael H. Breitner, User Acceptance of Mobile Services to Support and Enable Car Sharing: A First Empirical Study, 19 S., #56, 01. August 2013.

Tim A. Rickenberg, Hans-Jörg von Mettenheim und Michael H. Breitner, Design and implementation of a decision support system for complex scheduling of tests on prototypes, 6 S. #57, 19. August 2013.

Angelica Cuylen, Lubov Kosch, Valentina, Böhm und Michael H. Breitner, Initial Design of a Maturity Model for Electronic Invoice Processes, 12 S., #58, 30. August 2013.

André Voß, André Koukal und Michael H. Breitner, Revenue Model for Virtual Clusters within Smart Grids, 12 S., #59, 20. September 2013.

Benjamin Küster, André Koukal und Michael H. Breitner, Towards an Allocation of Revenues in Virtual Clusters within Smart Grids, 12 S., #60, 30. September 2013.

My Linh Truong, Angelica Cuylen und Michael H. Breitner, Explorative Referenzmodellierung interner Kontrollverfahren für elektronische Rechnungen, 30 S., #61, 01. Dezember 2013.

Cary Edwards, Tim Rickenberg und Michael H. Breitner, Innovation Management: How to drive Innovation through IT – A conceptual Mode, 34 S., #62, 29. November 2013.

Thomas Völk, Kenan Degirmenci und Michael H. Breitner, Market Introduction of Electric Cars: A SWOT Analysis, 13 S., #63, 11. Juli 2014.

Cary Edwards, Tim A. Rickenberg und Michael H. Breitner, A Process Model to Integrate Data Warehouses and Enable Business Intelligence: An Applicability Check within the Airline Sector, 14 S., #64, 11. November 2014.

Mina Baburi, Katrin Günther, Kenan Degirmenci und Michael H. Breitner, Gemeinschaftsgefühl und Motivationshintergrund: Eine qualitative Inhaltsanalyse im Bereich des Elektro-Carsharing, 53 S., #65, 18. November 2014.

IWI Discussion Paper Series/Diskussionsbeiträge
ISSN 1612-3646

Mareike Thiessen, Kenan Degirmenci und Michael H. Breitner, Analyzing the Impact of Drivers' Experience with Electric Vehicles on the Intention to Use Electric Carsharing: A Qualitative Approach, 22 S., #66, 2. Dezember 2014.

Mathias Ammann, Nadine Guhr und Michael H. Breitner, Design and Evaluation of a Mobile Security Awareness Campaign – A Perspective of Information Security Executives, 22 S., #67, 15. Juni 2015.

Raphael Kaut, Kenan Degirmenci und Michael H. Breitner, Elektromobilität in Deutschland und anderen Ländern: Vergleich von Akzeptanz und Verbreitung, 75 S., #68, 29. September 2015.

Kenan Degirmenci und Michael H. Breitner, A Systematic Literature Review of Carsharing Research: Concepts and Critical Success Factors, 12 S., #69, 29. September 2015.

Theresa Friedrich, Nadine Guhr und Michael H. Breitner, Führungsstile: Literaturrecherche und Ausblick für die Informationssicherheitsforschung, 29 S., #70, 29. November 2015.

Maximilian Kreutz, Phillip Lüpke, Kathrin Kühne, Kenan Degirmenci und Michael H. Breitner, Ein Smartphone-Bonussystem zum energieeffizienten Fahren von Carsharing–Elektrofahrzeugen, 11 S., #71, 09. Dezember 2015.

Marc-Oliver Sonneberg, Danny Wei Cao und Michael H. Breitner, Social Network Usage of Financial Institutions: A SWOT Analysis based on Sparkasse, 12 S., #72, 14. Januar 2016.

Jan Isermann, Kathrin Kühne und Michael H. Breitner, Comparison of Standard and Electric Carsharing Processes and IT-Infrastructures, 21 S., #73, 19. Februar 2016.

Sonja Dreyer, Sören C. Meyer und Michael H. Breitner, Development of a Mobile Application for Android to Support Energy-Efficient Driving of Electric Vehicles, 15 S., #74, 29. Februar 2016.

Claudia M. König und Michael H. Breitner, Abschlussbericht des KIQS-Projekts „Verbesserung der Koordination von, der Interaktion Studierende-Lehrende in und der Integration aller Lehrinhalte in sehr großer/n Lehrveranstaltungen im Bachelor Grundstudium", 45 S., #75, 17. April 2016.

Wilhelm G. N. Jahn, Kenan Degirmenci und Michael H. Breitner, Portallösungen für Elektro-Carsharing: Stakeholderanalyse und Konzepte, 80 S., #76, 12. Mai 2016.

Mareike Thiessen, Kenan Degirmenci und Michael H. Breitner, Electric Carsharing Usage and Shifting Effects between Public Transport, Car Ownership, Carsharing, and Electric Carsharing: A Data Mining Analysis and a Survey of Electric Carsharing Users, 128 S., #77, 12. Mai 2016.

Bjarne Neels, Marc-Oliver Sonneberg und Michael H. Breitner, IKT-basierte Geschäftsmodellinnovationen im Gütertransport: Marktübersicht und Analyse, 31 S., #78 6. Oktober 2016.

Ines Thurk, Nadine Guhr und Michael H. Breitner, Unterstützung des Wissensmanagments mit Electronic Learning – Eine Literaturanalyse, 22 S., #79, 30. Oktober 2016.

Vie Kien Dang, Marc-Oliver Sonneberg und Michael H. Breitner, Analyse innovativer Logistikkonzepte für urbane Paketdienstleister, 66 S., #80, 03. November 2016.

Christoph Thermann, Marc-Oliver Sonneberg and Michael H. Breitner, Visualisierung von Verkehrsdaten der Landeshauptstadt Hannover, 16 p., #81, February 17, 2017.

Rouven-B. Wiegard, Kenan Degirmenci and Michael H. Breitner, What Influences the Adoption of Electronic Medical Record Systems? An Empirical Study with Healthcare Organizations Executives, 28 p., #82, May 30, 2017.

Jens Passlick, Sonja Dreyer, Daniel Olivotti, Benedikt Lebek and Michael H. Breitner, Assessing Research Projects: A Framework, 13 p., #83, February 5, 2018.

Michael Stieglitz, Marc-Oliver Sonneberg and Michael H. Breitner, TCO-Comparison of Fuel and Electric Powered Taxis: Recommendations for Hannover, 30 p., #84, June 2, 2018.