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)

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

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.