Versicherbarkeit von Cyber-Risiken?

Reader zum Studienprojekt

„Versicherbarkeit von Cyber-Risiken“

Prof. Dr. Thomas Hartung

Professur für Versicherungswirtschaft an der
Universität der Bundeswehr München

Winter- und Frühjahrstrimester 2020

der Bundeswehr
Universität München

Inhaltsverzeichnis

Vorwort

Cyber-Risiken gehören zu den sich am schnellsten entwickelnden Risikoarten. Privatpersonen, Gewerbetreibende und Industrieunternehmen stehen gleichermaßen im Fokus vorsätzlich handelnder Krimineller. Phänomene wie Pishing, Ransomware, Denial of Service-Attacken oder Identitätsdiebstahl finden zunehmend mehr Opfer. Hinzu kommen Täuschungsmanöver wie „Fake President"- oder CEO-Fraud, die immer wieder prominente Fälle hervorrufen. Aber auch zufällige Cyber-Ereignisse, wie der Ausfall von Hardware und damit verbundener Datenverlust oder Zerstörung von IT-Infrastruktur können zu erheblichen wirtschaftlichen Schäden führen. Letztlich lässt die zunehmende elektronische Vernetzung der Gesellschaft sowie die rapide fortschreitende Digitalisierung die gleichzeitig anwachsende Verwundbarkeit der damit verbundenen Infrastruktur unvermeidbar erscheinen.

Aus Sicht der Versicherungswirtschaft generierte der kontinuierlich anwachsende Absicherungsbedarf zunächst eine Art Goldgräberstimmung. Vergleiche mit der bisher bedeutendsten Sachversicherung, der Kfz-Versicherung, wurden angestellt, und Prognosen, wann deren Beitragsaufkommen im Cyber-Bereich erreicht würde, wurden mit immer kürzeren Zeiträumen unterlegt. Zwischenzeitlich hat Ernüchterung Einzug gehalten. Etliche Versicherer, die anfangs großzügig im Zeichnungsgebaren auftraten, agieren inzwischen deutlich zurückhaltender und verstärkt wird Versicherung als Bestandteil eines ganzen Bündels von Maßnahmen akzeptiert, das eine Erhöhung der Cyber-Sicherheit bewirken soll. Anlass hierfür waren einige Großschäden, wie beispielsweise die Ransomware „WannaCry" und „NotPetya", die beide 2017 zu weltweiten Schäden jenseits der 10 Mrd. USD führten und damit das Kumulpotential von Cyber-Ereignissen vor Augen führten.

Nichtsdestotrotz bietet die zunehmende Digitalisierung eine Vielzahl neuer Geschäftsmodelle für Versicherungsunternehmen, sorgt aber auch für eine verstärkte Anfälligkeit der daran beteiligten Akteure im Hinblick auf Cyber-Risiken. Ziel im Studienprojekt „Cyber-Risiken" der Professur für Versicherungswirtschaft an der Universität der Bundeswehr München war es deshalb, Cyber-Risiken zu systematisieren, deren grundsätzliche risikopolitische Behandlung tiefgehender zu betrachten und den aktuellen Markt für Cyber-Versicherung zu analysieren. Dabei waren u. a. folgende Fragen von Relevanz:

- Welche konkreten Risiken fallen in die Kategorie Cyber-Risiken? Wie lassen sich Cyber-Risiken kategorisieren?
- Welche Absicherungsmaßnahmen gegen Cyber-Risiken gibt es? Welche Strategien für Cyber-Sicherheit werden vorgeschlagen / umgesetzt?
- Welche Formen der Versicherung von Cyber-Risiken sind per dato

vorzufinden? Welche Herausforderungen bezüglich der Versicherbarkeit existieren?

Die folgenden Beiträge von Studierenden, die einen Teil der Ergebnisse des Studienprojektes darstellen, beschäftigen sich mit verschiedenen Aspekten von Cyber-Risiken. Wir hoffen, mit der Zusammenstellung der Beiträge als Reader einen umfassenden Einblick in die Thematik „Cyber-Risiken und Versicherung“ zu liefern und wünschen viel Vergnügen sowie Erkenntnisse beim Lesen der Beiträge!

Neubiberg, im Dezember 2020
Prof. Dr. Thomas Hartung

Versicherbarkeit von Cyber-Risiken – Cyber-Risiken vor dem Hintergrund der Kriterien der Versicherbarkeit

Von Laura Brobeil

Einleitung

Die fortschreitende Digitalisierung verändert Wirtschaft und Gesellschaft. Menschen werden vernetzter, Geräte smarter. In zehn Jahren werden voraussichtlich 125 Milliarden Geräte online sein – das wären fünfmal so viele wie noch im Jahr 2017. Durch intelligente Maschinen und automatisierte Prozesse profitieren Unternehmen in nahezu allen Branchen von Effizienz- und Produktivitätssteigerungen.[1] Offenbar wächst in der Wirtschaft aber auch das Bewusstsein für mögliche Risiken, die die Digitalisierung mit sich bringt. Laut dem aktuellen Allianz Risk Barometer werden Cyber-Vorfälle weltweit erstmals als wichtigstes Unternehmensrisiko eingeschätzt. Organisationen sehen sich zunehmend mit Datendiebstählen, Cyber-Angriffen und -Erpressungen konfrontiert.[2] Laut Expertenschätzungen werden Unternehmen weltweit durchschnittlich alle 14 Sekunden Opfer von Cyber-Angriffen. Der gesamtwirtschaftliche Schaden, der im Jahr 2018 durch Cyber-Angriffe entstanden ist, wird auf circa 600 Milliarden US-Dollar geschätzt. Für die Versicherungswirtschaft könnten sich durch die Versicherung der neuartigen Cyber-Risiken neue Marktchancen bieten. Allerdings sind einige Branchenvertreter der Meinung, Cyber-Risiken seien nicht versicherbar.[3] In dieser Arbeit wird deshalb untersucht, ob Cyber-Risiken die sog. Kriterien der Versicherbarkeit erfüllen. Um eine Ausgangsbasis zu schaffen, sollen Cyber-Risiken zuerst definiert und in ihren Ursachen abgegrenzt werden. Anschließend wird kurz darauf eingegangen, von welchen Faktoren die Versicherbarkeit eines Risikos abhängt. Danach werden die Kriterien der Versicherbarkeit zunächst erläutert, um daraufhin mögliche Probleme hinsichtlich Cyber-Risiken erörtern zu können. Zuletzt werden die Ergebnisse zusammengefasst und eine Einschätzung zur Versicherbarkeit von Cyber-Risiken gegeben.

Theoretische Grundlagen: Cyber-Risiken und Versicherbarkeit

Begriffsbestimmung und Ursachen des Cyber-Risikos

In der Literatur existiert bereits eine Vielzahl an Definitionen, die den Charakter des Cyber-Risikos aus unterschiedlichen Perspektiven zu beschreiben versuchen.[4] Häufig werden Cyber-Risiken in Anlehnung an operationelle Risiken beschrieben. Cyber-Risiken gelten demnach als „operational risks to information and technology assets that have consequences affecting the

confidentiality, availability, or integrity of information or information systems."[5]

Gemäß den Rahmenbedingungen von Basel II[6] und Solvency II[7] werden operationelle Risiken in die vier Kategorien (1) menschliches Verhalten, (2) Systemfehler, (3) fehlerhafte interne Abläufe und (4) externe Ereignisse unterteilt. Menschliches Fehlverhalten kann aus willentlichen, unwillentlichen oder unterlassenen Handlungen resultieren, während die Ursache für Systemfehler in der Hardware, Software oder den Systemen selbst liegen kann. Für fehlerhafte interne Abläufe können das Design und die Kontrolle von Prozessen sowie sämtliche Unterstützungsprozesse sorgen. Als externe Ereignisse gelten schließlich Katastrophen, rechtliche Änderungen, geschäftsbezogene Probleme und Abhängigkeiten von Dritten.[8]

Das Cyber-Risiko lässt sich auf kriminelle und nicht kriminelle Ursachen zurückführen. Bei kriminellen Ursachen wird in physische Angriffe, Hackerangriffe und Erpressung differenziert, während nicht kriminelle Ursachen höhere Gewalt sowie technisches und menschliches Versagen umfassen.[9]

Versicherbarkeit von Risiken

Neben der erzielbaren Prämie hängt die Entscheidung über die Deckung eines Risikos noch von weiteren Faktoren ab:

1. Dem subjektiven Risikoverhalten des Versicherers.
2. Der individuellen Struktur seines Risikogeschäfts. Diese umfasst die vorhandenen Sicherheitsmittel, die Struktur des bisher versicherten Kollektivs und die Risikopolitik des Versicherers.
3. Die Eigenschaften der zu versichernden Zufallsvariablen.[10]

Das Risikoverhalten und die Gesamtstruktur sind für jeden Versicherer individuell und erlauben deshalb keine allgemeine Diskussion über die Versicherbarkeit von Cyber-Risiken.[11] Vielmehr interessieren die Eigenschaften eines Risikos, die sich erschwerend auf dessen Deckung auswirken können.[12] Anhand dieser sog. Kriterien der Versicherbarkeit soll die Versicherbarkeit von Cyber-Risiken im Folgenden näher betrachtet werden.

Abgleich von Cyber-Risiken mit den Kriterien der Versicherbarkeit

Zufälligkeit des Schadenereignisses

Das Kriterium der Zufälligkeit fordert, dass das den Versicherungsfall auslösende Ereignis zufällig eintritt. Das Eintreten dieses Ereignisses muss also für alle Vertragsparteien unvorhersehbar und unbeeinflussbar sein.[13] Der Fall der vollständigen Unbeeinflussbarkeit ist jedoch in der Realität nicht gegeben. Der Versicherungsnehmer kann Einfluss auf das Eintreten eines Versicherungsfalls sowie auf dessen Schadenhöhe ausüben. Hierbei wird vom sog.

moralischen Risiko gesprochen.[14] „Das moralische Risiko [bezieht sich] auf die Änderungen des Risikoverhaltens der Versicherungstechnischen Einheiten nach Versicherungsvertragsabschluß.“[15] Diese Verhaltensänderung kann sich z. B. im Grad der Leichtfertigkeit äußern oder eine geringere Bereitschaft zur Schadenverhütung zur Folge haben.[16]

Im Bereich der Cyber-Risiken können einfache Maßnahmen zu einer massiven Erhöhung der Cybersicherheit führen. Diese umfassen bspw. das regelmäßige Durchführen von Sicherheitsupdates, die Nutzung eines Virenschutzprogramms, das Einrichten passwortgeschützter Benutzerkonten oder ein vertrauensvoller Umgang mit persönlichen Daten.[17] Führt der Abschluss einer Cyber-Versicherung dazu, dass solche präventiven Maßnahmen reduziert oder unterlassen werden, kann sich das folglich auf die Eintrittswahrscheinlichkeit und Schadenhöhe auswirken.[18] Außerdem stellen die zunehmend zusammenhängenden IT-Systeme und die damit verbundene Abhängigkeit von Dritten ein signifikantes Problem hinsichtlich des moralischen Risikos dar: So mindern Unternehmen, die wenige Cyberschutzmaßnahmen ergreifen den Cybersicherheitsschutz derer, die von ihnen abhängig sind. Dies könnte den Anreiz für Investitionen in die eigene Cyber-Sicherheit zusätzlich verringern und damit das Problem des moralischen Risikos weiter verstärken.[19]

Eindeutigkeit des Versicherungsfalls

Das Kriterium der Eindeutigkeit verlangt nach einer eindeutigen Definition der versicherten Risiken und der im Schadenfall zu entrichtenden Leistungen. Im Versicherungsvertrag muss also objektiv überprüfbar festgelegt werden, welche Versicherungsleistung bzw. Schadenzahlung bei welchem Ereignis fällig wird. Als Voraussetzung für das Zustandekommen eines Versicherungsvertrages stellt die Erfüllung des Kriteriums der Eindeutigkeit eine notwendige Bedingung für die Versicherbarkeit von Risiken dar. Eindeutigkeit ist prinzipiell so gestaltbar, dass sich keine Probleme hinsichtlich der Erfüllung des Kriteriums ergeben. So werden bspw. auch Risiken, deren Schadenhöhe nicht intersubjektiv überprüfbar ist, mithilfe einer begrenzten Versicherungssumme versichert.[20] Trotzdem existieren für Cyber-Risiken in Bezug auf die Ursachen eines Schadens sowie dessen indirekte Folgen Herausforderungen, die möglicherweise zu einer mangelnden Eindeutigkeit führen können.

In Abschnitt 2.1 wurden die kriminellen und nicht kriminellen Ursachen des Cyber-Risikos mit ihren Ausprägungen aufgezeigt und damit die Vielfältigkeit in den Schadenursachen dargestellt. Diese Vielfältigkeit führt dazu, dass es zu Spezifikationslücken in den Versicherungsverträgen kommen kann,[21] welche gleichzeitig Raum für juristische Interpretationen lassen.[22] Verdeutlicht werden kann das an einem aktuellen

Rechtsstreit zwischen dem US-Lebensmittelkonzern Mondelez und der US-Tochter der Schweizer Zürich-Versicherungsgruppe. Die zwischen den beiden Parteien bestehende Cyberpolice schließt Schäden aus IT-Ausfällen durch Schadsoftware bis 100 Millionen US-Dollar ein. Die Malware „NotPetya“, die 2017 bei Mondelez einen Schaden in Höhe von 180 Millionen US-Dollar verursachte, ließ sich ursächlich einem kriminellen Hackerangriff zuordnen. Zunächst schien der durch Schadsoftware entstandene Schaden eindeutig versichert zu sein, sodass erste Schadenzahlungen geleistet wurden. Da später Hinweise darauf deuteten, „NotPetya“ könnte ein staatlicher Hackerangriff gewesen sein, bewertet die US-Tochter der Zürich-Versicherungsgruppe den Schaden als Folge eines Angriffs mit einer Kriegswaffe, welcher als Ausschluss gilt.[23] Die vermeintlich eindeutig versicherte Schadenursache führt je nach Auslegung zu unterschiedlichen Bewertungen.

Auch die indirekten Auswirkungen eines Schadens bzw. genauer genommen ihre fehlende Messbarkeit können problematisch hinsichtlich der Eindeutigkeit des Cyber-Risikos sein. Vor allem Datenschutzverletzungen führen oft zu Reputationsschäden, deren Höhe nicht exakt bestimmt werden kann. Gleichzeitig kann sich dieser negativ auf den Aktienwert der betroffenen Unternehmen auswirken.[24] Die Höhe des insgesamt entstanden Schadens scheint nur schwer ermittelbar zu sein. Lediglich eine begrenzte Versicherungssumme kann in diesem Fall zur Gewährleistung der Eindeutigkeit beitragen.

Schätzbarkeit der Eintrittswahrscheinlichkeit

Das Kriterium der Schätzbarkeit bezieht sich auf die Eintrittswahrscheinlichkeit der Versicherungsfälle. Die Schätzbarkeit bzw. Kenntnis der Wahrscheinlichkeitsverteilung der Zufallsvariablen werden häufig als Voraussetzung für das Zustandekommen einer Versicherung genannt. Je nach Auffassung ist es jedoch möglich, entweder jedes oder gar kein Risiko als schätzbar einzustufen.[25] Einerseits werden rationale Entscheidungen unter Risiko ausschließlich aufgrund subjektiver Wahrscheinlichkeiten getroffen und können auch bei völligem Informationsmangel sinnvoll zugeordnet werden. Daraus folgt, dass das Zustandekommen einer Versicherung auf Basis subjektiver Wahrscheinlichkeiten immer möglich ist - auch wenn keinerlei statistische Informationen über die Schadenwahrscheinlichkeiten vorliegen. Andererseits ist es nahezu unmöglich, Wahrscheinlichkeiten exakt zu bestimmen, da auch die aus objektiv nachprüfbarer Weise gewonnenen Wahrscheinlichkeiten mit Schätzfehlern behaftet sein können. Das bedeutet, dass das Schätzbarkeitsproblem selbst bei Risiken, die ausreichend mit Daten hinterlegt und deshalb verlässlich modelliert sind, nicht vollständig verschwindet. Die zuvor genannte These, die Kenntnis über die Schadenverteilung

des zu versichernden Risikos sei Voraussetzung für die Versicherbarkeit wird somit nicht vertreten. Die Praxis zeigt, dass selbst Risiken, für die keine statistischen Schadenerfahrungen vorliegen, versichert werden. Bei asymmetrischer Informationsverteilung zwischen den Vertragspartnern kann die fehlende Kenntnis über die Schadenverteilung allerdings zu Problemen bei der Versicherbarkeit führen.[26]

In Bezug auf die Versicherbarkeit von Cyber-Risiken zeigt sich, dass Unternehmen, die Bereits Opfer eines Cyber-Angriffs geworden sind, potenziell eher dazu neigen, eine Cyber-Versicherung abzuschließen.[27] Gleichzeitig sind Unternehmen, die bislang unzureichende Cybersicherheitsmaßnahmen ergriffen haben, einer erhöhten Gefahr ausgesetzt, ebenfalls von Cyber-Angriffen betroffen zu sein. Wenn auch diese Unternehmen vermehrt Cyber-Versicherungen nachfragen, setzt der Prozess der Negativauslese bzw. adversen Selektion ein.[28] Die sich in demselben Versicherungskollektiv befindlichen Risiken unterscheiden sich in ihrer Schadenwahrscheinlichkeit. Aufgrund der asymmetrischen Informationsverteilung ist es dem Versicherer allerdings nicht möglich, die beiden Risikotypen zu unterscheiden.[29]

Insgesamt müssen Cyber-Risiken als sehr dynamisch betrachtet werden, da sie sich aufgrund des technologischen Fortschritts oder des Einsatzes neuartiger Systeme permanent verändern.[30] Das führt dazu, dass historische Daten nur eine geringe Aussagekraft in Bezug auf Risiken, die aus neuartigen Technologien resultieren besitzen und zur Einschätzung künftiger Ereignisse nicht geeignet sind.[31] Die Einschätzung ganzer Kollektive kann daher insgesamt sehr unsicher sein und sollte laufend überprüft und an technologische Neuerungen angepasst werden.[32]

Unabhängigkeit der Risiken

Für den Risikoausgleich im Kollektiv ist vor allem die Unabhängigkeit der Risiken voneinander von großer Bedeutung. Damit der Effekt des Ausgleichs im Kollektiv überhaupt zustande kommen kann, müssen die Zufallsvariablen des versicherten Bestandes stochastisch unabhängig sein. Bei nicht unabhängigen bzw. korrelierenden Einzelrisiken wird dieser Ausgleichseffekt erheblich beeinträchtigt, wie es bspw. bei einem Kumulrisiko der Fall sein kann.[33]

Dass Cyber-Risiken ein erhebliches und weltweites Kumulpotenzial aufweisen, verdeutlichen Szenarien wie Störungen und Ausfälle zentraler IT-Dienste oder kritischer Infrastruktur. Auch Cyber-Angriffe durch Schadsoftware können weltweit volkswirtschaftliche Schäden in Milliardenhöhe verursachen. Der Großteil dieser Kumulszenarien ist auf menschliches Handeln zurückzuführen. Dabei ist belanglos, ob die Ursache krimineller Natur wie bspw. Hackerangriffe oder nicht krimineller Natur wie menschliches Versagen ist. Durch die fortschreitende Digitalisierung wird das

Schadenpotenzial stetig erhöht. Die zunehmende Vernetzung innerhalb der Wertschöpfungskette und die Nutzung gemeinsamer Hardware- und Softwarekomponenten führen zu einer Vergrößerung der Anfälligkeit für Cybervorfälle jeglicher Art, wodurch sich das Kumulpotenzial weiter erhöht.[34]

Größe des Schadens

Das Kriterium der Größe bezieht sich auf den maximal möglichen Schaden eines Einzelrisikos.[35] Ist dieser nicht ermittelbar, so ist es trotzdem nicht unmöglich, das Risiko zu versichern, da sich die im Schadenfall für den Versicherer zu leistende Zahlung durch eine Versicherungssumme begrenzen lässt.[36]

Dass die Größe des Cyber-Risikos schwer zu ermitteln ist, lässt sich leicht an einem Beispiel verdeutlichen: Im Falle eines Datenverlusts ist das Risiko nicht nur auf die fehlende temporäre Verfügbarkeit der Daten beschränkt, sondern beinhaltet auch Folgeschäden wie bspw. den Reputationsschaden. Dieser kann je nach Sensibilität der Daten unterschiedlich hoch ausfallen. Auch in Cyber-Versicherungspolicen werden diese Probleme mit entsprechenden Haftungsbegrenzungen gelöst.[37] Insgesamt kann sich also aus dem Kriterium der Größe kein prinzipielles Problem der Versicherbarkeit von Cyber-Risiken ergeben. Durch die Schadensummenbegrenzung ist zumindest eine teilweise Deckung des Risikos möglich.[38]

Fazit

Durch die Existenz des moralischen Risikos auf dem Cyber-Versicherungsmarkt kann die Forderung nach der Unbeeinflussbarkeit nicht erfüllt werden, weshalb das Kriterium der Zufälligkeit nicht vollständig erfüllt wird. Auch die Eindeutigkeit ist nicht immer gegeben, da vielfältige Schadenursachen einen vertraglichen Interpretationsspielraum lassen und die indirekten Auswirkungen der Cyber-Risiken kaum messbar sind. Der technologische Fortschritt und die damit zunehmende Vernetzung vorher unabhängiger Systeme wirken sich erschwerend auf die Schätzbarkeit und Unabhängigkeit der Cyber-Risiken aus. Die daraus resultierende Dynamik des Cyber-Risikos verhindert den Rückgriff auf historische Daten zur verlässlichen Modellierung. Gleichzeitig erhöht sich das Schaden- und Kumulpotenzial mit fortlaufender Digitalisierung stetig. Auch der maximal mögliche Schaden durch Cyber-Risiken ist dadurch nur schwer ermittelbar.

Abschließend kann festgehalten werden, dass das Cyber-Risiko keines der fünf Kriterien der Versicherbarkeit vollständig erfüllt. Allerdings kann den zuvor erörterten Problemen durch den Einsatz verschiedener Instrumente der Vertragsgestaltung wie Selbstbeteiligungen und begrenzten Versicherungssummen entgegengewirkt werden.[39] Die Entscheidung über die Deckung

von Cyber-Risiken liegt letztlich bei dem Versicherer selbst und hängt von seiner gesamten Risikosituation sowie seinem subjektiven Risikoverhalten ab. Trotzdem gibt es eine Reihe von extremen Cyber-Risiken, die die Versicherungswirtschaft alleine nicht tragen kann. Um auch diese Risiken beherrschbar zu machen bedarf es womöglich der Zusammenarbeit mit Regierungen, bspw. in Form von Pool-Lösungen.[40]

---

[1] Vgl. Munich Re, o. J.
[2] Vgl. Allianz Global Corporate & Specialty SE, 2020.
[3] Vgl. Munich Re, o. J.
[4] Vgl. Biener et al., 2015a, S. 4.
[5] Cebula / Young, 2010, S. 1.
[6] Vgl. Bank for International Settlements, 2006, S. 144-156.
[7] Vgl. Committee of European Insurance and Occupational Pensions Supervisors, 2009, S. 3-18.
[8] Vgl. Cebula / Young, 2010, S. 3.
[9] Vgl. Biener et al., 2015a, S. 9.
[10] Vgl. Karten, 1972, S. 285.
[11] Vgl. Karten et al., 2018, S. 106.
[12] Vgl. Karten, 1972, S. 286-293.
[13] Vgl. Karten, 1972, S. 287.
[14] Vgl. Karten et al., 2018, S. 107-108.
[15] Helten / Karten, 1991, S. 134.
[16] Vgl. Helten / Karten, 1991, S. 134.
[17] Vgl. Bundesamt für Sicherheit in der Informationstechnik, o. J.
[18] Vgl. Karten et al., 2018, S. 110.
[19] Vgl. Eling / Wirfs, 2016, S. 25.
[20] Vgl. Karten et al., 2018, S. 117.
[21] Vgl. Haas, 2016, S. 109.
[22] Vgl. Karten et al., 2018, S. 117-118.
[23] Vgl. Fuerst, 2018.
[24] Vgl. Eling / Wirfs, 2016, S. 26.
[25] Vgl. Karten, 1972, S. 290.
[26] Vgl. Karten et al., 2018, S. 120.
[27] Vgl. Eling / Wirfs, 2016, S. 25.
[28] Vgl. Lesch / Richter, 2000, S. 628.
[29] Vgl. Karten et al., 2018, S. 121-122.
[30] Vgl. Biener et al., 2015b, S. 142.
[31] Vgl. Jeworrek, 2018.
[32] Vgl. Lesch / Richter, 2000, S. 627.
[33] Vgl. Karten et al., 2018, S. 123-124.
[34] Vgl. Glaab, 2018.
[35] Vgl. Karten, 1972, S. 292.
[36] Vgl. Karten et al., 2018, S. 126.
[37] Vgl. Haas, 2016, S. 113-114.
[38] Vgl. Karten et al., 2018, S. 126.
[39] Vgl. Karten et al., 2018, S. 126.
[40] Vgl. Munich Re, o. J.

Literaturverzeichnis

Allianz Global Corporate & Specialty SE (2020): Allianz Risk Barometer 2020: Cyber steigt zum weltweiten Top-Risiko für Unternehmen auf, https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html, Stand 27.03.2020.

Bank for International Settlements (2006): International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version, https://www.bis.org/publ/bcbs128.pdf, Stand 27.03.2020.

Biener, Christian / Eling, Martin / Matt, Andreas / Wirfs, Jan Hendrik (2015a): Cyber Risk: Risikomanagement und Versicherbarkeit, in: I. VW-HSG Schriftenreihe des Instituts für Versicherungswirtschaft Universität St. Gallen, Vol. 54, St. Gallen 2015.

Biener, Christian / Eling, Martin / Wirfs, Jan Hendrik (2015b): Insurability of Cyber Risk: An Empirical Analysis, in: The Geneva Papers on Risk and Insurance - Issues and Practice, Vol. 40, S. 131 –158.

Bundesamt für Sicherheit in der Informationstechnik (o. J.): Zehn Maßnahmen zur Absicherung gegen Angriffe aus dem Internet, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html, Stand 27.03.2020.

Cebula, James J. / Young, Lisa R. (2010): A Taxonomy of Operational Cyber Security Risks, in: CMU/SEI-2010-TN-028, Carnegie Mellon University.

Committee of European Insurance and Occupational Pensions Supervisors (2009): CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR Standard Formula - Article 111 (f): Operational Risk, CEIOPS-DOC-45/09.

Eling, Martin / Wirfs, Jan Hendrik (2016): Cyber Risk: Too Big to Insure?: Risk Transfer Options for a Mercurial Risk Class, in: I. VW-HSG Schriftenreihe des Instituts für Versicherungswirtschaft Universität St. Gallen, Vol. 59, St. Gallen 2016.

Fuerst, Benedikt (2018): Dieser Fall entscheidet, ob Hacken eine Kriegswaffe ist, https://www.welt.de/wirtschaft/article185510234/Notpetya-Dieser-Fall-entscheidet-ob-Hacken-eine-Kriegswaffe-ist.html, Stand 27.03.2020.

Glaab, Holger (2018): Cyber-Kumulrisiken, https://www.munichre.com/topics-online/de/digitalisation/cyber/dealing-with-cyber-accumulation-risk.html, Stand 27.03.2020.

Haas, Andreas (2016): Management von Cyber-Risiken und Möglichkeit des Risikotransfers - eine ökonomische und versicherungstechnische Analyse, Diss., Universität Hohenheim, Hohenheim 2016.

Helten, Elmar / Karten, Walter (1991): Das Risiko und seine Kalkulation (Teil I), in: Grosse, Walter (Hrsg.): Versicherungsenzyklopädie, Band 2: Versicherungsbetriebslehre, Wiesbaden 1991, S. 125-276.

Jeworrek, Torsten (2018): Cyberpolicen: Mehr als Risikotransfer, https://www.munichre.com/topics-online/de/digitalisation/cyber/cyber-policies.html, Stand 27.03.2020.

Karten, Walter (1972): Zum Problem der Versicherbarkeit und zur Risikopolitik des Versicherungsunternehmens – betriebswirtschaftliche Aspekte, in: Zeitschrift für die gesamte Versicherungswissenschaft, 61. Bd., S. 279-299.

Karten, Walter / Nell, Martin / Richter, Andreas / Schiller, Jörg (2018): Risiko und Versicherungstechnik: Eine ökonomische Einführung, Wiesbaden 2018.

Lesch, Torsten / Richter, Andreas (2000): Risiken aus kommerzieller Nutzung des Internet - Möglichkeiten der Schadenverhütung und Versicherung, in: Zeitschrift für die gesamte Versicherungswissenschaft, 89. Bd., S. 605-633.

Munich Re (o. J.): Cyber-Risiken: Cyber-Bedrohungen zählen zu den größten Risiken des 21. Jahrhunderts, https://www.munichre.com/de/risiken/cyber-risiken.html, Stand 27.03.2020.

	Cyber-Risiken					
Ursache	**Vorsätzliches Ereignis**			**Zufälliges Ereignis**		
Bedrohungs-art	**Hackerangriffe**	**Physische Angriffe**	**Informations-verbreitung**	**Menschliches Versagen**	**Technisches Versagen**	**Höhere Gewalt**
Angriffs-form	- Malware - Phishing - Ransomware - DoS	- physisches Eindringen in Unternehmens-gebäude - Diebstahl vertraulicher Informationen	- E-Mail-Kampagnen - Boykottaufrufe über soziale Medien	- Programmierungs-fehler - Verlust von Datenträgern - Versehentliches Veröffentlichen - Falsche Adressierung	- Hardwaredefekte - Softwarefehler	- Naturkatastrophen
Auswirkung	- Betriebs-unterbrechung - Datenverlust - Datenschutz-verletzung	- Datenverlust - Datenschutz-verletzung	- Reputationsschaden - Datenschutz-verletzung	- Betriebs-unterbrechung - Datenverlust - Datenschutz-verletzung	- Betriebs-unterbrechung - Datenverlust	- Betriebs-unterbrechung - Datenverlust

Charakteristika des Cyber-Versicherungsmarktes - Gründe für das verhaltene Marktwachstum in Deutschland

Von Marcel Heinrichsmeier

Einleitung

9 von 10 Unternehmen in Deutschland sehen die Digitalisierung als Chance und nicht als Risiko.[1] Dennoch haben Entwicklungen wie das Internet of Things oder Cloud Computing nicht nur positive Auswirkungen auf Gesellschaft und Wirtschaft. Cyber-Vorfälle stellen im Jahr 2020 erstmals weltweit die größte Gefahr für Unternehmen dar.[2] Nach einer Studie von Bitkom wurden in den Jahren 2018 und 2019 75% der befragten Unternehmen in Deutschland Opfer von Datendiebstahl, Industriespionage oder Sabotage.[3] Die daraus entstandenen finanziellen Schäden betrugen circa 100 Milliarden Euro jährlich.[4] Um dieser Entwicklung entgegenzusteuern, bedarf es Investitionen in unternehmensinterne IT-Sicherheit. Ausgaben im Bereich IT-Sicherheit deutscher Unternehmen werden 2020 voraussichtlich auf ein Rekordhoch von 4,9 Milliarden Euro wachsen.[5] Parallel zu IT-Sicherheitsmaßnahmen stellt der versicherungsbasierte Risikotransfer eine Ergänzung bei der Abwehr von Cyber-Risiken dar. Allianz und AXA halten für Deutschland eine Verzehnfachung der Cyber-Versicherungs-Prämie innerhalb von fünf Jahren von 30 Millionen Euro 2016 auf bis zu 300 Millionen Euro im Jahr 2021 für möglich.[6] Ende 2018 betrug das Prämienvolumen in Deutschland jedoch nur 50 Millionen Euro.[7] Das entspricht einem Anteil von 1%[8] am weltweiten Cyber-Versicherungsmarkt. Der nachfolgende Beitrag untersucht die Charakteristika des Cyber-Versicherungsmarktes, um die Gründe für das verhaltene Marktwachstum der Cyber-Versicherung in Deutschland zu erörtern.

Zuerst wird der zentrale Begriff Cyber-Risiken definiert. Im Anschluss findet eine genaue Analyse der Friktionen für Versicherer sowie Kunden in diesem Markt statt. Im Schlussteil wird ein Fazit gezogen und ein Ausblick zur künftigen Marktentwicklung der Cyber-Versicherung in Deutschland gegeben.

Begriffsdefinition Cyber-Risiken

In dieser Arbeit liegt der Fokus auf Cyber-Risiken, die im Kontext einer Cyber-Versicherung eine Gefahr für Unternehmen darstellen. Nach den vom Gesamtverband der deutschen Versicherungswirtschaft (GDV) veröffentlichten Musterbedingungen der Cyber-Versicherung tritt der Versicherungsfall ein, wenn aus einer Informationssicherheitsverletzung ein Vermögensschaden resultiert.[9] Eine Informationensicherheitsverletzung wird als „Beeinträchtigung

der Verfügbarkeit, Integrität und Vertraulichkeit von elektronischen Daten“[10] bezeichnet. Diese Definition weist Ähnlichkeit mit der Definition von Cyber-Risiken als „operative Risiken für Informations- und Technologieressourcen, welche Auswirkungen auf die Vertraulichkeit, Verfügbarkeit oder die Integrität von Informationen oder Informationssystemen haben“[11] nach CEBULA/YOUNG auf, die in diesem Beitrag aufgrund des Versicherungsbezugs Anwendung findet.

Friktionen auf der Angebotsseite des deutschen Cyber-Versicherungsmarktes

Quantifizierung von Cyber-Risiken

Anbietende Versicherungsunternehmen sehen sich mit dem Problem der Quantifizierung von Cyber-Risiken konfrontiert. Diese Herausforderung lässt sich in drei Komponenten unterteilen: (i) Geringe Verfügbarkeit historischer Daten; (ii) dynamischer Wandel der Natur der Cyber-Risiken; (iii) Kumulrisiken.[12] Die mangelnde Datenverfügbarkeit ist einerseits durch die Neuartigkeit des Cyber-Risikos und anderseits durch die intransparente Berichterstattung von Cyber-Vorfällen durch Unternehmen aufgrund der Angst vor Reputationsschäden[13] zu erklären. Die unklare Datenlage zur Häufigkeit und Ausmaß von Cyber-Schäden erschwert die Kalkulation von Versicherungsprämien. Dies macht hohe Risikozuschläge notwendig[14] und führt somit zu hohen Prämien. Der technologische Fortschritt als zweite Komponente verändert fortlaufend die Charakteristik des Cyber-Risikos und kann vorhandene historische Daten unbrauchbar machen.[15] Durch dieses Änderungsrisiko können sich Eintrittswahrscheinlichkeit sowie Ausmaß des Schadens signifikant verändern.[16] Durch steigende Interkonnektivität bieten sich größere Angriffsflächen für Cyber-Attacken. Aus diesem Änderungsrisiko können Deckungslücken entstehen, was den versicherungsbasierten Risikotransfer unattraktiver macht und ein Grund für das verhaltene Marktwachstum darstellen kann.[17] Die Interkonnektivität wird durch vermehrtes Cloud Computing verstärkt. Die interdependente Netzwerkstruktur führt dazu, dass Einzelrisiken nicht mehr unabhängig sind und somit können Kumulrisiken als weitere Herausforderung auftreten.[18] Ein einzelner Cyber-Angriff besitzt das Potenzial viele Versicherte zur selben Zeit zu treffen, was im Worst Case zur Zahlungsunfähigkeit eines Versicherers führen kann.[19] Die Kumulproblematik kann entweder zu niedrigen Deckungssummen[20] und höheren Prämien[21] führen oder sogar zu einer Einschränkung des Angebots an Versicherungsschutz[22].

Informationsasymmetrien – Adverse Selektion und Moral Hazard

In der Literatur werden Adverse Selektion und Moral Hazard als Formen asymmetrischer Informationsverteilung als

Hemmnisse für die Cyber-Versicherung gesehen. Als Adverse Selektion wird die Gefahr bezeichnet, dass sich nur schlechte Risiken versichern wollen, da für gute Risiken der Abschluss einer Versicherung irrelevant ist.[23] Die Tatsache, dass viele Unternehmen intransparent hinsichtlich vorgefallener Cyber-Vorfälle und interner Sicherheitsmaßnahmen sind[24], verhindert die Differenzierung zwischen guten und schlechten Risikotypen[25] durch den Versicherer. Diese versuchen die Effekte der Adversen Selektion durch das Erstellen von individuellen Risikoprofilen, durch bspw. Vorab-Fragebögen zu firmeninternen IT-Sicherheitsmaßnahmen, zu mindern.[26] Moral Hazard dagegen beschreibt grundsätzlich eine Verhaltensänderung nach dem Abschluss einer Versicherung und entsteht aus dem Mangel an Anreizen, Präventionsmaßnahmen zur Verhinderung eines Schadenseintritts zu ergreifen.[27] Im Kontext der Cyber-Risiken kann eine Versicherung aufgrund des moralischen Risikos die Motivation in die IT-Sicherheit zu investieren, negativ beeinflussen.[28] Da Versicherer keine Möglichkeit haben, das Verhalten des Versicherungsnehmers nach Vertragsabschluss zu beobachten, begegnen sie diesem Problem mit Selbstbeteiligungen, Deckungslimiten sowie ex-post Schadenaufklärung, um vorsätzliches Handeln zu prüfen.[29] Es besteht auch die Gefahr, dass das eigene Unternehmen trotz Investitionen in die eigene IT-Sicherheit angreifbar bleibt, wenn Angreifer andere verbundene Unternehmen als Einfallstore nutzen.[30] Dies reduziert den Nutzen von IT-Sicherheitsmaßnahmen und verstärkt das Moral Hazard Problem. Informationsasymmetrien stellen weiterhin einen Grund für unattraktiven Versicherungsschutz dar.

Friktionen auf der Nachfrageseite des deutschen Cyber-Versicherungsmarktes

Mangelndes Risikobewusstsein für Cyber-Risiken

In Deutschland fehlt sowohl auf gesellschaftlicher als auch auf individueller Unternehmensebene ein Bewusstsein für Cyber-Risiken und den daraus entstehenden Gefahren und Schäden.[31] Obwohl im Rahmen der Digitalisierung Entwicklungen hin zu vernetzten Businesssystemen die Relevanz des Managements von Cyber-Risiken steigert[32], ist der Stellenwert im firmeninternen Risikomanagement noch niedrig und eine angemessene Beachtung dieser Cyber-Risiken durch die Geschäftsleitung fehlt[33]. Die Unterschätzung der erheblichen Schadenpotentiale und die mangelnde Risikowahrnehmung führen oftmals zu der Fehlinterpretation seitens der Unternehmen, die Cyber-Versicherung als Äquivalent anstatt Bestandteil für ein internes Cyber-Risiko-Management zu sehen.[34] Zusätzlich erkennen viele Unternehmen den Bedarf einer Cyber-Versicherung nicht, da sie fälschlicherweise davon ausgehen, dass Schäden durch Cyber-Risiken durch

vorhandene Versicherungslösungen ausreichend abgedeckt sind.[35] Um Gefahren zu identifizieren, ist eine interne Analyse der individuellen Cyber-Risk-Exposition durch bspw. das Untersuchen von Geschäftsprozessen im Risikomanagement notwendig.[36] Dies fehlt bis heute in vielen kleineren Unternehmen, da sie irrtümlicherweise[37] aufgrund ihrer geringen Größe davon ausgehen, nicht als Ziel für einen Cyber-Angriff in Frage zu kommen, womit die mangelnde Risikowahrnehmung verstärkt wird.[38] Dazu kommt, dass Unternehmen die großen potentiellen finanziellen Verluste eines Cyber-Vorfalls aufgrund fehlender Modellierung nicht bewusst sind, sowie Pläne zum Umgang mit diesen Risiken fehlen.[39] Das fehlende Risikobewusstsein der Unternehmen verhinderte bisher eine größere Nachfrage nach Cyber-Versicherungen.

Unzureichende Regulatorik

Ein umfassendes regulatorisches Umfeld spielt eine wesentliche Rolle bei der Marktentwicklung der Cyber-Versicherung. Dies belegt der amerikanische Cyber-Versicherungsmarkt mit einem Prämienvolumen von circa 2 Milliarden Euro im Jahr 2018.[40] Seit 1996 gibt es dort strikte Datenschutzgesetze, die den Umgang mit Datenschutzverletzungen regeln und somit die Kunden schützen.[41] Dies, sowie Sammelklagen als zusätzliches Instrumentarium für Kunden, ziehen bei Verstößen erhebliche finanzielle Konsequenzen für Unternehmen nach sich.[42] Dieses regulatorische Umfeld erhöhte die Risikowahrnehmung der nachfragenden Unternehmen[43] und die Nachfrage nach einem versicherungsbasierten Risikotransfer[44]. Dies stellt eine Erklärung für den größeren US-Cyberversicherungsmarkt dar. In Deutschland wurde 2009 eine Meldepflicht bei Datenschutzverstößen nach Bundesdatenschutzgesetz (BDSG) eingeführt.[45] Doch durch fehlende Konkretisierung und Verhängung von Strafzahlungen, sowie die fehlende Möglichkeit von Sammelklagen, konnte sich in Deutschland das Risikobewusstsein für Cyber-Risiken sowie die Nachfrage nach einer Cyber-Versicherung nicht erhöhen.[46] Am 25. Mai 2018 wurde von der EU die Datenschutzgrundverordnung (DSGVO) eingeführt, die für die Beurteilung des Umgangs mit Datenschutz das einschlägige Gesetz darstellt. Bei Verstößen gegen die DSGVO können strikte Strafzahlungen in Höhe von bis zu 20 Millionen Euro bzw. 4% des gesamten weltweiten jährlichen Jahresumsatzes des Unternehmens verhängt werden.[47] Ein Internetsuchanbieter wurde in Frankreich schon aufgrund von Verstößen gegen die DSGVO mit einer Strafe in Höhe von 50 Millionen Euro sanktioniert.[48] Außerdem kann nun erstmals auch ein immaterieller Schaden geltend gemacht werden[49] und die Meldepflichten bei Verlust von personenbezogenen Daten wurden verschärft.[50] Diese neuen Regeln zum Datenschutz werden in der Literatur als Chance für einen Nachfrageschub in Bezug auf eine Cyber-Versicherung gesehen.[51]

Fazit und Ausblick

In diesem Beitrag konnte gezeigt werden, dass der Cyber-Versicherungsmarkt viele unterschiedliche Herausforderungen zu bewältigen hat und die Gründe für das bisherige geringe Marktwachstum sowohl bei den anbietenden Versicherern, als auch bei den nachfragenden Kunden, zu finden sind. Die Versicherer werden in Zukunft aufgrund der weiter voranschreitenden Digitalisierung innovative Ansätze zur Bewältigung des Problems der Quantifizierung von Daten entwickeln müssen, um ein ansprechendes Produkt für den Kunden anzubieten. Fachliche Expertise, um Cyber-Risiken bspw. durch Szenarioanalysen[52] adäquat bewerten und bepreisen zu können, wird für Versicherer von Bedeutung sein. Ein Erfahrungsaustausch zwischen Unternehmen innerhalb der Versicherungsbranche zu den Cyber-Risiken im Sinne eines kollektiven Lernprozesses[53], könnte einen positiven Einfluss auf eine Standardisierung der Policen sowie auf das Preisniveau nehmen. Durch die Einführung der DSGVO wurden Informationsasymmetrien aufgrund einer Erhöhung an Transparenz von Cyber-Vorfällen verringert. Zunehmende Angriffe auf Unternehmen und große medial wirksame Cyber-Attacken wie NotPetya bzw. WannaCry sowie die Schaffung eines strikteren regulatorischen Umfelds dürften das Risikobewusstsein der Unternehmen für Cyber-Risiken erhöht haben und somit zu einer erhöhten Nachfrage an Cyber-Versicherungen führen. Die Versicherungsbranche sagt für die Cyber-Versicherung ein dynamisches Wachstum mit einer nahezu jährlichen Verdopplung an Vertragsabschlüssen im Neukundengeschäft voraus.[54] Aktuelle Zahlen des GDV bestätigen diese Aussagen. Das Prämienvolumen der Cyber-Versicherung ist 2019 um 70% auf 85 Millionen Euro gewachsen.[55] Es wird sich zeigen, ob die von Allianz und AXA für das Jahr 2021 prognostizierten 300 Millionen Euro an Cyber-Versicherungsprämie eintreten werden.

---

1 Vgl. Berg, 2019, S. 5.
2 Vgl. Allianz Global Corporate and Specialty, 2020, S. 11.
3 Vgl. Bitkom, 2020, S. 7.
4 Vgl. Bitkom, 2020, S. 23.
5 Vgl. Bitkom, 2019.
6 Vgl. KPMG AG Wirtschaftsprüfungsgesellschaft, 2017, S. 29.
7 Auskunft des GDV an den Verfasser.
8 Siehe Aon, 2019, S. 13.
9 Vgl. GDV, 2017, S. 6.
10 GDV, 2017, S. 6.
11 Cebula/Young, 2010, S. 1.
12 Vgl. OECD, 2017, S. 94.
13 Vgl. CRO Forum, 2014, S. 8.
14 Vgl. Biener et al., 2015, S. 65 – 66.
15 Vgl. Biener et al., 2015, S. 46.
16 Vgl. Haas, 2016, S. 214.
17 Vgl. Haas, 2016, S. 215.
18 Vgl. Haas / Hofmann, 2014, S. 404.
19 Vgl. Haas / Hofmann, 2014, S. 400.
20 Vgl. Haas, 2016, S. 114.
21 Vgl. Haas, 2016, S. 108.
22 Vgl. KPMG AG Wirtschaftsprüfungsgesellschaft, 2017, S. 50.
23 Vgl. Biener et al., 2015, S. 61.
24 Vgl. OECD, 2017 S. 96.
25 Vgl. Majuca et al., 2006, S. 8.
26 Vgl. Majuca et al., 2006, S. 9.
27 Vgl. Biener et al., 2015, S. 61.
28 Vgl. Majuca et al., 2006, S. 11.
29 Vgl. Haas, 2016, S. 209 – 210.
30 Vgl. Eling / Wirfs, 2016, S. 25.
31 Vgl. BIGS, 2017, S. 32

[32] Vgl. Kosub, 2015, S. 630.
[33] Vgl. Biener et al., 2015, S. 85.
[34] Vgl. Wrede et al., 2018, S. 407.
[35] Vgl. OECD, 2017, S. 102.
[36] Vgl. Haas / Hofmann, 2014, S. 388.
[37] Vgl. GDV, 2019, S. 5.
[38] Vgl. Wrede, 2019, S. 420.
[39] Vgl. Marsh, 2016, S. 7.
[40] Vgl. Aon, 2019, S. 3.
[41] Vgl. Kesan et al., 2005, S. 6 – 10.
[42] Vgl. BIGS, 2017, S. 47 – 51.
[43] Vgl. Eling et al., 2016, S. 20.
[44] Vgl. BIGS, 2017, S. 47 – 51.
[45] Vgl. § 42a BDSG a.F.
[46] Vgl. Haas, 2014, S. 175.
[47] Vgl. Art. 83 Abs. 5 EU DSGVO.
[48] Vgl. Marsh, 2019, S. 14.
[49] Vgl. Art. 82 Abs. 1 EU DSGVO.
[50] Vgl. Art. 33 EU DSGVO.
[51] Vgl. Eling et al., 2016, S. 20.
[52] Vgl. Lloyd's, 2015, S. 29 – 40.
[53] Vgl. BIGS, 2017, S. 64.
[54] Vgl. Wrede et al., 2019, S. 422.
[55] Auskunft des GDV an den Verfasser.

Literaturverzeichnis

Allianz Global Corporate and Specialty (2020): Allianz Risk Barometer. Identifying the major business risks for 2020, URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf, Stand 29.03.2020.

Aon (2019): US Cyber Market Update. 2018 US Cyber Insurance Profits and Performance. June 2019, URL: http://thoughtleadership.aon.com/Documents/201906-us-cyber-market-update.pdf, Stand 29.03.2020.

Berg, Achim (2019): Digitalisierung der Wirtschaft, URL: https://www.bitkom.org/sites/default/files/2019-04/bitkom_charts_hub_-_digitalisierung_der_wirtschaft_10_04_2019_final.pdf, Stand 29.03.2020.

Biener, Christian / Eling, Martin / Matt, Andreas / Wirfs, Jan Hendrik (2015): Cyber Risk: Risikomanagement und Versicherbarkeit, Institut für Versicherungswirtschaft der Universität St. Gallen, St. Gallen 2015, URL: https://www.kessler.ch/fileadmin/user_upload/Cyber_Risk_Risikomanagement_und_Versicherbarkeit_de.pdf, Stand 29.03.2020.

Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS) (2017): Cyberversicherungen als Beitrag zum IT-Risikomanagement – Eine Analyse der Märkte für Cyberversicherungen in Deutschland, der Schweiz, den USA und Großbritannien. BIGS Standpunkt Nr. 8, September 2017, Potsdam: Brandenburgisches Institut für Gesellschaft und Sicherheit, URL: https://www.bigs-potsdam.org/images/weitere_Publikationen/Standpunkt_8_2017%20Online.pdf, Stand 29.03.2020.

Bitkom (2019): Rekordjahr im Markt für IT-Sicherheit, URL: https://www.bitkom.org/Presse/Presseinformation/Rekordjahr-im-Markt-fuer-IT-Sicherheit, Stand 29.03.2020.

Bitkom (2020): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt, URL: https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf, Stand 29.03.2020.

Cebula, James J. / Young, Lisa R. (2010): A Taxonomy of Operational Cyber Security Risks, Hanscom. URL: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf, Stand 29.03.2020.

Chief Risk Officer (CRO) Forum (2014): Cyber resilience. The cyber risk challenge and the role of insurance, URL:https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf, Stand 29.03.2020.

Eling, Martin / Wirfs, Jan Hendrik (2016): Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class, Institute of Insurance Economics, University of St. Gallen, 2016, URL: https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf, Stand 29.03.2020.

GDV (2017): Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber), URL: https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0cc207/01-allgemeine-

versicherungsbedingungen-fuer-die-cyberrisiko-versicherung--avb-cyber--data.pdf, Stand 29.03.2020.

GDV (2019): Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung. Frühjahr 2019, URL: https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf, Stand 29.03.2020.

Haas, Andreas / Hofmann, Annette (2014): Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit, in: Zeitschrift für die gesamte Versicherungswissenschaft (ZversWiss) 103, S. 377–407, Berlin/Heidelberg 2014, URL: https://link.springer.com/content/pdf/10.1007/s12297-014-0285-3.pdf, Stand 29.03.2020.

Haas, Andreas (2016): Management von Cyber-Risiken und Möglichkeiten des Risikotransfers - eine ökonomische und versicherungstechnische Analyse, Diss., Universität Hohenheim, Hohenheim 2016, URL: http://opus.uni-hohenheim.de/volltexte/2016/1192/pdf/Diss_Haas_Buchdruck_Final.pdf, Stand 29.03.2020.

Kesan, Jay P. / Majuca, Ruperto P. / Yurcik, William J. (2005): Cyberinsurance as a market-based solution to the problem of cybersecurity – a case study, Workshop on Economics of Information Security (WEIS), URL: http://infosecon.net/workshop/pdf/42.pdf, Stand 29.03.2020.

Kosub, Thomas (2015): Components and challenges of integrated cyber risk management, in: ZVersWiss (2015) 104, S. 615–634, Berlin/Heidelberg, 2015, URL: https://link.springer.com/content/pdf/10.1007/s12297-015-0316-8.pdf, Stand 29.03.2020.

KPMG AG Wirtschaftsprüfungsgesellschaft (2017): Neues Denken, Neues Handeln. Insurance Thinking Ahead. Versicherungen im Zeitalter von Digitalisierung und Cyber. Studienteil A: Digitalisierung, URL: https://assets.kpmg/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-digitalization-de.pdf, Stand 29.03.2020.

Lloyd's (2015): Emerging Risk Report. Business Blackout: the insurance implications of a cyber attack on the U.S. power grid, URL: http://empgridservices.com/wp-content/uploads/2015/07/Business-Blackout-July-2015.pdf, Stand 29.03.2020.

Majuca, Ruperto P. / Kesan, Jay P. / Yurcik, William (2005): The Evolution of Cyber-insurance, Working Paper, University of Illinois 2005, URL: https://arxiv.org/ftp/cs/papers/0601/0601020.pdf, Stand 29.03.2020.

Marsh (2016): Continental European Cyber Risk Survey: 2016 Report, URL: https://www.marsh.com/de/de/insights/research-briefings/continental-european-cyber-risk-survey-2016-report.html, Stand 29.03.2020.

Marsh (2019): Versicherungsmarktreport 2019 Deutschland, URL: https://www.marsh.com/de/de/insights/research-briefings/versicherungsmarktreport-2019-fur-deutschland.html, Stand 29.03.2020.

OECD (2017): Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris, URL: http://dx.doi.org/10.1787/9789264282148-en, Stand 29.03.2020.

Wrede, Dirk / Freers, Thorben / Graf von der Schulenberg, Johann-Matthias (2018): Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse, in: ZVersWiss (2018) 107, S. 405–434, URL: https://link.springer.com/content/pdf/10.1007/s12297-018-0425-2.pdf, Stand 29.03.2020.

Bundesdatenschutzgesetz in der Fassung vom 01.09.2009 durch Artikel 1 G. v. 14.08.2009 geändert, BGBl. I S. 2814.

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, in: ABl. L119, Jg. 59, S. 1-88.

Versicherbarkeit von Cyber-Risiken - Herausforderungen und Maßnahmen zur Verbesserung der Versicherbarkeit

Von Nadja Schlett

Einleitung

600 Milliarden US-Dollar betrugen laut einer Schätzung der Munich Re die gesamtwirtschaftlichen Schäden durch Cyber-Angriffe alleine im Jahr 2018.[1] Dabei beschränken sich die Schäden nicht auf verlorene oder beschädigte Daten, sondern schließen zunehmend auch Schäden durch Betriebsunterbrechungen oder an der Reputation eines Unternehmens ein. Neben dem immer größeren Ausmaß der Schäden, führen auch die digitale Transformation, die Nutzung internetfähiger Geräte sowie die sich ausbreitenden Hackerangriffe zu den wachsenden Cyber-Bedrohungen.[2] Organisationen wie das Weltwirtschaftsforum halten Cyber-Angriffe für eines der gewichtigsten Risiken in der heutigen Zeit.[3] Der Schutz vor diesen Risiken wird deshalb für Unternehmen immer wichtiger und neben den eigenen Verteidigungsmöglichkeiten wie verstärkte Investition in Sicherheitstechnologien, ist insbesondere der Risikotransfer an Dritte von großer Bedeutung. Die Absicherung von Cyber-Risiken stellt Versicherer allerdings vor verschiedenste Probleme.[4]

Nachfolgend soll deshalb zunächst auf unterschiedliche Herausforderungen bei der Versicherung dieser Risiken eingegangen werden. Auf Basis dessen wird anschließend eine Reihe von Maßnahmen betrachtet, wie diesen Problemen begegnet werden kann, um die Versicherbarkeit von Cyber-Risiken zu gewährleisten und zu verbessern. Abschließend erfolgt ein Fazit, ob damit die Grenzen der Versicherbarkeit erweitert werden können.

Herausforderungen bei der Versicherung von Cyber-Risiken

Mangel an Informationen

Eine der größten Herausforderungen besteht in der technologischen Neuartigkeit des zu versichernden Risikos. Während in traditionellen Versicherungssparten zum Teil jahrzehntelange Schadenerfahrung mit meist gleichbleibenden Schaden-Wirkungsketten besteht, mangelt es bei Cyber-Risiken an der Schadenhistorie und der Erfahrung der Versicherer im Umgang mit diesen Risiken.[5] Daneben fehlt es an einer allgemeinen Erfassung von Informationen über Cyber-Vorfälle. Zusätzlich zu der Tatsache, dass Cyber-Bedrohungen sowie -Schäden nicht so leicht zu erkennen oder zu erfassen sind wie physische Bedrohungen, spielt hier auch eine Rolle, dass Unternehmen Angriffe und insbesondere

Sicherheitslücken oftmals aus Angst vor Reputationsschäden nicht freiwillig publik machen möchten. Der Mangel an Daten erschwert in Folge die Modellierung von Cyber-Risiken hinsichtlich der Häufigkeit und Schwere künftiger Schäden.[6]

Dynamik des Cyber-Risikos

Selbst wenn Daten zur Verfügung stehen, stellt sich die Frage, ob diese auch einen aussagekräftigen Indikator für zukünftige Entwicklungen darstellen.[7] Denn Cyber-Risiken entwickeln sich stetig weiter. Dies liegt insbesondere an der Zunahme von Geschwindigkeit und Ausmaß des digitalen Wandels. Infolge sind bestehende Systeme der IT-Sicherheit schnell veraltet und reichen nicht mehr aus. Gleichzeitig erhöht sich mit der Verbreitung von internetfähigen Geräten die Vernetzung und damit die Anzahl an Schwachstellen. So verfügen viele dieser Geräte kaum über Sicherheitsfunktionen und vergrößern damit die Angriffsfläche für Hacker. Ein weiterer sich stetig verändernder Risikofaktor liegt in den Angreifern. Auch diese verwenden immer komplexere Technologien und neue Angriffsmethoden.[8] Da sich das Risiko sowie die zugrunde liegenden Risikofaktoren kontinuierlich weiterentwickeln, verlieren Informationen über vergangene Angriffe an Relevanz zur Vorhersage künftiger Risiken und auch bisher noch gänzlich unbekannte Cyber-Bedrohungen sind möglich.[9] Für den versicherungstechnischen Risikotransfer von Cyber-Risiken stellt der technologische Wandel folglich eine bedeutende Herausforderung dar.[10]

Informationsasymmetrie

Ein weiteres Problem bei der Versicherbarkeit von Cyber-Risiken stellt die bestehende Informationsasymmetrie zwischen Versicherer und Kunde dar. So kommt es zu adverser Selektion, da die Versicherer weniger als die Versicherungsnehmer über deren Risikosituation wissen, was eine Differenzierung zwischen guten und schlechteren Risiken verhindert. Intransparenz herrscht insbesondere bezüglich des individuellen Schadenrisikos der Unternehmen und der verwendeten IT-Sicherheitssysteme.[11] Dabei ist es wahrscheinlicher, dass Unternehmen, die schon einmal von einem Cyber-Angriff betroffen waren, Versicherungsschutz nachfragen. Darüber hinaus ist auch das moralische Risiko von Bedeutung, das darin besteht, dass Versicherte nach Vertragsabschluss weniger in eigene IT-Sicherheit investieren.[12] Die beschriebene Informationsasymmetrie hat infolge bedeutenden Einfluss auf die Bereitschaft der Versicherer Cyber-Risiken zu tragen.[13]

Kumulrisiko

Eine weitere Herausforderung bezüglich der Versicherbarkeit von Cyber-Risiken ist, dass diese oft stark voneinander abhängig sind. Innerhalb von Unternehmen kann diese Interdependenz dazu führen, dass Angreifer durch ein kompromittiertes System auf alle anderen IT-Systeme, Software

und Infrastrukturen Zugriff erhalten. Darüber hinaus ist insbesondere problematisch, dass bei der von Unternehmen genutzten IT, bspw. den Betriebssystemen oder Sicherheitsprogrammen, größtenteils Monokulturen bestehen. Dies hat zur Folge, dass ein erfolgreicher Angriff auf ein Online-Gerät bei einem Unternehmen bedeutet, dass dieser auch bei vielen weiteren IT-Komponenten möglich wäre.[14] Ein einzelnes Schadenereignis könnte zu einer weltweiten Schadenkumulierung führen. Dieses Ansteckungsrisiko besteht besonders dann, wenn mögliche Sicherheitsmaßnahmen unterlassen werden.[15] Das Risiko solch großer Kumulschäden ist damit ein weiterer Aspekt, der die Bereitschaft der Versicherer Cyber-Risiken zu übernehmen beeinflusst.[16]

Maßnahmen zur Verbesserung der Versicherbarkeit von Cyber-Risiken

Versicherungstechnische Risikopolitik

Auf Basis der beschriebenen Herausforderungen, soll nun betrachtet werden, wie Versicherungslösungen aussehen und wie darüber hinaus die Versicherbarkeit verbessert werden könnte.

Grundsätzlich ist Rückversicherung die gängigste Art des Risikotransfers für Erstversicherer.[17] Hierdurch kann insbesondere dem Kumulrisiko und den seltenen Großrisiken begegnet werden. Rückversicherer sind in der Regel besser diversifiziert als Erstversicherer, bieten den Erstversicherern also indirekt die Möglichkeit ihr Portfolio zu diversifizieren und damit ihre Deckungskapazität zu erhöhen.[18] Die bereits beschriebene Gefahr von möglichen sehr hohen Kumulschäden bei Cyber-Risiken beunruhigt allerdings auch die Rückversicherer, solange es keine wirksame Kontrolle gibt.[19]

Darüber hinaus hat ein Versicherer hinsichtlich der asymmetrischen Informationsverteilung verschiedene Möglichkeiten, um diese zu reduzieren. Um der adversen Selektion entgegenzuwirken und das Informationsdefizit hinsichtlich des Risikoprofils der Kunden zu reduzieren, kann ein Versicherer je nach Versicherungssumme mittels standardisierter Fragebögen oder spezieller technologischer Untersuchungen Informationen über die verwendeten IT-Systeme einholen und dieses Screening obligatorisch für den Vertragsabschluss machen. Das Problem des moralischen Risikos kann mithilfe von Ausschlüssen, Obliegenheiten, Selbstbeteiligungen und Haftungs-Sublimiten beschränkt werden, da auf diese Weise Anreize zur eigenen Prävention des Versicherungsnehmers geschaffen werden. Guten Risiken wird dadurch zusätzlich die Möglichkeit des Signalings hinsichtlich der eigenen Risikolage und der vorhandenen IT-Sicherheit gegeben.[20]

Pool-Lösungen

Der Großrisiken- sowie Kumulproblematik kann neben der Rückversicherung auch durch Pool-Lösungen begegnet werden. Indem die einzelnen Versicherer Risiken teilen, kann insgesamt die Versicherbarkeit von Katastrophenschäden aus Cyber-Vorfällen erhöht werden. Die Versicherer können durch einen Cyber-Pool ihre Verbindlichkeiten entsprechend ihrer Risikobereitschaft begrenzen und trotzdem gleichzeitig ihre Deckungskapazitäten ausweiten.[21] Möglich macht dies der Vorteil von Versicherungspools, Risiken der gleichen Art in einem Portfolio zu akkumulieren und dieses dadurch soweit zu vergrößern, dass von den entstehenden Diversifikationseffekten profitiert werden kann. Darüber hinaus können neben Kapital auch Ressourcen wie Wissen, Erfahrung und Daten ausgetauscht und gebündelt werden, wodurch die Zeichnung großer Risiken ermöglicht wird. Bei einer solchen Lösung muss allerdings beachtet werden, dass das Bilden von Versicherungspools unter Beteiligung des Staates einen Eingriff in den freien Markt darstellt, was nur durch Marktversagen zu rechtfertigen wäre. Ein Grund für eine solche Intervention kann im Falle von Cyber-Risiken in der mangelnden Versicherbarkeit bzw. Deckungskapazität gesehen werden.[22]

Risikotransfer über die Kapitalmärkte

Eine weitere Möglichkeit zur Erhöhung der Versicherbarkeit von Cyber-Risiken stellt die Übertragung von Großrisiken auf die Kapitalmärkte dar. Die Entwicklung von Anlageinstrumenten bzw. Verbriefung von Versicherungsrisiken zu Cyber-Katastrophenanleihen ermöglicht, dass Kapitalmarktinvestoren einen Teil des Risikos übernehmen. Mittels solcher Katastrophenanleihen können selbst für Rückversicherer zu große Schadenausmaße abgedeckt werden. Ihr Vorteil besteht zudem darin, dass die zugrunde liegenden Gefahren in der Regel nicht zeitgleich mit anderen Ereignissen auftreten, die sich auf die Kredit- und Aktienmärkte auswirken und den Investoren damit eine Diversifizierung ihres Risikos ermöglichen. Dies ist allerdings ein Punkt, der in Bezug auf Cyber-Risiken noch fraglich ist und wo potenzielle Anleger überzeugt werden müssen, dass ein Cyber-Angriff nicht gleichzeitig auch den Wert von Aktien und anderen Anleihen schmälern könnte. Eine weitere Hürde für den Cyber-Risikotransfer auf die Kapitalmärkte besteht darin, dass Anleger häufig Verbriefungen erwarten, bei denen die Auszahlung an eindeutige, beobachtbare Kennzahlen geknüpft ist. Bei Cyber-Risiken sind, wie zuvor beschrieben, die Risikofaktoren zum Teil unklar oder schwer beobachtbar, bspw. die Motivation zur Schadensbegrenzung in Form von IT-Sicherheit. In diesem Punkt kann jedoch mehr Informationsaustausch

helfen, um Klarheit über z. B. Deckungsbedingungen oder Ausschlüsse zu schaffen. Auch wenn der Markt für die Übertragung von Cyber-Risiken auf die Kapitalmärkte noch eher am Anfang steht, zeigt die Erfahrung mit Naturkatastrophenanleihen, dass dieser z. B. durch Produktinnovationen oder verbesserte Standardisierung von Cyber-Bedrohungen an Bedeutung zunehmen wird.[23]

Informations- und Datenaustausch

Um aus versicherungsmathematischer Sicht Risikoereignisse und ihre Folgen richtig abschätzen und modellieren zu können, ist Wissen über die Bandbreite und Auswirkungen möglicher Cyber-Risiken genauso wie die Zuverlässigkeit der Daten essenziell. Die Erfassung und Analyse von relevanten Informationen und Daten ist damit ein entscheidender Faktor für die Versicherbarkeit von Cyber-Risiken. Doch wie zuvor beschrieben stellt die Verfügbarkeit von ausreichend Informationen, vor dem Hintergrund der Neuartigkeit des Risikos, aber auch der herrschenden Informationsasymmetrie, eine große Herausforderung dar. Generell ist eine Bereitschaft vieler Unternehmen vorhanden, Informationen über Cyber-Vorfälle auszutauschen, wenn dies bessere Versicherungslösungen zur Folge hat. Um dabei die von den Unternehmen befürchteten Reputationsschäden zu vermeiden, könnten Daten bspw. über einen Drittanbieter gesammelt sowie anschließend anonymisiert weitergegeben werden und somit ein allgemeiner Rahmen für die Erfassung wichtiger Daten zu Cyber-Vorfällen und Schwachstellen geschaffen werden.[24] Zudem sollte auch die Versicherungswirtschaft selbst auf globaler Ebene zusammenarbeiten, um relevante Informationen zu sammeln und zu verbreiten, um bisher fehlende einheitliche Standards zu setzen und um bewährte Verfahrensweisen im Umgang mit Cyber-Risiken zu teilen. Mit der Implementierung eines anonymisierten Datenpools könnte folglich die Unsicherheit in Bezug auf Daten und Modellierung reduziert werden. Darüber hinaus ist es mit Blick auf den stetigen technologischen Wandel besonders wichtig, dass Versicherer neue Entwicklungen kontinuierlich verfolgen und dabei auch selbst über die benötigte IT-Sicherheitsexpertise verfügen, um Cyber-Risiken ausreichend zu verstehen. Auch dies wird durch den Austausch zwischen den Versicherern vereinfachter ermöglicht.[25]

Unterstützung durch den Staat

Solange es bei anderen Risikotransfermechanismen noch Schwierigkeiten gibt, kann auch der Staat eine wichtige Rolle bei der Stärkung der Cyber-Widerstandsfähigkeit und damit auch -Versicherbarkeit spielen. Hierbei sind vor allem zwei Bereiche relevant, zum einen die Erfassung sowie Verbreitung von Informationen zu Cyber-Bedrohungen und -Schäden und zum anderen die Schaffung rechtlicher Rahmenbedingungen.[26]

Um den Datenaustausch bezüglich Cyber-Risiken zu fördern, können Regierungen die Einrichtung von Plattformen bzw. anonymisierten Datenbanken unterstützen und den branchenweiten Informationsaustausch koordinieren. Auch Versicherer bekommen auf diese Weise Zugang zu diesen wichtigen Informationen, welche ihnen dabei helfen die Risiken besser zu verstehen und zu modellieren. In Folge kann risikogerechtere Versicherung angeboten werden mit bspw. niedrigeren Prämien und höheren Kapazitäten für Cyber-Schutz.[27] Regierungen könnten diesen Austausch zudem auf internationaler Ebene fördern, was insbesondere bei einem Risiko wie Cyber, bei dem sich Bedrohungen oder Angriffe relativ leicht auf globaler Ebene ausbreiten könnten, von Bedeutung ist. Um verbesserte IT-Sicherheitsstandards zu erreichen, kann der Staat des Weiteren zum einen zu Aufklärung und Sensibilisierung zum Thema Cyber-Risiken beitragen und damit das Risikobewusstsein erhöhen oder zum anderen auch Mindeststandards entwickeln. Solche Mindeststandards zur IT-Sicherheit würden damit das zuvor beschriebene Problem des moralischen Risikos, nach Vertragsabschluss weniger in IT-Sicherheit zu investieren, reduzieren.[28] Versicherern ist es je nach Einhaltung der Standards zudem möglich die Risikolage des potentiellen Versicherungsnehmers vorab besser einzuschätzen, was in Folge die Bereitschaft Cyber-Versicherung anzubieten erhöhen kann.[29]

Aus einer rechtlichen Perspektive könnte der Staat darüber hinaus Cyber-Versicherung zumindest für Schlüsselindustrien mit einem hohen Angriffsrisiko obligatorisch machen. Dies könnte neben einem größeren Pool an Versicherten dazu führen, dass Unternehmen verstärkt in ihre Cyber-Sicherheit investieren, um Prämien zu senken. Andererseits wären neben einem hohen administrativen Aufwand allerdings zum Teil auch wieder Moral-Hazard-Probleme zu befürchten, da sich Unternehmen auf ihre Versicherung verlassen könnten, anstatt in Sicherheit zu investieren. Letztlich hätte der Staat auch die Möglichkeit zur Bildung von Pool-Lösungen beizutragen und damit wie zuvor beschrieben die Versicherbarkeit zu erhöhen. Neben der Übernahme eines Teiles der Verwaltungskosten könnte die Beteiligung des öffentlichen Sektors insbesondere die Zusammenarbeit und den Informationsaustauch erleichtern sowie sicherstellen, dass Pooling-Vereinbarungen dem Wettbewerbsrecht entsprechen.[30]

Fazit

Angefangen mit dem Mangel an Informationen durch die Neuartigkeit des Risikos, über den technologischen Wandel und die herrschende Informationsasymmetrie, bis hin zur Kumulproblematik ergeben sich in Bezug auf die Versicherbarkeit von Cyber-Risiken verschiedenste Herausforderungen. Durch versicherungstechnische Risikopolitik, in Form von bspw. Selbst-

behalten, Haftungslimits oder Obliegenheiten wird Informationsasymmetrie reduziert und Versicherung grundsätzlich möglich gemacht. Der Nutzerkreis wird hierdurch jedoch limitiert und die Grenzen der Versicherbarkeit werden demnach nicht erweitert.[31] Möglichkeiten, um den Versicherungsmarkt trotz der beschriebenen Beschränkungen zu vergrößern, können Rückversicherung oder der Risikotransfer auf die Kapitalmärkte sein. Darüber hinaus kann mithilfe von Pool-Lösungen der Problematik von Kumulschäden und mangelnder Informationen zum Risiko begegnet werden. Die Einführung eines solchen Versicherungspools, könnte auch gut mit der Implementierung eines Datenpools kombiniert werden.[32] Denn insbesondere die Erfassung und der Austausch von Daten und Wissen sind zur Bewältigung vieler der Herausforderungen essenziell. So können Risiken durch ausreichend Informationen zunächst besser verstanden und modelliert werden, Informationsasymmetrie z. B. durch einheitliche Standards abgebaut werden und durch Verknüpfung von Expertise auch neue technologische Entwicklungen erkannt und berücksichtigt werden. Hierbei und auch bei der Schaffung rechtlicher Rahmenbedingungen kann dem Staat eine wichtige unterstützende Rolle zukommen.

Auch wenn es letztlich nicht versicherbare Cyber-Risiken geben kann, die im Zusammenhang mit extremen, katastrophalen Schadenereignissen stehen und bei denen die natürlichen Grenzen für die Risikotragung privater Versicherer erreicht sind, kann mittels der verschiedensten beschriebenen Maßnahmen sowie der Zusammenarbeit von Versicherern und Versicherungsnehmern die Versicherbarkeit von Cyber-Risiken verbessert werden.[33] Durch den technologischen Wandel und die dynamische Natur des Cyber-Risikos wird es jedoch immer neue Herausforderungen geben und Anpassungen werden stetig erforderlich sein.[34]

---

1 Vgl. Munich Re, o. J.
2 Vgl. Swiss Re, 2017, S. 1-3.
3 Vgl. World Economic Forum, 2020, S. 12.
4 Vgl. Swiss Re, 2017, S. 1.
5 Vgl. Haas, 2016, S. 214.
6 Vgl. Swiss Re, 2017, S. 19.
7 Vgl. Eling / Schnell, 2016, S. 30.
8 Vgl. Swiss Re, 2017, S. 4-8.
9 Vgl. Swiss Re, 2017, S. 19.
10 Vgl. Haas, 2016, S. 31.
11 Vgl. Haas, 2016, S. 205-206.
12 Vgl. Eling / Schnell, 2016, S. 31.
13 Vgl. Swiss Re, 2017, S. 30.
14 Vgl. Swiss Re, 2017, S. 20.
15 Vgl. Haas, 2016, S. 31.
16 Vgl. Swiss Re, 2017, S. 22.
17 Vgl. Eling / Wirfs, 2016, S. 36.
18 Vgl. Klimaszewski-Blettner, 2010, S. 12-13.
19 Vgl. Swiss Re, 2017, S. 22.
20 Vgl. Haas, 2016, S. 206-210.
21 Vgl. Swiss Re, 2017, S. 33-34.
22 Vgl. Eling / Schnell, 2016, S. 34.
23 Vgl. Swiss Re, 2017, S. 34-35.
24 Vgl. Swiss Re, 2017, S. 30-31.
25 Vgl. Eling / Schnell, 2016, S. 33-34.
26 Vgl. Swiss Re, 2017, S. 35.
27 Vgl. Swiss Re, 2017, S. 35-37.
28 Vgl. Eling / Schnell, 2016, S. 35-36.
29 Vgl. Swiss Re, 2017, S. 37.
30 Vgl. Swiss Re, 2017, S. 37-38.
31 Vgl. Haas, 2016, S. 218.
32 Vgl. Eling / Schnell, 2016, S. 34.
33 Vgl. Swiss Re, 2017, S. 39.
34 Vgl. Eling / Wirfs, 2016, S. 134.

Literaturverzeichnis

Eling, Martin / Schnell, Werner (2016): Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Zürich 2016.

Eling, Martin / Wirfs, Jan Hendrik (2016): Cyber Risk: Too Big to Insure?: Risk Transfer Options for a Mercurial Risk Class, in: I. VW-HSG Schriftenreihe des Instituts für Versicherungswirtschaft Universität St. Gallen, Bd. 59, St. Gallen 2016.

Haas, Andreas (2016): Management von Cyber-Risiken und Möglichkeiten des Risikotransfers: eine ökonomische und versicherungstechnische Analyse, Diss., Universität Hohenheim, Hohenheim 2016.

Klimaszewski-Blettner, Barbara (2010): Management von Katastrophenrisiken: Herausforderungen, Ansatzpunkte und Strategien im Rahmen einer Public-Private-Partnership, Karlsruhe 2010.

Munich Re (o. J.): Cyber-Risiken: Cyber-Bedrohungen zählen zu den größten Risiken des 21. Jahrhunderts, https://www.munichre.com/de/risiken/cyber-risiken.html, Stand 24.03.2020.

Swiss Re (Hrsg.) (2017): Cyber: Bewältigung eines komplexen Risikos, sigma Nr. 1/2017, Zürich 2017.

World Economic Forum (Hrsg.) (2020): The Global Risks Report 2020, Cologny 2020.

Schadenszenario im Cyber-Angriffsfall auf ein Versicherungsunternehmen

Von Maximilian Lang

Einleitung

„Das Internet ist für uns alle Neuland“[1] gab Kanzlerin Angela Merkel am 23.06.2013 auf einer Pressekonferenz zu verstehen. Dies geschah zu einem Zeitpunkt als Barack Obama noch den Präsidentenposten der USA innehatte und in Deutschland eine heftige Debatte losgebrochen war, weil deutsche Privatpersonen und Unternehmen durch die Amerikaner vor allem über das von Merkel erwähnte Internet ausspioniert wurden. Fünf Jahre später haben deutsche Unternehmen das Internet und die Digitalisierung näher kennengelernt und in die meisten Teile ihrer Unternehmen implementiert. Das eröffnet völlig neue Möglichkeiten und Chancen, erhöht aber auch das Risiko, Opfer eines Cyberangriffes zu werden. „Fast neun von zehn Institutionen erwarten von der Digitalisierung eine Verschärfung der Bedrohungslage“[2] hat eine Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Jahre 2018 herausgefunden. Dementsprechend stellt sich die Frage welche Eigenschäden einem Unternehmen im Angriffsfall entstehen können? Die Beantwortung dieser Frage ist das Ziel dieser Arbeit.

Die Beschäftigung mit den aktuellen Cyber-Angriffsformen ist für den Entwurf von Schadenszenarien und ihrer wirtschaftlichen Bewertung unabdingbar. Deshalb entwirft dieser Beitrag nach der Einführung in verschiedene Cyber-Angriffsszenarien ein Schadenszenario für ein Unternehmen, das in der Versicherungsbranche tätig ist und zeigt mögliche Kosten auf, die in einem solchen Fall entstehen können.

Die große Zahl an zu berücksichtigenden Faktoren führt dazu, dass nur in einer Einzelfallanalyse konkrete Zahlen zuverlässig benannt werden könnten.[3]

Entwicklung eines Schadenszenarios

Definition Cyber-Angriff und Schadenszenario

Im Kapitel zwei werden erst die Definitionen des Cyber-Angriffs und eines Schadenszenarios erläutert, um dann auf die Angriffsformen eingehen zu können. Danach wird ein fiktives Schadenszenario auf ein Unternehmen durch einen ATP-Angriff erstellt und mögliche entstehende Eigenschäden aufgezeigt.

Um Schadenszenarien entwerfen zu können muss zuerst eingegrenzt werden, was ein Cyber-Angriff ist und wie ein Schaden in diesem Zusammenhang definiert werden kann. Laut dem Glossar der Cyber-Sicherheit des BSI ist „ein Cyber-Angriff [..] eine Einwirkung auf ein oder mehrere andere

informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen."[4]

Ein Schaden ist definiert durch die Auswirkung auf die Erreichung der Unternehmensziele. Schäden können immaterielle oder materielle Gestalt haben. Als Szenario werden denkbare Schadenereignisse beschrieben.[5] Unterteilt werden die entstandenen Schäden, angelehnt an den Leitfaden der Bitkom, nach Eigenschäden (zum Beispiel Schäden durch Betriebsunterbrechung) und Fremdschäden (zum Beispiel Haftungskosten gegenüber Dritten). Die Grenzen können hier teilweise fließend verlaufen und müssen im Einzelfall abgewogen werden.[6] Diese Arbeit konzentriert sich auf entstehende Eigenschäden.

Angriffsformen

Zum besseren Verständnis der einem Unternehmen im Angriffsfall entstehenden Schäden sind Grundkenntnisse über die wichtigsten Cyber-Angriffsformen unabdingbar. Die Aufzählung der Cyber-Angriffsformen ist an den aktuellen Lagebericht IT-Sicherheit des BSI[7] angelehnt. Beschrieben werden die für ein Unternehmen, das in der Finanz- und Versicherungsbranche tätig ist, relevantesten Formen.

1. Identitätsdiebstahl: im Internet und auch in der für uns relevanten Cyber-Welt wird hiermit der Diebstahl von Identifikations- und Authentifizierungsdaten beschrieben. Beim sogenannte Pishing werden mithilfe von Werkzeugen des Social Engineerings beispielsweise der Benutzername und das Passwort eines Individuums erbeutet.

2. Schadprogramme: sind Bestandteil der meisten Angriffsszenarien und können unerwünschte und schädigende Funktionen auf einem Computersystem ausführen. Sie setzen „sich zusammen aus Trojanern (mit dem Zweck, Information zu stehlen bzw. Systemzugang zu ermöglichen), Viren (mit dem Zweck, ein System zu zerstören), oder Würmern (Viren, die besonders leicht auf andere Systeme gelangen)."[8]

3. Ransomware: verwehrt oder schränkt den Zugang zum eigenen Rechner oder den eigenen Daten durch Verschlüsselung ein um ein Lösegeld zu erpressen oder das Opfer betriebsunfähig zu machen. Bekannte Ransomware-Angriffe sind der NotPetya- und der WannaCry-Fall.

4. Distributed Denial of Service (DDoS): während eines DDoS-Angriffes wird eine große Anzahl von durch einen Aggressor übernommenen Computer zu einem Command-and-Control-Server zusammengeschlossen. Diese werden dann dafür genutzt, Webseiten, Netzwerke oder Server zu überlasten und damit zu verlangsamen oder ganz vom Netz zu nehmen.

5. Hybrid-Angriffe: in dieser Angriffsart werden mehrere der genannten Formen miteinander kombiniert. Besonders hervorzuheben sind in diesem Bereich die Advanced Persistent Threat (APT)-Angriffe. APT-Angriffe sind meist auf die Verteidigungsstrategie ihrer Opfer angepasst, wodurch die Möglichkeit einer Abwehr minimiert wird.

Alle genannten Angriffsarten können alleinstehend ein Unternehmen in große Schwierigkeiten bringen. Werden die Angriffsarten jedoch wie bei einem APT zusammen verwendet, kann sich der Schaden für das Unternehmen nochmals maximieren. Mit welchen Schäden und Kosten muss ein Unternehmen in einem konkreten Angriffsszenario rechnen?

Schadensszenario: APT Angriff auf das Unternehmen XY

Das Unternehmen XY ist ein kleines Unternehmen mit 250 Mitarbeitern, welches in der Versicherungsbranche tätig ist. Herr Maier arbeitet in der Schadenregulierung des Versicherungsunternehmens XY und übernimmt für dieses die Vorbereitung der eingehenden Schadensfälle (Scannen und Sortierung) und einfache Regulierungsaktivitäten.

Herr Maier bekommt eine Mail, welche vorgibt vom Unternehmen XY zu stammen. Der Mitarbeiter soll seinen Benutzernamen und sein Passwort eingeben, um testen zu lassen, ob das Passwort sicher sei. Durch diesen Trick bekommt der Angreifer Zugriff auf den Computer des Mitarbeiters und alle Regulierungsprogramme, mit denen die Schäden aufbereitet und reguliert werden. Er schleust eine Schadsoftware ein, die sich über das Netzwerk auf alle anderen Rechner und Programme im Unternehmen ausbreitet. Mittels einer Ransomware, die das Schadprogramm eigenständig nachlädt, werden alle Daten auf den Rechnern verschlüsselt und eine Schadenbearbeitung unmöglich. Der Erpresser fordert vom Unternehmen XY ein Lösegeld, um die Daten wieder zu entschlüsseln.

Welche Schäden können dem Unternehmen XY aufgrund dieses Angriffes entstehen?

Eigenschäden

Wie schon in der Einleitung erwähnt wird auf die Eigenschäden eingegangen, die dem Unternehmen XY in diesem Fall entstehen könnten. Die Zusammenstellung der Kostenpositionen ist angelehnt an den Leitfaden des Bitkom[9]:

1. Betriebsunterbrechung: aufgrund des Angriffes kommt es zu Betriebsunterbrechungen, da betroffene kritische Prozesse und Anwendungen nicht zur Verfügung stehen. Dadurch kann unter anderem ein System-Shutdown notwendig werde, sodass diese Ausfallzeiten berücksichtigt werden müssen. Außerdem kann eine Neuinstallation des Systems notwendig sein, welche Zeit

und Ressourcen bindet. Während dieser Zeit ist keine Fallbearbeitung möglich.

2. Schadenermittlung und IT-Forensik: das Unternehmen XY versucht die Ursachen des Angriffes und das Ausmaß zu ermitteln, sodass dies zum Beispiel für die juristische Nachbearbeitung genutzt werden kann.

3. Management der Schadenbewältigung und Krisenberatung: da das Unternehmen XY nur ein kleines Unternehmen ist, hat es sich zwar schon mit Maßnahmen zur Krisenbewältigung auseinandergesetzt, jedoch wurde entschieden, dass die Gründung eines permanenten Krisenstabes und die Erstellung von Krisenmanagementplänen und die Einübung von Notfall- und Wiederanlaufmaßnahmen wirtschaftlich nicht lohnenswert sei. Deshalb muss sich das Unternehmen ein externes Krisenmanagement und eine externe Beratung einkaufen, die diese Aufgaben in der Krise übernehmen.

4. Wiederherstellungskosten: für die Wiederherstellung der Regulierungssysteme und der Daten auf einen Zustand vor dem Angriff durch ein Backup, welches zwei Tage vor dem Angriff erstellt wurde, kommen Personalkosten auf das Unternehmen zu. Die Daten der letzten zwei Tage müssen rekonstruiert werden und der Systemausfall analysiert werden. Das nimmt Zeit in Anspruch und verzögert den Betriebsablauf.

5. Verbesserung der Organisations- und IT-Strukturen: damit Angreifer nach Wiederherstellung des Systems nicht sofort wieder in die gleiche Sicherheitslücke eindringen können, muss das System davor gehärtet werden. Dazu fallen Kosten für eine Schwachstellenanalyse und -adressierung zusammen mit der Entwicklung von Lösungsmöglichkeiten und deren Umsetzung an. Hier sollten zum Beispiel Mitarbeiterschulungen zur Sensibilisierung durchgeführt werden.

6. Rechtsberatungskosten: während und nach der Krise müssen sowohl Datenschutzverletzungen und Haftungsansprüche gegenüber Dritten, als auch Informationspflichten geprüft werden. Außerdem kann der Angriff Auswirkungen auf die Vertragsbeziehungen haben, da bestimmte Servicelevel-Vereinbarungen mit beispielsweise Großkunden nicht eingehalten werden konnten, die für den Fortbestand des Vertrages essenziell gewesen wären.

7. Informationskosten sowie Vertragsstrafen und Bußgelder: das Unternehmen muss seinen gesetzlich festgeschriebenen Informationspflichten im Falle eines Angriffes nachkommen und die betroffenen Kunden oder Behörden informieren. Dazu müssen Rückmeldekanäle zur Verfügung gestellt werden.

Zusätzlich können bei der Verletzung der gesetzlichen Pflichten Strafen ausgesprochen werden. In diesem Fall muss XY analysieren, ob der Angreifer die Möglichkeit hatte, die verschlüsselten Daten einzusehen und diese abzugreifen (IT-Forensik).

8. Reputationskosten: während der Betriebsunterbrechung können keine Schäden bearbeitet werden, sodass sich für die Kunden Verzögerungen in der Auszahlung ergeben. Dies führt zu einem Reputationsschaden für die Firma XY. Deshalb ist eine schnelle und aufrichtige Krisenkommunikation wichtig, sodass der Ärger der Kunden aufgefangen werden kann und diese Informationen zum aktuellen Stand der Krisenbewältigung erhalten. Auch wird damit versucht, die Kundenabwanderung präventiv einzudämmen, sodass im Nachhinein weniger Kosten notwendig sind, um die Reputation unter anderem mit zusätzlichen Marketing- und Kundebindungsmaßnahmen wiederaufzubauen.

9. Lösegeldkosten: die Behörden raten davon ab, in Fällen von Ransomware-Angriffen das geforderte Lösegeld zu überweisen. Hier ist eine genaue Betrachtung notwendig, ob es sich kostentechnisch lohnen würde, das Lösegeld zu zahlen und, ob damit zu rechnen ist, dass der Angreifer die verschlüsselten Daten nach der Zahlung wieder freigibt.

In diesem Kapitel wurden die relevanten Definitionen des Cyberangriffs und des Schadenszenarios, sowie unterschiedliche Cyber-Angriffsformen vorgestellt und als Beispiel die entstehenden Eigenschäden in einem fiktiven APT Angriff auf ein Unternehmen beleuchtet.

Ausblick

Dieser Beitrag enthält nur eine Aufzählung der Schäden, die dem Unternehmen direkt aus einem Cyberangriff entstehen könnten. Schäden gegenüber Dritten sind nicht erwähnt worden, können jedoch einen beträchtlichen Teil des Schadens für Unternehmen ausmachen. Am Ausmaß dieser ist schon zu erkennen, dass ein Cyber-Angriff Unternehmen, ob kleinen oder großen, schwere Schäden zufügen kann. Es gibt dennoch heutzutage Möglichkeiten, wie sich Unternehmen gegen diese Art der Bedrohung absichern können. Durch Cyberversicherungen kann ein Großteil der Kostenrisiken, wie sie weiter oben beschrieben wurden, abgedeckt werden. Jedoch ist der Markt noch jung und befindet sich im Aufbau, weshalb die Auswahl und der Service nicht das Level erreicht, welches in anderen Versicherungsbereichen Standard ist. Auch muss auf einige Prozesse, welche im Moment noch im Gange sind, hingewiesen werden. In diesen soll unter anderem geklärt werden, ob Angriffe, die vermeintlich durch Staaten gestartet wurden, wie das beispielsweise beim Virus „NotPetya“ angenommen wird, in den Policen versichert

sind. Hier ist aber zu erwarten, dass sich der Markt und der Umfang der Policen schnell erweitern wird und die rechtlichen Unsicherheiten aus dem Weg geräumt werden können, sodass es für jedes Unternehmen, ob klein oder groß, zukünftig ratsam sein wird, sich eine Cyberversicherung zuzulegen.

---

[1] Waleczek (2013).
[2] Bundesamt für Sicherheit in der Informationstechnik (18.04.2019), S. 7.
[3] Vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2016), S. 4.
[4] Bundesamt für Sicherheit in der Informationstechnik (2020).
[5] Vgl. Klipper (2015), S. 28.
[6] Vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2016), S.4.
[7] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2019), S. 6-35.
[8] Leopold u.a. (2015), S. 49.
[9] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2016).

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (2019): Die Lage der IT-Sicherheit in Deutschland 2019, Bonn, URL: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

Bundesamt für Sicherheit in der Informationstechnik (18.04.2019): Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen, URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9.

Bundesamt für Sicherheit in der Informationstechnik (2020): Glossar der Cyber-Sicherheit, URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817276, Stand: 28. März 2020.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2016): Kosten eines Cyber-Schadensfalles - Leitfaden, URL: https://www.bitkom.org/sites/default/files/file/import/160426-LF-Cybersicherheit.pdf.

Klipper, Sebastian (2015): Cyber Security. Ein Einblick für Wirtschaftswissenschaftler, 1. Aufl., Wiesbaden.

Leopold, Helmut/Skopik, Florian/Bleier, Thomas (Hrsg.) (2015): Cyber Attack Information System. Erfahrungen und Erkenntnisse aus der IKT-Sicherheitsforschung, Berlin/Heidelberg.

Waleczek, Torben (2013): Merkels "Neuland" wird zur Lachnummer im Netz, URL: https://www.tagesspiegel.de/politik/die-kanzlerin-und-das-internet-merkels-neuland-wird-zur-lachnummer-im-netz/8375974.html, Stand: 29. März 2020.

Übersicht zu möglichen Kumulrisiken im Bereich der Cyber-Versicherungen

Von Antong He

Einleitung

Die Digitalisierung schreitet mit großen Schritten voran. Dies kann neben Chancen auch viele Risiken bergen. Für die Versicherungsbranche öffnet sich ein neues Geschäftsfeld: die Cyber-Versicherung. Dabei stellt sich die Frage, wie ein solch unbekanntes Risiko versicherbar gemacht werden kann. Dabei spielt die Betrachtung von Kumulrisiken eine große Rolle. Nach einer Befragung der OECD ist das Kumulrisiko der wichtigste Treiber von Cyber-Risiken und mehr als 60% der Befragten sehen das Kumulrisiko mit Sorge.[1] Im folgenden Beitrag sollen nun unterschiedliche Kumulrisiken gezeigt und Szenarien analysiert werden. Dafür wird betrachtet, welche Art von Kumulen bei Cyber-Versicherungen entstehen können, wie diese entstehen und welche Auswirkungen dies auf ein Versicherungsunternehmen haben könnte.

Einführung in Kumulrisiken

Zunächst soll der Begriff des Kumuls definiert werden. Unter Kumul versteht man eine „*Anhäufung **mehrer[er]** Schäden* aufgrund ***eines** Ereignisses* bei ***einem** Versicherungsunternehmen*“[2]. Herkömmlicherweise wird dieser Begriff bei Naturkatastrophen und bei Brandgefahren verwendet. Dabei kann durch ein einziges Ereignis ein hoher Schaden entstehen. Dies passiert zum Beispiel dann, wenn innerhalb eines kleinen geographischen Gebiets aufgrund eines Feuer- oder Elementarereignisses mehrere Gebäude zerstört werden, die alle bei einem Versicherungsunternehmen versichert sind. Dieses geographische Gebiet wird auch als Footprint (zu dt. Fußabdruck) bezeichnet.[3]

Bei Cyber-Risiken ist es, anders als bei den herkömmlichen Gefahren, eine große Herausforderung eine solche Einteilung des Footprints vorzunehmen. Gründe dafür sind unter anderem die zunehmende Digitalisierung von Wertschöpfungsketten, die industrieübergreifende Vernetzung in Clouds und der zunehmende Einsatz von Internet of Things-Geräten in Privathaushalten. Dies führt zu einem Risiko, das weitgehend undurchsichtig ist, keine strikten Grenzen kennt und sich über Landesgrenzen und unterschiedliche Industriesektoren hinaus verbreiten kann.[4] Des Weiteren kann es sein, dass bereits viele Schäden durch ein Cyber-Ereignis eingetreten sind und noch nicht bemerkt wurden. Nur mit der Zeit und weiteren Akkumulation der Schäden wird manchmal klar, dass diese von einem Auslöser ausgehen, z. B. einer Lücke in einer Software.[5] All diese Tatsachen erschweren die Einschätzung des Cyber-Kumulrisikos der Versicherungsunternehmen im Vergleich zu herkömmlichen Gefahren. Für Cyber-Risiken gibt es unterschiedliche

Arten von Cyber-Versicherungen. Unternehmen und auch Privatpersonen können Eigenschäden und Schäden bei Dritten, für die sie haften müssen, versichern. Eigenschäden beinhalten zum Beispiel Betriebsunterbrechungen und Kosten zur Wiederherstellung der Daten. Bei Drittschäden kann es sich um Ansprüche von Dritten handeln, wenn beispielsweise sensible Daten öffentlich werden und das betroffene Unternehmen oder die Privatperson dafür haften muss.

Virus, Sicherheitslücken und Malware als Auslöser von Kumulschäden

Entstehung des Risikos

Als erstes sind Viren, Sicherheitslücken in der Software und andere Malware als einer der Auslöser für Kumulrisiken im Cyber-Bereich zu nennen. Diese sind stark voneinander abhängig, d. h. dass durch eine Schwachstelle in einem System gleich mehrere Unternehmen auf einmal betroffen sein könnten.[6] Des Weiteren herrscht eine Monokultur an Software. Dies führt dazu, dass durch eine Sicherheitslücke eine große Zahl an Computern betroffen sein kann.[7] Käme es also zu einem großen Angriff, könnten gleichzeitig viele Unternehmen, die ähnliche Software (z. B. das Betriebssystem Windows), lahmgelegt werden. Für Versicherungsunternehmen sind solche Schäden besonders schwerwiegend, wenn sie mehrere der betroffenen Unternehmen gegen eine Betriebsunterbrechung, die durch einen Cyber-Vorfall ausgelöst worden ist, versichert haben.

Schadensszenario

Prominente Beispiele für Malware-Angriffe sind die Ransomware-Attacken „WannaCry“ und „NotPetya“, die im Frühjahr 2017 großen Schaden anrichteten. „NotPetya“, das eine Kombination aus zwei Sicherheitslücken im Betriebssystem ausnutzte, verschlüsselte die Daten des Computers irreversibel und forderte eine Lösegeldzahlung. Diese Ransomware hat nach Schätzungen des Weißen Hauses bei Unternehmen einen Schaden von 10 Milliarden US-Dollar verursacht.[8] Dabei wurden Unternehmen aus unterschiedlichen Sektoren getroffen, besonders jedoch die dänische Reederei Maersk, die ihr komplettes IT-System danach neu aufsetzen musste. Dies führte zu erheblichen Kosten durch eine Betriebsunterbrechung und die Wiederherstellung der IT.[9]

Neben solchen Ransomware-Attacken können Sicherheitslücken und Viren auch genutzt werden, um vertrauliche Daten zu extrahieren. Ein Beispiel dafür ist die sog. Sicherheitslücke „Heartbleed“. Dabei war es 2013 möglich, verschlüsselte Verbindungen zu und von Websites auszuhebeln und den Datenverkehr abzuhören.[10] In diesem Fall konnte die Sicherheitslücke gefunden und behoben werden, bevor es öffentlich wurde, es ist also kein größerer Schaden entstanden. Würden sensible Daten an

die Öffentlichkeit kommen, so müssten die davon betroffenen Unternehmen dafür haften. Somit wäre in diesem Fall der Haftpflichtversicherungsteil der Cyber-Versicherung betroffen.

Störung oder Angriff eines IT-Provider oder Infrastrukturprovider als Auslöser eines Kumulschadens

Entstehung des Risikos

Mit der zunehmenden Digitalisierung setzen immer mehr Unternehmen auf Cloud Service Provider (CSP) und sind somit auch auf das Funktionieren der Systeme bei den CSPs angewiesen.[11] Als Gründe für den zunehmenden Einsatz von CSPs werden von Unternehmen vor allem die Flexibilität und Effizienz von Cloud Systemen genannt.[12] Allein die größten vier Anbieter, Amazon AWS, Microsoft, IBM und Google hatten 2016 einen Marktanteil von über 50%.[13]

Der Ausfall eines CSPs könnte nicht nur zu Betriebsunterbrechungen bei den Kunden, sondern auch zu Forderungen aus der Haftpflichtversicherung führen, wenn sensible Daten an die Öffentlichkeit gelangen. Es kann auch zu hohen Wiederherstellungskosten führen, wenn durch den Ausfall Daten und Programme irreversibel gelöscht werden. Gleichzeitig kaufen auch CSPs Cyber-Deckungen, um sich gegen Ausfälle und Angriffe zu schützen. Dann müsste die Versicherung bei möglichen Regressansprüchen der Kunden aufkommen. Dies stellt hinsichtlich des Kumulrisikos bei den Versicherungsunternehmen eine große Herausforderung dar, da es die Möglichkeit für große Schäden von vielen unterschiedlichen Unternehmen durch den Ausfall eines CSPs, egal aufgrund welcher Ursache, gibt.[14]

Schadensszenario

Bis jetzt gab es keinen systemischen Großschaden, der durch eine Störung bei einem CSP entstanden ist, dennoch ist es wichtig die mögliche Gefahr zu verstehen.[15] Deswegen modellieren Lloyd's & Cyence (2017) dazu ein wahrscheinliches Szenario.[16]

Besonders anfällig für Attacken sind sog. „Hypervisors", die auf den Servern eine virtuelle Plattform generieren, auf denen verschiedene Virtual Machines gehostet werden.[17] Durch eine Störung des Hypervisors könnten unter anderem Daten verloren gehen und Virtual Machines außer Betrieb gesetzt werden.[18]

Lloyd's & Cyence modellieren in ihrem Szenario den Angriff von Hacktivisten auf einen CSP. Dabei versehen die Angreifer über einen Eingeweihten im Unternehmen schädlichen Code in einem Update, das eine neue Funktion für den sog. Hypervisor hinzufügen soll. Diese Schadsoftware wird so eingebaut, dass sie unerkennbar bleibt und erst nach einer gewissen Zeit ausgelöst wird. Nach etwa einem Jahr, nachdem das

Update auf Hypervisors bei verschiedenen CSPs installiert wurde, stürzen die Systeme aufgrund der Schadsoftware ab.[19] Lloyd's & Cyence schätzen, dass es für große Unternehmen mit priorisiertem Support bei den CSPs etwa 55 Stunden dauern könnte, bis der Fehler erkannt und behoben wird und somit der Betrieb wieder aufgenommen werden kann. Für kleinere Unternehmen, die einen schlechteren Support bei den CSPs haben, könnte dies fast bis zu sechs Tagen dauern.[20] Geschätzte Schadensummen bei dem genannten Szenario variieren je nach Sektor, besonders in den Sektoren Finanzdienstleistungen und Online-Handel sind hohe Schäden zu erwarten. Durchschnittlich schätzen Lloyd's & Cyence einen möglichen Großschaden, der von einer Cyber-Versicherung gedeckt wäre, auf etwa 4,6 Milliarden US-Dollar. Dabei berücksichtigen Lloyd's und Cyence nur Schäden durch Betriebsunterbrechung und zusätzliche Kosten, wie aus Datenrettung und -wiederherstellung. In der Praxis müsste man dazu noch mögliche Imageschäden und Materialschäden hinzurechnen.[21]

Ausfall oder Störung eines kritischen Infrastrukturproviders

Die Risiken, die durch eine Störung oder den Ausfall von kritischen Infrastrukturprovidern entstehen, sind grundsätzlich ähnlich zum o. g. Ausfall eines CSPs. Ein solcher Ausfall würde unterschiedliche Branchen treffen, selbst solche, die nicht auf ein funktionierendes IT-System angewiesen sind oder Unternehmen, dessen IT-Systeme voll funktionsfähig sind.

Beispielsweise kann die Lahmlegung des Systems der Flugverkehrskontrolle zu hohen Betriebsunterbrechungsschäden bei Fluggesellschaften führen, obwohl ihre eigenen IT-Systeme einwandfrei funktionieren.[22]

Interferenz bei finanziellen Transaktionen als Auslöser eines Kumulschadens

Entstehung des Risikos

Versicherer bieten für finanzielle Institutionen in ihren Cyber-Policen Schutz für Schäden, die durch Cyber-Diebstahl, Betrug oder kompromittierte Systeme entstehen. Kriminelle setzen nun weniger auf physische Banküberfälle und mehr auf Cyber-Kriminalität. Besonders davon betroffen sind Banken und Dienste für Zahlungsabwicklung und -transfers, wie Paypal, Visa und Mastercard.[23] Das Kumulrisiko entsteht zum einen daraus, dass durch einen Angriff sehr hohe Schadensummen möglich sind. Risk Management Solutions schätzt, dass durch Cyber-Kriminalität jährliche Kosten in Höhe von 445 Milliarden US-Dollar für die globale Wirtschaft aufkommen.[24] Zum anderen können durch einen Angriff gleich mehrere Unternehmen gleichzeitig angegriffen werden. 2011 wurden Visa, Mastercard und Paypal Opfer der gleichen Distributed-Denial-of-Service-Attacke. Dabei

wollten sich Hacktivisten an den Unternehmen für die Unterbindung von Zahlungen an Wikileaks rächen. Dies führte zu reduzierten Transaktionskapazitäten bei den Unternehmen.[25]

Schadensszenario

2013 wurde bekannt, dass eine Gruppe aus fünf Hackern mehrere Netzwerke von Finanzdienstleistern angegriffen hat. Dabei haben sie 160 Millionen Kreditkartendetails gestohlen und weitere 300 Millionen US-Dollar aus Visa Zahlungsströmen abgeleitet. Sie nutzten dabei eine Schwachstelle in Datenbanken, die es ihnen erlaubte, die vertraulichen Daten auszulesen.[26]

Aus Sicht der Versicherungen stellt dies ein großes Kumulrisiko dar, da durch den Angriff einer kleinen Gruppe viele Unternehmen getroffen wurden. Dies ist schwer vorherzusehen und würde besonders die Haftpflichtversicherung treffen, die wegen einer Datenschutzverletzung leisten müssten. Zudem müssten die Versicherungen für das abgezweigte Geld bei den Finanzdienstleistungsunternehmen aufkommen.

Fazit und Ausblick

Wie in dieser Übersicht dargestellt, gibt es im Cyber-Bereich Kumulrisiken aufgrund unterschiedlichster Ursachen. Es gibt bereits Ansätze, Kumulrisiken mit herkömmlichen Methoden zu modellieren, beispielsweise wird versucht, mit Modellen zu epidemischen Infektionskrankheiten mögliche Kumule bei Haftpflichtrisiken abzuschätzen.[27]

Damit ein Versicherungsunternehmen wettbewerbsfähig im Bereich der Cyber-Versicherung bleiben kann, muss es die Kumulrisiken kennen, bewerten und bepreisen können. Nur so kann die Versicherbarkeit von Cyber-Risiken und somit auch ein langfristig nachhaltiges Wachstum für diesen Markt gewährleistet werden.

---

1 Vgl. OECD (2017), S. 96.
2 Herberich (1992), S. 2.
3 Vgl. The Geneva Association (2018), S. 15.
4 Vgl. The Geneva Association (2018), S. 15.
5 Vgl. Risk Management Solutions, Inc. (2016), S. 22.
6 Vgl. Swiss Re (2017), S. 20.
7 Vgl. Z/Yen Group Limited (2015).
8 Vgl. Greenberg (2018).
9 Vgl. Greenberg (2018).
10 Vgl. Durumeric (2014), S. 475.
11 Vgl. Risk Management Solutions, Inc. (2016), S. 40.
12 Vgl. Lloyd's & Cyence (2017), S. 20.
13 Vgl. Forbes (2016).
14 Vgl. Risk Management Solutions, Inc. (2016), S. 40.
15 Vgl. Risk Management Solutions, Inc. (2016), S. 42.
16 Vgl. Lloyd's & Cyence (2017), S. 27-35.
17 Vgl. Oracle (2014).
18 Vgl. Lloyd's & Cyence (2017), S. 21.
19 Vgl. Lloyd's & Cyence (2017), S. 24.
20 Vgl. Lloyd's & Cyence (2017), S. 28.
21 Vgl. Lloyd's & Cyence (2017), S. 29-31.
22 Vgl. OECD (2017), S. 97.
23 Vgl. Risk Management Solutions, Inc. (2016), S. 46.
24 Vgl. Risk Management Solutions, Inc. (2016), S. 47.
25 Vgl. Risk Management Solutions, Inc. (2016), S. 48.
26 Vgl. Risk Management Solutions, Inc. (2016), S. 49.
27 Vgl. Swiss Re (2017), S. 27.

Literaturverzeichnis

Durumeric, Zakir et al. (2014): The matter of heartbleed. In: Proceedings of the 2014 conference on internet measurement conference. S. 475-488.

Forbes (2016): Amazon Continues To Gain Share In Cloud Infrastructure Services Market, https://www.forbes.com/sites/greatspeculations/2016/08/17/amazon-continues-to-gain-share-incloud-infrastructure-services-market/#572554ae15b8, Stand 28.03.2020

Greenberg, Andy (2018): The Untold Story of NotPetya, the Most Devastating Cyberattack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world, Stand 28.03.2020.

Herbrich, Mark (1992): Kumulkontrolle. In: Versicherung und Risikoforschung, vol 9. Gabler Verlag, Wiesbaden.

Lloyd's & Cyence (2017): Counting the cost; Cyber exposure decoded, Lloyd's, London.

OECD (2017): Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris.

Oracle (2014): Concepts Guide for Release 33 – 13: What are Hypervisors?, https://docs.oracle.com/cd/E50245_01/E50249/html/vmcon-hypervisor.html, Stand 28.03.2020

Risk Management Solutions, Inc. (2016): Managing Cyber Insurance Accumulation Risk; erstellt in Kollaboration mit und basierend auf ursprünglicher Forschung des Centre for Risk Studies, University of Cambridge.

SwissRe (2017): Cyber: Bewältigung eines komplexen Risikos, sigma 1/2017, Zürich.

The Geneva Association (2018): Advancing Accumulation Risk Management in Cyber Insurance; Prerequisites for the development of a sustainable cyber risk insurance market, The Geneva Association (Hrsg.), Zürich.

Z/Yen Group Limited (2015): Promoting UK Cyber Prosperity: Public Private Cyber Catastrophe Reinsurance, London.

Silent-Cyber – Risiken und Chancen für Versicherungsunternehmen

Von Paul Büchting

Einleitung

Durch die Entstehung neuer Megatrends wie z. B. der Konnektivität und Algorithmisierung, die den gesellschaftlichen Wandel global beeinflussen[1], müssen sich auch Versicherungsunternehmen neu aufstellen und im Bereich Cyber-Space innovativ sein. Um bei genannten Entwicklungen weiterhin relevant zu bleiben, bedeutet das für Versicherungsunternehmen, Produkte und Versicherungslösungen zu entwickeln, um die neu entstehenden Risiken im Cyber-Space zu versichern. Cyber-Versicherung gilt dabei als die Feuerversicherung des 21. Jahrhunderts.[2]

Es stellt sich die Frage, ob ein Teil dieser neuen Cyber-Risiken nicht bereits von Versicherungsunternehmen in traditionellen Verträgen unbewusst mitversichert wird. Dies kann eine Folge der stetigen Weiterentwicklung der zugrundeliegenden Informationstechnologie sein, die diese Risiken begründet.[3]

Das vorliegend beschriebene Silent-Cyber-Risiko, auch genannt Silent-Cyber, ist eine zentrale Thematik in der Versicherungswirtschaft, die alle Branchenteilnehmer betrifft: die Versicherungsnehmer und Makler, sowie die Erst- und Rückversicherer.[4] Laut dem Allianz Risk Barometer gehören Cyber-Risiken seit dem Jahr 2019 zu den größten Geschäftsrisiken weltweit.[5] Das steigende Interesse bei Versicherungsnehmern für Cyber-Versicherung sowie die steigende Intensität und Anzahl von Schäden, ausgelöst durch Silent-Cyber-Vorfälle, bieten inhärente Risiken aber auch zukunftsorientierte Chancen[6] für Versicherungsunternehmen. Im Folgenden werden zuerst die Begriffe Cyber-Risiko und Silent-Cyber-Risiko definiert und anschließend die Risiken und Chancen von Silent-Cyber für Versicherungsunternehmen erörtert.

Begriffsdefinitionen

Cyber-Risiko

Im IT-Sektor und der Versicherungswirtschaft werden Cyber-Risiken unterschiedlich definiert. Kosub (2015) führt hierzu aus, dass Cyber-Vorfälle in der Versicherungswirtschaft nicht nur von Hackern verursacht werden, sondern auch durch technische Fehler oder Handlungen der Mitarbeiter entstehen können, unabhängig davon, ob sie böswillige Absichten haben. Während Cyber-Kriminalität auf böswillige Angriffe beschränkt ist, umfasst das Cyber-Risiko sowohl digitale, nicht böswillige Vorfälle als auch kriminelle Angriffe.[7] Folgen von Cyber-Vorfällen können Betriebsunterbrechung oder andersartige finanzielle Verluste sein.[8]

Silent-Cyber

In der Versicherungswirtschaft gehört die Problematik Silent-Cyber zu den meist diskutierten Themen, dennoch existiert keine einheitliche Definition zu den Begriffen Silent-Cyber oder Silent-Cyber-Risiko. “Versicherungswirtschaft heute“ schreibt in einem Artikel zum Thema Silent-Cyber: „Unter dem Schlagwort „Silent Cyber“ befasst sich der Versicherungsmarkt mit der Fragestellung, ob und ggfs. in welchem Umfang cyber-induzierte Sach- und Personenschäden in den konventionellen Sparten – also außerhalb von Versicherungsverträgen der Sparte Cyber - möglicherweise stillschweigend versichert sind."[9]

Dabei gibt es in der Versicherungswirtschaft drei Kriterien, um die dynamische Natur der Cyber-Gefahr zu beschreiben:

- das zunehmende Ausmaß und die steigende Geschwindigkeit der digitalen Transformation,
- die Zunahme der Schwachstellen durch Hyperkonnektivität und
- die Weiterentwicklung der Bedrohungsakteure.[10]

Diese Kriterien und die sich daraus ergebende Dynamik des zugrundeliegenden Cyber-Risikos sind ursächlich für die Entstehung von Silent-Cyber-Risiko in traditionellen Versicherungsverträgen und damit verantwortlich für die in der Versicherungswirtschaft intensiv geführte Diskussion über die Problematik des Silent-Cyber-Risikos.

Risiken für Versicherungsunternehmen

Fehlende Kumulkontrolle

Vorliegende Problematik des Silent-Cyber-Risikos birgt Risiken für die Versicherer. Im Folgenden wird näher darauf eingegangen wie die stark begrenzte Menge an Schadendaten und die fehlende Kumulkontrolle bei Silent-Cyber-Risiken in traditionellen Versicherungssparten zusammenhängen. Dabei führt die begrenzte Menge an Schadendaten, und wenn es Schadendaten zu Silent-Cyber gibt, deren mangelnde Verfügbarkeit für die Versicherungswirtschaft, zu einem weiteren Problem: einem nicht risikoadäquaten Preis für ein Risiko mit unwissentlich mitversicherter Silent-Cyber-Exponierung. Diese Exponierung kann unter bestimmten Bedingungen und aufgrund der Natur dieses hochdynamischen und komplexen Risikos sogar noch wachsen.[11]

Eine zentrale Aufgabe der Versicherungsunternehmen ist es in diesem Zusammenhang ihre Exponierung gegenüber verschiedenster Schadenszenarien inklusive des Silent-Cyber-Schadenszenarios in ihren Sparten Property und Casualty genau zu kennen und eine funktionierende Kumulkontrolle aufzusetzen. Das hilft dabei die Kumulgefahr richtig einschätzen zu können. Durch Konnektivität und das weit fortgeschrittene technologische Umfeld in Industriestaaten können Einzelereignisse wie NotPetya, eine große Menge an Verträgen, sowohl Cyber-Policen als auch konven-

tionelle Policen, triggern und zu enormen Kumulschäden für Versicherer führen. Die Malware NotPetya, die durch das Ausnutzen einer Sicherheitslücke in der Standardsoftware Microsoft Windows ermöglicht wurde, hat gezeigt, wie sich ein Kumulschaden im Bereich Cyber für Versicherer auswirken kann. Die Besonderheit dieses enormen Kumulschadens lag dabei in den Schadenzahlungen, die durch eine Mischung von affirmativen Cyber-Deckungskomponenten (Stand-alone Cyber-Versicherungspolicen) und Silent-Cyber-Deckungskomponenten in konventionellen Policen ausgelöst wurden.[12]

Wird diese Kumulgefahr nicht oder nur teilweise erkannt und berücksichtigt, birgt das erhebliche Risiken für das beteiligte Versicherungsunternehmen.[13] "Unter Kumul wird [..] eine Anhäufung mehrerer Schäden aufgrund eines Ereignisses bei einem Versicherungsunternehmen verstanden."[14] Gerade Rückversicherungslösungen, die sich mit diesen neuen Risikosituationen wie Silent-Cyber und den sich daraus potenziell ergebenden Kumulen für Erstversicherer beschäftigen, werden immer gefragter.[15]

Property Schadenszenario

Weitere Risiken für Versicherungsunternehmen wie die hohe Unsicherheit bei Silent-Cyber werden ersichtlich, wenn auf mögliche Property- und Casualty-Schadenszenarien, ausgelöst durch Silent-Cyber, zurückgegriffen wird. Dabei handelt es sich um Schadenszenarien aus den traditionellen Non-Life Versicherungssparten, in denen Silent-Cyber-Risiko zusätzliche Exponierung für die Versicherungsunternehmen darstellt.[16] Da meist kein expliziter Ausschluss zu Cyber-Angriffen in Versicherungspolicen genannt ist, ist auch nicht ausdrücklich definiert in welchem Rahmen und Umfang ein solches Cyber-Ereignis unter einer konventionellen Police ohne entsprechenden Ausschluss gedeckt wäre und somit als mitversichertes Silent-Cyber-Risiko charakterisiert werden kann.[17]

Die Unsicherheit des Versicherungsmarkts bzgl. dieser Risiken hat sich auch bei der Malware-Attacke NotPetya im Jahr 2017 deutlich gezeigt. Cyber-Angriffe wie NotPetya können sich heute innerhalb weniger Tage über die gesamte Welt ausbreiten. Die Schadsoftware NotPetya, die sich von der Ukraine aus ausbreitete, hat als sehr prominentes Beispiel gezeigt wie groß die Auswirkungen von Silent-Cyber-Risiken auf die Versicherungswirtschaft sein können. In Sparten wie Property und Casualty, die als traditionelle Versicherungssparten gelten, kam es zu großen Verlusten. Im Folgenden wird ein Silent-Cyber-Schadenszenario zu Property erörtert.[18]

Angelehnt an die Funktionsweise der NotPetya-Attacke, die zu weitreichenden Störungen von Systemen führte und als sehr anschauliches Beispiel für Silent-Cyber-Exponierung und enorme Silent-Cyber-Kumulschäden in traditionellen Versicherungssparten gilt, wird in Property folgendes Schadenszenario erörtert: Ein Cyber-

Angriff führt zur Störung und anschließenden Fehlfunktion eines Kühlsystems. Die fehlende Kühlung führt zu einer Überhitzung der Hardware und nach einiger Zeit zu einem Brand.[19] Aus diesem Brand resultiert die Zerstörung der Hardware und damit ein Schaden. Da die Kriterien der versicherten Gefahr Brand bei vorliegendem Property Schadenszenario erfüllt sind, ist der resultierende Schaden im Rahmen der Feuerversicherung gedeckt, auch wenn der ursprüngliche Auslöser des Brands ein Cyber-Angriff war. Ansprüche auf Versicherungsleistung aus diesen Silent-Cyber-Risiken können, sofern sie erheblich sind, die Solvabilität und Liquidität von Versicherungsunternehmen beeinträchtigen.[20]

Chancen für Versicherungsunternehmen

Lösungsansätze und Strategien

Non-silent Cyber

Mit dem vorliegend erörterten Silent-Cyber in traditionellen Versicherungssparten gehen für die Versicherer aber nicht nur Risiken einher. Durch die Entstehung einer eigenständigen Versicherungssparte für Cyber ergeben sich auch Chancen für die Versicherungsunternehmen. Der Ursprung dieser Sparte liegt im Silent-Cyber-Risiko und dem Ziel dies schrittweise zu bewältigen. Die Versicherungsunternehmen müssen, um ihre Silent-Cyber-Exponierung einschätzen zu können, ihre Verträge und Policen diesbezüglich prüfen und reevaluieren. Dabei muss es das erklärte Ziel der Versicherungsunternehmen sein das Silent-Cyber-Risiko in jedem Fall non-silent zu machen.[21] Anschließend gibt es zwei Lösungsansätze damit umzugehen. Der erste Ansatz beinhaltet das jetzt affirmative Cyber-Risiko in den bestehenden Policen weiterhin zu decken z. B. in Form eines Cyber-Bausteins. Der zweite Lösungsansatz besteht darin das Silent-Cyber-Risiko mit einer eigenständigen Versicherungslösung, einer sog. Stand-alone Cyber-Versicherung, abzusichern.[22] Beide Lösungsansätze werden nachfolgend erläutert.

Cyber-Bausteinlösungen

Das Decken affirmativer Silent-Cyber-Risiko-Exponierung in bestehenden Verträgen oder in der Folge das Anbieten von Cyber-Bausteinlösungen, ist für die Versicherer eine Chance mit ihren Versicherungsnehmern aktiv in Kontakt zu treten. Des Weiteren komplettieren solche Bausteine den Versicherungsschutz und führen zu mehr Klarheit. Es ist ein kundenorientierter Lösungsansatz, da diese keine neue Police abschließen müssen.

Es stellt sich aber die Frage wie Silent-Cyber-Risiko non-silent gemacht werden kann. Dies geschieht durch Änderungen des Wordings, um in einem zweiten Schritt die sich veränderten Gegebenheiten mit dem Kunden zu besprechen und z. B. eine bestehende Versicherungspolice gegen Betriebsunterbrechungsschäden um einen

Cyber-Baustein zu erweitern. Diese neu hinzugekommene Deckungskomponente würde zu mehr Prämie für den Versicherer führen und den bestehenden Versicherungsschutz für Betriebsunterbrechungsrisiken komplettieren.[23]

Abhängig vom Profil des Versicherers kommt es auf die Strategie an, die das Versicherungsunternehmen bei der Silent-Cyber-Problematik verfolgt. Hier liegt der Fokus darauf die bestehende Police anzupassen, und damit das Silent-Cyber-Risiko affirmativ im bestehenden Vertrag abzusichern. Dabei sehen die Unternehmen die Cyber-Versicherungskomponenten als Teil eines Baukastensystems, durch den das Silent-Cyber-Risiko affirmativ wird und in einem zweiten Schritt die Erweiterung des bestehenden Versicherungsschutzes jederzeit durch Zukauf einer weiteren Cyber-Deckungskomponente ermöglicht. Dieser Ansatz beseitigt Unsicherheiten, fördert Kundenzufriedenheit und generiert Prämienwachstum. Er wird beispielsweise von der AXA verfolgt.[24]

Stand-alone Cyber

Als zweiter möglicher Lösungsansatz der vorliegenden Silent-Cyber-Problematik sind Stand-alone Cyber-Policen zu nennen deren Ursprung in den USA liegen. Über Großbritannien sind die Policen und die kommerzielle Versicherung von Cyber-Risiken dann nach Europa und damit auch nach Deutschland gekommen.[25] Die Idee ist es, die Silent-Cyber-Exponierung affirmativ in einem eigenständigen Vertrag abzusichern. Das Hauptargument für Versicherer Stand-alone Cyber-Policen anzubieten ist wie Stefan Golling folgend formuliert: „Konventionelle Policen sehen den Einschluss potenzieller Cyber-Risiken nicht vor."[26]

Auf diesem Ansatz der Stand-alone Cyber-Policen bauen große Erwartungen der Versicherungswirtschaft auf. Viele Versicherer sehen die Entstehung einer neuen Versicherungssparte, die als solche im Gegensatz zu Cyber-Bausteinlösungen komplett eigenständig von anderen (traditionellen) Versicherungssparten ist. Der Vorteil dieser Strategie für den Kunden ist eine größere Sicherheit bezüglich des Deckungsumfangs. Auf Seiten der Versicherungswirtschaft ist ein starkes Prämienwachstum durch das neue Produkt bzw. die neue Sparte Cyber als Chance zu sehen. Mitunter wählt die Allianz den hier dargelegten Ansatz, Silent-Cyber-Exponierung mit Hilfe von Stand-alone Cyber-Policen entgegen zu treten.[27]

Wachstumspotenzial

Obwohl Bedrohungen durch Cyber-Angriffe immer weiter zunehmen, ist man bei einer großen Anzahl von Unternehmen noch weit davon entfernt ein risikoadäquates Bewusstsein für die Thematik Cyber-Risiko zu haben.[28] Durch eine Untersuchung zum Thema Cyber-Security, für die 270 Entscheider in mittelständischen Unternehmen und Konzernen verschiedener Branchen

befragt wurden, zeigte sich, dass nur 15 % eine Versicherung gegen Cyber-Risiken abgeschlossen haben.[29] Ein Risikobewusstsein für derartige Risiken bei den Unternehmen zu schaffen, ist Aufgabe der Versicherer.

Die Zukunft von Cyber-Versicherungen wird von den Anbietern trotz der bestehenden Herausforderungen wie Silent-Cyber optimistisch gesehen, da ein starkes Prämienwachstum erwartet wird.[30]

Den neu entstandenen Cyber-Versicherungsmarkt teilen sich heute vor allem große und international aufgestellte Industrie-Versicherer, die das langfristige Wachstumspotenzial in dieser neuen Versicherungssparte früh erkannt haben (siehe Abbildung 1).[31]

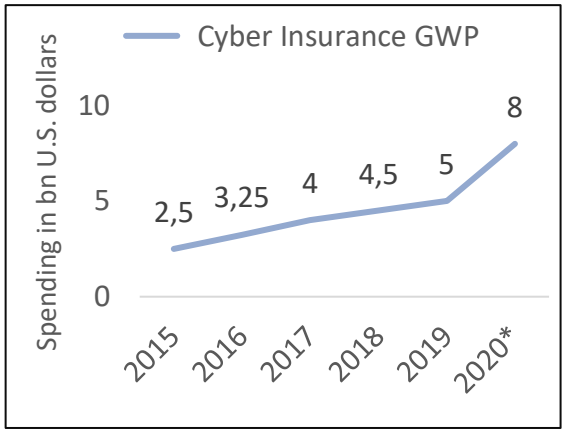

Abbildung 1: Annual Cyber Insurance Spending worldwide from 2015 to 2020[32]

Die stetig ansteigende Anzahl von Versicherern, die Cyber-Policen verkaufen, zeigt, dass Cyber-Risiko nun schon länger versicherbar ist. Die Kritik aus der Wirtschaft, die auf unzureichende Deckungssummen und sehr restriktive Einschlüsse hinweist, ist verstummt.

Die Versicherer fangen nun an, auch induziert durch Silent-Cyber, größere eigene Datenmengen zu Cyber-Risiken zu erfassen und sich so auf die zukünftigen Herausforderungen, die diese neue Versicherungssparte mit sich bringt, vorzubereiten.[33]

Fazit

Die in diesem Beitrag erörterten Risiken und Chancen sind keinesfalls eine abschließende Aufzählung, sondern vielmehr eine gezielte Auswahl und Zusammenstellung der wichtigsten Argumente. Der zentrale Punkt im Umgang mit Silent-Cyber besteht für die Versicherungsunternehmen darin, die Exponierung in den bestehenden Verträgen non-silent oder affirmativ zu machen. Wird dieses Ziel erreicht, werden aus Risiken im Zusammenhang mit der Problematik Silent-Cyber Chancen in Form von zwei Ansätzen: Die Versicherer decken das Cyber-Risiko, ehemals Silent-Cyber, in ihren bestehenden Verträgen mit Hilfe von Bausteinlösungen und besprechen dies mit ihren Kunden. Oder sie entscheiden sich für eine strikte Trennung von traditionellem und Cyber-Geschäft und versichern die Gesamtheit der IT-Risiken in eigenständigen Verträgen, in sog. Stand-alone Cyber-Policen. Beide Ansätze bieten die Möglichkeit zusätzlicher Prämieneinnahmen und viele neue Technologien, die in den letzten Jahren entwickelt wurden, werden den Cyber-Versicherungsmarkt weiter beflügeln.[34]

Trotz des noch bei vielen Unternehmen fehlenden Risikobewusstseins, ist das Thema Silent-Cyber-Risiko als eine Chance für die Versicherungsunternehmen zu sehen. Zusammen mit einem parallellaufenden Bildungsauftrag der Versicherungswirtschaft, die Kunden und Marktteilnehmer für ihre IT-Risiken und mögliche Schadenszenarien zu sensibilisieren, entsteht eine komplett neue und stark wachsende Versicherungssparte, die großes Potenzial hat.

---

[1] Vgl. zukunftsInstitut (2020).
[2] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2019).
[3] Vgl. Munich Re (2019).
[4] Vgl. Munich Re (2019).
[5] Vgl. Allianz Global Corporate & Specialty (2019).
[6] Vgl. Munich Re (2020).
[7] Vgl. Kosub (2015), S. 619 ff..
[8] Vgl. Mukhopadhyay u.a. (2013), S. 11.
[9] Versicherungswirtschaft heute (2019).
[10] Vgl. Pain/Johnathan (2017), S. 4.
[11] Vgl. Pain/Johnathan (2017), S. 2.
[12] Vgl. Munich Re (2018).
[13] Vgl. Herbrich (1992), S. 14 f.
[14] Herbrich (1992), S. 2.
[15] Vgl. Choudhry (2014), S. 10.
[16] Vgl. Munich Re (2019).
[17] Vgl. WillisTowersWatson (2019).
[18] Vgl. Munich Re (2019).
[19] Vgl. Goh u.a. (2020).
[20] Vgl. Goh (2020).
[21] Vgl. Munich Re (2019).
[22] Vgl. WillisTowersWatson (2019).
[23] Vgl. Choudhry (2014), S. 16 f.
[24] Vgl. AXA Deutschland (2020).
[25] Vgl. Choudhry (2014), S. 2.
[26] Munich Re (2019).
[27] Vgl. Allianz (2020).
[28] Vgl. Choudhry (2014), S. 15.
[29] Vgl. Choudhry (2014), S. 14.
[30] Vgl. Choudhry (2014), S. 26.
[31] Vgl. Choudhry (2014), S. 2.
[32] Gartner & Munich Re (2019).
[33] Vgl. Choudhry (2014), S. 1.
[34] Vgl. Petratos u.a. (2018), S. 818.

Literaturverzeichnis

Allianz (2020): CyberSchutz-Versicherung, URL: https://www.allianz.de/business/cyber-schutz-versicherung/, Stand: 12. März 2020.

Allianz Global Corporate & Specialty (AGCS) (2019): Allianz Risk Barometer 2019, URL: https://www.allianz.com/de/presse/news/studien/190115_allianz-risk-barometer-2019.html, Stand: 3. März 2020.

AXA Deutschland (2020): Cyber-Versicherung: Umfassend und flexibel versichert, URL: https://www.axa.de/geschaeftskunden/cyber-versicherung, Stand: 12. März 2020.

Choudhry, Umar (2014): Der Cyber-Versicherungsmarkt in Deutschland. Eine Einführung, Wiesbaden.

Gartner & Munich Re (2019): Annual cyber security and cyber insurance spending worldwide from 2015 to 2020, URL: https://www.statista.com/statistics/387868/it-cyber-securiy-budget/, Stand: 10. März 2020.

Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) (2019): Interview mit Aktuar Onnen Siems, URL: https://www.gdv.de/de/themen/news/-wir-werden-die-cyberversicherung-als-einen-standard-sehen--44082, Stand: 3. März 2020.

Goh, Joseph/Kang, Heedon / Xing Koh, Zhi / Lim, Jin Way/Wei Ng, Cheng / Sher, Ga-len / Yao, Chris (2020): Cyber Risk Surveillance: A Case Study of Singapore, IMF Working Paper WP/20/28, Singapore 2020, URL: https://scholar.google.de/scholar?as_ylo=2020&q=silent+cyber&hl=de&as_sdt=0,5, Stand: 29. Februar 2020.

Herbrich, Mark (1992): Kumulkontrolle, Wiesbaden.

Kosub, Thomas (2015): Components and challenges of integrated cyber risk management, in: Zeitschrift für die gesamte Versicherungswissenschaft, 104. Jg., Nr. 5, S. 615–634.

Mukhopadhyay, Arunabha / Chatterjee, Samir / Saha, Debashis / Mahanti, Ambuj / Sadhukhan, Samir K. (2013): Cyber-risk decision models: To insure IT or not?, in: Decision Support Systems, 56. Jg., Nr. 1, S. 11–26.

Munich Re (2018): Topics Cyber - Cyberversicherung: Von Risiken zu Chancen, URL: https://www.munichre.com/topics-online/de/digitalisation/cyber/cyber-insurance-from-risks-to-opportunities.html, Stand: 5. März 2020.

Munich Re (2019): Topics Cyber - Silent Cyber, URL: https://www.munichre.com/topics-online/de/digitalisation/cyber/silent-cyber-risks.html, Stand: 29. Februar 2020.

Munich Re (2020): Cyber-Risiken - Cyber-Bedrohungen zählen zu den größten Risiken des 21. Jahrhunderts, URL: https://www.munichre.com/de/risiken/cyber-risiken.html, Stand: 3. März 2020.

Petratos, Pythagoras / Sandberg, Anders / Zhou, Feng: Cyber Insurance, in: Carayannis, Elias G. / Campbell, David F. J. / Efthymiopoulos, Marios Panagiotis (Hrsg.) (2018): Handbook of cyber-development, cyber-democracy, and cyber-defense, Cham, Switzerland, S. 809-836.

Swiss Re (2017): Cyber: Bewältigung eines komplexen Risikos, in: sigma, 2017. Jg., Nr. 1, S. 1–43.

Versicherungswirtschaft heute (2019): Problemfall Silent Cyber: Versicherungskunden

drohen harte Ausschlüsse, URL: https://be.in-value.de/d/publikatio-nen/vwheute/2019/07/04/Problemfall-Silent-Cyber-Versicherungskunden-drohen-harte-Ausschluesse.html, Stand: 29. Februar 2020.

WillisTowersWatson (2019): Industrieversiche-rungen MARKTspot 2019. Rückblick / Ausblick, S. 10–11.

zukunftsInstitut (2020): Megatrend Konnektivi-tät, URL: https://www.zukunftsinstitut.de/dos-sier/megatrend-konnektivi-taet/?gclid=EAIaIQobChMI_KzRtaj-5wIVC4GyCh2mvQSEE-AAYASAAEgLGCPD_BwE, Stand: 3. März 2020.