DAV

DEUTSCHE
AKTUARVEREINIGUNG e.V.

Ergebnisbericht des Ausschusses Schadenversicherung

Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement in Versicherungsunternehmen

Köln, den 30. Juni 2022

Präambel

Der Ausschuss Schadenversicherung der Deutschen Aktuarvereinigung e. V. hat den vorliegenden Ergebnisbericht erstellt.[1]

Zusammenfassung

Der Ergebnisbericht thematisiert das Risikomanagement von Cyberrisiken in Versicherungsunternehmen. Er stellt zunächst die spezifischen Eigenschaften von Cyberrisiken dar, denen ein Versicherungsunternehmen durch das Zeichnen von Cyberpolicen ausgesetzt sein kann. Auf dieser Grundlage zeigt der Ergebnisbericht Maßnahmen auf, die geeignet sind, um das versicherungseigene Risikomanagement an die Spezifika von Cyberrisiken anzupassen.

Der Ergebnisbericht richtet sich spartenübergreifend an Aktuare, Risikomanager und andere Interessierte, die sich mit dem Management von Cyberrisiken im Versicherungskontext beschäftigen, und unterrichtet über den Stand der Diskussion und die durch die Arbeitsgruppe erzielten Erkenntnisse; er stellt keine berufsständisch legitimierte Position der DAV dar.[2]

Verabschiedung

Der Ergebnisbericht ist durch den Ausschuss Schadenversicherung am 30. Juni 2022 verabschiedet worden.

---

[1] Der Ausschuss dankt der Arbeitsgruppe *Daten und Methoden zur Bewertung von Cyberrisken* ausdrücklich für die geleistete Arbeit, namentlich den Mitarbeitenden der UAG Cyberrisikomanagement Dr. Clemens Frey (Leitung), Christine Fonger, Dr. Leonie Ruderer und Frank Sagerer.

[2] Die sachgemäße Anwendung des Ergebnisberichts erfordert aktuarielle Fachkenntnisse. Dieser Ergebnisbericht stellt deshalb keinen Ersatz für entsprechende professionelle aktuarielle Dienstleistungen dar. Aktuarielle Entscheidungen mit Auswirkungen auf persönliche Vorsorge und Absicherung, Kapitalanlage oder geschäftliche Aktivitäten sollten ausschließlich auf Basis der Beurteilung durch eine(n) qualifizierte(n) Aktuar DAV/Aktuarin DAV getroffen werden.

Inhaltsverzeichnis

1. Einleitung

1.1. Motivation

Cyberrisiken werden in der Bevölkerung und in der Wirtschaft zunehmend als relevante, teilweise sogar als bedrohliche Risikokategorie wahrgenommen, derzeit insbesondere als Begleiterscheinung des russischen Angriffs auf die Ukraine. Ganz objektiv nimmt daher auch die Bedeutung der Cyberversicherung zu, und zwar einerseits als risikoabsicherndes Instrument für Industrie, Gewerbe und private Versicherungsnehmer, und andererseits als (übernommene) Risiken, denen sich Versicherungsunternehmen stellen und die sie aktiv managen müssen.

Einer repräsentativen Unternehmensbefragung zu Cyberangriffen gegen Unternehmen in Deutschland (Kriminologisches Forschungsinstitut Niedersachsen, 2020) zufolge gaben zwei Fünftel der Unternehmen an, dass sie in den letzten zwölf Monaten Ziel eines Cyberangriffs waren. Stärker belastete Wirtschaftszweige waren dabei Handel, Instandhaltung/Reparatur von KFZ, freiberufliche, wissenschaftliche und technische Dienstleistungen sowie Erziehung und Unterricht.

In Deutschland gab es im Jahr 2018 nahezu 100.000 Fälle von Cyberkriminalität, und die weltweiten Schäden belaufen sich Ende 2020 laut einer Studie von McAfee mittlerweile insgesamt auf 1.000 Mrd. USD und haben sich damit seit 2018 fast verdoppelt. Das Prämienvolumen, das durch den Cyberversicherungsmarkt generiert wird, ist schwer zu schätzen. Aktuelle Schätzungen geben ein weltweites Prämienvolumen von etwas mehr als 7 Mrd. US-Dollar für das Jahr 2020 an. Bis 2025 wird von einem Wachstum auf über 20 Mrd. US-Dollar ausgegangen, bei jährlichen Steigerungsraten von über 20%.

Allein diese Zahlen zeigen, dass das angemessene Management von Cyberrisiken in ihren Portefeuilles für Versicherungsunternehmen ein Thema ist.

1.2. Ikonische Schadenfälle

Cyberrisiken und Cyberereignisse sind in vielerlei Hinsicht speziell. Einige ikonische Schadenfälle können dies beispielhaft demonstrieren.

Infrastrukturangriff mit Folgewirkung

Erhebliches Schadenpotential sowohl für affirmative Deckungen als auch für traditionelle Deckungen bieten Angriffe auf Infrastruktur. Ein Beispiel hierfür stellt der Angriff auf die Colonial Pipeline dar (im Mai 2021[3]).

Tatsächlich war die eigentliche Infrastruktur der Pipeline vom Angriff nicht betroffen, aber die Entscheidung der Firma, die Versorgung aus Angst vor

[3] Berichte der York Times, bei tagesschau und Reuters, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html, https://www.tagesschau.de/wirtschaft/unternehmen/colonial-pipeline-loesegeld-hacker-angriff-ransomware-101.html, https://www.reuters.com/technology/us-issue-first-cyber-regulations-pipelines-after-hack-washington-posst-2021-05-25/

finanziellen Verlusten einzustellen, führte zu Versorgungsengpässen und Hamsterkäufen in der Bevölkerung.

Generell bergen Angriffe auf Infrastruktur großes Kumulpotential bis hin zu systemischen Katastrophen. Aus diesem Grund findet man aktuell häufig Ausschlüsse für entsprechende Schadenereignisse in Cyberdeckungen.

Angriff auf Lieferketten

Bei einer Supply-Chain-Attacke wird die Schadsoftware in eine vermeintlich vertrauenswürdige Software eingeschleust und mit dieser dann ggf. weltweit verbreitet.

Hierfür gibt es mittlerweile viele prominente Beispiele. Journalistisch aufgearbeitet ist zum Beispiel der Schaden bei Maersk durch NotPetya (im Juni 2017[4]). Jüngere Beispiele sind die Fälle von SolarWinds, bei der sogar US-Ministerien betroffen waren (im Dezember 2020[5]) oder von Kaseya (im Juli 2021[6]). Diese Beispiele zeigen die potenziell weltweite Kumulexponierung, die steigende Bedeutung von Ransomware-Attacken, aber auch die Schwierigkeit, Schadenereignisse kausal wie zeitlich einzugrenzen.

Silent Cyber

Ein anderer bekannter Cyberangriff wurde über vergleichsweise simples Spearfishing durchgeführt und damit die Steuerung eines deutschen Hochofens übernommen. Der Hochofen konnte nicht reguliert heruntergefahren werden und die gesamte Anlage erlitt gravierende Schäden. Dies ist ein mittlerweile doch recht bekanntes Beispiel für einen Sachschaden in Folge eines Cyberangriffs (im Jahr 2014[7]). Hier wird deutlich, wie leicht Cyberereignisse gravierende materielle und finanzielle Schäden nach sich ziehen können und damit in Form von Silent Cyber zu signifikanten Risiken führen.

Cyber Event nicht als Auslöser, sondern als Folgeschaden

Ein Szenario, das nur wenige Ausschlüsse abdecken, ist, dass ein traditioneller Auslöser, wie zum Beispiel Feuer, einen Cyberschaden auslöst. So geschehen

[4] Bericht auf Wired und heise, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, https://www.heise.de/hintergrund/3-Jahre-NotPetya-Der-Erpressungstrojaner-der-keiner-war-4797250.html

[5] Bericht in Spektrum, https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187

[6] Bericht bei reuters, https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/

[7] Bericht auf heise, https://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html

Anfang 2021 in einem Rechenzentrum[8]. Da viele der Kunden Backups in anderen Rechenzentren nicht mitgekauft hatten, sind tatsächlich große Datenmengen unwiderruflich verloren gegangen. Somit hat ein Feuer den Cyberschaden Cloud Outage ausgelöst und zu Betriebsunterbrechungen geführt.

Ungewollte Übernahme von Angreifern

Eine ungewöhnliche Haftungsfrage entstand schon vor längerer Zeit bei der Übernahme der Hotelkette Starwood durch Marriott. Angreifer hatten sich in die Systeme der ersteren eingearbeitet und waren dort unbemerkt präsent (vermutlich seit 2014). Nach der Übernahme im Jahr 2015 nutzten die Angreifer diesen Zugang, um die wesentlich größere Datenmenge von Marriott abzugreifen. Die einzelnen verursachten Schadenhöhen waren nicht außergewöhnlich hoch, aber die schiere Anzahl an kleinen Schäden durch Verlust von privaten Daten im Kumul führten im Jahr 2018 zu einem massiven Schaden[9]. Wie weiter oben wird auch hier deutlich, wie schwierig es ist, einzelne Schadenereignisse voneinander abzugrenzen und entsprechende Haftungsfragen zu klären.

1.3. Zielsetzung des Ergebnisberichts

Ausgehend von der weiter oben beschriebenen zunehmenden Relevanz von Cyberrisiken für das Versicherungsgeschäft soll dieser Ergebnisbericht spezifische Eigenschaften von Cyberrisiken zusammenfassen. Auf dieser Grundlage soll der Bericht Denkanstöße für eine mögliche Weiterentwicklung des Risikomanagements liefern, das den spezifischen Eigenschaften von Cyberrisiken gerecht wird.

Das heißt einerseits, dass die operationellen Risiken, denen ein Versicherungsunternehmen im Rahmen seines Geschäftsbetriebs wie jedes andere Unternehmen ausgesetzt ist, gerade nicht im Mittelpunkt der Diskussion stehen sollen. Andererseits sei darauf hingewiesen, dass die spezifische Risikoexponierung eines Versicherungsunternehmens und die Gewichtung der einzelnen Herausforderungen ganz wesentlich von den Produkten, Deckungskonzepten sowie Rückversicherungsdeckungen abhängt, die ein Versicherungsunternehmen an den Markt bringt bzw. einkauft. Daher sind mögliche Maßnahmen des Risikomanagements immer individuell auf die spezifische Situation und die beabsichtigte Geschäftsentwicklung des Cybergeschäfts des jeweiligen Versicherungsunternehmens abzustimmen. Aus diesem Grund kann dieser Ergebnisbericht auch keinen Anspruch auf Vollständigkeit erheben, sondern soll vielmehr Denkanstöße für die individuelle Weiterentwicklung des Risikomanagements liefern.

[8] Berichte der FAZ und des Spiegel, https://www.faz.net/aktuell/feuilleton/medien/groesstes-rechenzentrum-europas-brennt-komplett-nieder-17241629-p2.html, https://www.spiegel.de/netzwelt/web/ovh-grossbrand-in-datenzentrum-in-strassburg-sorgt-fuer-stoerungen-a-dff1fc32-8bd0-4305-a026-b6221e079455

[9] Bericht bei BBC, https://www.bbc.com/news/technology-54748843

1.4. Überblick

In den Abschnitten 2 bis 6 werden die spezifischen Eigenschaften von Cyberrisiken erörtert. Dabei gehen wir insbesondere auf die Dynamik von Cyberexponierungen und -schadenbildern ein, auf mögliche Akkumulationswirkungen bei Eintritt eines Cyberereignisses, auf die Datenverfügbarkeit und die Modellierung von Cyberrisiken sowie die potenzielle (Nicht-)Verfügbarkeit von Rückversicherung oder anderen Werkzeugen der Risikomitigation. Jeder Abschnitt leitet im letzten Teil zu den möglicherweise angezeigten Anpassungsbedarfen im Risikomanagement über. Letztere werden in Abschnitt 7 des Ergebnisberichts nochmals kurz zusammengefasst und mit einem Ausblick versehen.

In Bezug auf die hier verwendete Begrifflichkeit sei auf den vorangegangenen Ergebnisbericht der AG *Daten und Methoden zur Bewertung von Cyberrisken* verwiesen, der am 30.07.2020 unter dem Titel *Daten und Methoden zur Bewertung von Cyberrisiken* veröffentlich wurde und Begriffe wie Cyberereignis, Cyberrisiko etc. definiert.

2. Dynamik in Produkten und Exposures

Wie in der Motivation herausgestellt ist das Feld der Cyberversicherung stark „in Bewegung" – sowohl auf Seiten der angebotenen Produkte wie auch auf Seiten der gedeckten Risiken.

2.1. Produkteigenschaften

Im Bereich der Cyberversicherung ändern sich Produkte und angebotene Kapazitäten nach wie vor dynamisch, ebenso wie Konditionen und Preise. Dabei sind diese Effekte wiederum je nach Geschäftsfeld (Industrie vs. Gewerbe vs. Privatkundengeschäft) und Markt (weiter entwickelter US-Markt vs. Rest der Welt) unterschiedlich stark ausgeprägt.

2.2. Risikoeinschätzung und Exposure-Messung

Auf der Seite der gedeckten Risiken sind schnell ändernde Angriffsvektoren zu beobachten, aber auch die Abwehrmechanismen werden mit entsprechender Geschwindigkeit nachgezogen. Die technologische Entwicklung führt weiterhin zu veränderten Schadenbildern in nahezu jedem Jahr. Zuletzt war beispielsweise eine deutliche Verschiebung hin zu Ransomware-Angriffen zu beobachten. Angreifer nutzen immer neue Schwachstellen auf unterschiedlichste Art aus und setzen hierzu immer neue Schadsoftware ein. Gleichzeitig werden gezielte Angriffe auf lohnenswerte Ziele häufiger und elaborierter. In sehr ähnlichem Maße verändern sich entsprechend die Abwehrmöglichkeiten und Verteidigungsmechanismen. Allerdings erfordert dies umgehende Anpassungen in der IT der Versicherungsnehmer, regelmäßige Systemupdates und ausgefeilte Backup-Strategien. Das kann nicht jeder Versicherungskunde in der nötigen Frequenz leisten.

Insofern besteht in der Sparte weiterhin große Unsicherheit auf Ebene der Risikoeinschätzung und der Exposuremessung. Eine zuverlässige und belastbare Risikoeinschätzung zum Zeitpunkt der Zeichnung ist schwierig und potenziell schnell überholt aufgrund der beschriebenen Dynamik der Rahmenbedingungen. Expertenwissen aus dem IT-Umfeld kann hier zumindest teilweise Abhilfe schaffen, aufgrund der damit verfügbaren Einschätzung, z.B. in Hinblick auf Art und Geschwindigkeit vorhersehbarer technologischer Entwicklungen.

2.3. Klassifizierbarkeit und Rechtsprechung

Die Auslöser von Cyberereignissen sind oft schwer zu erkennen, einerseits aufgrund der Komplexität der Technologie, andererseits aber auch, weil insbesondere im Kontext krimineller Aktivitäten Ursachen und Urheber häufig verschleiert werden. Diese an sich bereits schwierige Attribution von Cyberschäden bekommt besonderes Gewicht in der Frage der Abgrenzung von Cyberereignissen zu kriegerischen oder terroristischen Aktivitäten (siehe die aktuelle Diskussion im Kontext des russischen Angriffs auf die Ukraine). Staaten können als Akteure auftreten, eine Abgrenzung zwischen „von staatlicher Stelle ausgeführt", „staatlich beauftragt", „vom Staat toleriert" und „ohne staatliche Intervention" ist – zumindest aus Sicht von Versicherungsunternehmen – praktisch unmöglich.

Zudem ist es ein prinzipielles Problem, wie „kriegerische Cyberangriffe" charakterisiert und damit identifiziert werden können. In Policen fehlt daher häufig eine klare Definition von (Cyber-)Kriegsgeschehen, die Frage der Deckung bzw. des Ausschlusses ist damit rechtlich (noch) nicht geklärt. Ähnlich stellt sich die Situation in Bezug auf Terrordeckungen dar. Eine eindeutige Definition eines „terroristischen Aktes" ist ohnehin schwierig, zudem aber oft nicht in cyber-spezifischer Form in vorhandenen Ausschlüssen enthalten. Rechtssicherheit in Bezug auf die Charakterisierung von „terroristischen Cyberangriffen" ist ebenfalls (noch) nicht gegeben. Ebenso fehlt in Policen verschiedentlich eine klare Abgrenzung zur Herstellerhaftung von Soft-/Hardware.

2.4. Bedeutung für das Risikomanagement

Was bedeutet diese Dynamik in Produkten und Exposures für das Management von Cyberrisiken?

- Um das Underwriting-Risiko auch bei Veränderung der Risikosituation steuern zu können, ist ein aktives Management von Deckungen und Auschlüssen nötig, das sich an aktuellen Schadenfällen ebenso wie Industrie-Benchmarks orientiert. Branchenübergreifende Standards sind erwartungsgemäß häufiger einer Anpassung zu unterziehen als bei anderen Produkten.
- Dies bedingt ein sehr detailliertes und aktuelles Bild über die in einem Cyber-Versicherungsportfolio gedeckten Risiken; inklusive der vorhandenen Silent-Cyberdeckungen.
- Um Anpassungen schnell portfolioweit umsetzen zu können, sind kürzere Laufzeiten von Cyberdeckungen denkbar, ebenso wie unterjährige Anpassungsmöglichkeiten in Preisen und Deckungsumfängen. Automatische Vertragsverlängerungen zu gleichen Konditionen sollten aus Risikomanagementsicht gründlich hinterfragt werden.
- Gleichzeitig ist eine intensive und ständige Beobachtung der Risikosituation im Sinne der „Schere" zwischen Bedrohungssituation und zur Verfügung stehenden und eingesetzten Abwehrmechanismen nötig, unter unmittelbarer Integration von IT-/Cyber-Expertenwissen in das Risikomanagement, um kurzfristige Warnmöglichkeiten und eine Neubewertung der eingegangenen Risiken zu ermöglichen.
- Ähnliches gilt in Bezug auf die Beobachtung der sich ggf. ändernden Rechtsprechung, die Einschätzung der Bedeutung für das eigene Portfolio und die Gestaltung entsprechender reaktiver Maßnahmen in der Produktgestaltung, z.B. Hinzunahme oder Anpassung von Ausschlüssen.

3. Akkumulationswirkungen

3.1. Kumulgefährdung

Eine Kumulgefährdung entsteht dadurch, dass eine große Zahl (individuell gesehen kleiner) Einzelrisiken durch ein einziges Cyberevent getroffen wird. Dadurch kann dieses einzige Ereignis einen sehr großen Versicherungsschaden hervorrufen – ähnlich wie andere bekannte Kumulgefahren (z.B. Stürme, Erdbeben, Epidemien, terroristische Bedrohungen).

Die fortgeschrittene Technologie in Industriestaaten, zunehmende elektronische Vernetzung der Gesellschaft und schnell fortschreitende Digitalisierung verstärken die Anfälligkeit gegenüber kumlierten Cyberrisiken. Das mögliche Schadenpotenzial auch kleiner Schwachstellen nimmt durch Hyperkonnektivität deutlich zu (u.a. vernetzte Businesssysteme, Digitalisierung von Wertschöpfungsketten, industrieübergreifende Vernetzung in Clouds, massenhafter Einsatz von IoT-Geräten in Privathaushalten). Außerdem stehen Privatpersonen, Gewerbetreibende und Industrieunternehmen gleichermaßen im Fokus vorsätzlich handelnder Krimineller.

Ein Cyberereignis hat das Potenzial, viele Versicherte zur selben Zeit zu treffen. Viele Unternehmen benutzen IT mit einer Monokultur an Betriebssystemen, Software und Sicherheitsprogrammen. Im Bereich des Cloudcomputings ist der Markt auf wenige Cloud Service-Provider fokussiert. Die Nutzung gemeinsamer Hard- und Softwareprodukte verstärkt die Anfälligkeit. Nicht zuletzt bestehen auch innerhalb der Unternehmen Abhängigkeiten, so dass alle IT-Systeme bzw. die Software-Infrastruktur betroffen sein könnte.

Cyberrisiken weisen dabei ein weltweites Kumulpotential auf. Durch Ausfall von zentralen IT-Diensten oder kritischer Infrastruktur, aber auch durch Schadsoftware können erhebliche Schäden entstehen. Diese Schäden können – anders als beispielsweise Naturgefahren – über geographische Grenzen und über unterschiedliche Industriesektoren hinweg bei Unternehmen und Privatpersonen Schäden verursachen. Dabei können versicherte Schäden eine Mischung von affirmativen und Silent Cyber-Deckungskomponenten in konventionellen Policen triggern und damit verschiedene Versicherungszweige (von der Feuerversicherung über Haftpflicht- oder Assistanceversicherung bis hin zu dezidierten Cyberdeckungen) und verschiedene Schadenarten betreffen.

Dass große Schäden für Versicherer möglich sind, zeigen die bereits bekannten Cyber-Ereignisse wie WannaCry und NotPetya mit weltweiten Schäden von jeweils über 10 Mrd. USD.

3.2. Unternehmensumfassende Akkumulation

Neben der Passivseite kann auch die Aktivseite eines Versicherungsunternehmens der Bilanz durch ein Cyberereignis getroffen werden, etwa wenn durch das Ereignis Unternehmen oder Staaten, in die investiert wurde, Schäden erleiden (Cross Balance Sheet Accumulation). In der Folge entstehen Aktienwertverluste oder

Ausfälle von Anleihen. Gerade nicht zielgerichtete Cyberangriffe wie etwa NotPetya können hierbei eine große Anzahl an Unternehmen gleichzeitig treffen, d.h. Anlage- und Versicherungsportfolien gleichermaßen.

Auch die IT, Prozesse und Daten des Versicherungsunternehmens selbst sind gegenüber Cyberereignissen exponiert. In der Vergangenheit gab es bereits eine beträchtliche Anzahl von Events, in denen Versicherer direkt betroffen waren. Vorfälle reichen von nicht mehr verfügbaren Betriebs- oder Vertriebssystemen über Datenverluste bis hin zu Datenmanipulationen.

Ein Fall, der das besondere Akkumulationspotential über operationelle und versicherungstechnische Risiken hinweg zeigt, ist ein gezielter Cyberangriff auf Versicherungsdaten. Solche Angriffe – mit dem Ziel, Kundeninformationen und Vertragskonditionen von Cyberverträgen zu erbeuten – sind real (zum Beispiel der Hackerangriff[10] auf die Haftpflichtkasse Darmstadt aus dem Jahr 2021). Mit Hilfe der erbeuteten Daten können Hacker Versicherungskunden gezielt angreifen und Lösegeldforderungen in der Höhe der Versicherungsdeckung stellen.

3.3. Bedeutung für das Risikomanagement

Gerade das Potenzial der Schadenhäufung kann besondere Maßnahmen und Anpassungen im Risikomanagement erforderlich machen. Maßnahmen zum Kumulmanagement sollten an diese allgemeinen Rahmenbedingungen angepasst werden:

- Für das Kumulmanagement ist wichtig zu wissen, welche Verträge gegenüber welchen Schadenszenarien exponiert sind. Dies erfordert detaillierte und flexible Analysemöglichkeiten für den Versicherungsbestand und die zugrunde liegende Cyberexponierung, die idealerweise mit häufigen Anpassungen der Schadenszenarien umgehen können.
- Dabei sind Szenarien von besonderem Interesse, die potenziell die gesamte Bilanz betreffen, sowie die Festlegung einer entsprechenden übergreifenden Risikotoleranz.
- Kumule erhöhen den Risikokapitalbedarf. Daher ist zu überlegen, inwieweit diese bereits bei der Tarifgestaltung und im Underwriting der betroffenen Sparten eingepreist werden.
- Assistance-Leistungen als Teil der Versicherungsleistung senken den Schadenaufwand. Ihre schadenmindernde Wirkung kann im Kumulfall allerdings verloren gehen. Dieser Sekundäreffekt (Post Event Loss Amplification) sollte in der Modellierung berücksichtigt werden, bzw. die Skalierbarkeit der Gegenmaßnahmen und der schadenbegrenzenden Services insbesondere für den Fall von Massen-/Großschadenlagen sichergestellt werden.

[10] Bericht des Handelsblattes vom 16.07.2021, https://www.handelsblatt.com/finanzen/banken-versicherungen/versicherer/cyberangriff-die-haftpflichtkasse-meldet-datenklau-durch-hacker/27426796.html

- Versicherer sollten ihren eigenen operativen Betrieb sowie Kundendaten besonders schützen und ggf. selbst mit geeigneten Cyberversicherungen absichern. Dabei ist zu berücksichtigen, dass Versichertendaten ein ganz besonders lohnendes Ziel für Cyberangriffe (oder auch sog. Social Engineering) sein können.

4. Verfügbarkeit von Informationen

4.1. Produktinformationen

Vor der Adressierung von Cyberrisiken im Risikomanagement steht die Herausforderung zu analysieren, welche Art von Cyberrisiken ein Portfolio exponieren. Diese reichen von unspezifischen Exponierungen in traditionellen Sparten (sog. Stille Cyberrisiken, Silent Cyber), bis zu affirmativen, auf die Übernahme von Cyberrisiken spezialisierten Deckungen.

Derzeit wird eine breite Vielfalt an unterschiedlich ausgestalteten affirmativen Deckungen angeboten (siehe für einen Überblick hierzu den vorangegangenen Ergebnisbericht[11] der AG). Diese Vielfalt besteht in allen Segmenten, d.h. vom Privatgeschäft bis zum Industriegeschäft. Allerdings lässt sich ein Trend hin zu engeren Deckungskonzepten beobachten, d.h. der Spezifizierungsgrad und damit die Ausschlüsse nehmen zu, bspw. in Hinblick auf den Ausfall von Infrastruktur oder auf Cloud Outage. Eine weitreichende Haftungsfrage mit großem Einfluss auf das Risikomanagement ist der mögliche Aus- bzw. Einschluss von Sachschäden, die im Zuge eines Cyberereignis entstehen.

Letztlich ist auch der Bereich der Deckung von Cyberschäden in klassischen Policen zu beachten. Hier kann das Risikomanagement via Ausschlussklausel vereinfacht werden. Allerdings bleibt auch hier eine gewisse Unsicherheit, denn die auszuschließenden Szenarien ändern sich, und somit sind ggf. nötige Anpassungen fortlaufend zu beobachten.

4.2. Historische Schadendaten

Historische Exposure- und Schadendaten, die für die Bewertung und das Management von Cyberrisiken benötigt werden, sind meist nicht im eigentlich benötigten Umfang bzw. in der notwendigen Qualität vorhanden.

Die Cyberrisikomessung benötigt Daten, die die jeweilige Cyberexponierung beschreiben. In Bestandssystemen werden entsprechende Merkmale oft nicht erfasst, insbesondere in den klassischen Produkten mit potenzieller Silent Cyber-Exponierung. Auch auf Marktebene haben sich noch keine geeigneten Datenbanken entwickelt, die ausreichend Informationen für eine umfassende „klassische" Risikoeinschätzung zur Verfügung stellen. Im Ergebnispapier der Arbeitsgruppe von 2020[11] wurden einige Marktdatenbanken vorgestellt.

Externe Modellanbieter arbeiten meist mit Scoring-Datenbanken, welche eine Anreicherung der eigenen Bestandsdaten mit risikorelevanten Informationen (Data Enrichment) ermöglichen. Auch eigene Onlinerecherchen mit selbstlernenden Algorithmen werden verwendet.

[11] Siehe https://aktuar.de/unsere-themen/fachgrundsaetze-oeffentlich/DAV_AGCyber_Ergebnisbericht_.pdf

4.3. Auslöser der Deckung

Eine besondere Schwierigkeit im Zusammenhang mit Cyberdeckungen besteht in der Feststellung des Auslösers Cyber. Auch entsteht häufig die Frage nach dem Zeitpunkt des Schadeneintritts: Angreifer sind mitunter lange vor einer sichtbaren Schadwirkung im System aktiv, der genaue Zeitpunkt des Schadeneintritts ist somit potenziell nur schwierig festzustellen. Die vom GDV vorgeschlagenen Musterbedingungen[12] sehen in diesem Kontext das Manifestationsprinzip vor.

Für den Versicherungsnehmer entsteht zudem oft eine besondere Abwägungssituation nach Eintritt eines Cyberereignisses; nämlich zwischen der Inanspruchnahme einer vorhandenen Deckung (und damit einem potenziellen Imageschaden) und einer Selbsttragung des Schadens zu entscheiden. Dies erhöht noch einmal die in Abschnitt 4.2. beschriebene Datenunsicherheit auf Seiten der Versicherer. Wird dem Versicherer ein Cyberschaden gemeldet, so schließt sich die Analyse der zugehörigen Versicherungsdeckung an. Neben der Frage der Laufzeit der Police in Zusammenhang mit dem eventuell unklaren Zeitpunkt des Schadeneintritts können die vielfältigen Haftungen und oft unklaren Schadenauslöser zu Unsicherheiten in der Deckungsfeststellung und damit in der Schadenregulierung inkl. juristischer Klärungen führen.

Schließlich ist eine weitere besondere Herausforderung die Attribution von eingetretenen Schäden. Es stellt sich die Frage, welche Schäden den gleichen Auslöser haben – in vielen Fällen auch bei Einsatz forensischer Expertise kaum zu klären.

4.4. Bedeutung für das Risikomanagement

Aufgrund der Neuartigkeit der Cybersparte sind versicherungsinterne Daten meist (noch) nicht aussagekräftig. Die dynamische technische Entwicklung und sich verändernde Versicherungsbedingungen führen oft zu schwer interpretierbaren, ggf. unzuverlässigen Datenbeständen; dies sollte im Risikomanagement entsprechend Berücksichtigung finden:

- Eine Weiterentwicklung der Aktivitäten rund um Datensammlung und -bewertung ist wichtig, sowohl in Richtung besserer Strukturierung als auch höherer Datengranularität. Dies ist sowohl auf Exposure-Seite als auch auf Schadenseite sehr wichtig. Die Daten sollten in Datenplattformen, die eine flexible, ggf. automatische Analyse und Modellierung erlauben, zusammengeführt werden. Dies erfordert eine entsprechende Erweiterung der Datensammlung in Vertrieb, Underwriting und Schadenregulierung, damit granulare Daten unternehmensintern überhaupt erst verfügbar werden.
- Schulung von Mitarbeitenden: Data Citizenship ist nötig, um eine kompetenzübergreifende Sicht auf die Exposure- und Schadendaten zu entwickeln. Außerdem erscheint ein kontinuierlicher Wissenstransfer

[12] Stand April 2017, siehe https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0cc207/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung-avb-cyber--data.pdf

notwendig, um zum Beispiel aktuelle Methoden zur Messung von Cyberrisiken zu vermitteln und Kenntnisse über die Wirkungsweise neuer Angriffsarten fortlaufend zu teilen.

- Externe Daten: Datenpools entstehen allmählich, um eine objektivierbare Sicht auf breiterer Basis zu erzeugen. Externe Datenquellen sind wohl verfügbar, aber ihre Aussagekraft ist schwer einzuschätzen und oft liegen auf den ersten Blick gewichtige Abweichungen zum eigenen Buch vor. Beispielsweise sind viele Datenquellen nach wie vor mit Vorfällen aus dem nordamerikanischen Raum gefüllt, unter anderem da dort ein entsprechendes Meldewesen besteht. Aber auch der Abgleich der Daten mit den eigenen Risiken ist oft erschwert, da viele Datenbanken versicherungstechnisch wichtige Merkmale nicht enthalten. Deshalb sollte das Risikomanagement hier nur Daten verwenden, von denen es ein gutes Verständnis hat. Für deutsche Versicherer baut der GDV seit drei Jahren eine Cyber-Risikostatistik auf, die eine Kalkulationsgrundlage insbesondere für die Cyberversicherung von kleinen und mittelgroßen Unternehmen schaffen soll.

5. Modellierung von Cyberrisiken

5.1. Einsatz von Modellen

Aktuell stellt die eigene Modellierung von Cyberrisiken Versicherungsunternehmen vor große Herausforderungen. Nur wenige Unternehmen haben es bisher geschafft, umfassende Modelle aufzubauen. Dies liegt vor allem an drei Herausforderungen.

Es existieren noch keine allgemein akzeptierten (state-of-the-art) Mess- oder Modellierungsmethoden für Cyberrisiken, so dass eine eigene Modellbildung inhaltlich wie aufwandsseitig herausfordernd sein kann.

Die Entwicklung eigener Modellansätze ist aufwändig und komplex, u.a. aufgrund eingeschränkter oder dynamischer Datenlage, schwieriger Identifikation von Schäden, fehlender Erfahrung, hoher Dynamik des Risikos. So muss typischerweise eine Vielzahl von unterschiedlichen Risiken modelliert werden: Schäden mit Basisschadencharakter (Privatgeschäft, KMU Erpressung), Schäden mit Großschadencharakter (Angriff auf eine Industrieanlage) und Katastrophenrisiken (Malware, Angriff auf Infrastruktur, Softwarebug), dazu operationelle Risiken. Weiter sind verschiedene Schadenarten zu berücksichtigen (Eigenschäden, Drittschäden, Kosten für Assistance etc.).

Externe Modelle sind von Interesse, da aus eigenen historischen Daten Markttrends und die potenziellen Auswirkungen von Extremereignissen nur selten verlässlich eingeschätzt werden können. Externe Anbieter bieten potenziell eine breitere und reifere Datenbasis, wobei auf den jeweiligen Einsatzzweck zu achten ist: von der Bewertung im Underwritingprozess (z.B. als kennzahlbasierte Einzelrisikobewertung in Form von Unternehmensscorings), in der Risiko-/ Portfolioanalyse bis hin zur Identifizierung, Bewertung und Steuerung von Kumulrisiken.

Unabhängig davon, welcher Weg jeweils gewählt wird, erscheint es hochgradig wichtig, dass Versicherer modellseitige Trends und Entwicklungen aktiv verfolgen. Nur so ist es möglich, das für ein zielführendes Cyberrisiko-Management notwendige Know-How aufzubauen und zu pflegen und in die gesamte Risikosteuerung einzubringen. Dies ist auch nötig, um auf Augenhöhe mit externen Stakeholdern, mit Modellanbietern und Kunden über Cyberrisiken sprechen zu können.

5.2. Bedeutung für das Risikomanagement

Sowohl für externe als auch für interne Modelle gilt:

- Ein versicherungseigenes Verständnis der in Modellen abgebildeten Cyberrisiken ist zwingend notwendig. Externe Modelle basieren auf vielfältigen Ansätzen und bilden unterschiedliche Szenarien ab. Die Modellierung von Kumulrisiken ist mit Hilfe anpassbarer Szenarien zwar möglich, doch ist eine Verwendung im Risikomanagement nur dann sinnvoll, wenn Transparenz und ein grundsätzliches Verständnis in Bezug auf die im

externen Modell abgebildeten Cyberereignisse besteht. Damit können die Modellergebnisse eingeschätzt werden und Aussagen bzgl. der Vollständigkeit der Modelle und der Grenzen ihrer Anwendbarkeit getroffen werden.

- Daher sollte eine regelmäßige Validierung der Modelle eingeplant werden, um sie verstehen und interpretieren zu können.
- Um dem Modellrisiko begegnen zu können, ist eine detaillierte Kenntnis der Schaden- und Exposuredaten und der verwendeten Modellierungsmethoden notwendig, mit dem Ziel, die daten- und methodenseitigen Treiber der Risikobewertung verlässlich einschätzen zu können.
- Die Plausibilisierung der Ergebnisse sollte im Fokus stehen, um die Bewertung der Gesamtrisikoposition vornehmen zu können und um für weitere Schritte im Risikomanagementprozess zur Steuerung und Kontrolle der Cyberrisiken verwendbar zu sein. Dabei sollten zugrunde liegende Annahmen regelmäßig überprüft und wenn nötig angepasst werden. Die Kenntnis und der Vergleich mit Resultaten aus anderen (externen) Challenger-Modellen ist in diesem Zusammenhang sehr hilfreich.

6. Rückversicherung

6.1. Verfügbarkeit von passenden Deckungen

Rückversicherungsdeckungen für Cyberereignisse können in zwei Kategorien eingeteilt werden. Auf der einen Seite stehen Deckungen als Teil von „klassischen Rückversicherungsverträgen". Diese schließen physische Schäden wie Personen- und Sachschäden als Folge von Cyberereignissen ein. Aus aktueller Sicht ist am Markt ausreichend Deckung für solche Policen gegeben, weil der Cyberschutz nicht im Mittelpunkt steht und ein physischer Schaden aus einer versicherten Gefahr (z.B. Feuer) Kern der Deckung ist. Allerdings gibt es auch hier Bestrebungen, – zum Beispiel am Londoner Markt (konkret etwa Lloyd´s of London) – Ausschlüsse in Rückversicherungsdeckungen einzuführen.

Die zweite Kategorie stellen affirmative Cyberdeckungen, beziehungsweise Deckungen von reinen finanziellen Schäden dar. Gerade aufgrund der oben genannten Neuartigkeit und Kumulneigung dieser Deckungen und der erheblichen Unsicherheiten ist es aktuell schwierig, geeignete Deckungen in ausreichendem Umfang einzukaufen. Außerdem ist damit zu rechnen, dass ein Ereignis mit großer Reichweite bzw. großem Marktschaden schnell zu einer deutlichen weiteren Verknappung, Verteuerung oder dem kompletten Kollaps des RV-Marktes führen kann. Zusätzlich ist es möglich, dass hohe Schäden im eigenen Portfolio das Vertrauen der Rückversicherer erschüttern und dazu führen, dass die Erneuerung der Rückdeckung extrem teuer oder unmöglich wird.

Erstversicherer folgen beim Markteinstieg oft dem klassischen Vorgehen, nach dem zunächst ein überschaubares, stark durch Rückversicherung abgesichertes Cyberportfolio aufgebaut wird – etwa durch Quotenrückversicherung mit nennenswerten prozentualen Übernahmen durch die Rückversicherer. Für den Versicherer ermöglicht dies einen kontrollierten Einstieg in eine unbekannte Sparte und federt die Volatilität eines kleinen Buches ab, allerdings entsteht eine starke Abhängigkeit vom Rückversicherer mit den oben beschriebenen Risiken.

Der Markt für die Zession von Basisschäden, etwa über Quotenrückversicherung (mit Haftungsbeschränkung), scheint auch nach größeren Ereignissen eine gewisse Stabilität zu haben. Nichtproportionale Deckungen, d.h. Excess-of-Loss-Deckungen oder Stop-Loss-Konstruktionen sind in diesem Zusammenhang eher kritisch zu sehen. Bei nichtproportionalen Deckungen besteht zudem das Risiko, dass die unterliegende Ereignisdefinition zu Streitigkeiten und langen Gerichtsverfahren führt, denn aktuell hat sich diesbezüglich noch kein Marktstandard etabliert. Versuche, eine Ereignisdefinition in Anlehnung an bekannte Klauseln für Naturkatastrophenschäden zu verfassen, scheitern oft an der mangelhaften Möglichkeit der Attribuierung, am hohen Aufwand für die Forensik, um solche Zusammenhänge zu erkennen, oder auch an der schwierigen zeitlichen Erfassung des Schadeneintritts (siehe hierzu auch 4.3).

Malicious Attack ist als Kernbestandteil von Cyberpolicen gedeckt, mit deutlichen Parallelen zu Terror und mit verschwimmenden Grenzen, z.B. im Fall von staatlich

unterstützten Attacken. Auch dies führt zu einer potenziell starken Kumulexponierung, die nach Möglichkeit rückversichert werden sollte.

6.2. Bedeutung für das Risikomanagement

Aus Risikomanagementsicht sollte hier besonderes Augenmerk auf die Konsistenz von Erst- und Rückversicherung gelegt werden. Für affirmatives Geschäft sollte insbesondere die Möglichkeit geschaffen werden, Anpassungen vorzunehmen, indem etwa Originalverträge nicht deutlich länger als die Rückversicherungsverträge im Portfolio laufen. Auch eine schnelle Reaktionsmöglichkeit mit schnell änderbaren oder kündbaren Verträgen ist wichtig. Solche Anpassungen können sowohl Deckungsstrukturen als auch Deckungsumfang, bzw. Ausschlussregelungen, betreffen. Die Gewährung von Anschlussdeckungen oder automatische Erneuerungen sind vor diesem Hintergrund kritisch zu sehen. Mit Hinblick auf Silent-Cyberdeckungen, sollte im Rückversicherungsvertrag darauf geachtet werden, dass Ausschlussklauseln zum bestehenden Originalrisiko passen und auch inhaltlich keine Deckungslücken entstehen. Insbesondere die (Rück-)Versicherung von physischen Schäden nach einem auslösenden Cyberereignis ist zu beachten.

7. Zusammenfassung

7.1. Auswirkungen im Risikomanagement

Wie in den vorangegangenen Abschnitten beschrieben, sind die Auswirkung von Cyberrisiken auf das Risikomanagement potenziell vielfältig. Sie hängen insbesondere sehr stark vom betriebenen Geschäftsmodell und der Struktur des entstehenden Cyberportfolios ab. Zusätzlich zu den oben bereits aufgeführen möglichen Maßnahmen dienen die folgenden Punkte der übergreifenden Orientierung:

- Über Grenzen hinweg denken (d.h. über Sparten, Deckungsarten, Cyberszenarien und organisatorische Strukturen): Die potenziellen Auswirkungen von Cyberereignissen sollten ganzheitlich analysiert werden und auf dieser Basis ein Cyber-Risikoappetit bestimmt werden. Die Vernetzung im Unternehmen über Funktionen hinweg ist auch wichtig, um schnelle Reaktionsmöglichkeiten zu gewährleisten, die der Dynamik von Cyberrisiken gerecht werden.
- Kenntnis des Portfolios: Versicherer sollten die Exponierung (inkl. Silent Cyber und affirmative Deckungen) so genau wie möglich kennen und ggf. neue, zielgerichtete Kenngrößen festlegen und beobachten. Hierzu gehört, die Grenzen von Ausschlüssen und Klauseln auf Erst- und Rückversicherungsseite zu untersuchen und zu beobachten, und nicht blind auf eingesetzte Modelle zu vertrauen.
- IT/Cyber Security Know-How: Die umfassende Einbeziehung dieser Expertise ist sehr wichtig, um Cyberrisken und potenzielle Kumule bei der Tarifgestaltung, in der Steuerung des Underwritings und im Schadenmanagement berücksichtigen zu können.
- Trends und Entwicklungen berücksichtigen: Das Management von Cyberrisiken erfordert ggf. kurzfristige Reaktionsmöglichkeiten, d.h. Versicherer sollten sich organisatorisch und vertraglich so aufstellen, dass erkannte Risiken zeitnah kommuniziert und adressiert, dass Annahmen häufig überprüft und wenn nötig geändert und dass Risikoeinschätzungen entsprechend angepasst und kommuniziert werden können.

7.2. Ausblick

Der Markt für die Absicherung von Cyberrisiken durch Versicherungsunternehmen wird aus unserer Sicht zukünftig weiter wachsen, die Versicherungsprodukte werden weiter reifen und damit auch eine weitere Standardisierung einher gehen. Die oben angeführten spezifischen Eigenschaften von Cyberrisiken werden sich dabei teilweise relativieren – einfach aufgrund zunehmender Erfahrung im Umgang mit dieser noch neuen Versicherungssparte. Andere Eigenschaften allerdings werden bleiben, und daher wird sich das Risikomanagement entsprechend weiter entwickeln. Mit diesem Ergebnispapier haben wir erste Impulse gegeben, und wir sind zuversichtlich, dass Aktuare auch weiterhin – nicht zuletzt unter Verwendung

neuer Ansätze und Methoden – einen wichtigen Beitrag zur Etablierung des Cyber-Risikomanagements leisten werden.