Cyberrisiken und ihr Einfluss auf das Risikomanagement

Der Markt für Cyberversicherung wächst stetig, nicht zuletzt als Folge der Coronapandemie. Versicherer zeichnen Cyberrisiken zwar derzeit restriktiver; dennoch wird auch aus Sicht der Deutschen Aktuarvereinigung e.V. (DAV) die volkswirtschaftliche Bedeutung dieser Versicherungssparte weiter zunehmen. Aus diesem Grund sollte weiter daran gearbeitet werden, diese Risiken besser zu verstehen und das Management auf ihre speziellen Eigenschaften abzustimmen.

Einer repräsentativen Unternehmensbefragung in Deutschland zufolge gaben zwei Fünftel der Unternehmen an, dass sie in den vergangenen zwölf Monaten Ziel eines Cyberangriffs waren. In Deutschland gab es bereits im Jahr 2018 nahezu 100.000 Fälle von Cyberkriminalität, und die weltweiten Schäden beliefen sich Ende 2020 laut einer Studie von McAfee auf eine Billion, also 1.000 Milliarden US-Dollar, und haben sich damit seit 2018 fast verdoppelt. Entsprechend steigt der Bedarf für Cyberversicherungen. Aktuelle Schätzungen zum Markt für Cyberpolicen geben ein weltweites Prämienvolumen von mehr als sieben Milliarden US-Dollar für das Jahr 2020 an. Bis 2025 wird von einem Wachstum auf über 20 Milliarden US-Dollar ausgegangen, bei jährlichen Steigerungsraten von über 20 Prozent.

Risiken der Cyberversicherung

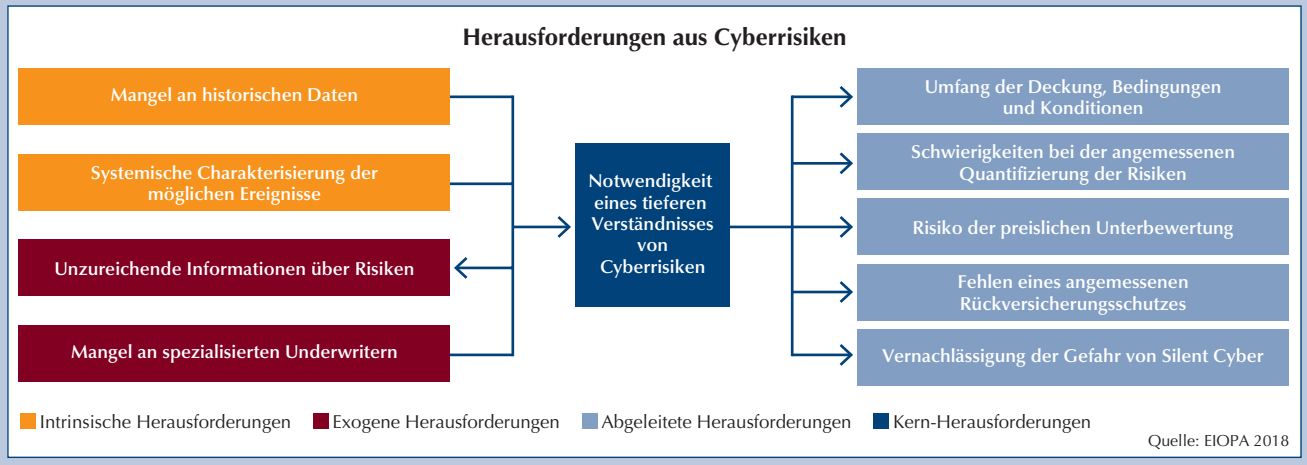
Das Management eines Cyberversicherungsbestandes birgt eine Reihe spezieller Herausforderungen. Cyberrisiken unterscheiden sich teilweise stark von anderen, klassischen Versicherungssparten. Sie erwachsen aus drei Quellen: aus der eigenen Geschäftstätigkeit des Versicherungsunternehmens, aus speziell entwickelten Cyberpolicen und aus klassischen Versicherungsprodukten, bei denen Schäden auch durch Cyberereignisse hervorgerufen werden – sogenanntes Silent Cyber.

Cyberrisiken an sich unterliegen starken Dynamiken, und zwar in Bezug auf die Produktlandschaft, auf die rechtliche Situation und auf die Risikolage. Es ist davon auszugehen, dass sich die ersten beiden über die Zeit weiter festigen, die Risikolage allerdings wird durch stetig neue Angriffs- und Abwehrmechanismen dynamisch bleiben. Weiter weisen Cyberrisken eine starke Kumulgefährdung auf: Ein einzelnes Cyberereignis kann eine enorm große Anzahl von Einzelschäden hervorrufen und Versicherer auf beiden Seiten der Bilanz treffen. Das führt potenziell zu einem großen, geografisch nicht begrenzten Gesamtschaden – anders als bei Stürmen oder Erdbeben.

Schließlich stehen Versicherer vor der Herausforderung, Cyberrisken mit geeigneten mathematischen Modellen zu messen, Cyberprodukte mit einem angemessenen Preis zu versehen und die Gesamtrisikolage zu steuern. An allen Stellen dieses Prozesses gibt es eine Reihe von Herausforderungen – wobei vor allem das Thema unzureichender Daten hervorzuheben ist. Die Europäische Aufsichtsbehörde für das Versicherungswesen (EIOPA) hat bereits 2018 die entsprechenden Herausforderungen zusammengefasst, wie in der Abbildung zu sehen ist.

Dynamik und Kumulgefährdung

Wie können Versicherungsunternehmen mit den besonderen Herausforderungen von Cyberrisken umgehen? Um



auf die Dynamik von Cyberrisiken, also auf neue Risikoszenarien reagieren zu können, ist ein aktives Management von Deckungen und Ausschlüssen nötig. Dieses sollte sich sowohl an aktuellen Schadenszenarien als auch an Industrie-Benchmarks orientieren.

Gleichzeitig ist eine ständige Beobachtung der Risikosituation im Sinne der „Schere" zwischen Bedrohungssituation und zur Verfügung stehenden Abwehrmechanismen nötig. Technologischer Sachverstand wie IT-/Cyber-Expertenwissen wird zunehmend auch im Risikomanagement verankert. Ähnliches gilt in Bezug auf Änderungen in der Rechtslage. Nur Expert*innen können eine unmittelbare Einschätzung der Auswirkungen liefern sowie Maßnahmen zum Beispiel in der Produktgestaltung vorschlagen. Das Kumulmanagement für Cyberrisiken erfordert detaillierte und flexible Analysemöglichkeiten der vorhandenen Cyberexponierung. Als Teil der Analysen sollten umfassende Extremszenarien betrachtet werden, die die Auswirkung von Cyberereignissen auf die gesamte Bilanz testen.

Häufiger Bestandteil von Cyberpolicen sind Assistance-Leistungen. Dabei werden Versicherungsnehmende im Schadenfall unterstützt – zur zeitnahen Behebung eingetretener Schäden und zur Verringerung des finanziellen Gesamtschadens. Im Kumulfall kann die schadenmindernde Wirkung allerdings aufgrund der Masse auftretender Schadenfälle verloren gehen. Dieser potenzielle Sekundäreffekt sollte in der Risikomessung berücksichtigt werden beziehungsweise die Skalierbarkeit von Assistance-Leistungen insbesondere für den Fall von Massenschäden so weit wie möglich abgesichert werden. Und schließlich sollten Versicherer, die aufgrund des eigenen Datenschatzes selbst ein besonders lohnendes Ziel für Cyberangriffe darstellen, ihren eigenen operativen Betrieb entsprechend gegen Cyberschäden absichern.

Daten und Modellierung

Die Grundlage für alle weitergehenden Maßnahmen des Cyberrisikomanagements sind umfassende, aktuelle und detaillierte Informationen – sowohl über frühere Schadenszenarien als auch über aktuelle und potenzielle zukünftige Bedrohungssituationen. Die hierfür notwendigen Daten sind strukturiert zu erheben, auf einer Datenplattform zusammenzuführen und verfügbar zu machen, um notwendige Analysen flexibel und zeitnah durchführen zu können. Eine Data Citizenship – also die breite Teilhabe an den in den Unternehmen vorhandenen Daten – ist im Kontext von Cyberrisiken aufgrund der Vielzahl beteiligter Fachleute besonders wichtig. Da oftmals ein Mangel an verlässlichen Daten zu Cyberrisiken besteht, werden Versicherungsunternehmen auch weiterhin auf externe Datenpools zurückgreifen.

Versicherer nutzen zur Risikomessung oftmals mathematische Modelle, die von externen Dritten entwickelt werden. Aufgrund der Vielzahl eingesetzter Modellvarianten ist es für Versicherer allerdings unerlässlich, auch ein eigenes Verständnis über die konkreten Risikoszenarien beziehungsweise Modellierungsansätze zu entwickeln.

Steuerung von Cyberrisiken

Wegen der Dynamik von Cyberrisken sollte es möglich sein, auch kurzfristig portfolioweite Anpassungen an Cyberpolicen vorzunehmen. Daher sind kürzere Laufzeiten von Cyberdeckungen denkbar, ebenso wie unterjährige Anpassungsmöglichkeiten in Deckungsumfängen und -preisen.

Im Rahmen der Risikosteuerung wird zunehmend auf das Zusammenpassen von Produkt- und Rückversicherungsseite geachtet. Es wird somit hinterfragt, ob die auf Kundenseite eingegangenen Risiken auch wie erwartet zum Rückversicherer transferiert werden. Insbesondere in Hinblick auf Silent Cyber sollte sichergestellt werden, dass etwaige Ausschlussklauseln in Rückversicherungsverträgen zum Originalrisiko passen, um unerwartete Deckungslücken zu vermeiden.

Fazit

Cyber bleibt eine große Herausforderung

Nicht zuletzt durch die Coronapandemie sind IT- und Cyberrisiken noch stärker in das allgemeine Blickfeld gerückt. Der gesamtwirtschaftliche Bedarf an Cyberversicherungen wird weiter steigen. Das macht es für Versicherungsunternehmen, die Absicherungen gegen Cybergefahren anbieten, umso wichtiger, den daraus entstehenden speziellen Herausforderungen angemessen zu begegnen. Hierzu müssen alle Elemente der Wertschöpfungskette einbezogen werden, von der Produktgestaltung über das Risikomanagement bis hin zur Schadenregulierung. Zudem muss über Grenzen von Sparten, Funktionen und Expertenbereichen hinweg gedacht werden. Dabei ist die Integration von technologischem Know-how genauso wichtig wie die Beobachtung der Entwicklung im Bereich des cyberspezifischen Haftungsrechts. Gleichzeitig müssen die Sammlung und Nutzung von Daten intensiviert werden, beispielsweise durch die Speicherung von Daten über Cyberschadenfälle in der Schadenregulierung, durch die umfassende Analyse von Silent-Cyber-Exponierungen oder auch durch die zusätzliche Nutzung externer Datenquellen. Insgesamt arbeiten Versicherer sehr aktiv an der Verbesserung ihrer Datenlage und ihren Fähigkeiten zur Risikomessung und -steuerung. Gerade im Fall von Cyberrisken ist es essenziell, auf erkannte neue Risikoszenarien flexibel und zielgerichtet zu reagieren.