Cyber-Risiken: Eine Standortbestimmung

Wirtschaft und Gesellschaft befinden sich mitten in einem umfassenden digitalen Transformationsprozess. Die intensive Nutzung von Smart Devices, die Entwicklung des Internet of Things und die Abhängigkeit von Cloud Services sind nur einige Anzeichen hierfür. Gleichzeitig erhöht die zunehmende Vernetzung die Anfälligkeit für Cyber-Risiken. Die steigende Anzahl von Cyber-Attacken sowie die fortschreitende Regulierung erhöhen das Bewusstsein für derartige Risiken weiter.

Dabei sind Cyber-Risiken nicht leicht zu definieren. So gehören beispielsweise Systemfehler und -ausfälle eines Cloud-Anbieters dazu. Sie können sehr kostspielig werden, denn sie führen zur Unterbrechung der Geschäftstätigkeit eines Unternehmens oder ganzer Lieferketten. Fehlfunktionen können Schäden an Maschinen hervorrufen oder sogar die Gesundheit von Menschen gefährden. Auch eine durch Computerviren verursachte Zerstörung oder Verfälschung von Daten kann zu erheblichen Schäden führen. Oftmals schlagen auch hohe Kosten für die Wiederherstellung der Daten und für die Abwehr von Rechtsstreitigkeiten mit Lieferanten und Kunden zu Buche – von den drohenden Reputationsschäden ganz zu schweigen.

Gemeinsam ist derartigen Szenarien, dass sie aus der allgegenwärtigen Nutzung von Informations- und Kommunikationstechnologien resultieren und dass Vertraulichkeit, Verfügbarkeit oder Integrität von Daten oder Systemen beeinträchtigt wird. Dabei ist es unerheblich, ob diese Beeinträchtigungen natürliche Ursachen haben oder von Menschen – absichtlich oder unabsichtlich – herbeigeführt werden.

Cyber-Resilienz verbessern

Die Schätzungen zu weltweiten Cyber-Schäden reichen von etwa 600 Milliarden bis zwei Billionen US-Dollar pro Jahr, wobei selbst einzelne Ereignisse oder Attacken enorme Kosten verursachen können.

Daher ist es sehr wichtig, die allgemeine Cyber-Resilienz, das heißt die Widerstandsfähigkeit gegenüber zukünftigen Cyber-Schadenszenarien, von Wirtschaft und Gesellschaft zu steigern. Das kann nur gelingen, wenn alle Beteiligten eng zusammenarbeiten. Hierzu zählen neben Unternehmen und der Öffentlichkeit auch Technologiebetreiber und öffentliche Einrichtungen sowie der Gesetzgeber. Die Versicherungswirtschaft spielt als Risikoträger hierbei eine besondere Rolle. Sie kann nicht nur finanzielle Verluste ausgleichen, sondern mit ihrer Erfahrung und ihren Daten wertvolle Beiträge zur Risikoerfassung, zur Risikoprävention und zum Schadenmanagement leisten.

Die Absicherung von Cyber-Risiken durch Versicherungslösungen stellt ein relativ neues, stark wachsendes und derzeit profitables Geschäftsfeld für Erst- und Rückversicherer dar. In den USA hat sich bereits ein entsprechender Versicherungsmarkt gebildet, wo heute auch etwa 90 Prozent des weltweiten Geschäfts mit Cyber-Versicherungen stattfinden. Schätzungen zufolge beträgt das Prämienvolumen etwa acht Milliarden US-Dollar pro Jahr, mit steigender Tendenz.

Damit macht dieses neue Geschäftsfeld einen verschwindend kleinen Anteil am gesamten Prämienaufkommen der Schadenversicherung aus. Dies liegt nicht nur an der Neuartigkeit des Produktes Cyber-Versicherung. Vielmehr gibt es systematische Herausforderungen, die eine Entwicklung und umfassende Vermarktung entsprechender Versicherungslösungen bislang erschweren.

Versicherbarkeit von Cyber-Risiken

Ganz allgemein sind Risiken umso eher versicherbar, je besser sich zukünftige Schäden abschätzen lassen, und das bei einer möglichst geringen Schätzunsicherheit. Außerdem sollte der Ausgleich im Kollektiv und in der Zeit funktionieren: Unter allen versicherten Risiken sollten jeweils nur wenige von Schäden getroffen werden. Diese Bedingungen treffen zum Beispiel für die Auto- oder die Krankenversicherung zu. Eine reiche Datenhistorie bietet den Versicherungsmathematikern hier eine verlässliche Basis, um zukünftige Schäden abzuschätzen. Und grundsätzlich funktioniert der Risikoausgleich auch, wenn hin und wieder Naturkatastrophen oder Epidemien eintreten.

Im Gegensatz dazu gibt es bei der Einschätzung von Cyber-Risiken größere Hürden:

- Komplexe, vernetzte IT-Systeme erschweren die Risikoeinschätzung.
- Ein Mangel an verlässlichen (historischen) Daten und die Dynamik von Cyber-Bedrohungen machen die Abschätzung zukünftiger Schäden schwierig.
- Selbst einzelne Cyber-Ereignisse oder -Attacken können zu umfassenden, gegebenenfalls netzweiten Schäden führen. Dies hebelt den Ausgleich im (Cyber-) Kollektiv aus.

- Eine mangelnde Standardisierung erschwert den Produktvergleich: Auch wenn die Versicherungsbedingungen oftmals Eigenschäden, zum Beispiel Betriebsunterbrechungen, Kosten für die Wiederherstellung von Daten, beziehungsweise Drittschäden wie die Haftung für die unbeabsichtigte Weiterverteilung von Viren oder für Folgeschäden aus Systemausfällen sowie Kosten für die Schadenfeststellung, Schadenbegrenzung und das Krisenmanagement umfassen, gibt es im Detail erhebliche Unterschiede.

Eine weitere Herausforderung sind sogenannte „stille" Cyber-Risiken. Das sind implizite Cyber-Haftungen, die in klassischen Sach- oder Haftpflichtversicherungen eingeschlossen sind, jedoch bei der Kalkulation der Prämien und im internen Risikomanagement erst allmählich Berücksichtigung finden. Insgesamt führt dies dazu, dass Versicherer derzeit die Kapazitäten für Cyber-Deckungen eher knapphalten und erhebliche Sicherheitszuschläge einkalkulieren.

Grundsätzlich ist die Dynamik in diesem Bereich aber sehr groß: So liefern verschiedene Verbände und Organisationen wie der Gesamtverband der Deutschen Versicherungswirtschaft regelmäßig Beiträge für eine Systematisierung und Standardisierung der Cyber-Deckungsumfänge. Produktentwickler und Aktuare arbeiten daran, die Probleme der Komplexität und der unzureichenden Datenbasis durch den Einsatz neuartiger Methoden und die Erschließung neuer Datenquellen zu lösen. Gleichzeitig werden reine Versicherungslösungen immer stärker durch die Kooperation mit Dienstleistern und die Bildung neuartiger „Anbieter-Ökosysteme" ersetzt, um einerseits das Risikoverständnis zu erhöhen und andererseits im Fall der Fälle durch aktives Schadenmanagement das Schadenausmaß so gering wie möglich zu halten. Und schließlich sind Versicherungsunternehmen bemüht, auch „stille" Cyber-Risiken zu messen beziehungsweise diese Risiken durch Haftungsausschlüsse oder -begrenzungen zumindest beherrschbar zu machen.

Aktuarielles Know-how gefragt

Die Entwicklung und Vermarktung von Cyber-Versicherungslösungen erfordern Anpassungen über die gesamte Wertschöpfungskette von Versicherungsunternehmen hinweg. Die Aktuare sind durch die beschriebenen Entwicklungen in folgenden Feldern gefordert:

Mathematische Modellierung:
- Erschließung neuer Datenquellen zur Risikobeurteilung und zur Bewertung von Cyber-Risiken sowie Sicherstellung von Qualität und Relevanz der Datenquellen
- Einbeziehung von szenariobasierten Analyse- und Bewertungsmethoden
- Weiterentwicklung aktuarieller Tools und Erweiterung von bestehenden Risikomodellen um das Cyber-Kumulrisiko
- Aktive Vernetzung mit Wissenschaft und spezialisierten Drittanbietern

Risikomanagement und Prozesse:
- Intensive Beschäftigung mit Gegenmaßnahmen und fortlaufendes Risikomanagement
- Flexibilisierung und Beschleunigung der Produktentwicklungsprozesse
- Nutzung von Risikotransfers mittels Rückversicherung
- Intensive übergreifende Kommunikation, zum Beispiel mit Netzwerk- und IT-Experten, Haftungsexperten, Schadenmanagern

Geschäftsmodelle von Versicherungen:
- Ausbau des Verständnisses für die zugrunde liegenden technischen Mechanismen sowie für die Möglichkeiten der Schadenprävention und des Schadenmanagements
- Stärkere Vernetzung mit dem Risikomanagement im Versicherungsunternehmen
- Enge Kooperation mit Dienstleistern zur Schadenprävention und zum Schadenmanagement

Um den in diesem Bereich tätigen Aktuaren eine Orientierung zu geben und eine vertieftes aktuarielles Verständnis für Cyber-Risiken zu entwickeln, hat die Deutsche Aktuarvereinigung vor einigen Monaten eine Arbeitsgruppe eingesetzt, die die Aktuare mit praktischen Hilfestellungen unterstützen wird.

Ausblick

Aktuare werden zum Treiber der Entwicklung

Die Versicherungswirtschaft ist gefordert, Wirtschaft und Gesellschaft mit geeigneten Versicherungsprodukten dabei zu unterstützen, den aus einer zunehmenden Digitalisierung entstehenden Risiken zu begegnen. Nur dadurch können Risiken reduziert und die Cyber-Resilienz insgesamt gesteigert werden. Diesem Anspruch stellen sich allerdings noch einige komplexe Probleme in den Weg.
Um diese Herausforderungen zu überwinden, sind nicht zuletzt Versicherungsmathematiker gefordert. Sie sollten in enger Zusammenarbeit mit Experten anderer Disziplinen neue Datenquellen erschließen und aktuarielle Methoden weiterentwickeln und somit die notwendige Verbesserung von Prozessen und Geschäftsmodellen unterstützen. Auf diese Weise wird es der Versicherungswirtschaft möglich, integrierte Cyber-Deckungen im benötigten Umfang und mit der nötigen Leistungsfähigkeit auf den Markt zu bringen.