Cyberrisiken: Methodenkompetenz muss erweitert werden

Die Digitalisierung erfasst – nicht zuletzt getrieben durch die Entwicklungen rund um Corona – mittlerweile immer weitere Bereiche unseres privaten wie beruflichen Lebens. Im Zuge dieser Entwicklung rückt das Thema Cyberrisiken regelmäßig in unser Bewusstsein, insbesondere und regelmäßig dann, wenn Cyberereignisse Datenlecks oder Ausfälle von IT-Systemen hervorrufen. In diesen Momenten wird intensiv über praktische Maßnahmen zum Schutz gegen derartige Ereignisse nachgedacht. Gleichzeitig wächst der Markt für Versicherungslösungen zur Absicherung von Cyberrisiken beständig. Eine Arbeitsgruppe der Deutschen Aktuarvereinigung e.V. (DAV) hat sich daher in den vergangenen Monaten intensiv mit diesem Thema beschäftigt. Sie hat analysiert, inwiefern bereits Versicherungsprodukte existieren und inwieweit verlässliche Daten sowie Methoden vorhanden sind, um diese zu entwickeln und zu managen.

Die Zahlen zeigen: Cyberrisiken sind eine reale Gefahr für Unternehmen sowie Privatpersonen und die dadurch verursachten Schäden sind enorm. So gab es im Jahr 2018 mehr als 87.000 Fälle von Cyberkriminalität in Deutschland und weltweit verursachte die Cyberkriminalität Schäden in Höhe von mehr als 500 Milliarden Euro. Die Versicherungsprämien für Cyberversicherungen lagen im gleichen Jahr bei etwa 3,5 Milliarden US-Dollar. Bis zum Jahr 2025 wird mit einem Prämienwachstum auf bis zu 20 Milliarden US-Dollar gerechnet.

Cyberrisiken und deren Management

Ein Cyberrisiko besteht darin, dass die erwartete Verfügbarkeit von Informationssystemen oder Daten eingeschränkt ist oder dass die Informationssicherheit – zum Beispiel Vertraulichkeit oder Integrität von Daten – verletzt wird. Mithilfe der Versicherungsmathematik machen die Aktuar*innen Cyberrisiken messbar. Erst dadurch wird es möglich, entsprechende Versicherungsprodukte zu entwickeln und zu vermarkten.

Die Messung von Cyberrisiken beinhaltet jedoch eine Reihe spezifischer, teilweise kaum überwindbarer Herausforderungen: Die starke Vernetzung der heutigen IT führt zu einer hohen Abhängigkeit von Cyberrisiken untereinander – vergleichbar mit großen Erdbeben oder Stürmen. Kurze Innovationszyklen in der Informationstechnik bedingen eine hohe Veränderungsgeschwindigkeit. Gegenmaßnahmen werden schnell unwirksam. Und Daten über bekannte Schadenereignisse veralten ebenso schnell.

In der gewerblichen Cyberversicherung unterscheiden sich die angebotenen Versicherungsprodukte stark. Allerdings beinhaltet die Mehrheit der Produkte eine Abdeckung von Haftpflichtschäden sowie von Schäden aus Betriebsunterbrechungen, und viele Policen decken zusätzlich Dienstleistungen ab, die infolge eines Cyberevents notwendig werden: die unmittelbare Hilfeleistung im Schadenfall, eine Wiedereinrichtung von IT-Systemen oder notwendige Kommunikationsmaßnahmen. Die vom Gesamtverband der Deutschen Versicherungswirtschaft herausgegebenen Musterbedingungen für die Cyberrisikoversicherung umfassen diese Maßnahmen ebenfalls. Der Markt für private Cyberversicherung ist in Deutschland noch klein. Auch hier sind die Versicherungsangebote heterogen, der angebotene Deckungsumfang bezieht sich überwiegend auf Eigenschäden aus Online-Aktivitäten wie Online-Shopping oder -Banking.

Insgesamt zeigt die Analyse, dass vor dem Kauf einer entsprechenden Versicherungsdeckung eine sehr klare Vorstellung über den tatsächlich benötigten Deckungsumfang vorhanden sein sollte, um aus dem vielfältigen Angebot eine geeignete Auswahl zu treffen. Aufgrund der dynamischen Entwicklung im gesamten IT-Bereich ist umso genauer zu verfolgen, wie sich eingekaufte Deckungen gegenüber dynamischen Feldern wie dem autonomen Fahren oder der wachsenden Bedeutung des Internet of Things (IoT) verhalten.

Herausforderung Silent Cyber

Können Versicherer zumindest einen klaren Trennstrich zwischen „klassischen Risiken" und Cyberrisiken ziehen? Leider keineswegs! Ein Beispiel: Sofern kein ausdrücklicher Ausschluss vorgesehen ist, deckt die Feuerversicherung eines Rechenzentrums Brände, ganz gleich, ob diese aufgrund eines Kurzschlusses oder aufgrund eines Hackerangriffs entstehen. Das klingt zunächst gut für den Versicherungsnehmer. Es kann für den Versicherer jedoch bedeuten, dass Risiken unterschätzt werden. Aus diesem Grund werden diese als Silent Cyber bekannten Risiken derzeit verstärkt analysiert.

Auch die Aufsichtsbehörden widmen sich dem Thema. Die europäische Versicherungsaufsichtsbehörde EIOPA hat 2018 eine Analyse zu Cyber veröffentlicht. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) plant nach einer im Jahr 2019 durchgeführten Abfrage weitere Untersuchungen, nicht zuletzt zu Silent Cyber.

Methoden und Daten

Anders als in vielen anderen Versicherungssparten gibt es keine Standardmethode zur Messung von Cyberrisiken. Von einfachen faktorbasierten Ansätzen über statistische und probabilistische Verfahren bis hin zu Predictive Models und künstlicher Intelligenz finden sehr unterschiedliche Methoden Anwendung – immer in Abhängigkeit von den zur Verfügung stehenden Daten. Daher arbeiten Versicherungsunternehmen und spezialisierte Dienstleister an der Erschließung sowie der Aufbereitung neuer Datenquellen.

Sogenannte Datenschemata strukturieren die risikorelevanten Informationen und umfassen Daten zum Unternehmensprofil, zu Datenbeständen, zu IT-Systemen sowie zu getroffenen Sicherheitsmaßnahmen. Statistiken zu Schadenursachen liefern Informationen über die Häufigkeit der verschiedenartigen Cyberattacken, differenziert etwa nach Branchen und geografischen Regionen. Die Schadenanfälligkeit ist kundenspezifisch und misst, wie anfällig ein Versicherungsnehmer gegenüber Cyberrisiken ist – zum Beispiel gemessen durch die Anzahl betriebener Server, den Datendurchsatz oder die Komplexität des internen IT-Netzes.

Schadendaten messen den monetären Schaden spezifischer Cyberangriffe sowie weitere Größen, wie die Anzahl verlorener Datensätze oder die Dauer einer Betriebsunterbrechung. Neben „echten" Schäden werden oft auch Beinaheschäden analysiert. Dabei stellt man sich die Frage, welcher Schaden entstanden wäre, wenn glimpflich abgelaufene Ereignisse einen schlimmeren Verlauf genommen hätten. Ein Beispiel: Während des Cyberangriffs WannaCry 2017 wurden über 230.000 Computer in 150 Ländern infiziert und jeweils Lösegeldzahlungen verlangt. Der Schaden wäre vermutlich ungleich größer gewesen, wäre nicht durch Zufall ein hemmender Schalter gefunden worden.

Nicht jeder einzelne Versicherer kann derart umfangreiche Informationen selbst erfassen. Daher müssen externe Datenquellen genutzt werden. Die DAV-Ausarbeitung enthält umfassende Listen derartiger Quellen, um Aktuar*innen einen Startpunkt für eigene Analysen zu geben. Der Ergebnisbericht steht allen Interessierten auf der DAV-Webseite unter www.aktuar.de zur Verfügung. Unabhängig von Datenquellen und eingesetzten Methode steht es in der Verantwortung der Aktuar*innen, sich kritisch mit der Qualität der verwendeten Daten auseinanderzusetzen. Gleichermaßen müssen die entwickelten Rechenmodelle verständlich gestaltet werden, damit fortlaufende Prüfungen und Weiterentwicklungen möglich sind. Zudem ist interdisziplinäre Zusammenarbeit entscheidend. Nur so kann sichergestellt werden, dass die genannten speziellen Herausforderungen von Cyberrisiken gemeistert werden können.

Fazit

Datenbasis wird sich deutlich vergrößern

Die Cyberversicherung ist bereits heute relevant und ihre Bedeutung wird mit dem Voranschreiten der Digitalisierung und der Vernetzung noch wesentlich zunehmen. Damit werden auch die Messung von Cyberrisiken und die Sammlung, Strukturierung sowie Auswertung der dazu benötigten Daten in diesem Zuge stark ansteigen. Auf der methodischen Seite sowie im Bereich von Silent Cyber sind noch etliche Fragen offen, die zu einem hohen Schätzrisiko und damit tendenziell zu Sicherheitsaufschlägen in den entsprechenden Versicherungsprämien führen. Es gibt allerdings vielversprechende Ansätze zur Lösung der Fragen rund um Methoden und Daten. Daher geht die DAV davon aus, dass die finanziellen Folgen zunehmend besser einschätzbar werden und Cyberversicherung damit auf immer stabilerer Basis betrieben werden kann.