Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Mehr als die stille Gefahr aus dem Netz

Silent Cyber

GDV
DIE DEUTSCHEN VERSICHERER

Die wichtigsten Fragen im Überblick

Was ist der Status Quo beim Thema Cyber?
Die Anzahl der durch Cyber-Risiken verursachten Schäden nimmt ebenso weiter zu wie auch das Schadensausmaß nach einem Risikoeintritt. Immer seltener müssen Versicherer heute noch Aufklärungsarbeit leisten: Das Risiko Opfer einer Cyberattacke zu werden, ist bei Versicherungs- und Risikomanagern bekannt. Die bisher gesammelten Erfahrungen der Branche mit Schadensverläufen haben für ein gewisses Bewusstsein gesorgt. Geklärt ist das Thema deshalb aber noch lange nicht.

Was macht Cyber-Schäden besonders?
Die aus einem Cyberrisiko resultierenden Schäden sind äußerst heterogen. Nicht selten treten mehrere Schadenszenarien gleichzeitig auf. Sehr häufig spielen Ertragsausfälle infolge von Betriebsunterbrechungen eine zentrale Rolle.

Was hat es mit Silent Cyber auf sich?
Unter Silent Cyber bzw. non-affirmative Cyber verstehen Versicherer potentielle Risiken, die teilweise über die klassischen Versicherungen, und nicht ausschließlich über eine spezielle Cyber-Versicherung abgedeckt sind - die unbeabsichtigte Cyberexponierung. Sie kann sich in Policen aus allen Versicherungssparten wiederfinden. Über 60 Prozent der für den „Silent Cyber Risk Outlook" des Risikomanagementunternehmens Willis Towers Watson befragten Personen (Vorjahr: knapp 50 Prozent) schätzen, dass der „Silent Cyber-Faktor" in den nächsten zwölf Monaten auf mehr als einen Cyberschaden im Vergleich zu 100 anderen „Nicht-Cyberschäden" steigt. Versicherer erwarten überdies in steigendem Maße Großangriffe wie die der Schadprogramme WannaCry oder NotPetya.

Welche Schadenssummen kommen auf die Unternehmen zu?
Den betroffenen Unternehmen sind durch Schadsoftware teilweise Kosten im dreistelligen Millionenbereich entstanden. Zugleich erhöhen sich die Cyberrisiken mit zunehmender Vernetzung von Endgeräten und Maschinen.

Wie wird sich der Markt für Cyber-Versicherungen entwickeln?
Mit steigendem Risikobewusstsein bei Versicherungs- und Risikomanagern wächst auch die Nachfrage nach eindeutigem, adäquaten Deckungsschutz inklusive Assistance-Leistungen kontinuierlich. Die größten Herausforderungen dabei sind die Abgrenzungen zu non-affirmative Cyber, das Kumul- und das Änderungsrisiko.

„Die Digitalisierung verändert Cyberrisiken permanent"

Dr. Stefan Sigulla und Klaus M. Przybyla über die Entwicklung von (Silent) Cyber-Risiken, die Zukunft des Risikodialogs und die Frage, wie Versicherer und Versicherungsnehmer gemeinsam zum Ziel kommen.

Wie schätzen Sie die Fallhöhe von Cyber-Risiken derzeit ein?
Sigulla: *Ob wir es wollen oder nicht: Cyber ist ein Risiko mit stark zunehmender Bedeutung – für das kreative Lösungen gefragt sind. Denn hinter "Cyber" verbergen sich Risiken, die bisher nicht immer ausreichend erfasst beziehungsweise eingeschätzt wurden. Insbesondere in älteren Standard-Policen werden häufig durch Cyber verursachte Schäden nicht erwähnt, sie sind nicht explizit ein- oder ausgeschlossen ("All Risk"). Aus der Vertragstechnik heraus halten viele Versicherungs- und Risikomanager das Risiko damit für ausreichend gedeckt, weil Allgefahrendeckungen einen umfassenden Schutz bieten, soweit keine ausdrücklichen Ausschlüsse vereinbart wurden. Als naturgemäß gerade nicht auf das Risiko zugeschnittenes Produkt ist die All-Risk-Police aber für Cyber-Fälle nicht mehr zeitgemäß.*

Przybyla: *Richtig. Bislang erinnert die Diskussion zu Cyber an die Fabel von Hase und Igel: Wenn die Notwendigkeit spezieller Cyberversicherungen angesprochen wird, heißt es meist: Die gibt es doch schon im Rahmen der All-Risk-Deckung. Nur weil kein Ausschluss greift, führt das aber nicht*

zwangsläufig zur Deckung. Vermögensschäden etwa sind oft in der in der Höhe begrenzt oder gar ausgeschlossen. Ich glaube, dass das Hase-und-Igel-Spiel beendet werden muss, weil es der tatsächlichen Risikoentwicklung nicht gerecht wird. Angesichts steigender Cyber-Gefahren muss unser gemeinsames Hauptaugenmerk auf Transparenz und Wissen liegen – im Interesse des Kunden und des Versicherers.

Klaus Przybyla ist Mitglied des Expertennetzwerks Internationales Geschäft des GDV.

Transparenz und Wissen – wie meinen Sie das konkret?

Przybyla: *Je intransparenter die Deckungssituation ist, desto schwieriger ist es, die notwendigen Deckungssummen zur Verfügung zu stellen. Wir müssen also gemeinsam definieren, wo welche Risiken versichert sind. Die Abgrenzung der Risiken versetzt uns Versicherer dann in die Lage, individuellere Angebote und somit langfristig Risikoschutz zur Verfügung zu stellen. Die komplizierte Lage von Cyber-Szenarien führt sonst dazu, dass Kunden keine Sicherheit darüber haben, welcher Versicherungsschutz tatsächlich besteht. Aus dem gleichen Grund ist es für die Versicherer schwierig, das selbst getragene Risiko einzuschätzen. Hier müssen wir gemeinsam die berechtigten Interessen aller Beteiligten zu einem zufriedenstellenden Ausgleich führen. Und zum Thema Wissen: Wir müssen das hohe Tempo unserer Zeit als permanente Weiterbildungs-Aufgabe verstehen. Im Zuge der Digitalisierung verändern sich die Cyberrisiken und Schadensszenarien schnell und fortwährend. Deswegen ist es entscheidend, die eigenen Ansätze und Kenntnisse stetig weiterzuentwickeln und zu teilen.*

Dr. Stefan Sigulla ist Mitglied des Präsidialausschusses Risikoschutz für Gesellschaft und Wirtschaft des GDV

Sigulla: *Wir brauchen dringend belastbare Definitionen, die dem Wandel Rechnung tragen: Wann ist ein Virus ein neuer Virus? Welche zeitlichen Begrenzungen gibt es? Wie sieht es mit Re-Infektionen aus? Hier müssen Versicherer und Versicherungsnehmer für Einheitlichkeit sorgen. Offen und transparent muss auch das Thema Kumul angegangen werden. Sind einzelne Cyber-Schäden sowohl in klassischen Verträgen wie auch in speziellen Cyber-Policen versichert, bedeutet dies für den Versicherer letzlich ein anders zu kalkulierendes Risiko.*

Wie gelangte das Thema Cyber vom Rand-Phänomen in den Fokus der Aufmerksamkeit?

Sigulla: *Die Welt entwickelt sich weiter. Eigentlich sollte "All Risk" historisch betrachtet vor überraschenden, unvorhersehbaren Entwicklungen schützen. Diesen Charakter hat das Thema Cyber längst verloren. Cyber ist im Lauf der Jahre erwachsen geworden, prägt das zu versichernde Risiko und benötigt deshalb eigens abgestimmten Schutz. Cyber ist nicht mehr silent, eine Police sollte es auch nicht mehr sein. Cyber deswegen einfach aus der All-Risk-Versicherung auszuschließen, kann jedoch nicht die befriedigende Antwort sein. Insgesamt muss es uns als Versicherer vielmehr darum gehen, die einzelnen Komponenten des "Cyber"-Risikos – silent oder nicht - transparent zu machen, eine ganzheitliche Risikoanalyse in den Vordergrund zu stellen und neben adäquatem Risikotransfer insbesondere auch Serviceleistungen anzubieten.*

Wie hat das Thema Cyber die Anforderungen an Versicherungs- und Risikomanager verändert?

Sigulla: Unternehmen sollten heute sehr viel mehr Zeit und Energie und Geld aufwenden als früher, um sich gegen potentielle Hacker zu schützen. Ein professioneller Angreifer, der systematisch über die Schwachstellensuche mit langem Atem und unter Zuhilfenahme von Social Engineering die Löcher eines Systems planmäßig erkundet, kann nur durch jemanden aufgehalten werden, der sich mit mindestens der gleichen Intensität der Analyse des Risikos und der Abdeckung des Restrisikos beschäftigt.

Wie sehen Sie die Zukunft der Cyber-Versicherung?

Sigulla: *Versicherer mit dem Anspruch, Enabler der deutschen Wirtschaft zu sein, haben die Verantwortung, Risikoentwicklung mit Versicherungsschutz zu begleiten – weshalb nicht der Risikoausschluss das Ziel von Versicherungsgebern und Versicherungsnehmern und Kunden sein kann, sondern eine nachhaltige Verfügbarkeit von Versicherungsschutz. Dieser kann nur durch Zuordnung der Risiken zum notwendigen Risikokapital ermöglicht werden.*

Przybyla: *Versicherer müssen wissen und verstehen, wie sich das Risiko darstellt, um die angemessene Deckung dafür anbieten zu können. Eine klare Zuordnung ist zwingende Voraussetzung, das definitiv weiter existierende und stark wachsende Risiko Cyber nachhaltig versicherungstechnisch begleiten zu können.*

“Wir müssen uns in die Karten schauen lassen”

Alexander Mahnke ist Vorstandsvorsitzender des Gesamtverbands der versicherungsnehmenden Wirtschaft (GVNW).

Welchen Stellenwert messen Sie dem Thema Cyber in der Industrieversicherung heute bei?
Cyber wird immer wichtiger. Das hat natürlich mit dem digitalen Wandel zu tun, dem auch einst klassisch produzierende Unternehmen ausgesetzt sind. Einsen und Nullen können heute Unternehmen in Gefahr bringen.

Was bedeutet das für die Versicherungswirtschaft?
Der Bedarf nach speziellen Abdeckungen wird immer größer. Unternehmen brauchen heute nicht nur adäquaten Schutz, sondern viele darüber hinaus eine qualifizierte Beratung und Prävention. Die Risikolandschaft und die einst einkäuferfreundliche Situation auf dem Industrieversicherungsmarkt haben sich für Cyber verändert. Cyber-Policen gelten nun als etwas, mit dem man sich unbedingt beschäftigen muss. Dahinter steckt in Einzelfällen auch ein wenig Angstmache und nicht immer wird mit dem Aufzeigen von Schadensszenarien ausreichend professionell umgegangen. Voraussetzung ist bei dem Thema für mich, dass die Diskussion zwischen Versicherer und Versicherungsnehmer unter der Beteiligung von Fachexperten geführt wird.

Wie beurteilen Sie das Risiko von Silent Cyber?
Viele Versicherer stellen nun fest, dass sie Cyberrisiken schon in der Bilanz haben, die sie aber offenbar vergessen hatten zu bewerten. Das kann ein Problem darstellen. Erstens ist es immer schlecht, Risiken zu versichern, ohne sie ausreichend zu verstehen und zu bewerten. Zweitens fängt die BaFin inzwischen an, sich unter Solvency-Gesichtspunkten für das Thema zu interessieren. Und drittens sind es die Ratingagenturen, die hellhörig werden, was die Bewertung der Versicherer und ihr Finanzrating negativ beeinflussen könnte. Kurzum: Silent Cyber beschäftigt aus Sicht des GVNW den Industrieversicherungsmarkt zunehmend und wir sind versicherungsnehmerseitig sehr daran interessiert, ernsthafte Gespräche mit allen Beteiligten zu führen.

Wie könnte eine Lösung der Silent-Cyber-Frage aussehen, die Versicherer und Versicherungsnehmer gleichermaßen in ihren Bedürfnissen zufriedenstellt?
Nicht alle Cyber-Risiken können mit den Verträgen versichert sein, die wir schon haben. Kompletten Versicherungsschutz kann man sich nie kaufen. Als Verband schlagen wir vor, dass wir den aktuellen Lernprozess nutzen und im Zweifel auf ein Geben und Nehmen setzen. Alle Akteure sollten bei ihren Mitarbeitern größtmögliches technisches Verständnis sicherstellen. Die Versicherer müssen in meinen Augen stark in ihre technischen Ressourcen und Teams investieren, die Versicherten müssen immer besser darin werden, alles nötige Wissen über sich selbst zur Verfügung zu stellen, kurz: Wir müssen uns in die Karten schauen lassen. Ziel muss es sein, in Vertragsverhandlungen durch die Versicherer nicht möglichst viel von vornherein auszuschließen, sondern Werthaltigkeit und Nachhaltigkeit im Versicherungsschutz anzubieten. Ich plädiere für einen Markt, der stark von Vertrauen lebt. Wo Schutz vertrauensvoll eingekauft wird, werden Schäden später auch bezahlt.

Impressum

Herausgeber
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43/43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel. 030 2020–5000, Fax 030 2020–6000
www.gdv.de, berlin@gdv.de

Bildnachweis: Titel: iStock/gorodenkoff

Verantwortlich:
Oliver Hauner
Leiter Sach- und Technische Versicherung, Schadenverhütung, Statistik
Tel. +49 30 2020–5350 | o.hauner@gdv.de

Maike Lamping
Leiterin Versicherungstechnik
Tel. +49 30 2020–5351 | m.lamping@gdv.de