ASA | SVV

«Das Gefahrenbild von Cyber verändert sich ständig»

Interview | 02. November 2022

Der globale ökonomische Schaden durch Cyberkriminalität wird von einem der grössten Rückversicherer für das Jahr 2021 auf 6000 Milliarden US-Dollar geschätzt. Das entspricht etwa der Höhe der Schäden, die durch die Pandemie und die damit verbundenen Massnahmen entstanden sind. In der Prävention und Risikominderung von Cyberrisiken kommt den Versicherern eine wichtige Rolle zu. Auch wenn es darum geht, Unternehmen und Behörden mit Expertise zu unterstützen, sagt der SVV-Cyberexperte Gabor Jaimes.

Gabor Jaimes, was macht Cyber zu einem Toprisiko – ähnlich wie eine Pandemie oder ein grosses Erdbeben?

Das Bundesamt für Bevölkerungsschutz BABS hat in seinem «Risikobericht 2020» identifiziert, welche Gefahren die Schweiz bedrohen. Dazu gehören unter anderem Naturkatastrophen aller Art, grossflächige Cyberattacken, Pandemien oder eine Strommangellage. Solche Toprisiken können zu immensen ökonomischen und immateriellen Schäden für Wirtschaft und Gesellschaft führen. Aufgrund der zunehmenden Globalisierung und Digitalisierung können einige Toprisiken heute grössere Ausmasse annehmen, als dies früher der Fall gewesen wäre. Sie können unsere vernetzte Welt teilweise zum Erliegen bringen – ganz besonders im Falle von Cyber.

Der globale ökonomische Schaden durch Cyberkriminalität wird für das Jahr 2021 auf 6000 Milliarden US-Dollar geschätzt. Eine riesige Zahl – und wir wissen, dass nur ein kleiner Bruchteil davon überhaupt versichert ist.

Cyberrisiken kennen keine Kantons- oder Landesgrenzen und sind für praktisch alle Branchen relevant. Deshalb braucht es eine konstruktive Zusammenarbeit auf allen Stufen: SVV-Cyberexperte Gabor Jaimes.

Warum braucht es das Zusammenspiel diverser Akteure zur Bekämpfung von Cyberrisiken?

Bei einem Cyberangriff von globalem Ausmass sprechen wir von einem Schadenpotenzial von hundert

Milliarden US-Dollar oder mehr weltweit. Die Versicherer können den vom Markt benötigten Deckungen auch via Rückversicherer kaum nachkommen. Solche systemischen Risiken können auch global tätige Versicherer und Rückversicherer in finanzielle Schwierigkeiten bringen. Um Schadenzahlungen in anderen Bereichen der Versicherten nicht zu gefährden, muss die Versicherungsindustrie diese Risiken gut im Auge behalten und entsprechend managen. Um dennoch den bestmöglichen Schutz unserer Wirtschaft und Gesellschaft zu gewährleisten, müssen wir über partnerschaftliche Lösungsansätze mit allen Stakeholdern – inklusive Bund – nachdenken. Nur so können wir die Cyberresilienz stärken. Diese ist nicht nur für unsere Gesellschaft zentral, sondern auch für die nachhaltige Stärkung des Wirtschaftsstandorts Schweiz.

> Cyber ist eine Sparte, die anders als andere Bereiche funktioniert. Es braucht nebst dem traditionellen Versicherungswissen vertiefte digitale Skills.

Welche Chancen ergeben sich für die Versicherungsindustrie im Zusammenhang mit Cyberrisiken?

Für die Versicherer bietet Cyber ein enormes Wachstumspotenzial. Einerseits durch den grossen «Cyber Protection Gap» und die Ambition vieler Organisationen und Staaten, sich besser zu schützen, also resilienter zu werden. Anderseits bieten sich Chancen durch die unaufhaltsame Digitalisierung zahlreicher Abläufe im geschäftlichen wie auch im privaten Alltag. Was die Prämien betrifft, so wird sich das heutige Volumen bis ins Jahr 2025 wohl mehr als verdoppeln – von neun auf geschätzte 22 Milliarden US-Dollar. Das bedeutet, dass Cyberversicherung als Sparte in zehn Jahren für jede Versicherung und Rückversicherung in einem gut entwickelten Marktumfeld zu einem wichtigen Standbein werden kann – ähnlich wie heute die Sach-, Motorfahrzeug-, Haftpflicht oder Krankenversicherung.

Nicht zu unterschätzen sind auch die geschätzten 300 Milliarden US-Dollar an jährlichen Ausgaben für Cybersicherheit weltweit. Da Prävention eine Voraussetzung für eine Versicherungsdeckung ist, gibt es entlang der ganzen Wertschöpfungskette grosses Potenzial für Partnerschaften zwischen Versicherern und IT-Dienstleistern, was die Innovation zusätzlich ankurbeln wird.

Cyber ist zudem eine Sparte, die anders als andere Bereiche funktioniert. Es braucht nebst dem traditionellen Versicherungswissen vertiefte digitale Skills, die heute insbesondere die jüngeren Generationen mitbringen. Das ist eine Chance für die Versicherungsindustrie, diese Talente längerfristig für sich zu gewinnen – und neues Denken oder neue Lösungsansätze auch auf andere Sparten zu überführen.

Wie funktioniert die Zusammenarbeit im Bereich Cyber über Branchen hinweg?

Cyberrisiken kennen keine Kantons- oder Landesgrenzen und sind für praktisch alle Branchen relevant. Deshalb braucht es bei Cyber eine konstruktive Zusammenarbeit auf allen Stufen. Diese beginnt damit, dass Vorfälle so rasch wie möglich gemeldet werden, um eine mögliche Ausbreitung, etwa von Malware in einem Unternehmen, zu verhindern – oder zumindest die Auswirkungen zu reduzieren. Transparenz ist von zentraler Bedeutung, aber gleichzeitig auch eine Herausforderung, denn keine Firma gibt gerne zu, dass sie Opfer eines Cyberangriffs geworden ist. Deshalb braucht es einen «sicheren Hafen», wo dieser Informationsaustausch zeitnah und nach klaren Spielregeln stattfinden kann.

Eine solche Plattform bietet der Bund mit dem Nationalen Zentrum für Cybersicherheit NCSC. Das NCSC ist eine schweizweite Anlaufstelle für Privatpersonen, Unternehmen, Behörden und IT-Spezialisten, wo Cybervorfälle und Schwachstellen gemeldet werden können. Das NCSC ist auch verantwortlich für die koordinierte Umsetzung der Nationalen Cyber-Strategie (NCS) zum Schutz der Schweiz vor Cyberrisiken. Für die überarbeitete NCS 2023 konnte die Versicherungsbranche ihre Anliegen bisher gut einbringen und

steht hinter dieser Strategie.

Daraus abgeleitet haben sich auch die Finanzdienstleister zusammengeschlossen, um ihren Beitrag zur Cyberresilienz in gegenseitiger Abstimmung zu leisten. Sie bieten mit dem Swiss Financial Sector Cyber Security Centre (FS-CSC), zu dessen Gründungsmitgliedern auch der SVV zählt, eine Plattform für Wissensaustausch, Vernetzung und Krisenbewältigung und fördern die institutionelle Zusammenarbeit zwischen Finanzinstituten und Behörden bei strategischen und operationellen Fragen.

> Eine der Aufgaben der Versicherungsindustrie liegt darin, ihre Unternehmens- und Privatkunden, aber auch die Gesellschaft, auf das Thema Cybersicherheit zu sensibilisieren.

Welche Rolle kann die Versicherungsindustrie in der Prävention oder Bekämpfung der Cyberkriminalität einnehmen?

Im Bereich Cyberversicherung reicht es nicht, eine Police auszuhändigen, aufgrund deren im Schadenfall bezahlt wird. Eine der Aufgaben der Versicherungsindustrie liegt darin, ihre Unternehmens- und Privatkunden, aber auch die Gesellschaft, auf das Thema Cybersicherheit zu sensibilisieren und auf unvorsichtiges Verhalten – ob bewusst oder unbewusst – aufmerksam zu machen. Versicherer wollen zuerst sicherstellen, dass die Kunden über ein solides Abwehrsystem verfügen – und sie dann im Schadenfall bei der Bewältigung eines Angriffs bestmöglich unterstützen. Eine rasche und partnerschaftliche Kommunikation kann ein Problem idealerweise isolieren, grössere Schäden abwenden und einen möglichen Betriebsunterbruch in Grenzen halten.

Stichwort Resilienz: Was kann jede und jeder von uns selbst tun, um Cyberangriffen vorzubeugen?

Cyberangriffe zielen oft auf das Unwissen oder auf die Unvorsichtigkeit von Mitarbeitenden ab. Mitarbeitende müssen ihre Rolle kennen und wissen, wie sie sich schützen können. Denn sie sind ein wichtiges Mosaiksteinchen im Kampf gegen Cyberattacken. Als Privatperson ist man vor möglichen Angriffen nicht gefeit. Wird etwa der private E-Mail-Account angegriffen oder das Bankkonto gehackt, kann sich ein Virus von da aus weiterverbreiten. Man muss sicherstellen, dass alle Programme und Apps regelmässig aktualisiert werden und der Virenschutz dem neuesten Standard entspricht. Prävention ist immer noch der beste Schutz. Danach kommt eine Versicherung zum Zug. Aber sie kann den immateriellen Wert nicht ersetzen, wenn zum Beispiel persönliche Daten verlorengehen.

Über Gabor Jaimes

Gabor Jaimes ist Fachverantwortlicher Sach-, Cyber- und Elementarschadenversicherung im Schweizerischen Versicherungsverband SVV. Er verfügt über 20 Jahre Erfahrung in der Rückversicherungsbranche, davon rund 15 Jahre bei Swiss Re. Seit rund 5 Jahren beschäftigt er sich intensiv mit dem Thema Cyberversicherung und hat Einsitz im Steuerungsausschuss des Swiss Financial Sector Cyber Security Center (FS-CSC).

Cyberrisiken Digitalisierung Toprisiken

Lesen Sie mehr zum Thema

Add to PDF generator

Cybersicherheit im Schweizer Finanzmarkt stärken

Mit der Gründung des Vereins «Swiss Financial Sector Cyber Security Centre» (Swiss FS-CSC) wappnet sich der Schweizer Finanzplatz gegen die zunehmende Bedrohung durch Cybervorfälle.

News 06.04.2022 Weiterlesen

Add to PDF generator

«Je stärker ein Unternehmen digitalisiert ist, desto mehr gerät es in den Fokus»

Die Kriminalität im Internet hat stark zugenommen. Florian Schütz, Delegierter des Bundes für Cybersicherheit, beantwortet die drängendsten Fragen.

Interview 22.09.2021 Weiterlesen

Add to PDF generator

Cyber / Silent Cyber als Emerging Risk

Private und öffentliche Unternehmen sind heute in allen Bereichen ihrer Geschäftstätigkeit auf IT-Systeme angewiesen und entsprechend anfällig auf Störungen verursacht durch Cyber-Risiken.

Emerging Risks – eine Wertung aus Sicht der Haftpflicht 15.06.2022 Weiterlesen