Cyberkatastrophenrisiken – ein zunehmendes Problem

CHUBB®

Cyber-Vorfälle können Schäden verursachen, die keinen zeitlichen oder geografischen Einschränkungen unterliegen

Im Zuge der globalen Digitalisierung und der damit einhergehenden größeren Abhängigkeit von Technologien nimmt die Häufigkeit, Schwere und Raffinesse von Cyberangriffen zu. Die steigende Vernetzung führt zu einer Vervielfachung der Anzahl an Schwachstellen und Gefährdungspotenzialen. Hierdurch entstehen immer mehr systemische Risiken von großer Reichweite, die schwer zu erkennen und zu kontrollieren sind. Die Dimension dieser systemischen Risiken ermöglicht mit ihren potenziell schweren und weitgehenden Auswirkungen Cyberkatastrophen.

Ähnlich wie bei einer Pandemie können Cybervorfälle Schäden verursachen, die keinen zeitlichen oder geografischen Einschränkungen unterliegen. Dabei geht es längst nicht mehr um bloße Fiktion – Cyberkriminelle haben ihre Fähigkeit, Lieferketten von Unternehmen auf der ganzen Welt und kritische Infrastrukturen zu unterbrechen, bereits unter Beweis gestellt. Besonders deutlich zeigt dies zum Beispiel die Attacke auf Colonial Pipeline, das größte Pipelinesystem in den Vereinigten Staaten. Dies musste infolgedessen ihre Kraftstoffleitungen, die die Ostküste der Vereinigten Staaten versorgen, abschalten. Angesichts der jüngsten Cybervorfälle, die Schäden in Milliardenhöhe verursachten, kann man sich nur zu gut vorstellen, dass ein Angriff katastrophalen Ausmaßes die Bilanzstärke der Versicherungsbranche auf die Probe stellen würde.

Anders als bei früheren unvorhergesehenen Katastrophenereignissen erleben wir derzeit eine rasante und kontinuierliche Eskalation von Cyberrisiken. Diese Vorwarnung ermöglicht es, schon jetzt eine adäquate Cyberabwehr und wirtschaftliche Sicherungsmechanismen vorzuhalten, speziell für den Fall, dass es zur unvermeidlichen Katastrophe kommen sollte.

Cyberversicherungen erlangen Reifegrad

Die stetig steigende Zahl an Cyber-Versicherungen zeigt, dass viele Unternehmen inzwischen über eine Absicherung verfügen. Gleichzeitig bedeutet dies auch, dass die Aggregation des Cyber-Risikos für die Versicherungsbranche wächst.

Cyberversicherungen haben das gegebene Versprechen in den letzten Jahren in jeder Hinsicht gehalten. Die Versicherer kamen nach schwerwiegenden Cybervorfällen für den Schaden auf und konnten somit zahlreiche Unternehmen und Einrichtungen in der ganzen Welt schützen.

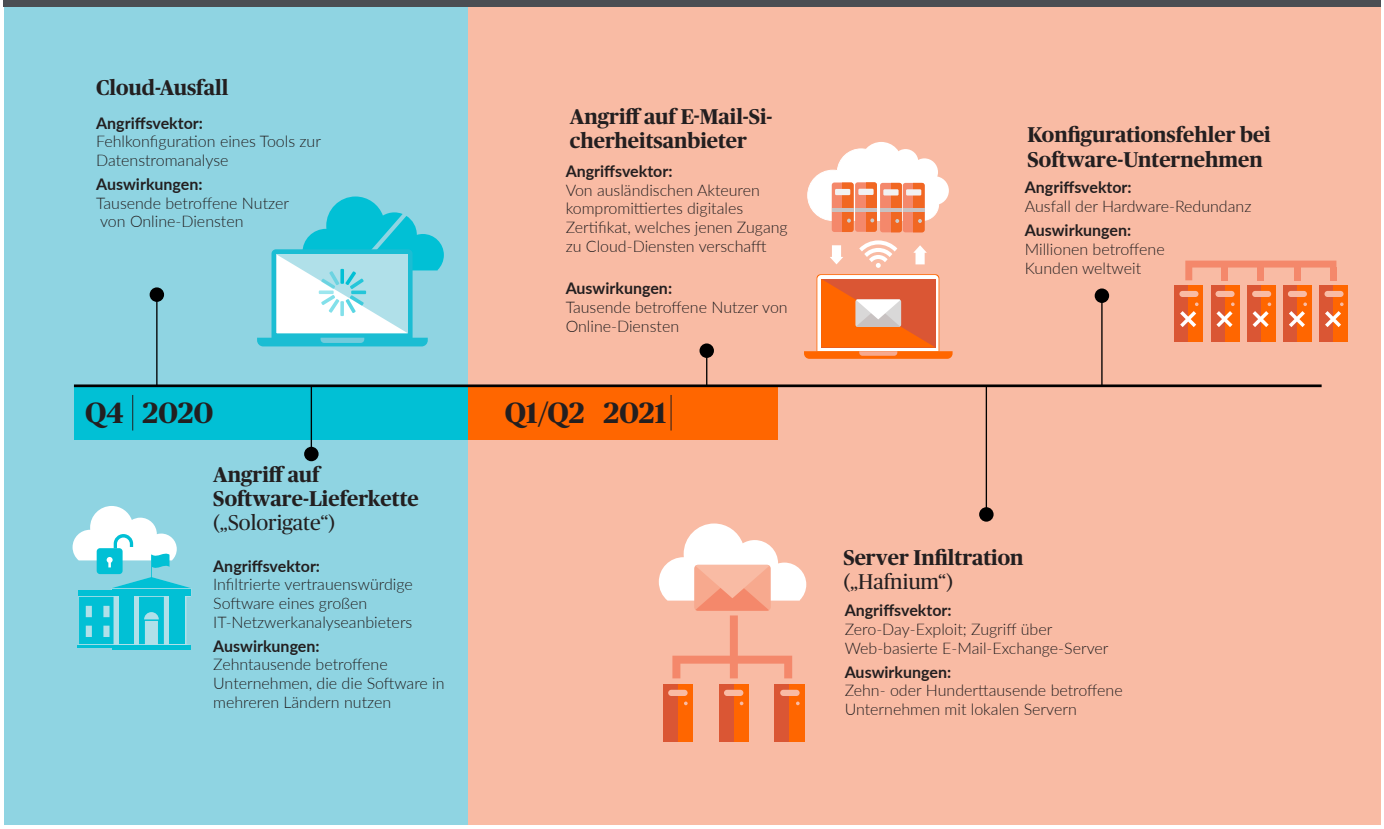
Heute bieten die Grunddeckungen (Incident Response-Kosten, Eigenschaden Cyberrisiken, Cyberhaftpflicht sowie Vermögensschadenhaftpflicht) Unternehmen aller Größen und Branchen wichtige Risikotransfer- und Risikomanagement-Lösungen. Darüber hinaus haben die von den Versicherern angebotenen Dienstleistungen im Bereich Cyber-Risikomanagement einen wertvollen Beitrag dazu geleistet, dass Unternehmen ihre Risiken minimieren und die technologische Abwehr am Front End verbessern konnten. Auch haben sich Incident Response-Teams bewährt, da sie Unternehmen dabei unterstützen, nach einem Cybervorfall schneller wieder online gehen zu können.

Die stetig steigende Zahl an Cyberversicherungen zeigt, dass viele Unternehmen inzwischen über eine Absicherung verfügen. Laut einem Bericht des Government Accountability Office von Mai 2021 beläuft sich die Zahl der Polizzen für in den USA ansässige sowie nicht in den USA ansässige Kompositversicherer auf geschätzt fast vier Millionen und entspricht damit nahezu 50 Prozent der in den Vereinigten Staaten versicherten Unternehmen. Dies bedeutet auch, dass die Aggregation des Cyberrisikos für die Versicherungsbranche wächst.

Gleichzeitig haben Unternehmen in den vergangenen Jahren ihre Widerstandsfähigkeit gegenüber Cyberangriffen verbessert. 2020 gaben 53 Prozent der IT- und Security-Fachkräfte an, dass ihre Organisationen bereits einen hohen Grad an Cyberresilienz erlangt hätten, 2015 waren es noch 35 Prozent gewesen.

Cyberversicherungen spielen beim Management von Cyberrisiken von Unternehmen sicherlich eine immer wichtigere Rolle, allerdings ist ungewiss, ob die Versicherer langfristig in der Lage sein werden, das gesamte Schadenpotenzial zu tragen.

Die Auswirkungen von Cybervorfällen werden immer drastischer



Zunehmende Risiken und Auswirkungen

In einem Zeitraum von 100 Tagen (Dezember 2020 bis März 2021) wurden bei mehreren Großangriffen Ziele kompromittiert, die von Software-Lieferketten- und E-Mail-Sicherheitsanbietern bis hin zu Hosting-Providern und kommunalen Infrastruktureinrichtungen reichten.

Zwar sind sich Unternehmen der Cyberrisiken und ihrer Implikationen bewusster geworden, doch nehmen Cybervorfälle und -bedrohungen immer weiter zu und auch neue Formen an.

Im Jahr 2020 wurden mehr als 18.000 neue Software-Schwachstellen gemeldet, nahezu dreimal so viele wie 2015 - und die Zahl steigt kontinuierlich. Bereits im Jahr 2020 wurden fast 1,2 Millionen neue Schadsoftware-Bedrohungen erkannt und damit mehr als doppelt so viele wie noch 2015. 2020 waren 85 Prozent der Sicherheitsvorfälle auf menschliche Interventionen wie Social Engineering zurückzuführen.

Aufgrund von Taktiken, wie dem Einsatz von Erpresser-Software (Ransomware), die inzwischen alltäglich und auch immer kostspieliger geworden sind, werden bei der Häufigkeit kompromittierter E-Mails und Datenverstöße in Unternehmen immer neue Höchststände erreicht, gerade auch in Zeiten der Corona-Pandemie und der hieraus resultierenden verbreiteten Home-Office-Vereinbarungen.

Auch die Auswirkungen von Cybervorfällen haben sich vergrößert: In einem Zeitraum von 100 Tagen (Dezember 2020 bis März 2021) wurden bei mehreren Großangriffen Ziele kompromittiert, die von Software-Lieferketten- und E-Mail-Sicherheitsanbietern bis hin zu Hosting-Providern und kommunalen Infrastruktureinrichtungen reichten. Weltweit waren mehr als 100.000 Organisationen betroffen.

Bei einem dieser Vorfälle („Solorigate“) wurde bei einem großangelegten Angriff auf die Lieferkette ein Schadcodeprogramm in ein Update einer vertrauenswürdigen Netzwerk-Analysesoftware integriert. Dieser Vorfall blieb fast acht Monate lang unbemerkt und betraf rund 20.000 Unternehmen und Behörden.

Bei einem anderen Angriff nutzte eine Gruppierung mutmaßlich nationalstaatlicher Akteure und krimineller Syndikate namens „Hafnium“ eine bis dahin unbekannte („Zero Day“)-Schwachstelle einer gängigen Software aus, um sich Zugriff auf firmeninterne Server von möglicherweise Hunderttausenden Unternehmen zu verschaffen.

Gravierende Vorfälle sorgen für erhöhte Anspannung

Wann wird es angesichts des sich entwickelnden großen Schadenpotenzials zu einem wirklich katastrophalen Cybervorfall kommen, der sowohl ein weitverbreitet als auch zerstörerisches Ausmaß hat?

So verbreitet und kostenintensiv die sogenannten Solorigate- und Hafnium-Angriffe auch waren, es hätte weitaus schlimmer kommen können. Offenbar dienten die Attacken vor allem Spionagezwecken. Wäre es jedoch darum gegangen, kritische Daten oder sonstige Informationen zu stehlen oder zu zerstören, wären die wirtschaftlichen Folgen um ein Vielfaches größer gewesen. Nach Aussage von Kevin Mandia, CEO der Cybersecurity-Firma FireEye, verfügten die Täter hinter der Solorigate-Attacke, so wie es auch das Intelligence Committee des US-Senats befand, über die erforderlichen Zugriffsmöglichkeiten und -fähigkeiten, um gravierenden Schaden anzurichten.

Zur weiteren Veranschaulichung: 2017 wurde beim NotPetya-Angriff ein Steuersoftware-Tool namens M.E.Doc ausgenutzt, das fast ausschließlich in der Ukraine verwendet wurde. Die Malware breitete sich dann allerdings unkontrolliert aus und richtete letztlich bei vielen in Europa, in den USA und anderenorts ansässigen Großunternehmen Schäden in Höhe von schätzungsweise 10 Milliarden US-Dollar an. Manche Unternehmen, die der NotPetya-Attacke zu Opfer fielen, erlitten Schäden in Höhe von mehr als 100 Millionen US-Dollar. Wäre diese Art zerstörerischen Schadcodes beim Solorigate- oder Hafnium-Angriff zum Einsatz gekommen, hätten die wirtschaftlichen Gesamtschäden insgesamt deutlich höher als bei der NotPetya-Attacke sein können.

Im selben Jahr waren weltweit mehr als 200.000 Computer vom WannaCry-Ransomware-Angriff betroffen. Glücklicherweise wurde eine bekannte Schwachstelle genutzt, für die es bereits einen Patch gab, sodass die meisten Nutzer schon immunisiert waren. Doch wie beim zuvor erwähnten Beispiel von Hafnium hätten die Auswirkungen hinsichtlich ihrer geografischen Reichweite viel größer und auch schwerwiegender sein können, wenn eine Zero Day-Schwachstelle ausgenutzt worden wäre.

Wir haben inzwischen weitverbreitete Ereignisse (wie Solorigate und Hafnium) und auch Angriffe von großer Zerstörungskraft (wie NotPetya und WannaCry) erlebt. Schäden aus diesen Ereignissen waren aber bisher handhabbar. Angesichts dessen stellt sich jedoch die Frage: Wann wird es angesichts des sich entwickelnden großen Schadenpotenzials zu einem wirklich katastrophalen Cybervorfall kommen, der sowohl ein weitverbreitetes als auch zerstörerisches Ausmaß hat?

Potenzielle Cyberkatastrophenrisiken

Die wachsende technologische Abhängigkeit der Unternehmen und Konsumenten sowie die Vernetzung von Technologien und Geschäftspartnern haben eine Umgebung geschaffen, in der Cyberrisiken exponentiell zunehmen können. Die folgenden Arten von Ereignissen können potenzielle Katastrophenereignisse sein, insbesondere wenn mehrere dieser Gegebenheiten zusammentreffen.

Bekannt gravierende Schwachstellen-Exploits:

Durchschnittlich werden jeden Tag rund 50 neue Software-Schwachstellen veröffentlicht. Wird hier nicht mit Patches reagiert, können diese Schwachstellen ausgenutzt werden. Etwa 15 Prozent von ihnen sind dahingehend gravierend, dass sie leicht kompromittiert und aus der Ferne mit nur geringen Zugriffsrechten angegriffen werden können. Der entstehende Schaden kann zudem erheblich sein. Da gravierende Schwachstellen größtenteils bekannt sind und mittels herkömmlichen Internet-Scan-Techniken in den Netzwerken der potentiellen Opfer detektiert werden können, sind Unternehmen, die nichts gegen solche massiven Software-Sicherheitslücken unternehmen, hochgradig gefährdet.

Zero Day Exploits:

Zero Day-Softwareschwachstellen sind Sicherheitslücken, die zunächst nur Cyberkriminellen bekannt sind. Sie geben besonderen Anlass zu Sorge, weil manche leicht zu kompromittieren und potenziell gravierend sind und darüber hinaus oftmals nicht abgesichert sind. Mit anderen Worten können auch Unternehmen, die über ein gutes Risikomanagement-Programm ihrer Cyberrisiken verfügen, Zielscheibe von Zero Day-Angriffen werden.

Software-Lieferketten Exploits:

Bei Software-Lieferkettenangriffen handelt es sich im Grunde um Trojaner, mit denen Täter über eine vertrauenswürdige, zertifizierte Software in Systeme eindringen können. Die Solorigate-Attacke wies einen hohen Grad an Raffinesse seitens der Angreifer auf, die sich bei ihrer Kompromittierung in der Technologiebranche allgemein übliche Software-Ausbreitungspraktiken zunutze machten. Es wird davon ausgegangen, dass sich diese Attacken, die oftmals auf Anordnung von staatlichen Akteuren oder mit deren Unterstützung zu erfolgen scheinen, fortsetzen und vielleicht auch noch häufen werden. Geopolitische Spannungen, vor allem zwischen dem Westen und dessen Gegnern, könnten die Bedrohung durch solche Ereignisse künftig weiter verschärfen.

Ausfälle kritischer Infrastruktur:

Cyberangriffe und andere Cybervorfälle, die auf kritische Infrastrukturen abzielen, können weitreichende Konsequenzen haben. So gelang es beispielsweise ausländischen Cyberkriminellen im Mai 2021 beim Angriff auf Colonial Pipeline, einem Unternehmen, das die Ostküste der USA mit Benzin versorgt, mittels einer Ransomware-Attacke die Infrastruktur zu unterbrechen – mit massiven Folgen: Die Pipeline musste mehrere Tage stillgelegt werden, sodass es in mehreren Bundesstaaten zu einer Kraftstoffverknappung für Millionen von Bürgerinnen und Bürgern sowie Unternehmen kam. Insgesamt waren 45 Prozent der Benzinversorgung der USA betroffen. Das Ausfallrisiko im Infrastrukturbereich ist seiner Art nach einzigartig, da es nicht nur aus Cyberattacken resultiert, sondern auch aus Systemfehlern, menschlichem Fehlverhalten, Programmierfehlern und nicht zuletzt auch nicht-böswilligen Cybervorfällen.

Sonstige weitverbreitete Ereignisse:

Bestimmte Arten von Cyberattacken, die gegen eine große Anzahl von Opfern gerichtet sind, können gleichzeitig oder automatisiert erfolgen. Das Internet sowie einige Telekommunikationsdienste sind für die Gesellschaft mittlerweile zu kritischen Infrastrukturen geworden, sodass das potenzielle Risiko eines Ausfalls ein gewaltiges Ausmaß angenommen hat. Vereinzelt können Telefongesellschaften der einzige Anbieter in einer großen oder mittelgroßen Stadt sein oder die Dienste einiger großer Cloudcomputing-Unternehmen werden so stark genutzt, dass ein flächendeckender Ausfall zeitgleich den Geschäftsbetrieb von Tausenden oder gar Millionen Unternehmen beeinträchtigen würde. Angriffe, die massenhaft stattfinden können, haben das Potenzial, Cyberkatastrophen auszulösen.

Ransomware-Angriffe:

Ransomware-Angriffe, bei denen elektronische Dateien oder Informationen der angegriffenen Organisationen oder Privatpersonen so lange in Besitz genommen werden, bis eine Lösegeldzahlung erfolgt, sind nicht zwangsläufig Katastrophenereignisse, werden aber inzwischen hoch professionell durchgeführt. Die Lösegeldforderungen, die sich früher auf einige Tausend US-Dollar beliefen, haben mittlerweile astronomische zweistellige Millionenbeträge erreicht, und die Täter nehmen inzwischen Organisationen jeder Größe ins Visier.

Stärkung der Cyberresilienz

Für Firmen und Organisationen kommt es mehr denn je darauf an, noch besser für eine Cyber-Katastrophe gerüstet zu sein.

Angesichts der zunehmenden Cyberrisiken (direkte Zunahme aufgrund der Art der Geschäftstätigkeit oder IT-Umgebung; indirekte Zunahme wegen des Ausfalls verbreitet genutzter Infrastrukturen oder weil sich Kriminelle Schwachstellen zunutze machen) kommt es für Firmen und Organisationen mehr denn je darauf an, noch besser für eine Cyberkatastrophe gerüstet zu sein.

Ein guter Ausgangspunkt ist es, sich zunächst einen Überblick über die spezifischen Risiken einer Organisation im Hinblick auf die in diesem Whitepaper erläuterten Cyberkatastrophenrisiken zu verschaffen und dann die erforderlichen Ressourcen für die Verbesserung der Cyberabwehr und -resilienz bereitzustellen. Da IT-Anbieter, deren Dienste von vielen auf Shared-Basis in Anspruch genommen werden, ein erhebliches systemisches Risiko darstellen, müssen Organisationen umfassende Due Diligence-Prüfungen für diese Anbieter durchführen und um diese herum eine Redundanz und Resilienz aufbauen. Darüber hinaus müssen Verträge hinsichtlich der Haftungsfreistellung geprüft werden, um zu beurteilen, wie das Risiko übertragen wird.

Außerdem sollten Organisationen die angebotene Expertise ihrer Versicherungsmakler und Cyberversicherer vollumfassend nutzen. Auch wenn die IT-, Risikomanagement- und Geschäftskontinuitätsteams voll und ganz auf ihre Cybersicherheits- und Incident Response-Maßnahmen vertrauen, ist dennoch kein Unternehmen in der Lage, sich zu 100 Prozent und gegen jegliche Cybervorfälle abzusichern – erst recht nicht gegen katastrophale Vorfälle.

Viele Versicherungsträger bieten verschiedene Pre-Incident-Dienstleistungen an, um Unternehmen bei der Stärkung ihre Cyberabwehr zu unterstützen. Hierzu zählen die Beurteilung der Reaktionsfähigkeit, Benchmarkings der Sicherheitsarchitektur, Vulnerabilitätstests der Netzwerke und allgemeine Angriffssimulationen. Unternehmen sollten auch auf den Eintritt eines Cybervorfalls vorbereitet sein. Ein Incident Response-Expertenteam kann dabei helfen, den durch solche Ereignisse angerichteten Schaden einzudämmen und den Geschäftsbetrieb schnellstmöglich wieder in vollem Umfang aufzunehmen. Diese Dienstleistungen können entscheidend sein, ob ein Cybergroßereignis gerade noch „irgendwie durchgestanden“ wird oder ob Unternehmen einem solchen Vorfall mit Zuversicht entgegenblicken können.

Entwicklung neuer Lösungen

Die Cyber-Versicherung ist wie die Sachversicherung dem Risiko von Katastrophenereignissen ausgesetzt

Aus globaler Sicht haben katastrophale Cyberangriffe das Potenzial, den weltweiten Handel zum Erliegen zu bringen und kritische Infrastrukturen auszuschalten. Ähnlich wie bei der Coronavirus-Pandemie erfordert dies, dass Regierung und Privatsektor bei wichtigen Themen zusammenarbeiten, zum Beispiel bei der Offenlegung und Meldung von Cybervorfällen, um die Kohärenz der Daten zu verbessern. Dies gilt auch im Hinblick auf die Schaffung rechtlicher Rahmenbedingungen zur Abschreckung und Bestrafung von Cyberkriminellen.

Die Häufigkeit und Schwere von Cybervorfällen veranlasst die Versicherer dazu, ihre Preise und Bedingungen neu auszuloten. Einen robusten Markt für Cyberversicherungen anbieten zu können und dabei auch das potenzielle Ausmaß von Katastrophen-Risiken zu berücksichtigen, erfordert neue Lösungen wie etwa eine Partnerschaft mit der Regierung sowie die Anpassung des Produktangebotes der Versicherer. Für die Versicherungsbranche besteht die Herausforderung darin, Deckungen zu erstellen, die Sicherheit und ein hohes Maß an Schutz bieten und dabei sowohl das Management von Standard- als auch von Cyberkatastrophenereignissen für Kunden und Versicherer zu vereinfachen.

Traditionell haben Versicherer Katastrophenereignisse wie Überschwemmungen und Erdbeben als separate Deckungsbestandteile in ihre Sachversicherungen aufgenommen, um diese Risiken preislich transparent ausweisen und überwachen zu können. Dies hat dazu beigetragen, die Marktstabilität aufrechtzuerhalten und Verfügbarkeit von Deckungen zu gewährleisten. So waren zum Beispiel viele der großen Erdbeben, Überschwemmungen und Hurrikane der letzten 50 Jahre gravierende finanzielle Ereignisse für die Sach- und Haftpflichtversicherer, haben aber selten zu Insolvenzen von Versicherungsträgern geführt. Als Folge dessen blieb die Versicherungsbranche zum Vorteil der Versicherungsnehmer widerstandsfähig und stabil, auch nach dem Eintritt von Katastrophenereignissen.

Die Cyberversicherung ist wie die Sachversicherung dem Risiko von Katastrophenereignissen ausgesetzt, und daher muss die Cyberversicherungsbranche möglicherweise genauso reagieren wie die Sachversicherungsbranche. Die Industrie muss proaktiv vorgehen und die Deckung für Katastrophenereignisse getrennt von den Grunddeckungen anbieten. Die Deckung für Katastrophenereignisse würde nicht ausgeschlossen, sondern klarer abgegrenzt werden, um sicherzustellen, dass die Preise für die separate Deckung transparent sind und angemessene Zeichnungsrichtlinien, Deckungsgrenzen und Selbstbehalte der Kunden gelten. Dieser Ansatz wird es der Cyberversicherungsbranche ermöglichen, weiterhin innovative Lösungen für Versicherungsnehmer anzubieten und gleichzeitig die Nachhaltigkeit des Marktes zu gewährleisten.

Über den Autor

Michael Kessler ist Vice President der Chubb Group und Division President der Global Cyber Risk Practice von Chubb. Seine Funktion beinhaltet sämtliche geschäftlichen Aspekte wie die Strategie, die Produkt- und Geschäftsentwicklung, das Underwriting- und Dienstleistungsgeschäft, nebst der gesamten Gewinnentwicklung. Michael Kessler verfügt über fast 30 Jahre Erfahrung in der Versicherungsbranche und in der aktuariellen Beratung. Zuvor war er bei Chubb Chief Reinsurance Officer und Chief Actuary für die internationale Industrieversicherung. Er verfügt über den Abschluss eines Bachelor of Arts in Mathematik der Cornell University und ist Mitglied der American Academy of Actuaries und Fellow der Casualty Actuarial Society.

Verweise

1. Cyber Resilient Organization Report (2020). Quelle: https://www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/.
2. National Vulnerability Database des National Institute of Standards and Technology der USA. Website://nvd.nist.gov/vuln/search.
3. AV-TEST Institute (2021). Website: https://www.av-test.org/en/statistics/malware/.
4. Verizon 2021 Data Breach Investigations Report (2021). Quelle: https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf.
5. Select Committee on Intelligence des US-amerikanischen Senats (2021). Website: https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.
6. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Quelle: https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf.

Über Chubb

Chubb ist der größte börsennotierte Industrieversicherer der Welt. Mit eigenen Niederlassungen in 54 Ländern bietet Chubb Industrie- und Personenversicherungen für einen vielfältigen Kundenkreis. Als Underwriting-Unternehmen erfolgen Bewertung, Übernahme und Management von Risiken mit fachlichem Verständnis und Disziplin. Die Regulierung der Schadenfälle erfolgt fair und unverzüglich. Das Unternehmen zeichnet sich durch ein breitgefächertes Produkt- und Serviceangebot, umfassende Vertriebskapazitäten, eine außerordentliche Finanzstärke sowie weltweite Niederlassungen aus. Die Muttergesellschaft Chubb Limited ist an der New York Stock Exchange notiert (NYSE: CB) und Bestandteil des Aktienindex S&P 500. Chubb verfügt über Direktionsbüros in Zürich, New York, London und Paris sowie an anderen Standorten und beschäftigt weltweit rund 31.000 Mitarbeiterinnen und Mitarbeiter. Weitere Informationen auf www.chubb.com/at.

Nähere Informationen über Chubbs branchenführende Erfahrung und Expertise im Management von Cyberrisiken erhalten Sie:

Chubb European Group SE, Direktion für Österreich, Kärntner Ring 5-7, 1010 Wien
Telefon: +43 1 710 9355-0 | Fax: +43 1 710 9520 | E-Mail: InfoAT@chubb.com

Chubb. Insured.℠

AT0427-MD 06/2022