Systemische Cyber-risiken/Produkt-Update:

FAQ für Makler

CHUBB®

Chubb ist bestrebt, auch künftig entscheidenden Marktgestaltungseinfluss im Bereich der Cyberversicherung auszuüben, indem wir Wege gehen und Strukturen verankern, die uns eine langfristig nachhaltige Entwicklung ermöglichen.

Aufgrund der Häufigkeit und Schwere der Cybervorfälle der jüngsten Vergangenheit sehen sich viele Versicherer, unter ihnen auch Chubb, veranlasst, ihre bisherigen Tarife und Bedingungen zu prüfen. In den vergangenen Monaten wurden bei verschiedenen Cybervorfällen Ziele wie Software-Lieferketten- und E-Mail-Security-Anbieter bis hin zu Datenserver und kritische Infrastrukturen angegriffen. Zudem waren Cyber-Angriffsarten festzustellen, die ohne Weiteres zu Katastrophenereignissen hätten führen können.

Um solche Risiken bewältigen zu können, arbeitet Chubb derzeit an neuen und innovativen Lösungen. Chubb wird seinen Versicherungsnehmern und Vertriebspartnern auch künftig die ihnen bereits bekannten und vertrauten Cyber-Grunddeckungen anbieten, jedoch auch die Bedingungen für die Absicherung von Großereignissen neugestalten.

Außerdem wird Chubb in verschiedener Hinsicht Partnerschaften mit Branchenverbänden und Regierungen eingehen, mit dem Ziel, allen Beteiligten mehr Gewissheit und eine bessere Orientierung in Bezug auf Deckungsschutzvereinbarungen geben zu können.

Auswirkungen für Cyber-Makler und-Versicherungs-nehmer

Wir sind uns sicher, dass die neuen Lösungen den Vertriebspartnern von Chubb auf längere Sicht mehr Stabilität und Wachstumschancen auf dem Cyber-Versicherungsmarkt bieten werden. Makler werden künftig die Möglichkeiten haben den Umfang des verfügbaren Deckungsschutzes für systemische Risiken präziser darzustellen, maßgeschneiderte Bedingungen für kundenspezifische Risiken zu gestalten und die jeweiligen Deckungen durch Schadeneindämmungs- und Risikoberatungsdienstleistungen aufzuwerten. Chubbs neuer Ansatz wird auf Konzepten aufbauen, die Maklern und Kunden, die sich mit Sachversicherungen und Katastrophen-Sachversicherungen auskennen, bereits größtenteils bekannt sein dürften. Durch die strukturierte Vorgehensweise bei der Quantifizierung von Katastrophen-Cyberrisiken sollten künftig zusätzliche Cyber-Versicherungskapazitäten am Markt verfügbar sein.

Der Markt für Cyberrisiken

Welche Motivation steht hinter den derzeitigen strategischen Veränderungen bei der Cyber-Versicherung?

Cybervorfälle und -bedrohungen nehmen hinsichtlich ihrer Häufigkeit und Schwere zu und auch immer neue Formen an. 2020 wurden mehr als 18.000 neue Software-Schwachstellen gemeldet, fast dreimal so viele wie noch 2015, und ihre Zahl steigt kontinuierlich weiter.[1] Im Jahr 2020 wurden bereits nahezu 1,2 Mio. neue Malware-Bedrohungen erkannt, mehr als doppelt so viele wie 2015.[2] Während Taktiken wie der Einsatz von Erpresser-Software (Ransomware) inzwischen Gang und Gäbe und überaus kostspielig geworden sind, sind, was die Häufigkeit von Cybervorfällen anbelangt, kompromittierte E-Mails und Datenverstöße in Unternehmen die Bereiche, in denen immer neue Höchststände erreicht werden, beispielsweise aufgrund von getroffenen Homeoffice-Regelungen. Diese immer häufigeren und gravierenderen Cyberereignisse belasten die Basisschadenquote der Versicherer, während systemische Risiken mit Katastrophenpotenzial immer weiter zunehmen.

Teilen andere Unternehmen die von Chubb im Hinblick auf systemische Cyberrisiken vertretenen Standpunkte?

Ja, wir gehen davon aus, dass das Ausmaß und die Dringlichkeit des Themas auch von anderen Unternehmen, sowie von Regierungen, Aufsichtsbehörden und Ratingagenturen erkannt wurden. 2020 setzte der US-amerikanische Kongress die Cyberspace Solarium Commission unter dem Vorsitz von Senator Angus King (I-ME) und des Abgeordneten Mike Gallagher (R-WI) ein. Nach einer einjährigen Untersuchung kam die Kommission zu dem Schluss, dass für die USA ein Cyber-Katastrophenrisiko besteht und das Land „im Hinblick auf Cyberereignisse hochgradig gefährdet ist".[3]

In Europa wurde vor mehr als 15 Jahren die Agentur der Europäischen Union für Cybersicherheit (ENISA) eigens zur Lösung des Problems der steigenden Zahl schwerwiegender Cybervorfälle eingerichtet, mit denen sich der öffentliche und private Sektor konfrontiert sahen. In dem neuen im April 2021 veröffentlichten Bericht der ENISA wird darauf hingewiesen, dass Unternehmen angesichts der aktuellen Cybersicherheitsbedrohungen ihr weltweites Cybersecurity-Personal um 89 % aufstocken müssen, um ihre kritische Informations- und Kommunikationstechnologie effektiv schützen zu können. In Anbetracht der kritischen Lage haben die Regierungen verschiedener Länder inzwischen entsprechende Programme und Richtlinien verabschiedet.

Der britische Verteidigungsminister Ben Wallace kündigte im Oktober 2021 an, dass in Großbritannien ein neues Zentrum für digitale Kriegsführung eingerichtet würde, um Cyberangriffe künftig besser abwehren zu können.

Die Versicherungsratingagentur AM Best sprach im Juni 2021 von „trüben Aussichten für den Cyberversicherungsmarkt" und wies auf die „weitreichenden Auswirkungen des Dominoeffekts von Cyberrisiken und fehlenden geografischen und kommerziellen Grenzen" hin. Sie kam zu dem Schluss, dass sich Versicherer „mit einem im Cyberbereich defizitären Risikomanagementansatz mit einem Kumulrisiko konfrontiert sehen könnten, das über ihre Risikotoleranz hinausgeht, und unter Ratingdruck geraten könnten."[4]

Stellungnahmen anderer Organisationen zum Thema finden Sie unter folgenden Links:

- Durchführungsverordnung zur Erhöhung der nationalen Cybersicherheit der US-Regierung: www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Cyber-Versicherungen: Versicherer und Polizzeninhaber sehen sich angesichts der Veränderungen am Markt mit Problemen konfrontiert (US-Rechnungshof): www.gao.gov/products/gao-21-477
- Möglicher Preisanstieg um 50 % bei Cyberversicherungen in 2021 (MarshMcLennan Agency): www.marshmma.com/blog/cyber-insurance-rates-could-rise-50-in-2021
- Ausgleich von Chancen und Risiken durch bessere Entscheidungen (Aon): www.aon.com/2021-cyber-security-risk-report/

Wie sieht die Strategie von Chubb im Branchenvergleich aus?

In der Cyber-Versicherungsbranche gilt das Hauptaugenmerk den Teilbereichen Ransomware und Adäquatheit der Preise. Das sind Themen, die mit einer Verringerung der Kapazitäten, Preiserhöhungen und branchen- bzw. deckungsspezifischen Underwriting-Anpassungen angegangen werden. Wenngleich Chubb hier ähnliche Maßnahmen ergreift, verfügen wir doch über den Vorteil jahrzehntelanger Erfahrung und eines deutlich größeren Geschäftsvolumens, sodass wir uns auf die Gesamtperspektive systemischer Risiken konzentrieren können. Auch wenn von anderen Unternehmen viel über dieses für unsere Branche so wichtige Erfordernis zu hören war, sind dort bisher kaum Maßnahmen erfolgt. Chubb wird hier künftig eine Vorreiterrolle einnehmen.

Wird es möglich sein, das Risiko von Cyberkatastrophen durch moderne Cyber-Underwritingverfahren zu begrenzen?

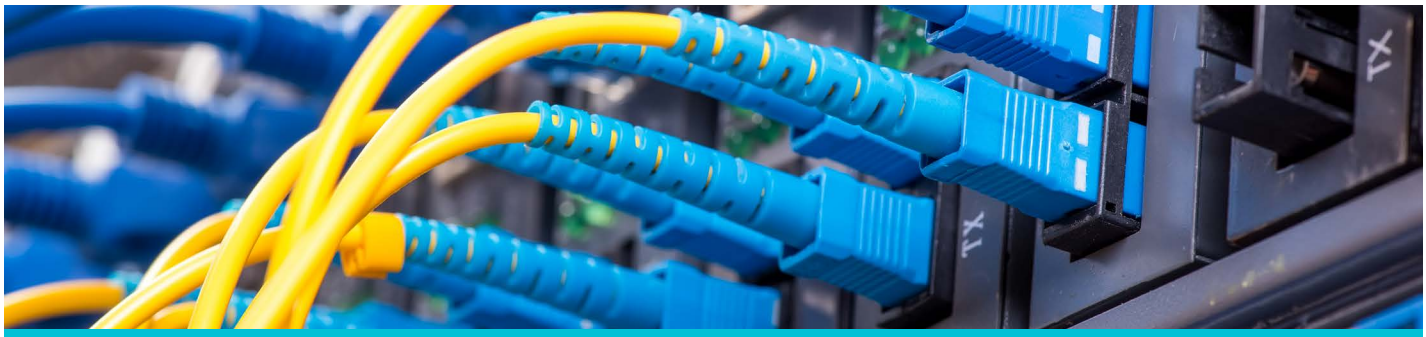
Chubb verfügt über ein spezialisiertes Cyberrisk-Engineering- und Underwriting-Team und integriert zurzeit neue Bedrohungsanalyse- und Künstliche Intelligenz-Tools in seine Underwriting-Prozesse. Darüber hinaus bieten wir unseren Cyber-Versicherungsnehmern Zugang zu unserem umfassenden Angebot an Schadenpräventions- und Schadenminderungsdienstleistungen. Dank unserer proaktiven Investitionen in diesen Bereichen hat Chubb im Underwriting bessere Ergebnisse erzielt als die Cyberversicherungsbranche in ihrer Gesamtheit.[5] Doch trotz der hohen Investitionen gelingt es Cyberkriminiellen oftmals, Cyberbedrohungen so zu gestalten, dass interne Kontrollen und Best Practices umgangen werden können. Underwriting- und Schadenpräventionskontrollen bieten keinen 100%-igen Schutz vor dem Risiko einer Cyberkatastrophe.

Was versteht man unter einem systemischen Cyberrisiko und wie ist der Begriff bei Chubb definiert?

„Systemisch" ist für uns ein Risiko, das aufgrund von Gemeinsamkeiten oder gemeinschaftlich genutzten Risikoelementen das Potenzial hat, bei vielen Kunden Schaden anzurichten. „Katastrophen"-Risiken dagegen sind systemische Risiken, die bei einer Vielzahl an Versicherungsnehmern effektiv gravierende oder große Schäden verursachen.

Welche neuen Cyber-Katastrophenrisiken sind in den letzten Jahren hinzugekommen?

Die immer größere Abhängigkeit der Unternehmen und Verbraucher von Technologien unddie Vernetzbarkeit von Technologien und Partnern haben ein Umfeld geschaffen, in dem Cyberrisiken exponentiell wachsen können. Darüber hinaus haben Cybervorfälle inzwischen viel weitreichendere Auswirkungen als früher. 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 Datenservern und kritischen Infrastrukturen reichten. Insgesamt waren mehr als 100.000 Unternehmen weltweit von Vorfällen dieser Art betroffen, die nicht nur finanzielle Schäden verursachten, sondern auch zu Serviceunterbrechungen für Millionen von Kunden und Bürgern führten. So waren z. B. vom Solorigate-Angriff auf eine Software-Lieferkette, bei dem ein Schadcode in das Update einer bisher verlässlichen Netzwerkanalyse-Software integriert wurde, 20.000 Unternehmen und Behörden betroffen. Viel schlimmer wäre es gekommen, wenn der Diebstahl oder die Zerstörung kritischer Daten oder sonstiger Informationen beabsichtigt gewesen wären.



Folgende Arten von Risiken und v. a. Kombinationen dieser Risiken wurden als potenzielle Verursacher von Katastrophenereignissen eingestuft:

Bekannte schwere Sicherheitslücken:
Bekannte Software-Schwachstellen, die nicht gepatcht werden, können schwerwiegende Folgen haben, da sie leicht und mit nur geringen Zugriffsrechten aus der Ferne kompromittiert werden können und gravierende Schäden anrichten können.[6]

Schwerwiegende Zero-Day-Schwachstellenausnutzung:
Bestimmte Software-Schwachstellen, die meist nur Cyberkriminelle kennen, können leicht ausgenutzt werden, gravierende Folgen haben und sind häufig nicht ausreichend gesichert.

Software-Lieferketten-Ausnutzung:
Bei diesen Angriffen handelt es sich im Grunde um Trojaner, mit denen Täter über eine vertrauenswürdige, zertifizierte Software in Systeme eindringen können.

Ausfälle kritischer Infrastruktur:
Für die Gesellschaft wichtige Infrastrukturen wie Stromnetze und Telekommunikationsdienste sind hochgradig ausfallgefährdet, sei es durch Cyberattacken oder nicht böswillige Cyberereignisse, darunter Systemausfälle, menschliches Versagen und Programmierfehler. Im Frühjahr 2021 wurde beim Ransomware-Angriff auf Colonial Pipeline, einem Unternehmen, das die Ostküste der USA mit Benzin versorgt, die Infrastruktur in einer Weise beeinträchtigt, so dass für Millionen von Bürgern und Unternehmen in mehreren Bundesstaaten keine ausreichende Kraftstoffversorgung mehr gewährleistet war.

Alle anderen weitverbreiteten Ereignisse:
Bestimmte Arten von Cyberattacken können zeitgleich oder automatisch eine Vielzahl an Opfern treffen und so zu einem Cyber-Katastrophenereignis werden. Das Internet und verschiedene Telekommunikationsdienste sind für die Gesellschaft zu kritischen Infrastrukturen geworden, aber auch die Dienste mancher Cloudcomputing-Großunternehmen werden inzwischen so verbreitet genutzt, dass ihr Ausfall Auswirkungen auf den Geschäftsbetrieb Tausender, wenn nicht Millionen, von Unternehmen haben kann.

Ransomware-Vorfälle:
Ransomware-Angriffe, auch nicht-systemische, bei denen die angegriffenen Firmen und Privatpersonen so lange nicht mehr auf ihre elektronischen Dateien und Informationen zugreifen können, bis eine Lösegeldzahlung erfolgt, werden inzwischen hoch professionell durchgeführt und die verlangten Beträge steigen immer weiter. Angriffe mit dem Ziel, Schaden anzurichten, können als Ransomware getarnt sein, so wie es bei „NotPetya“ und „WannaCry“ der Fall war.

Chubbs Cyber-Versicherungsangebot

Ransomware ist seit Jahren ein großes Thema am Cyberversicherungsmarkt. Hat sich Chubbs Einstellung hierzu im Laufe der Zeit geändert?

Schon seit mehreren Jahren analysieren wir die Entwicklungen im Bereich Ransomware. So, wie sich hier neue Entwicklungen gezeigt haben, wurden auch unsere Underwriting-Strategien angepasst. Um Risiken besser steuern zu können, haben wir unsere Underwriting-Strategie dahingehend geändert, dass wir u. a. bestimmte Branchen und Unternehmen meiden, die nicht über entsprechende Kontrollmechanismen verfügen, und haben Anpassungen in Bezug auf Selbstbehalte, Sublimits und Mitversicherungen vorgenommen. Darüber hinaus kommt bei Chubb für Risiken dieser Art ein gewichtetes Underwriting zum Einsatz, d. h. wir analysieren gewichtete Faktoren, die aus verschiedenen internen und externen Quellen stammen, um die Risikofaktoren unserer Bestands- und Neukunden besser identifizieren zu können. Chubbs neue Cyber-Produktangebote werden sogar noch mehr Optionen für die Gestaltung vertragsübergreifender Sublimits, Mitversicherungen und Selbstbehalte für Ransomware-Vorfälle umfassen.

Wie viele systemische Cyberrisiko-Schäden wurden Chubb bisher gemeldet?

Bei Chubb sind in den vergangenen Monaten Hunderte Cyber-Schadenmeldungen im Zusammenhang mit verbreitet eingetretenen Cyber-Großereignissen eingegangen.

Warum sehen wir immer noch so viele Veränderungen am Cybermarkt? Hat die Versicherungsbranche in anderen Sparten ähnliche Umwälzungen erlebt?

Cyberversicherungen als eigenständiges Segment haben erst in den letzten Jahren ihren Reifegrad erlangt und sind nach wie vor eine stark veränderliche Sparte. Gleichzeitig sind die Risiken, die hier versichert werden, dynamisch und steigen hinsichtlich ihrer Komplexität und Schwere rasant. Auf dem Sachversicherungsmarkt hat es infolge plötzlich eingetretener Ereignisse schon immer Schocks von unvorhergesehenem Ausmaß gegeben, so z. B. 1906 beim Erdbeben von San Francisco und bei den Terroranschlägen am 11. September 2001. Hier wurden erst im Nachhinein Lösungen entwickelt, die für mehr Klarheit in Bezug auf die benannten Gefahren und für die Verfügbarkeit separater Deckungen für Katastrophenrisiken gesorgt haben. Cyberversicherungen geben uns die Möglichkeit, schon jetzt an der Produktgestaltung zu arbeiten und auch in Kooperation mit Regierungen Lösungen zu konzipieren, die dem Versicherungsmarkt Stabilität und Kunden Deckungssicherheit bieten.

Wird Chubb künftig dieselben Cyber-Deckungen wie bisher anbieten?

Die bisherigen Grunddeckungen (Incident Response-Kosten, Eigenschaden-Cyberrisiken, Cyber- und Berufshaftpflicht) werden auch weiterhin verfügbar sein. Chubb wird darüber hinaus eine Unterscheidung zwischen Ereignissen mit begrenzten Auswirkungen und weitverbreiteten Ereignissen treffen. Wir haben ausgewertet, dass 90 % der historischen Schäden in die Kategorie Ereignisse mit begrenzten Auswirkungen gehören.

Chubb wird auch als Erweiterung des Cyber-Hauptversicherungsprodukts in einer strukturierteren und nachhaltigeren Weise zusätzliche Deckungen für systemische Risiken mit weitreichenden Auswirkungen und Katastrophenpotenzial anbieten. In ihrer Gesamtheit werden diese unter den Begriff Deckungen für Weitverbreitete Ereignisse fallen und die jeweiligen in der Polizze aufgeführten Einzelkomponenten beinhalten. Für weitverbreitete Ereignisse und ihre jeweiligen Bestandteile werden spezifische Sublimits, Selbstbehalte und Mitversicherungssummen gelten. Auf ähnliche Weise wird schon seit mehr als hundert Jahren bei Sachversicherungen verfahren, um Katastrophenrisiken wie Überschwemmungen und Erdbeben bewältigen zu können.

Underwriting-Prozess

Von welchen Arten von Deckungserweiterungen kann ausgegangen werden?

Chubb hat bereits zahlreiche Verbesserungen in den aktuellen Bedingungen aufgenommen, dazu gehören Erweiterungen, wie z. B. für behördliche Bußen (soweit gesetzlich zulässig), Kartenzahlungsschäden, Cyber-Kriminalität, präventive Systemabschaltungen und vieles Weitere. Chubb wird darüber hinaus Deckungsbausteine anbieten, die weitverbreitete Ereignisse wie Software-Lieferketten-Ausnutzung, schwerwiegende Zero-Day-Schwachstellenausnutzung und bekannte schwere Sicherheitslücken umfassen. In der Grafik links sind die Deckungsbestandteile im Einzelnen aufgelistet. Für Kunden und Interessenten gilt es, gemeinsam mit ihren Maklern die spezifischen Cyber-Risiken zu ermitteln, die sich aus ihrer Geschäftstätigkeit und IT-Umgebung ergeben könnten, und sodann die für sie geeignetsten Deckungserweiterungen auszuwählen.

Wird es bei Chubb preisliche Veränderungen für die Cyberversicherungen geben?

Wir werden bei der Preisgestaltung auch künftig die spezifischen Bedürfnisse und das Risikoprofil des einzelnen Kunden berücksichtigen. Wo für die Ausstellung von Lokalpolizzen eine staatliche Genehmigung vorliegen muss, werden die jeweils aktuellen Tarife hinterlegt. Hier werden wir uns beim Underwriting und der Preisgestaltung auf von staatlicher Seite genehmigte Tarife stützen.

Ab wann gelten die Produktänderungen?

Wir haben die neue Vorgehensweise bereits bei Großkunden von Chubb angewendet und werden diese ab Juni 2022 auf andere Marktsegmente ausweiten. Ganz entscheidend ist es, dass Sie vor einer Vertragsverlängerung gemeinsam mit den Risikomanagern Ihrer Kunden deren spezifische Risiken ermitteln und die Deckungserweiterungen prüfen, die ihnen einen adäquaten Schutz bieten können. Die Umsetzung der neuen Verfahrensweise für Lokalpolizzen wird sich nach den jeweiligen Regionen und länderspezifischen Zulassungen richten.

Wird es ein Factsheet geben, in dem die Vorteile erläutert sind und das wir dem Angebot beifügen können?

Ja, es gibt eine Produktübersicht, die als Download verfügbar ist.

Wie kann ich mich auf die Änderungen vorbereiten? Wird es Ressourcen geben, die mir bei Gesprächen mit Bestands- und Neukunden als Orientierungshilfe dienen?

Außer der sorgfältigen Lektüre dieser FAQ, empfehlen wir Ihnen die Teilnahme an allen von Chubb künftig angebotenen Schulungen und Webinaren. Es wird auch entsprechendes Infomaterial, wie u. a. Whitepaper, Webinare und Videos, für Ihre Versicherungsnehmer zur Verfügung stehen. Nähere Informationen hierzu erhalten Sie auf unserer Webseite chubb.com/at oder von Ihrem Chubb Cyber- Underwriter.

Angebots-prozess

Gibt es bestimmte Underwriting-Aspekte, die im Hinblick auf Chubbs systemischen Deckungsschutz und die angebotenen Tarife zu berücksichtigen sind?

Ja. In Chubbs systemischen Deckungsschutz und die Preisgestaltung fließen mehrere Faktoren ein, so u. a. die kritischen Abhängigkeiten eines Unternehmens, Vertragsschutz in Bezug auf Dienstleister, Cybersecurity-Hygiene und -kontrollen sowie die Incident Response/Resilienzplanung und die entsprechenden Tests.

Inwiefern wird sich die Preisstruktur der Deckungen weitverbreiteter Ereignisse ändern?

Chubb ist bestrebt, allen Kunden ein Höchstmaß an Transparenz zu bieten und wird ihnen künftig separate Tarif-, Versicherungssummen- und Selbstbehaltsoptionen für systemische Deckungen anbieten.

Polizzen-formular

Welche Deckungen sind in den neuen Cyberprodukten von Chubb nicht enthalten?

Der Deckungsschutz für weitverbreitete Ereignisse wird nicht ausgeschlossen. Er wird so gestaltet, dass er die Kapazitäten für die versicherten Ereignisse transparent ausweist. Und der Versicherte ist auch nicht verpflichtet, den Deckungsschutz für weitverbreitete Ereignisse abzuschließen.

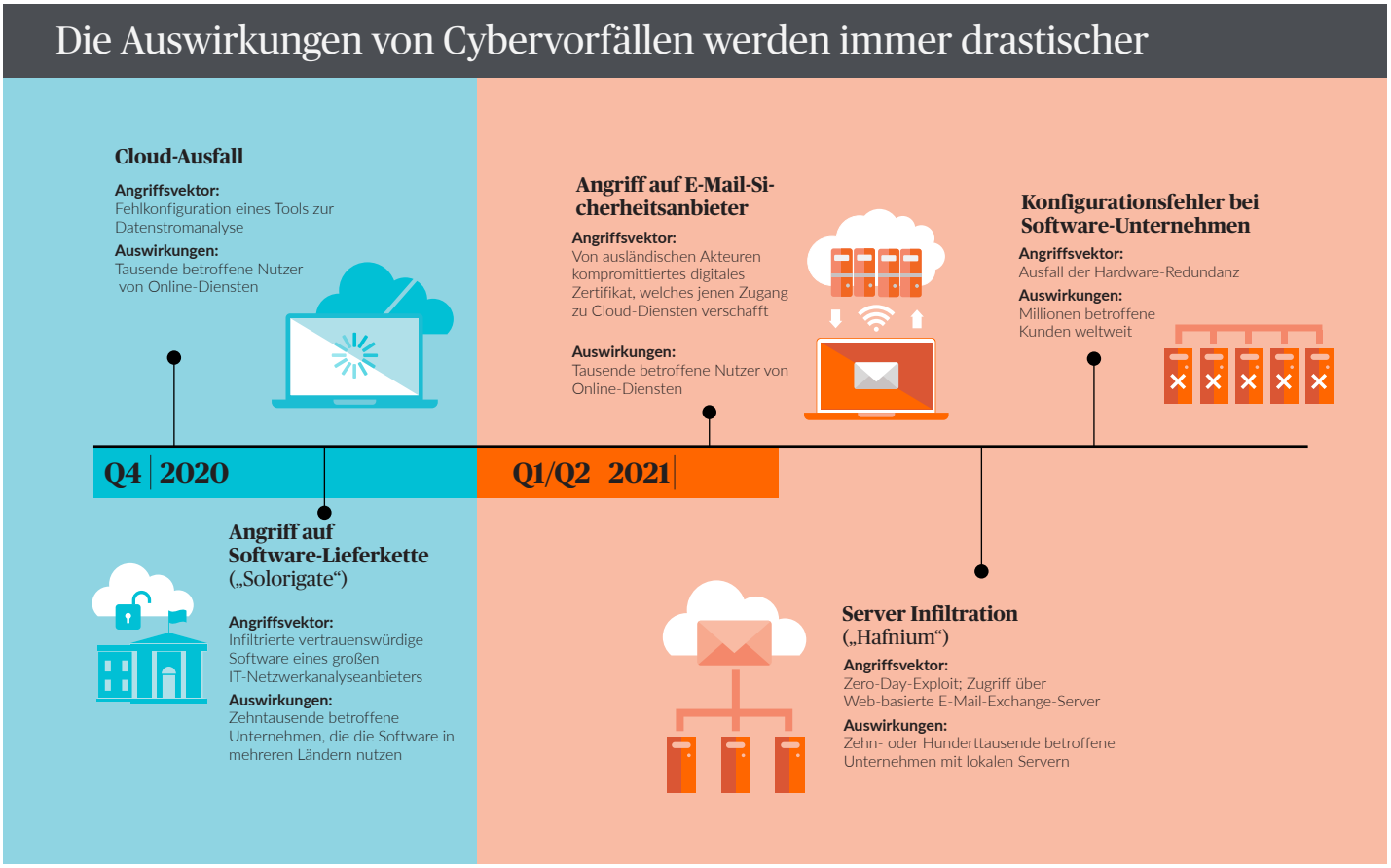
Wo werden Ereignisse mit begrenzten Auswirkungen und weitverbreitete Ereignisse in der Polizze im Einzelnen beschrieben?

Auf der ersten Seite der Polizze ist angegeben, dass Cybervorfälle entweder als Ereignisse von geringer (Ereignisse mit begrenzten Auswirkungen) oder von großer Tragweite (weitverbreitete Ereignisse) kategorisiert werden; die genauen Definitionen sind in der Polizze aufgeführt. Weitere wichtige Definitionen, die innerhalb dieser Konzepte zum Tragen kommen, sind u. a. auch Weitverbreitete Auslöser und Gruppe mit beschränkten Auswirkungen.

Bei Polizzen, die für alle Arten von weitverbreiteten Ereignissen dieselben Versicherungssummen, Selbstbehalte und Mitversicherungen vorsehen, muss nicht zwischen den vier Unterkategorien von weitverbreiteten Ereignissen unterschieden werden. Gelten jedoch verschiedene Versicherungssummen, Selbstbehalte und Mitversicherungen, sind bei der Prüfung die folgenden Begriffsbestimmungen der Unterkategorien von weitverbreiteten Ereignissen zu berücksichtigen:

- Bekannte schwere Sicherheitslücken
- Schwerwiegende Zero- Day-Schwachstellenausnutzung
- Software-Lieferketten-Ausnutzung
- Alle anderen weitverbreiteten Ereignisse

Die Polizze befasst sich mit den „Pflichten im Falle eines Cybervorfalls“ und enthält eine detaillierte Erläuterung der Zusammenarbeit zwischen Chubb und dem Versicherungsnehmer bei Eintritt eines Cybervorfalls. U. a. handelt es sich hierbei um Informationen über den Zeitpunkt und die Methoden der Feststellung, ob es sich bei einem Cybervorfall um ein Ereignis mit begrenzten Auswirkungen oder ein weitverbreitetes Ereignis handelt.



Gibt es Beispiele für tatsächlich stattgefundene weitverbreitete Ereignisse?

Aktuelle Beispiele für Ereignisse mit weitreichenden Auswirkungen sind der obigen Grafik zu entnehmen.

Wie gestaltet sich die Mitversicherung? Gibt es hierzu ein Beispiel?

Bei der Mitversicherung für weitverbreitete Ereignisse, Ransomware-Vorfälle und die Ausnutzung veralteter Software handelt es sich um eine „schadenmindernde“ Versicherung, d. h. durch die Mitversicherung des Versicherungsnehmers wird die Versicherungssumme nicht aufgebraucht. Die Haftung für die einzelnen Schäden wird vielmehr zwischen Versicherungsnehmer und Versicherer aufgeteilt und der Anteil des Versicherers richtet sich nach der für das jeweilige Risiko geltenden Versicherungssumme.

Hat die Polizze beispielsweise ein Sublimit von 5 % des aggregierten Polizzenlimits für weitverbreitete Ereignisse von 5 Mio. EUR, haftet der Versicherer im Rahmen der Deckung für die durch das weitverbreitete Ereignis verursachten Schäden maximal mit 250.000 EUR.

Sofern im Falle eines weitverbreiteten Ereignisses eine Mitversicherung von 50 % gilt, würde ein Schaden in Höhe von 1 Mio. EUR im Verhältnis 50:50 zwischen dem Versicherungsnehmer und dem Versicherer aufgeteilt und das Sublimit des weitverbreiteten Ereignisses wäre damit aufgebraucht, da der Versicherer das zur Verfügung stehende Sublimit von 500.000 EUR gänzlich ausgezahlt hätte.

Auch ein Schaden für ein weitverbreitetes Ereignis in Höhe von 500.000 EUR würde im Verhältnis 50:50 geteilt. Da aber der Versicherer in diesem Fall nur 250.000 EUR zahlen würde, blieben im Rahmen des Sublimits für weitverbreitete Ereignisse für künftige Schäden noch 250.000 EUR übrig.

Fußnoten

1. National Institute of Standards and Technology's National Vulnerability Database. Accessed at https://nvd.nist.gov/vuln/search
2. AV-TEST Institute (2021). Accessed at www.av-test.org/en/statistics/malware/
3. Federal Commission Warns Dangerously Insecure U.S. At Risk of 'Catastrophic' Cyber Attack (2020). Accessed at www.forbes.com/sites/daveywinder/2020/03/14/make-america-safe-again-federal-commission-warns-us-at-risk-of-catastrophic-cyber-attack/?sh=244402e34d27
4. Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk (2021). Accessed at www.insurancejournal.com/research/research/ransomware-and-aggregation-issues-call-for-new-approaches-to-cyber-risk/
5. ebd.
6. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

Über Chubb

Chubb ist der größte börsennotierte Sach- und Haftpflichtversicherer der Welt. Das Unternehmen verfügt über Niederlassungen in 54 Ländern und Regionen und ist Anbieter von Sach- und Haftpflichtversicherungen für Privatpersonen und Unternehmen, privaten Unfall- und Krankenzusatzversicherungen sowie Rück- und Lebensversicherungen für einen vielfältigen Kundenkreis. Als Versicherer beurteilen, übernehmen und handhaben wir Risiken mit Sachverstand und Disziplin. Unser Unternehmen steht für Kundenservice und eine faire und umgehende Schadenregulierung. Zudem zeichnen wir uns durch ein breites Produkt- und Dienstleistungsspektrum, umfassende Vertriebskapazitäten, eine außerordentliche Finanzstärke sowie weltweite Repräsentanzen 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 Direktionen in Zürich, New York, London, Paris und an weiteren Standorten und beschäftigt weltweit mehr als 31.000 Mitarbeiter. Weitere Informationen finden Sie unter www.chubb.com.

Nähere Informationen über Chubbs Erfahrung und Expertise im Management von Cyberrisiken finden Sie hier: chubb.com/at

Chubb. Insured.℠