Chubb setzt beim Umgang mit zunehmenden Cyberrisiken auf Flexibilität und Zukunftsfähigkeit

CHUBB®

Policeninhaber haben die Möglichkeit, Ihre Cyberversicherungen so zu gestalten, dass die Risiken weitverbreiteter Ereignisse («Widespread Events»), Ransomware-Vorfälle oder vernachlässigte Software-Sicherheitslücken bedarfsgerecht abgesichert sind.

Weitverbreitete Ereignisse

Wir leben in einer zunehmend digitalisierten und vernetzten Welt. Verbreitet eingesetzte Software, aber auch Kommunikations- und Technologieplattformen werden nicht selten von Tausenden oder gar Millionen von Firmen genutzt. Schon ein einziger Angriff auf eine häufig eingesetzte Technologie oder vielgenutzte Plattform bzw. deren Ausfall kann zu einer Risikoaggregation führen, welche die Underwriting-Kapazitäten der gesamten Versicherungsbranche übersteigt. Um Policeninhabern Deckungssicherheit und einen stabilen Markt zu bieten, gewährt Chubb Deckungszusagen mit spezifischen Limits, Selbstbehalten und Mitversicherungen für Ereignisse von grosser Reichweite, die sogenannten «Widespread Events».

Arten von weitverbreiteten Ereignissen, die von Chubb versichert werden:

Grossangelegte Software-Lieferketten-Exploits
Mit diesen Cyberangriffen gelingt es Tätern, mittels einer vertrauenswürdigen zertifizierten Software in Systeme einzudringen. Im Grunde handelt es sich hierbei um Trojaner.

Beispiele: Solorigate (2020), NotPetya (2017)

Schwerwiegende Zero-Day-Exploits grossen Ausmasses
Attacken dieser Art konzentrieren sich auf bestimmte Software-Sicherheitslücken, die in einigen Fällen nur Cyberkriminellen bekannt sind. Die oftmals nicht ausreichend geschützten Schwachstellen können leicht ausgenutzt werden – mit gravierenden Konsequenzen.

Beispiel: Hafnium (2021)

Grossangelegte Exploits bekannter gravierender Sicherheitslücken
Angriffe dieser Art resultieren aus gravierenden Software-Schwachstellen, die zwar bekannt sind, aber nicht durch Patches behoben werden. Diese Sicherheitslücken werden als gravierend eingestuft, da sie leicht ausgenutzt und aus der Ferne mit nur geringen Zugriffsrechten angegriffen werden können und der entstehende Schaden erheblich sein kann.

Beispiel: MSSP-Angriff (2021)

Alle sonstigen weitverbreiteten Ereignisse
Bestimmte Arten von Cyberangriffen können zeitgleich oder automatisch eine Vielzahl von 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 stark in Anspruch genommen, dass ihr Ausfall Auswirkungen auf den Geschäftsbetrieb Tausender, wenn nicht Millionen von Unternehmen haben kann.

Beispiel: Cloud-Ausfall im US-Bundesstaat Virginia (2020)

Der weitverbreitete Ereignis-Nachtrag enthält präzise und sinnvolle Schadenregulierungsregeln

- Damit z. B. die weitverbreiteten Ereignis-Limits erst dann durch die Incident Response-Kosten aufgebraucht werden, wenn feststeht, dass es sich bei einem Ereignis tatsächlich um ein weitverbreitetes Ereignis handelt. Es erfolgt keine Rückerstattung von Kosten, die vor der Feststellung entstanden sind.

- Policeninhaber haben die Option, bestimmte Arten investigativer Daten nicht herauszugeben, wenn in beiderseitigem Einvernehmen vereinbart wird, dass es sich bei einem Ereignis um ein weitverbreitetes Ereignis handelt.

- Um es Policeninhabern zu ermöglichen, den für ihr Unternehmen geeignetsten Deckungsschutz zu kaufen, werden Cybervorfälle entweder als

  - Limited-Impact Event (z. B. ein lokales Ereignis mit «Business as usual»-Schadenregeln)
  - oder als weitverbreitetes Ereignis (z. B. ein systematisches Ereignis mit strukturellen Schadenregulierungsdifferenzen wie Limit, Selbstbehalt und Mitversicherung) eingestuft.

Ransomware

Ransomware-Angriffe haben sowohl hinsichtlich ihrer Häufigkeit als auch Schwere deutlich zugenommen. Die Schadenauswirkungen für Policeninhaber sind bei dieser Art von Attacken deutlich höher als die Lösegeldsumme. Unabhängig davon, ob letztlich ein Lösegeld gezahlt wird: Policeninhabern entstehen häufig Rechtskosten, Auslagen für forensische Untersuchungen, Betriebsunterbrechungsschäden, Kosten im Zusammenhang mit der Wiederherstellung digitaler Daten und möglicherweise auch mit Schadenersatzzahlungen oder der Abwehr von Ansprüchen.

Über einen Ransomware-Nachtrag können die Deckungslimits, Selbstbehalte und Mitversicherungen bei durch Ransomware verursachte Schäden kundenspezifisch angepasst werden.

Vernachlässigte Software-Sicherheitslücken

Ein wesentlicher Aspekt einer guten Cyberrisiken-Hygiene sind kontinuierliche Softwareaktualisierungen. Viele Schäden lassen sich durch das Patchen anfälliger Software vermeiden, noch bevor es Cyberkriminellen gelingt, Sicherheitslücken auszunutzen. Doch nicht in jedem Unternehmen werden Schwachstellen unverzüglich behoben. In einigen Fällen gibt es legitime Gründe dafür, Software-Updates vor dem Rollout zu testen. Kompatibilitäts-, Kapazitäts- oder einfach nur logistische Probleme können dazu führen, dass zur Verfügung stehende Patches selbst in einer optimal gemanagten Information Security-Organisation nicht schon am ersten Tag oder innerhalb der ersten Woche installiert werden. Aus diesem Grund gewährt Chubb Policeninhabern eine 45-tägige Nachfrist, um Software-Sicherheitslücken schliessen zu können, die in der National Vulnerability Database des US-amerikanischen National Institute for Standards and Technology (NIST) als Common Vulnerabilities and Exposures (CVEs) öffentlich gemacht werden.

Der Neglected Software Exploit-Nachtrag bietet nach Ablauf der 45-tägigen Frist Deckungsschutz, indem die Risikoaufteilung zwischen dem Policeninhaber und dem Versicherer mit der Zeit auf den Policeninhaber übergeht, dessen Risikobeteiligung zunehmend höher wird, wenn die Sicherheitslücke nicht innerhalb von 46, 90, 180 oder 365 Tagen durch ein Patch behoben wird.

Kontakt

Chubb Versicherungen (Schweiz) AG
Bärengasse 32
8001 Zürich

O +41 43 456 76 00
infoch@chubb.com
chubb.com/ch

Dirk Wietzke
Financial Lines Manager
M +41 76 557 81 21
E dwietzke@chubb.com

Sylvie Verdier
Cyber Practice Lead
M +41 76 434 77 82
E sylvie.verdier@chubb.com

Stefan Wohl
Teamleader Financial Lines, Middle Market
M +41 79 231 02 90
E swohl@chubb.com

Chubb. Insured.[SM]

CH0422 03/22