Cyber Enterprise Risk Management

Ein zukunftsfähiger Ansatz für die Absicherung von vielfältigen Cybervorfällen, einschließlich weitverbreiteter Ereignisse (Widespread Events)

CHUBB®

Chubb versichert seit mehr als 20 Jahren Cybervorfälle und -risiken. In dieser Zeit ist die Abhängigkeit von der zunehmenden Vernetzung von Technologien und Daten weltweit immer größer geworden. Heute sehen sich Unternehmen mit zahlreichen Cyberrisiken konfrontiert, von denen viele systemrelevante Gefahren sind und eine Vielzahl an Branchen gleichermaßen betreffen. Systemrelevante Risiken können zu weitverbreiteten Ereignissen (Widespread Events) von katastrophalem Ausmaß führen, weshalb das Management dieser unternehmensübergreifenden Risiken eine spezielle Lösung erfordert.

Mit dem Cyber Enterprise Risk Management (Cyber ERM) und den Lösungen von Chubb für weitverbreitete Ereignisse können Unternehmen ihren Versicherungsschutz individuell auf ihre spezifischen Risiken und Bedürfnisse zuschneiden. Dies ermöglicht ihnen eine größere Deckungssicherheit und bietet zugleich langfristige Stabilität auf dem Cyberversicherungsmarkt.

Dreiteiliger Ansatz

- **Services zur Schadenminderung:** Zugang zu Tools und Ressourcen, die erforderlich sind, um wichtige Bereiche von Cybersicherheitsrisiken zu managen, bevor es zu einem Vorfall kommt.
- **Incident Response-Services:** Unterstützung im Schadenfall durch ein vielfältiges Experten-Team aus den Bereichen Recht, Computerforensik, Kunden-Benachrichtigungen, Callcenter, Öffentlichkeitsarbeit, Betrugsberatung, Bonitätsüberwachung und Identitätswiederherstellung zur Eindämmung von Verlusten.
- **Risikotransfer:** breiter, nachhaltiger Deckungsschutz, gestützt durch die Finanzstärke von Chubb.

Der Chubb Unterschied

- Innovative, maßgeschneiderte Lösungen - unabhängig von Unternehmensgröße, Branche und Risikoart.
- Künftige Änderungen bei regulatorischen, rechtlichen und Cyber Security-Standards werden berücksichtigt und in die Deckung integriert.
- Keine Mindestprämien. Prämienstaffelung für alle Risikogrößen je nach Deckungsumfang und Limits.
- Cyber Incident Response-Prozess mit umfangreichen verbraucherorientierten, über regulatorischen Mindestanforderungen hinausgehenden Lösungen.
- Online-Angebotserstellung und Policen-Ausstellung in Echtzeit für bestimmte Kleinrisiken möglich.

DE0421 10/21

- Leicht verständliches, auf den Ablauf eines typischen Cybervorfalls ausgerichtetes Formular.
- Weltweiter Geltungsbereich für die kontinuierliche Entwicklung im Bereich Hosting und Datenspeicherung.

2021 eingeführte Vertragsveränderungen

- Weitverbreitete Ereignisse: Gilt für Vorkommnisse, die weitreichende Folgen für Dritte haben, die in keiner Weise in Verbindung zum Versicherten stehen. Ähnlich wie bei Überschwemmungs- und Erdbebenrisiken in Sachpolicen können Limits, Selbstbehalte und Mitversicherungen für alle weitverbreiteten Ereignisse oder ganz bestimmte Risiken kundenspezifisch angepasst werden:
  - Widespread Severe Vulnerability Exploits
  - Widespread Severe Zero-Day Exploits
  - Widespread Software Supply Chain Exploits
  - alle sonstigen weitverbreiteten Ereignisse
- Ransomware: Für das steigende Risiko von Erpressungssoftware sind massgeschneiderte Deckungen, Limits, Selbstbehalte und Mitversicherungen einheitlich auf alle Cyber-Deckungen anwendbar.
- Neglected Software Exploit: Gute Software-Patching-Hygiene wird mit 45 Tagen vollem Deckungsschutz belohnt. Für Software, deren Fehler nach Ablauf von 45 Tagen nicht durch Patches behoben werden, wird die Risikoteilung zwischen dem Versicherten und dem Versicherer mit der Zeit graduell neu gewichtet.

Der Deckungsschutz im Überblick

Im Rahmen von Cyber ERM sind folgende Deckungen erhältlich:

Third-Party Liability Coverage	First-Party Coverage

Haftung bei Cyber-, Datenschutz- und Netzwerksicherheitsverletzungen
Unterlassung des Schutzes privater oder vertraulicher Daten Dritter sowie das Unvermögen zu verhindern, dass infolge eines Cybervorfalls die Systeme Dritter geschädigt werden

Zahlungskartenverlust
Vertragshaftung gegenüber Unternehmen der Zahlungskartenbranche infolge von Cybervorfällen

Regulatorische Verfahren
Abwehr aufsichtsbehördlicher Maßnahmen und Deckung für Bußgelder und Strafen, sofern diese gemäß geltendem Recht versicherbar sind

Medienhaftung
Copyright- und Trademark-Verstöße im Hinblick auf bestimmte Medieninhalte

Cyber Incident Response-Fonds
Rechtskosten, Forensik, Benachrichtigungskosten, Bonitätsüberwachung Öffentlichkeitsarbeit, etc.

Betriebsunterbrechung
Gewinnausfall und Kosten infolge von Unterbrechungen der Systeme des Versicherten sowie zusätzliche Ausgaben. Bei notfallbedingten Betriebsunterbrechungen sind auch durch Unterbrechungen verursachte Schäden an Systemen Dritter versichert

Wiederherstellung digitaler Daten
Kosten, um verlorengegangene oder beschädigte Daten/Software wiederherzustellen bzw. zu ersetzen.

Telefongebührenbetrug
Durch Betrüger verursachte Kostenpositionen auf Telefonrechnungen

Netzwerk-Erpressung
Digitale Zerstörungen/Schädigungen, die gegen Zahlung einer Geldsumme verhindert werden sollen

Kontakt

Chubb European Group SE
Direktion für Deutschland
Baseler Straße 10
60329 Frankfurt am Main

O +49 69 75613 0
F +49 69 746193
info.de@chubb.com
chubb.com/de

Johannes Gschossmann
Line Manager Financial Lines, Eastern Region
M +49 162 1351812
E johannes.gschossmann@chubb.com

Naci Cagras
Senior Underwriter Cyber, Major Accounts
O +49 211 8773224
E naci.cagras@chubb.com

Benedikt Klingenheben
Senior Underwriter Cyber, Middle Market
O +49 211 8773210
E benedikt.klingenheben@chubb.com

Simon Carpels
Small Commercial Segment Leader Germanics
O +49 69 756136814
E simon.carpels@chubb.com

Chubb. Insured.℠

DE0421 10/21