Cyberversicherungen am Limit

Viele Versicherer haben ihre Zeichnungspolitik im letzten Jahr mehrfach verschärft. Der Transfer von Cyberrisiken wird zur Herausforderung.


© ADOBESTOCK

Wer jetzt eine Cyberversicherung abschliesst, muss mit höheren Prämien rechnen.

VON MAX KELLER

Autor

Max Keller ist Leiter des Funk Risk Lab bei Funk Insurance Brokers AG

> *www.funk-gruppe.ch*

Unternehmen, die ihre Cyber-Police zum Jahreswechsel erneuern wollten, mussten tief in die Tasche greifen. Eine deutliche Erhöhung von Prämien bei gleichzeitiger Verdopplung der Selbstbehalte und Reduzierung der Limiten ist Realität.

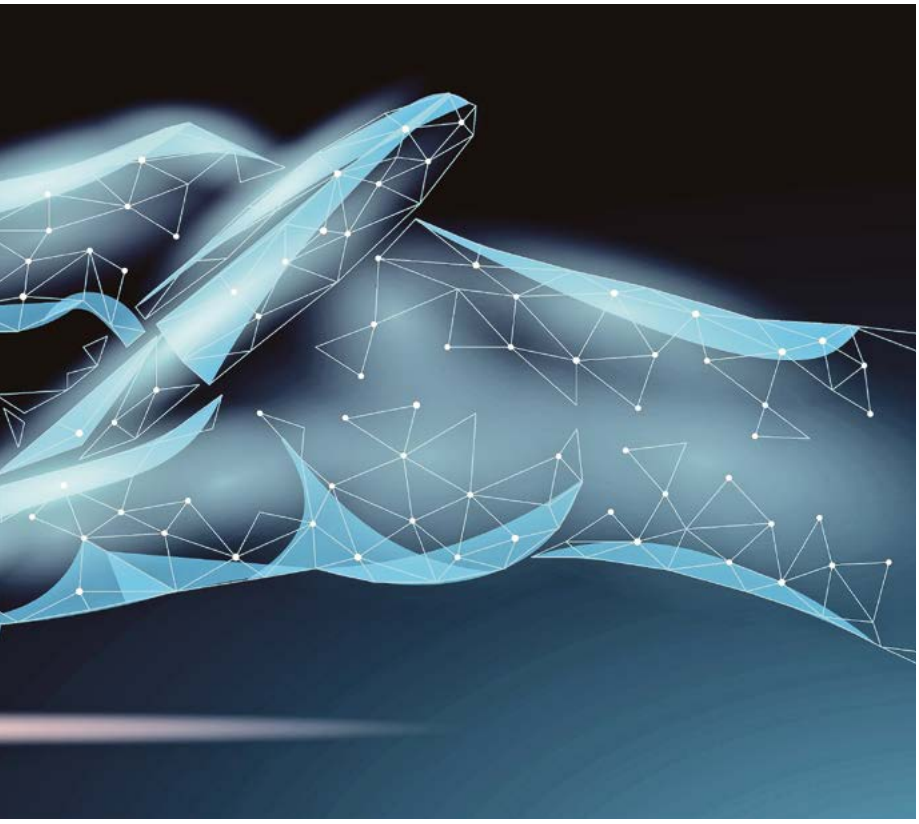
Die Schadenssituation spitzt sich währenddessen immer weiter zu. Meist handelt es sich dabei um Ransomware-Attacken, die stets professioneller und frequentierter werden. Das Geschäftsmodell «Ransomware-as-a-Service» entwickelt sich stetig weiter: Zum einen verschlüsseln die Angreifenden aktive Systeme und falls möglich auch Backups. Zum anderen stehlen sie vertrauliche Daten oder schützenswerte Personendaten, um zusätzlich Druck ausüben zu können (Double-Extortion). So sollen angegriffene Unternehmen in die Knie gezwungen und die Entscheider zur Zahlung des Lösegeldes bewogen werden. Die individuelle Lösegeldforderung wird dabei an die finanziellen Möglichkeiten des angegriffenen Unternehmens angepasst, lässt sich erfahrungsgemäss jedoch runterhandeln.

«Versicherer formulieren inzwischen konkrete Vorgaben an die Cyber-Security.»

Cyber-Security-Anforderungen für den Versicherungsschutz

Als Antwort auf die deutliche Schadenzunahme formulieren Versicherer inzwischen konkrete Vorgaben an die Cyber-Security. Diese müssen Unternehmen zwingend erfüllen, wenn sie eine seriöse Cyber-Police abschliessen wollen. Die wesentlichen Anforderungen an die CyberSecurity sind:

1. Transparenz über alle Assets (IT-Systeme und verarbeitete Daten)
2. Multi-Faktor-Authentifizierung für jeglichen Fernzugriff (z.B. aus dem Homeoffice) auf IT-Systeme
3. Starke Passwörter (Länge- und Komplexitätsanforderungen)
4. Jährliche Sensibilisierung der Mitarbeitenden auf Informationssicherheit und Cyberrisiken, kombiniert mit einem simulierten Phishing-Angriff
5. Strikte Netzwerksegmentierung von Operational Technology und/oder Legacy-Systemen sowie nach geografischen oder organisatorischen Gesichtspunkten
6. Kontinuierliches und reaktionsfähiges Patchmanagement (Überwachung von Schwachstellen, Installation kritischer Patches innerhalb von 72 Stunden)



«Eine Stabilisierung des Marktes scheint nicht in greifbarer Nähe.»

7. Solide Backup-Strategie (nach der 3-2-1-Regel sowie einem offline oder stand-alone Cloud-Backup für Ransomware-Vorfälle)
8. Dokumentierter und jährlich geübter Disaster Recovery Plan (inklusive Backup-Recoveries)
9. Für grosse und international ausgerichtete Unternehmen: Einheitliche Cybersecurity-Standards bei allen Tochtergesellschaften

Deckungseinschränkungen

Eine wichtige Entwicklung beim Transfer von Cyberrisiken ist, dass immer mehr Versicherer den Deckungsumfang im Zusammenhang mit Schäden durch Ransomware massiv einschränken. Dies lässt sich auf die hohe Frequenz von Ransomware-Vorfällen zurückführen. Folglich bieten einige Versicherer überhaupt keine Deckungen für diese Angriffstaktik bzw. dieses Schadprogramm an. Andere beschränken ihre Leistungen auf max. 50% von der Versicherungssumme oder beteiligen den Versicherungsnehmer zusätzlich an solchen Vorfällen. Sporadisch werden beim Versicherungsabschluss auch Schäden durch bekannt gewordene kritische Schwachstellen wie Microsoft Exchange oder Log4Shell vom Deckungsumfang ausgeschlossen.

Erhöhung von Versicherungsprämien

Die Prämien für Cyberversicherungen haben in den letzten Jahren aufgrund der stetig zunehmenden Bedrohungs- und Schadenssituation eine Korrektur erfahren. Bei der Erneuerung einer Cyberversicherung sind Prämienaufschläge von 50–100% üblich. Nach grösseren Schadenfällen kann auch eine Vervierfachung der Prämie zur Anwendung kommen. Zudem haben ausgewählte Versicherer Mindestprämien eingeführt, um Frequenzschäden in ihren Büchern besser kontrollieren zu können.

Auch für 2022 haben Versicherungsgesellschaften Strategieanpassungen für Cyberversicherungen angekündigt. Eine Stabilisierung des Marktes scheint also nicht in greifbarer Nähe.

Ein 10-Punkte-Plan zur Bewältigung eines Cyberernstfalls

Eine Cyberattacke ist heute wahrscheinlicher als je zuvor. Studien des IT-Sicherheitsdienstleisters Sophos, wie etwa «The State of Ransomware 2021», belegen, dass international 37 Prozent der befragten Unternehmen allein von Ransomware betroffen sind. Zwar richtete Ransomware innerhalb der letzten Jahre die vermutlich verheerendsten Schäden an, sie ist allerdings bei Weitem nicht die einzige Malware-Art, die zu ernsthaften Problemen für Unternehmen führen kann. Ein gut vorbereiteter und durchdachter Incident-Response-Plan, den alle betroffenen Parteien im Unternehmen sofort umsetzen können, kann die Folgen eines Cyberangriffs erheblich abmildern. Experten von Sophos Labs haben dementsprechend aus ihren Erfahrungen folgenden 10-Punkte-Plan zur Bewältigung eines Cyberernstfalls ausgearbeitet:

1. Alle Beteiligten und Betroffenen festlegen
2. Kritische Ressourcen identifizieren
3. Ernstfallszenarien üben und durchspielen
4. Security-Tools bereitstellen
5. Maximale Transparenz sicherstellen
6. Zugriffskontrolle implementieren
7. In Analyse-Tools investieren
8. Reaktionsmassnahmen für den Cyberernstfall festlegen
9. Awareness-Trainings durchführen
10. Managed Security Services in Anspruch nehmen

> Quelle: www.sophos.com