



Angespannte Sicherheitslage: Cyberrisiken als neue Normalität für Versicherer

Cyberangriffe, Regulierung und technologische Aufrüstung prägen zunehmend den Alltag von Versicherern. In seinem Kommentar ordnet Sören Brokamp, Geschäftsführer der Perseus Technologies GmbH, die aktuelle IT-Sicherheitslage ein und beschreibt, warum Cyberrisiken längst zur neuen Normalität geworden sind. Der Text erschien zuerst im **expertenReport 03/26.**

Technologische Entwicklungen beschleunigen dies zusätzlich. Angriffe werden dynamischer und komplexer. Für Unternehmen bedeutet dies, dass IT-Sicherheit nicht mehr isoliert betrachtet werden kann. Eine ganzheitliche Cybersicherheitsstrategie ist unerlässlich, um hohe Kosten, Betriebsunterbrechungen und Reputationsschäden zu vermeiden.

Die größten Bedrohungen für deutsche Unternehmen

Internen Analysen des Incident-Response-Teams des Cybersicherheitsunternehmens Perseus zufolge machen kompromittierte geschäftliche E-Mail-Konten mit einem Anteil von 40 Prozent den größten Teil aller Sicherheitsvorfälle aus. Ransomware- und Phishing-Angriffe folgen. Für datenintensive Branchen wie wie unter anderem die Versicherungswirtschaft stellen solche Vorfälle ein erhebliches Risiko dar. In vielen Fällen ermöglicht der Faktor Mensch den Angriff – etwa durch Unachtsamkeit, Unwissenheit oder gezielte Manipulation.

Daneben spielen technische und organisatorische Schwachstellen eine zentrale Rolle. Zu einfache Passwörter, fehlende Multi-Faktor-Authentifizierung oder nicht eingespielte Sicherheitsupdates erleichtern Angreifern den Zugang. Fehlen zusätzlich aktuelle Datensicherungen, kann ein einzelner Vorfall schnell existenzbedrohende Ausmaße annehmen.

KI als Herausforderung für die IT-Sicherheit

Eine weitere Verschärfung erfährt die Bedrohungslage durch den zunehmenden Einsatz künstlicher Intelligenz (KI). Richtig eingesetzt kann KI die IT-Sicherheit stärken, etwa durch das frühzeitige Erkennen von Anomalien oder neuer Schadsoftware. Gleichzeitig nutzen jedoch auch Kriminelle KI, um Phishing-Angriffe zu automatisieren oder Schwachstellen in kürzester Zeit aufzuspüren.

Politik gibt Regulierungen vor

Um die Cyberresilienz von Unternehmen zu stärken, setzt die Politik zunehmend auf Regulierung. Mit der NIS-2-Richtlinie wurden Unternehmen wichtiger und wesentlicher Sektoren stärker in die Verantwortung genommen. Ergänzend schafft die KI-Verordnung einen Rahmen für den sicheren Einsatz künstlicher Intelligenz, indem Anwendungen nach ihrer Kritikalität eingestuft und mit entsprechenden Pflichten versehen werden. Ziel ist es, Sicherheit und Stabilität für Wirtschaft und Gesellschaft langfristig zu gewährleisten.

Die IT-Sicherheitslage bleibt angespannt. Cyberangriffe, menschliche Fehler und neue Technologien prägen das Bedrohungsbild. Für Versicherer wird IT-Sicherheit zunehmend zu einer strategischen Aufgabe, die durch regulatorische Vorgaben zusätzlich an Bedeutung gewinnt.

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4950654/Angespannte-Sicherheitslage-Cyberisiken-als-neue-Normalitaet-fuer-Versicherer/>