expertenReport

Quelle: Redaktion experten.de / KI-generiert

Cyber-Erpressung eskaliert: Lösegeldforderungen steigen um 47 Prozent

Michael Fiedler

Ransomware-Angriffe werden teurer, doch immer mehr Unternehmen verweigern die Zahlung von Lösegeld. Das zeigt der aktuelle Cyber Claims Report 2026 des Cyberversicherers Coalition. Besonders häufig bleiben jedoch weiterhin E-Mail-basierte Betrugsformen wie Business Email Compromise.

Verbesserte Cyber-Resilienz

Nach Einschätzung der Autoren deutet diese Entwicklung darauf hin, dass Unternehmen ihre Widerstandsfähigkeit gegenüber Cyberangriffen verbessert haben. Insbesondere Daten-Backups und strukturierte Incident-Response-Pläne ermöglichen es vielen Organisationen inzwischen, auf Lösegeldzahlungen zu verzichten. „Die Daten deuten auf einen Wendepunkt im Geschäftsmodell von Ransomware hin: Während die Angreifer ihre Forderungen bis in den siebenstelligen Bereich eskalieren lassen, hilft die Unterstützung durch den Cyber-Versicherer den Unternehmen dabei, Verluste effektiv zu begrenzen“, sagt Rob Jones, Global Head of Claims bei Coalition.

Ransomware bleibt teuerste Schadenart

Trotz der sinkenden Zahlungsbereitschaft bleibt Ransomware die kostspieligste Form von Cyberangriffen. Im Jahr 2025 lag der durchschnittliche Schaden bei 269.000 US-Dollar. Besonders verbreitet ist inzwischen die sogenannte doppelte Erpressung. Dabei verschlüsseln Angreifer nicht nur Systeme, sondern entwenden zusätzlich sensible Daten und drohen mit deren Veröffentlichung. Diese Methode machte 70 Prozent aller Ransomware-Schadenfälle aus. Cyberangriffe mit Datendiebstahl verursachten laut Bericht mehr als doppelt so hohe Schäden wie andere Ransomware-Vorfälle.

E-Mail-Betrug bleibt häufigste Angriffsmethode

Während Ransomware häufig die Schlagzeilen dominiert, entstehen die meisten Cyber-Schäden weiterhin durch klassische Betrugsformen. Laut Coalition entfielen 58 Prozent aller Cyber-Vorfälle auf Business Email Compromise (BEC) oder Funds Transfer Fraud (FTF). Dabei manipulieren Angreifer geschäftliche E-Mail-Kommunikation oder geben sich als Geschäftspartner aus, um Unternehmen zu betrügerischen Überweisungen zu bewegen. Mehr als die Hälfte aller FTF-Schäden (52 Prozent) ging auf vorherige BEC-Angriffe zurück. „Auch wenn es ermutigend ist, dass immer mehr Organisationen bereit sind, Erpressungsforderungen abzulehnen, zeigen unsere

Schadendaten, dass die klassische E-Mail-Kriminalität keineswegs verschwunden ist“, sagt Jones.

Schäden sinken trotz steigender Angriffszahlen

Die Daten zeigen ein differenziertes Bild: Die Schadenfrequenz stieg im Jahr 2025 zwar um drei Prozent, gleichzeitig sank jedoch die durchschnittliche Schadenshöhe um 19 Prozent auf rund 116.000 US-Dollar. Dies deutet darauf hin, dass Unternehmen Cybervorfälle zunehmend schneller erkennen und begrenzen können.

Große Unternehmen besonders häufig betroffen

Besonders häufig registriert der Bericht Cyber-Schäden bei Unternehmen mit einem Jahresumsatz von über 100 Millionen US-Dollar. In dieser Gruppe treten Vorfälle laut Analyse etwa fünfmal häufiger auf als bei kleineren Unternehmen. Gleichzeitig zeigen sich auch hier Fortschritte bei der Schadenbegrenzung: Die durchschnittliche Schadenshöhe sank in dieser Kategorie auf 268.000 US-Dollar.

Cyberversicherung entwickelt sich weiter

Der Bericht basiert auf Daten von mehr als 100.000 Versicherungsnehmern in den USA, Kanada, Großbritannien, Australien und Deutschland. Nach Angaben von Coalition wurden 64 Prozent der abgeschlossenen Cyber-Schadenfälle ohne finanzielle Eigenbelastung der Versicherungsnehmer reguliert.

Lesetipp: Cyberrisiken als neue Normalität

Cyberangriffe gehören für Unternehmen längst zum Alltag. Welche Bedrohungen aktuell besonders relevant sind und wie sich die Sicherheitslage für Versicherer verändert, analysiert Sören Brokamp von der Perseus Technologies GmbH im aktuellen expertenReport (03/2026).

Im Beitrag „Angespannte Sicherheitslage: Cyberrisiken als neue Normalität für Versicherer“ zeigt der Cybersecurity-Experte unter anderem, warum kompromittierte E-Mail-Konten, Ransomware und Phishing weiterhin zu den wichtigsten Angriffsvektoren zählen – und welche Rolle Regulierung, Digitalisierung und künstliche Intelligenz für die Sicherheitsstrategie von Unternehmen spielen.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4948702/Cyber-Erpressung-eskaliert-Loesegeldforderungen-steigen-um-47-Prozent/