expertenReport

Quelle: Redaktion experten.de / KI-generiert

Warum immer mehr Unternehmen bei Cyberangriffen kein Lösegeld zahlen

Michael Fiedler

Cyberkriminelle erhöhen ihre Lösegeldforderungen massiv – doch immer mehr Unternehmen verweigern die Zahlung. Hinter diesem Trend stehen bessere Sicherheitsstrategien, strengere Compliance-Regeln und eine wachsende Debatte über die Rolle von Cyberversicherern.

Strategiewechsel im Umgang mit Cyber-Erpressung

Mehrere Faktoren treiben diesen Wandel voran. Unternehmen investieren verstärkt in Datensicherungen, Notfallpläne und Incident-Response-Teams, die eine Wiederherstellung von IT-Systemen ohne Zahlung ermöglichen. Zudem wächst die Sorge, dass Lösegeldzahlungen kriminelle Geschäftsmodelle weiter stärken. Auch Cyberversicherer beschäftigen sich seit Jahren intensiv mit dieser Frage. So hatte der Versicherer AXA 2021 in Frankreich angekündigt, bei neuen Cyberpolicen keine Lösegeldzahlungen mehr zu erstatten. Die Entscheidung löste damals eine branchenweite Diskussion über die Rolle von Versicherungen im Umgang mit Ransomware aus.

Regierungen und Ermittler warnen vor Lösegeldzahlungen

Auch Strafverfolgungsbehörden raten zunehmend davon ab, Lösegeldforderungen nachzugeben. Neben dem finanziellen Schaden besteht das Risiko, dass Unternehmen durch eine Zahlung weitere Angriffe anziehen oder gegen Sanktionsregeln verstoßen. In einigen Fällen können Lösegeldzahlungen sogar rechtliche Konsequenzen haben, etwa wenn Gelder an sanktionierte Organisationen oder Staaten fließen.

Cyberangriffe bleiben ein Milliardenrisiko

Trotz sinkender Zahlungsbereitschaft bleibt Ransomware eine der teuersten Formen der Cyberkriminalität. Neben Produktionsausfällen und Datenverlust können auch Wiederherstellungskosten und Reputationsschäden erhebliche wirtschaftliche Folgen haben. Cyberversicherungen versuchen deshalb zunehmend, den Schwerpunkt von der reinen Schadenregulierung hin zu präventiven Sicherheitsmaßnahmen zu verschieben. Der Trend deutet darauf hin, dass sich das Kräfteverhältnis im Cyberraum langsam verändert: Während Angreifer ihre Forderungen erhöhen, werden Unternehmen zunehmend widerstandsfähiger gegen digitale Erpressung.

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/4948711/Warum-immer-mehr-Unternehmen-bei-Cyberangriffen-kein-Loesegeld-zahlen/