Warum immer weniger Ransomware-Opfer zahlen

12.10.2026, 09:41 | IT, New Media & Software

Pressemitteilung von: *FAST LTA GmbH*



Die Zahl, die aus dem Rahmen fällt

Der Anteil der Ransomware an allen untersuchten Sicherheitsverletzungen stieg laut DBIR 2026 von 44 auf 48 Prozent. Gleichzeitig zahlten 69 Prozent der Opfer kein Lösegeld, und die mediane Forderung sank von 150.000 auf 139.875 US-Dollar.

Mehr Angriffe bei schrumpfender Beute ergibt für ein Geschäftsmodell wenig Sinn. Für die Angegriffenen ergibt es sehr viel Sinn: Wer seine Daten zurückbekommt, verhandelt nicht.

Auch in Deutschland zeigt sich dieses Bild. Bitkom befragte im Frühjahr 2026 repräsentativ 1.003 Unternehmen ab zehn Beschäftigten. 45 Prozent waren in den vergangenen zwölf Monaten von Ransomware betroffen, im Jahr davor lag der Wert bei 58 Prozent. Gezahlt hat jedes fünfte betroffene Unternehmen.

Die Abwehr kommt nicht hinterher

Die zweite Gruppe von Zahlen erklärt, warum sich die Aufmerksamkeit verschiebt. Die Ausnutzung bekannter Schwachstellen ist mit 31 Prozent zum häufigsten Eintrittsvektor geworden. Im Vorjahr führte der Missbrauch gestohlener Zugangsdaten die Liste mit 13 Prozent an.

Gleichzeitig wurden 2025 nur 26 Prozent der kritischen Schwachstellen vollständig behoben. Ein Jahr zuvor waren es 38 Prozent. Die mittlere Zeit bis zur vollständigen Behebung stieg von 32 auf 43 Tage, und zwar bei 50 Prozent mehr kritischen Lücken als im Jahr davor.

Die Aufgabe wächst also schneller, als die Teams sie abarbeiten können. Jede dieser 43 Tage ist ein Fenster, das offen steht.

Das Risiko sitzt zunehmend außerhalb

Hinzu kommt ein Faktor, den keine interne Patch-Strategie erreicht. Sicherheitsverletzungen über Dritte haben im Jahresvergleich um 60 Prozent zugenommen und machen inzwischen 48 Prozent aller Verstöße aus. Fast jeder zweite Vorfall beginnt damit in einem System, das dem betroffenen Unternehmen gar nicht gehört.

Dienstleister, Softwarelieferanten und Partnerzugänge lassen sich vertraglich regeln. Patchen lassen sie sich nicht.

Was die Zahlen zusammen ergeben

Einzeln gelesen sind das vier unauffällige Entwicklungen. Zusammen beschreiben sie eine Verschiebung: Die Wahrscheinlichkeit, einen Einbruch zu verhindern, sinkt. Die Wahrscheinlichkeit, ihn zu überstehen, steigt bei denen, die vorbereitet sind.

Damit wandert die entscheidende Kennzahl von der Abwehr zur Wiederherstellung. Nicht die Zahl der blockierten Angriffe zeigt, wie gut eine Organisation aufgestellt ist, sondern die Zeit bis zum ersten wieder produktiven System.

Wie FAST LTA das umsetzt

Eine Sicherung hilft im Ernstfall nur, wenn Angreifer sie nicht erreichen. Die Silent Bricks trennen die Sicherung deshalb physikalisch vom Netz. Ein Air Gap, der sich nicht per Skript, gestohlenem Admin-Konto oder Fernzugriff aushebeln lässt, hält auch dann, wenn die produktive Umgebung bereits übernommen wurde.

Erasure Coding fängt zusätzlich Hardwareausfälle ab, bevor sie Daten kosten. Angebunden wird das System als VTL, NAS oder S3, passend zur vorhandenen Backup-Software. Entwickelt in München, gefertigt in Deutschland.

Was daraus folgt

Patch-Management, Monitoring und Awareness bleiben notwendig. Die Zahlen des DBIR 2026 zeigen allerdings, dass sie das Risiko nicht mehr allein tragen. Wer heute über Resilienz spricht, sollte prüfen, wie lange der Wiederanlauf tatsächlich dauert, und wer in dieser Zeit noch Zugriff auf die Sicherung hätte.

Ihr Backup schützt Sie vor Ransomware. Oder doch nicht?

Wenn das Backup nicht startet, helfen zehn Kopien nicht. Wir sprechen über reale Wiederanlaufzeiten, über Air Gap, der wirkt, und über die Frage, warum Ransomware-Erpressung bei richtig aufgesetzten Backups ins Leere läuft. Dafür brauchen wir Ihre Umgebung und eine halbe Stunde.

Quellen

- Verizon, Data Breach Investigations Report 2026, Executive Summary (deutsche Fassung): www.verizon.com/business/resources/de/executivebriefs/2026-dbir-executive-summary.pdf
- Bitkom, Pressemitteilung vom 4. September 2026, „Jedes fünfte Ransomware-Opfer hat schon einmal Lösegeld gezahlt", repräsentative Befragung von 1.003 Unternehmen ab zehn Beschäftigten: Ransomware-Opfer-hat-

Loesegeld-gezahlt"

FAST LTA

Tölzer Str. 1
81379 München
Deutschland

Portrait

FAST LTA ist der Spezialist für Datensicherheit und Data-Privacy in Enterprise Storage sowie für Systeme, die lokalen KI-Betrieb ermöglichen. Die Kombination aus langlebiger und wartungsarmer Hardware, integrierter Software und Wartungsverträgen mit bis zu zehn Jahren Laufzeit sorgt für langfristig kostengünstigen Betrieb – von der Archiv- und Backup-Speicherung bis zum lokalen KI-Einsatz. Die Lösungen für sichere Datenspeicherung Made in Germany und digitale Souveränität des Münchner Anbieters haben sich in über 3.500 Installationen bewährt, unter anderem in Healthcare, öffentlicher Verwaltung, Dienstleistung sowie Industrie & Handel.

News-ID: 1326416 • Views: 151 (Stand: 24.11.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1326416/Warum-immer-weniger-Ransomware-Opfer-zahlen.html