Ransomware setzt Einzelhandel massiv unter Druck: Forderungen steigen, IT-Teams am Limit

Anteil der Einzelhandelsunternehmen, die zur Datenwiederherstellung Lösegeld zahlen, steigt im Vergleich zu den Vorjahren stark an.

Die internationale Sophos-Studie „The State of Ransomware in Retail 2025“ zeigt, wie sich Ursachen, Auswirkungen und Strategien im Umgang mit Ransomware verändern und mit welchen Konsequenzen IT- und Cybersicherheitsteams im Einzelhandel zu rechnen haben.

Technisch wie organisatorisch: Standardursachen für Cyberangriffe im Einzelhandel
Nach den Vorgängerstudien aus den Jahren 2023 und 2024 nannten Einzelhändler ausgenutzte Schwachstellen zum dritten Mal in Folge als häufigste technische Ursache für Ransomware-Angriffe. In 30 Prozent der Fälle war diese Form der kriminellen Infiltration nach wie vor ausschlaggebend.
Auch operative Faktoren trugen dazu bei, dass Einzelhandelsunternehmen Opfer von Ransomware werden. Am häufigsten nannte fast die Hälfte (46 Prozent) der Befragten unbekannte Sicherheitslücken als initialen Einstiegspunkt für die Kriminellen. Dicht dahinter rangiert mangelnde Fachkenntnis, die in 45 Prozent der Angriffe eine Rolle spielte – was dem höchsten Wert entspricht, der in irgendeiner der untersuchten Branchen festgestellt wurde.

Weniger Datenverschlüsselung, aber Zunahme neuer Angriffsmethoden
Die Datenverschlüsselung durch Cyberkriminelle ist im Einzelhandel deutlich gefallen. Nur noch 48 Prozent der Angriffe führten 2025 zu einer tatsächlichen Verschlüsselung der Daten, verglichen mit 71 Prozent im Jahr 2023. Parallel dazu erreichte die Zahl der vereitelten Verschlüsselungsversuche ein Rekordhoch, was auf verbesserte Abwehrmechanismen der Unternehmen schließen lässt.
Doch Cyberkriminelle passen sich an: Der Anteil reiner Erpressungsangriffe, bei denen keine Daten verschlüsselt, aber dennoch Lösegeld für die Nichtveröffentlichung sensibler Daten gefordert wird, hat sich innerhalb von zwei Jahren verdreifacht. Während 2023 lediglich zwei Prozent der Befragten betroffen waren, lag der Anteil 2025 bereits bei sechs Prozent.

Resignation als Strategie für Datenwiederherstellung
Die Art und Weise, wie Einzelhändler Daten nach einem Cyberangriff wiederherstellen, hat sich spürbar verändert. Während 2021 noch 32 Prozent der Unternehmen das Lösegeld zahlten, um ihre Daten zurückzuerlangen, waren es 2025 bereits 58 Prozent – deutlich mehr als der branchenübergreifende Durchschnitt von 49 Prozent. Im Gegenzug sank die Nutzung von Backups auf ein Vierjahrestief. Zwar sind Backups nach wie vor die etwas häufiger gewählte Lösung, doch die abnehmende Tendenz deutet auf eine zunehmende Abhängigkeit von anderen Wiederherstellungsmöglichkeiten hin.

Forderungen steigen rasant, dennoch bleiben Zahlungen stabil
Die Studie belegt außerdem einen drastischen Anstieg der Lösegeldforderungen. Im Jahr 2025 lag die durchschnittliche Forderung bei 1,71 Millionen Euro – doppelt so hoch wie noch im Jahr zuvor. Besonders stark zugenommen hat die Zahl der Forderungen von über 4,28 Millionen Euro, die von 17 Prozent im Jahr 2024 auf 27 Prozent im Jahr 2025 gestiegen sind.
Verglichen mit dieser Entwicklung zeigt sich der Einzelhandel im Durchschnitt widerstandsfähiger: Die durchschnittliche Lösegeldzahlung erhöhte sich um fünf Prozent von 813.563 Euro im Jahr 2024 auf 856.382 Euro im Jahr 2025. Gleichzeitig sanken die durchschnittlichen Kosten für die Wiederherstellung nach einem Angriff –

ohne Lösegeldzahlungen – um 40 Prozent auf 1,41 Millionen Euro und damit auf den niedrigsten Wert seit drei Jahren.

Bis an die Substanz: Belastung für IT- und Sicherheitsteams
Die Studie macht zudem deutlich, dass die Folgen von Ransomware weit über finanzielle Schäden hinausgehen. Nahezu die Hälfte der Befragten (47 Prozent) berichtete von verstärktem Druck seitens des Managements, wenn es infolge eines Angriffs zu einer Datenverschlüsselung kam. Viele IT- und Cybersicherheitsverantwortliche gaben außerdem an, unter erhöhter Angst oder Stress vor künftigen Angriffen zu leiden (43 Prozent). Auch krankheitsbedingte Abwesenheit aufgrund von Stress oder psychischen Belastungen (37 Prozent) sowie Schuldgefühle, den Angriff nicht verhindert zu haben (34 Prozent), wurden häufig genannt.

Über die Studie
Die Ergebnisse basieren auf einer unabhängigen, anbieterneutralen Befragung von 3.400 IT- und Cybersicherheitsverantwortlichen in 17 Ländern in Amerika, EMEA und Asien-Pazifik. Darunter befanden sich 361 Teilnehmer aus dem Einzelhandel. Die befragten Unternehmen beschäftigen jeweils zwischen 100 und 5.000 Mitarbeiter. Die Erhebung wurde von Vanson Bourne zwischen Januar und März 2025 durchgeführt. Grundlage waren die Erfahrungen der Befragten aus den vergangenen zwölf Monaten.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de