Einzelhandel im Visier von Ransomware – 75 Prozent mehr Angriffe

Eine Wachstumsrate von 75 Prozent kann im richtigen Segment fantastisch klingen, doch für den Einzelhandel bedeutete das im vergangenen Jahr eine Cyberkatastrophe: 77 Prozent wurden Opfer eines Ransomware-Angriffs, so die Ergebnisse des aktuellen Ransomware-Reports in Retail 2022 von Sophos. Damit liegt der Einzelhandel auf Platz zwei nach der Freizeit- und Medienbranche. Es gibt aber auch gute Nachrichten: Der Einzelhandel zahlte nur knapp ein Drittel des branchenübergreifenden Lösegelds.

Wiesbaden, 8. September 2022 – Sophos hat aktuelle Branchenergebnisse seines weltweit angelegten Ransomware-Reports veröffentlicht. Die Analyse „The State of Ransomware in Retail 2022" zeichnet für den Einzelhandel jedoch kein zuversichtliches Bild ab: nach der Medien-, Freizeit- und Unterhaltungsbranche wird sie von sämtlichen untersuchten Branchen am zweithäufigsten von Ransomware angegriffen. Insgesamt 77 Prozent weltweit litten 2021 darunter – im Vergleich zum Vorjahr ein Zuwachs von 75 Prozent. Zur Einordnung: die branchenübergreifende durchschnittliche Angriffsrate liegt bei 66 Prozent.

Chester Wisniewski, Principal Research Scientist bei Sophos, ordnet die Ergebnisse ein: „Einzelhändler sind weiterhin von einer der höchsten Ransomware-Angriffsraten aller Branchen betroffen. Mit mehr als drei von vier attackierten Unternehmen im Jahr 2021 fällt ein Ransomware-Vorfall in die Kategorie ‚wann' und nicht ‚falls'. Sophos hat die Erfahrung gemacht, dass die Unternehmen, die sich erfolgreich gegen diese Angriffe wehren, nicht nur mehrstufige Schutzmechanismen einsetzen. Sie verlassen sich auch auf Experten, die für die Überwachung von Sicherheitsverletzungen geschult sind und aktiv Bedrohungen von Cyberkriminellen aufspüren, die auf Schleichfahrt im Unternehmensnetzwerk unterwegs sind. Die diesjährige Umfrage zeigt, dass nur etwa ein Viertel (28 Prozent, gegenüber 31 Prozent branchenübergreifend) der angegriffenen Einzelhandelsunternehmen in der Lage war, die Verschlüsselung ihrer Daten zu verhindern. Dies zeigt, dass ein großer Teil der Branche seine Sicherheitslage mit den richtigen Tools und entsprechend geschulten Sicherheitsexperten verbessern muss."

Lösegeldzahlung im Einzelhandel weniger als ein Drittel des weltweiten Durchschnitts
Mit dem Anstieg der Angriffe auf Einzelhandelsunternehmen wächst auch die durchschnittliche Lösegeldzahlung. 2021 lag diese bei 226.044 US-Dollar, ein Zuwachs von 53 Prozent im Vergleich zu 2020 (147.811 US-Dollar). Der Durchschnitt über alle Branchen hinweg betrug jedoch 812.000 US-Dollar. Der Einzelhandel zahlte damit weitaus weniger als alle Industriesegmente zusammengenommen. Eine Erklärung dafür liefert die nähere Betrachtung der Lösegeldhöhe: Mehr als ein Fünftel (22 Prozent) der Einzelhandelsunternehmen bezahlte Lösegeld in Höhe von weniger als 1.000 US-Dollar gezahlt, während mehr als zwei Drittel (70 Prozent) weniger als 100.000 US-Dollar ausgaben. Diese niedrigen Zahlungen tragen dazu bei, dass der Branchendurchschnitt im Vergleich zu vielen anderen Branchen niedrig ist.

„Es ist wahrscheinlich, dass unterschiedliche Bedrohungsgruppen verschiedene Branchen angreifen. Einige der kleinen Ransomware-Gruppen mit geringen Kenntnissen verlangen 50.000 bis 200.000 US-Dollar an Lösegeldzahlungen, während die größeren, raffinierteren Kriminellen mit wachsender Sichtbarkeit 1 Million US-Dollar oder mehr verlangen", so Wisniewski.
„Mit Initial Access Brokern (IAB) und Ransomware-as-a-Service (RaaS) ist es für Cyberkriminelle der unteren Level leider ein Leichtes, Netzwerkzugang und ein Ransomware-Kit zu kaufen, um ohne großen Aufwand einen Angriff zu starten. Einzelne Läden und kleine

Ketten werden eher von diesen kleineren, opportunistischen Angreifern ins Visier genommen", weiß Wisniewski über die Angriffsstrukturen zu berichten.

Weitere Ergebnisse der Ransomware-Studie zum Einzelhandel in 2021:

- Der Einzelhandel war zwar die am zweithäufigsten angegriffene Branche, doch die wahrgenommene Zunahme des Umfangs und der Komplexität von Cyberangriffen gegen dieses Segment lag leicht unter dem branchenweiten Durchschnitt (55 Prozent)

- 92 Prozent der Einzelhandelsunternehmen, die von Ransomware betroffen waren, gaben an, dass der Angriff ihre Betriebsfähigkeit beeinträchtigt hat, und 89 Prozent beklagten Geschäfts- und Umsatzeinbußen.

- Im Jahr 2021 beliefen sich die Gesamtkosten für Einzelhandelsunternehmen zur Behebung eines Ransomware-Angriffs auf 1,27 Mio. US-Dollar, ein Rückgang gegenüber 1,97 Mio. US-Dollar im Jahr 2020.

- Im Vergleich zu 2020 sank die Menge der nach Zahlung des Lösegelds wiederhergestellten Daten (von 67 Prozent auf 62 Prozent), ebenso wie der Prozentsatz der Einzelhandelsunternehmen, die alle ihre Daten zurückerhalten haben (von 9 Prozent auf 5 Prozent).

In Anbetracht der Umfrageergebnisse empfehlen die Experten von Sophos die folgenden Best Practices für Unternehmen in allen Branchen:

1. Installieren und pflegen Sie qualitativ hochwertige Schutzmaßnahmen an allen Stellen des IT-Ökosystems. Überprüfen Sie die Sicherheitskontrollen regelmäßig und stellen Sie sicher, dass sie weiterhin den Anforderungen des Unternehmens entsprechen.

2. Suchen Sie proaktiv nach Bedrohungen, um Angreifer zu identifizieren und zu stoppen, bevor sie Angriffe ausführen können. Stehen dem eigenen Team weder Zeit noch Fähigkeiten dafür zur Verfügung, sollten Sie Spezialisten wie ein MDR-Team (Managed Detection and Response) ins Boot holen.

3. Stärken Sie die IT-Umgebung, indem Sie nach wichtigen Sicherheitslücken suchen und diese schließen: nicht gepatchte Geräte, ungeschützte Rechner und offene RDP-Ports, zum Beispiel. Extended Detection and Response (XDR)-Lösungen sind für diesen Zweck ideal.

4. Spielen Sie das schlimmste Szenario einmal durch und halten Sie einen aktualisierten Aktions- und Wiederherstellungsplan für solch einen Fall bereit.

5. Erstellen Sie Backups und üben Sie deren Wiederherstellung, um minimale Unterbrechungen und Wiederherstellungszeiten zu gewährleisten.

Weitere Details über den Status von Ransomware im Einzelhandel 2022 finden Sie im angehängten PDF.

Über die Studie

„State of Ransomware in Retail 2022“ ist Teil der branchen- und sektorenübergreifenden State of Ransomware 2022 Studie, bei der 5.600 IT-Fachleute in mittelgroßen Organisationen (100-5.000 Mitarbeiter) in 31 Ländern zu ihren Erfahrungen über das vergangene Jahr hinweg befragt wurden, darunter 422 Befragte aus dem Einzelhandel.

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/
Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Anwendern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist in Oxford, U.K. Weitere Informationen unter http://www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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