Finanzsektor zahlt bei Ransomware-Angriffen Rekordsummen

Sophos zeichnet mit seinem jährlichen Ransomware-Report für unterschiedliche Branchen eine weltweite Bedrohungslandschaft ab.
Der Finanzsektor hat in der jüngsten Umfrage abermals unter mehr Angriffen zu leiden, mit enormen Wiederherstellungskosten. Ein positiver Aspekt: Backups und Cyberversicherungen helfen schnell.

Stetig wächst die Zahl der jährlichen Ransomware-Attacken auf Unternehmen des Finanzsektors: waren es in 2021 noch 34 Prozent, stieg die Zahl in 2022 auf 55 Prozent und liegt im 2023-Report bei 64 Prozent.

Der unbefugte Einstieg in die Systeme erfolgt zumeist über ausgenutzte Schwachstellen (40 Prozent). Kompromittierte Zugangsdaten sind hingegen nur zu 23 Prozent für Angriffe verantwortlich – eine der niedrigsten Raten im Finanzsektor. Hier könnte die Aufklärungsarbeit in der Belegschaft für ein höheres Sicherheitsbewusstsein gesorgt haben, oder auch strengere interne Sicherheitsmaßnahmen.

Die Verschlüsselung von Daten ist mittlerweile auch ein regulärer Teil einer Ransomware-Attacke. Im letzten Jahr waren davon 54 Prozent im Finanzbereich betroffen (weltweit 65 Prozent), 2023 bereits 81 Prozent (weltweit 76 Prozent) – die höchste Quote in den letzten drei Jahren. In jedem vierten Fall von Verschlüsselung wurden Daten auch gestohlen.

Cyberversicherungen beeinflussen den Verlauf der Attacke
Neben Eigenleistungen zu Prävention und Schadensbegrenzung haben auch Cyberversicherungen zunehmenden Einfluss auf den Verlauf von Ransomware-Attacken: In der Ransomware-Studie 2022 hatten 83 Prozent der Unternehmen der Finanzbranche eine Cyberversicherung abgeschlossen. In der Analyse 2023 zeigt sich nun: Wer eine singuläre Police besitzt, kann zu 99 Prozent seine verschlüsselten Daten wiederherstellen, bei Unternehmen, die über einen Cyber-Teilschutz im Rahmen einer bestehenden Versicherung verfügen, liegt dieser Wert bei 97 Prozent. Zum Vergleich: dies gelang ohne Versicherung mit 89 Prozent deutlich weniger Betroffenen.

Finanzsektor ist Superzahler
Auch die Zahlungsquote wächst mit dem Versicherungsschutz: 59 Prozent der Finanzunternehmen mit Cyber-Einzelpolice bezahlten das geforderte Lösegeld, von den Unternehmen mit allgemeiner Versicherungspolice taten dies 24 Prozent. Nur 11 Prozent der Dienstleister ohne Versicherungsschutz waren bereit, die Kassen der Cyberkriminellen zu füllen.

Die Anzahl der derjenigen Finanzunternehmen, die höhere Ransomware-Raten zahlten, stieg zudem drastisch: gaben 2021 nur 5 Prozent an, 1 Million US-Dollar oder mehr überwiesen zu haben, waren dies 2022 bereits 39 Prozent. Auf der anderen Seite blieb die Zahl der Unternehmen, die weniger als 100,000 US-Dollar zahlten mit rund 40 Prozent in 2022 und 2023 gleich.

Und noch ein Superlativ zeigt sich in der diesjährigen Ransomware-Studie für den Finanzsektor: mit durchschnittlichen Wiederherstellungskosten von 2,23 Millionen US-Dollar verglichen mit dem Branchendurchschnitt von 1,82 Millionen US-Dollar gehört der Finanzbereich zur absoluten Spitze weltweit. Zurückzuführen ist dieses Ergebnis vermutlich

auf die hohe Wachstumsrate an verschlüsselten Daten und der daraus resultierenden größeren Herausforderung, Attacken zu stoppen *bevor* Daten verschlüsselt werden.

Backups als Eigenstrategie bei Ransomware-Angriffen
Auch der zunehmend fragwürdige Sinn einer Lösegeld-Zahlung ist mittlerweile in vielen Unternehmen angekommen:
Hatte sich in 2022 die Zahl der Payments im Finanzbereich von 25 Prozent (2021) auf 52 Prozent nahezu verdoppelt, ging sie 2023 etwas auf 43 Prozent zurück. Womöglich auch ein Ergebnis der (belegten) Erkenntnisse, dass sich mit der Bezahlung nicht alle Daten wieder zurückbekommen lassen, aber auch, dass sich Unternehmen mit Hilfe von Backups unabhängig von den Erpressern machen. So vertrauten 2023 69 Prozent (2022: 66 Prozent) auf Backups zur Datenwiederherstellung (weltweit 70 Prozent). Sie verringern auch die Wiederherstellungskosten: im Durchschnitt liegen diese bei 1,58 Millionen US-Dollar – wer das Lösegeld zahlte, musste summa summarum aber rund 4,05 Millionen US-Dollar hinlegen, also gut das 2,5-Fache.
Und noch ein Pluspunkt spricht für Backups: Finanzunternehmen, die auf Backup setzen, erholten sich schneller von einem Angriff als diejenigen, die Lösegeld zahlten.
So waren von den angegriffenen Unternehmen 10 Prozent mit Backups und 7 Prozent mit Lösegeldzahlung nach weniger als einem Tag wieder betriebsfähig. Betrachtet man im Vergleich dazu den Zeitraum von einem Monat, so lief es bei 21 Prozent der Unternehmen, die auf ein Backup gesetzt hatten und bei 35 Prozent nach einer Lösegeldzahlung wieder rund.

Über die Studie
„The State of Ransomware in Financial Services 2023“ ist Teil der branchen- und sektorenübergreifenden Sophos-Studie „The State of Ransomware 2023“ bei der Anfang 2023 3.000 IT-Fachleute in mittelgroßen Organisationen (100-5.000 Mitarbeiter) in 14 Ländern zu ihren Erfahrungen über das vergangene Jahr hinweg befragt wurden.

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

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