Mehr als 1,7 Millionen Euro Wiederherstellungskosten – wenn Ransomware Finanzdienstleister weltweit trifft

Internationale Sophos Ransomware-Studie zeigt: Finanzdienstleister trifft Ransomware monetär besonders hart – gleichzeitig erweisen sie sich aber auch als widerstandsfähiger, da sie auf Backups setzen.
Und: DACH-Region scheint im weltweiten Vergleich etwas anders aufgestellt zu sein.

Im Durchschnitt 1,72 Millionen Euro müssen Finanzdienstleister weltweit aufwenden, um nach einer Ransomware-Attacke wieder arbeitsfähig zu werden. Das hat Sophos in seiner Analyse „The State of Ransomware in Financial Services 2021“ eruiert. Der globale Mittelwert aller Branchen liegt etwas darunter bei 1,59 Millionen Euro. Zugleich zeigen die Untersuchungen, dass der Finanzsektor gegenüber Ransomware-Angriffen recht widerstandsfähig ist: 62 Prozent der in 2020 attackierten Unternehmen weltweit konnten ihre verschlüsselten Daten aus Backups wiederherstellen. Aber: in der DACH-Region gelang dies nur 47 Prozent der befragten Unternehmen.

Einige Ergebnisse in der Übersicht:

- Ransomware traf in 2020 34 Prozent der befragten internationalen Finanzdienstleister, in der DACH-Region waren 46 Prozent betroffen.
- Während international 51 Prozent der befragten, betroffenen Unternehmen angaben, dass die Angreifenden ihre Daten verschlüsseln konnten, lag dieser Wert in DACH mit 61 Prozent deutlich höher.
- 25 Prozent international (und 29 Prozent in der DACH-Region) überwiesen das geforderte Lösegeld zur Datenbefreiung. Die zweitniedrigste Zahlungsquote aller Branchen, weltweit und über alle Branchen hinweg zahlen rund 32 Prozent der Unternehmen ein Lösegeld.
- 47 Prozent aller befragten Finanzdienstleister halten sich für potenziell gefährdet, ein Opfer von Ransomware zu werden, weil die Angriffe so raffiniert und schwer zu stoppen geworden sind. Finanzdienstleister der DACH-Region gehen gar zu 58 Prozent von diesem Szenario aus.
- 58 Prozent der befragten DACH-Finanzdienstleiter glauben in Zukunft ins Visier geraten zu können, weil bereits andere Unternehmen ihres Sektors Kontakt mit Ransomware hatten. Unternehmen anderer Regionen teilen diese Sorge zu 45 Prozent.

„Strikte Richtlinien im Finanzsektor erfordern starke Defensivmaßnahmen. Leider führen sie auch dazu, dass ein Ransomware-Angriff wahrscheinlich sehr kostspielig für die betroffenen Organisationen wird. Summiert man die Kosten von behördlichen Geldstrafen, Neuaufbau des IT-Systems und der Stabilisierung der Markt-Reputation – besonders bei Verlust von Kundendaten – erklären sich die gut 1,7 Millionen Euro der Sophos-Untersuchung,“ sagt John Shier, Senior Security Advisor bei Sophos.

DACH-Region setzt auf Technologie
Finanzdienstleister gehören zu den reguliertesten Branchen weltweit. Für sie gelten sehr viele Vorschriften, die exorbitant hohe Strafen für Nichteinhaltung und Datenpannen vorsehen. Darüber hinaus sind viele von ihnen dazu verpflichtet, Pläne zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung im Katastrophenfall zu erstellen, um jeglichen Schaden, der aus Cyberangriffen entstehen kann, zu minimieren.

Während international also viele gewissenhaft Backups machen, setzt die DACH-Region im Vergleich stärker auf Technologie-Lösungen. So geben international 66 Prozent und DACH-weit 71 Prozent an, IT-Sicherheit-trainiertes Personal zu haben, 59 Prozent weltweit und 79 Prozent in der DACH-Region setzen demnach Anti-Ransomware-Technologien ein. Entsprechende Versicherungen haben in der DACH-Region 71 Prozent der befragten Unternehmen, weltweit sind es 41 Prozent.

Zwei Faktoren, die Sorge bereiten

Die Tatsache, dass die kleine, aber aussagekräftige Menge von acht Prozent der Finanzdienstleister bereits Erfahrung mit „erpresserischer Ransomware“ gemacht hat, bietet laut Shier einen kleinen Anlass zur Sorge. Hierbei werden Daten nämlich nicht verschlüsselt, sondern gestohlen. „Und den Beraubten wird mit Online-Veröffentlichung gedroht, wenn sie sich gegen die Zahlungen wehren. Die bei Unternehmen aus dem Finanzsektor beliebten und gut gepflegten Backups bieten genau gegen diese Bedrohung nämlich keinen Schutz.“

Ebenfalls ein Grund zur Besorgnis bei den Sophos-Expert:innen bietet die Tatsache, dass 11 Prozent der Befragten (DACH: 36 Prozent) der Ansicht waren, gar nicht Opfer von Ransomware werden zu können, da sie „kein Ziel“ seien.

„Eine mehr als gefährliche Annahme,“ so John Shier, wirklich jeder könne zur Zielscheibe eines Ransomware-Angriffs werden. „Der beste Weg ist, zunächst einmal anzunehmen, dass man irgendwann ins Visier von Cyberkriminellen gerät und entsprechende Abwehr zu implementieren, denn für den Finanzsektor steht schlichtweg zu viel auf dem Spiel, als dass er ohne Abwehrmechanismen gegen Cyberattacken agieren könnte. Während Unternehmen deshalb weiterhin bei Backups und Wiederherstellungsplan am Ball bleiben sollten, ist es außerdem wichtig zugleich ihre Anti-Ransomware Defensive auszuweiten – am besten durch Kombination von Technologie mit Menschen-geführtem Threat Hunting.“

Zur Studie „The State of Ransomware in Financial Services 2021“

Sophos befragte rund 5.400 IT-Entscheider, darunter 550 in Finanzdienstleistern, in 30 Ländern aus Europa, Afrika, Amerika, Zentralasien sowie dem Asia-Pazifik-Raum und Mittleren Osten.

Neu: 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