Kostenexplosion nach Ransomware-Attacken: Gesundheitswesen muss tief in die Tasche greifen

Die Healthcare-Branche überrascht: entgegen dem weltweiten Trend ist in diesem Sektor ein Ransomware-Rückgang zu sehen. Jedoch zu einem sehr hohen (Wiederherstellungs-)Preis. Und: Backups sind ein Gamechanger.

Sophos veröffentlicht seinen aktuellen Ransomware-Report für den Gesundheitssektor. The State of Ransomware in Healthcare 2023 bildet auch die generelle Entwicklung in der Cyberkriminalität ab: die Angriffe sind hochkomplex und gezielt, Datenverschlüsselungen nahezu immer das Ziel und damit einhergehend eine Kostenexplosion bei der Wiederherstellung zur Betriebsfähigkeit.

Im Gegensatz zum weltweiten Trend verzeichnet die Healthcare-Branche einen Rückgang an Ransomware-Attacken von 66 Prozent im Jahr 2022 auf 60 Prozent im Jahr 2023.

Kompromittierte Zugangsdaten als Einfallstor
Am häufigsten ermöglichen es kompromittierte Zugangsdaten (32 Prozent) den Kriminellen in die Systeme einzudringen. Das Ausnutzen von Schwachstellen (29 Prozent) folgt an zweiter Stelle. Auch auf E-Mail basierende Angriffe, zum Beispiel mit schadhaften E-Mails oder Phishing, sind für über ein Drittel (36 Prozent) aller Attacken in der Gesundheitsbranche verantwortlich. Branchenübergreifend liegt diese Vorgehensweise bei 30 Prozent.

Knapp Dreiviertel der Betriebe in diesem Sektor verzeichnen eine Verschlüsselung ihrer Daten – die höchste Quote in den letzten drei Jahren. In 37 Prozent dieser Fälle wurden Daten auch gestohlen. Sämtliche Healthcare-Organisationen erhielten ihre verschlüsselten Daten zurück. Der weltweite Durchschnitt liegt hier bei 97 Prozent.

Auf der Kostenseite eines Ransomware-Angriffs stehen einerseits die Lösegeldzahlungen und andererseits die Aufwendungen zur Wiederherstellung der Systeme und Daten, damit die Organisationen wieder voll betriebsfähig sind.

Lösegeld
Der Healthcare-Bereich weicht nur wenig vom weltweiten, branchenübergreifenden Verhalten ab: 42 Prozent (gegenüber 46 Prozent transsektoral) bezahlten die Lösegeldforderungen, um ihre verschlüsselten Daten zu befreien. 73 Prozent (gegenüber 70 Prozent transsektoral) vertrauten ihren Backups zur Wiederherstellung.

Die Rate der Ransomware-Zahlungen insgesamt sank erheblich von 61 Prozent (2022) auf 42 Prozent (2023). Der Gebrauch von Backups blieb nahezu gleich (72 Prozent 2022; 73 Prozent 2023).

Unternehmen mit einer Cyber-Versicherung waren eher zu einer Lösegeld-Zahlung bereit als Unversicherte. Mit einer eigenständigen Police zahlten 53 Prozent der Healthcare-Organisationen. Im Gegensatz zu 34 Prozent der Unternehmen, deren Versicherungsschutz unter anderem auch den Cyberbetrug deckt.

Wiederherstellungskosten
Mit einem Anstieg von 1,85 Millionen US-Dollar in 2022 auf 2,2 Millionen US-Dollar mussten Healthcare-Unternehmen 2023 deutlich tiefer in die Tasche greifen, um wieder betriebsfähig zu werden. Zum Vergleich: 2021 reichten noch 1,27 Millionen US-Dollar. Innerhalb von zwei Jahren haben sich die Wiederherstellungskosten also fast verdoppelt. Zwei Gründe lassen

sich dafür ausmachen: zum einen die Zunahme verschlüsselter Daten bei einem Cyberangriff auf Healthcare-Organisationen, und zum anderen die mangelnden Fähigkeiten, eine Attacke zu stoppen, bevor die Daten verschlüsselt werden.

Einkommenseinbußen
Für 85 Prozent der Organisationen aus dem privaten Gesundheitswesen, die von Ransomware betroffen waren, bedeuten die Attacke einen Einkommensverlust. Damit sind die Unternehmen nicht allein, wie der weltweite, branchenübergreifende Wert von 84 Prozent zeigt.

Mit Backups günstiger und schneller wieder auf den Beinen
Im Vergleich zur Lösegeldzahlung kommen Unternehmen der Healthcare-Branche mit eigenen Backups zur Wiederherstellung günstiger weg: hier fallen „nur" 2,11 Millionen US-Dollar an, gegenüber 2,58 Millionen US-Dollar bei der Lösegeld-Variante. Backups haben aber noch einen weiteren Vorteil: die Betriebe, die daraus ihre Daten wiederherstellen konnten, erholten sich weitaus schneller als diejenigen, die den Entschlüsselungscode durch die Lösegeldzahlung erhielten. 27 Prozent der Befragten mit Backups benötigten mehr als einen Monat zur wiederhergestellten, kompletten Betriebsfähigkeit; bei den Lösegeldzahlern waren dies 40 Prozent.

Über die Studie
Die Daten der Studie „State of Ransomware 2023" stammen aus einer herstellerunabhängigen Umfrage unter 3.000 Führungskräften im Bereich Cybersicherheit/ IT, darunter 400 aus dem Bildungssektor, die zwischen Januar und März 2023 durchgeführt wurde. Die Befragten stammen aus 14 Ländern in Nord- und Südamerika, EMEA und dem asiatisch-pazifischen Raum. Die interviewten Unternehmen beschäftigen zwischen 100 und 5.000 Mitarbeiter und generieren einen Umsatz zwischen weniger als 10 Millionen und mehr als 5 Milliarden US-Dollar.

Die Sophos-Studie „State of Ransomware 2023" steht unter sophos.com als Download zur Verfügung.

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, 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