Sophos Ransomware-Studie im Gesundheitswesen: Erpressungen auf Höchststand, Lösegeldforderungen gesunken, Stress bei den Teams

292 Führungskräfte aus den Bereichen IT und Cybersicherheit zu Ursachen und Auswirkungen von Ransomware-Attacken auf Menschen und Systeme im Gesundheitswesen.

In der aktuellen jährlichen Studie „*State of Ransomware Healthcare 2025*“ untersuchte der Cybersicherheitsanbieter Sophos die Erfahrungen mit Ransomware global bei 292 Gesundheitsdienstleistern. Der Bericht beleuchtet Ursachen, Folgen und die Entwicklung dieser Angriffe. Zudem gibt die Studie Auskunft über bisher unerforschte Bereiche: Dazu gehören organisatorische Faktoren, durch die Gesundheitsorganisationen angreifbar wurden, sowie belastende Auswirkungen auf die IT- und Cybersicherheitsteams.

Schwachstellen und Kapazitätsprobleme sind die Hauptursachen für Angriffe
Zum ersten Mal seit drei Jahren nannten die Befragten im Gesundheitssektor ausgenutzte Schwachstellen mit 33 Prozent als häufigste technische Ursache für Angriffe. Damit überholt diese Art der Attacken die Angriffe aufgrund von kompromittierten Anmeldedaten (18 Prozent), die 2023 und 2024 die häufigste Ursache darstellten.

Mehrere organisatorische Faktoren tragen dazu bei, dass Gesundheitsdienstleister Opfer von Ransomware werden. Mit 42 Prozent ist der häufigste Grund der Mangel an Personal beziehungsweise eine unzureichende Anzahl von Cybersicherheitsexperten, die Systeme zum Zeitpunkt des Angriffs überwachten. Dicht dahinter folgen bekannte Sicherheitslücken, die bei 41 Prozent der Angriffe eine Rolle spielten.

Datenverschlüsselung auf Fünfjahrestief, Angriffsstopps auf Fünfjahreshoch
Die Verschlüsselung von Daten im Gesundheitswesen durch Cyberkriminelle ist auf den niedrigsten Stand seit fünf Jahren gesunken. Nur 34 Prozent der Angriffe führte zu einer Verschlüsselung der Daten – der zweittiefste Wert in der diesjährigen Umfrage und weniger als die Hälfte der 74 Prozent aus dem Jahr 2024. Parallel dazu erreichte der Anteil der Angriffe, die vor der Verschlüsselung gestoppt wurden, mit 53 Prozent einen Fünfjahreshoch. Dies deutet darauf hin, dass Gesundheitsorganisationen ihre Abwehrmaßnahmen verstärken.

Erpressungen auf Allzeithoch
Die Angreifer passen sich jedoch an: Der Anteil der Organisationen im Gesundheitswesen, die von reinen Erpressungsangriffen betroffen waren und bei denen keine Daten verschlüsselt jedoch Lösegeld gefordert wurde, verdreifachte sich von nur 4 Prozent im Jahr 2022/23 auf 12 Prozent. Dies ist der höchste jemals verzeichnete Wert in der Studie – vermutlich, weil medizinische Daten (z. B. Patientendaten) besonders sensibel sind.

Lösegeldzahlungen sinken, das Vertrauen in Backups schwindet
Im Jahr 2025 zahlten nur noch 36 Prozent der Gesundheitsorganisationen das geforderte Lösegeld. Dies ist ein deutlicher Rückgang insgesamt, lag dieser Wert im Jahre 2022 z.B. noch bei 61 Prozent. Damit gehört dieser Sektor zu den vier Sektoren, die am seltensten über Lösegeldzahlungen ihre Daten wiederherstellten. Gleichzeitig sank auch die Nutzung von Backups zur Datenrekonstruktion nach einem Angriff auf 51 Prozent. Dies könnte auf eine stärkere Widerstandsfähigkeit aber auch mangelndes Vertrauen in die Backup-Resilienz hinweisen.

Lösegeldforderungen, Zahlungen und Wiederherstellungskosten sinken drastisch
Die Höhe der Lösegelder im Gesundheitswesen hat sich drastisch verändert:

- Die durchschnittlichen Lösegeldforderungen sanken um 91 Prozent auf 295.000 Euro im Vergleich zu 3.4 Millionen Euro in der Vorjahresstudie.
- Die tatsächlich gezahlten Beträge sind von knapp 1.5 Millionen Euro auf nur noch 129.000 Euro zurückgegangen. Dies ist der niedrigste Wert aller in der Studie erfassten Branchen.

Der Rückgang spiegelt einen starken Einbruch bei Forderungen und Zahlungen in mehrstelliger Millionenhöhe wider. Gleichzeitig stiegen die Forderungen im mittleren Bereich 860.000 bis 4.3 Millionen Euro.

Die durchschnittlichen Wiederherstellungskosten (ohne Lösegeldzahlungen) sind auf dem niedrigsten Stand seit drei Jahren und sanken um 60 Prozent auf rund 877.000 Euro, im Vergleich zu rund 2.2 Millionen Euro in der Vorjahresstudie. Insgesamt deuten die Ergebnisse ein robusteres und effizienteres Gesundheitswesen hin, das schwieriger auszubeuten ist, auch wenn kleinere Fälle häufiger vorkommen.

Druck durch Führungsetagen, Angst, Stress, Schuldgefühle
Die Umfrage macht darüber hinaus deutlich, dass die Verschlüsselung von Daten bei einem Ransomware-Angriff auch erhebliche Auswirkungen auf die Cybersicherheitsteams im Gesundheitswesen hat. 39 Prozent der Befragten gaben an, dass der Druck seitens der Führungsetage gestiegen ist. Weitere Auswirkungen sind unter anderem

- Zunehmende Angst oder Stress vor zukünftigen Angriffen (37 Prozent)
- Veränderte der Prioritäten oder Schwerpunkte (37 Prozent)
- Schuldgefühle, weil der Angriff nicht verhindert werden konnte (32 Prozent)

Über die Studie
Die Studie basiert auf den Ergebnissen einer unabhängigen Umfrage, die von Sophos unter 3.400 IT-/ Cybersicherheitsverantwortlichen in 17 Ländern in Amerika, EMEA und im asiatisch-pazifischen Raum, darunter 292 aus dem Gesundheitswesen, durchgeführt wurde. Alle Befragten vertreten Unternehmen mit 100 bis 5.000 Mitarbeitern. Die Umfrage wurde zwischen Januar und März 2025 vom Forschungsunternehmen Vanson Bourne durchgeführt. Die Teilnehmer wurden gebeten, ihre Antworten auf der Grundlage ihrer Erfahrungen im vergangenen Jahr zu geben.

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