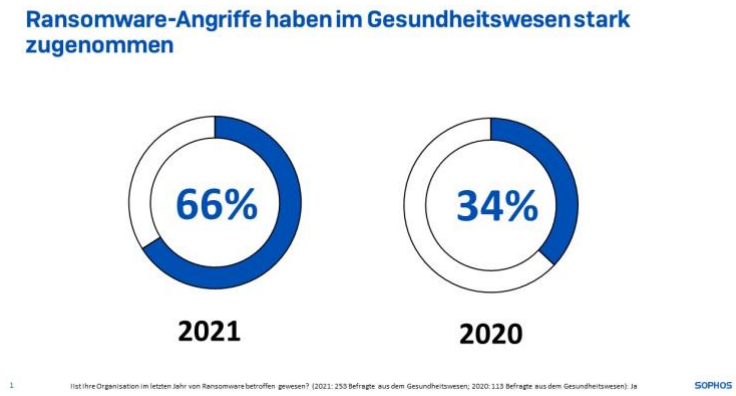
Starker Trend in 2021:
Organisationen im Gesundheitswesen zu 94% stärker von Ransomware betroffen

Angriffe steigen deutlich, gleichzeitig sind Organisationen im Gesundheitswesen besser in der Lage, mit den Folgen umzugehen
Der Gesundheitssektor zahlt am häufigsten Lösegeld, im Branchenvergleich jedoch die niedrigsten Summen
Mehr Gesundheitsorganisationen entscheiden sich für Cyberversicherungen, stellen aber fest, dass es schwieriger geworden ist, Versicherungsschutz zu bekommen

Wiesbaden, 23.Juni 2022 Sophos hat seinen Branchenanalyse „The State of Ransomware in Healthcare 2022" veröffentlicht. Die Ergebnisse beschreiben einen weltweiten Anstieg der Ransomware-Angriffe auf diesen Sektor von 94 %. So war das Gesundheitswesen im Jahr 2021 zu 66 % betroffen, wohingegen im Jahr zuvor dieser Wert noch bei 34 % lag.



Trotz dieser dynamischen Entwicklung zeigt sich auch ein positiver Aspekt: die Organisationen des Gesundheitswesens sind den Umfragedaten zufolge immer besser in der Lage, mit den Folgen von Ransomware-Angriffen umzugehen. Der Bericht zeigt, dass 99 % der von Ransomware betroffenen Organisationen zumindest einen Teil ihrer Daten zurückerhalten haben, nachdem die Cyberkriminellen sie während der Angriffe verschlüsselt hatten.

Weitere Auswirkungen von Ransomware auf den Gesundheitssektor weltweit:

- Organisationen des Gesundheitswesens hatten mit 1,85 Millionen US-Dollar die zweithöchsten durchschnittlichen Wiederherstellungskosten für Ransomware und benötigten im Durchschnitt eine Woche, um sich von einem Angriff zu erholen
- Basierend auf ihren eigenen Erfahrungen glauben 67 % der Unternehmen des Gesundheitswesens, dass Cyberangriffe komplexer geworden sind. Dies ist der höchste Prozentsatz im weltweiten Branchenvergleich.
- Unternehmen des Gesundheitswesens zahlen zwar am häufigsten Lösegeld (61 %), aber im Vergleich zum weltweiten Durchschnitt von 812.000 US-Dollar (über alle in der Umfrage erfassten Sektoren hinweg) mit 197.000 US-Dollar das niedrigste Durchschnittslösegeld.
- Von den Unternehmen, die das Lösegeld gezahlt haben, erhielten nur 2 % alle ihre Daten zurück

- 61 % der Angriffe führten zu einer Verschlüsselung, 4 % weniger als der weltweite Durchschnitt (65 %)

Mehr Gesundheitsorganisationen (78 %) entscheiden sich jetzt für eine Cyberversicherung, aber 93 % der Organisationen mit Versicherungsschutz berichten, dass es im letzten Jahr schwieriger geworden ist, Versicherungsschutz zu erhalten. Da Ransomware der Hauptgrund für Versicherungsansprüche ist, gaben 51% der Befragten an, dass ein höheres Maß an Cybersicherheit erforderlich ist, um sich für eine Versicherung zu qualifizieren. Dies stellt eine Belastung für Gesundheitsorganisationen mit geringeren Budgets und weniger technischen Ressourcen dar.

Daten im Gesundheitswesen besonders attraktiv für Cyberkriminelle
„Ransomware im Gesundheitswesen ist in Bezug auf Schutz und Wiederherstellung differenzierter als in anderen Branchen", sagt John Shier, Senior Security Experte bei Sophos. „Die Daten, die Unternehmen im Gesundheitswesen nutzen, sind äußerst sensibel und wertvoll, was sie für Angreifer sehr attraktiv macht. Darüber hinaus bedeutet die Notwendigkeit eines effizienten und weit verbreiteten Zugriffs auf diese Art von Daten – damit medizinisches Fachpersonal die richtige Pflege leisten kann –, dass typische Zwei-Faktor-Authentifizierung und Zero-Trust-Verteidigungstaktiken nicht immer durchführbar sind. Dies macht Organisationen des Gesundheitswesens besonders verwundbar, und wenn sie betroffen sind, entscheiden sie sich möglicherweise dafür, Lösegeld zu zahlen, um Zugang zu wichtigen, oft lebensrettenden Patientendaten zu erhalten." Aufgrund dieser einzigartigen Faktoren müssten Organisationen des Gesundheitswesens ihren Schutz vor Ransomware ausbauen, indem sie Sicherheitstechnologien mit einer von Menschen geführten Bedrohungsjagd kombinieren, um sich gegen die modernen Cyberangreifer zu verteidigen, so der Experte weiter.

Sophos empfiehlt folgende Schritte für eine bessere Sicherheit:

- Installation und Pflege von hochwertigen Schutzmaßnahmen an allen Stellen der Unternehmensumgebung. Regelmäßige Prüfung der Sicherheitskontrollen und Anpassung an die Anforderungen des Unternehmens.
- Härtung der IT-Umgebung durch Aufspüren und Schließen der wichtigsten Sicherheitslücken: ungepatchte Geräte, ungeschützte Rechner und offene Ports des Remote Desktop Protocol. Extended Detection and Response (XDR)-Lösungen sind ideal, um diese Lücken zu schließen
- Erstellung von Backups und Training der Wiederherstellung der Daten, damit das Unternehmen so schnell wie möglich und mit minimalen Unterbrechungen den Betrieb wieder aufnehmen kann.
- Proaktive Bedrohungssuche, um Angreifer zu identifizieren und zu stoppen, bevor sie ihren Angriff ausführen können. Wenn das interne Team nicht die Zeit oder die Fähigkeiten hat, dies selbst zu tun, ist es ratsam externe Spezialisten für Managed Detection and Response (MDR) zu beauftragen.
- Mit einem Plan auf den Worst Case vorbereitet sein. Wissen, was zu tun ist, wenn ein Cybervorfall eintritt, und den Plan auf dem neuesten Stand halten

Für die weltweite Studie „State of Ransomware in Healthcare 2022" wurden 5.600 IT-Experten, darunter 381 Befragte aus dem Gesundheitswesen, in mittelgroßen Unternehmen (100-5.000 Mitarbeiter) in 31 Ländern befragt. Für die DACH-Region standen 63 deutsche, 16 österreichische und 8 schweizer IT-Leitungen Rede und Antwort.

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