Kritische Infrastrukturbereiche im Visier von Ransomware

Sophos-Report „The State of Ransomware in Critical Infrastructure 2024“: Unternehmen der KRITIS-Bereiche Energie und Wasser haben eine mit 67 Prozent deutlich höhere Angriffsrate als der weltweite Durchschnitt (59 Prozent). 55 Prozent benötigten mehr als einen Monat für die Wiederherstellung nach der Attacke. Mit einem Wert von durchschnittlich 2,8 Millionen Euro haben sich die Wiederherstellungskosten nach Ransomware-Angriffen bei den befragten KRITIS-Unternehmen zudem vervierfacht.

Wiesbaden, 25. Juli 2024 – Sophos hat die Ergebnisse seiner Branchenstudie mit dem Titel „The State of Ransomware in Critical Infrastructure 2024“ veröffentlicht, in dem die Bereiche Wasser, Energie, Öl und Gas, die zu den sechzehn von der CISA definierten kritischen Infrastruktursektoren gehören, näher beleuchtet werden.
Die Ergebnisse aus der Befragung von weltweit 5.000 Führungskräften aus der Cybersicherheit/IT, worunter 275 dem Bereich KRITIS zuzuordnen sind, belegen, dass sich die durchschnittlichen Wiederherstellungskosten für die beiden Infrastruktursektoren Energie und Wasser im letzten Jahr auf 2,8 Millionen Euro vervierfacht haben. Damit sind die Kosten in diesem Sektor rund viermal so hoch wie der globale und branchenübergreifende Mittelwert (Median).

„Cyberkriminelle konzentrieren sich auf Industriebereiche, in denen sie den größten Schmerz und die meisten Störungen verursachen. Gleichzeitig fordert die Öffentlichkeit speziell im KRITIS-Umfeld schnelle Lösungen, um die Dienste wiederherzustellen – wenn nötig auch mit der Bezahlung von Lösegeldern. Dies macht Versorgungsunternehmen zu bevorzugten Zielen für Ransomware-Angriffe“, sagt Chester Wisniewski, Global Field CTO. „Leider sind Versorgungsunternehmen in vielerlei Hinsicht anfällig für Angriffe, unter anderem aufgrund der hohen Anforderungen an Verfügbarkeit und einer auf die physische Sicherheit ausgerichteten technischen Denkweise. Hinzu kommen teils ältere Technologien ohne moderne Sicherheit und der allgemeine Mangel an IT-Security-Personal.“

Fast die Hälfte der Angriffe erfolgte durch ausgenutzte Schwachstellen
Zusätzlich zu den steigenden Wiederherstellungskosten stieg auch der Mittelwert (Median) der Lösegeldzahlungen für Organisationen der beiden Sektoren Energie und Wasser auf mehr als 2,3 Millionen Euro im Jahr 2024. Das ist um rund 460.000 Euro höher als der globale, sektorübergreifende Mittelwert. Die beiden Sektoren meldeten mit 67 Prozent zudem die zweithöchste Rate an Ransomware-Angriffen im Jahr 2024 – gemessen am branchenübergreifenden Durchschnitt von 59 Prozent. Darüber hinaus begannen 49 Prozent der Ransomware-Angriffe auf diese beiden kritischen Infrastruktursektoren mit einer ausgenutzten Sicherheitslücke.

Die Energie- und Wasserversorger melden zudem zunehmend längere Wiederherstellungszeiten. Nur 20 Prozent der Unternehmen, die von Ransomware betroffen waren, konnten sich im Jahr 2024 innerhalb einer Woche oder weniger erholen, verglichen mit 41 Prozent im Jahr 2023 und 50 Prozent im Jahr 2022. Fünfundfünfzig Prozent benötigten mehr als einen Monat für die Wiederherstellung, gegenüber 36 Prozent im Jahr 2023. Im Vergleich dazu benötigten über alle Sektoren hinweg nur 35 Prozent der Unternehmen mehr als einen Monat für die Wiederherstellung.

Höchste Rate an kompromittierten Backups, steigende Wiederherstellungszeiten
Unter Betrachtung der Möglichkeiten der schnellen Wiederherstellung, spielen unversehrte Backups eine entscheidende Rolle. Die beiden kritischen Infrastruktursektoren meldeten im

Vergleich zu den anderen untersuchten Branchen die höchste Rate an kompromittierten Backups (79 Prozent) und die dritthöchste Rate an bösartiger Verschlüsselung (80 Prozent).

„Eine steigende Zahl (61 Prozent) zahlte das Lösegeld als Teil ihrer Wiederherstellungsstrategie und dennoch dauerte die Wiederherstellung länger. Die Zahlung hoher Lösegelder ermutigt die Cyberkriminellen nicht nur zu weiteren Angriffen, die Unternehmen erreichen zudem damit nicht das angestrebte Ziel einer kürzeren Wiederherstellungszeit“, so Wisniewski. „Versorgungsunternehmen sollten aktiv Maßnahmen ergreifen, um ihre Fernzugangs- und Netzwerksysteme auf Schwachstellen zu überwachen. Sie sollten sicherstellen, dass sie rund um die Uhr Überwachungs- und Reaktionsmöglichkeiten haben, um Ausfälle zu minimieren und Wiederherstellungszeiten zu verkürzen. Reaktionspläne für Vorfälle sollten im Voraus geplant werden, genau wie für Brände, Überschwemmungen, Wirbelstürme und Erdbeben, und regelmäßig geprobt werden.“

Über die Studie:
Die Daten für den Bericht „State of Ransomware in Critical Infrastructure 2024“ stammen von 275 Befragten aus den Bereichen Energie, Öl und Gas sowie Versorgungsunternehmen, die zu den Sektoren Energie und Wasser. Die Ergebnisse dieser Branchenumfrage sind Teil einer breiteren, unabhängigen Umfrage unter 5.000 Führungskräften aus dem Bereich Cybersicherheit/IT, die zwischen Januar und Februar 2024 in 14 Ländern und 15 Branchen durchgeführt wurde.

Der vollständige Report „The State of Ransomware in Critical Infrastructure 2024“ steht hier zum Download bereit.

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

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter fortschrittlicher Lösungen zur Abwehr von Cyberangriffen, darunter Managed Detection and Response (MDR) sowie Incident Response Services. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 600.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr. Die Dienste und Produkte von Sophos sind über die cloudbasierte Management-Konsole Sophos Central verbunden und werden vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen.
Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung. Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.
Weitere Informationen unter: www.sophos.de

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