Sophos State of Ransomware 2024:
Teurer geht immer: Lösegeldzahlungen steigen um 500 Prozent

Zahl der Ransomware-Angriffe steigt in Deutschland minimal und sinkt weltweit leicht.
Wiederherstellungskosten erreichen mit gut 2,5 Millionen Euro einen Höchststand
Deutsche Unternehmen zahlten weniger häufig, dafür aber mehr Lösegeld

Wiesbaden, 30. April 2024 – Sophos veröffentlicht heute die globale Studie „State of Ransomware 2024“, laut der die durchschnittliche Lösegeldzahlung im vergangenen Jahr um 500 Prozent gestiegen ist. Im internationalen Vergleich melden Organisationen, die Lösegeld gezahlt haben, eine durchschnittliche Zahlung von 1.86.260 Euro (2 Millionen US-Dollar), gegenüber 372.520 Euro (400.000 US-Dollar) im Jahr 2023. Deutsche Unternehmen griffen sogar noch tiefer in die Tasche, hier lag die mittlere Lösegeldzahlung bei 5.14 Millionen Euro (5.5 Millionen US-Dollar).
Lösegeldzahlungen sind jedoch nur ein Teil der Kosten bei einem Cyberangriff. Ohne diesen Faktor beliefen sich die weltweiten durchschnittlichen Kosten für die Wiederherstellung auf 2.542.449 Euro (2,73 Millionen US-Dollar), was einem Anstieg von 847.783 Euro gegenüber den 1.694.966 Euro (1,82 Millionen US-Dollar) vom Vorjahr entspricht.

Die durchschnittlichen Kosten, die deutschen Unternehmen ohne die Berücksichtigung von Lösegeldzahlungen nach einem Ransomware-Angriff zusätzlich entstehen, belaufen sich auf 2.054.987 Euro (2,20 Millionen US-Dollar). Darin enthalten sind zum Beispiel Kosten für Ausfallzeiten, Personalzeit, Gerätekosten, Netzwerkkosten oder entgangene Geschäftschancen.
Was die Zahlung von Lösegeld betrifft, sind deutsche Unternehmen trotz im weltweiten Vergleich höherer Ausgaben aber offenbar zurückhaltender geworden: 42 Prozent der Unternehmen, deren Daten verschlüsselt wurden, zahlten das Lösegeld. Dieser Wert liegt unter dem des Vorjahres (44 Prozent) sowie unter dem weltweiten Durchschnitt von 56 Prozent im aktuellen Jahr.

Rückgang weltweit, minimale Steigerung in Deutschland
Trotz der steigenden Lösegelder deutet die diesjährige Umfrage auf einen leichten Rückgang der Zahl der Ransomware-Angriffe im weltweiten Vergleich hin: 59 Prozent der Unternehmen sind weltweit betroffen; im Jahr 2023 lag diese Zahl bei 66 Prozent. Während die Wahrscheinlichkeit einer Ransomware-Attacke mit dem Umsatz steigt, werden selbst die kleinsten Unternehmen (weniger als 9.313.000 Euro / 10 Millionen US-Dollar Umsatz) immer noch regelmäßig angegriffen, wobei mit 47 Prozent knapp die Hälfte der Unternehmen im letzten Jahr von Ransomware betroffen war.

Deutsche Unternehmen waren zu knapp einem Prozent mehr als im Report des vergangenen Jahres Opfer von Ransomware. Dies bedeutet aber auch einen Rückgang gegenüber den 67 Prozent aus 2022. Im aktuellen Vergleich liegt Deutschland knapp unter dem weltweiten Durschnitt von 59 Prozent der Befragten. In deutschen Organisationen waren bei erfolgreichen Angriffen 54 Prozent der Computer betroffen, was etwas über dem weltweiten Durchschnitt von 49 Prozent liegt.

Fünf europäische Länder vermelden Steigerungen
Insgesamt meldeten neun Länder eine niedrigere Angriffsrate als im Jahr 2023. Die fünf Länder, die eine höhere Angriffsrate als im Jahr 2023 meldeten, liegen alle in Europa:

Österreich, Frankreich, Deutschland, Italien und das Vereinigte Königreich. Der Anstieg in Deutschland stellte sich, wie eingangs beschrieben, aber nur minimal dar und betrug weniger als 1 Prozent. Die Steigerungen in Europa könnten auf eine Zunahme der Angriffe auf europäische Organisationen zurückzuführen sein oder darauf, dass die europäischen Verteidigungssysteme weniger gut mit dem sich verändernden Verhalten der Angreifer Schritt halten konnten als in anderen Regionen.

Frankreich meldete 2024 mit 74 Prozent die höchste Rate an Ransomware-Angriffen, gefolgt von Südafrika (69 Prozent) und Italien (68 Prozent). Umgekehrt meldeten die Befragten in Brasilien (44 Prozent), Japan (51 Prozent) und Australien (54 Prozent) die niedrigsten Angriffsraten.

„Ransomware-Angriffe sind nach wie vor die größte Bedrohung und treiben die Wirtschaft der Cyberkriminalität an. Die Ransomware-Landschaft bietet dabei für jeden Cyberkriminellen etwas, unabhängig von seinen Fähigkeiten. Während sich einige Gruppen auf Lösegelder in Höhe von mehreren Millionen Dollar konzentrieren, gibt es andere, die sich mit geringeren Summen zufriedengeben und dieses ‚Manko' durch schiere Masse ausgleichen," sagt John Shier, Field CTO, Sophos.

Schwachstellen weltweit häufigste Ursache, Österreich und Schweiz mit Abweichungen

99 Prozent der Unternehmen, die von Ransomware betroffen waren, konnten die Ursache des Angriffs identifizieren, wobei ausgenutzte Schwachstellen (32 Prozent) das zweite Jahr in Folge die am häufigsten festgestellte Ursache für einen Angriff waren. Es folgen kompromittierte Zugangsdaten (29 Prozent) und schädliche E-Mails (23 Prozent). Dies deckt sich mit den Ergebnissen der jüngsten Active Adversary-Studie von Sophos, in der die Reaktion auf Vorfälle vor Ort untersucht wurde.

Auch in Deutschland zeigt sich eine ähnliche Konstellation: hierzulande waren ausgenutzte Sicherheitslücken zu 34 Prozent das häufigste Einfallstor für Ransomware, kompromittierte Anmeldedaten stellten mit 28 Prozent den zweithäufigsten Angriffsvektor dar. Anders ist es in Österreich und der Schweiz – bei unseren Nachbarn gelangte Ransomware am häufigsten über den Weg der kompromittierten Zugangsdaten in Unternehmen, gefolgt von Schwachstellen.

Unternehmen, bei denen der Angriff statt mit kompromittierten Anmeldeinformationen mit ausgenutzten Schwachstellen begann, berichten schwerwiegende Auswirkungen auf ihre Organisation. Dazu gehören eine höhere Rate an kompromittierten Datensicherungen (75 Prozent), Datenverschlüsselung (67 Prozent) und der Bereitschaft, das Lösegeld zu zahlen (71 Prozent). Die befragten Unternehmen erfahren auch erheblich größere finanzielle und betriebliche Auswirkungen: Die durchschnittlichen Wiederherstellungskosten beliefen sich auf 3.344.024 Euro (3,58 Millionen US-Dollar) im Vergleich zu 2.409.939 Euro (2,58 Millionen US-Dollar), wenn ein Angriff mit kompromittierten Anmeldeinformationen begann, und ein größerer Anteil der angegriffenen Unternehmen benötigte mehr als einen Monat für die Wiederherstellung.

In 94 Prozent der Ransomware-Angriffe auf deutsche Organisationen versuchten Cyberkriminelle während des Angriffs zusätzlich auch Backups zu kompromittieren. 63 Prozent dieser Versuche, waren erfolgreich, was etwas über dem weltweiten Durchschnitt von 57 Prozent liegt. Bei 32 Prozent der Vorfälle (im Vorjahr 30 Prozent), bei denen Daten verschlüsselt wurden, sind zusätzlich auch Daten gestohlen worden.

Weitere wichtige Ergebnisse der Studie für Deutschland

- **Zahlung von Lösegeld:** Weniger als ein Viertel (24 Prozent) derjenigen, die das Lösegeld zahlen, überweisen den ursprünglich geforderten Betrag. 44 Prozent der Befragten zahlen weniger als die ursprüngliche Forderung.
    - Die durchschnittliche Lösegeldzahlung beträgt 94 Prozent der ursprünglichen Lösegeldforderung.
    - In 82 Prozent der Fälle stammt die Finanzierung des Lösegelds aus mehreren Quellen. 40 Prozent der gesamten Lösegeldfinanzierung kommen von den Organisationen selbst und 23 Prozent von Versicherungsanbietern.
- **Backups sind meist verwendete Methode zur Wiederherstellung von Daten**. 75 Prozent der deutschen Befragten, deren Daten verschlüsselt waren, nutzten diese Methode. Dies ist ein leichter Rückgang gegenüber den 78 Prozent, die in unserer Umfrage von 2023 auf Backups zurückgriffen.
- **Wiederherstellungsmethoden:** 46 Prozent der deutschen Unternehmen, deren Daten verschlüsselt waren, nutzten mehrere Wiederherstellungsmethoden, um ihre Daten wiederherzustellen, was knapp unter dem weltweiten Durchschnitt von 47 Prozent liegt.

„Risikomanagement ist ein entscheidendes Element der Verteidigung. Die beiden häufigsten Ursachen für Ransomware-Angriffe – ausgenutzte Schwachstellen und kompromittierte Anmeldedaten – sind vermeidbar. Unternehmen müssen kritisch prüfen, inwieweit sie ihre Angriffsfläche im Blick haben und potenzielle Gefahrenherde sofort angehen. In einer Zeit, in der die Ressourcen knapp sind, müssen Unternehmen die Messlatte für die Anforderungen an einen Einbruch in Netzwerke so hoch wie möglich legen – und dazu zählt auf jeden Fall auch eine genaue Evaluierung des Status Quo“, so Shier.

Sophos empfiehlt folgende bewährte Praktiken zum Schutz vor Ransomware und anderen Cyberattacken

- Klarheit über Risikoprofil erlangen mit Tools wie Sophos Managed Risk, die die externe Angriffsfläche eines Unternehmens bewerten, die risikoreichsten Schwachstellen priorisieren und maßgeschneiderte Abhilfemaßnahmen anbieten können
- Endpoint-Schutz implementieren, der eine Reihe von sich ständig ändernden Ransomware-Techniken stoppt, wie z. B. Sophos Intercept X
- Verstärken des Schutzes mit einer rund um die Uhr verfügbaren Erkennung, Untersuchung und Reaktion auf Bedrohungen, entweder durch ein internes Team oder mit Unterstützung eines Managed Detection and Response (MDR)-Anbieters
- Erstellung und Pflege eines Plans zur Reaktion auf Zwischenfälle sowie regelmäßige Erstellung von Sicherungskopien und Übungen zur Wiederherstellung von Daten aus Sicherungskopien

Über die Studie

Die Daten der Studie „State of Ransomware 2024“ stammen aus einer herstellerunabhängigen Umfrage unter 5.000 Führungskräften im Bereich Cybersicherheit/IT, die zwischen Januar und Februar 2024 durchgeführt wurde. Die Befragten stammten aus 14 Ländern in Nord- und Südamerika, EMEA und dem asiatisch-pazifischen Raum. 500 Unternehmen aus Deutschland standen Rede und Antwort. Die befragten Unternehmen hatten zwischen 100 und 5.000 Mitarbeiter und einen Umsatz zwischen weniger als 10 Millionen und mehr als 5 Milliarden US-Dollar.

Die Sophos-Studie „State of Ransomware 2024” 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

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