State of Ransomware 2023: Datenverschlüsselung durch Ransomware erreicht höchstes Niveau

Lösegeldzahlung verdoppelt Wiederherstellungskosten
58 Prozent der befragten Organisationen in Deutschland waren von Ransomware betroffen

Wiesbaden, 10. Mai 2023 – Sophos veröffentlicht heute die neue globale Studie „State of Ransomware 2023“, nach der es Cyberkriminellen in Deutschland in 71 Prozent (international 76 Prozent) der Ransomware-Angriffe auf Organisationen gelingt, Daten zu verschlüsseln. Aus internationaler Perspektive ist es die höchste Rate an Datenverschlüsselung durch Ransomware, seit Sophos den jährlich erscheinenden Ransomware-Report erstmals im Jahr 2020 veröffentlichte.

Die Umfrage zeigt aus weltweiter Sicht, dass Unternehmen, die Lösegeld für die Entschlüsselung ihrer Daten zahlten, ihre Wiederherstellungskosten zusätzlich verdoppelten (750.000 Dollar Wiederherstellungskosten gegenüber 375.000 Dollar für Unternehmen, die Backups zur Datenwiederherstellung verwendeten). Außerdem bedeutet die Zahlung des Lösegelds in der Regel eine längere Wiederherstellungszeit: 45 Prozent der Unternehmen, die Backups verwendeten, konnten die Daten innerhalb einer Woche wiederherstellen, verglichen mit 39 Prozent der Unternehmen, die das Lösegeld zahlten.

Insgesamt wurden in Deutschland 58 Prozent (international 66 Prozent) der befragten Unternehmen von Ransomware angegriffen. Dies deutet darauf hin, dass die Zahl der Ransomware-Attacken trotz des vermeintlichen Rückgangs während der Pandemiejahre doch konstant hoch geblieben ist.
„Die Verschlüsselungsraten sind nach einem vorübergehenden Rückgang während der Pandemie wieder auf ein sehr hohes Niveau angestiegen, was besorgniserregend ist. Ransomware-Kriminelle haben ihre Angriffsmethoden verfeinert und ihre Attacken beschleunigt, um die Zeit zu verkürzen, in der die Verteidiger ihre Pläne durchkreuzen könnten“, ordnet Chester Wisniewski, Field CTO, Sophos die Studienergebnisse ein
„Die Kosten der Vorfälle steigen erheblich, wenn Lösegeld gezahlt wird. Die meisten Opfer werden nicht in der Lage sein, alle ihre Dateien wiederherzustellen, indem sie einfach die Verschlüsselungsschlüssel kaufen; sie müssen auch Backups einspielen. Die Zahlung von Lösegeld bereichert nicht nur die Kriminellen, sondern verlangsamt auch die Reaktion auf den Vorfall und erhöht die Kosten in einer ohnehin schon verheerenden Situation", führt Wisniewski fort.

Bei der Analyse der Ursache von Ransomware-Attacken waren die häufigsten Ausgangspunkte eine ausgenutzte Schwachstelle mit 24 Prozent (international 36 Prozent) sowie kompromittierte Zugangsdaten mit 36 Prozent (international 29 Prozent). Dies deckt sich mit den jüngsten Incident Response-Erkenntnissen aus dem „2023 Active Adversary Report for Business Leaders" von Sophos zur Reaktion auf Vorfälle vor Ort.

Weitere wichtige Ergebnisse der Studie

- In 30 Prozent der Ransomware-Fälle mit Datenverschlüsselung in Deutschland stahlen die Angreifer auch Daten. Dies deutet darauf hin, dass diese „Double-Dip“-Methode (Datenverschlüsselung und Datenexfiltration) immer häufiger vorkommt.
- International meldet der Bildungssektor die meisten Ransomware-Angriffe: 79 Prozent der befragten Organisationen im Hochschulbereich und 80 Prozent der befragten

Organisationen im unteren Bildungsbereich geben an, dass sie Opfer von Ransomware waren.
- Insgesamt zahlten 44 Prozent (international 46 Prozent) der befragten Organisationen in Deutschland, deren Daten verschlüsselt wurden, Lösegeld und erhielten Daten zurück Allerdings kamen Lösegeldzahlungen bei größeren Organisationen aus internationaler Sicht weitaus häufiger vor. Mehr als die Hälfte der Unternehmen mit einem Umsatz von 500 Millionen US-Dollar oder mehr zahlten das Lösegeld, wobei die höchste Rate von Unternehmen mit einem Umsatz von über 5 Milliarden US-Dollar gemeldet wurde. Dies könnte zum Teil darauf zurückzuführen sein, dass größere Unternehmen eher über eine eigenständige Cyber-Versicherungspolice verfügen, die Lösegeldzahlungen abdeckt.

„Zwei Drittel der Unternehmen geben an, im zweiten Jahr in Folge Opfer von Ransomware geworden zu sein. Der Schlüssel zur Reduzierung dieses Risikos liegt darin, sowohl die Zeit bis zur Entdeckung als auch die Zeit bis zur Reaktion drastisch zu verkürzen. Die von Menschen geleitete Bedrohungsjagd ist sehr effektiv, um diese Kriminellen zu stoppen, aber die Warnungen müssen untersucht und die Kriminellen innerhalb von Stunden aus den Systemen entfernt werden, nicht erst während Wochen und Monaten. Erfahrene Analysten können die Muster eines aktiven Eindringens innerhalb von Minuten erkennen und sofort in Aktion treten. Dies ist wahrscheinlich der Unterschied zwischen dem Drittel der Unternehmen, die sicher bleiben, und den zwei Dritteln, die nicht sicher sind. Unternehmen müssen rund um die Uhr in Alarmbereitschaft sein, um heutzutage eine wirksame Verteidigung aufzubauen“, so Wisniewski.

Drei Tipps von Sophos zum Schutz vor Ransomware und anderen Cyberattacken

1. Verstärken der Verteidigungsschilde durch:
   - Sicherheits-Tools, die die häufigsten Angriffsvektoren abwehren. Diese sollten Endpoint-Schutz mit starken Anti-Exploit-Funktionen einschließen, um die Ausnutzung von Schwachstellen zu verhindern, und Zero Trust Network Access (ZTNA) beinhalten, um den Missbrauch kompromittierter Anmeldedaten zu vereiteln.
   - Adaptive Technologien, die automatisch auf Angriffe reagieren, Angreifer stören und den Verteidigern Zeit verschaffen, um zu reagieren
   - 24/7 Bedrohungserkennung, -Untersuchung und -Reaktion. Entweder intern oder durch einen spezialisierten Anbieter von Managed Detection and Response (MDR)
2. Optimierung der Angriffsvorbereitung, einschließlich regelmäßiger Backups, Tests zur Wiederherstellung von Daten aus Backups und Pflege eines aktuellen Reaktionsplans für Zwischenfälle
3. Aufrechterhaltung einer guten Sicherheitshygiene, einschließlich rechtzeitiger Patches und regelmäßiger Überprüfung der Konfigurationen von Sicherheitstools

Über die Studie

Die Daten der Studie „State of Ransomware 2023“ stammen aus einer herstellerunabhängigen Umfrage unter 3.000 Führungskräften im Bereich Cybersicherheit/ IT, 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/
Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. 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 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.
Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und 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, 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