Sophos-Report "The State-of-Ransomware 2021": Horrende Kosten, zu komplex

und kaum Datenrückgabe

(PresseBox) Wiesbaden, 28.04.2021

- Ransomware-Wiederherstellung kostet in Deutschland im Schnitt rund 970.000 Euro – weit mehr als das Doppelte im Vergleich zu 2020
- Nur acht Prozent der Unternehmen weltweit erhalten nach der Lösegeldzahlung ihre Daten vollständig zurück
- 54 Prozent der Unternehmen weltweit bewerten die Cyberattacken für die eigene IT als zu komplex

Sophos gibt die Ergebnisse seiner weltweit angelegten Studie „The State of Ransomware 2021" bekannt. Besonders auffallend: die internationalen Durchschnittskosten für die Wiederherstellung nach einem Ransomware-Angriff haben sich in einem Jahr mehr als verdoppelt, konkret von rund 630.000 Euro in 2020 (Deutschland 390.000 Euro) zu 1,53 Millionen Euro in 2021 (Deutschland 970.000 Euro). Die durchschnittliche Lösegeldzahlung beträgt weltweit 140.000 Euro und in Deutschland 115.000 Euro.

Die Sophos-Studie zeigt auch, dass nur acht Prozent der betroffenen Organisationen im Falle einer Zahlung alle Daten wiederbekommen haben. Knapp ein Drittel (29 Prozent) weltweit bekam nicht mehr als die Hälfte der verschlüsselten Daten zurück. Die Zahl der Organisationen, die Opfer einer Ransomware-Attacke wurden, sank von 51 Prozent (Deutschland 57 Prozent) in 2020 auf 37 Prozent

(Deutschland 46 Prozent) in 2021 und weniger Unternehmen litten unter Datenverschlüsselung (54 Prozent in 2021 gegenüber 73 Prozent in 2020).

Dennoch enthüllen die neuen Studienergebnisse einen beunruhigenden Trend im Hinblick auf die Auswirkungen eines Ransomware-Angriffs.

Änderungen im Verhalten der Angreifer

„Der vermeintliche Rückgang der betroffenen Organisationen ist eine gute Nachricht, wird aber durch die Tatsache beeinträchtigt, dass diese Zahl zumindest teilweise, Änderungen im Verhalten der Angreifer widerspiegelt", so Chester, Wisniewski, Principal Research Scientist bei Sophos. „Wir haben beobachtet, wie Angreifer von groß angelegten, generischen und automatisierten Angriffen zu gezielteren Angriffen übergehen, die auch menschliches Hacking via Tastatur umfassen. Während die Gesamtzahl niedriger ist, zeigt unsere Erfahrung, dass das Schadenspotenzial dieser zielgerichteten Angriffe weitaus höher ist. Sich von derartigen Attacken zu erholen, ist viel aufwändiger, was sich in den verdoppelten Kosten für die Wiederherstellung der Daten abbildet."

Die wichtigsten Ergebnisse des Sophos-Reports zur Ransomware in 2021:

Die durchschnittlichen Kosten für die Erholung nach einer Ransomware-Attacke haben sich in den letzten zwölf Monaten weltweit mehr als verdoppelt (1,5 Millionen Euro 2021). Inklusive zum Beispiel Produktionsstillstand, verlorene Aufträge, Betriebskosten. Im Durchschnitt ist dieser Betrag rund zehn Mal so hoch wie die Lösegeldzahlung selbst.

Während die durchschnittliche Lösegeldhöhe weltweit wie erwähnt 140.000 Euro beträgt, belief sich der höchste Betrag auf rund 2,65 Millionen Euro; Zahlungen in Höhe von etwas über 8.000 Euro wurden am häufigsten genannt. Zehn der befragten Organisationen überwiesen 800.000 Euro und mehr.

Die Anzahl der Organisationen, die Lösegeld zahlten, stieg weltweit von 26 Prozent in 2020 auf 32 Prozent in 2021. Nur acht Prozent erhielten ihre vollständigen Daten zurück. „Diese Ergebnisse bestätigen die brutale Ransomware-Wirklichkeit: Zahlen lohnt sich nicht“, so Wisniewski. „Obwohl mehr Organisationen Lösegeld zahlen, bekommt nur eine Minderheit der Zahlenden die Daten komplett zurück. Das könnte zum Teil daran liegen, dass die Nutzung von Entschlüsselungs-Keys zur Wiederherstellung kompliziert ist. Und selbst wenn die Hacker nach Zahlung des Lösegelds den Code für die verschlüsselten Daten herausrücken, ist das keine Garantie für die erfolgreiche Wiederherstellung. Wie wir zum Beispiel kürzlich bei Ransomware-Attacken durch DearCry und Black Kingdom gesehen haben, können Angriffe, die mit minderwertigen oder überstürzt kompilierten Codes und Techniken gestartet werden, die Datenrettung schwierig, wenn nicht gar unmöglich machen."

Mehr als die Hälfte der Befragten, nämlich 54 Prozent weltweit (51 Prozent in Deutschland), meint, die Cyberattacken seien zu fortgeschritten, als dass ihre IT-Abteilung diese alleine handhaben können. Bedenklicher Trend: Erpressung ohne Verschlüsselung. Sieben Prozent der Befragten weltweit gaben an, dass sie zur Zahlung von Lösegeld aufgefordert wurden, obwohl ihre Daten nicht verschlüsselt wurden. Möglicherweise geschah dies, weil die Angreifer es geschafft hatten, Informationen zu stehlen. In 2020 waren das noch drei Prozent.

„Sich von einem Ransomware-Angriff zu erholen, kann Jahre dauern. Dazu gehört weitaus mehr als nur die Entschlüsselung und Wiederherstellung von Daten“, so Wisniewski. „Komplette Systeme müssen neu aufgebaut werden und auch die operativen Ausfallzeiten und Auswirkungen auf die Kunden dürfen nicht außer Acht gelassen werden.“ Zudem ist noch nicht abschließend definiert, was eine Ransomware-Attacke genau umfasst. Für eine kleine aber signifikante Minderheit der Befragten beinhalten die Attacken auch Zahlungsaufforderungen ohne Datenverschlüsselung. Das kann daran liegen, dass sie bereits über Anti-Ransomware-Technologien verfügen, die den Verschlüsselungsprozess blockieren. Ein anderer Grund könnte sein, dass die Angreifer schlichtweg beschlossen haben, keinerlei Daten zu verschlüsseln. Es ist anzunehmen, dass die Angreifer in solchen Fällen eine finanzielle Gegenleistung für die Nicht-Veröffentlichung vorab online gestohlener Daten fordern. „Wichtiger denn je ist es also, Hackern so früh wie möglich den Zugang zum Unternehmen zu verwehren, damit sie erst gar nicht die Chance bekommen, mit ihren immer facettenreicheren Angriffen auf Unternehmensdaten zuzugreifen. Zum Glück stehen betroffene Organisationen nicht alleine da. Unterstützung gibt es rund um die Uhr in Form von externen Sicherheitszentren, die unter anderem von Menschen durchgeführtes Threat Hunting und Incident Response-Services anbieten, um solche Attacken schnellstmöglich zu erkennen und zu eliminieren“, so Wisniewski.

Sophos empfiehlt die folgenden sechs praxisbewährten Tipps zum Schutz vor Ransomware:

Jeden kann es treffen. Ransomware bleibt weit verbreitet, und macht weder vor Sektor, Land oder Unternehmensgröße Halt. Jeder sollte sich auf dieses Szenario vorbereiten, um im Ernstfall handlungsfähig zu bleiben. Backups nach Industriestandards. Laut der Studie stellen die meisten

Organisationen ihre Daten nach einer Attacke wieder aus ihren Backups her. Dabei sollte der Industrie-Standard 3:2:1 berücksichtigt werden, sprich: dreifaches Backup, zwei unterschiedliche Medien und eins davon offline aufbewahren. Schutzschichten einrichten. Da immer mehr Ransomware-Angriffe auch Erpressung beinhalten ist es wichtiger denn je, die Gegner von vornherein fernzuhalten. Deshalb sollte Schutzmechanismen auf verschiedenen Ebenen (multi-layered) verwendet werden, um Angreifer zu blocken.

Menschliche Expertise in Kombination mit Anti-Ransomware-Technologie. Der Schlüssel, um Ransomware zu stoppen, ist die Verteidigung in der Tiefe. Dabei werden dedizierte Anti-Ransomware-Techniken mit von Menschen durchgeführtes Threat Hunting verbindet. Die Technologie liefert Skalierung und Automation, während menschliche Expertise unschlagbar beim Entdecken von Verschleierungstaktiken, Techniken und Verfahren, die darauf hinweisen, dass ein Angreifer versucht, in die Umgebung einzudringen, ist. Hat man diese Fähigkeiten nicht im Haus, bieten spezialisierte Security Operations Center (SOCs) Unterstützung für Organisationen verschiedener Größen.

Niemals Lösegeld zahlen. Lösegeldzahlung ist schlichtweg der ineffektivste Weg, um Daten zurückzubekommen. Wer dennoch bezahlen möchte, sollte im Hinterkopf behalten, dass, die Gegner im Durchschnitt nur bis zu Zweidrittel der Dateien wiederherstellen. Recovery Plan haben. Der beste Weg, eine Cyberattacke nicht zu einem kompletten Datenverlust werden zu lassen, ist ein vorab erstellter und jederzeit griffbarer Notfallplan.

Zur Studie

Für die „The State of Ransomware 2021“ Studie wurden im Januar und Februar 2021 5.400 IT-Entscheider in mittelgroßen Organisationen (100 bis 5.000 Mitarbeiter) in 30 Ländern in Europa, Nord- und Südamerika, dem Asia-Pazifik-Raum, Zentralasien, dem Mittleren Osten und Afrika befragt. Die Untersuchung wurde von Sophos in Auftrag gegeben und von Vanson Bourne, einem unabhängigen Marktforschungsinstitut, durchgeführt. Der komplette englische Report kann hier heruntergeladen werden.

Über die Sophos Technology GmbH

Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 53.000 Partnern und Managed Service Providern (MSP).

Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien. Weitere Informationen unter www.sophos.de.

Ansprechpartner

Jörg Schindler

PR Manager EMEA

Telefon +49 (721) 25516-263