



Ransomware in Fertigung und Produktion: Der verarbeitende Sektor zahlt das höchste Lösegeld

Sophos State of Ransomware zeigt: Unternehmen aus Fertigung und Produktion zahlten weltweit seltener Lösegeld, mit durchschnittlich 2.036.189 US-Dollar gleichzeitig aber mehr als doppelt so viel wie Unternehmen anderer Branchen

Sophos hat die diesjährige Branchenstudie "The State of Ransomware in Manufacturing and Production" veröffentlicht, in der speziell der Bereich Fertigung und Produktion betrachtet wurde. Die Studie zeigt, dass dieser Sektor die höchsten durchschnittlichen Lösegeldzahlungen aller untersuchten Branchen aufweist. Betroffene Unternehmen brachten hier 2.036.189 US-Dollar für die Forderungen der Erpresser auf, wogegen Unternehmen anderer Branchen 812.360 US-Dollar aufwendeten. Auch was die Zunahme bei der Komplexität sowie der Anzahl der Cyberangriffe angeht, liegt die Branche vorn: 66 Prozent der befragten Fertigungs- und Produktionsunternehmen berichteten von einer zunehmenden Komplexität von Cyberangriffen und 61 % hatten im Vergleich zur Vorjahresumfrage eine Zunahme an Cyberangriffen zu verzeichnen. Beide Steigerungen liegen sieben bzw. vier Prozent über dem Durchschnitt anderer Branchen.

„Das verarbeitende Gewerbe ist ein attraktives Ziel für Cyberkriminelle, da es eine privilegierte Position in der Lieferkette einnimmt. Veraltete Infrastrukturen und mangelnde Transparenz der OT-Umgebung (operative Technologie) bieten Angreifern einen einfachen Zugang und eine Ausgangsbasis für Angriffe in einem angegriffenen Netzwerk,“ sagt John Shier, Senior Security Advisor bei Sophos. „Die Konvergenz von IT und OT vergrößert die Angriffsfläche und verschärft eine ohnehin schon komplexe Bedrohungslage.“

Weniger Unternehmen zahlen, dafür sind die Summen höher

Während die durchschnittliche Lösegeldzahlung in der Fertigungs- und Produktionsbranche am höchsten war, war der Prozentsatz der Unternehmen, die das Lösegeld tatsächlich gezahlt haben, dagegen einer der niedrigsten in allen Branchen (33% gegenüber 46% im branchenübergreifenden Durchschnitt).

Weitere Ergebnisse der Studie in der Übersicht:

- Der Fertigungs- und Produktionssektor wies die niedrigste Angriffsrate auf, gleichauf mit dem Finanzdienstleistungssektor, wo nur 55 % der befragten Unternehmen von Ransomware betroffen waren.
- Allerdings stieg der Prozentsatz der von Ransomware betroffenen Unternehmen in der Fertigungs- und Produktionsbranche im Vergleich zum Vorjahresbericht um 52 % (gegenüber 36 % im Umfragebericht 2021).
- Der Sektor wies auch die niedrigste Verschlüsselungsrate auf (57 % gegenüber 65 % im branchenübergreifenden Durchschnitt).
- Nur 75 % der Befragten gaben an, über eine Cyberversicherung zu verfügen – der niedrigste Prozentsatz in allen Branchen.

Sophos gibt allen Unternehmen in allen Branchen die folgenden fünf Empfehlungen zum besseren Schutz vor Ransomware:

1. Installation und Pflege von qualitativ hochwertigen Schutzmaßnahmen an allen Stellen der Umgebung. Regelmäßige Überprüfung von Sicherheitskontrollen und

- Sicherstellung dass diese weiterhin den Anforderungen des Unternehmens entsprechen.
2. Proaktiv nach Bedrohungen suchen, um Angreifer zu identifizieren und zu stoppen, bevor sie Angriffe ausführen können. Wenn intern keine Ressourcen hierfür verfügbar sind, sollten ein MDR-Team (Managed Detection and Response) hinzugezogen werden.
 3. Härtung der IT-Umgebung durch Identifizierung und Schließung wichtiger Sicherheitslücken wie etwa nicht gepatchte Geräte, ungeschützte Rechner und offene RDP-Ports. Extended Detection and Response (XDR)-Lösungen sind für diesen Zweck ideal.
 4. Entwicklung eines Worst Case-Szenarios und Bereithaltung eines stetig aktualisierten Handlungsplans.
 5. Erstellen von Backups und Übung der Wiederherstellung dieser, um minimale Unterbrechungen und Wiederherstellungszeiten zu gewährleisten.

„Zuverlässige Backups sind ein wichtiger Bestandteil der Wiederherstellung, zusätzlich benötigt die heutige Ransomware-Bedrohung einen detaillierten Reaktionsplan, der auch Fähigkeiten zur Bedrohungsjagd unter menschlicher Führung umfasst,“ sagt John Shier. „Komplexe Angriffe erfordern einen umfassenden Schutz, der für viele Unternehmen den Einsatz von Managed Detection and Response (MDR)-Teams beinhaltet, die darin geschult sind, aktive Angreifer zu finden und zu neutralisieren.“

Zur Studie:



Im Rahmen der Studie "State of Ransomware 2022" wurden 5.600 IT-Experten in mittelständischen Unternehmen in 31 Ländern befragt, darunter 419 Befragte aus der Fertigungs- und Produktionsbranche.

Die gesamte Studie findet sich hier:

<https://www.sophos.com/en-us/whitepaper/the-state-of-ransomware-in-manufacturing-and-production-2022>

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

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