Sophos-Untersuchung zeigt: Fertigungs- und Produktionsbetriebe zahlen am seltensten Ransomware-Lösegeld

19 Prozent. Nur so wenige Unternehmen aus der Fertigung und Produktion bezahlen Lösegeld nach einem Ransomware-Angriff, um ihre verschlüsselten Daten zu befreien. Weitaus weniger als der branchenübergreifende Durchschnitt mit 32 Prozent.

Der Untersuchungsbericht The State of Ransomware in Manufacturing and Production 2021 von Sophos offenbart, dass mit nur 19 Prozent die Fertigungs- und Produktionsbetriebe am wenigsten geneigt sind, einer Ransomware-Lösegeldforderung nachzugeben, um ihre verschlüsselten Daten zu dechiffrieren. Zugleich sind diese Unternehmen mit 68 Prozent am ehesten in der Lage, ihre Daten aus Backups wiederherzustellen. Dennoch ist dieser Sektor mit am stärksten von erpresserischer Ransomware betroffen. Denn die Cyberkriminellen setzen als Druckmittel nicht nur die Verschlüsselung der Daten ein, sondern drohen auch mit der Veröffentlichung gestohlener Dateien im Internet, wenn das Opfer der Lösegeldforderung nicht nachkommt.
Der Untersuchungsbericht von Sophos befasst sich mit dem Ausmaß und der Auswirkung von Ransomware-Angriffen bei 5.400 Befragten in führenden IT-Positionen aus 30 Ländern (darunter 438 in Fertigung und Produktion).

Weitere Studienergebnisse belegen:

- Aus globaler Sicht wurden 36 Prozent der untersuchten Fertigungs- und Produktionsunternehmen wurden im letzten Jahr von Ransomware-Attacken betroffen. Für die DACH-Region bestätigen dies sogar 50 Prozent der befragten Unternehmen.
- Weltweit verfügen 89 Prozent der Fertigungs- und Produktionsunternehmen über einen Wiederherstellungsplan für Malwarevorfälle. Diesen Schnitt können die Unternehmen in der DACH-Region mit 92 Prozent sogar noch toppen.
- Die durchschnittlichen Wiederherstellungskosten betrugen 1,52 Millionen US-Dollar (1,31 Millionen Euro) – weniger als im globalen Mittelmaß mit 1,85 Millionen US-Dollar (1,59 Millionen Euro).

Chester Wisniewski, Principal Research Scientist, Sophos, ordnet die Ergebnisse ein:
„Die ausgeprägte Fähigkeit dieses Sektors, die eigenen Daten mithilfe eines Backups wiederherzustellen, ermöglicht es vielen Betrieben, sich den Forderungen der Angreifer im Fall einer klassischen Ransomware-Verschlüsselung zu widersetzen. Das bedeutet aber auch, dass die Gegner dazu übergehen, andere Hebel zu finden, um die Opfer zur Zahlung zu zwingen. Wie zum Beispiel der Datendiebstahl mit der Androhung, die erbeuteten Informationen zu veröffentlichen.
Backups sind lebenswichtig, aber viele klassische Backup-Konzepte bieten keinen Schutz vor diesem Risiko. Daher sollten sich Unternehmen aus Fertigung und Produktion nicht darauf verlassen, dass sie einen wirksamen Schutz vor Erpressung haben. Organisationen müssen ihre Anti-Ransomware-Defensive ausweiten, und zwar auf die Kombination von Technologie und Menschen-gesteuerter Bedrohungsjagd. So lassen sich die heutigen fortschrittlichen Cyberattacken rechtzeitig entdecken und neutralisieren."

Die Ergebnisse der Analyse zeigen darüber hinaus, dass Betriebe dieser Branchen weitaus mehr Sorge vor einem Ransomware-Angriff in der Zukunft haben als jeder andere Sektor:

60 Prozent der Antwortenden halten die Attacken für derart ausgefeilt, dass es immer schwieriger wird, sie zu stoppen. Für 46 Prozent ist Ransomware so weit verbreitet, dass sie damit rechnen, davon betroffen zu werden.

Empfehlungen der Sophos Sicherheitsexperten – branchenübergreifend:

1. Man muss davon ausgehen, dass ein Unternehmen von Ransomware betroffen sein wird. Ransomware bleibt weit verbreitet und weder Sektor, Land noch Organisationsgröße sind immun gegen dieses Risiko.

2. Regelmäßig Backups erstellen.
   Backups mit einer Technologie, die von Ransomware nicht verschlüsselt werden können, sind das beste Mittel, mit dem Unternehmen ihre Daten nach einem Angriff wiederherstellen können. Denn selbst wenn Betriebe das Lösegeld bezahlen, erhalten Unternehmen selten die kompletten Dateien zurück. Das Backup-Konzept sollte dem 3-2-1-Industriestandard entsprechen: drei Kopien auf zwei unterschiedlichen Systemen, wobei eine Kopie offline gelagert wird.

3. Schutz auf verschiedenen Ebenen verwenden.
   In Vorahnung wachsender erpresserischer Ransomware ist es immens wichtig, Angreifer überhaupt gar nicht ins Netzwerk eindringen zu lassen. Dazu verhelfen Schutzmechanismen auf unterschiedlichen Ebenen.

4. Menschliche Expertise in Kombination mit Anti-Ransomware-Technologie.
   Der Schlüssel, Ransomware zu stoppen, ist die Verteidigung in der Tiefe, die gezielte Anti-Ransomware-Technologie und Menschen-geführte Bedrohungssuche miteinander verbindet. Die Technologie beinhaltet Skalierung und Automation, während Experten aus Fleisch und Blut unschlagbar sind, wenn es um das Entdecken von verräterischen Taktiken, Techniken und Prozeduren geht. Security Operations Center (SOCs) können mangelnde betriebsinterne Security-Expertise ergänzen und sind eine realistische Möglichkeit für Organisationen jeder Größe.

5. Kein Lösegeld bezahlen.
   Unabhängig von moralischen Überlegungen ist das Bezahlen von Lösegeld der ineffektivste Weg, seine Daten zurückzubekommen. Sophos Untersuchungen zeigen, dass selbst nach Zahlungen im Durchschnitt nur rund Zweidrittel der verschlüsselten Dateien freigegeben wurden.

6. Entwickelung eines Malware-Wiederherstellungsplans.
   Der beste Weg einen malware-Vorfall nicht zur Katastrophe ausufern zu lassen, ist die Vorbereitung. Ein detaillierter Wiederherstellungsplan speziell für den Fall eines Malware-Angriffs hilft im Notfall die richtigen Schritte einzuleiten. Dieser Plan sollte zudem in regelmäßigen Abständen getestet und der eventuell veränderten IT-Umgebung angepasst werden.

Über Sophos
Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Verbrauchern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist in Oxford, U.K. Weitere Informationen unter www.sophos.de.

Neu: 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