SOPHOS

Jahresbericht zur Bedrohungslage durch Cyberkriminelle

Was der Threat Report 2025 über die Zukunft der Cybersicherheit für KMUs verrät

Und warum Ransomware weiterhin die größte Gefahr für kleine und mittlere Unternehmen ist

Cyberkriminelle werden immer geschickter darin, die blinden Flecken in der Sicherheitsarchitektur eines Unternehmens auszunutzen — und bewegen sich möglichst unauffällig auf Schleichfahrt innerhalb der Netzwerke bevor sie tatsächlich zuschlagen. Diese Entwicklung hat laut dem aktuellen Sophos Threat Report 2025 zum anhaltenden Wachstum von Ransomware als Bedrohung für kleine und mittelständische Unternehmen (KMU) geführt. Die jährliche Studie hebt die wichtigsten Cybersicherheitsbedrohungen hervor, denen KMU ausgesetzt sind. Die Daten des Reports stammen unter anderem aus der Telemetrieerfassung in Sophos Endpoint sowie den Analysedaten der Sophos-Services Managed Detection and Response (MDR) und Incident Response (IR).

5 WICHTIGE ERGEBNISSE DES REPORTS

1. Ransomware bleibt die größte Bedrohung für kleine und mittelständische Unternehmen.
Die Verschlüsselung oder der Diebstahl von Daten mit anschließender Lösegeldforderung machten 70 % der Sophos Incident Response-Fälle bei kleinen und über 90 % bei mittelständischen Unternehmen aus.

2. 25 %
Komprimierte Geräte an den Netzwerkgrenzen waren die Hauptursache für Unternehmenseinbrüche und diente in 25 % der untersuchten MDR/IR-Vorfälle als erstes Einfallstor für Kriminelle. Diese Zahl unterstreicht die Notwendigkeit von Firewall- und Perimeterschutz im Zeitalter der Remote-Arbeit.

3. Angreifer entwickeln ihre Social-Engineering-Tricks weiter und nutzen Methoden wie Vishing, E-Mail-Bombing oder Quishing, um Anmeldedaten zu stehlen und Netzwerke zu infiltrieren.
Bei Vishing handelt es sich um eine Abwandlung des klassischen Phishings per E-Mail, allerdings als Telefonanruf. Beim E-Mail-Bombing werden innerhalb kürzester Zeit Hunderte, wenn nicht Tausende E-Mails in kürzester Zeit als "Störfeuer" versandt und Quishing beinhaltet die Verwendung gefälschter QR-Codes, um Anmeldedaten für Anwendungen wie Microsoft SharePoint zu stehlen.

4. Angreifer setzen auf legitime Apps und Social Engineering, um Netzwerke zu infiltrieren, anstatt maßgeschneiderte Malware zu verwenden.
Das bedeutet, dass traditionelle Erkennungsmethoden und Signaturen häufig nicht mehr ausreichend sind. Die proaktive Überwachung durch Managed Detection and Response-Dienste kann verdächtige Aktivitäten erkennen, bevor Bedrohungsakteure beispielsweise Daten verschlüsseln oder stehlen können.

5. 20 %
VPNs (Virtual Private Network) sind mit 20 % aller MDR und IR-Fälle das häufigste Einfallstor für Kompromittierungen. Hier sind starke Passwortregeln essentiell.

Um sich effektiv vor den im Threat Report beschriebenen Bedrohungen zu schützen, kontaktieren Sie Sophos noch heute und erfahren Sie mehr über Sophos Managed Detection and Response (MDR), Sophos Firewall und andere Lösungen.

Möchten Sie mehr erfahren?
Lesen Sie hier den Sophos Threat Report 2025 >

© Copyright 2025. Sophos Ltd. Alle Rechte vorbehalten.
Registriert in England und Wales Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK. Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

2025-05-21