Sophos Threat Report 2025:
Schlendrian an den Netzwerkgrenzen torpediert die Cyberresilienz

- *Ransomware weiterhin der Platzhirsch – die Angriffsart machte 90 Prozent der Sophos Incident Response Vorfälle bei mittelständischen Unternehmen 2024 aus*
- *Immer mehr Geräte sind im EOL-Modus (Ende der Lebenszyklus), also ohne Unterstützung vom Hersteller, aktiv und sorgen so für immer mehr „digitalen Detrius", der die Arbeit der Sicherheitsverantwortlichen erschwert*

Sophos hat heute seinen „Annual Threat Report: Cybercrime on Main Street 2025" veröffentlicht. Die Cybersecurity-Fachteams analysieren darin die im Jahr 2024 angesammelten Telemetriedaten aus Sophos-Lösungen, Incident-Response-Fällen sowie MDR-Services. Demnach ist Ransomware nach wie vor die größte Bedrohung gerade für KMUs – und profitiert stark von veralteten oder falsch konfigurierten Netzwerkgeräten – sie waren Einfallstor Nummer 1 für die Cyberkriminellen.

Ransomware machte 2024 etwa 70 Prozent der Sophos Incident Response-Fälle bei kleinen Unternehmenskunden aus. Bei mittelständischen Unternehmen von 500 bis 5000 Mitarbeitern lag dieser Wert sogar bei und über 90 Prozent. 25 Prozent der durch die Telemetrie bestätigten initialen Kompromittierungen gingen von Netzwerk-Edge-Geräten aus – Firewalls, virtuelle private Netzwerkgeräte und andere Zugangsgeräte. Die tatsächliche Zahl dürfte noch einmal deutlich höher sein. Entsprechend sind auch die fünf beliebtesten Einfallstore für Kriminelle zum Großteil an den Netzwerkgrenzen zu finden: VPN Exploits (19 Prozent aller untersuchten Fälle) liegt mit großem Abstand auf Platz 1, gefolgt von kompromittierten Zugangsdaten (10,4 Prozent), den Remote Access Tools RDP und RDWeb (8 Prozent), Phishing (6,7 Prozent) und anderen Netzwerkgeräte (3 Prozent).

Sean Gallagher, Principal Threat Researcher bei Sophos, ordnet die Ergebnisse des Reports wie folgt ein: „In den letzten Jahren haben Angreifer gezielt Edge-Geräte ins Visier genommen. Erschwerend kommt hinzu, dass immer mehr Geräte am Ende ihrer Lebensdauer (EOL) im Umlauf sind – ein Problem, das Sophos als „digitalen Detrius", also die Infrastruktur „zumüllende Zerfallsprodukte", bezeichnet. Da diese Geräte dem Internet ausgesetzt sind und Patches oft nur eine geringe Priorität haben, sind sie für Kriminelle ein hochattraktives Ziel, um in Netzwerke einzudringen. Der Angriff auf Edge-Geräte ist jedoch nur Teil eines größeren Wandels, den wir beobachten: Angreifende müssen keine maßgeschneiderte Malware mehr einsetzen. Stattdessen können sie die Systeme von Unternehmen ausnutzen, deren Agilität erhöhen und sich an Orten verstecken, wo Sicherheitsverantwortliche nicht hinsehen."

Weitere wichtige Ergebnisse des Berichts:

- Multifaktor-Authentifizierung (MFA) reicht immer häufiger nicht mehr aus. Angreifende umgehen MFA durch die Erfassung von Authentifizierungstoken. Dabei nutzen die Kriminellen eine Phishing-Plattform, um den Authentifizierungsprozess zu imitieren und die Anmeldedaten des Ziels zu erfassen.
- Die Top-3-Ransomwarefamilien, die 2024 beobachtet wurden sind Akira (15,3 Prozent aller untersuchten Fälle), Lockbit (13,6 Prozent) und Fog (10,9 Prozent). Über alle Malwaregruppen hinweg liegen die Comand-and-Control-Angriffe vorne. Web Shell belegt mit 9,8 Prozent Platz 1, gefolgt von Cobalt Strike mit 8 Prozent und dem Ransomware-Anführer Akira mit 4,9 Prozent.

- Angreifende bevorzugen kommerzielle Remote-Access-Tools. Die am häufigsten missbrauchten legitimen und vertrauenswürdigen Tools waren PSExec (18,3 Prozent aller untersuchten Fälle) und AnyDesk (17,4 Prozent). Insgesamt waren Remote Access Tools in 34 Prozent der IR/MDR-Fälle involviert.
- Cyberkriminelle entwickeln ihre Social-Engineering-Taktiken weiter. Sie missbrauchen zunehmend QR-Codes (Quishing) und Telefonnachrichten (Vishing), um Unternehmen zu kompromittieren. Sie nutzen außerdem E-Mail-Bombing – eine Taktik, bei der innerhalb von ein bis zwei Stunden Tausende von Spam-E-Mails versendet werden.
- Software-as-a-Service-Plattformen, die während der COVID-Pandemie von Unternehmen häufig eingesetzt wurden, um Remote-Arbeit zu unterstützen und die allgemeine Sicherheitslage zu verbessern, werden weiterhin auf neue Weise für Social Engineering, initiale Kompromittierung und die Verbreitung von Malware missbraucht.
- Kompromittierungen von Business-E-Mails machen einen wachsenden Anteil der initialen Kompromittierungen bei Cybersicherheitsvorfällen aus – genutzt für die Verbreitung von Malware, den Diebstahl von Anmeldeinformationen und Social Engineering für eine Vielzahl krimineller Zwecke.

Alle Details zu den Analyseergebnissen der Sophos X-Ops gibt es im englischsprachigen Bericht „Annual Threat Report: Cybercrime on Main Street 2025".

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/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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