Sophos Active Adversary Report: „Freier Eintritt“ per Log-in bei 56 Prozent der analysierten Angriffsfälle

- *Kompromittierte Zugangsdaten sind im zweiten Jahr in Folge die Hauptursache von Cyber-Angriffen*
- *IR- und MDR-Fälle zeigen, dass Angreifer Daten in nur drei Tagen ausspähen*

WIESBADEN, 2. April 2025 – Sophos hat den Sophos Active Adversary Report 2025 veröffentlicht, der das Verhalten und die Techniken von Cyberkriminellen aus über 400 tatsächlichen Angriffen analysiert, die das MDR-Team (Managed Detection and Response) und die Incident-Response-Spezialisten 2024 durchgeführt haben. Der Report zeigt, dass sich die Angreifenden in erster Linie über externe Remote-Dienste Zugang zu Netzwerken verschafften (56 Prozent aller MDR- und IR-Fälle), indem sie gültige Konten ausnutzten, darunter Edge-Geräte wie Firewalls und VPNs.

Die Kombination aus externen Remote-Diensten und gültigen Konten deckt sich mit den Hauptursachen für Angriffe. Das zweite Jahr in Folge waren kompromittierte Anmeldedaten die Hauptursache für Angriffe (41 Prozent). Es folgen die Ausnutzung von Sicherheitslücken (22 Prozent) und Brute-Force-Angriffe (21 Prozent).

Tempo der Angriffe nimmt zu
Bei der Analyse von MDR- und IR-Untersuchen berücksichtigte das Sophos X-Ops Team insbesondere Ransomware-, Datenexfiltrations- und Datenerpressungsfälle, um zu ermitteln, wie schnell Cyberkriminelle die einzelnen Phasen eines Angriffs innerhalb eines Unternehmens durchlaufen. Bei diesen drei Arten von Fällen betrug die durchschnittliche Zeit zwischen dem Beginn eines Angriffs und der Datenexfiltration nur 73 Stunden, also etwa drei Tage. Darüber hinaus vergingen von der Exfiltration bis zur Entdeckung des Angriffs im Durchschnitt nur 2,7 Stunden.

„Passive Sicherheit ist mittlerweile nicht mehr ausreichend“, so John Shier, Field CISO bei Sophos. „Vorbeugung ist zwar wichtig, aber eine schnelle Reaktion ist entscheidend. Unternehmen müssen ihre Netzwerke aktiv überwachen und schnell auf beobachtete Auffälligkeiten reagieren. Koordinierte Angriffe von professionellen Cyberkriminellen erfordern auch eine koordinierte Verteidigung. Für viele Unternehmen bedeutet dies eine Kombination aus geschäftsspezifischem Wissen und von Experten geleiteter Erkennung und Reaktion. Unser Bericht bestätigt, dass Unternehmen mit aktiver Überwachung Angriffe schneller erkennen und bessere Ergebnisse bei der Abwehr erzielen.“

Weitere Ergebnisse des Sophos Active Adversary Reports 2025

- **Angreifer benötigen im Schnitt in nur elf Stunden zur Systemübernahme**
  Zwischen der ersten Aktion eines Cyberkriminellen und seinem ersten (oft erfolgreichen) Versuch, in das Active Directory – eines der wichtigsten Elemente in jedem Windows-Netzwerk – einzudringen, vergingen im Durchschnitt der untersuchten Fälle nur elf Stunden. Wenn dies gelingt, können Angreifer sehr leicht die Kontrolle über das ganze Unternehmen übernehmen.

- **Alte Bekannte bei den häufigsten Ransomware-Gruppen**

In den von Sophos untersuchten Fällen war Akira die am häufigsten auftretende Ransomware-Gruppe im Jahr 2024, gefolgt von Fog und LockBit – und das, obwohl LockBit Anfang des Jahres durch eine konzertierte Aktion der Strafverfolgungsbehörden vom Netz genommen wurde.

- **MDR als entscheidender Faktor für die Verweildauer der Kriminellen**
  Insgesamt ist die Verweildauer, also die Zeit vom Beginn eines Angriffs bis zu seiner Entdeckung, im Jahr 2024 von vier auf zwei Tage gesunken. Dies ist hauptsächlich auf die Aufnahme von MDR-Fällen in den Datensatz zurückzuführen. Die Verweildauer in IR-Fällen blieb stabil bei vier Tagen für Ransomware-Angriffe und 11,5 Tagen für Nicht-Ransomware-Fälle**.** In den untersuchten MDR-Fällen betrug die Verweildauer bei Ransomware-Angriffen drei Tage und bei Nicht-Ransomware-Fällen nur einen Tag. Dies deutet darauf hin, dass MDR-Teams in der Lage sind, Angriffe schneller zu erkennen und darauf zu reagieren.

- **Ransomware-Gruppen arbeiten über Nacht**
  Im Jahr 2024 wurden 84 Prozent der Ransomware-Binärdateien außerhalb der normalen, örtlichen Arbeitszeiten der Zielpersonen verbreitet.

- **Schwachstelle Remote Desktop Protokoll**
  Das Remonte Desktop Protokoll (RDP) war in 84 Prozent der MDR/IR-Fälle involviert und damit das am häufigsten missbrauchte Microsoft-Tool.

Der vollständige, englische Bericht “The 2025 Sophos Active Adversary Report” kann hier nachgelesen werden.

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

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter fortschrittlicher Sicherheitslösungen zur Abwehr von Cyberangriffen. Das Unternehmen übernahm Secureworks im Februar 2025 und brachte damit zwei Pioniere zusammen, die die Cybersicherheitsbranche mit ihren innovativen, nativen und KI-optimierten Dienstleistungen, Technologien und Produkten neu definiert haben. Sophos ist der größte, reine Anbieter von Managed Detection and Response Services (MDR) und unterstützt mehr als 28.000 Organisationen. Zusätzlich zu MDR und anderen Dienstleistungen umfasst das komplette Portfolio von Sophos branchenführende Endpunkt-, Netzwerk-, E-Mail- und Cloud-Sicherheitslösungen, die über die Sophos-Central-Plattform zusammenarbeiten und sich für bestmöglichen Schutz kontinuierlich anpassen. Secureworks bietet das innovative, marktführende Taegis XDR/MDR, Identity Threat Detection and Response (ITDR), SIEM-Funktionen der nächsten Generation, Managed Risk und ein umfassendes Angebot an Beratungsdienstleistungen. Sophos vertreibt all diese Lösungen über Reseller-Partner, Managed Service Provider (MSPs) sowie Managed Security Service Provider (MSSPs) und schützt damit mehr als 600.000 Organisationen weltweit vor Phishing, Ransomware, Datendiebstahl sowie anderer alltäglicher und staatlich initiierter Cyberkriminalität. Die Lösungen stützen sich auf historische und Echtzeit-Bedrohungsdaten von Sophos X-Ops sowie der neu hinzugefügten Counter Threat Unit (CTU). Der Hauptsitz von Sophos befindet sich in Oxford, U.K. Weitere Informationen unter www.sophos.de.

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