SOPHOS

Active Adversary Report 2025

Prävention und Schutz gegen Angreifer

Unternehmen können sich – egal wie groß sie sind – beim Thema Cybersicherheit nicht mehr nur auf Verteidigungsmaßnahmen verlassen. Sie müssen proaktiv handeln, um mit den neuesten Trends und Taktiken der Bedrohungsakteure Schritt zu halten – so die Kernaussage des Active Adversary Reports 2025 von Sophos. Dieser Bericht, der auf der Analyse hunderter Fälle des Sophos Incident Response Teams und des Managed Detection and Response (MDR) Services basiert, zeigt, dass viele Cyberangriffe des vergangenen Jahres bei entsprechender Wachsamkeit bereits in der Anfangsphase der Infektion erkannt werden können.

5 WICHTIGE ERGEBNISSE DES REPORTS

1. In 41,16 % der von Sophos analysierten Fälle wurden kompromittierte Anmeldedaten verwendet.

Angreifer müssen nicht mehr einbrechen. Sie loggen sich einfach ein – und bei vielen Unternehmen reicht das bereits aus. Sophos MDR hilft, solche Aktivitäten frühzeitig zu erkennen, bevor sie sich zu etwas Schlimmerem ausweiten.
Sophos MDR lässt sich direkt in Microsoft Office 365 integrieren und stellt sicher, dass bei verdächtigen Anmeldeversuchen oder auffälligen Aktivitäten innerhalb von Minuten, nicht Stunden, Alarm geschlagen wird.

Ausgenutzte Schwachstellen (21,79 %) und Brute-Force-Angriffe (21,07 %) waren die zweit- bzw. dritthäufigste Ursache der beobachteten Vorfälle.

> Die Häufigkeit von Brute-Force-Angriffen sank bei Unternehmen mit über 1.000 Mitarbeitern (auf 20 %). Angreifer nutzten stattdessen häufiger Schwachstellen aus (in 29 % der Vorfälle bei größeren Unternehmen).

2. Die Verweildauer der Angreifer wird kürzer.

Die Zeit, die Angreifer im Netzwerk verbringen, bevor sie aktiv werden, ist im letzten Jahr gesunken. Dies deutet darauf hin, dass proaktive Cybersecurity-Lösungen wie MDR Wirkung zeigen.

3. Datenexfiltration bei Ransomware-Angriffen begann schon drei Tage nach der ersten Infektion.

Es vergingen im Median nur 2,7 Stunden von der Exfiltration bis zur Erkennung des Angriffs. Bei Ransomware-Fällen bedeutet das, dass Unternehmen nur etwa 3 Stunden Zeit bleibt, um eine Datenverschlüsselung zu verhindern, sobald Angreifer mit der Datenexfiltration beginnen.

4. 65 % aller Sophos IR-Fälle betrafen Ransomware

Ransomware bleibt die Bedrohung Nummer 1 für Unternehmen aller Größen und tritt in 65 % der Sophos IR-Fälle auf. Unternehmen, die MDR einsetzen, sind eher in der Lage, Ransomware-Angriffe zu stoppen, indem sie diese erkennen, bevor sie die Verschlüsselungsphase erreichen oder Angreifer beginnen, Daten zu stehlen.

Die drei aktivsten Ransomware-Gruppen im Jahr 2024:

- Akira
- Fog
- LockBit

5. Angreifer benötigen weniger maßgeschneiderte Malware, um sich Zugriff zu verschaffen.

Der Grund dafür ist, dass weniger Unternehmen Multi-Faktor-Authentifizierung (MFA) nutzen, was es Angreifern erleichtert, Anmeldedaten für gültige Konten zu stehlen. Sie können sich damit dann einfach anmelden und gelangen unbemerkt – oft über externe Remote-Dienste – in die Unternehmensumgebung.

Diese Taktik wird bei größeren Unternehmen mit mehr als 1.000 Mitarbeitern jedoch seltener beobachtet – vermutlich, weil dort strengere Passwort-Regeln gelten.

BERECHNEN SIE DEN ROI, DEN SIE DURCH 24/7 CYBERSECURITY ERZIELEN KÖNNEN – MIT UNSEREM SOPHOS MDR ANGEBOTSGENERATOR.

Lesen Sie hier den Sophos Active Adversary Report >

2025-05-12