Sophos Active Adversary Report 2026: Identitätsangriffe dominieren, KI sucht ihren Weg und Bedrohungsgruppen reiben sich gegenseitig auf

Zwei Drittel der Sicherheitsvorfälle lassen sich auf Schwachstellen im Zusammenhang mit Identitäten zurückführen. Gleichzeitig agieren die Angreifer schneller und schlagen immer noch primär außerhalb der Geschäftszeiten zu.

Wiesbaden, 24. Februar 2026. Sophos stellt heute seinen neuen Active Adversary Report 2026 vor, der die Ergebnisse aus der Analyse von weit mehr als 600 realen Cyberangriffen präsentiert. Die Forschungen der Sophos Incident Response (IR)- und Managed Detection and Response (MDR)-Teams bestätigen, dass die Masche Identitätsklau weiter auf dem Vormarsch ist - 67 Prozent aller untersuchten Vorfälle waren identitätsbezogene Angriffe. Die Telemetrieauswertung zeigt, wie Angreifer vornehmlich kompromittierte Anmeldedaten, schwache oder fehlende Multifaktor-Authentifizierung (MFA) und schlecht geschützte Identitätssysteme ausnutzen – oft ohne neue Tools oder Techniken einsetzen zu müssen.

Zentrale Ergebnisse aus dem aktuellen Active Adversary Report:

- Eine Verlagerung von ausgenutzten Schwachstellen hin zu kompromittierten Anmeldedaten, wobei Brute-Force-Angriffe mit 15,6 Prozent als initiale Zugangsmethode fast gleichauf mit Exploits mit 16 Prozent liegen.
- Die durchschnittliche Verweildauer sank auf drei Tage. Dies ist auf mehr Effizienz der Angreifer, aber auch die schnellere Reaktion der Verteidiger zurückzuführen. Der Rückgang ist in MDR-Umgebungen besonders auffällig.
- Angreifer gelangen immer schneller zum Active Directory (AD). Hat es der feindliche Akteur ins Innere der Organisation geschafft, braucht er nur 3,4 Stunden, um den AD-Server zu erreichen.
- Ransomware-Angriffe finden hauptsächlich außerhalb der Geschäftszeiten statt. 88 Prozent der Attacken fanden zu den Schließzeiten der Unternehmen statt, ebenso wie 79 Prozent der Datenexfiltration.
- Ein Mangel an Telemetrie untergräbt die Verteidigung zusätzlich. Die Anzahl fehlender Protokolle aufgrund von Problemen bei der Datenspeicherung hat sich im Vergleich zum Vorjahr verdoppelt. Dieser Anstieg ist vor allem auf Firewalls zurückzuführen, bei denen die Standardeinstellung für die Log-Dateien nur sieben Tage und in einigen Fällen sogar nur 24 Stunden betrug.
- Die Multifaktor-Authentifizierung ist bei vielen Unternehmen immer noch nicht als wichtiges Sicherheitselement angekommen. In 59 Prozent der Fälle mangelte es an MFA und erleichtert so den Missbrauch gestohlener und kompromittierter Zugangsdaten.

„Die beunruhigendste Erkenntnis des Reports hat sich bereits über Jahre hinweg entwickelt: Die Dominanz identitätsbezogener Ursachen für einen erfolgreichen ersten Zugriff. Kompromittierte Anmeldedaten, Brute-Force-Angriffe, Phishing und andere Taktiken nutzen Schwächen aus, die sich nicht einfach durch Patch-Hygiene lösen lassen. Organisationen müssen einen proaktiven Ansatz zur Identitätssicherung verfolgen“, mahnt John Shier, Field CISO und Hauptautor des Berichts.

Mehr Bedrohungsgruppen, größere Risiken

Die Sophos-Analysten beobachteten die höchste Anzahl an aktiven Bedrohungsgruppen, die jemals in der Geschichte des Active Adversary Reports aufgezeichnet wurde. Damit weitet sich die Bedrohungslandschaft insgesamt aus und es wird immer schwieriger, die kriminellen Aktivitäten zuzuordnen. Akira (GOLD SAHARA) und Qilin (GOLD FEATHER) waren die

aktivsten observierten Ransomware-Gruppen, wobei Akira mit 22 Prozent der zugeordneten Vorfälle dominierte. Insgesamt tauchten 51 verschiedene Ransomware-Gruppen in allen Fällen auf, inklusive 27 wiederkehrende und 24 neue Gruppen. Nur vier Gruppen beziehungsweise Techniken bestehen dauerhaft seit 2020, dem ersten Jahr seit dem diese Daten im Active Adversary Report erhoben werden: LockBit, MedusaLocker, Phobos und der Missbrauch von BitLocker.

„Die Strafverfolgung sorgt weiterhin für Störungen im Ransomware-Ökosystem. Auch wenn wir immer noch Aktivitäten von LockBit sehen, sind dessen einstige Dominanz und Reputation eindeutig beeinträchtigt. Das bedeutet jedoch auch, dass eine Vielzahl an Gruppen um die Vorherrschaft wetteifern und dass wir viele neue aufstrebenden Gruppen sehen. Für die Verteidiger ist es wichtig, diese Dynamik und ihre TTPs zu verstehen, um die eigene Organisation bestmöglich zu schützen“, so Shier.

KI-Hype trifft auf Realität
Trotz weitverbreiteter Prognosen hat Sophos im vergangenen Jahr noch keinen Beweis für eine bedeutende, KI-getriebene Veränderung im Angreiferverhalten finden können. Während generative KI die Geschwindigkeit und Raffinesse von Phishing und Social Engineering ansteigen ließ, hat sie bislang noch keine grundlegend neue Angriffstechnik hervorgebracht.

„KI sorgt für mehr Umfang und Lärm, ersetzt aber noch keine Angreifer. Während generative KI in Zukunft der nächste Turbo sowohl für Angreifer als auch Verteidiger sein könnte, geht es heute noch immer um die Grundlagen: starker Identitätsschutz, zuverlässige Telemetrie und die Fähigkeit, schnell zu reagieren, wenn etwas schiefgeht“, so Shier.

Wichtige Erkenntnisse zur Verteidigung
Basierend auf den Ergebnissen des Active Adversary Reports 2026 empfiehlt Sophos Unternehmen fünf wichtige Schutzmaßnahmen:

- Phishing-resistente MFA bereitstellen und deren Konfiguration überprüfen
- Gefahr für die Identitätsinfrastruktur und der mit dem Internet verbundenen Dienste im Betrieb reduzieren
- Bekannte Schwachstellen unmittelbar patchen, besonders auf Edge-Geräten
- Mit MDR oder vergleichbaren Fähigkeiten für 24/7-Monitoring sorgen
- Sicherheitsprotokolle sichern und aufbewahren, um eine schnelle Entdeckung und Untersuchung zu unterstützen.

Für den Active Adversary Report 2026 wurden 661 IR- und MDR-Fälle zwischen 1. November 2024 und 31. Oktober 2025 analysiert. Die Angriffe betrafen Organisationen aus 70 Ländern und in 34 Branchen.

Den kompletten Active Adversary Report 2026 gibt es hier.

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 führender Anbieter im Bereich Cybersicherheit und schützt weltweit über 600.000 Unternehmen und Organisationen mit einer KI-gestützten Plattform und von Experten bereitgestellten Services. Sophos unterstützt Unternehmen und Organisationen unabhängig von ihrem aktuellen Sicherheitsniveau und entwickelt sich mit ihnen weiter, um Cyberangriffe erfolgreich abzuwehren. Die Lösungen von Sophos kombinieren maschinelles Lernen, Automatisierung und Echtzeit-Bedrohungsinformationen mit der menschlichen Expertise der Sophos X-Ops. So entsteht modernster Schutz mit einer 24/7 aktiven Erkennung, Analyse und Abwehr von Bedrohungen. Das Sophos-Portfolio beinhaltet branchenführende Managed Detection and Response Services (MDR) sowie umfassende Cybersecurity-Technologien – darunter Schutz für Endpoints, Netzwerke, E-Mails und Cloud-Umgebungen, XDR (Extended Detection and Response), ITDR (Identity Threat Detection and Response) und Next-Gen-SIEM. Ergänzt wird das Angebot durch Beratungs-Services, die Unternehmen und Organisationen helfen, Risiken proaktiv zu reduzieren und schneller zu reagieren – mit umfassender Transparenz und Skalierbarkeit, um Bedrohungen immer einen Schritt voraus zu sein. Der Vertrieb der Sophos-Lösungen erfolgt über ein globales Partner-Netzwerk, das Managed Service Provider (MSPs), Managed Security Service Provider (MSSPs), Reseller und Distributoren, Marketplace-Integrationen und Cyber Risk Partner umfasst. So können Unternehmen und Organisationen flexibel auf vertrauensvolle Partnerschaften setzen, wenn es um die Sicherheit ihres Geschäfts geht. Der Hauptsitz von Sophos befindet sich in Oxford, Großbritannien. Weitere Informationen finden Sie 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