Ransomware auf Speed ist die große Herausforderung für CISOs
Mit KI lasen Cyberkriminelle kaum noch Raum zwischen Angriff und Abwehr

Ein Kommentar von Michael Veit, Security-Experte bei Sophos

Künstliche Intelligenz (KI) verändert die Cyberbedrohungslandschaft nicht durch völlig neue Angriffsarten, sondern durch Skalierung, Geschwindigkeit und Präzision. Das bestätigen die Ergebnisse unseres neuen Sophos Active Adversary Report 2026**.** Angreifer nutzen KI als „Turbo“. Sie automatisieren bekannte Methoden wie Phishing oder Social Engineering und passen sie in Echtzeit an. In Folge stehen Unternehmen vor einer neuen Realität, in der Angriffe komplizierter zu erkennen sind und gleichzeitig schneller erkannt werden müssen.

KI ist Beschleuniger und kein Revolutionär
KI hat Cyberangriffe nicht neu erfunden, sondern ihre Ausführung optimiert. Statt handgefertigter Intrusionen dominieren heute automatisierte, adaptive Kampagnen, die auf bekannten Schwachstellen abzielen, darunter Identitäten, Zugriffslücken und Fehlkonfigurationen.

Der Active Adversary Report zeigt, dass beispielsweise die mittlere Verweildauer von Angreifern in Netzwerken bei nur noch drei Tagen liegt und Versuche, kritische Systeme wie Active Directory zu kompromittieren, oft innerhalb von Stunden erfolgen. KI verkürzt die Aufenthaltszeit der Cyberkriminellen, und damit auch die Reaktionszeit der Verteidiger, maßgeblich. Entscheidend ist also, wie gut Unternehmen auf diese schnellen Attacken vorbereitet sind. Zwei blinde Flecken bei Risiken durch KI-unterstütze Attacken werden von Unternehmen gerne unterschätzt.

An erster Stelle stehen die Gefahren durch eine fehlende Governance für nicht-menschliche Identitäten. Maschinenidentitäten – wie Service-Accounts oder API-Schlüssel – agieren rund um die Uhr, oft mit privilegiertem Zugriff, aber ohne klare Richtlinien. Wenn Zero Trust zwar für Nutzer und Geräte gilt, jedoch nicht für nicht-menschliche Identitäten, bleibt diese Angriffsfläche offen.

Die zweite große Gefahr liegt in den KI-Systemen selbst. Sie bieten eine zusätzliche Angriffsfläche. Zwar werden die KI-Plattformen wie andere Anwendungen auch gesichert und geschützt, jedoch werden oftmals die KI-spezifischen Risiken wie Prompt-Injection oder Datenmanipulation ignoriert.

Drei Strategien für CISOs im KI-Zeitalter

1. **Identitätsbasierte Erkennung**: Anmeldeinformations- und Token-Missbrauch sind bereits Angriffe und nicht nur Indikatoren für eine bevorstehende Attacke. Unternehmen sollten die Transparenz und Sicherheit aller Arten von Identitäten priorisieren.
2. **Tiefere Telemetrie statt Tool-Vielfalt:** Mehr Tools bedeuten nicht schnellere Reaktion. Ausschlaggebend ist die Korrelation und Anreicherung von Daten, um Angriffe in Echtzeit zu erkennen.
3. **Automatisierung mit klaren Grenzen**: Reversible Maßnahmen – wie Token-Sperrung oder Geräteisolation – sollten automatisiert werden. Bei irreversiblen Entscheidungen bleibt der Mensch im Loop.

Die Geschwindigkeit ist entscheidet. Denn die größte Gefahr ist aktuell nicht die kreative Kraft der künstlichen Intelligenz in Händen der Bedrohungsakteure, sondern die Lücke zwischen Angriffs- und Abwehrgeschwindigkeit. Während Angreifer die KI nutzen, um die erste Phase ihres Angriffs – die Reconnaissancen – in Minuten durchzuführen und Angriffe zu optimieren, hinken viele Unternehmen aufgrund der fehlenden Vernetzung und Automatisierung ihrer Abwehrmechanismen hinterher. Die Bündelung in einem synchronisierten Cybersecurity-Ökosystem inklusive der effektiven KI-Nutzung auf Unternehmensseite kann „Ransomware auf Speed“ in die Grenzen weisen.

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