KEEPER | Pressemitteilung

Neue Keeper Security Studie:
KI ist Treiber einer neuen Generation fortschrittlicher Cyberangriffe

Neue Daten zeigen, dass KI die Erkennung von Phishing- und Smishing-Angriffen erschwert. 84 % der IT-Führungskräfte bestätigen die zunehmende Herausforderung.

MÜNCHEN, 10. Oktober 2024 – Das Aufkommen und die kontinuierliche Weiterentwicklung von Künstlicher Intelligenz (KI) verändert die Cybersicherheit und führt zu einer neuen Komplexität bei der Erkennung und Abwehr von Bedrohungen. Neue Forschungsergebnisse von Keeper Security, einem führenden Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Passwörtern, Passkeys, privilegiertem Zugang und Remote-Verbindungen, zeigen, dass Organisationen zwar KI-bezogene Richtlinien umsetzen, jedoch nach wie vor eine erhebliche Herausforderung besteht, vollständig auf den Umgang mit KI-gesteuerten Bedrohungen vorbereitet zu sein.

Laut der Keeper-Umfrage sind 84 Prozent der IT- und Sicherheitsverantwortlichen der Meinung, dass Phishing- und Smishing-Angriffe – ohnehin schon eine kritische Bedrohung – durch KI-Tools noch schwieriger zu erkennen sind. Als Reaktion darauf haben 81 Prozent der Unternehmen KI-Nutzungsrichtlinien für Mitarbeiter eingeführt. Das Vertrauen in diese Richtlinien ist ebenfalls hoch: 77 Prozent der Führungskräfte geben an, dass sie mit den Best Practices für die KI-Sicherheit entweder sehr gut oder gut vertraut sind.

Trotz dieser Bemühungen besteht die Lücke zwischen Richtlinien und dem Umgang mit KI-gesteuerten Bedrohungen weiterhin. Der Bericht „2024 Top Data Threats“ von Keeper zeigt, dass 51 Prozent der Sicherheitsverantwortlichen KI-gestützte Angriffe als die größte Bedrohung für ihre Unternehmen ansehen. Zudem sind 35 Prozent der Meinung, dass ihre Unternehmen im Vergleich zu anderen Arten von Cyber-Bedrohungen am wenigsten auf die Bekämpfung dieser Angriffe vorbereitet sind.

Um diese neuen Herausforderungen zu bewältigen, konzentrieren sich Unternehmen auf mehrere Schlüsselstrategien:

- **Datenverschlüsselung:** Dies ist die am weitesten verbreitete Maßnahme: 51 Prozent der IT-Leiter haben sie in ihre Sicherheitsstrategien aufgenommen. Verschlüsselung hilft dabei, sensible Daten vor unbefugtem Zugriff zu schützen, was für die Abwehr von KI-gesteuerten Angriffen entscheidend ist.
- **Schulung und Sensibilisierung der Mitarbeiter:** Mit hoher Priorität konzentrieren sich 45 Prozent der Unternehmen auf die Verbesserung ihrer Schulungsprogramme, um ihre Mitarbeiter besser auf die sich entwickelnde Bedrohungslandschaft vorzubereiten. Wirksame Schulungen können den Mitarbeitern helfen, KI-gestützte Phishing- und Smishing-Versuche zu erkennen und darauf zu reagieren.
- **Erweiterte Erkennungssysteme für Bedrohungen:** Mit 41 Prozent der Organisationen, die in diese Systeme investieren, liegt ein klarer Schwerpunkt darauf, die Fähigkeit zur Erkennung und Reaktion auf ausgeklügelte, KI-gesteuerte Bedrohungen zu verbessern. Fortschrittliche Threat-Detection-Lösungen können frühzeitige warnen und potenziellen Schaden durch diese Angriffe mindern.

Das Aufkommen von KI-gesteuerten Cyberangriffen stellt neue Herausforderungen dar. Die grundlegenden Cybersicherheitspraktiken – wie Datenverschlüsselung, Mitarbeiterschulungen oder fortschrittliche Bedrohungserkennung – bleiben weiterhin essenziell. Organisationen müssen sicherstellen, dass diese grundlegenden Maßnahmen regelmäßig aktualisiert und an neue Bedrohungen angepasst werden.

Zusätzlich zu diesen grundlegenden Maßnahmen kann die Einführung von fortschrittlichen Sicherheits-Frameworks wie Zero Trust und die Implementierung von Privileged Access Management (PAM)-Lösungen wie KeeperPAM die Widerstandsfähigkeit erheblich verbessern. Zero Trust stellt sicher, dass jeder Anwender, jedes Gerät und jede Anwendung kontinuierlich überprüft wird, bevor auf kritische Systeme zugegriffen wird. Damit wird das Risiko eines unbefugten Zugriffs minimiert und der Radius der Ausbreitung im Falle eines Angriffs begrenzt. PAM trägt dazu bei, die sensiblen Konten eines Unternehmens zu schützen, indem es den privilegierten Zugriff kontrolliert, überwacht und prüft. Dies ist für die Abwehr ausgeklügelter KI-gesteuerter Angriffe, die auf sensible Anmeldeinformationen abzielen, besonders wichtig.

Unternehmen sollten zudem proaktiv handeln, indem sie regelmäßig ihre Sicherheitsrichtlinien überprüfen, Routine-Audits durchführen und eine Kultur des Cybersecurity-Bewusstseins fördern. Auch wenn Unternehmen Fortschritte machen, ist Cybersicherheit ein sich ständig weiterentwickelnder Bereich, der ständige Wachsamkeit erfordert. Die Kombination grundlegender Praktiken mit modernen Ansätzen wie Zero Trust und PAM hilft Unternehmen, den sich entwickelnden KI-gestützten Bedrohungen einen Schritt voraus zu sein.

Weitere Informationen zu den Erkenntnissen und wichtigen Statistiken finden Sie in der Infografik von Keeper.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die intuitiven Lösungen von Keeper basieren auf einer End-to-End-Verschlüsselung, um jeden Anwender auf jedem Gerät und an jedem Standort zu schützen. Die Keeper Zero-Trust-Plattform für die Verwaltung von privilegierten Zugängen ist in wenigen Minuten einsatzbereit. Sie lässt sich nahtlos in jeden Technologie-Stack integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern und Tausenden von Unternehmen und ist führend bei der Verwaltung von Passwörtern, Passkeys und Geheimnissen, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie, wie die Zero-Trust- und Zero-Knowledge-Lösungen vor Cyber-Bedrohungen schützen auf KeeperSecurity.com.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de