KEEPER | Pressemitteilung

Keeper Security Insight Report 2024: Cyberangriffe sind ausgefeilter denn je und KI-gestützte Angriffe stellen das größte Risiko dar

Keeper Security Insight Report zeigt, dass IT-Verantwortliche auf die neue Welle von Bedrohungsvektoren nicht genügend vorbereitet sind

München, 26. März 2024 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, veröffentlicht heute seinen Keeper Security Insight Report 2024 „*The Future of Defense: IT Leaders Brace for Unprecedented Cyber Threats*“.

Die Umfrage, die weltweit unter mehr als 800 IT- und Sicherheitsverantwortlichen durchgeführt wurde zeigt, welche Rolle aufkommende Technologien in der sich entwickelnden Bedrohungslandschaft spielen und wie sehr IT-Führungskräfte damit kämpfen, Schritt zu halten. Die Umfrageteilnehmer bezeichnen KI-gestützte Angriffe als den schwerwiegendsten neuen Angriffsvektor und als die größte Herausforderung, die es zu bewältigen gilt. Cyberkriminelle werden zunehmend raffinierter, knacken Lösungen, die bisher als sicher galten und fügen Organisationen in allen Branchen Schaden zu. Diese Risikopotenziale machen eine weitreichende und gezielte Cybersicherheit wichtiger als je zuvor.

Mehr Raffinesse durch neue Technologien

Weltweit gaben 92 Prozent (in Deutschland 97 Prozent) der Befragten an, dass die Zahl der Cyberangriffe im Vergleich zum Vorjahr zugenommen hat. Parallel zur zunehmenden Häufigkeit geben 95 Prozent der IT-Führungskräfte weltweit und in Deutschland an, dass Cyberangriffe ausgefeilter sind als je zuvor und dass sie auf diese neue Welle von Bedrohungsvektoren nicht vorbereitet sind.

IT-Führungskräfte nennen folgende neue Angriffsvektoren für ihr Unternehmen als am schwerwiegendsten:

- KI-gestützte Angriffe - 51 Prozent (50 Prozent in Deutschland)
- Deepfake-Technologie und Angriffe auf die Lieferkette - beide 36 Prozent (31 Prozent in Deutschland)
- Cloud Jacking - 35 Prozent (22 Prozent in Deutschland)
- Angriffe auf das Internet der Dinge (IoT) und 5G-Netzwerke - beide 34 Prozent (29 Prozent in Deutschland)
- Dateilose Angriffe – 24 Prozent (24 Prozent in Deutschland)

IT-Führungskräfte sehen ihr Unternehmen bei folgenden Angriffsvektoren schlecht gerüstet, da es ihnen an Abwehrmöglichkeiten fehlt:

- KI-gestützte Angriffe – 35 Prozent (30 Prozent in Deutschland)
- Deepfake-Technologie - 30 Prozent (34 Prozent in Deutschland)
- Ausnutzung von 5G-Netzwerken - 29 Prozent (34 Prozent in Deutschland)
- Cloud Jacking – 25 Prozent (20 Prozent in Deutschland)
- Dateilose Angriffe – 23 Prozent (14 Prozent in Deutschland)

Auch bei einer Vorbereitung für die Bewältigung neuer Angriffstechniken, müssen sich IT- und Sicherheitsverantwortliche mit aktuellen Problemen auseinandersetzen: 73 Prozent weltweit und 71 Prozent der in Deutschland Befragten haben Cyberangriffe erlebt, die zu einem finanziellen Verlust geführt haben. Direkte finanzielle Auswirkungen sind eine von vielen Folgen eines „erfolgreichen“ Cyberangriffs, neben der Unterbrechung des Geschäftsbetriebs, den dauerhaften Umsatzeinbußen, der Abwanderung von Kunden und Partnern und einem geschädigten Ruf.

„Cyberkriminelle richten auf neuartige Art und Weise Schaden in Organisationen an und nutzen dafür neue Technologien, um die verheerenden Cyberangriffe durchzuführen", sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Dies zeigt klar die Notwendigkeit eines kontinuierlich proaktiven Ansatzes für die Cybersicherheit, der fortschrittliche Verteidigungsmechanismen und Best Practices kombiniert, um neue Bedrohungen zu erkennen und Cyberangriffe abzuwehren.“

Angriffe von heute bewältigen
Während neuartige Bedrohungen ihren Schatten vorauswerfen, sind IT-Führungskräfte bei der Bekämpfung der heute am häufigsten vorkommenden Bedrohungsvektoren überfordert – wobei die folgenden Angriffsarten direkte Auswirkungen auf ihre Unternehmen haben:

- Phishing - 61 Prozent (64 Prozent in Deutschland)
- Malware - 59 Prozent (53 Prozent in Deutschland)
- Ransomware – 49 Prozent (39 Prozent in Deutschland)
- Passwortangriffe - 38 Prozent (26 Prozent in Deutschland)

Die explosionsartige Entwicklung von KI-Tools hat Probleme wie Phishing-Angriffe noch verschärft. Die KI-Tools täuschen bei Betroffenen eine höhere Glaubwürdigkeit der Betrugsversuche vor und ermöglichen es den Cyberkriminellen zudem, diese Betrugsmasche in größerem Umfang einzusetzen. 84 Prozent der Befragten gaben an, dass Phishing und Smishing mit der zunehmenden Popularität von KI-gestützten Tools schwieriger zu erkennen sind. Sie gaben zudem an, dass KI-gestütztes Phishing ihre größte Sorge (42 Prozent) ist, wenn es um KI-Sicherheit geht. Neben Phishing setzen Cyberkriminelle KI ein, um andere gängige Angriffstechniken wie das Knacken von Passwörtern zu beschleunigen und zu skalieren.

Zu den zahlreichen Cyberangriffen, die immer häufiger auftreten, gehören nach Ansicht der Befragten folgende:

- Phishing - 51 Prozent (52 Prozent in Deutschland)
- Malware - 49 Prozent (38 Prozent in Deutschland)
- Ransomware - 44 Prozent (32 Prozent in Deutschland)
- Passwortangriffe – 31 Prozent (20 Prozent in Deutschland)

Gestohlene oder schwache Passwörter und Anmeldedaten sind nach wie vor eine der Hauptursachen für Sicherheitsverletzungen. 52 Prozent weltweit und 48 Prozent der deutschen Umfrageteilnehmer gaben an, dass das IT-Team ihres Unternehmens häufig mit gestohlenen Passwörtern zu kämpfen hat. Dies bestätigt die Wichtigkeit, eindeutige Passwörter für jedes Konto zu erstellen und sicher zu speichern.

Die Zukunft der Verteidigung
Da neue Technologien bestehende Angriffsvektoren verstärken und zudem neue Bedrohungen schaffen, steht für IT- und Sicherheitsverantwortliche mehr denn je auf dem Spiel. Auch bei der sich ständig verändernden Bedrohungslandschaft bleiben die grundlegenden Regeln für den Schutz eines Unternehmens im digitalen Zeitalter relevant. Die Integration von Lösungen, die die häufigsten Cyberangriffe abwehren, einschließlich Passwort- und Privileged Access Management (PAM)-Lösungen, schafft einen mehrschichtigen Sicherheitsansatz, der heute und in Zukunft Bestand hat.

Laden Sie den vollständigen Bericht herunter, um mehr zu erfahren.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: Facebook Instagram LinkedIn X YouTube

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