KEEPER | Pressemitteilung

Keeper Security Insight Report: Steuerung einer hybriden Authentifizierungs-Landschaft

Keepers Report enthüllt: während 80 Prozent der Organisationen Passkeys einsetzen, berichten 57 Prozent der IT-Führungskräfte von Herausforderungen bei der Verwaltung von dualen Authentifizierungssystemen.

MÜNCHEN, 24. Januar 2025 – Keeper Security, der führender Anbieter der Zero-Trust- und Zero-Knowledge-Lösung Privileged Access Management (PAM)-Software zum Schutz von Passwörtern, Passkeys, privilegiertem Zugang und Remote-Verbindungen, veröffentlicht seinen aktuellsten Insight Report „Navigating a Hybrid Authentication Landscape“. Der Report untersucht, wie sich die Strategien von Organisationen entwickeln, um sensible Daten und Identitäten zu sichern, angesichts einer stetig komplexeren digitalen Umgebung. Während sich die traditionelle Passwort-basierte Authentifizierung wachsenden Gefahren gegenübersieht, inklusive Phishing und Credential Stuffing (Angreifer nutzen gestohlene Anmeldedaten für unberechtigte Zugänge zu Konten), setzen immer mehr Unternehmen auf innovative Lösungen wie Passkeys, um ihre Sicherheit zu stärken. Allerdings bleiben Passwörter ein integraler Bestandteil vieler veralteter Systeme, was die Notwendigkeit eines hybriden Ansatzes, der Passkeys und Passwörter kombiniert, zur Folge hat.

Die Ergebnisse des Keeper Reports, der auf den Einblicken von Führungskräften in den Bereichen IT und Sicherheit beruht, betonen die Verbindung zwischen aufstrebenden Authentifizierungs-Technologien und dem Fortbestehen von Passwörtern beim Schutz von Online-Systemen. Der Report liefert einen detaillierten Blick darauf, wie Organisationen mit diesen Herausforderungen umgehen und gleichzeitig eine solide Sicherheit aufrechterhalten.

Zentrale Ergebnisse des Keepers’ Reports:

- **Mehrheit der Organisationen wendet Passkeys an**: Passkeys, die die Kryptografie mit öffentlichen Schlüsseln verwenden, um Nutzer zu authentifizieren, ohne dass diese ein Passwort eingeben müssen, sind auf dem Vormarsch. 80 Prozent der Unternehmen nutzen oder planen die Nutzung von Passkeys, da sie deutlich die Risiken wie Phishing und Credential Stuffing gegenüber traditionellen Passwörtern verringern.

- **Hybride Authentifizierung ist üblich**: 40 Prozent der Unternehmen vertrauen weiterhin auf hybride Authentifizierungs-Systeme, die Passwörter und Passkeys mischen. Dieser hybride Aufbau ist oft notwendig aufgrund der noch weit verbreiteten alten Systeme und spezialisierter Anwendungen, die noch keine Passkeys unterstützen.

- **Phishing bleibt eine dauerhafte Gefahr**: Trotz der Anwendung von Passkeys bleibt Phishing eine große Bedrohung. 67 Prozent der Unternehmen benennen Phishing als ständiges Problem in hybriden Authentifizierung-Umgebungen, und unterstreichen damit die Notwendigkeit umfassender Sicherheitsmaßnahmen, die über die reinen Passkeys hinausgehen.

- **IT-Führungskräfte sind mit den Herausforderungen des dualen Systems konfrontiert**: Die Verwaltung von Passwörtern und Passkeys stellt für 57 Prozent der IT-Verantwortlichen eine große Herausforderung dar, beispielweise wegen der Verwirrung der Anwender, Integrationsschwierigkeiten und dem Schulungsbedarf bei der Verwaltung hybrider Systeme.

- **Schrittweise Annahme von Passkeys**: 70 Prozent der Organisationen, die Passkeys einsetzen, implementieren diese schrittweise, mit Fokus auf die wichtigen Systeme und der Gewährleistung operationaler Kompatibilität mit bereits bestehenden Passwort-basierten Systemen.

Der Report betont die Notwendigkeit für Organisationen, einen mehrschichtigen Ansatz zur Authentifizierung anzuwenden, und moderne Lösungen wie Passkeys mit bewährter Passwort-Praxis abzustimmen. Er betont auch die Bedeutung von Mitarbeiterschulungen, der Aufrüstung der Infrastruktur und verschlankter Integration, um die Sicherheit und Nutzbarkeit von Authentifizierungs-Systemen sicherzustellen, während Unternehmen ihre digitale Transformation fortsetzen.

„Organisationen sind dabei, einen entscheidenden Wandel bei der Authentifizierung herbeizuführen, indem sie die Notwendigkeit für moderne Passkeys mit der Verlässlichkeit von Passwörtern für viele ältere Systeme abwägen“, betont Darren Guccione, CEO und Co-Gründer von Keeper Security. „Unsere Mission ist es, umfassende Lösungen anzubieten, die jede Art der Berechtigung verwalten und absichern – von traditionellen Passwörtern bis zu Passkeys – all das innerhalb eines Zero-Trust und Zero-Knowledge-Rahmens. Dieser Ansatz gewährleistet, dass Organisationen sich vertrauensvoll an die hybride Authentifizierungs-Landschaft anpassen können, während sie gleichzeitig die höchsten Standards an Sicherheit und Nutzbarkeit beibehalten.“

Angesichts der Data Privacy Week diese Woche, ist der Report von Keeper Security eine rechtzeitige Erinnerung an die wichtige Rolle von Authentifizierung bei der Absicherung sensibler Informationen. Im Hinblick auf die kontinuierliche Zunahme von Cybergefahren müssen Organisationen bei der Umsetzung flexibler und sicherer Authentifizierungs-Methoden proaktiv bleiben, um für die neuen Risiken gewappnet zu sein.

Detaillierte Einblicke und den vollständigen Zugang zum Keeper Security Insight Report gibt es hier.

###

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