Ob es einem gefällt oder nicht, Passwörter werden bleiben

Der S&P Market Intelligence Business Impact Brief zeigt, dass Unternehmen in absehbarer Zukunft weiterhin Passwörter verwenden.

München, 12. Oktober 2023 – Keeper Security, führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, hat heute einen Bericht von S&P Market Intelligence veröffentlicht. Aus diesem geht hervor, dass Kombinationen aus Benutzername und Passwort immer noch die am häufigsten eingesetzte Form der Authentifizierung in Unternehmen sind (58 Prozent). Die nächstbeliebten Formen der Authentifizierung sind mobile Push-basierte Multi-Faktor-Authentifizierung (MFA) (47 Prozent), SMS-basierte MFA (40 Prozent) und biometrische Verfahren (31 Prozent).

„Passwörter werden nach wie vor am häufigsten eingesetzt, da Unternehmen ein Gleichgewicht zwischen Sicherheit, Einfachheit, Betriebskosten und Flexibilität anstreben - insbesondere in hybriden Arbeitsumgebungen", sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „SSO und passwortlose Authentifizierung werden - obwohl sie effektiv sind - nicht allgemein unterstützt und schaffen daher Sicherheitslücken, die Unternehmen angreifbar machen. Für Unternehmen, die noch immer auf die Kombination aus Passwort und Benutzername oder auf ein Hybridmodell aus Passwörtern und passwortlosen Technologien setzen, ist es entscheidend, dass diese angemessen und sicher verwaltet werden."

Passwortmanagement erhöht Sicherheit für alle Authentifizierungsmethoden
Der S&P Market Intelligence Business Impact Brief zeigt, dass die weit verbreitete Verwendung von Benutzernamen-Passwort-Kombinationen umfassende Passwort-Management-Richtlinien für Unternehmen erfordert, um sicherzustellen, dass die Passwort-Praktiken der Mitarbeiter so sicher wie möglich sind. Passwort-Manager erleichtern sowohl IT-Administratoren als auch Endbenutzern das Erstellen, Rotieren und Speichern von Passwörtern sowie von 2FA- und MFA-Codes. Tatsächlich verwenden viele Unternehmen eine Kombination aus mehreren Authentifizierungsfaktoren, um die Kombinationen aus Kennwort und Benutzername zu ergänzen, was die Integration eines Passwortmanagements zu einer noch größeren Notwendigkeit macht.

Der Passkey ist da, die breite Adaption dauert aber noch
Vor allem aufgrund der Dynamik der Fast Identity Online (FIDO) Alliance gewinnen Passkeys als eine Form der passwortlosen Authentifizierung mit Unterstützung von Apple, Microsoft und Google an Bedeutung. Passkeys sind passwortlose Berechtigungsnachweise, die es Verbrauchern wesentlich einfacher machen, FIDO-basierte Authentifizierungssysteme zu übernehmen. Im Hinblick auf die Einführung in Unternehmen befinden sich Passkeys jedoch noch in einem sehr frühen Stadium.

„Obwohl Passkeys verlockende Sicherheitsvorteile bieten, werden sie von Websites aus verschiedenen Gründen nur langsam unterstützt. Bei mehr als einer Milliarde Websites ist es noch ein langer Weg, bis eine passwortlose Option allgegenwärtig wird", so Guccione. „Da die Kombination aus Passwort und Benutzername auf absehbare Zeit ein wichtiger Bestandteil der Unternehmenslandschaft bleiben wird, sind Passwortmanagement-Lösungen, die eine breite Palette von Authentifizierungsmethoden integrieren und unterstützen und gleichzeitig Sicherheit und Cyber-Hygiene gewährleisten, für alle Unternehmen wichtig, um die Cyber-Resilienz zu erhöhen.

Der vollständige Bericht kann hier heruntergeladen werden:
https://www.keeper.io/hubfs/S&P_Global_Password_Report_2023.pdf

Über Keeper Security Inc.
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.

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