Pressemitteilung

Keeper Security unterstützt Hardware-Sicherheitsschlüssel als solitäre 2FA-Methode

Geschäfts- und Privatanwender haben jetzt noch mehr Kontrolle über die Verwendung von Sicherheitsschlüsseln zur bequemen und hochsicheren Authentifizierung

München, 17. Januar 2024 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, unterstützt die Benutzerauthentifizierung, bei der nur ein Hardwaresicherheitsschlüssel für die Zwei-Faktor-Authentifizierungsmethode (2FA) verwendet wird. Die Benutzerauthentifizierung mit nur einem Hardwareschlüssel erhöht die Sicherheit, indem sie einen robusten physischen zweiten Faktor bietet, Remote-Angriffe reduziert und die Abhängigkeit von mobilen Geräten reduziert. Administratoren können die Verwendung eines Hardwareschlüssels als einzige 2FA-Methode erzwingen und sogar noch strengere Einschränkunegn etablieren, indem sie die Verwendung einer PIN verlangen.

Stärkere Authentifizierungsfaktoren werden zunehmend wichtiger, da Cyberkriminelle immer raffinierter vorgehen und die bisher als sicher geltenden Schutzmechanismen aushebeln. Herkömmliche 2FA-Methoden wie SMS und Time-Based One-Time Password (TOTP) können für Social Engineering und SIM-Austausch anfällig sein. Das National Institute of Standards and Technology (NIST) hat die SMS-Authentifizierung aufgrund ihrer Schwachstellen sogar von der Liste der empfohlenen Authentifizierungsmethoden gestrichen. Dies hat dazu geführt, dass sowohl Unternehmen als auch Einzelpersonen nach sichereren 2FA-Alternativen suchen.

„Cyberkriminelle sind kreativ und unerbittlich, um bisher sichere Lösungen zu knacken", sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Als Reaktion darauf steigen viele Unternehmen auf hardwarebasierte 2FA-Geräte wie YubiKey um. Mit Keeper können Administratoren nun die Verwendung eines Hardware-Sicherheitsschlüssels als einzige 2FA-Option erzwingen und den Benutzern eine einfache und benutzerfreundliche und dennoch hochsichere Authentifizierungsmethode zur Verfügung stellen."

Die Unterstützung von Hardware-Security-Schlüsseln ist für Keeper nicht neu. Allerdings benötigten Benutzer bisher zusätzlich zur Verwendung des Sicherheitsschlüssels eine Backup-2FA-Option. Jetzt können Privat- und Geschäftskunden gleichermaßen einen Sicherheitsschlüssel als einzige 2FA-Methode verwenden. Keeper ermöglicht es Benutzern, mehrere Sicherheitsschlüssel zu haben, z. B. Backup-Schlüssel, Schlüssel an verschiedenen Orten oder Schlüssel für mehrere Geräte.

Bestehende Benutzer können sich im Keeper Web Vault oder in der Keeper Desktop App Version 16.10.12+ anmelden und andere 2FA-Methoden entfernen, wenn sie stattdessen lieber einen Sicherheitsschlüssel verwenden möchten. Administratoren können zudem die Verwendung einer PIN (FIDO2-Benutzerverifizierung) zusätzlich zur Verwendung des Sicherheitsschlüssels festlegen, um die Sicherheit noch weiter zu erhöhen.

Keeper unterstützt die Anmeldung mit einem Sicherheitsschlüssel auf iOS- und Android-Geräten. Die Einrichtung eines Sicherheitsschlüssels als einzige 2FA-Methode muss über den Web Vault oder die Keeper Desktop App erfolgen.

Dies ist die neuste einer ganzen Reihe von Keeper-Produkterweiterungen, einschließlich der letzten Ankündigung über Granular Sharing Enforcements. Unternehmen entscheiden sich für Keeper aufgrund seiner starken Sicherheitsarchitektur, der Fähigkeit, passwortlose Authentifizierung mit jedem Identitätsanbieter zu unterstützen, der nahtlosen Integration in lokale, Cloud- oder hybride Umgebungen sowie der einfachen Nutzung über Desktop- und Mobilgeräte. Der Keeper Security Government Cloud Password Manager und der Privileged Access Manager sind FedRAMP- und StateRAMP-autorisiert und bauen auf dem Keeper Security Zero-Trust-Sicherheitsframework sowie der Zero-Knowledge-Sicherheitsarchitektur auf. Damit haben Benutzer vollständige Transparenz, Verwaltung und Kontrolle über ihre Anmeldedaten und Verschlüsselungs-Keys.

###

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 Sie Keeper auf 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