Keeper Security führt 24-Word-Recovery-Phrasen ein, um die Account-Sicherheit zu erhöhen

München, 27. April 2023 – Keeper Security, führender Anbieter von Zero-Trust- und Zero-Knowledge-Cyber-Security-Lösungen zum Schutz von Passwörtern, Daten und Verbindungen, gibt heute die Einführung seiner neuesten Funktion, der 24-Word-Recovery-Phrasen, bekannt. Diese neue und sicherere Methode der Kontowiederherstellung wurde entwickelt, um Keeper-Anwendern ein Höchstmaß an Schutz vor neuen Bedrohungen zu bieten.

Die 24-Word-Recovery-Phrase ersetzt die derzeitige, vom Benutzer anpassbare Recovery-Methode mit Sicherheitsfrage und Antwort. Sie dient als "Break-Glass"-Methode zur Wiederherstellung eines Keeper Vault für den Fall, dass ein Anwender sein Master-Passwort vergisst. Diese Recovery-Phrase generiert einen einzigartigen 256-Bit-AES-Schlüssel, der eine Kopie des 256-Bit-AES-Datencode des Benutzers entschlüsselt. Der Datenschlüssel dekodiert dann jeden einzelnen Datensatzschlüssel, der seinerseits wiederum jeden Datensatz des Passwortmanagers entschlüsselt.

Keeper hat bei der Implementierung der Recovery-Phrasen die gleiche BIP39-Wortliste verwendet, die zum Schutz von Krypto-Wallets eingesetzt werden. Die in BIP39 verwendete Wortliste besteht aus 2.048 Wörtern, die zur Generierung eines Verschlüsselungscodes mit einer Entropie von 256 Bit verwendet werden. Diese Wiederherstellungsmethode wird häufig in beliebten Bitcoin- und Kryptowährungs-Wallets verwendet. Jedes Wort in der BIP39-Liste ist sorgfältig ausgewählt, um die Sichtbarkeit zu verbessern und Fehler bei der Wiederherstellung zu minimieren.

„Wir freuen uns, unseren Nutzern diese revolutionäre neue Funktion vorstellen zu können", sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Wir sind bestrebt, unseren Kunden die modernsten und sichersten Lösungen für ihr Passwortmanagement zu bieten. Die 24-Word-Recovery-Phrase ist nur ein Beispiel dafür, wie wir durch kontinuierliche Investitionen in neue und robustere Technologien, zukünftigen Cyber-Bedrohungen begegnen."

Anwender, die in ihrem Passwortmanager Sicherheitsfragen aktiviert haben, werden aufgefordert, ihre Sicherheitsantwort durch eine starke 24-Word-Recovery-Phrase zu ersetzen. Es ist wichtig, dass die Anwender diese Recovery-Phrase an einem sicheren Ort, beispielsweise in einem physischen Tresor aufbewahren und nicht auf einem Computer, Smartphone oder ähnlichem Gerät speichern. Zur Wiederherstellung des Kontos und zum Zurücksetzen des Hauptkennworts benötigen die Nutzer die Recovery-Phrase sowie einen E-Mail-Verifizierungscode. Anwender mit einer aktivierten Zwei-Faktor-Authentifizierung (2FA) müssen zusätzlich diesen Authentifizierungsschritt durchlaufen.

Administratoren von Geschäfts- und Unternehmenskonten haben die Möglichkeit, die Kontowiederherstellung für ihre Benutzer in den Rollenrichtlinien auf der Keeper Admin-Konsole zu deaktivieren. Die Kontowiederherstellung kann mit SSO-aktivierten Konten verwendet werden, sofern das vom Keeper-Administrator unterstützt wird.

Es ist wichtig zu wissen, dass ein Anwender, der sein Master-Passwort vergisst und seine Wiederherstellungsphrase verliert, keinen Zugriff auf seinen Keeper-Passwortmanager hat. Aufgrund der Zero-Knowledge-Architektur von Keeper kann das Keeper-Team nicht dabei helfen, eine verlorene Recovery-Phrase wiederherzustellen.

Um die neue Funktion nutzen zu können, sollten die Anwender sicherstellen, dass alle ihre Keeper-Anwendungen auf dem neuesten Stand sind.

Weitere Information über die Keeper Passwort-Management-Plattform sowie die 24-Word-Recovery-Phrase sind unter Keeper's Documentation Portal und Release Notes zu finden.

Über Keeper Security Inc.
Keeper Security verändert die Art und Weise, wie Menschen und Organisationen auf der ganzen Welt ihre Passwörter, Geheimnisse und vertraulichen Informationen schützen. Die benutzerfreundliche Cybersecurity-Plattform von Keeper basiert auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer und jedes Gerät zu schützen. Die Lösung ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in die Systemumgebung integrieren, um Datenschutzverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Einhaltung von Vorschriften zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelpersonen und Tausenden von Unternehmen auf der ganzen Welt und ist der führende Anbieter von erstklassigem Passwortmanagement, Geheimnismanagement, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Schützen Sie, was wichtig ist, auf 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