KEEPER | Pressemitteilung

Keeper Security jetzt mit integriertem Passphrase-Generator

Mit Passphrasen, die nahtlos in Keeper generiert und gespeichert werden, genießen Anwender einen verbesserten Cybersecurity-Schutz, ohne auf Komfort verzichten zu müssen.

MÜNCHEN, 17. April 2024 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, kündigt heute seinen neuen Passphrase-Generator an. Der Passphrase-Generator ist eine Erweiterung im Keeper Web Vault, der für mobile Endgeräte und als Browser-Erweiterung in Kürze zur Verfügung steht. Die neue Version enthält zudem ein Update des bestehenden Passwort-Generators. Dieser bietet den Benutzern zusätzliche Optionen, um spezifische Passwortanforderungen zu erfüllen. Neben der Möglichkeit, Großbuchstaben, Zahlen und Symbole zu verwenden, stehen nun auch bestimmte Symbole zur Wahl, die je nach den Anforderungen der Website, für die das Passwort erstellt wird, hinzugefügt werden können.

„Die neuen Updates für die Passphrasen-Integration und den Passwort-Generator von Keeper ermöglichen es den Nutzern, hochsichere Passphrasen und Passwörter zum Schutz ihrer Online-Konten zu erstellen", sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Die Neuerungen erhöhen nicht nur die Sicherheit für private und geschäftliche Anwender, sondern vereinfachen auch die Nutzererfahrung – was mit unserem Bestreben, leicht zu bedienende Cybersicherheitslösungen, die die Sicherheit verbessern und die Produktivität steigern, in Einklang steht."

Der Schutz sensibler Informationen ist in der heutigen vernetzten Welt von entscheidender Bedeutung. Die weit verbreitete Verwendung schwacher und sich wiederholender Passwörter führt dazu, dass viele Einzelpersonen und Unternehmen nur unzureichend gegen die zunehmend verbreiteten und ausgefeilten Cyber-Bedrohungen geschützt sind. Der integrierte Passwort- und Passphrasen-Generator von Keeper macht es einfach, starke, eindeutige Anmeldedaten für jedes Konto zu erstellen. Mit den granularen Administratorkontrollen können Unternehmen allgemeine Richtlinien für Passwörter und Passphrasen sowie zeichenspezifische Richtlinien für bestimmte Websites und Anwendungen durchsetzen.

Passphrasen bieten mehrere Vorteile gegenüber herkömmlichen Passwörtern. Beispielsweise sind sie länger und von Natur aus komplexer, jedoch leichter zu merken. Sie bestehen aus mehreren aneinandergereihten Wörtern. Je mehr Wörter eine Passphrase enthält, desto länger ist sie und desto schwieriger ist sie für Cyberkriminelle zu knacken. Passwörter hingegen bestehen aus einer Reihe von Zeichen. Um ein Konto richtig abzusichern, wird daher empfohlen, dass Passwörter mindestens 16 Zeichen lang sind und eine zufällige Kombination aus Buchstaben, Zahlen und Symbolen enthalten. Menschen versuchen jedoch oft, sich klassische Passwörter zu merken. Eine aktuelle Studie von Keeper bei Unternehmen bestätigt, dass mindestens 25 Prozent der genutzten Passwörter schwach sind und bei 35 Prozent der Befragten für mehrere Konten gleichzeitig verwendet werden.

Der neue Passphrase-Generator von Keeper ist in den bestehenden Passwort-Generator integriert und ermöglicht es Anwendern und Administratoren zu wählen, welcher der Generatoren für die Organisation bevorzugt oder erzwungen werden soll. Der Generator von Keeper nutzt die von der Electronic Frontier Foundation empfohlene Wortliste mit 7.776 Wörtern (bereinigt, um alle anstößigen Wörter zu entfernen). Anwender können kryptografisch sichere Passphrasen generieren, die auf ihre spezifischen Anforderungen zugeschnitten sind, z. B. wie viele Wörter sie enthalten, welche Art von Trennzeichen verwendet wird und ob sie Zahlen und Großbuchstaben enthalten. Das Verfahren zur Erstellung und Speicherung von Passphrasen mit Keeper ist dasselbe wie bei Passwörtern und Passkeys und es bietet eine nahtlose Anwendererfahrung.

Zu den wichtigsten Vorteilen des Passphrasen-Generators gehören:

- **Erhöhte Sicherheit -** Erzeugt starke und einzigartige Passphrasen, die gegen Brute-Force-Angriffe und passwortbezogene Cyber-Bedrohungen resistent sind.
- **Anpassungsoptionen -** Die Passphrasen können an die jeweiligen Sicherheitsanforderungen angepasst werden, einschließlich Länge, Zeichentypen und Komplexität.
- **Vereinfachte Herangehensweise -** Eine intuitive Benutzeroberfläche ermöglicht es Nutzern, die Passphrasen für ihre Konten einfach und nahtlos zu erstellen.

Mit der Integration des Passphrase-Generators gibt Keeper seinen Nutzern die benötigten Tools an die Hand, um böswilligen Akteuren und sich entwickelnden Cyber-Bedrohungen einen Schritt voraus zu sein.

Mehr über die Integration des Passphrase-Generators von Keeper und die Vorteile, die er sowohl für Einzelpersonen als auch für Unternehmen bietet, finden Sie hier.

###

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 TikTok

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