4. Mai 2023: Welt-Passwort-Tag
Die beste Gelegenheit, die Sicherheit von Passwörtern im Unternehmen auf den Prüfstand zu stellen

Wenn Unternehmen erkennen, wie wichtig sichere Passwörter zum Schutz vor Datenverletzungen sind, konzentrieren sie sich meist auf die offensichtlichsten Schwachstellen, wie die E-Mail-Konten der Mitarbeiter und die Passwörter für Netzwerke. Doch auch andere Passwörter, beispielsweise für soziale Medien, stellen erhebliche Sicherheitsrisiken dar, auf die Unternehmen manchmal nur unzureichend vorbereitet sind.

Passwortsicherheit für Social-Media-Konten im Unternehmen
Es sollte selbstverständlich sein, dass alle Social-Media-Konten mit starken und eindeutigen Passwörtern geschützt sind, die zudem sicher gespeichert und wenn nötig sicher weitergegeben werden - was auf keinen Fall per E-Mail, SMS oder über andere unsichere Kommunikationskanäle erfolgen sollte. Ein Passwortmanager erleichtert die Sicherung von Social-Media-Zugangsinformationen, indem er automatisch starke Passwörter generiert, diese in einem verschlüsselten Tresor speichert und es den Mitarbeitern ermöglicht, ihre Anmeldeinformationen sicher zu teilen.

Ein weiterer Vorteil von Passwortmanagern ist, dass sie die Möglichkeit bieten, Codes für die doppelte Authentifizierung (2FA) zu speichern. Das heißt, wenn Mitarbeiter Datensätze für Konten mit aktivierter Multi-Faktor-Funktion freigeben, müssen sie ihre Kollegen nicht bitten, ihnen den 2FA-Code über einen ungesicherten Kanal zu senden. Die Mitarbeiter können über ihren gemeinsam genutzten Ordner auf die 2FA-Codes zugreifen, wodurch das Risiko einer Kompromittierung des Kontos deutlich reduziert ist. Die Kontrolle des Zugriffs auf die Konten von Mitarbeitern und Auftragnehmern durch rollenbasierte Zugriffskontrolle (RBAC) in Verbindung mit dem Prinzip der geringsten Privilegien beschränkt den Zugriff auf die Social-Media-Konten des Unternehmens zudem auf genau die Mitarbeiter, die ihn tatsächlich benötigen.

Viele Unternehmen sichern ihre Passwörter nicht angemessen
Das Fehlen einer zentralen und sicheren Verwaltung von Passwörtern macht Unternehmen anfällig für Cyberbedrohungen – nicht nur intern, sondern auch in der Zusammenarbeit mit Geschäftspartnern. Am Beispiel von Social-Media-Agenturen ist das Risiko leicht erklärt, wobei das Prinzip auf viele weitere Szenarien im Unternehmen oder in der Zusammenarbeit mit Partnerunternehmen übertragbar ist. Hier beginnen die Schwachstellen bereits bei der Integration der Kunden.

- In der Regel teilen die Kunden ihre Social-Media-Passwörter oft auf unsichere Weise mit ihrer Agentur, etwa über E-Mails oder unverschlüsselte Nachrichten, die abgefangen werden können.
- Diese Passwörter werden häufig in einer Tabellenkalkulation oder Textdatei gespeichert, wodurch eine weitere Schwachstelle entsteht. Wenn dieses Dokument kompromittiert wird, sind alle darin aufgeführten Konten kompromittiert.
- Zudem wird oft dasselbe Passwort für alle Social-Media-Konten verwendet, wodurch ein Cyberkrimineller, der an das Passwort gelangt, auch auf alle anderen Konten zugreifen kann.
- Leider sind Passwörter oft schwach oder bereits durch eine Datenverletzung kompromittiert, wodurch die Konten anfällig für Angriffe durch "Credential-stuffing" und "Password spraying" werden.

Der weltweite Passwort-Tag ist also eine gute Gelegenheit, dass sich die Verantwortlichen in Unternehmen Gedanken darüber machen, wofür Passwörter im Business eingesetzt werden,

wer diese benutzt, mit wem sie geteilt werden und wie es um die Sicherheit dieser Passwörter bestellt ist. Denn die einzige zuverlässige Methode zur Passwortsicherheit in allen Bereichen eines Unternehmens ist ein professioneller Passwortmanager.

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.
Folgen Sie Keeper Security auf Facebook, Instagram, ,Linkedin, TikTok, and Twitter

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