Europäischer Datenschutztag: Wie wäre es mit einem Passwort-Manager?

Am 28. Januar ist Europäischer Datenschutztag – eine Erinnerung daran, sich über die eigene Passwortsicherheit Gedanken zu machen und die nötigen Schritte für einen besseren Schutz einzuleiten.

Alle Jahre kommt er wieder und zurecht: der Europäische Datenschutztag. Er ist eine Initiative des Europarats und wurde bereits 2007 am Tag der Unterzeichnung der Europäischen Datenschutzkonvention ins Leben gerufen. 15 Jahre später ist der 28. Januar aktueller denn je. Denn Passwörter gibt es in der hoch digitalisierten Welt für jedes und alles. Und viele gehen trotz der wachsenden Cyber- und Datenschutzgefahren immer noch lax mit ihren Passwörtern um – sowohl im privaten als auch im geschäftlichen Umfeld. Laut einer aktuellen Studie von Keeper Security überlassen es 31 Prozent der deutschen Unternehmen ihren Mitarbeitern, die Passwörter selbst zu wählen und nur 51 Prozent geben zumindest eine Anleitung für gute Passwörter– eine Praxis, die es Cyberkriminellen sehr leicht macht, ihren Weg ins Unternehmen zu finden. Lediglich 13 Prozent setzen auf ein ausgereiftes Passwortkonzept. Ergo ist der 28. Januar der richtige Tag, um sich mit der praktizierten Passwortsicherheit kritisch auseinanderzusetzen. Die gute Nachricht: Ein Passwortmanager kann Privatpersonen und Unternehmen helfen, das Malheur mit den Passwörtern elegant zu lösen.

Grundsätzlich gilt: Risiken minimieren und Daten schützen
An erster Stelle sei der Grundsatz genannt, dass man mit persönlichen Daten und mit Passwörtern so vorsichtig und restriktiv wie möglich im Internet umgehen sollte. Unbekannte und dubiose Links in E-Mails oder Online-Nachrichten, die nach persönlichen Daten fragen, sind tabu. Gleiches gilt für unbekannte Anhänge. Mindestens ebenso wichtig sind gute Passwörter und deren Sicherheit. Sie müssen eindeutig sein, komplex aus mindestens zwölf Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen in einer beliebigen Anordnung. Erst dann gilt ein Passwort als sicher und Cyberkriminelle haben keine realistische Chance, das Passwort ihres Opfers zu erraten. Ein guter Grund für einen Passwort-Manager ist es, dass er Anwendern und Unternehmen hilft, die Vielzahl der Passwörter zu erstellen, zu managen und zu speichern – verschlüsselt und sicher vor unberechtigtem Zugriff.

Passwort-Manager: bequem und sicher
Der Schutz von Zugangsdaten beginnt mit deren Sicherung. Soziale Netzwerke, Bankanwendungen, Netzwerkgeräte oder Zugänge ins Unternehmen müssen effizient vor unberechtigtem Zugang geschützt sein. Passwort-Manager wie die Lösungen von Keeper Security sind für diese Anforderung eine zuverlässige Lösung. Der Anwender kann von jedem seiner Geräte aus auf den Passwort-Manager zugreifen, um seine Passwörter zu erstellen und sicher zu nutzen. Anerkannte Verschlüsselungstechnologien und die Zero-Knowledge-Architektur sorgen dafür, dass niemand außer dem Nutzer Zugriff auf die Inhalte des Passwort-Tresors bekommt. Bei den Passwort-Manager-Lösungen für Unternehmen sind die Tresore der einzelnen Mitarbeiter separiert und in SaaS- oder Cloud-Umgebungen mit zusätzlichen Schutzmechanismen ausgestattet.

Was Unternehmen bei der Wahl eines Passwort-Managers hilft
Um die Wahl eines Passwort-Managers für Unternehmen zu erleichtern, gibt es fünf Aspekte, auf die Sicherheitsverantwortliche und IT-Administratoren achten sollten. Immerhin geht es darum, das Unternehmen vor Eindringlingen zu schützen und die Passwortsicherheit auch in einem Worst-Case-Szenario aufrecht zu erhalten.

1. Zero-Knowledge-Security: Das bedeutet, dass jeder Nutzer die vollständige Kontrolle über die Ver- und Entschlüsselung aller in seinem Tresor gespeicherten persönlichen Daten hat und dass keine seiner gespeicherten Daten für andere Personen zugänglich sind, nicht einmal für die eigenen IT-Administratoren und schon gar nicht für den Lösungsanbieter.

2. Verschlüsselung aller Daten im Tresor: Wichtig ist ein mehrschichtiges Verschlüsselungssystem, das auf vom Client erzeugten Schlüsseln basiert. 256-Bit-AES-Schlüssel auf Datensatzebene und Schlüssel auf Ordnerebene werden auf dem Client-Gerät generiert, die jeden gespeicherten Datensatz verschlüsseln. Damit sind alle Inhalte des Tresors verschlüsselt, einschließlich Logins, Dateianhänge, TOTP-Codes, Zahlungsinformationen, URLs und benutzerdefinierte Felder.

3. Effektiver Schutz des Datenschlüssels: Der Datenschlüssel ist eines der wichtigsten Elemente in einem Passwort-Tresor. Denn um den Tresor eines Benutzers zu entschlüsseln, muss der Datenschlüssel entschlüsselt werden. Für Benutzer, die sich mit einem Master-Kennwort anmelden, sollte der Schlüssel zum Ent- und Verschlüsseln des Datenschlüssels aus dem Master-Kennwort des Benutzers mithilfe der kennwortbasierten Schlüsselableitungsfunktion (PBKDF2) abgeleitet werden, wobei bis zu 1.000.000 Iterationen durchlaufen werden. Für Benutzer, die sich mit SSO oder passwortloser Technologie anmelden sollte zur Ver- und Entschlüsselung der Daten auf Geräteebene die Elliptic Curve Kryptographie verwendet werden. Ein lokaler privater ECC-256 (secp256r1)-Schlüssel wird zur Entschlüsselung des Datenschlüssels verwendet.

4. Sicherheit bei SaaS-Passwort-Managern: Passwort-Manager als SaaS-Plattform, sollten die Daten bei vertrauenswürdigen und im Idealfall vom Kunden wählbaren Hosting-Dienstleistern speichern. Dabei müssen die Daten und der Zugriff auf die Plattform auf die vom Kunden gewählte Region beschränkt sein. Alle verschlüsselten Daten sollten zusätzlich zur Transport Layer Security (TLS) mit einem 256-Bit-AES-Übertragungsschlüssel verschlüsselt sein, um vor Man-in-the-Middle-Angriffen zu schützen. Der Übertragungsschlüssel wird auf dem Client-Gerät generiert und mittels ECIES-Verschlüsselung über den öffentlichen EC-Schlüssel des Servers an den Server übertragen.

5. Zertifizierungen und Compliance: Passwort-Manager für Unternehmen (idealerweise auch für Privatpersonen) sollten von offizieller Stelle geprüft und zertifiziert sein. Dazu gehören internationale ebenso wie europäische Normen wie beispielsweise SOC 2- und ISO 27001 sowie die Konformität zu DSGVO, CCPA, FedRAMP, StateRAMP oder TrustArc und PCI DSS.

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@eskenzipr.com