Fonte: swz.it
Data: 29/11/2024
Categoria: Raiffeisen-Geldorganisation Print & Web | Link

Zukunft der sicheren Anmeldung: Von Passwörtern bis zu Passkeys

: 29/11/2024

Bozen – Solange Wertsachen greifbar sind, werden automatisch verschiedene Schutzmaßnahmen in Betracht gezogen: beispielsweise Tresore, Sicherheitstüren, Alarmanlagen oder Bankschließfächer. Liegen diese Werte aber nur in digitaler Form vor, dann ist die Maßnahmenliste meist ziemlich kurz: Zum Schutz wird ein einfaches Passwort gesetzt, möglichst jenes, welches man ohnehin schon für verschiedene andere Systeme verwendet. Wir haben in der digitalen Welt noch kein angemessenes Empfinden für die tatsächlichen Werte und für deren Sicherheit entwickelt.

Mag der Schutz mittels eines simplen Passworts in den Anfangszeiten der Digitalisierung noch ausreichend gewesen sein, so wissen wir heute, dass dies vollkommen unzureichend ist. Die Passwörter werden erraten, erschlichen, durch raffinierte Methoden massenhaft ausprobiert, oder sie können einfach aus den Datenbanken der Plattformbetreiber gestohlen werden. In regelmäßigen Abständen gibt es Schlagzeilen über Passwort-Klau in Millionenhöhe.

Mit den erbeuteten Passwörtern nutzt ein ganzes Heer von Betrügerinnen und Betrügern im Internet unsere Daten, um erheblichen Schaden anzurichten, etwa durch Einkäufe auf unsere Kosten, das Ausspionieren geschäftlicher Informationen oder das Kapern ganzer IT-Systeme mit anschließender Lösegeldforderung.

Zwei Faktoren für eine bessere Sicherheit

Die Sicherheit des Anmeldevorgangs lässt sich durch die Multifaktor-Authentisierung (MFA) verbessern. Dabei ist bei der Anmeldung neben der Eingabe des Passworts auch der Nachweis des Besitzes eines persönlichen Gegenstands erforderlich, etwa des eigenen Smartphones mit einer spezifischen App oder eines sogenannten Hardware-Tokens.

> Für die Sicherheit der Passwörter ist heute die Länge ausschlaggebend; die Komplexität und die regelmäßige Erneuerung haben sicherheitstechnisch an Bedeutung verloren.

Dieses Prinzip ist bereits aus dem Online-Banking bekannt, wo neben dem Passwort auch die App auf dem Smartphone zur Authentifizierung verwendet wird. Ein Betrüger, der zwar das Passwort kennt, aber keinen Zugriff auf das Smartphone hat, stößt hier auf erhebliche Hürden. Zahlungsdienstleister sind schon seit Jahren gesetzlich verpflichtet, den Anmeldevorgang durch MFA abzusichern. Mit dem neuen NIS2-Gesetz wird diese Verpflichtung nun jedoch auf viele weitere Unternehmen ausgeweitet.

In Unternehmen ist es besonders wichtig, die privilegierten Konten und die Fernwartung durch MFA abzusichern. Dadurch wird sichergestellt, dass nur eindeutig identifizierte Personen die Konfiguration der Systeme durchführen können. In der Vergangenheit wurde in vielen Fällen eine nicht ausreichend geschützte Fernwartung als Einfallstor für verheerende Angriffe verwendet.

Passwortflut: Abhilfe mit Passwort-Manager

Für jedes System ein eigenes Passwort, schön kompliziert, nicht aufschreiben, regelmäßig ändern und merken: So lautete die goldene Regel für die Wahl der Passwörter. Die zunehmende Anzahl an Systemen macht die Verwaltung sicherer Passwörter ohne Hilfsmittel kaum noch möglich. Passwort-Manager schaffen hier Abhilfe, indem sie alle Passwörter in einem sicheren digitalen Tresor speichern und bei Bedarf automatisch ausfüllen.

Diese Passwort-Manager erlauben die Erstellung komplexer, zufälliger Passwörter für neue Konten und erleichtern die regelmäßige Erneuerung sowie die Überprüfung der Nutzung. Auch die regelmäßige Erneuerung der Passwörter oder die periodische Kontrolle, ob die Passwörter überhaupt noch verwendet werden, wird dadurch erleichtert und sogar automatisiert.

> Viele Passwort-Manager werden als Cloudlösungen betrieben, um dadurch einen flexiblen Zugriff auf die Passwörter von jedem Gerät und von jedem Ort aus zu gewährleisten.

In Unternehmen besteht oft die Notwendigkeit, dass ein Zugang mit Passwort einer ganzen Gruppe von Personen bereitgestellt werden muss. Auch hier leisten Passwortmanager wertvolle Hilfe, ohne die Sicherheit der Passwörter aufs Spiel zu setzen.

Besonders wichtig ist der sichere Umgang mit dem Masterschlüssel, da dieser den Zugang zum Tresor ermöglicht. Ein Verlust oder Diebstahl des Masterschlüssels kann zu irreversiblen Konsequenzen führen. Der Schlüssel muss daher sowohl sicher verwahrt als auch jederzeit verfügbar sein.

Viele Passwort-Manager werden als Cloudlösungen betrieben, um dadurch einen flexiblen Zugriff auf die Passwörter von jedem Gerät und von jedem Ort aus zu gewährleisten. Somit befindet sich der Passwort-Tresor in der Cloud. Obwohl gerade Passwort-Manager mit höchster Sicherheit ausgestattet sind, muss

auch erwähnt werden, dass es bereits Einbrüche in Cloud-Passwort-Tresore gegeben hat und dadurch z. B. Bitcoin-Guthaben gestohlen worden sind.

Die Zukunft ohne Passwort

Nachdem das Anmelden mit dem Passwort mit so vielen Unsicherheitsfaktoren behaftet ist, wurden Anmeldeverfahren ganz ohne Passwort entwickelt. Beim FIDO2-Verfahren erfolgt die Identifizierung des Benutzers mittels kryptografischer Methoden über einen physischen Sicherheitsschlüssel (Token).

Passwort gibt es hier keines mehr und ein Angreifer muss in den physischen Besitz dieses Tokens kommen. Die Sicherheit liegt in den kryptografischen Schlüsseln, welche fix an die Hardware gebunden sind.

Das FIDO2-Verfahren gilt aktuell als das sicherste Anmeldeverfahren. Obwohl es dieses Verfahren schon seit einiger Zeit gibt, hat es sich im Internet bisher nicht richtig durchgesetzt. Dies liegt einerseits daran, dass viele Plattformen diese Anmeldemethode nicht unterstützen, und andererseits daran, dass der Einsatz eines zusätzlichen Tokens kostenintensiv und unpraktisch ist, da dieser stets mitgeführt werden muss.

Bequem und sicher: Passkeys

Ausgehend vom FIDO2-Verfahren wurde von den globalen Playern (Microsoft, Google, Apple) ein sicherheitstechnisch etwas abgeschwächtes, dafür aber recht bequemes Verfahren entwickelt: die Passkeys, welche in Zukunft das Passwort ersetzen sollen. Hier sind die kryptografischen Schlüssel nicht mehr fix an den Token gebunden, sondern sie können über sichere Kanäle in andere Hardware übertragen werden; dies geht optional bis hin zur Synchronisierung in die Cloud.

Als Sicherheitstoken ist keine separate Hardware mehr notwendig, sondern es wird das Smartphone oder der PC selbst mit dem eingebauten Sicherheitschip (TPM Trusted-Platform-Modul) verwendet. Die Anmeldung erfolgt nun über die Passkeys, die sich auf den Geräten befinden, welche man ohnehin

verwendet. So kann man sich etwa auf einem fremden PC auf einer Plattform anmelden, indem man einfach den Passkey des eigenen Smartphones verwendet; Passwort wird am fremden PC keines mehr eingegeben.

In der Umgebung von Microsoft365 wurde dieses Verfahren der passwortlosen Anmeldung so weit entwickelt, dass das Passwort aus dem Konto von Active Directory oder Entra-ID einfach gelöscht werden kann. Und wenn es kein Passwort mehr gibt, kann auch keines mehr gestohlen werden.

Wie es weitergeht

Die Tendenz ist vorgezeichnet und sie geht in Richtung von sicheren Passkeys, aber Passwörter werden uns noch eine Weile begleiten. Deshalb ist es nach wie vor wichtig, die Benutzer:innen für eine sichere Verwendung von Passwörtern zu sensibilisieren und vor allem vor Phishing zu warnen. Für die Sicherheit der Passwörter ist heutzutage vor allem die Länge ausschlaggebend; die Komplexität und die regelmäßige Erneuerung haben sicherheitstechnisch an Bedeutung verloren.

Und da kurzfristig die Anzahl der Passwörter eher im Steigen begriffen ist, leisten auch Passwort-Manager nach wie vor ihre guten Dienste.

 **Martin Galler**

DER AUTOR *ist Experte für Information Security & Privacy SOC beim IT-Unternehmen Konverto.*

Schlagwörter: 46-24freeTop4

Ausgabe 46-24**, Seite 17**