Passwörter

Passwörter sind ein zentraler Bestandteil der Computersicherheit. Sie werden unter anderem verwendet, um lokale Geräte zu sichern, Netzwerke im privaten oder betrieblichen Umfeld zu schützen oder um sich in Onlinedienste einzuloggen. Auch um den Zugriff auf Daten oder die unbefugte Weitergabe von Daten zu schützen, kommen Passwörter zum Einsatz. Sichere Passwörter haben deshalb eine enorme Bedeutung in der heutigen vernetzten Welt.

Die Kritikalität von Passwörtern wird oftmals (immer noch) unterschätzt. Zu einfache oder mehrmals verwendete Passwörter sind anfällig gegen Brute-Force-Attacken und Phishing-Angriffe. Zusätzliche Sicherheit wie z. B. Multi-Faktor-Authentisierung (MFA) ist immer noch nicht weit genug verbreitet und leidet vielerorts an der Akzeptanz der Anwender. Mit Passkeys steht eine neue Authentifizierungsmethode in den Startlöchern, die das Potenzial hat, die Verwendung von Passwörtern abzulösen oder zumindest deutlich zu reduzieren.

Was gilt heute als sicheres Passwort?

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat Rahmenbedingungen für ein sicheres Passwort auf einer Internetseite zusammengestellt.[1]

Es gibt zwei Strategien, nach denen Passwörter erstellt werden können:

- Weniger komplexe Passwörter mit mindestens 25 Zeichen. Diese Passwörter kommen mit zwei Zeichenarten aus (z. B. Groß- und Kleinbuchstaben).
- Komplexe Passwörter können mit 8-12 Zeichen auskommen, wenn vier Zeichenarten kombiniert werden (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).

Komplexe Passwörter kommen auch mit 8 Zeichen aus, wenn eine Multi-Faktor-Authentisierung verwendet wird.

Für jeden Zugang sollte ein eigenes Passwort verwendet werden. Diese können in einem Passwortmanager verwaltet werden. Passwortmanager bringen oft auch einen Passwortgenerator mit, mit dem nach bestimmten Kriterien Passwörter generiert werden können. Grundsätzlich können alle Zeichen bei der Verwendung von Passwörtern mit einbezogen werden. Besondere Zeichen aus unserer Sprache wie z. B. ü, ö, ä, ß sollten nicht verwendet werden, da nicht immer gewährleistet ist, dass alle Systeme oder Dienste diese Zeichen auch interpretieren können.

Das BSI ist vor einiger Zeit von der Empfehlung, Passwörter regelmäßig zu wechseln, auf die Empfehlung zu längeren und komplexeren Passwörtern ohne regelmäßige Wechsel übergegangen. Regelmäßige Passwortwechsel verringern über die Zeit die Sicherheit, da Anwender beim erzwungenen Passwortwechsel oft nur Abwandlungen oder Vereinfachungen des vorherigen Passwortes verwenden. Passwörter sollten nur noch gewechselt werden, wenn der Verdacht besteht, dass jemand Unbefugtes Kenntnis über das Passwort haben könnte.

Eine zusätzliche Multi-Faktor-Authentisierung (MFA) ist ergänzend zum Passwort empfehlenswert. Zusätzlich zum Passwort wird z. B. durch Gesichtserkennung, Fingerabdruck, Bestätigung in einer App oder Eingabe einer generierten PIN auf einem weiteren Gerät die Anmeldung mit Benutzername und Passwort vervollständigt. MFA kann auf einem Smartphone mit einer entsprechenden App oder auch als separates Gerät ausgeführt werden.

Das BSI hat das Thema Passwortsicherheit im IT-Grundschutz integriert. Im Baustein *ORP.4 Identitäts- und Berechtigungsmanagement*[2] wird auf die Grundschutz-Anforderungen zu Passwörtern eingegangen.

Ein Ausblick – Passkeys
Ein Passkey ist ein kryptografisches Verfahren bestehend aus einem privaten und öffentlichen Schlüssel und wurde von der FIDO-Allianz (nichtkommerzielle IT-Sicherheitsorganisation) entwickelt. Passkeys werden ähnlich wie Multi-Faktor-Authentisierung an einem Ort, z. B. einem Smartphone, gespeichert. Der enorme Vorteil ist, dass sich keine Passwörter ausgedacht, gemerkt oder diese verwaltet werden müssen. Es gibt auch keine zu kurzen oder nicht komplex genug gewählte Passkeys, da diese auf kryptografischen Berechnungen basieren. Bei Anbietern, die schon Passkeys

einsetzen, wird der Anwender beim Log-in gefragt, ob sich mit Benutzername und Passwort oder mit Passkeys angemeldet werden soll. Bei der Wahl von Passkeys wird der Passkey auf z. B. einem Smartphone freigegeben und der Dienstanbieter und das Smartphone tauschen im Hintergrund die benötigten Daten und Berechnungen aus und der Nutzer wird angemeldet. Große Online-Shoppinganbieter, Foren, Finanzportale oder auch Messengerdienste unterstützen bereits Passkeys. Auch zu diesem Thema hat das BSI Informationen veröffentlicht.[3]

Empfehlung des KDSZ
Das Katholische Datenschutzzentrum empfiehlt, die Anforderungen des BSI bei der Wahl der Passwörter oder dem Einsatz einer Passwortrichtlinie zu übernehmen. Wenn möglich sollte die Multi-Faktor-Authentisierung verwendet werden. Sind Passkeys in Zukunft weiter verbreitet, empfiehlt es sich, die Verwendung für genutzte Dienste zu prüfen.

[1] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_

[3] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html