Zwei-Faktor-Authentifizierung (2FA)

Plattformen, auf denen sensible Daten gespeichert sind, sollten neben einem sicheren Passwort mit einem weiteren Faktor geschützt werden, der die Identität der zugreifenden Personen verifiziert. In der Regel kombiniert man bei Zwei- oder Mehrfaktor-Authentifizierungen Faktoren aus verschiedenen Kategorien, z.B.

- Wissen (Passwort, PIN)
- Besitz (Zertifikat, Mobiltelefon per SMS, Chipkarte)
- Biometrie (Fingerabdruck)

Die am GGD eingesetzten Verfahren zur Zwei-Faktor-Authentifizierung kombinieren in der Regel ein sicheres Passwort (Wissen) mit einem kryptografischen Schlüssel (Besitz). Der Besitz des Schlüssels wird dabei über ein zeitabhängiges Einmalpasswort nachgewiesen. Der Schlüssel selsbt wird nie eingegeben und kann damit auch nicht auspioniert werden. Das Verwalten der Schlüssel übernimmt eine Authentifizierungs-App wieder FreeOTP Authenticator oder ein Passwort-Manager wie der Bitwarden Passwortmanager.

Weitere Informationen zur Zwei-Faktor-Authentifizierung gibt es z.B. beim Bundesamt für die Sicherheit in der Informationstechnik:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung.html

> **Tipp**
> Häufig wird empfohlen, Passworteingabe und Schlüsselverwaltung auf zwei separaten Geräten vorzunehmen. Da das Dienst-iPad aber durch eine weiteren Faktor (PIN bzw. Fingeabdruck) geschützt ist, erscheint mir das Risiko vertrebar, den Schlüssel auf dem gleichen Gerät zu speichern. — *Jan Köster 13.05.2024 19:07*