Two-Factor-Authentication (2FA)

von Marc-Niclas Harm, Kryptologie, TH-Lübeck

Was ist 2FA ❓

Die **Two-Factor-Authentication** (**2FA**) ist eine Unterform der **Multi-Factor-Authentication** (**MFA**). Der Hauptzweck der **MFA** liegt darin, einen Benutzer zu **identifizieren** und/oder zu **authentisieren**. Dabei müssen **mindestens zwei verschiedene** der folgenden Faktoren benutzt werden:

Faktor	Beispiel
Wissen 🔑	Passphrase wie *Passwort*, *PIN*
Besitz 💳	Security-Token wie *USB-Token*, *Chip-Karte*
Inhärenz 👀	biometrische Charakteristika wie *Fingerabdruck*, *Unterschrift*

Bei **2FA** sind es genau **zwei verschiedene** Faktoren, welche gegeben sein müssen. Diese **zwei** Faktoren sind überwiegend **Wissen** in Form eines Passworts und **Besitz** in Form eines **Software-Tokens**.

Wieso ist 2FA heutzutage wichtig/notwendig ❓

Immer häufiger liest man im Internet oder in der Zeitung, dass beim Unternehmen *XYZ* tausende persönliche Daten **gestohlen** wurden. Egal ob verursacht durch immer anspruchsvoller werdende **Kriminelle** oder durch ein **einfaches Datenleck**, am Ende ist es auch der Nutzer, der leidet.

Falls nun der unwahrscheinliche Fall eintritt, dass diejenigen, die die Daten in die Hände bekommen haben, es schaffen die **Passwörter** der Nutzer zu "entschlüsseln" (liegen meistens in *Hash-Form* vor), dann haben all jene Nutzer dieser Menge ein Problem, welche dieses **Passwort** noch bei anderen **Diensten** nutzen und dort keine **2FA** aktiviert haben. Der **Zugriff** auf diese **Accounts** ist nun ein Leichtes.

Man kommt somit zu dem Schluss, dass **Passwörter** alleine heutzutage **nicht mehr** zum Schutz beim **Login** von Diensten **ausreichen** und ein **zusätzlicher Schutz** wie die **2FA** nötig sind.

Zwei gängige Verfahren der 2FA: HOTP und TOTP

HOTP (RFC 4226 aus dem Jahr 2005)