MFA (Multi-Faktor-Authentifizierung)

Inhaltsverzeichnis

MFA verlangt zur Anmeldung mindestens zwei unabhängige Faktoren – etwa Wissen, Besitz oder Biometrie. Dadurch bleiben Konten auch bei gestohlenen Passwörtern deutlich besser geschützt.

1 Funktionsweise

Nach dem Passwort (oder statt dessen) wird ein zweiter Nachweis verlangt: App-Code, Hardware-Token, Push-Freigabe, Passkey oder Biometrie. Erst die Kombination gilt als erfolgreiche Anmeldung.

- **Wissen:** Passwort oder PIN
- **Besitz:** Smartphone, Security-Key, OTP-Token
- **Inhärenz:** Fingerabdruck, Face-ID u. Ä.

2 Typische Einsatzbereiche

- E-Mail, VPN, Admin-Zugänge und Cloud-Konsolen
- Single Sign-On und Unternehmensportale
- Absicherung privilegierter Konten

3 Wichtige Hinweise

- SMS-OTP ist besser als nichts, aber anfälliger als App- oder Hardware-Faktoren.
- Passkeys/FIDO2 gelten derzeit als besonders phishing-resistent.
- Recovery-Codes und Geräteverlust-Prozesse müssen mitgeplant werden.

4 Fazit

MFA ist eine der wirksamsten Schutzmaßnahmen gegen Account-Übernahmen – besonders für administrative und geschäftskritische Zugänge sollte sie Standard sein.