Mittelstand-Digital Zentrum Leipzig-Halle

Passwortsicherheit

Inhalt: Aufbau und Bedeutung sicherer Passwörter, Konzept der Mehr-Faktor-Authentifizierung

Warum sichere Passwörter?

- um Cyberangriffe und damit verbundenes Eindringen in Systeme, Datendiebstahl etc. zu vermeiden
- **Tipp**: Nutzen Sie Passwort-Manager und -Tools, um bequem sichere Passwörter erstellen zu lassen und zu verwalten

Leitfaden zur Erstellung eines sicheren Passwortes

Variante 1: lang & wenig komplex

- 20-25 Zeichen
- mind. 2 verschiedene Zeichenarten (z.B. Abfolge von Wörtern)
- Bsp.: BlockchainNeuesSofaGrün

Variante 2: kürzer & komplex

- 8-12 Zeichen
- 4 verschiedene Zeichenarten
- Bsp.: cYb€raTT4ckE

Variante 3: kurz & komplex, mit MFA

- 8 Zeichen
- 3 verschiedene Zeichenarten
- Bsp.: S0ftWar3
- Schutz durch Mehr-Faktor-Authentifizierung

Mehr-Faktor-Authentifizierung (MFA)

… kombiniert mehrere Identitätsprüfungen beim Anmeldeprozess, meist zwei (Zwei-Faktor-Authentifizierung oder 2FA)

1. Faktor: kann nur der Nutzer **wissen** (Passwort, PIN etc.)
2. möglicher Faktor: kann nur der Nutzer **haben** (Smartphone, Token etc.)
2. oder 3. möglicher Faktor: kann nur der Nutzer **sein** (Fingerabdruck, Gesichtserkennung etc.)

Exkurs: Brute-Force-Angriffe

… beschreiben eine Methode, mithilfe automatisierter Programme alle möglichen Kombinationen von Passwörtern auszuprobieren, um Zugang zu einem System zu erhalten

→ schwache/häufig verwendete Passwörter sind gefährdet, schnell ermittelt zu werden

→ mögliche Schutzmaßnahmen: starke Passwörter, Anmeldeüberwachung, MFA

Mittelstand-Digital

Web Based Training:

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages