



[Video ansehen](#)

Windows Kurs

Modul 1

Computer Grundlagen - Theorie Teil



[Online-Übung](#)

Übung 13 - Datensicherheit & Backup

1. Identität und Authentifizierung

Um unbefugten Zugriff zu verhindern, müssen Benutzer ihre Identität nachweisen.

Dies nennt man **Authentifizierung**.

Typische Methoden:

- Benutzername und Passwort
- PIN
- Fingerabdruck
- Gesichtserkennung

1.1 Eigenschaften eines sicheren Passworts

Ein sicheres Passwort sollte:

- Mindestens 8-12 Zeichen lang sein
- Groß- und Kleinbuchstaben enthalten
- Zahlen enthalten
- Sonderzeichen enthalten
- Nicht leicht zu erraten sein
- Nicht mehrfach verwendet werden

1.2 Zwei-Faktor-Authentifizierung (2FA)

Zusätzliche Sicherheit durch:

- Passwort + SMS-Code
- Passwort + App-Code
- Passwort + Fingerabdruck

Das erhöht die Sicherheit deutlich.

2. Authentifizierung vs. Autorisierung

Authentifizierung:

Wer bist du?

Autorisierung:

Was darfst du tun?

Beispiel:

Ein Mitarbeiter darf sich anmelden (Authentifizierung), aber nicht alle Daten bearbeiten (Autorisierung).

3. Datensicherheit

Datensicherheit bedeutet Schutz vor:

- Verlust
- Diebstahl
- Manipulation
- Zerstörung

Gefahren:

- Viren
- Ransomware
- Hardwaredefekte
- Menschliche Fehler

4. Backup (Datensicherung)

Backup bedeutet eine zusätzliche Sicherung wichtiger Daten.

Warum?

Daten können verloren gehen durch:

- Defekte Festplatten
- Viren
- Stromausfall
- Diebstahl

5. Arten von Backups

Vollbackup

Alle Daten werden gesichert.

Inkrementelles Backup

Nur neue oder geänderte Daten werden gesichert.

Differenzielles Backup

Alle Änderungen seit dem letzten Vollbackup werden gesichert.

6. Backup-Medien

- Externe Festplatte
- NAS
- Cloud
- USB-Stick (nur bedingt geeignet)

7. 3-2-1-Regel

- 3 Kopien
- 2 verschiedene Speichermedien
- 1 Kopie an einem anderen Ort

8. Verschlüsselung

Verschlüsselung schützt Daten vor unbefugtem Zugriff.

Beispiel:

- Festplattenverschlüsselung
- Verschlüsselte USB-Sticks

9. Schutz der Hardware

- Security Cable
- Abschließbare Räume
- Passwortschutz
- Automatische Bildschirmsperre

10. Cloud-Backup

Vorteile:

- Ortsunabhängig
- Automatisch

Nachteil:

- Internet erforderlich
- Datenschutz beachten

Zusammenfassung

- Starke Passwörter sind Pflicht.
- 2FA erhöht Sicherheit.
- Backups schützen vor Datenverlust.
- Verschlüsselung schützt vor Missbrauch.
- 3-2-1-Regel bietet hohe Sicherheit.