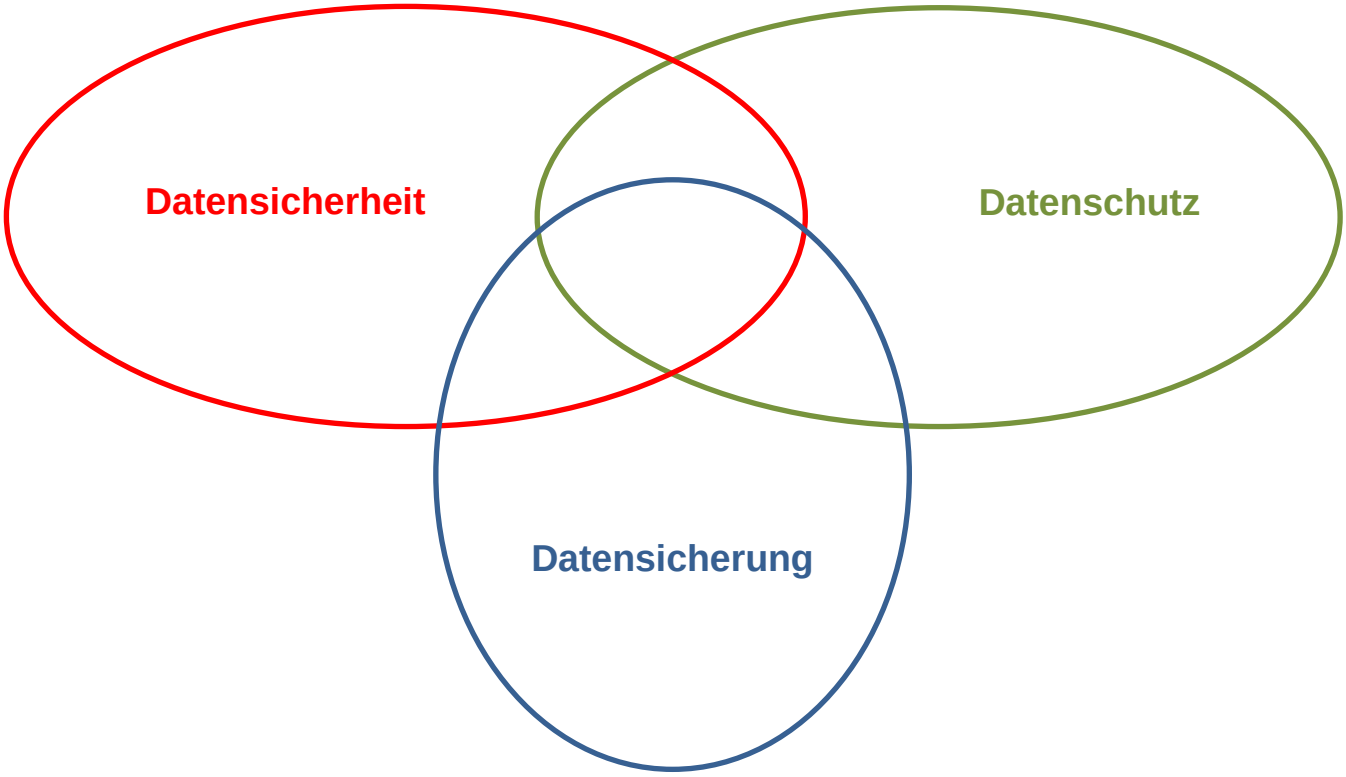
Typische Gefährdungen beim IT-Grundschutz



Technische Maßnahmen

Organisatorische Maßnahmen

Grundbedrohung der IT-Sicherheit
➔ Informationssicherheit

Verlust der Verfügbarkeit
- ➔ IT-Systeme müssen funktionieren
- ➔ Daten müssen verfügbar sein

Verlust der Vertraulichkeit
- ➔ Unbefugte haben keinen Informationszugriff
- ➔ Nur für einen beschränkten Empfängerkreis

Verlust der Integrität
- ➔ Daten sind vollständig
- ➔ Daten sind unverändert

- absichtlich
- unabsichtlich
- technische Fehler

Verlust der Authentizität
- ➔ Daten sind sicher einem Sender zuzuordnen
- ➔ Daten sind unabstreitbar

Typische Gefährdungen beim IT-Grundschutz können entstehen durch:

Elementare Gefährdungen

- Feuer
- Ungünstige klimatische Bedingungen
- Wasser
- Verschmutzung, Staub, Korrosion
- Naturkatastrophen
- Katastrophen im Umfeld
- Großereignisse im Umfeld
- Ausfall oder Störung der Stromversorgung
- Ausfall oder Störung von Kommunikationsnetzen
- Ausfall oder Störung von Versorgungsnetzen
- Ausfall oder Störung von Dienstleistern
- Elektromagnetische Störstrahlung
- Abfangen kompromittierender Strahlung
- Ausspähen von Informationen / Spionage
- Abhören
- Diebstahl von Geräten, Datenträgern oder Dokumenten
- Verlust von Geräten, Datenträgern oder Dokumenten
- Fehlplanung oder fehlende Anpassung
- Offenlegung schützenswerter Informationen
- Informationen oder Produkte aus unzuverlässiger Quelle
- Manipulation von Hard- oder Software
- Manipulation von Informationen
- Unbefugtes Eindringen in IT-Systeme
- Zerstörung von Geräten oder Datenträgern
- Ausfall von Geräten oder Systemen
- Fehlfunktion von Geräten oder Systemen
- Ressourcenmangel
- Software-Schwachstellen oder -Fehler
- Verstoß gegen Gesetze oder Regelungen
- Unberechtigte Nutzung oder Administration von Geräten und Systemen
- Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- Missbrauch von Berechtigungen
- Personalausfall
- Anschlag
- Nötigung, Erpressung oder Korruption
- Identitätsdiebstahl
- Abstreiten von Handlungen
- Missbrauch personenbezogener Daten
- Schadprogramme
- Verhinderung von Diensten (Denial of Service)
- Sabotage
- Social Engineering
- Einspielen von Nachrichten
- Unbefugtes Eindringen in Räumlichkeiten
- Datenverlust
- Integritätsverlust schützenswerter Informationen

1. **Höhere Gewalt**
    a. Personalausfall
    b. Ausfall von IT-Systemen
    c. Blitz
    d. Feuer
    e. Wasser
    f. Kabelbrand
    g. Unzulässige Temperatur und Luftfeuchte
    h. Staub, Verschmutzung
    i. Datenverlust durch starke Magnetfelder
    j. Ausfall eines Weitverkehrsnetzes
    k. Technische Katastrophen im Umfeld
    l. Beeinträchtigung durch Großveranstaltungen
    m. Sturm
    n. Datenverlust durch starkes Licht
    o. Ausfall von Patchfeldern durch Brand
    p. Ausfall oder Störung eines Funknetzes
    q. Ausfall eines Gebäudes
    r. Ausfall eines Dienstleisters oder Zulieferers

2. **Organisatorische Mängel**
    a. Fehlende oder unzureichende Regelungen
    b. Unzureichende Kenntnis über Regelungen
    c. Unzureichende Kontrolle der Sicherheitsmaßnahmen
    d. Unbefugter Zutritt zu schutzbedürftigen Räumen
    e. Unzureichende Trassendimensionierung
    f. Unzureichende Dokumentation der Verkabelung
    g. Ungesicherter Akten- und Datenträgertransport
    h. Ungeeignete Entsorgung der Datenträger und Dokumente

3. **Menschliche Fehlhandlungen**
    a. Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
    b. Fahrlässige Zerstörung von Gerät oder Daten
    c. Nichtbeachtung von Sicherheitsmaßnahmen
    d. Unzulässige Kabelverbindungen
    e. Unbeabsichtigte Leitungsbeschädigung
    f. Gefährdung durch Reinigungs- oder Fremdpersonal

4. **Vorsätzliche Handlungen**
    a. Manipulation oder Zerstörung von Geräten oder Zubehör
    b. Manipulation an Informationen oder Software
    c. Unbefugtes Eindringen in ein Gebäude
    d. Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz
    e. Manipulation durch Familienangehörige und Besucher
    f. Vertraulichkeitsverlust schützenswerter Informationen

5. **Technisches Versagen**
    a. Ausfall der Stromversorgung
    b. Ausfall interner Versorgungsnetze
    c. Ausfall vorhandener Sicherungseinrichtungen

6. **Vorsätzliche Handlungen**

a. Unbefugtes Eindringen in ein Gebäude
b. Diebstahl
c. Vandalismus
d. Anschlag
e. Gefährdung bei Wartungs-/Administrierungsarbeiten
f. Unberechtigter Zugang zu den aktiven Netzkomponenten
g. Sabotage

Datenschutz

➔ Schutz vor missbräuchlicher Datenverarbeitung
➔ Schutz des Rechts auf informationelle Selbstbestimmung
➔ Schutz des Persönlichkeitsrechts
➔ Schutz der Privatsphäre

Rechtsgrundlagen
- **BDSG**
- **LDSG**
- **Datenschutzbeauftragter**

Urheberrecht

Datensicherung
➔ Kopieren von Daten, um Datenverlust zu vermeiden (Backup)
➔ Datenwiederherstellung aus der Sicherungskopie (Restore)

Datensicherungshardware

Magnetische Speicher
- **Festplatten/RAID-Systeme**
- **Streamer**
- **...**

Optische Speicher
- **CD**
- **DVD**
- **Blu-Ray**

Flash-Speicher
- **Sticks**
- **SSD-Festplatten**
- **...**

Online-Speicherung (Cloud-Speicherung)

Datensicherungsstrategien

Zeitpunkt und Umfang muss geplant werden
- **Volldatensicherung**
- **inkrementelles Backup**
- **differentielles Backup**

Medienplanung
- **Großvater-Vater-Sohn-Prinzip**