Grundanforderungen an die IT-Sicherheit

IT-Sicherheit umfasst alle Prozesse, Strategien und das Know-how eines Unternehmens, um es vor Eingriffen durch Dritte zu schützen.

1) Funktionssicherheit des Systems (die „Werkzeuge“)

- Hardware
- Betriebssystem
- Software

2) Datensicherheit (unsere Daten sind das „Material“)

- Datensicherheit setzt zunächst die Funktionssicherheit des Systems voraus (Pkt. 1)
- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Authentizität

} Schutzziele (Security Goals) im engeren Sinne

Authentizität stellt in gewisser Weise eine Spezialvariante der Integrität als Sicherheitsziel dar. Es wird in mancher Literatur und nach Definition des BSI auch als Unterpunkt/Bestandteil der Integrität behandelt.

3) Datenschutz

- Schutz von personenbezogenen Daten vor Missbrauch
- Gesetzliche Vorschriften (z.B. DSGVO)
- Datenschutz nutzt zu Umsetzung die technisch-organisatorischen Maßnahmen der Datensicherheit

Schutzziele / Grundwerte

- Vertraulichkeit → Grundwert **C** = Confidendiality
- Verfügbarkeit → Grundwert **A** = Availability
- Integrität → Grundwert **I** = Integrity
- Authentizität → Grundwert **IA** = Authenticity
  (als spezifischer Unterpunkt der Integrität)

Inhalte und Beispiele für die Schutzziele

Vertraulichkeit => keine unautorisierten Zugriffe auf die Daten, Schutz vor Datendiebstahl …
- Zutrittskontrolle (z.B. Raum verschlossen, Alarm, Überwachungskamera)
- Zugangskontrolle (z.B. Zugang zu Windows mit Benutzername und Passwort)
- Zugriffskontrolle (z.B. Passwortschutz und Verschlüsselung der Datei oder Datenbank)

Verfügbarkeit => kein Verlust der Daten, jederzeit Zugriff von den berechtigten Personen möglich …
- Backup
- RAID
- USV
- Archivierung
- Redundanz allg.

Integrität => keine ungewollte Veränderung der Daten, Korrektheit …
- Prüfsummen, Hashwerte
- Schreibschutz
- Signatur

Authentizität => Urheber der Daten ist verifiziert, Echtheit der Daten …
- Zertifikat
- Signatur
- Benutzername und Passwort