**Lernzettel 1: Einführung in Sicherheit und Privatheit**

**1. Grundbegriffe der IT-Sicherheit**

* **IT-Sicherheit** bezieht sich auf den Schutz von IT-Systemen und den darin enthaltenen Informationen.
* **Wichtige Begriffe:**
  + **Funktionssicherheit (Safety):** Sicherstellung, dass ein System wie vorgesehen funktioniert.
  + **Informationssicherheit (Security):** Schutz vor unautorisierten Zugriffen und Manipulationen.
  + **Datensicherheit (Protection):** Vermeidung unautorisierter Zugriffe auf Daten.
  + **Privatheit und Datenschutz (Privacy):** Kontrolle über die Erhebung und Verarbeitung persönlicher Daten.

**Lernbrücke:** Verknüpfe Funktionssicherheit mit der Grundlage für Informations- und Datensicherheit. Ohne zuverlässige Funktionalität können andere Sicherheitsaspekte gefährdet sein.

**2. Schutzziele**

* **Authentizität:** Sicherstellung der Echtheit und Glaubwürdigkeit von Objekten und Subjekten.
* **Datenintegrität:** Schutz vor unbemerkten und unautorisierten Datenmanipulationen.
* **Vertraulichkeit:** Sicherstellung, dass keine unautorisierten Informationszugriffe erfolgen.
* **Verfügbarkeit:** Authentifizierte Subjekte sollen jederzeit Zugang zu den benötigten Ressourcen haben.
* **Verbindlichkeit:** Aktionen müssen nachweisbar einer Person zugeordnet werden können.

**Lernbrücke:** Die Schutzziele wirken oft zusammen, z.B. unterstützt Datenintegrität die Vertraulichkeit, da unbemerkte Manipulationen verhindert werden.

**3. Schwachstellen, Bedrohungen und Risiken**

* **Schwachstellen:** Schwächen eines Systems, die ausgenutzt werden können (z.B. fehlende Eingabeüberprüfungen).
* **Bedrohungen:** Potenzielle Ereignisse, die ein Schutzziel gefährden (z.B. Malware, Denial of Service).
* **Risiko:** Kombination aus Eintrittswahrscheinlichkeit und Schadensausmaß eines Bedrohungsszenarios.

**Lernbrücke:** Verknüpfe Schwachstellen mit Risiken, da eine Schwachstelle das Risiko für eine Bedrohung erhöht.

**4. Angreifer**

* **Typen von Angreifern:**
  + **Outsider:** Externe Angreifer mit oft begrenztem Zugang.
  + **Insider:** Personen mit berechtigtem Zugang, die das System von innen angreifen.
* **Profile von Angreifern:**
  + **White Hats:** Ethik und Schutzorientierung.
  + **Black Hats:** Böswillige Absichten.
  + **Gray Hats:** Zwischen White und Black Hats.

**Lernbrücke:** Die Rolle und das Profil eines Angreifers bestimmen oft die Strategie zur Bedrohungsabwehr.

**5. Sicherheitsmanagement**

* **Sicherheitsrichtlinien:** Festlegung von Regeln und Verfahren zum Schutz von Systemen und Daten.
* **Sicherheitsmaßnahmen:** Technische und organisatorische Mechanismen zur Umsetzung der Sicherheitsrichtlinien.

**Lernbrücke:** Sicherheitsmanagement integriert die zuvor genannten Aspekte (Schutzziele, Schwachstellen, Bedrohungen) zu einem ganzheitlichen Schutzkonzept.

**6. Mehrseitige Sicherheit**

* **Definition:** Berücksichtigung der Interessen aller Beteiligten in einem System, um Schutzkonflikte zu erkennen und zu lösen.
* **Vorgehen:** Formulieren der Sicherheitsinteressen, Erkennen von Konflikten, Aushandeln von Lösungen.

**Lernbrücke:** Mehrseitige Sicherheit verbindet alle Akteure eines Systems und stellt sicher, dass die Sicherheitsmaßnahmen für alle Parteien angemessen sind.