**Lernzettel 2: Identifikation und Authentifikation**

**1. Grundlagen der Authentifikation**

* **Identifikation:** Bestimmung einer Person durch Benutzerkennung oder Benutzernamen.
* **Authentifikation:** Prozess der Überprüfung, ob eine vorgegebene Identität echt ist.
  + **Authentisierung:** Der Mensch weist seine Identität nach.
  + **Authentifizierung:** Das IT-System überprüft die Identität.

**Lernbrücke:** Authentifikation ist ein Zusammenspiel von Mensch und IT-System. Beide müssen sich gegenseitig bestätigen, um sicheren Zugang zu gewährleisten.

**2. Authentifikation von Menschen durch IT-Systeme**

* **Ansätze:**
  1. **Was der Mensch ist:** Nutzung biometrischer Merkmale wie Fingerabdruck, Gesichtserkennung.
  2. **Was der Mensch hat:** Besitz von Schlüsseln, Chipkarten.
  3. **Was der Mensch weiß:** Nutzung von Passwörtern, PINs.
  4. **Wo der Mensch ist:** Standortbasierte Authentifizierung.

**Lernbrücke:** Die Kombination verschiedener Ansätze, z.B. biometrische Merkmale mit Passwörtern, erhöht die Sicherheit.

**3. Biometrische Merkmale**

* **Physiologische Merkmale:** Fingerabdruck, Iris-Muster, Gesicht, DNA.
* **Verhaltensbasierte Merkmale:** Handschrift, Gang, Tipp-Charakteristik.
* **Prinzip:** Vergleich von gespeicherten Merkmalen mit aktuellen Scans zur Authentifikation.
  + **Mögliche Angriffe:** Herstellung von künstlichen Fingerabdrücken, Verwendung von Fotos zur Umgehung von Gesichtserkennung.
  + **Abwehrmaßnahmen:** Überwachung der Authentifikation, z.B. Kontrolle von Lebenszeichen wie Augenbewegungen.

**Lernbrücke:** Während biometrische Merkmale schwer zu fälschen sind, bieten sie auch einzigartige Herausforderungen, wie den Schutz der gespeicherten Daten und die Verhinderung von Spoofing.

**4. Passwörter**

* **Alphanumerische Passwörter:** Kombination aus Buchstaben, Zahlen, und ggf. Sonderzeichen.
  + **NIST-Richtlinien:** Länge ist wichtiger als Komplexität; Sichtbarkeit bei der Eingabe und automatische Einfügen fördern stärkere Passwörter.
* **Graphische Passwörter:** Nutzung von Bildern oder Mustern zur Authentifikation.
* **Zwei-Faktor-Authentifizierung:** Kombination aus zwei verschiedenen Authentifikationsmethoden (z.B. Passwort und Fingerabdruck).

**Lernbrücke:** Die Wahl des richtigen Passworts und dessen sichere Speicherung sind entscheidend, um Angriffe wie Brute-Force zu verhindern.

**5. Authentifikation von IT-Systemen durch Menschen**

* **Merkmale:**
  + **Was das IT-System ist:** Physische Merkmale wie Gehäuse, Siegel.
  + **Was das IT-System weiß:** Passwörter oder Antworten auf Fragen.
  + **Manipulationen:** Beispiele sind Phishing oder Man-In-The-Middle-Attacken.

**Lernbrücke:** Nicht nur Menschen müssen authentifiziert werden, sondern auch IT-Systeme, um sicherzustellen, dass man mit dem richtigen System kommuniziert und nicht mit einem manipulierten.