**Lernzettel 3: Zugriffskontrolle**

**1. Grundbegriffe und Zugriffsrechte**

* **Objekte:** Repräsentieren Informationen (z.B. Dateien als passive Objekte, Prozesse als aktive Objekte).
* **Subjekte:** Benutzer oder aktive Objekte, die im Auftrag von Benutzern agieren.
* **Zugriff:** Interaktion zwischen Subjekt und Objekt, die Informationsfluss verursacht.

**Lernbrücke:** Der Zugriff auf ein Objekt bedeutet immer auch den Zugriff auf die damit repräsentierte Information. Daher ist die Kontrolle dieser Zugriffe entscheidend für die IT-Sicherheit.

**2. Zugriffskontroll-Modelle**

* **Benutzerbestimmbare Zugriffskontrolle (Discretionary Access Control - DAC):**
  + **Rollenbasierte Zugriffskontrolle (Role-based Access Control - RBAC):** Rechtevergabe basierend auf den Rollen der Subjekte, z.B. Administrator, Nutzer.
* **Systembestimmte Zugriffskontrolle (Mandatory Access Control - MAC):**
  + **Bell-La Padula Modell:** Fokussiert auf die Vertraulichkeit, mit Regeln wie "No-read-up" und "No-write-down".
  + **BIBA Modell:** Fokussiert auf Integrität, mit umgekehrten Regeln zu Bell-La Padula.
  + **Chinese Wall Modell:** Verhindert Interessenkonflikte, indem es den Zugriff auf Informationen basierend auf früheren Zugriffen einschränkt.

**Lernbrücke:** DAC erlaubt flexiblere Zugriffsentscheidungen durch Benutzer, während MAC striktere, systemweite Regeln durchsetzt, um spezifische Sicherheitsanforderungen wie Vertraulichkeit oder Integrität zu garantieren.

**3. Methoden der Zugriffskontrolle**

* **Zugriffskontrollmatrix:** Ein einfaches Modell, das die Zugriffsrechte in einer Matrix darstellt. Nachteile: Skaliert schlecht bei dynamischen Mengen von Subjekten.
* **Zugriffskontrollliste (Access Control List - ACL):** Ordnet jedem Objekt eine Liste zu, die festlegt, welche Subjekte welche Zugriffsrechte haben. Vorteile: Einfache Implementierung, aber ineffizient bei langen Listen.
* **Capabilities:** Zeilenweise Darstellung der Zugriffskontrollmatrix, bei der Subjekte Zugriffstickets (Capabilities) erhalten, die ihre Rechte repräsentieren. Vorteile: Flexibel, erlaubt Delegation von Rechten. Nachteile: Schwierige Verwaltung und sichere Speicherung erforderlich.

**Lernbrücke:** Die Wahl der Methode hängt stark vom Anwendungsfall ab. Während ACLs oft in Betriebssystemen genutzt werden, bieten Capabilities mehr Flexibilität in verteilten Systemen.

**4. Beispiele für Zugriffskontroll-Modelle**

* **RBAC im Bankszenario:** Rollen wie Zweigstellenleiter, Kassierer oder Kunde bestimmen die Zugriffsrechte auf Konten und Transaktionen.
* **Bell-La Padula im Regierungsumfeld:** Schützt geheime Informationen durch strenge Regeln zur Vertraulichkeit.
* **Chinese Wall im Finanzsektor:** Verhindert, dass Berater Zugang zu konkurrierenden Firmen in derselben Branche erhalten.

**Lernbrücke:** Diese Modelle zeigen, wie verschiedene Zugriffskontrollmethoden auf spezifische Anwendungsfälle angepasst werden können, um spezifische Sicherheitsziele wie Vertraulichkeit oder Integrität zu erreichen.

**5. Bedeutung der Zugriffskontrolle**

* **OWASP Top Ten:** Fehler in Zugriffskontrollen stehen an erster Stelle der Sicherheitsprobleme im Web, z.B. durch unzureichende Privilegienkontrolle oder falsche Standardkonfigurationen.

**Lernbrücke:** Die richtige Implementierung von Zugriffskontrollen ist entscheidend für die Sicherheit von Systemen, insbesondere im Webumfeld, wo Fehler gravierende Folgen haben können.