LU06a - Berechtigungskonzepte

Lernziele

- Die drei Varianten von Berechtigungskonzepten nennen und erläutern können.
- Zu jeder der drei Varianten mindestens ein konkretes Produkt/Anwendung nennen können.
- Die Datengrundlage (Datenbankmodell) für jedes Konzept aufzeichnen und erläutern können.

Einleitung

In modernen IT-Systemen greifen viele Benutzer gleichzeitig auf Daten, Anwendungen und Dienste zu. Damit nicht jeder alles darf, braucht es Berechtigungskonzepte. Sie legen fest, wer welche Ressourcen nutzen, ändern oder verwalten darf. Ziel ist es, Sicherheit, Datenschutz und Stabilität zu gewährleisten, ohne die Arbeit unnötig zu behindern.

Ein gutes Berechtigungskonzept sorgt für:

- Schutz sensibler Informationen (z. B. personenbezogene Daten, Finanzdaten)
- Minimierung von Risiken durch das Prinzip „least privilege“ (nur die Rechte, die wirklich nötig sind)
- Nachvollziehbarkeit von Zugriffen durch klare Rollen und Verantwortlichkeiten

Berechtigungskonzepte sind damit ein zentrales Element von IT-Sicherheit und unverzichtbar in Unternehmen, Verwaltungen und auch in privaten IT-Umgebungen.

Grundlagen

Ein Berechtigungskonzept beschreibt ein System, in dem die Nutzung von Ressourcen nicht uneingeschränkt möglich ist, sondern eine genaue Definition der Nutzung je Benutzer und Ressource erfolgt. Obwohl ursprünglich aus dem organisatorischen Umfeld kommend haben Berechtigungskonzepte, vor allem im Zusammenhang mit IT-Systemen eine wichtige Bedeutung.

Ressourcen sind hier beispielsweise Daten und Informationen, aber auch die technische Infrastruktur wie Systemzugänge, Speicherplatz, Rechnerleistung, Computerprogramme usw.

Merke: Ein Berechtigungskonzept dient dem Schutz eine Ressource vor Veränderung oder Zerstörung, verhindert aber auch ihren unrechtmäßigen Gebrauch.

Schützenswerte Ressourcen können beispielsweise Hardware sein:

```
* Computer
* Rechenzeit
* Prozess-Priorisierung
* Drucker
```

Aber auch Software oder Daten müssen oft geschützt werden:

- Datenbankobjekte wie Datenbanktabelle
- Files
- Ordner
- Zugriffsart

Schutz bedeutet also die Ressourcen vor Veränderung oder Zerstörung (z. B. Datensicherheit) zu schützen. Es bedeutet aber auch zu ihren unrechtmässigen Gebrauch (z. B. Datenschutz) zu verhindern.

Varianten

Es gibt unterschiedliche Kriterien für Benutzerkonzepte. Im vorliegenden Fall wollen wir uns auf die drei Elemente *Rollen*, *Gruppen* und *Rollen* konzentrieren.

Benutzerebene (User-Based Access Control – UBAC)

Bei diesem Konzept werden die Rechte direkt einem Benutzerkonto zugewiesen.

- **Vorteile:**
  - einfach zu verstehen
  - individuell anpassbar
  - Kkontrolle der Berechtigung ist direkt beim Owner
- **Nachteile:**
  - Unübersichtlich und schwer wartbar, wenn viele Benutzer existieren
  - Die Koordination der Berechtigungen wird komplex und aufwendig
- **Administrationsaufwand:**
  - Linear: Jede auch so kleine Anpassung muss überall durchgeführt werden

• Beispiel:

```
•   Benutzer Max Mustermann darf Ordner C:\\Projekte lesen und schreiben.
•   Benutzer Anna Müller hat nur Leserechte.
```

Rein benutzerbezogene Konzepte neigen zur Unübersichtlichkeit und sind deshalb oft nur rudimentär ausgeprägt. Das nachfolgende Entity Relationship Modell einer Benutzersteuerung auf Datenbankebene zeigt eine mögliche Umsetzung auf reiner Benutzerebene: