Sicherheit in Datenbanksystemen

Datenmodellierung, Datenbanksysteme

Ingo Claßen, Martin Kempa, Peter Morcinek

Hochschule für Technik und Wirtschaft Berlin

Sicherheit allgemein

Authentifizierung

Autorisierung

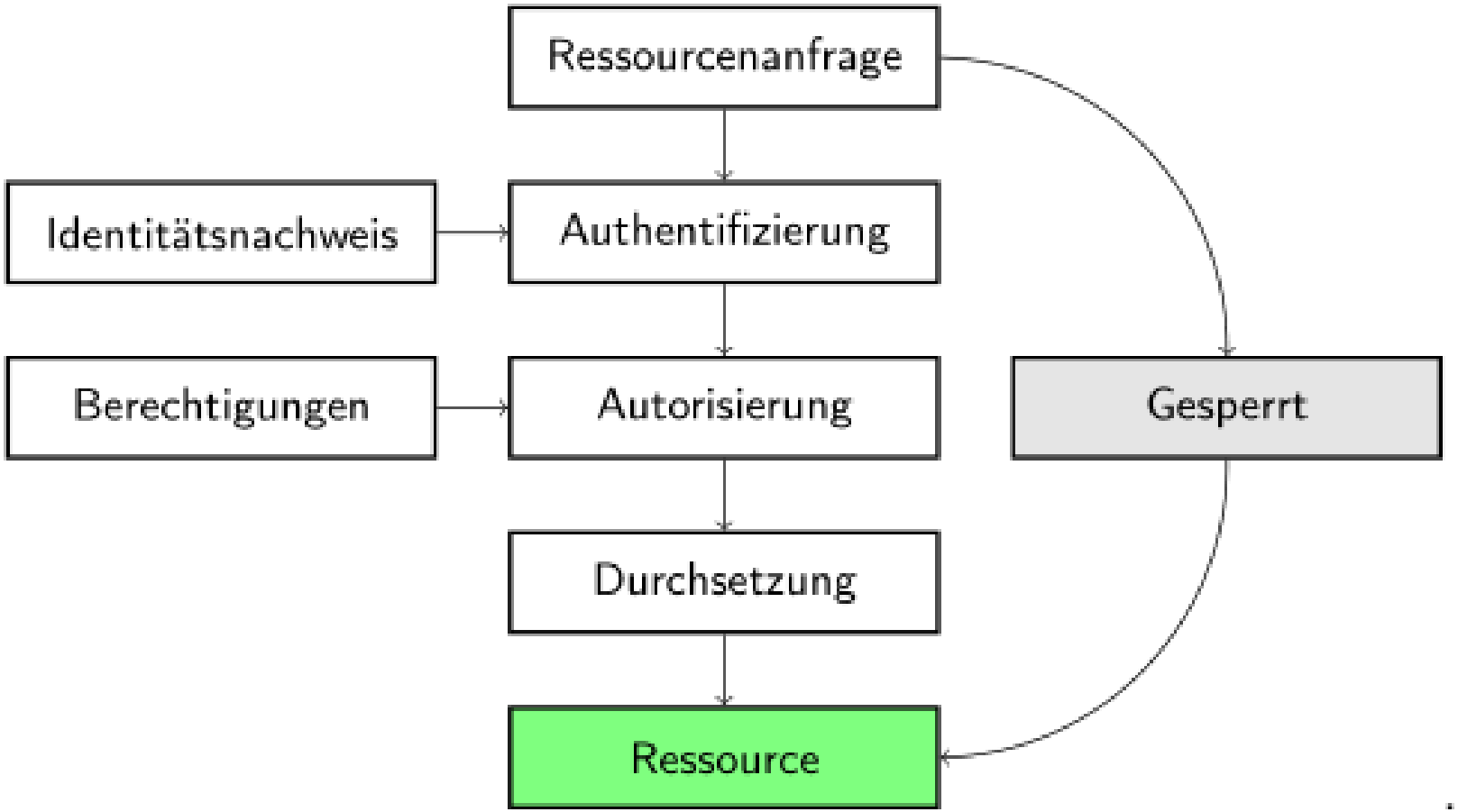
Weitere Mechanismen

Aspekte von Sicherheit

„A computer is secure if it behaves the way that you expect it will."

- Funktionssicherheit (safety)
  Ist-Funktionalität = Soll-Funktionalität
- Datensicherheit (protection)
  keine unautorisierten Zugriffe
- Informationssicherheit (security)
  keine unautorisierte Informationsänderung und/oder -gewinnung
- Datenschutz (privacy)
  Kontrolle der Weitergabe personenbezogener Daten

Struktur sicherer Systeme



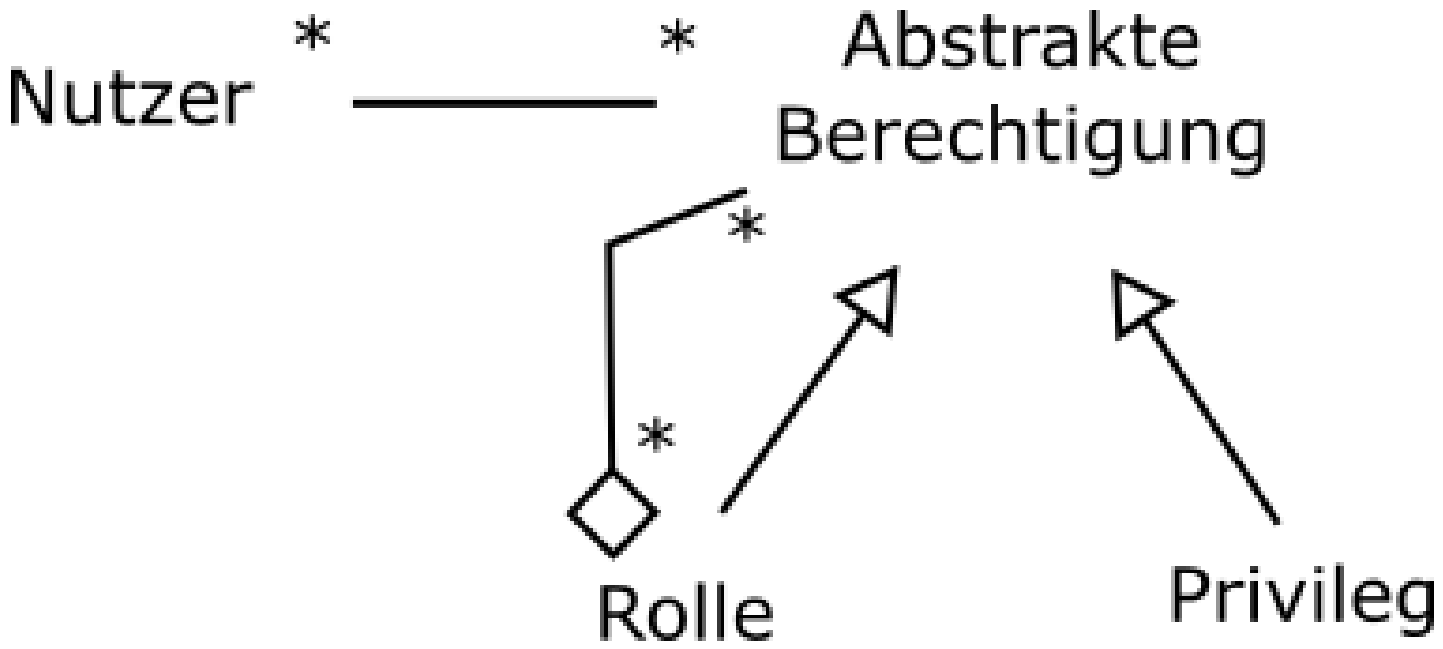
Möglichkeiten der Authentifizierung

- Interne Authentifizierung
  - Klassische Variante, Nutzer wird in DB angelegt
    ```
    create user u007 identified by p007;
    ```
  - Passwort wird in der Datenbank verschlüsselt
- Externe Authentifizierung
  - Verifizierung der Identität durch externe Quellen, z.B Betriebssystem
    ```
    create user ops$u007 identified externally;
    ```
  - Der Nutzer kann für mehrere DBs genutzt werden

Berechtigungsverwaltung

- Zugriffskontrolle auf die Datenbank und Datenbankobjekte
- DBS prüft vor dem Zugriff die Gültigkeit entsprechende Berechtigungen
- Voraussetzung:
  Der generelle Zugriff auf Betriebsystem- bzw. Dateiebene muss geregelt sein

Berechtigungsmodell



- Durch Privilegien werden Berechtigungen erteilt
- Rollen bündeln Privilegien, die zusammen erteilt werden sollen

Privilegien

- Auf der Ebene des Nutzerkontos

  `create table, drop table`
  `create view, drop view`
  `create role, drop role`

- Auf Objektebene, z.B. Tabellen

  `select`
  `insert`
  `delete`
  `update`

Erteilung von Berechtigungen

- Tabelle

Mitarbeiter
MNR
Name
Gehalt

- Sicht

MOhneGehalt
MNR
Name

```
create user mueller identified by ...;
create user krause identified by ...;

create role sachbearbeiter;
create role chef;

grant select on Mitarbeiter to chef;
revoke select on Mitarbeiter
  from sachbearbeiter;
grant select on MOhneGehalt
  to sachbearbeiter;

grant sachbearbeiter to mueller;
grant chef to krause
```

Weitere Mechanismen

- Verschlüsselung von Daten in Spalten
- Verschlüsselung der Kommunikation zwischen Client und Datenbankserver
- Protokollierung von Datenbankzugriffen
- Vergabe von Sicherheitsstufen für Nutzer und Datensätze
  - Ergänzung zu Privilegien
  - Nutzer dürfen nur Daten sehen, deren Sicherheitsstufe unter der eigenen Sicherheitsstufe liegt
- Private Datenbasen
  - Automatische Ergänzung von Abfragen um zusätzliche Where-Bedingungen
  - Transparent für alle Anwendungen
- Sicherheitsmechanismen in Anwendungsprogrammen