Multi-User-Applikationen objektorientiert realisieren

Informationssicherheit

25.11.24

Ziele

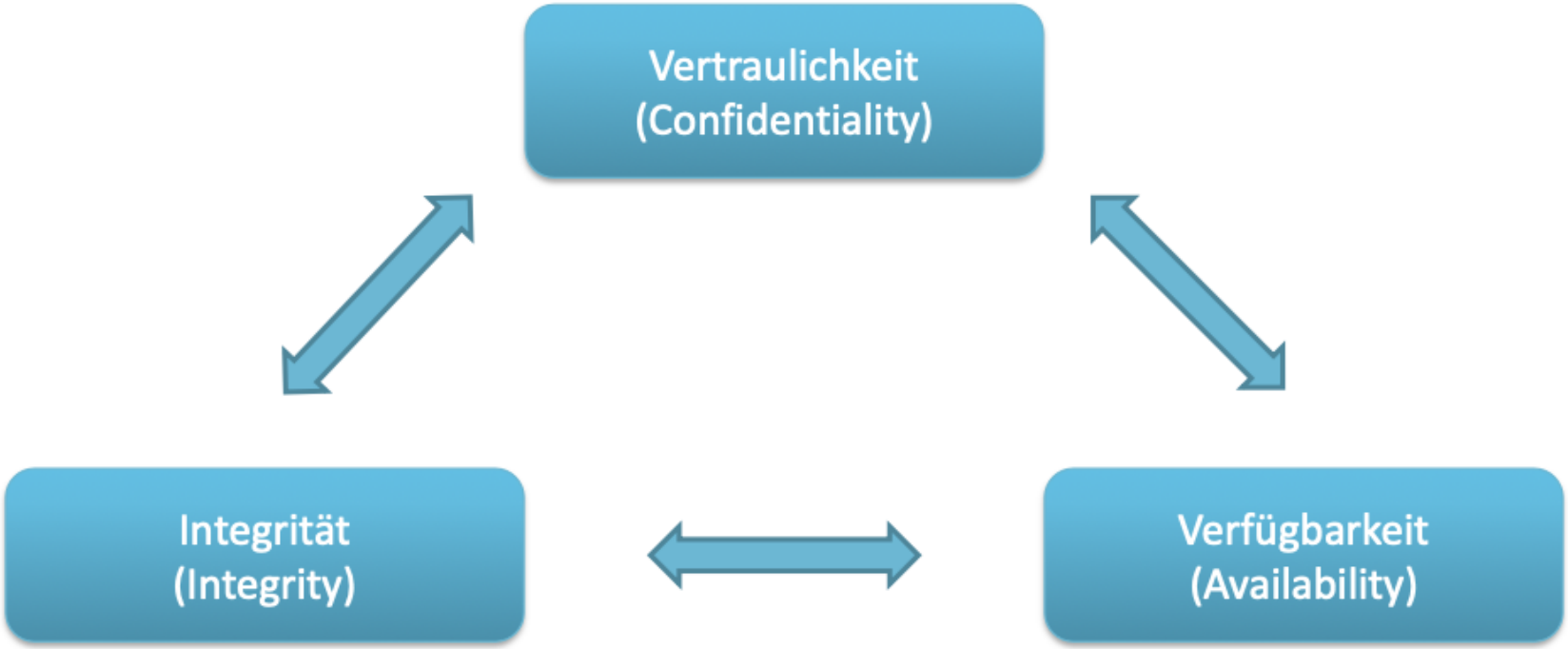
- Du kennst das Schichtenmodell der Informationssicherheit
- Du kennst den Unterschied zwischen Authorization und Authentication
- Du kannst erklären, was Authorization und Authentication bedeuten
- Du kennst das C.I.A. Dreieck

Informationssicherheit

- Daten sind schützenswerte Güter!
- Der Zugriff auf sensible Daten sollte beschränkt und kontrolliert sein
- Nur autorisierte Benutzer / Systeme dürfen auf die Daten zugreifen
- Informationssicherheit ist eine grosse Herausforderung bei Multiuser-Applikationen

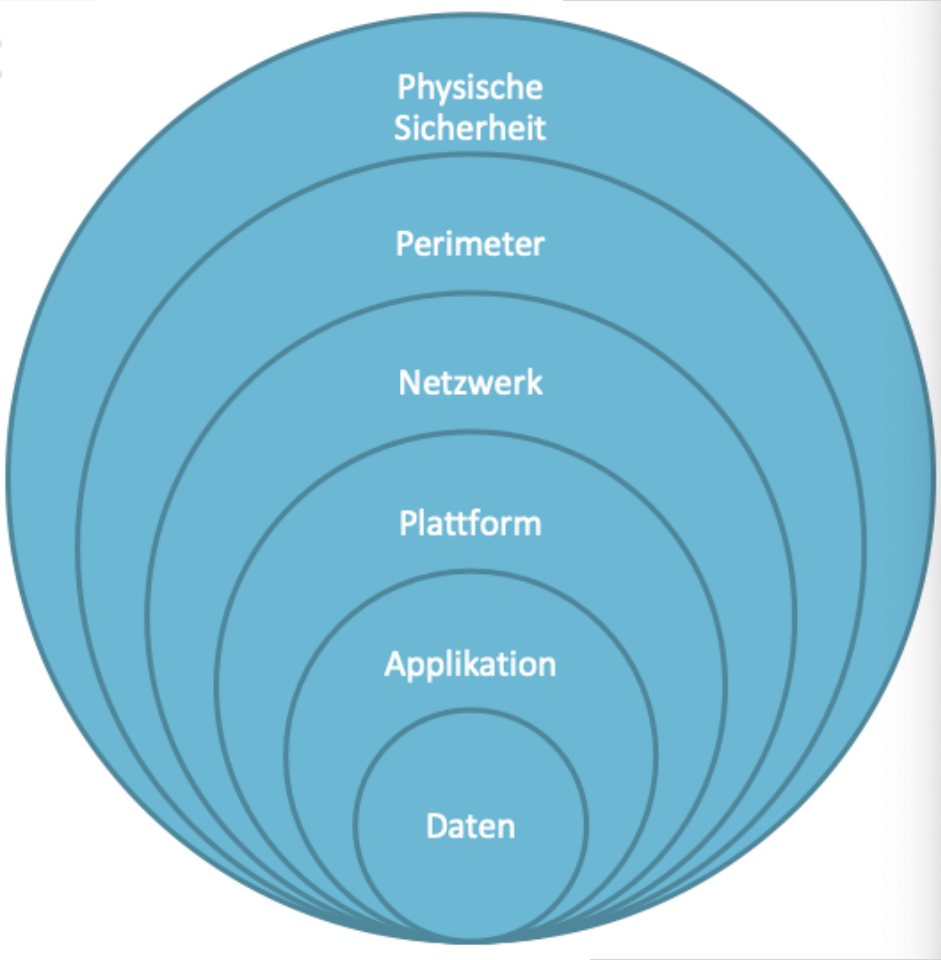
Informationssicherheit

C.I.A. Dreieck



Informationssicherheit
Ganzheitliche Sicherheit

Informationssicherheit
Schichtenmodell



Informationssicherheit
Schichtenmodell

- Physische Sicherheit
  - Zugangskontrolle für Gebäude, Serverräume, etc.
  - Geräte trennen
- Perimeter
  - Firewall, VPN, Router
- Netzwerk
  - Netzwerk Segmente

Informationssicherheit
Schichtenmodell

- Plattform / Betriebssystem
  - Security Update Management, Anti-Virus, lokale Firewall, Zugriffsberechtigungen
- Applikation
  - Sicherheitsstandards beim Programmieren beachten, Zugriffsberechtigungen
- Datenschutz
  - Daten verschlüsseln, starke Passwörter, hashen

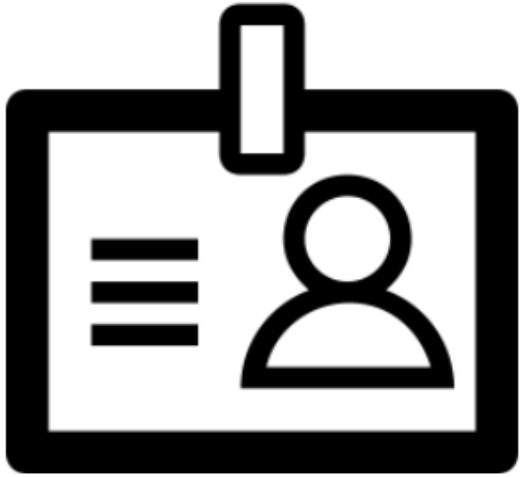
Authentication

- Nachweis / Verifizierung einer Echtheit einer Eigenschaft
- Z.B. der Nachweis, dass jemand wirklich der ist für den er sich ausgibt.
- Methoden:
  - Wissen (Passwort, PIN, Sicherheitsfrage)
  - Besitz (Karte, Schlüssel, Zertifikat)
  - Biometrie (Fingerabdruck, Gesichtserkennung, etc)

Authorization

- Welche Rechte hat ein authentifizierter Benutzer? / Was kann ein Benutzer tun?
  - Beispiel: User X darf die Operation Löschen der Resource Y ausführen
- Kann z.B. pro Applikation, Formular oder Methode definiert werden

Zusammenfassung



Authentication

Wer ist angemeldet? (Login)

Authorization

Was darf der angemeldete machen? (Rechte)

JWT
JSON Web Token

- Header
  - Typ und Algorithmus
- Payload
  - Data (Subject, expiration usw.)
- Signature
  - Verifizierungs Hash

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJtYXhAbXVzdGVyLmNoIiwiZXhwIjoxNjM0OTg5MjQyfQ.fwnOtD6KmwR7AUjk6ZnE0JgZPM5hyN-sXt4OETOlqEcxpDr9v7fWR6_66Ltsh6tp1EbFl2u-U95Rli1Gq_n8hw

JWT
JSON Web Token

```
{
  "typ":"JWT",
  "alg":"HS512"
}
{
  "sub":"max@muster.ch",
  "exp":1634989424
}
```

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIU
zUxMiJ9.eyJzdWIiOiJtYXhAbXVz
dGVyLmNoIiwiZXhwIjoxNjM0O
Tg5MjQyfQ.fwnOtD6KmwR7AU
jk6ZnE0JgZPM5hyN-
sXt4OETOlqEcxpDr9v7fWR6_6
6Ltsh6tp1EbFl2u-
U95RIi1Gq_n8hw
```

Hash von (header + ". " + payload, secret)

Fragen?