Netzwerksicherheit

Sicherheitsaspekte:

- Verfügbarkeit, Stabilität, Robustheit
- Einbruchssicherheit

Verfügbarkeit

- Redundanz
  - round robin, Bsp: google MX
  - ha-proxy (mehrere Backend-Server)
- Begriff des "single point of failure"
- anycast (eine IP, viele Server)
- stabile Betriebssysteme

Sicherheit vor Einbruch und Datendiebstahl

- Problematik: Hin und wieder knackt ein Mathematiker einen crypto-Algorithmus, daher:
- regelmäßiges Patchen aller beteiligten Software-Komponenten
- Inventory über Patch-Stände (eher junges Konzept, noch in den Kinderschuhen)
- Firewalls
  - Layer 3 (Paketfilter, stateful)
  - Layer 7 (deep inspection). Sog. Application-Level Firewalls, z.B. WAF (Web Application Firewall).
    Problematik hier: SSL ist End-to-End verschlüsselt
    "Intrusion Avoidance"
  - schlecht konfigurierte Firewalls, oft schwierig zu debuggen
- Cryptographie
  - TLS als verbreitetstes Crypto-Protokoll (xxx *over TLS*), z.B.:
    - https: http over TLS
    - smtps, imaps, ... usw
- Intrusion Detection
  - KI wird eingesetzt, um Anomalien zu erkennen. Zentrales Logging Voraussetzung.
- 2-factor authentication, Ausblick auf Layer 8
- Unterscheidung Authenticaton / Authorization
  - merke: Georg (authenticated) -> "is not authorized" (permission denied)