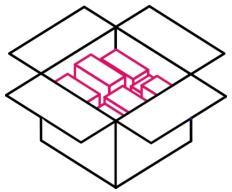
Netzwerksegmentierung

Hoai Viet Nguyen – TH Köln

Technology
Arts Sciences
TH Köln

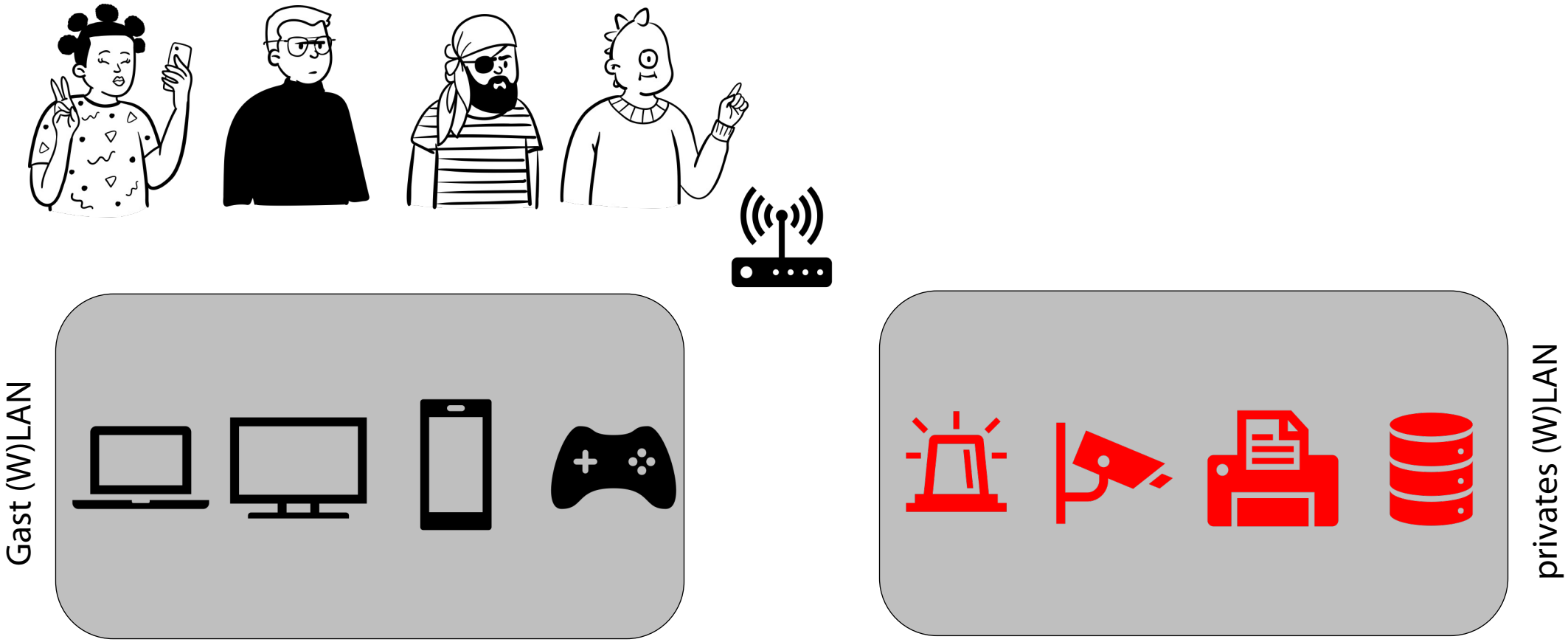


Jedes Mal wenn Besuch da ist…

WLAN-Passwort wird an (unbekannte) Personen weitergegeben

Systeme und Zugriffe im Heimnetzwerk

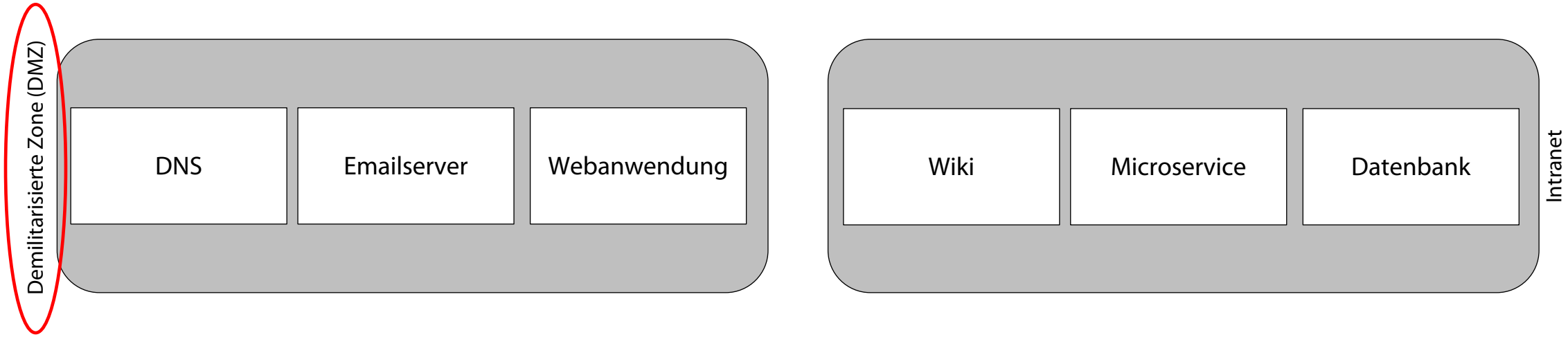
Netzwerksegmentierung in privates Netzwerk und Gastnetzwerk



Netzwerksegmentierung im Heimnetzwerk

- Isolierung von kritischen Systemen
- Individuelle Zugriffssteuerung für bestimmte Segmente wie z.B.
  - Kein Zugriff die Admin-Oberfläche des Routers innerhalb des Gastnetzwerks
  - Eingeschränkte Kommunikation von Geräten untereinander
  - Eingeschränkte Zugriff auf externe Dienste
  - Nur bestimmte Geräte dürfen auf privates Netzwerk zugreifen
- Vereinfachte Überwachung auf verdächtige Aktivitäten

Netzwerksegmentierung in Unternehmen und Organisationen



Demilitarisierte Zone (DMZ)

- Netzwerksegment zwischen internes und öffentliches Netzwerk
- Enthält i.d.R. öffentliche zugängliche Dienste wie z.B.
  - Webseite/Webanwendung
  - DNS
  - E-Mail
- Optimierte Sicherheit
  - Verkleinert die Angriffsfläche auf kritische Systeme im internen Netzwerk
  - Begrenzt die direkten Verbindungen zwischen internen Netzwerken und dem Internet

Warum verwenden Unternehmen/Organisation Netzwerksegmentierung?

Einschränkung der Angriffsfläche:
Ist ein System in einem Segment komprimiert, kann der Angreifer sich nur innerhalb des Abschnitts ausbreiten

Compliance:
Viele Branchenstandards und rechtliche Anforderungen (PCI DSS, DSVGO, BAIT, VAIT) verlangen es

Verwaltung:
Individuelle Sicherheitsrichtlinien für bestimmte Segmente

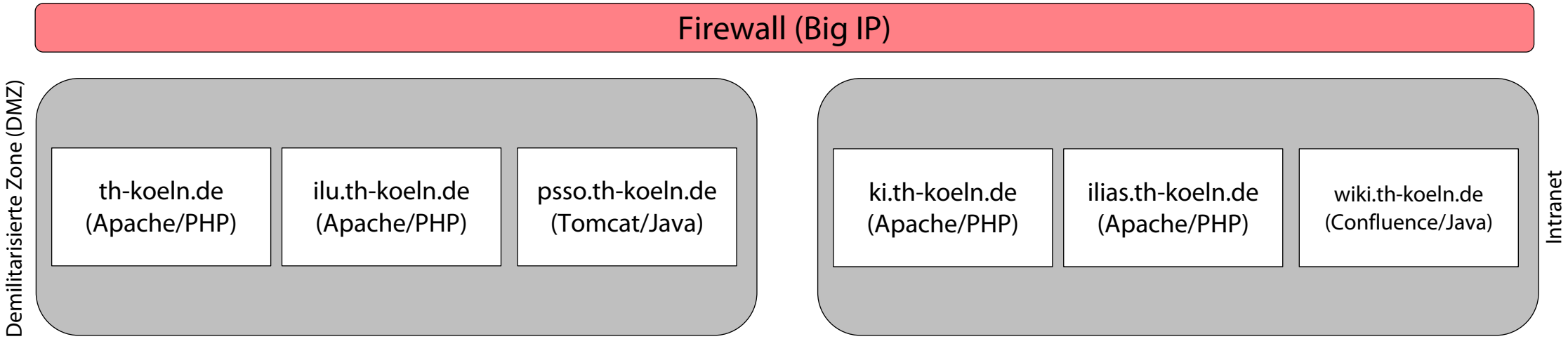
Performance:
Aktivitäten in einem Segment haben keinen Einfluss auf die Leistung anderer Netzwerkbereiche

Monitoring:
Übersichtliche Überwachung von einzelnen Segmenten

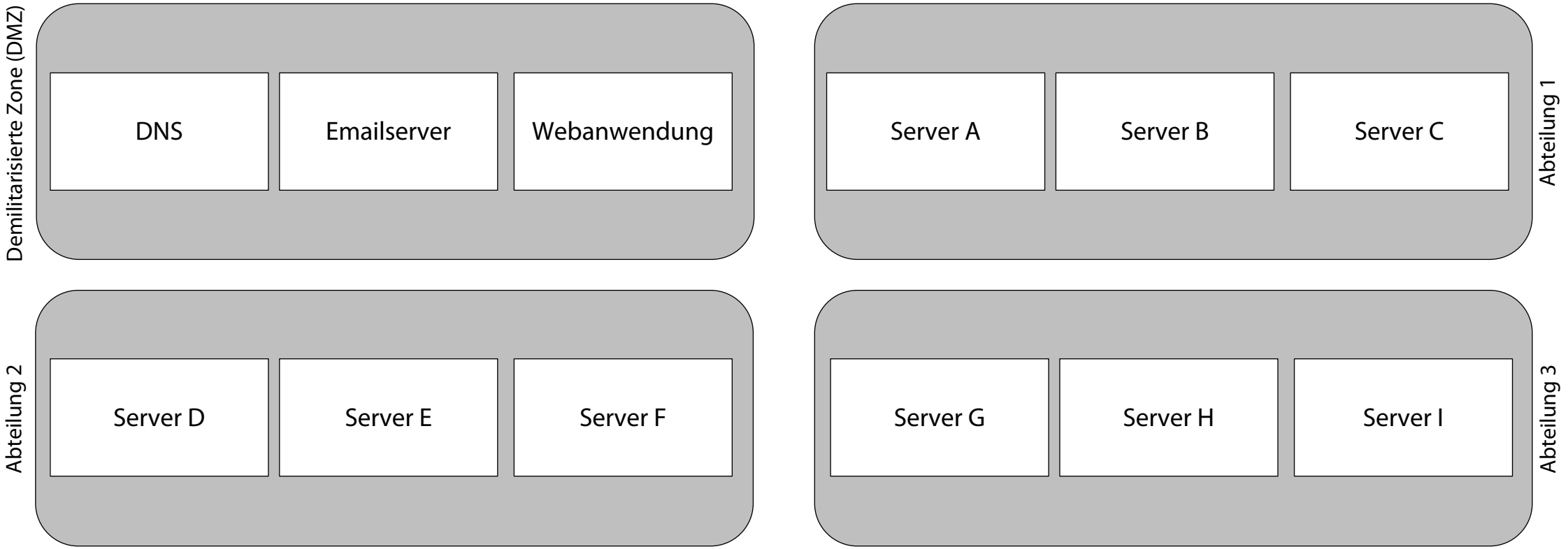
Implementierung der Netzwerksegmentierung

- Firewall (Hardware/Software)
- Router (Hardware/Software)
- (VLAN) Switches
- Subnetting
- Software-defined Networking (SDN)

Vermutliche Netzwerksegmentierung an der TH Köln (Ausschnitt)



Netzwerksegmentierung mit mehreren Bereichen



Lernzielkontrolle

- Was ist Netzwerksegmentierung?
- Welche Qualitätsmerkmale neben der Sicherheit optimiert Netzwerksegmentierung noch?
- Wie kann eine Netzwerksegmentierung implementiert werden?
- Was ist eine DMZ?

Zusammenfassung Netzwerksegmentierung

- Gängige und wichtige proaktive Sicherheitsmaßnahme, um Netzwerke in mehrere Bereiche zu isolieren
- Optimiert neben der Sicherheit andere Aspekte wie z.B.
  - Performance
  - Monitoring
  - Verwaltung von Sicherheitsrichtlinien
- Kann mit Firewalls, VLANs, Switches, Routern, Subnetting und SDNs implementiert werden
- DMZ
  - Ein Netzwerksegment, das zwischen Internet und internen Netzwerk liegt
  - Enthält öffentlich zugängliche Systeme