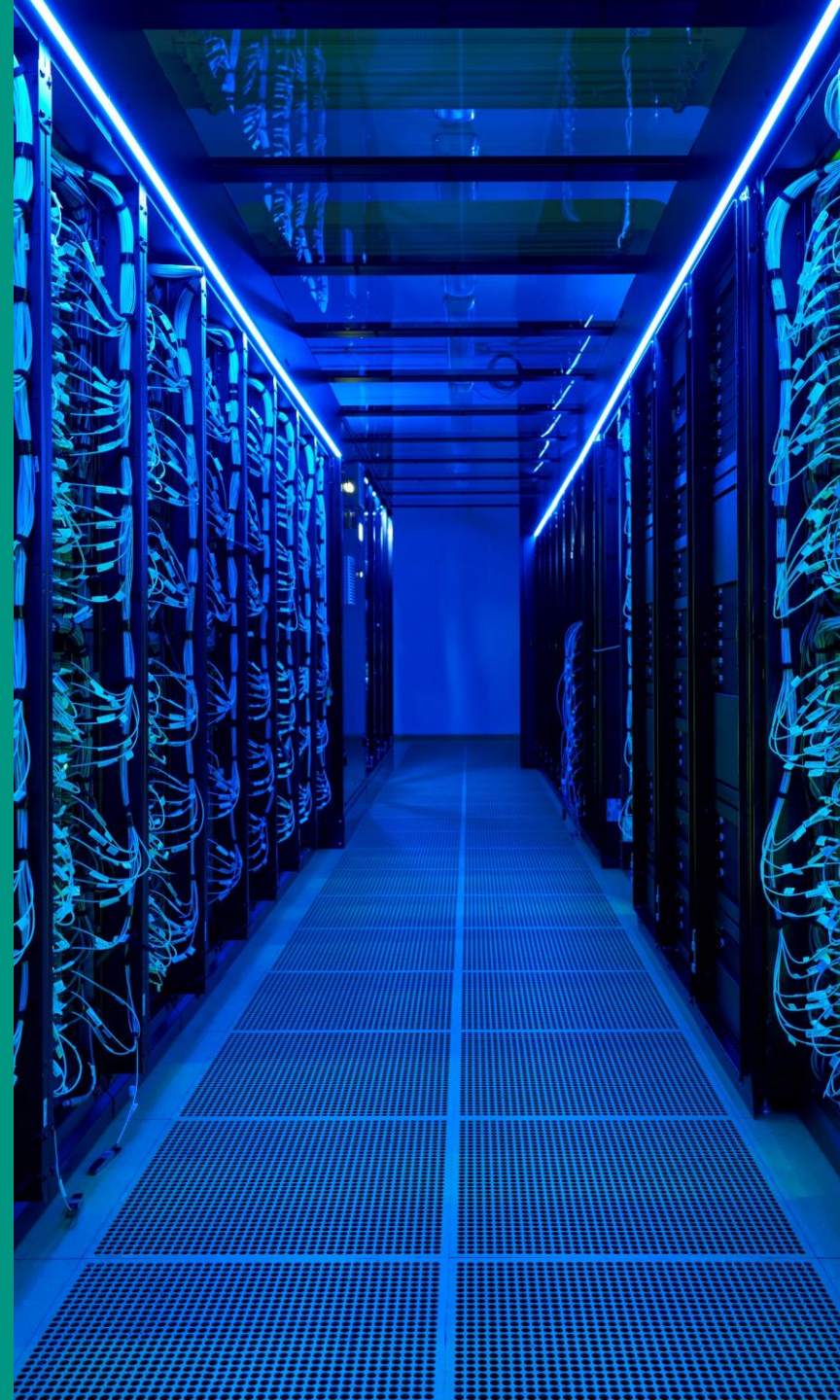


bwCampusnetz IT-Grundschutz

Klara Mall, Scientific Computing Center SCC,
05.11.2025



BSI IT-Grundschutz

Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit)

- <https://www.landesrecht-bw.de/bsbw/document/VVBW-VVBW000043884>
- „Alle Dienststellen und Einrichtungen der Landesverwaltung Baden-Württemberg setzen die Informationssicherheit gemäß IT-Grundschutz (BSI Standards 100-1 bis 100-3) um.“

Im Projekt betrachtet wurden die folgenden Bausteine:

- NET 1.1 Netzarchitektur
- NET 3.2 Firewall
- (NET.3.1 Router und Switches)

Begriffe in NET.1.1 und NET.3.2

- Firewall
- Netzwerksegment
- Zone
- Demilitarisierte Zone (DMZ)
- Internes Netz / Intranet
- Extranet
- Application-Layer-Gateway (ALG)
- Sicherheitsproxy

Zentrale Punkte

- Segmentierung
- Firewalling
- Unterteilung des Netzes in Zonen

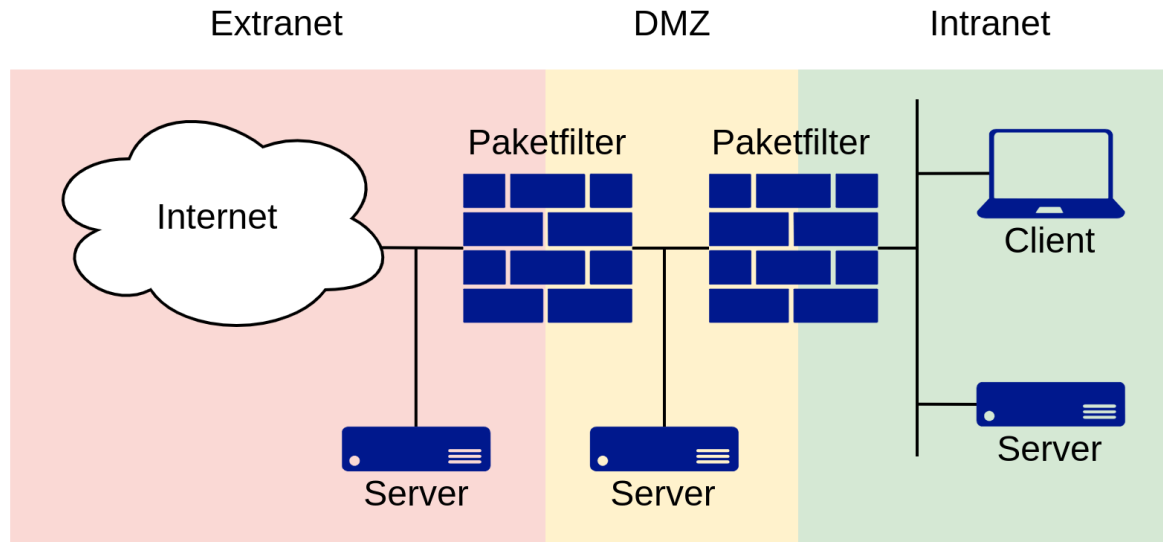
Fragliche Punkte

- Physische Separierung
 - Skalierbarkeit
 - Flexibilität
 - Wirtschaftlichkeit
- Application Layer Gateway / Sicherheitsproxy
 - Ende-zu-Ende-Prinzip verletzt
 - Performance
 - Keine strikte Trennung zwischen Netzwerk und Anwendung
 - Aufbrechen von Verschlüsselung
 - Tunnel-Techniken können das Erkennen von schadhafter Software verhindern
- Dynamische Routing-Protokolle
 - Skalierung
 - Anycast-Redundanz
 - Zu viele Änderungen im Netz
 - Routing-Protokolle sind abgesichert

Mögliche Architekturen

- Für kleine Campusnetze
 - Klassisch: DMZ zwischen zwei Perimeter-Firewalls
 - Intranet / Extranet
- Für größere Campusnetze; wenn Flexibilität benötigt
 - Unterteilung des Intranets in viele kleine Zonen
 - Firewallbypass
 - Extranet

Klassische DMZ



Alternative Architektur

