VLAN Security und Design

VLAN Attacks

- Switch Spoofing Attack: Gerät gibt sich als Switch aus und versucht per DTP eine Trunkleitung aufzubauen
- VLAN-Hoppimng durch Double-Tagging-Attack: 1.Tag: native VLAN, 2.Tag: Ziel-VLAN

Private VLANS (PVLAN Edge)

Kein Traffic zwischen protected Ports. PCs können nicht untereinander kommunizieren, sondern nur mit Gateway, Servern, ...

Best Practices for VLANs

- Alle Switchports sollen in einem anderen VLAN als VLAN 1 sein
- unbenutzte Switchports: im 'black hole' VLAN und deaktivieren
- Management- und User-Traffic trennen (in unterschiedliche VLANs)
- Switchkonfiguration nur über SSH
- Native-VLAN soll nicht VLAN 1 sein $\Rightarrow$ Control-Traffic im VLAN 1 wird getaggt
- DTP abschalten