# Netzwerkadministratoren

Netzwerkhardware Administration über SSH

Erbt von User

# Applikationsadministratoren

Administrieren aller Server über Microsoft RDP bzw. SSH bzw. VNC  
Adminrechte im AD

Erbt von User

# User

Internet, Intranet, Mails, Fileservices, Login im AD,

# Gäste

Kein Internet nur Zugriff auf Intranet

# Passwordpolicy

* Min 1 Großbuchstabe
* Min 1 Kleinbuchstabe
* Min 1 Zahl
* Min 8 Zeichen

# VLANS

* Server (Jeder in eigenem VLAN)
* NW Administratoren
* Applikationsadministratoren
* User
* Gäste

# Services

* Jegliche Kommunikation über SSH statt Telnet
* Jegliche Dateiübertragungen über SSH (SFTP) statt FTP
  + Telefone dürfen TFTP verwenden wenn nicht anders möglich ist
* Nur verschlüsselte Mail Ports statt unverschlüsselte Mail Ports
* Kein OSPF in Clientnetzen

**Anmerkungen:**

SNMP   
ACL Richtung Internet  
Verbindungen verschlüsseln (Routing)  
Konfigurationssicherheit (verändern)

# Überwachung

Alle Auslastungen von allen Netzwerkkomponenten, um die Übersicht zu behalten

Verdächtiger Traffic (Pings, http-requests, Active Directory, viele DNS- oder DHCP-Aufrufe)

Wenn Interfaces ausgeschaltet werden

Adminuser-Aktivitäten

Neustart & Herunterfahren von Servern bzw. wenn sie das Netzwerk verlassen