Dr. Orasch Sylvia

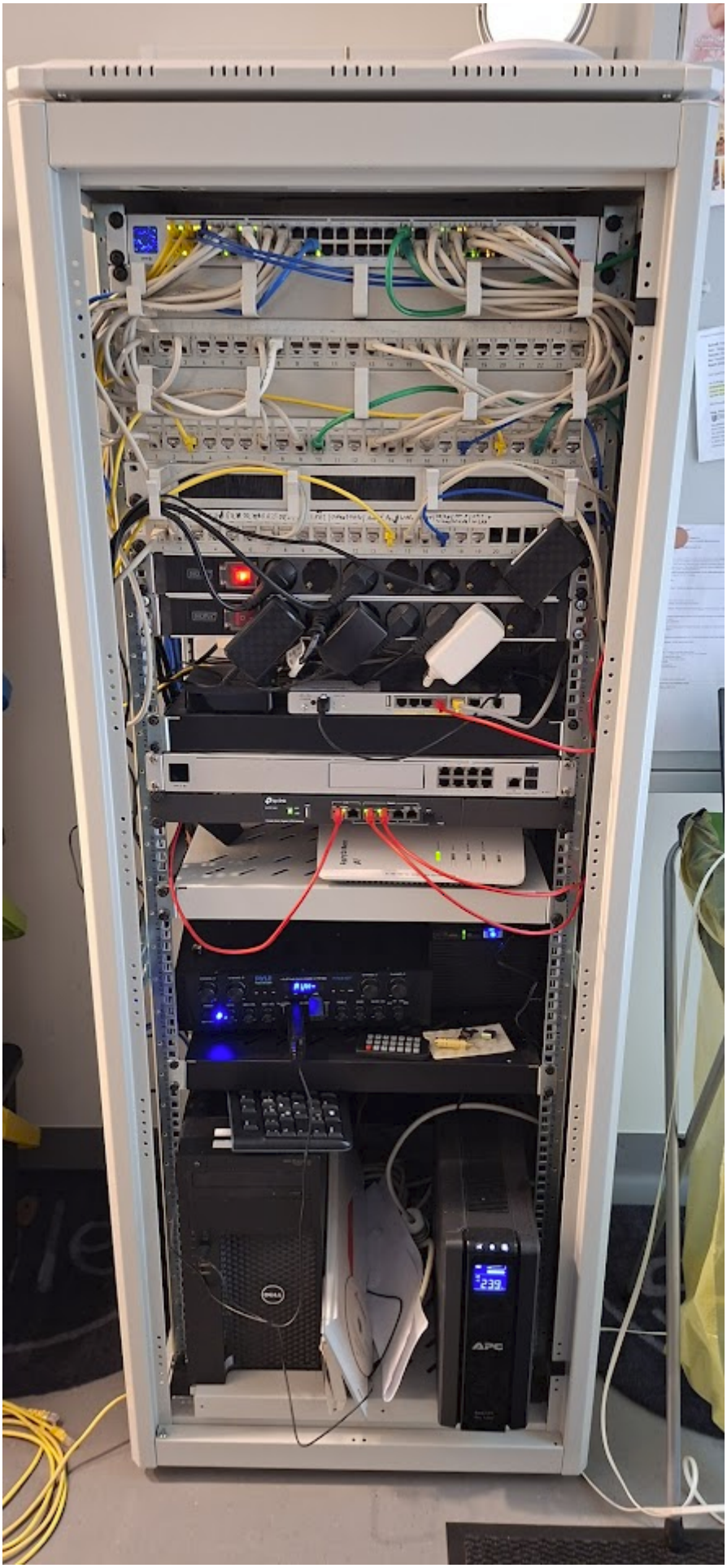
Allgemein

Überblick

Internet über A1 (Fritzbox), TP-Link als Gateway, 2x AP

Switches von Unifi, im Netzwerk ist auch ein Unifi Cloud Key. Wir haben allerdings keinen Zugriff auf die Unifi Geräte.

NFON


APC

Monitoring & Patchmanagement

Hosts (Agent)

Name	Typ	Anmerkung

Netzwerkgeräte (NMS)

Name	Typ	Anmerkung

Websites & Services

Name	Typ	Anmerkung

Regeln

Benachrichtigungen & Empfänger

In der folgenden Tabelle sind jene checks aufgelistet, die auch eine Aktion auslösen, im Normalfall Benachrichtigung per mail an die untenstehenden Empfänger.

HOST	CHECK-TYP	BEDINGUNG CHECK	AKTIONEN
Alle	Agent - File-System frei (beliebiger Datenträger) Prozent	Letze/r Wert ist < 5	Alarm
Alle	Agent - Speicher verfügbar in %	Durchschn. des letzten 3 Ergebnisse sind < 5 %	Warnung
Alle	Agent - CPU-Auslastung Leerlauf in % (gesamt)	Durchschn. des letzten 3 Ergebnisse sind < 10 %	Warnung

Empfänger

support@eitk.com	alle Alarme und Warnungen

Patch Management

Jedes Wochenende erfolgt eine automatisierte Suche und Installation von Windows Updates mit darauffolgenden Neustart des Servers.

Server	Updates	Reboot

Benutzeraccounts anlegen

Benutzeraccounts löschen

Technisch-organisatorische Maßnahmen (TOMs) zur Einhaltung der DSGVO

Kundenspezifisch anpassen!!

Zutrittskontrolle

Maßnahme, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet oder genutzt werden, zu verwehren.

- Eigener, versperrter Serverraum im Keller
- Zusätzlich versperrter EDV Schrank

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Zuordnung von Benutzerrechten
- Passwortvergabe
- Einsatz von VPN-Technologie
- Authentifikation mit Benutzername / Passwort
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Passwortrichtlinien inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung von Datenträgern
- Physische Löschung von Datenträger vor Wiederverwendung

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stelle eine Übermittlung personenbezogener Daten durch Einrichtung zu Datenübertragung vorgesehen ist

- Einrichtung von Standleitungen bzw. VPN-Tunneln

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen [inkl. Benutzergruppen)

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können.

- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlage
- Backup- & Recoverykonzepts
- Test von Datenwiederherstellungen

Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Berechtigungskonzept

Netzwerk

Netzwerk

Internetanschluss

	WAN1	WAN2
Provider/Name	A1	
Geschwindigkeit	~70Mbps	
Gateway/Mask	192.168.0.1/24	
Public IPs (verwendbar)		
DNS Server	9.9.9.9, 194.48.124.102	

IP Adressen Plan

Firewall

Routing laut Doku.

Layer 3

Policy	Protokoll	Source	Source Port(s)	Destination	Destination Port(s)	Anmerkung

Layer 7

#	Policy	Application	Detail

Internes Netzwerk

VLANs

VLAN	Name	Anmerkung

IP Adressen VLAN1

Adressbereich	192.168.0.0/24
Gateway	192.168.0.1
DHCP Server	192.168.0.1
DHCP Range	192.168.0.20-70
DNS Server	192.168.0.1
WINS Server	

IP	Name	Anmerkung
192.168.0.1	TP-Link Gateway	
192.168.0.72	Ecard Router	
192.168.0.140	Ecard Reader	
192.168.0.141	Ecard Reader	

VPN

Software

Software

Office Paket

AV & Security

Branchenspezifische Software (BMD, AutoCAD,...)

Hardware

Server

Server

Bezeichnung	CPU	RAM	HDD	Seriennummer	Garantie(ende)

Virtuelle Maschinen

Name	OS	Verwendung

Sonstige Hardware