GUARDING YOUR GATEWAYS: A HOLISTIC VIEW ON CYBERSECURITY

Workshop #3

FAKTEN

- **Workshop Zeiten:**
  - Mittwoch 05.06.2024
    08:00 - 12:00
  - Donnerstag 06.06.2024
    08:00 - 12:00
  - Freitag 07.06.2024
    08:00 - 12:00

- **Location:** Lakeside Science & Technology Park

WER BIN ICH

- Christian Gubesch - sehr gerne per du
- Ausbildung
  - HTL Villach Schwerpunkt: Netzwerk- und Medientechnik
  - Bachelor - Business Informatics
  - Master - Digital Entrepreneurship & Business Development
- Laufbahn
  - Cyber Security Professional - BearingPoint GmbH
    - Operations - Network and Cloud Security
    - Consulting - Cloud, Application, and OT Security
    - Business Development and Employee Training
  - Coach and Trainer for IT and CyberSec
    - TU Graz, FH Campus 02 & Fern FH Porsche
    - Freelance for Companies
    - Cyber Security Academy

WER SEID IHR

- Hintergrund
  - Job / Aufgabenbereiche
  - Erfahrungen im Bereich der IT-Security?
    (Privat als auch Unternehmen)
  - Erfahrungen im IT-Operations Bereich oder anderen IT bezogenen Tätigkeiten?
- Vorstellungen & Erwartungen
- Nach diesem Workshop will ich in der Lage sein, …

WORKSHOP ÜBERBLICK – FACTS

Mir ist es wichtig das wir über aktuelle Themen sprechen und einen guten Überblick über die wichtigsten Sachen bekommen!

Ich habe auch daher vier Focus Areas mitgebracht:

FA01: Erweiterte Security Techniken und Tools für Unternehmen

FA02: Security Architekturen für Unternehmens-ressourcen (KMU)

FA03: Cloud and Application Security Strategien

FA04: Compliance - Ganzheitliche Cybersecurity anhand von Cyber Trust Austria

Solltet ihr zu irgendeinem Thema Fragen haben: Bitte jederzeit Fragen!

Erweiterte Security Techniken und Tools für Unternehmen

Ein Überblick der gängigsten Methoden und ihre Anwendung.

Lernpfad

FA01: Erweiterte Security Techniken und Tools für Unternehmen

FA02: Security Architekturen für Unternehmens-ressourcen (KMU)

FA03: Cloud and Application Security Strategien

FA04: Compliance - Ganzheitliche Cybersecurity anhand von Cyber Trust Austria

Wie schaut es aus?

Welche “advanced” Techniken und Tools im Cybersecurity Bereich kennt ihr?

Lernziele

1. Verständnis für die Nutzung von Pentests.
2. Aufbau und Zweck von XDR und MDR kennen.
3. Mission, Aufbau, Funktionen und Rollen eines Security Operations Centers verstehen.
4. Verstehen wann Cyber-Versicherungen sinnvoll eingesetzt werden können.

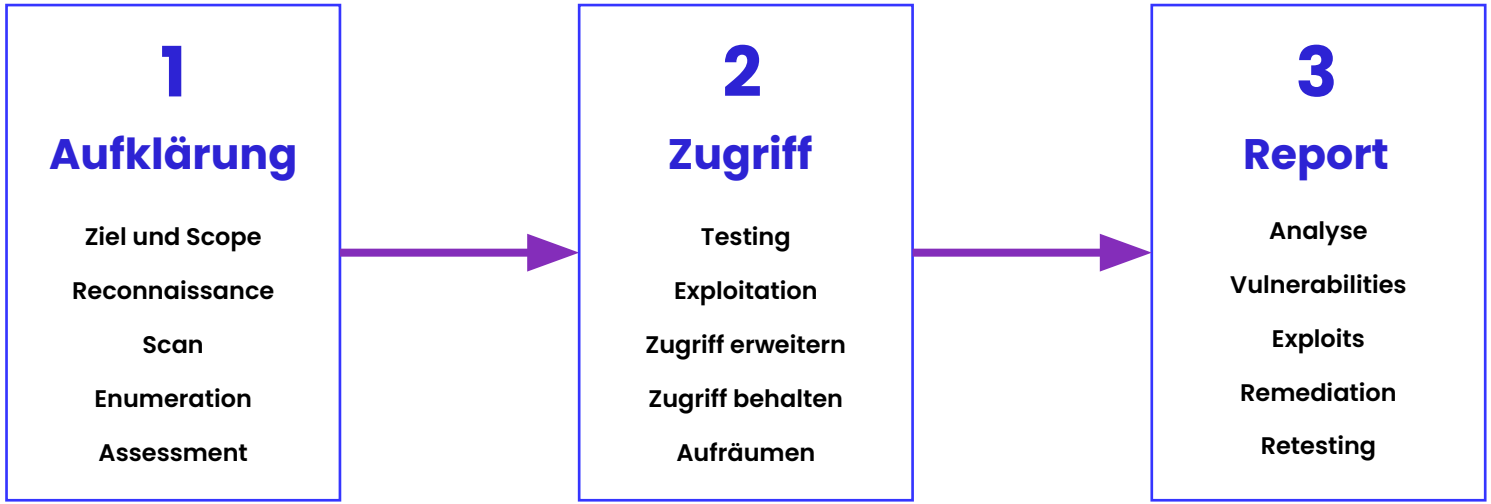
Pentests

Was ist ein Pentest?

Habt ihr sowas schon mal für euer Unternehmen gemacht?

Pentest – grober Überblick

In der Regel funktioniert ein Pentest folgendermaßen:



Quelle: https://cybercx.com.au/resource/penetration-testing-guide/

Pentest – grober Überblick

Was wird typischer Weise alles getestet:

Netzwerk

Physische Sicherheit

Anwendungen

Quelle: https://www.stationx.net/penetration-testing-steps/

Pentest – grober Überblick

Was man beachten sollte:

Momentaufnahme

Quelle: https://www.link11.com/de/glossar/pentest/

Pentest – grober Überblick

Was man beachten sollte:

Pannen

Quelle: https://www.link11.com/de/glossar/pentest/

Pentest – grober Überblick

Was man beachten sollte:

Betrüger

Quelle: https://www.link11.com/de/glossar/pentest/

Pentest – grober Überblick

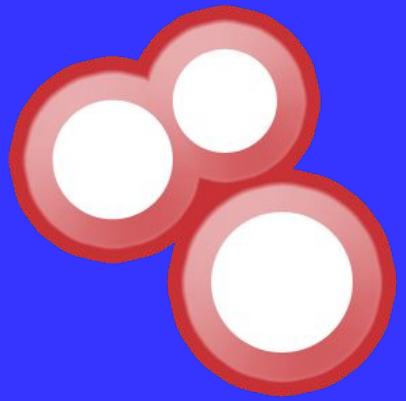
Was man beachten sollte:

Rechtliches

Quelle: https://www.link11.com/de/glossar/pentest/

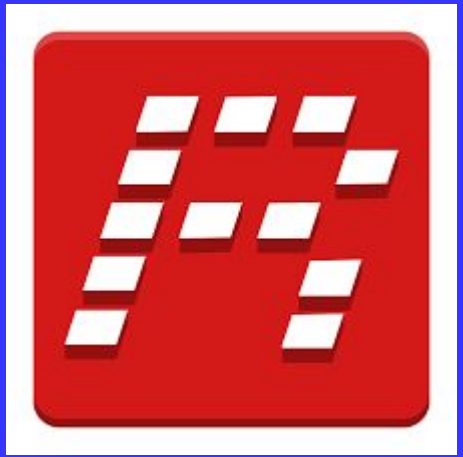
Live Demo

Online Scanner



Live Demo

PDFs Crawlen



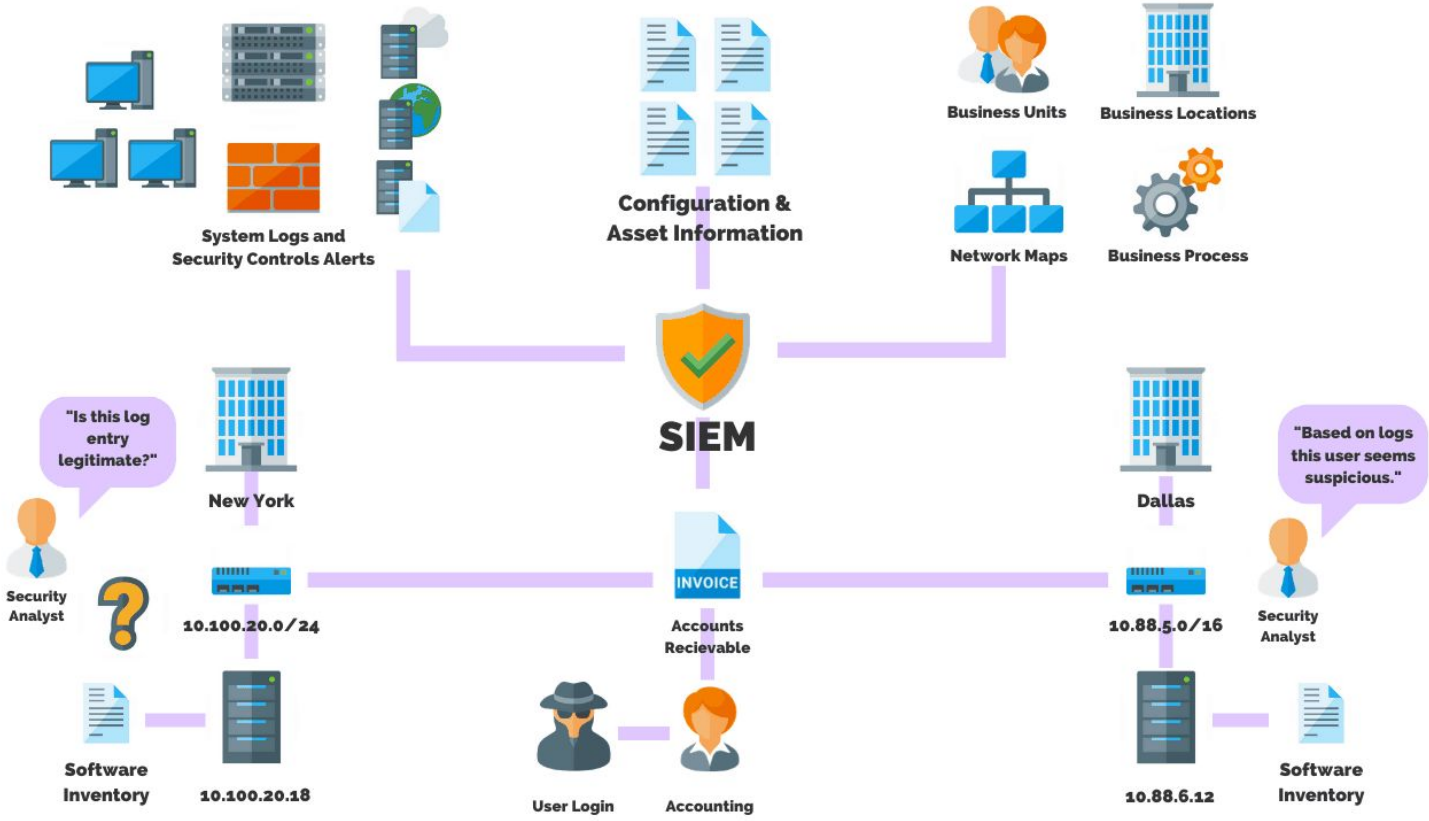
Security information and event management (SIEM)

Was stellt ihr euch darunter vor?

Habt ihr soetwas im Einsatz oder gibt es Berührungspunkte? Was ist die Grundvoraussetzung?

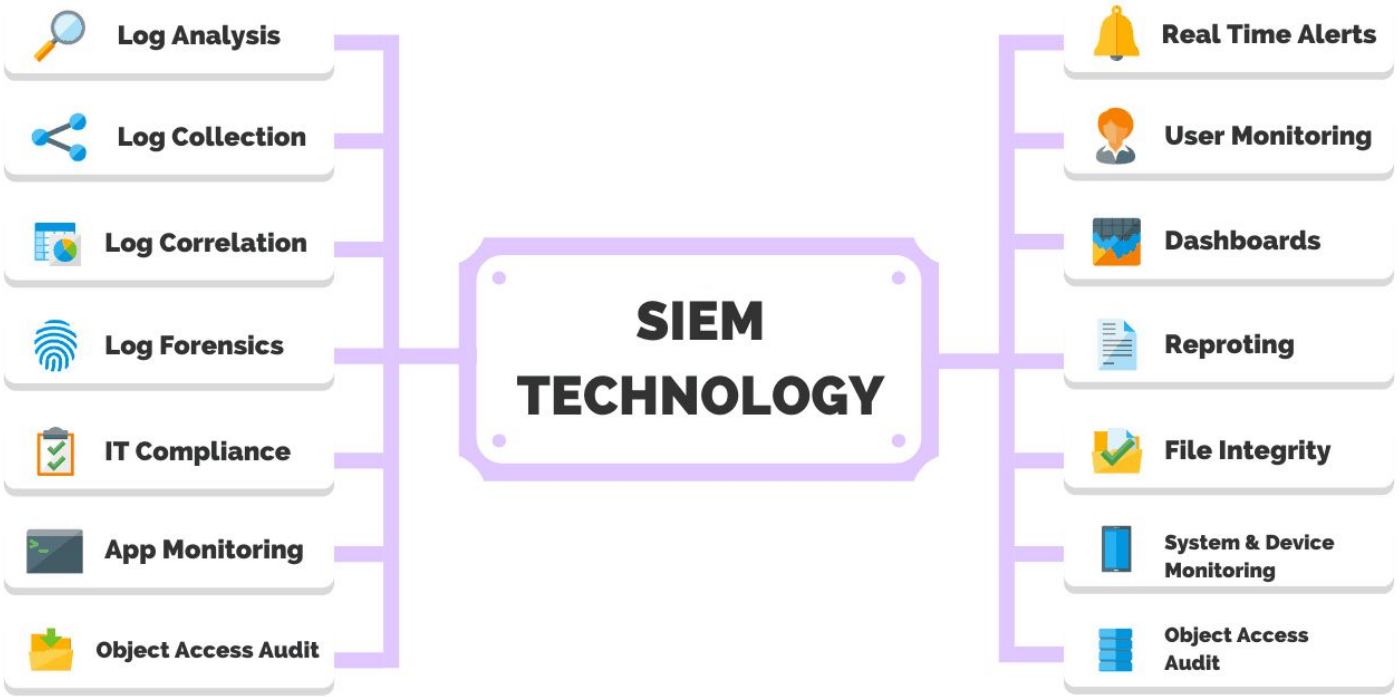
Thema: Monitoring

SIEM Logs zentral Sammeln



Quelle: https://purplesec.us/

SIEM Funktionsweise



Quelle: https://purplesec.us/

Extended Detection and Response

Habt ihr schon mal von XDR gehört?

oder EDR, managed XDR?

Begriffsüberblick

einordnung unterschiedlicher Lösungen aus dem Bereich

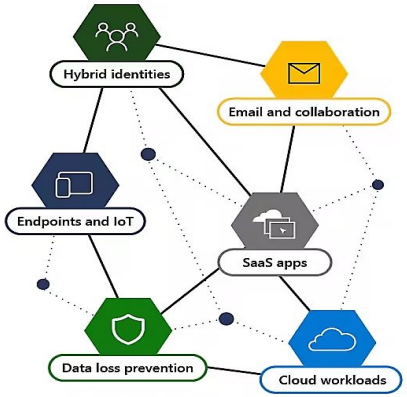
Managed

Quelle: @Andrew Quinn / Pro TEC Show / EDR, MDR & XDR explained

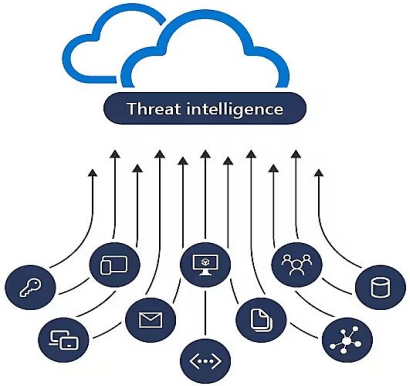
XDR - Einführung

Aus welchen Komponenten besteht XDR?

Extended



Detection



Response

Quelle: https://www.microsoft.com/de-at/security/business/solutions/extended-detection-response-xdr

XDR - Typische Funktionen

klassische Funktionen einer XDR Lösung

Vorfallbasierte Untersuchung

Sichtbarkeit der Cyberangriffskette

Automatische Wiederherstellung von Ressourcen

Automatische Unterbrechung erweiterter Cyberangriffe

Quelle: https://www.microsoft.com/de-at/security/business/security-101/what-is-xdr

XDR - Typische Anwendungsfälle

häufige Use Cases für eine XDR Lösung

Suche nach Cyberbedrohungen

Untersuchung von Sicherheitsvorfällen

E-Mail-Phishing und Schadsoftware

Endpunktgeräteüberwachung

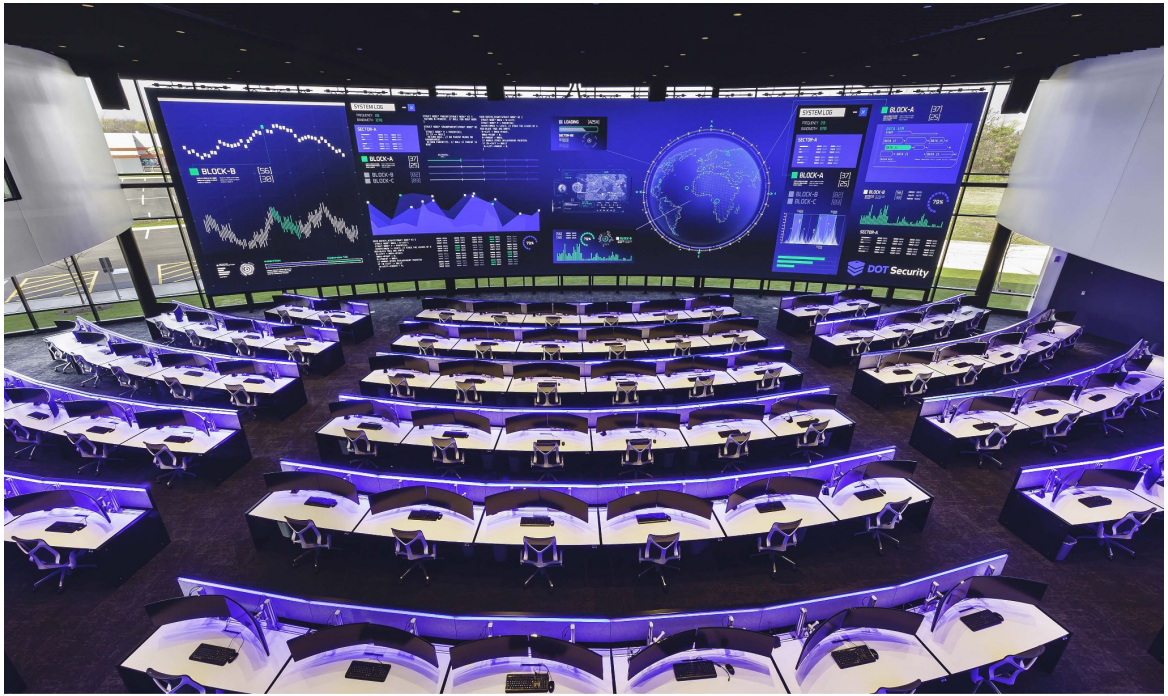
Insiderbedrohungen

Quelle: https://www.microsoft.com/de-at/security/business/security-101/what-is-xdr

Security Operations Center

SOC - kleine Demo

einer High End Variante für große Enterprises



Quelle: https://dotsecurity.com/insights/blog-why-a-security-operations-center-is-important

DOT Security
Tour DOT Security's Physical Location:
The Security Operations Center

Detection and Response

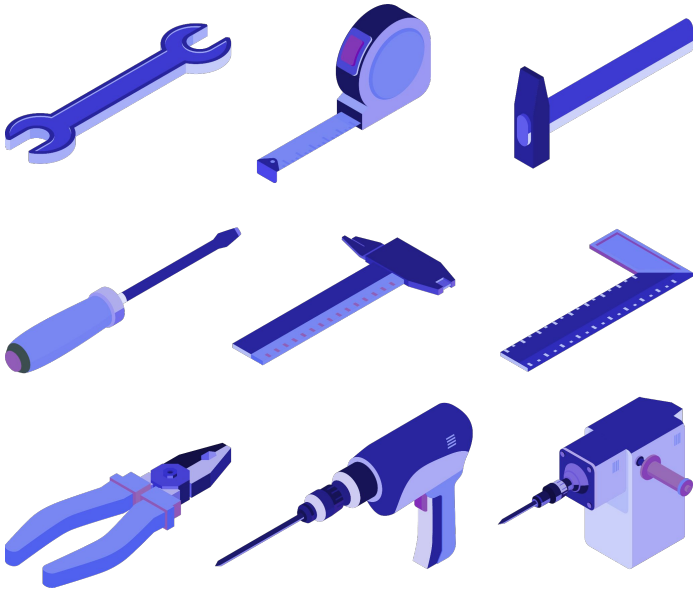
Quelle: https://www.ibm.com/de-de/topics/security-operations-center

SOC - Rollen

Manager
Ingenieur
Analyst
Threat Hunter

Quelle: https://www.ibm.com/de-de/topics/security-operations-center

SOC - Tools



Denial of Service
Angriff
Data Exfiltration
Malware-Infektion

Quelle: https://www.ibm.com/de-de/topics/security-operations-center

Cyber Versicherungen

Habt ihr eine Cyberversicherung?

Workout

Cyberversicherungen

- **Ziel:** optimale Cyberversicherung für Use Case finden
- **Output:** knappes Handout mit wichtigsten Fakten
- **Modus:** Ausarbeitung in Gruppen (15 min), anschließend Präsentation (5 min pro Gruppe)

Workout - Actionplan

1. Risikoanalyse:
   a. Identifiziert die größten Cyberbedrohungen für das Unternehmen.
   b. Welche Folgen hätten erfolgreiche Cyberangriffe (z.B. Datenverlust, Geschäftsausfall, Reputationsschaden)?
2. Versicherungsbedarf ermitteln:
   a. Welche Deckungen wären für dieses Unternehmen besonders wichtig (z.B. Haftpflicht, Datenwiederherstellung, Cyber-Erpressung)?
   b. Wie hoch sollten die Deckungssummen sein?
3. Vergleich von Angeboten:
   a. Recherchiert zwei verschiedene Cyberversicherungsangebote.
   b. Vergleicht diese hinsichtlich Deckung, Kosten, Selbstbeteiligung und zusätzlichen Leistungen.
4. Empfehlung:
   a. Welche Versicherung würdet Ihr empfehlen und warum?
   b. Präsentieren Eure Entscheidung vor der anderen Gruppe.

Zeitrahmen:

15 min Ausarbeitung und

5 min Präsentation

Gruppengröße:

3-4 Personen

Use Case A - IT Dienstleister Cloudify

Unternehmensprofil:

- **Branche:** IT-Dienstleistungen
- **Mitarbeiterzahl:** 50
- **Kunden:** Kleine bis mittlere Unternehmen
- **IT-Infrastruktur:** Eigene Server, Cloud-Dienste, Remote-Arbeitsplätze
- **Sicherheitsbedenken:** Datenlecks, Ransomware, Phishing-Angriffe

Kurzbeschreibung:

Cloudify bietet eine Vielzahl von Services, darunter Netzwerkmanagement, Cloud-Migration und IT-Support. Die Mitarbeiter arbeiten sowohl vor Ort als auch remote und nutzen eine Kombination aus eigenen Servern und Cloud-Diensten zur Datenverarbeitung und -speicherung.

Use Case B - Einzelhändler RetailHub

Unternehmensprofil:

- **Branche:** Einzelhandel
- **Mitarbeiterzahl:** 30
- **Kunden:** Endverbraucher, sowohl im Ladenlokal als auch online
- **IT-Infrastruktur:** POS-Systeme, E-Commerce-Plattform, Kundendatenbank
- **Sicherheitsbedenken:** Kreditkartenbetrug, Datenverlust, DDoS-Angriffe

Kurzbeschreibung:

Retailhub betreibt ein Ladenlokal sowie einen florierenden Online-Shop. Das Unternehmen nutzt POS-Systeme für den Verkauf vor Ort und eine E-Commerce-Plattform für Online-Transaktionen. Die Kundendaten werden in einer zentralen Datenbank verwaltet.

Wrap Up

Was nehmen wir uns mit?

Pentests zeigen Verbesserungsbedarf in der Security Strategie auf - sind jedoch nur eine Momentaufnahme!

XDR ist eine kostengünstige Alternative zu einem teuren SOC als Upgrade im Vergleich zu einer klassischen EDR Lösung.

Cyberversicherungen können bei passenden Anwendungsfall das Sicherheits Portfolio gut ergänzen.

Cloud and Application Security Strategies

Ein kurzer Einblick ins Thema Cloud Computing: Begriffe, Absicherung und Konzepte

Lernpfad

FA01: Erweiterte Security Techniken und Tools für Unternehmen

FA02: Security Architekturen für Unternehmens-ressourcen (KMU)

FA03: Cloud and Application Security Strategien

FA04: Compliance - Ganzheitliche Cybersecurity anhand von Cyber Trust Austria

Lernziele

1. Cloud Computing Grundlagen näher verstehen
2. Unterschiedliche Deployment/Service Modelle verstehen und die Security Aspekte dieser verstehen
3. Shared Responsibility Model in Kombination mit Security best Practices verstehen
4. Absichern der Cloud Control Plane
5. Cloud Migration Szenarien näher kennenlernen und Anwendungsfälle erkennen
6. Klassische Security Architekturen in der Public Cloud

Cloud Computing Definition und erweiterte Grundlagen

Wie würdet ihr Cloud Computing definieren?

Bzw. was könnt ihr euch darunter vorstellen?

Definition of Cloud Computing

According to the National Institute for Standards and Technology (NIST) there are:

5

ESSENTIAL CHARACTERISTICS

On-demand self-service

Broad network access

Resource pooling

Rapid elasticity

Measured service

4

DEPLOYMENT MODELS

Private Cloud

Community Cloud

Public Cloud

Hybrid Cloud

(Multi Cloud)

3

SERVICE MODELS

Software as a Service

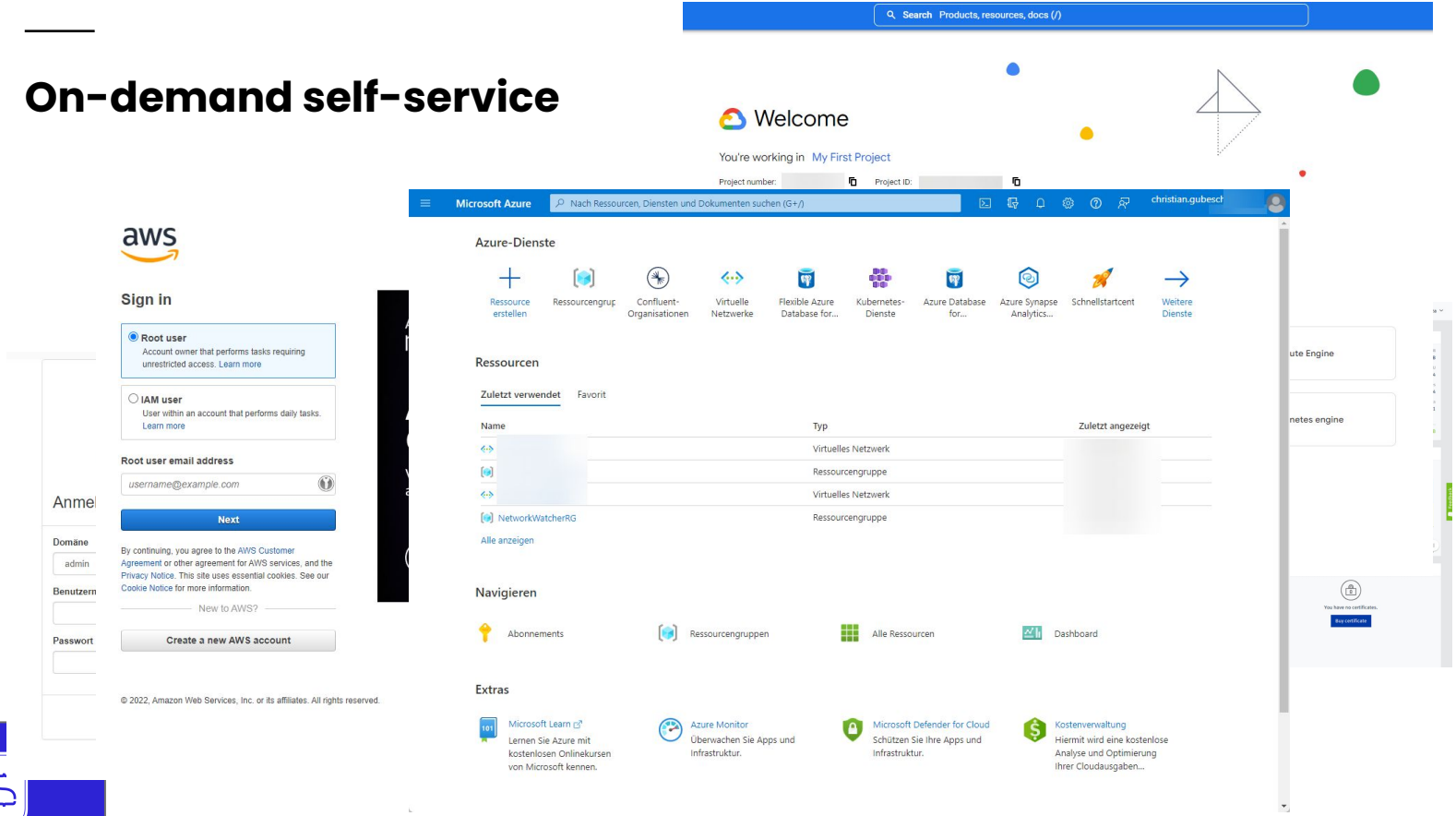
Platform as a Service

Infrastructure as a Service

(Everything as a Service)

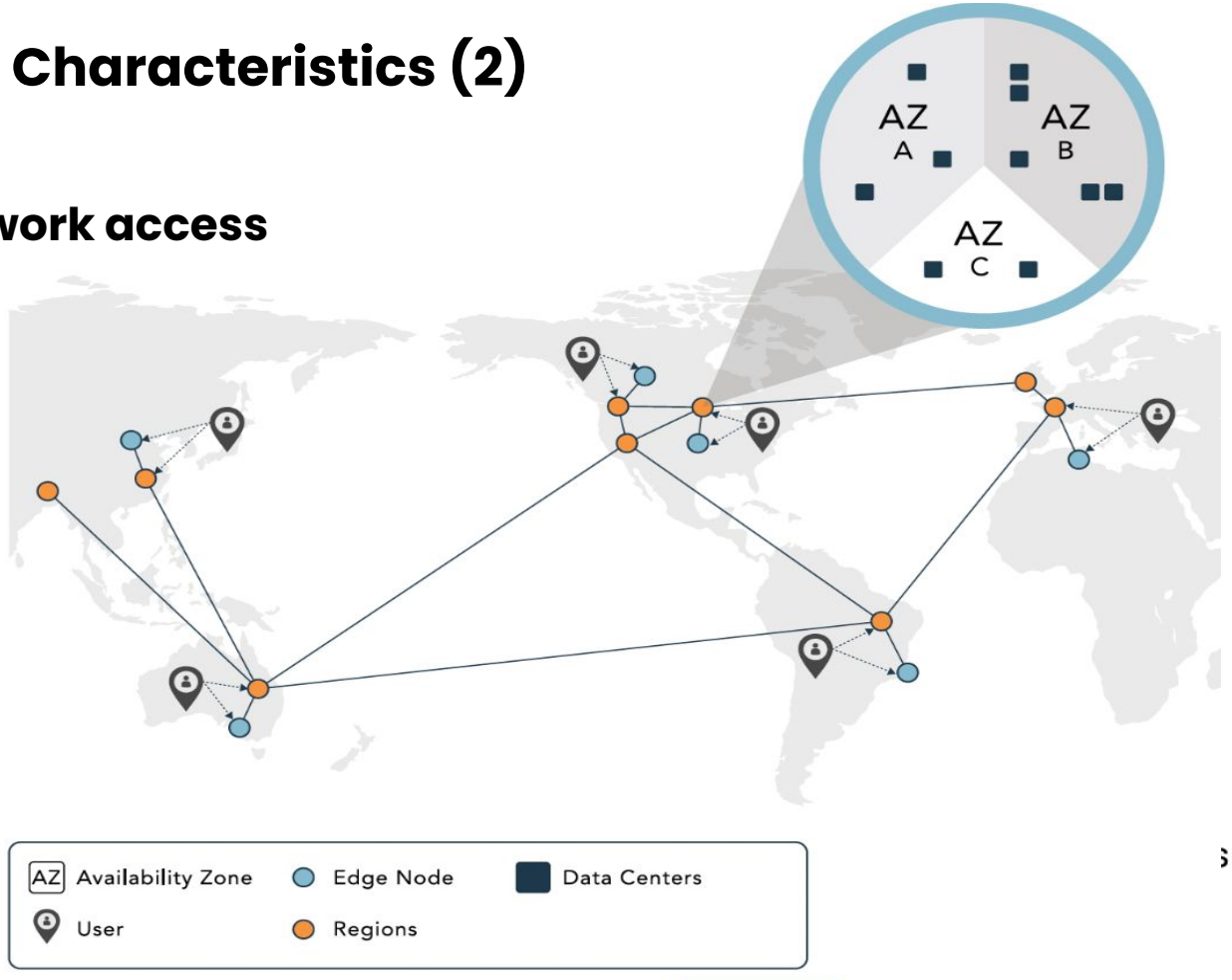
Essential Characteristics (1)

On-demand self-service



Essential Characteristics (2)

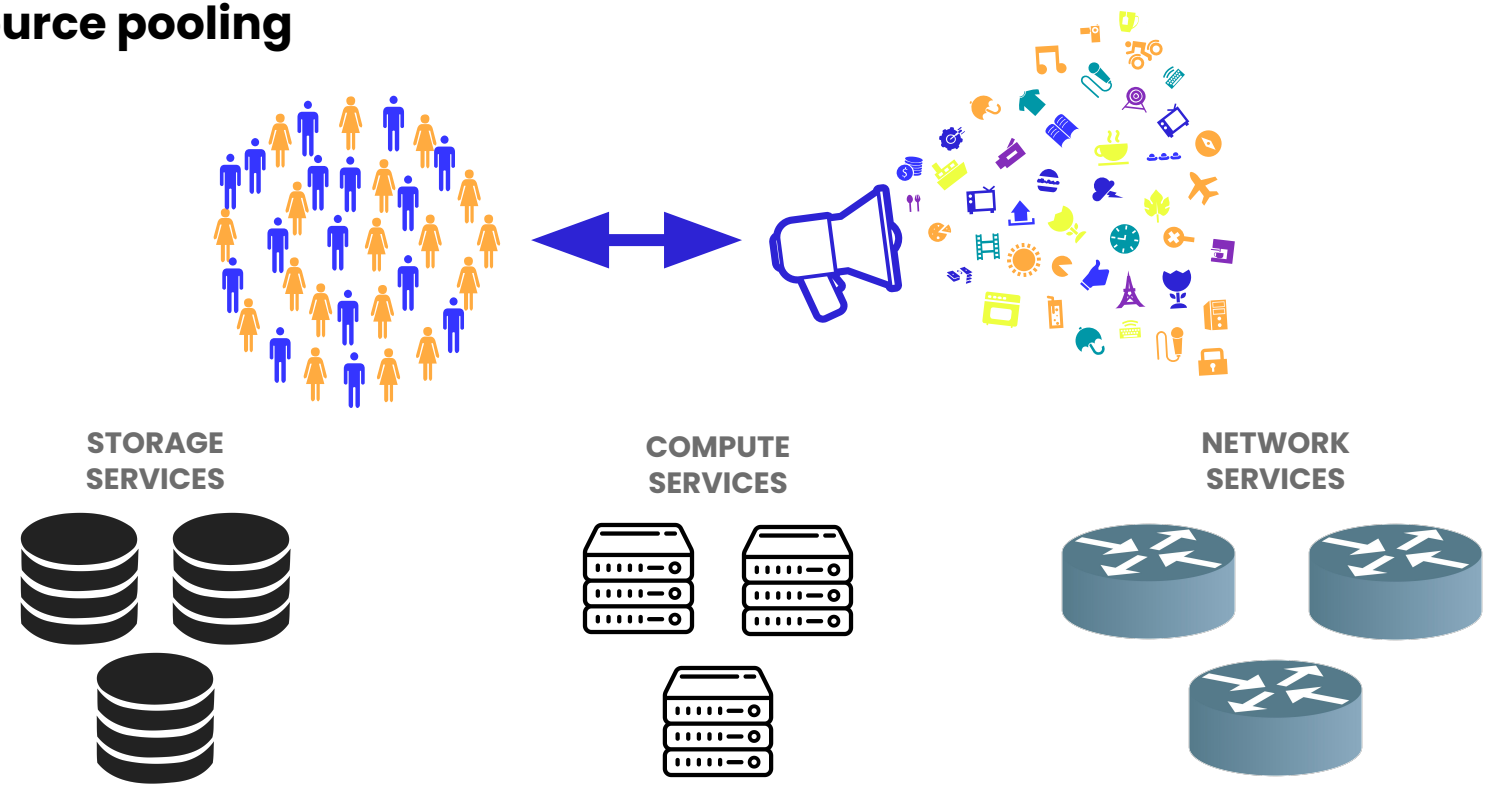
Broad network access



https://www.spiceworks.com/tech/cloud/articles/what-is-broad-network-access/

Essential Characteristics (3)

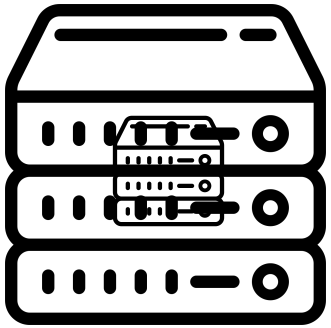
Resource pooling



Essential Characteristics (4)

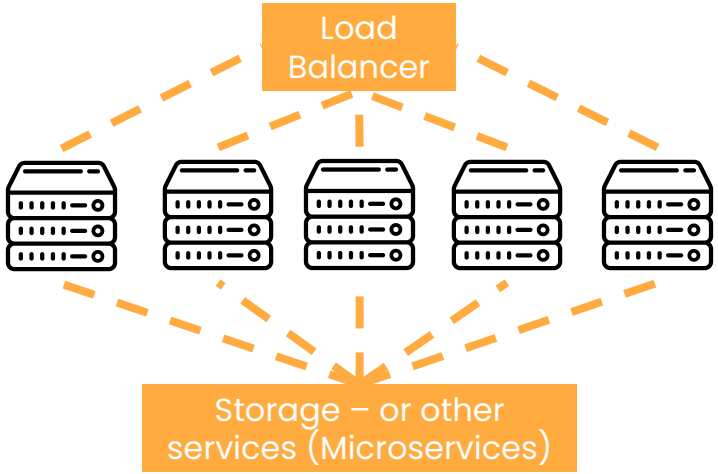
Rapid elasticity

VERTICAL SCALABILITY



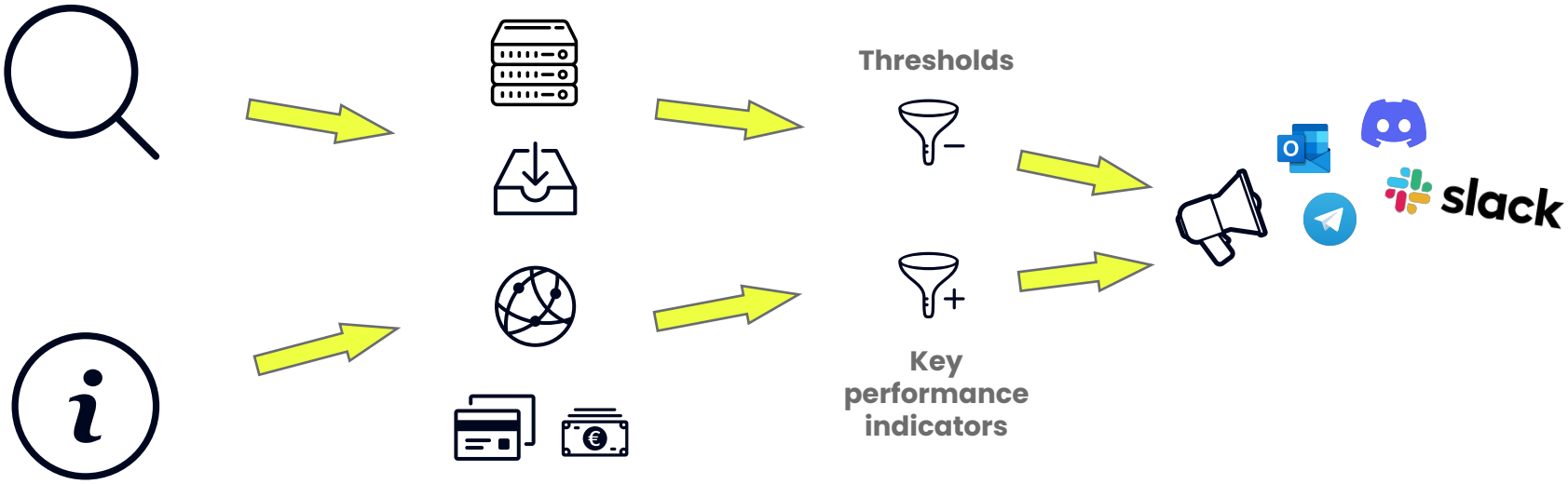
10 x more compute
10 x more storage
Of a single VM

HORIZONTAL SCALABILITY



Essential Characteristics (5)

Measured service

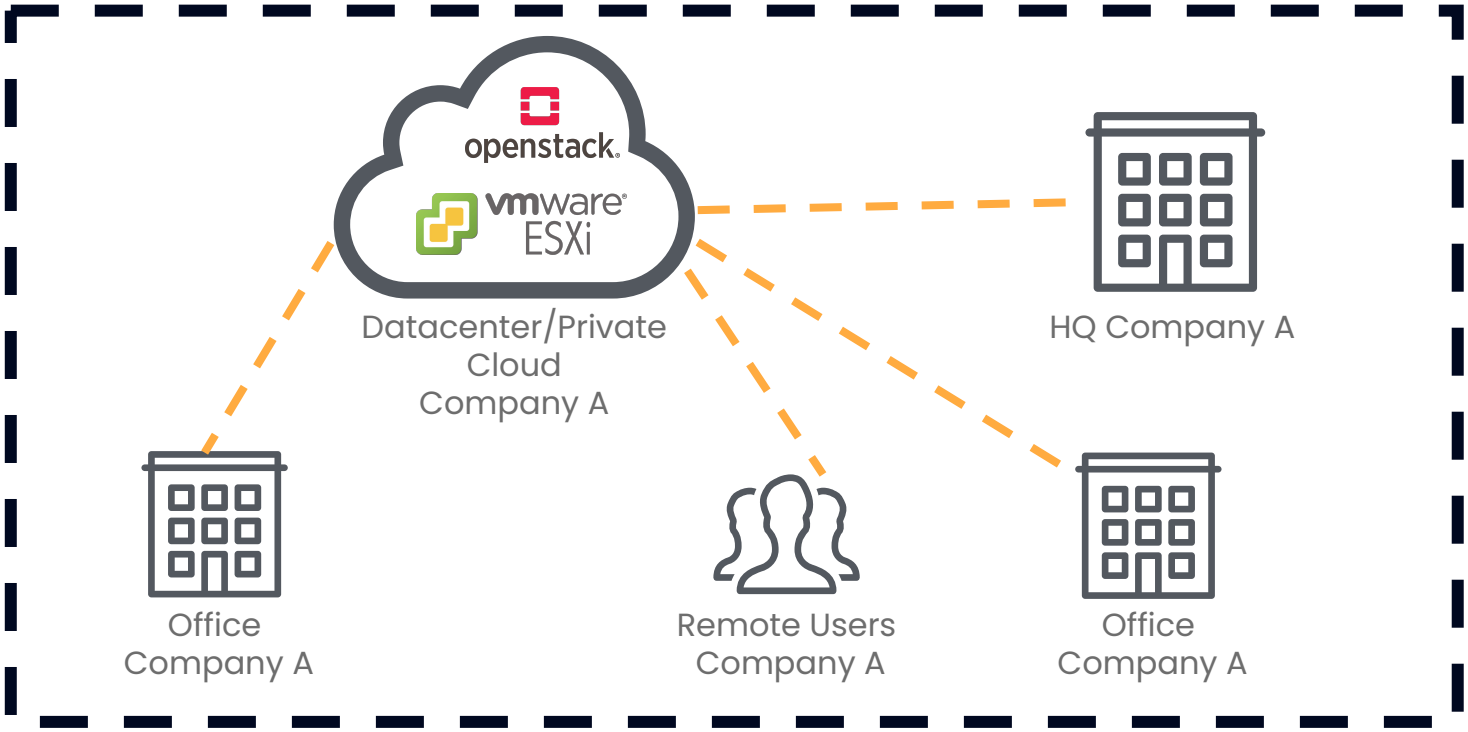


Habt ihr jetzt “Cloud Computing” wirklich im EInsatz?

Anhand der erwähnten Charaktereigenschaften

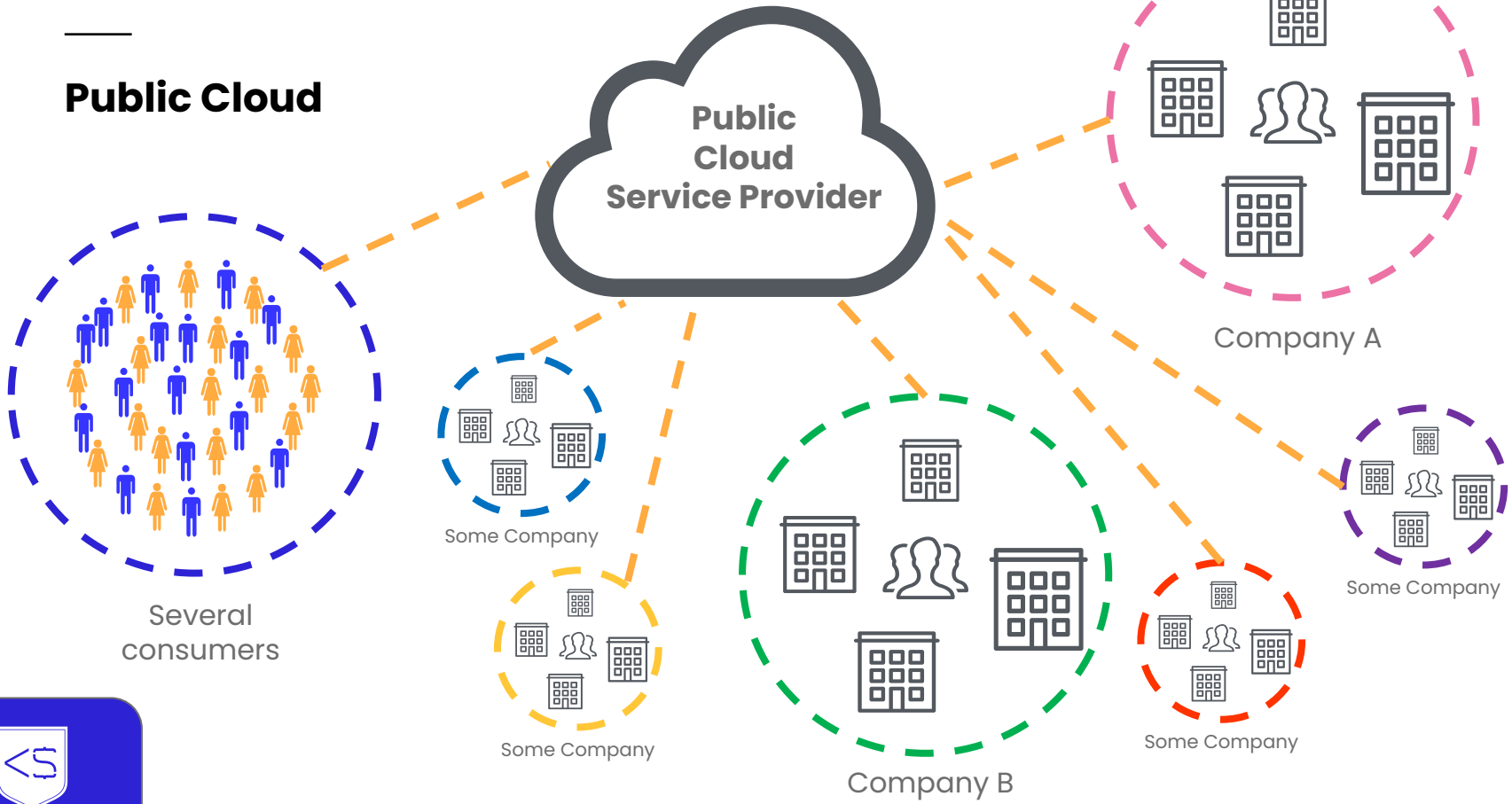
Deployment Models(1)

Private Cloud



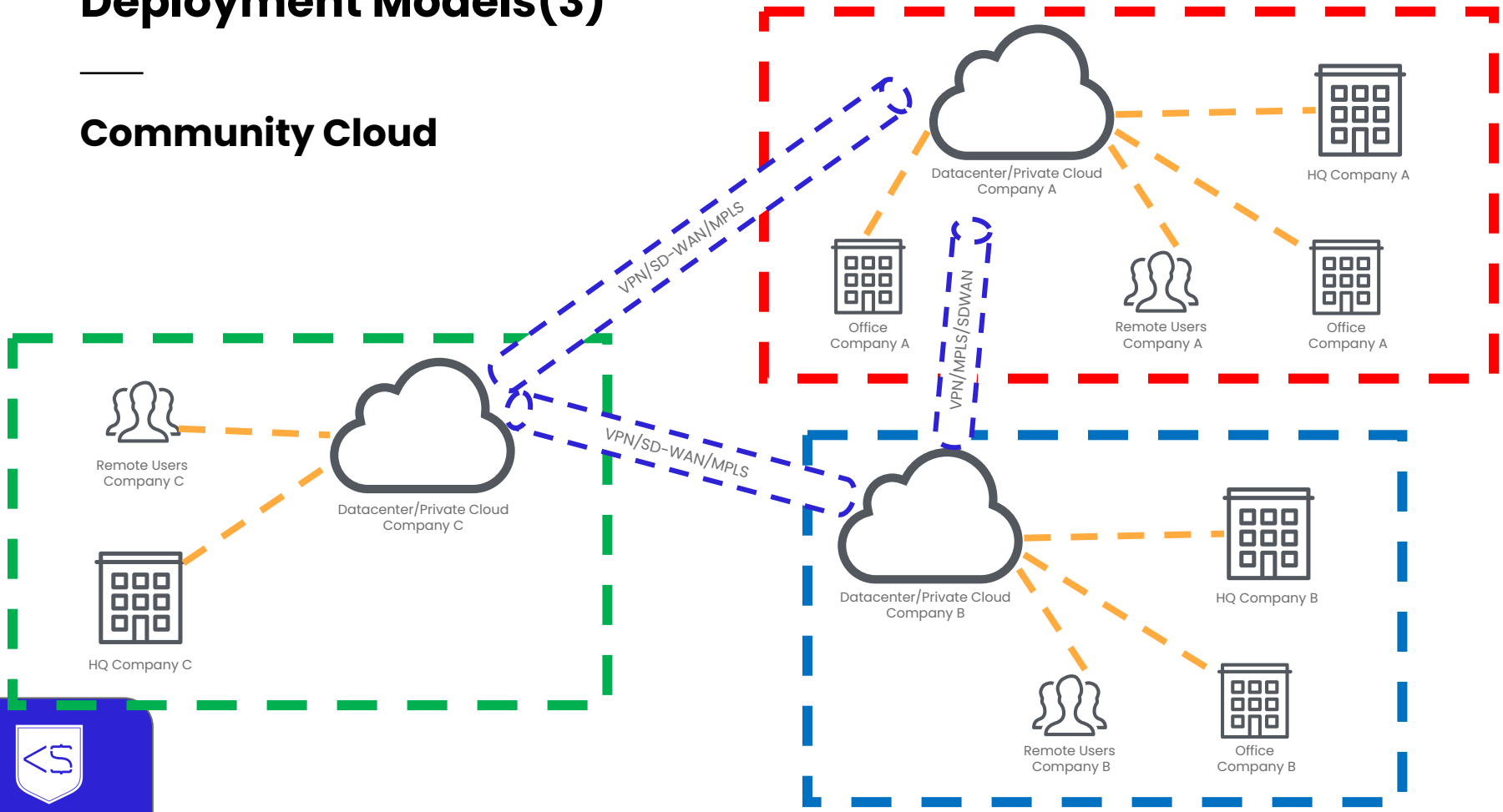
Deployment Models(2)

Public Cloud



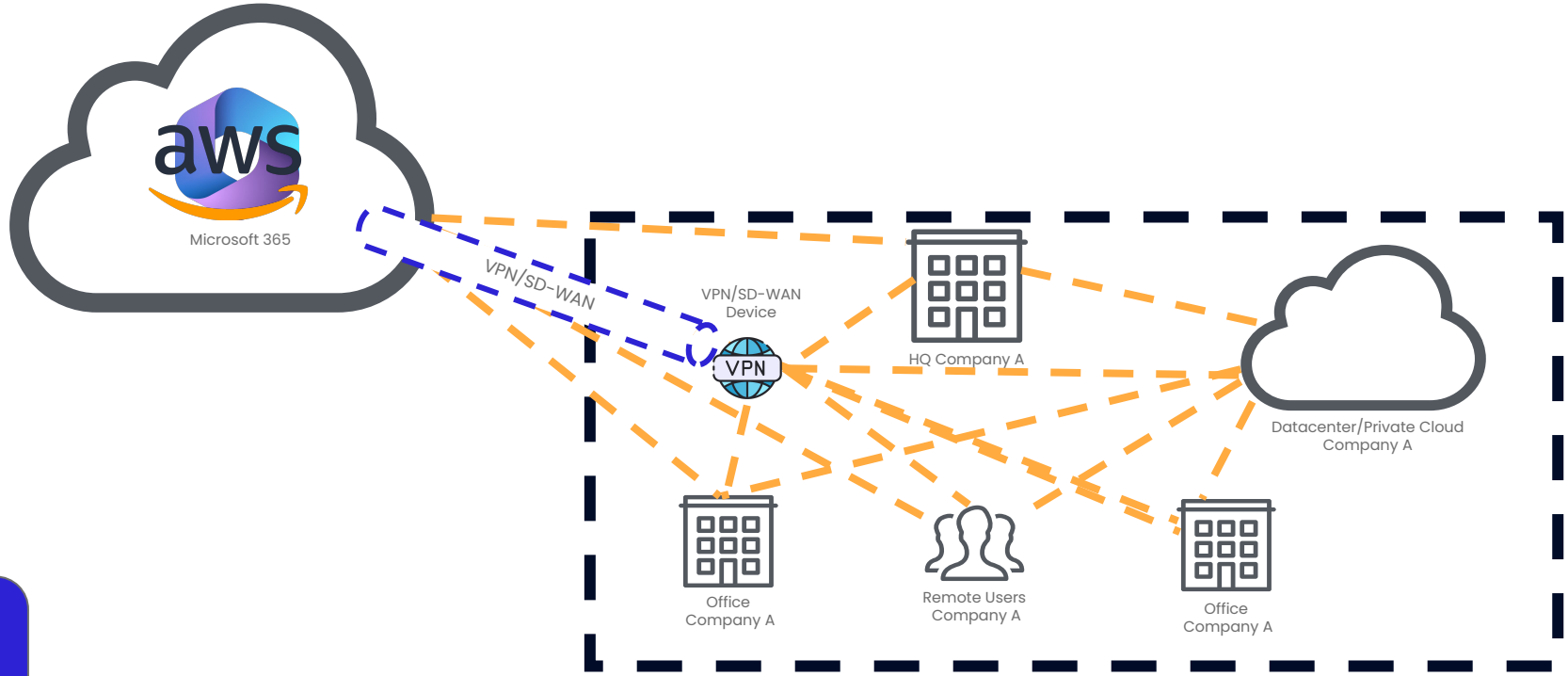
Deployment Models(3)

Community Cloud



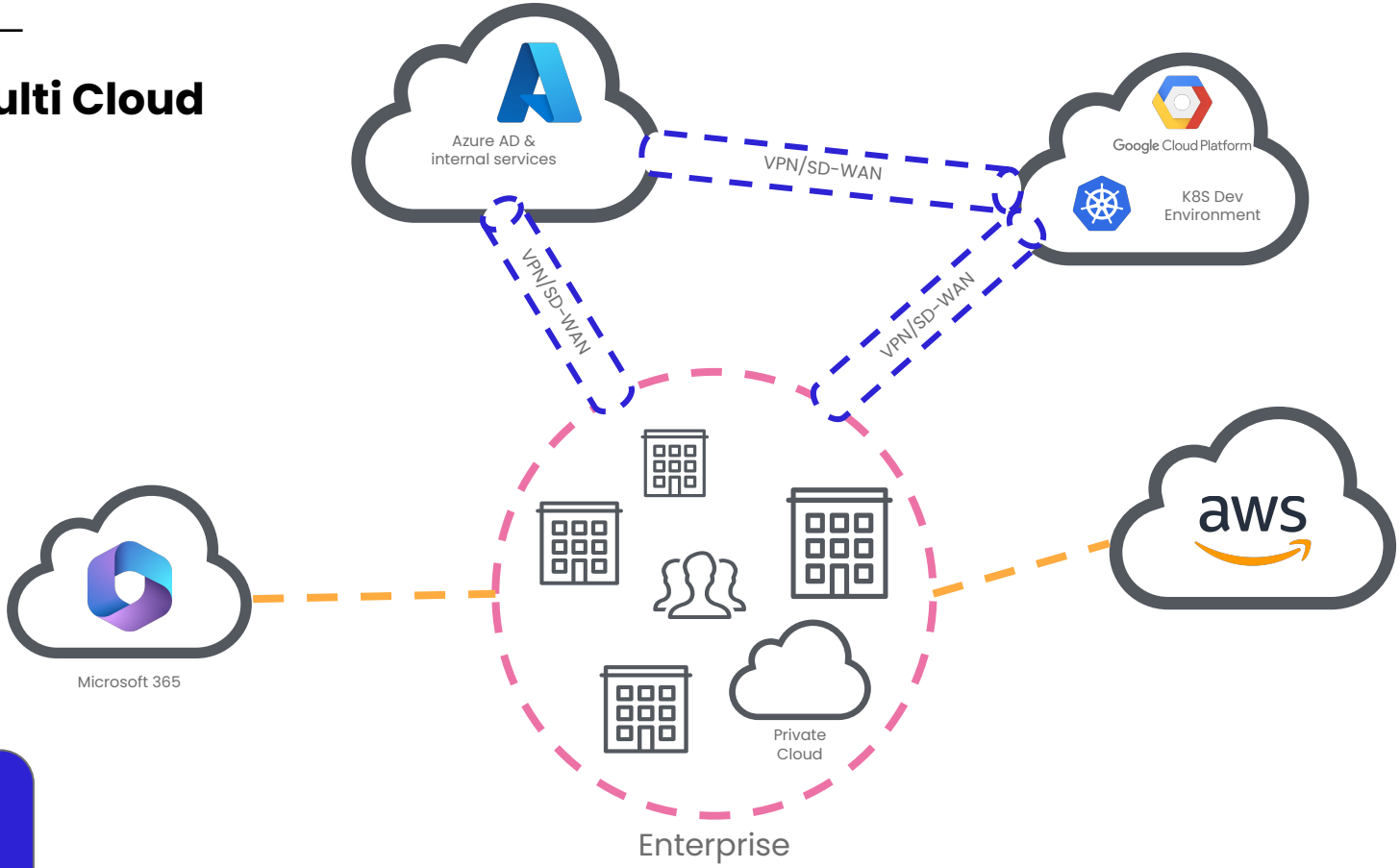
Deployment Models(4)

Hybrid Cloud



Deployment Models(5)

Multi Cloud



Welches Deployment Model habt ihr im Einsatz?

Oder habt ihr das eigentlich laut definitionen gar nicht im Einsatz?

Service Models(1)

Infrastructure-as-a-Service

IaaS

Actors:

- **Infrastructure/Network Architects**
- **Cloud Engineers**
- **DevOps Engineers**

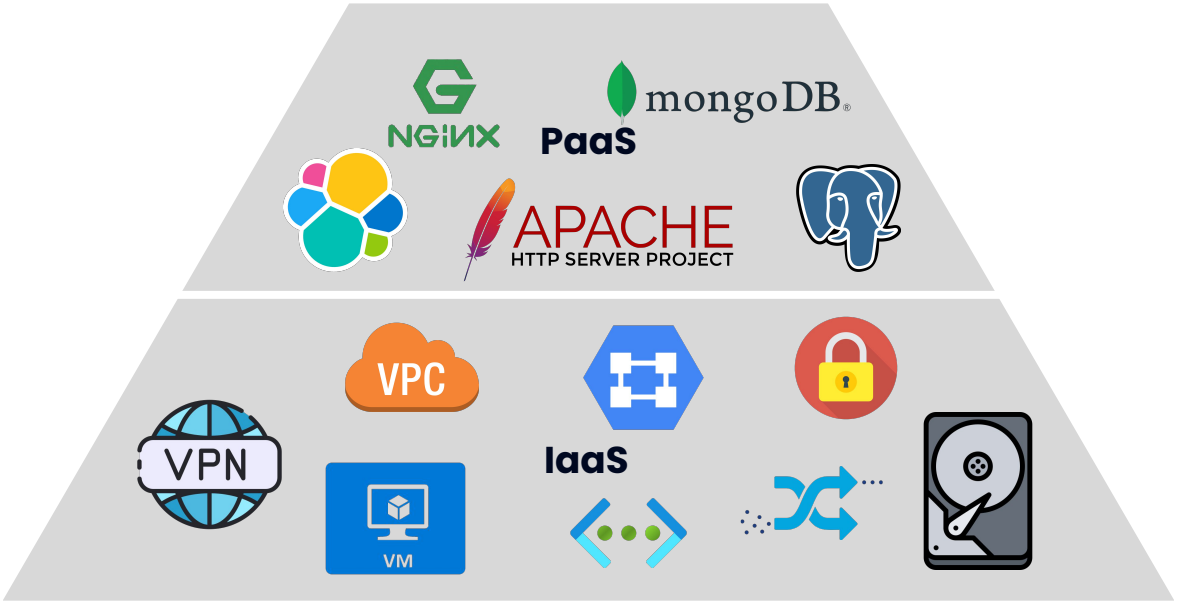
Service Models(2)

Platform-as-a-Service

PaaS

Actors:

- **Software Engineers**
- **Cloud Engineers**
- **DevOps Engineers**



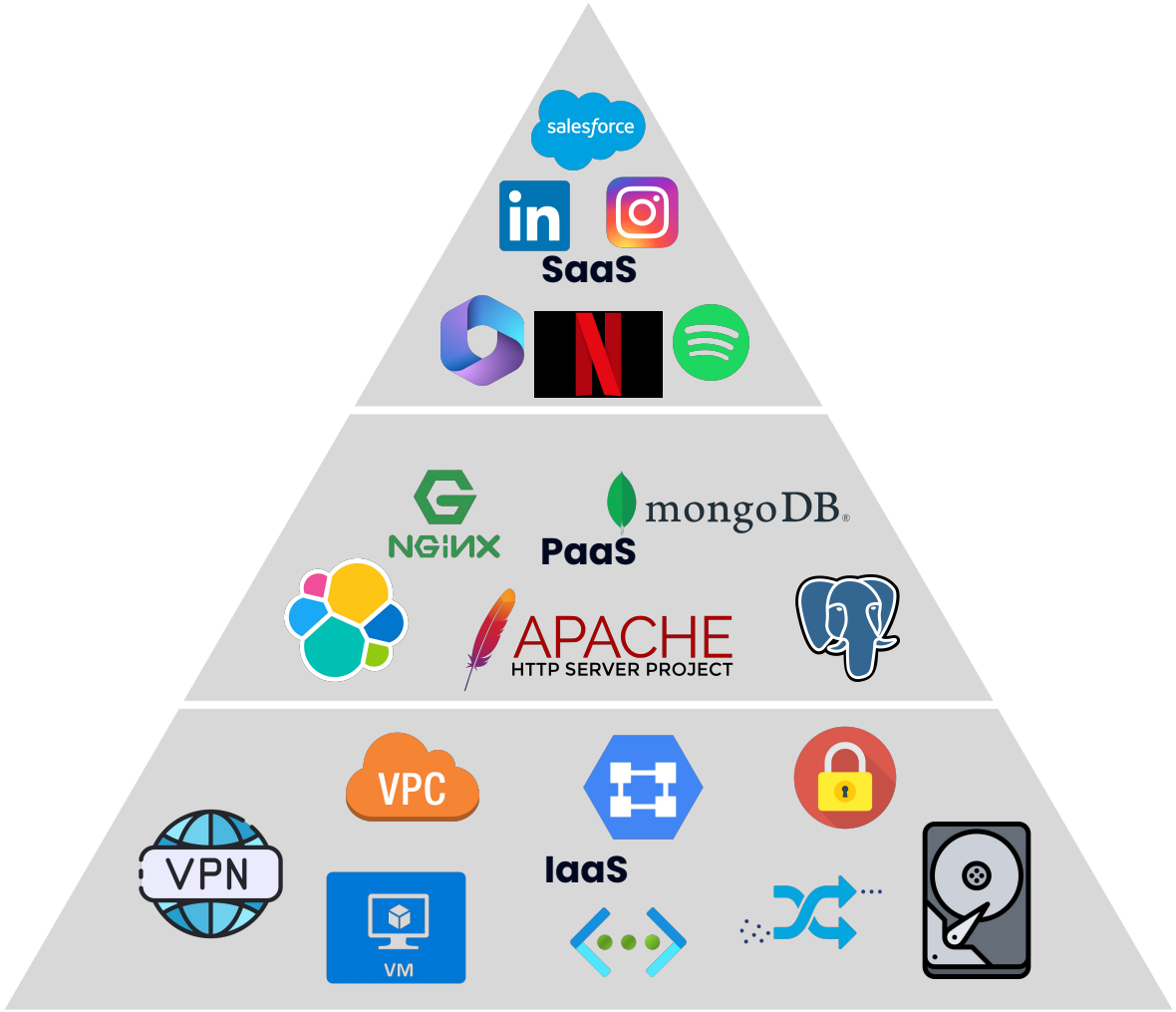
Service Models(3)

Software-as-a-Service

SaaS

Actors:

- **Users**
- **Businesses**



Additional Service Models

OpenAI

Artificial Intelligence-as-a-Service

```
function add(num1, num2) {
    // code
    return result;
}

let x = add(a, b);
// code
```

function call

Function-as-a-Service

Container-as-a-Service

Desktop-as-a-Service

Was habt ihr an Cloud Ressourcen im Einsatz?

SaaS, PaaS, IaaS, usw. und wo ist das alles deployed?

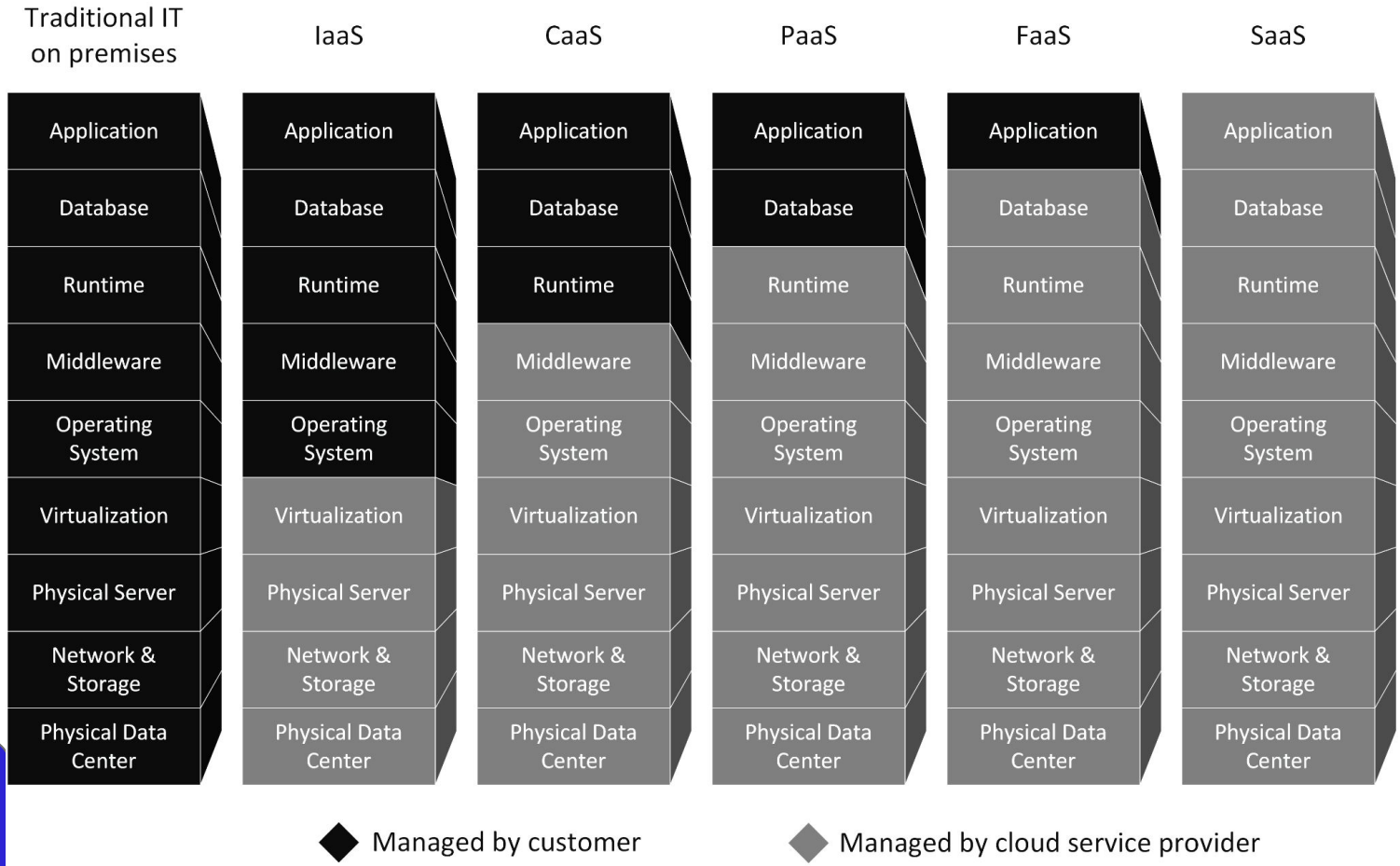
Welche Sicherheitsvorkehrungen sind aktiv?

Workout

- **Ziel:** Asset Management aller Cloud Computing Ressourcen (inkl. Stakeholder, Kosten und Security Maßnahmen)
- **Output:** Auflistung und Verantwortlichkeiten
- **Modus:** Einzel Ausarbeitung und Auflistung (15-20min anschließende Diskussion)

Cloud Computing Architektur und Security Gedanken

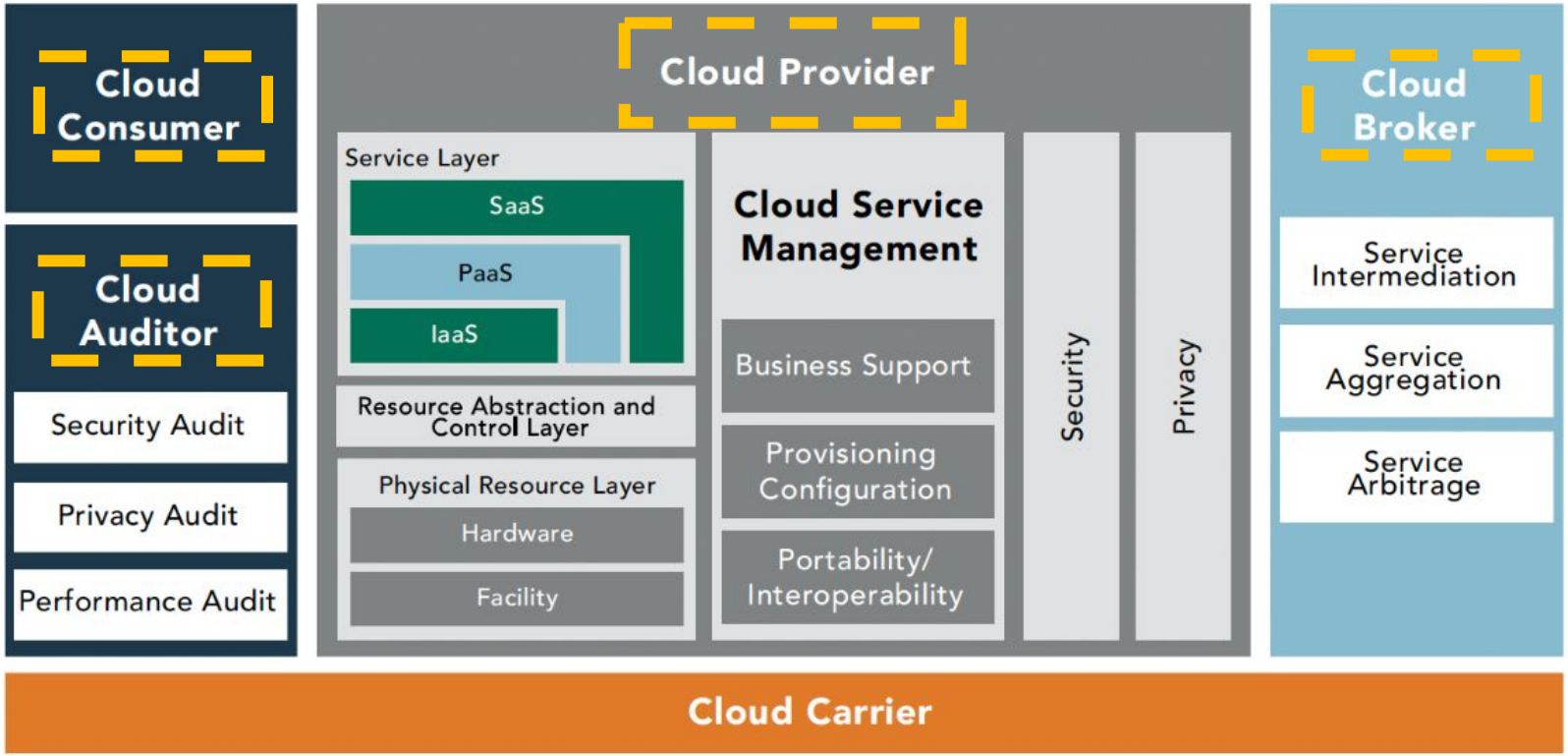
Generic Shared (Security) Responsibilities



Actors

NIST Cloud Computing Reference Architecture – NIST Reference Model

https://www.nist.gov/publications/nist-cloud-computing-reference-architecture



Cloud Service Providers

https://cloudsecurityalliance.org/star/

Basic Terms (1) - Networking

Networking

Generic Term	Definition	Azure	aws	GCP
Virtual Private Cloud (VPC) / Network	A logically isolated section of the cloud where you can launch resources	Virtual Network (VNet)	Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC)
Region	Worldwide locations where resources are hosted, consist of at least 2 Azs	Region	Region	Region
Availability Zone	Clusters of DataCenters, Distinct locations (within regions) where resources are housed - designed to be isolated from failiures in other AZ's	Availability Zone	Availability Zone	Availability Zone
Subnet	Logical subdivision of an IP network. Can be private or public, Divide a Network into multiple segments	Subnet	Subnet	Subnet
Content Delivery Network	global network that delivers content based in the geographic locations of the user	Azure CDN	CloudFront	Cloud CDN and/or CDN interconnect
VPN Gateway	Private connection to VPCs	Azure VPN Gateway	Virtual Private Gateway	Cloud VPN
Network Peering	A networking connection between two VPCs that enables the routing traffic between them using private IP addresses	Virtual Network Peering	VPC Peering Connections	VPC Network Peering
Auto-scaling	Scales resources (of a group) up or down basedon usage and rules	VM scale sets	Auto-scaling group	Compute engine autoscaler
Load Balancing	Pushes traffic (in a balanced way) across multiple targets in multiple AZs	Load Balancer, Application Gateway	ELB	Cloud Load Balancing

Basic Terms (2) – Security and Compute

	Generic Term	Definition	Azure	aws	GCP
Security	**Security Group**	Contains a list of security rules that allow or deny network traffic to resources	Network Security Group	Security Group	Compute Engine Firewall Rules
	Identity Access Management (IAM)	Manage access to cloud services and resources securely	Azure Role-based ACL (RBAC) and/or Azure AD	Identity access Management (IAM)	Cloud IAM
Compute	**Compute Instances**	Scalable compute instances (servers)	Azure VM	Elastic Compute Cloud (EC2)	Compute engine
	Managed Kubernetes (K8s) services	Allows you to run K8s without needing to install and operate your own K8s cluster	Azure Kubernetes Service (AKS)	Elastic Kubernetes Service (EKS)	Google Kubernetes Engine (GKE)
	Serverless Container services	Run containers without managing servers	Azure Container Instances (ACI)	Fargate	Cloud Run (+GKE)
	Serverless Functions	Event-driven, serverless computing service that runs code in response to events and automatically manages the computing resources required by that code	Azure Functions	Lambda Functions	Cloud Functions

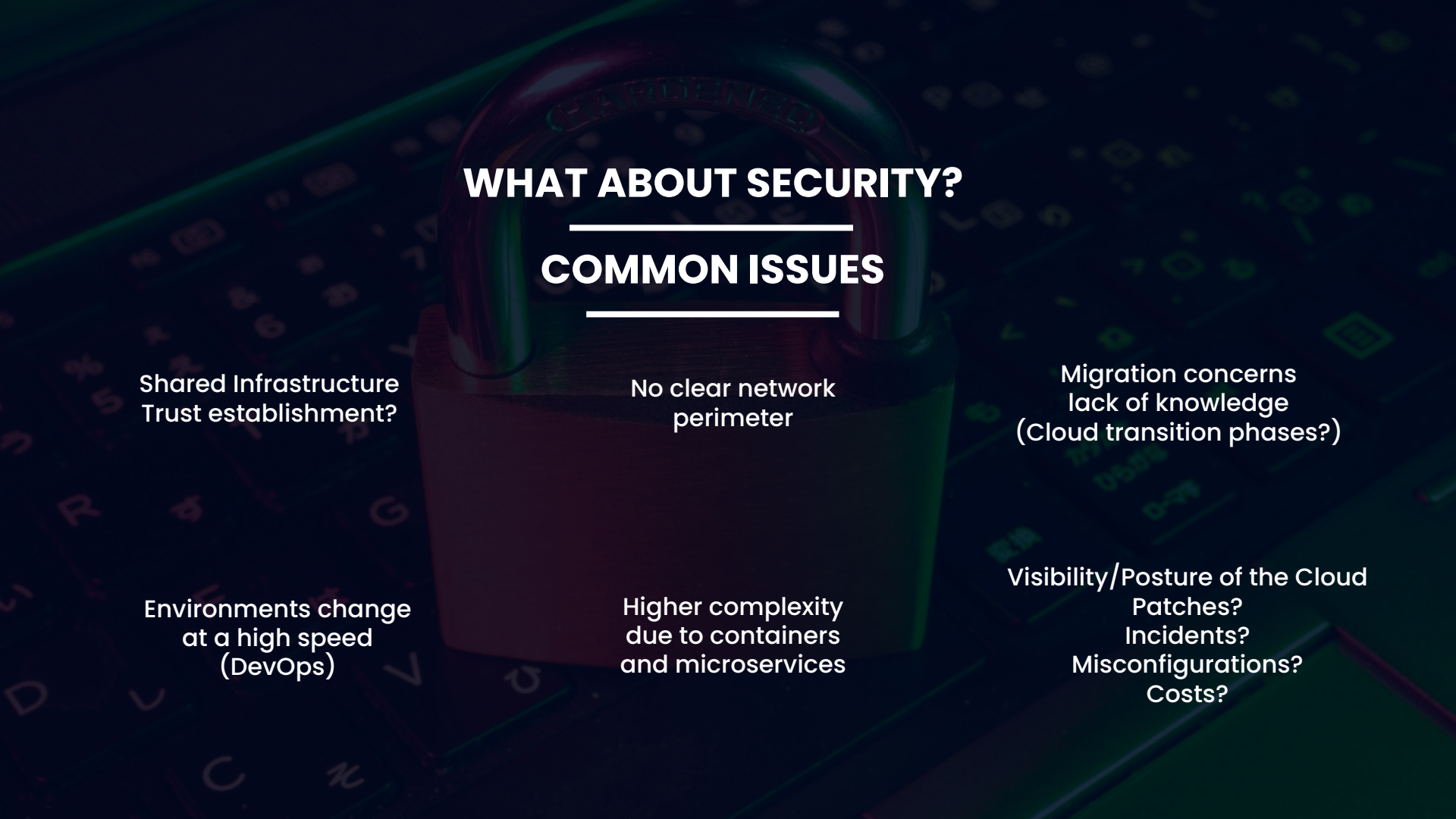
Basic Terms (3) - Other

Others

Generic Term	Definition	Azure	aws	GCP
Object Storage	Scalable, highly available storage for objects	Blob Storage	S3 Buckets	Cloud Storage
Managed SQL Database services	High performance managed SQL engine that runs on a cloud's managed SQL service	SQL Database or Azure Database for MySQL	RDS - Relational Database Service	Cloud SQL
Serverless Orchestration	Task, processes, and workflow orchestration	Logic Apps	Step Functions	Google Cloud Dataflow
Pub/Sub Messaging	Fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications	Event Grid	SNS Topics	Cloud Pub/Sub

Wir haben jetzt schon einiges gehört:

Aber wie schaut es jetzt eigentlich mit der Security in der Public Cloud aus?



WHAT ABOUT SECURITY?

COMMON ISSUES

Shared Infrastructure
Trust establishment?

No clear network perimeter

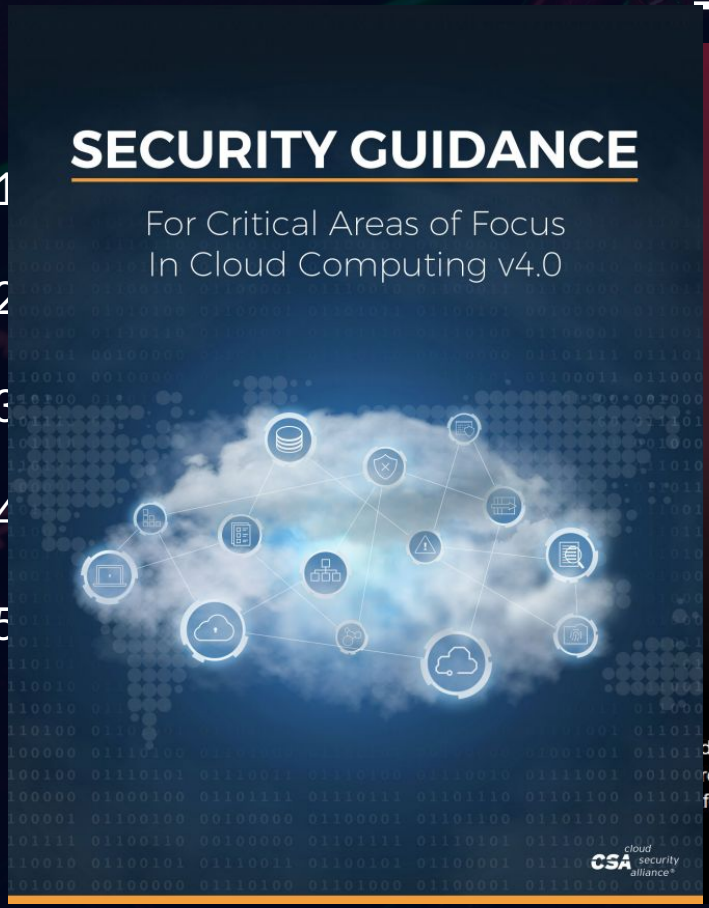
Migration concerns
lack of knowledge
(Cloud transition phases?)

Environments change at a high speed (DevOps)

Higher complexity due to containers and microservices

Visibility/Posture of the Cloud
Patches?
Incidents?
Misconfigurations?
Costs?

TYPICAL APROACH



Cloud Security Technical Reference Architecture

Coauthored by:
Cybersecurity and Infrastructure Security Agency,
United States Digital Service, and
Federal Risk and Authorization Management Program

June 2022
Version 2.0

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 500-291, Version 2

NIST Cloud Computing Standards Roadmap

NIST Cloud Computing Standards Roadmap Working Group
NIST Cloud Computing Program
Information Technology Laboratory

NIST National Institute of Standards and Technology • U.S. Department of Commerce

THE WELL ARCHITECTURED FRAMEWORKs

Those are frameworks by large CSPs
Which should guide CSCs to build the cloud infrastructure in a proper way

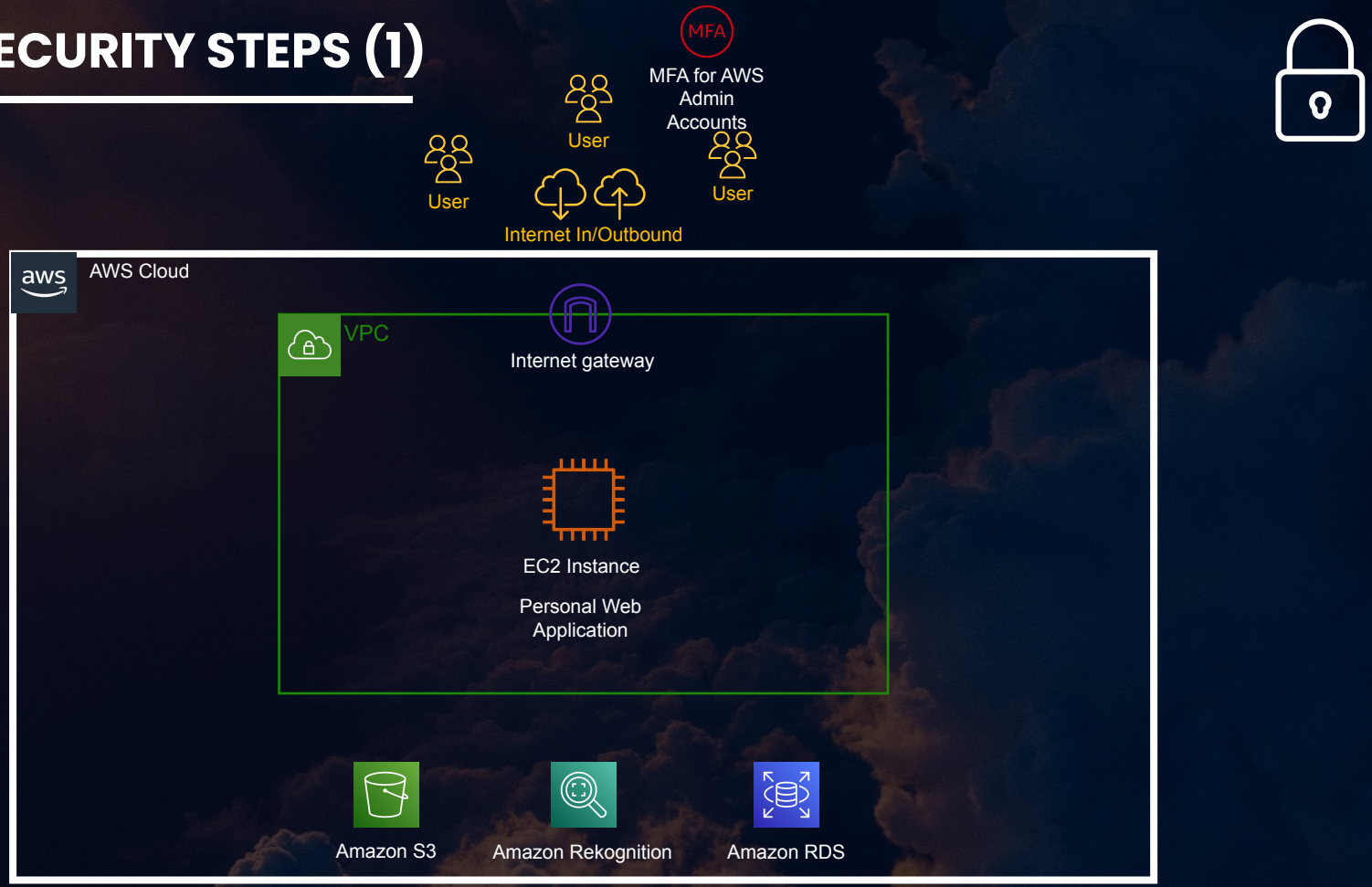
Fallbeispiel: Basic Security Steps in einer Umgebung anhand von AWS

BASIC SECURITY STEPS

BASIC SECURITY STEPS

1. Protect privileged credentials
2. Use temporary credentials
3. Replace hardcoded credentials
4. Limit network access
5. Apply patches
6. Restrict public storage

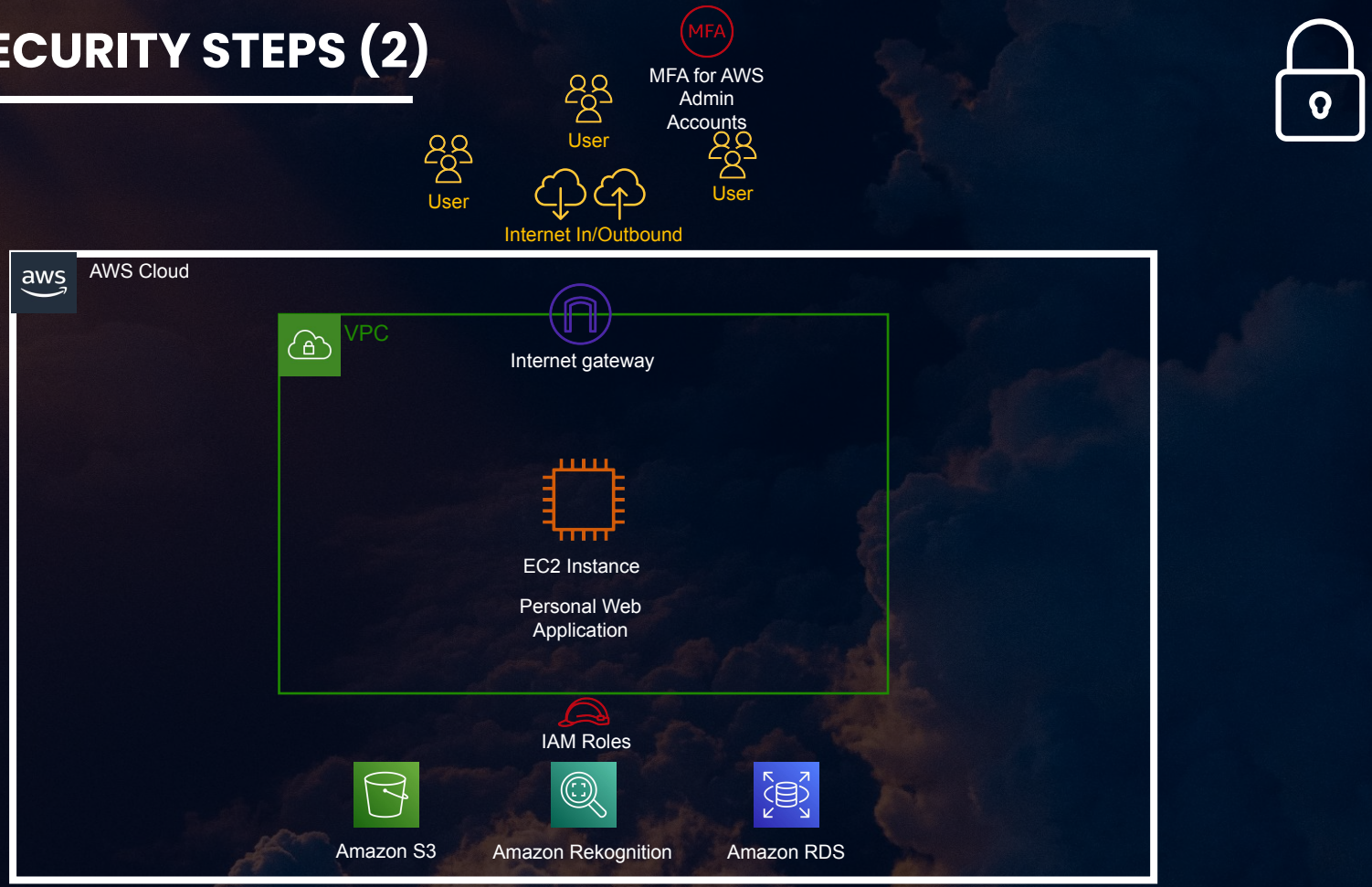
BASIC SECURITY STEPS (1)



BASIC SECURITY STEPS

1. Protect privileged credentials
2. Use temporary credentials
3. Replace hardcoded credentials
4. Limit network access
5. Apply patches
6. Restrict public storage

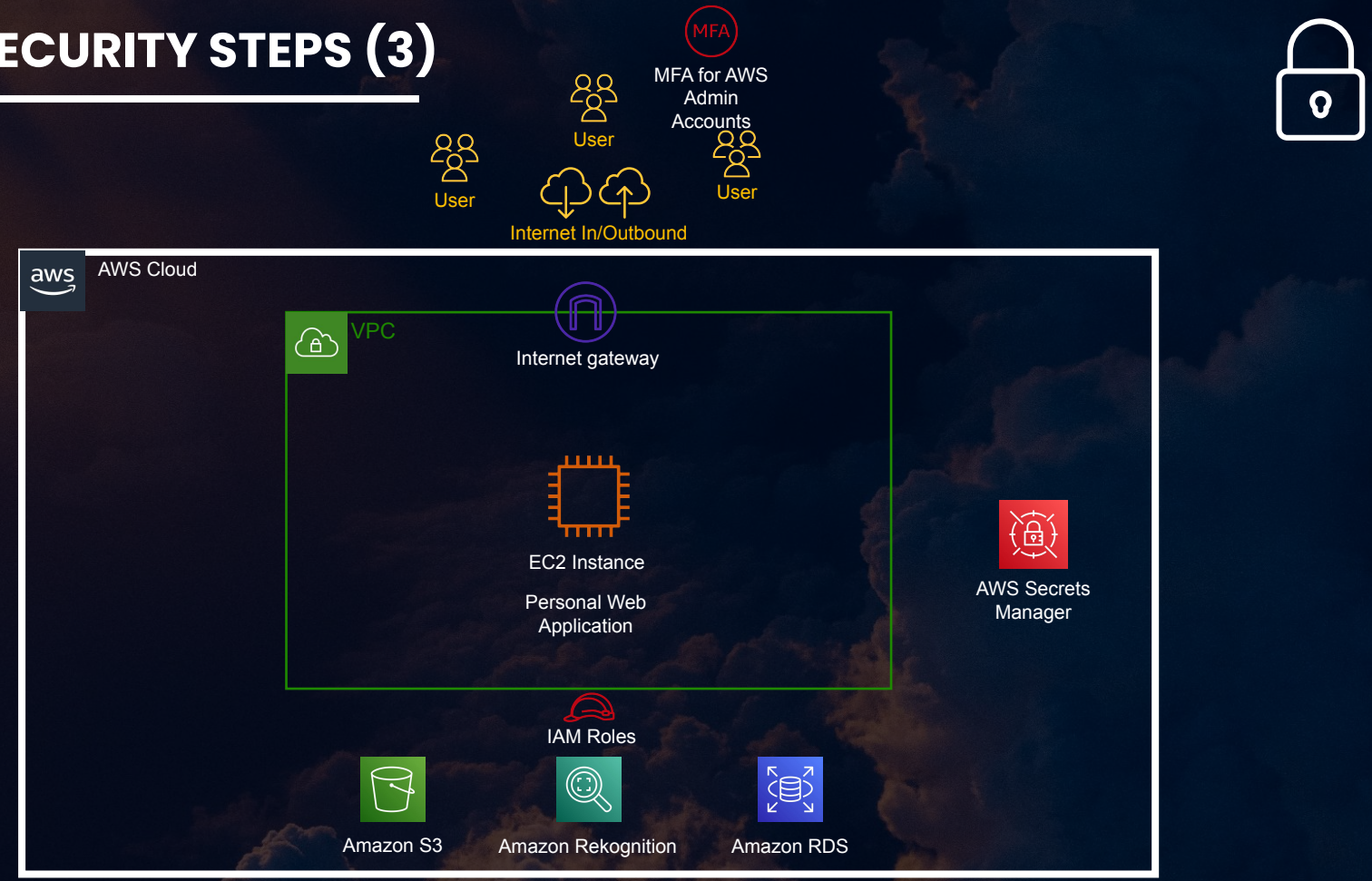
BASIC SECURITY STEPS (2)



BASIC SECURITY STEPS

1. Protect privileged credentials
2. Use temporary credentials
3. Replace hardcoded credentials
4. Limit network access
5. Apply patches
6. Restrict public storage

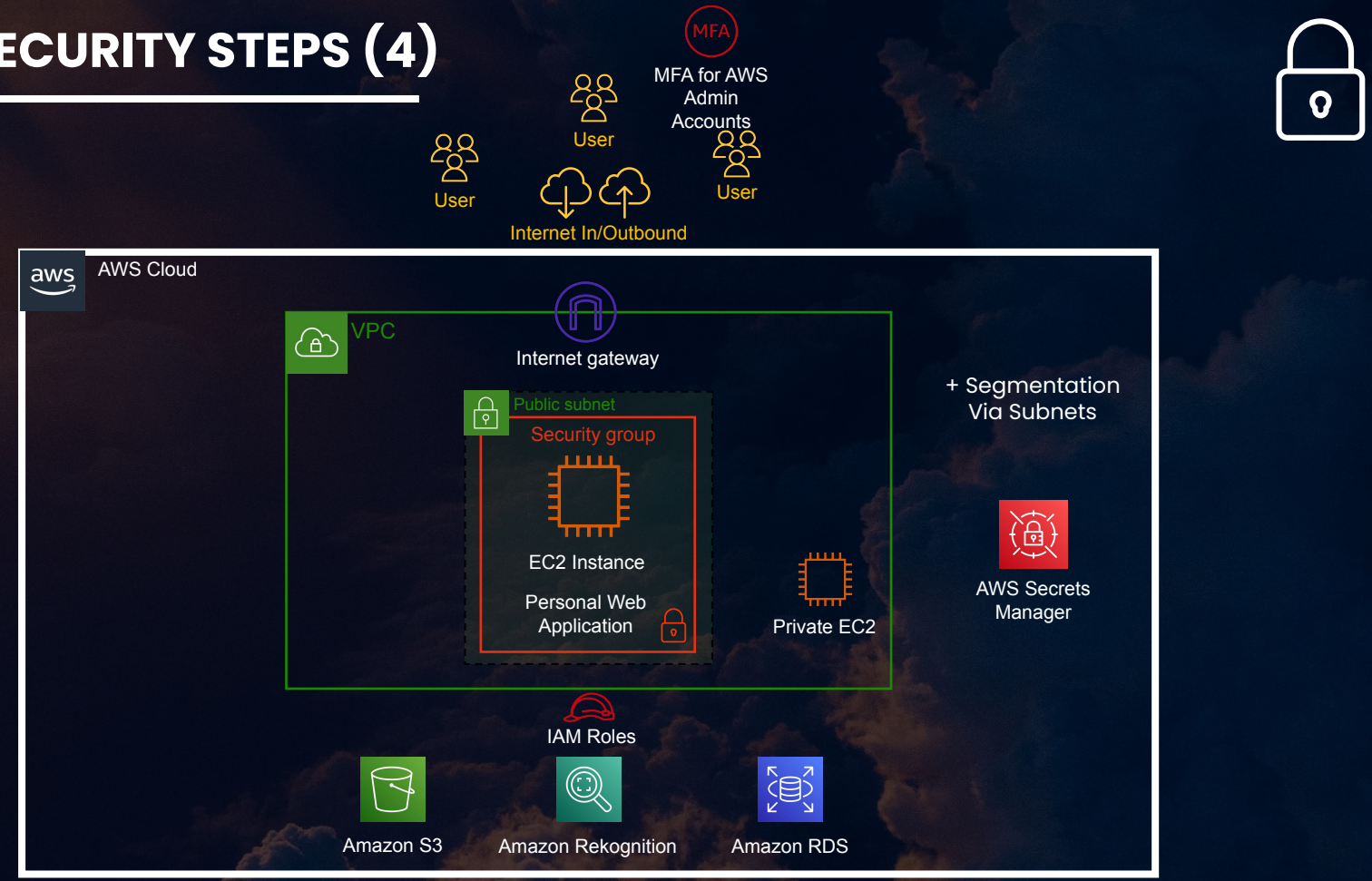
BASIC SECURITY STEPS (3)



BASIC SECURITY STEPS

1. Protect privileged credentials
2. Use temporary credentials
3. Replace hardcoded credentials
4. Limit network access
5. Apply patches
6. Restrict public storage

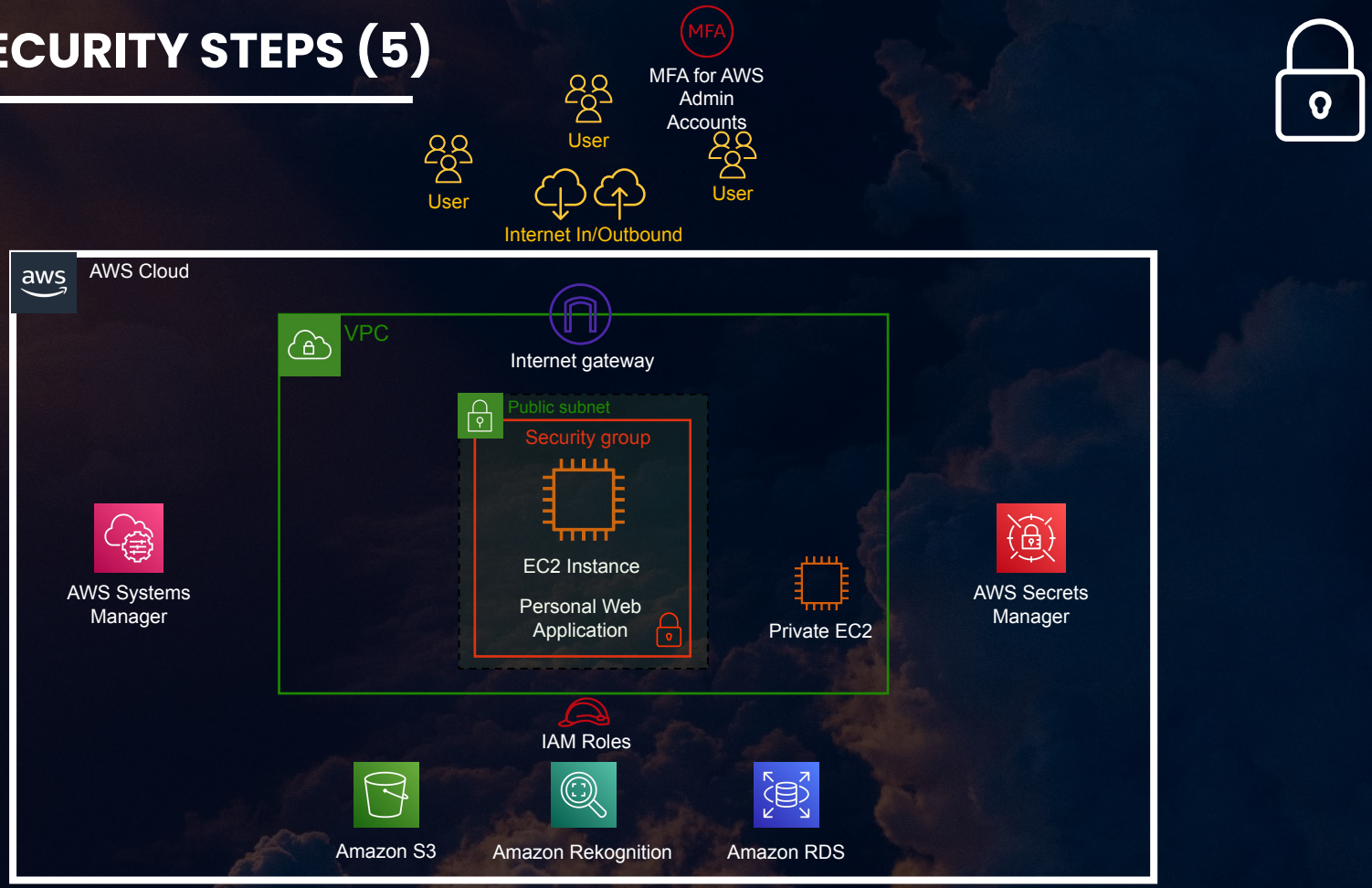
BASIC SECURITY STEPS (4)



BASIC SECURITY STEPS

1. Protect privileged credentials
2. Use temporary credentials
3. Replace hardcoded credentials
4. Limit network access
5. Apply patches
6. Restrict public storage

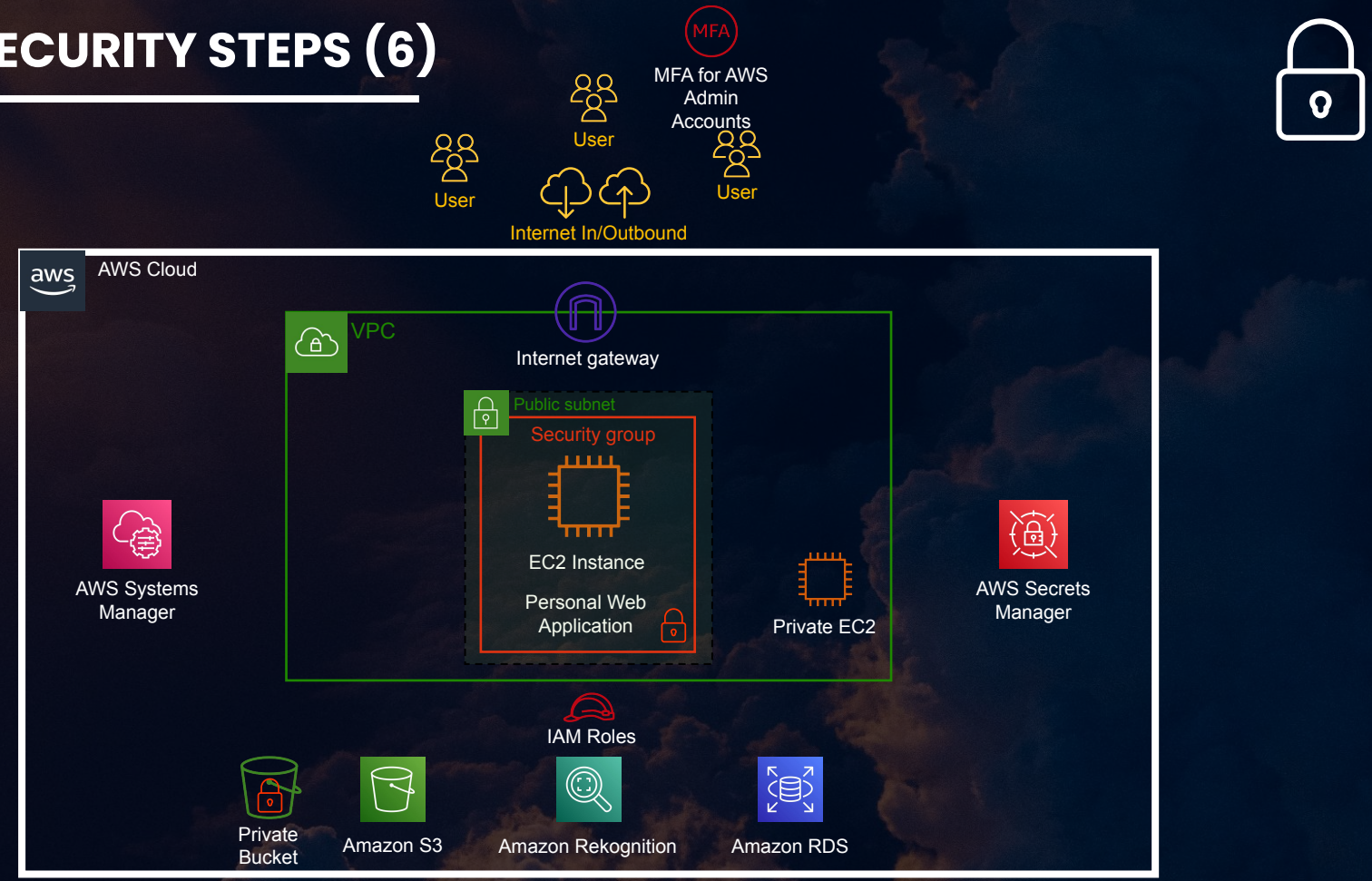
BASIC SECURITY STEPS (5)



BASIC SECURITY STEPS

1. Protect privileged credentials
2. Use temporary credentials
3. Replace hardcoded credentials
4. Limit network access
5. Apply patches
6. Restrict public storage

BASIC SECURITY STEPS (6)



BASIC SECURITY STEPS

1. Protect privileged credentials
2. Use temporary credentials
3. Replace hardcoded credentials
4. Limit network access
5. Apply patches
6. Restrict public storage

Pickt einen Use Case aus eurem Unternehmen:

Welche Ressourcen bzw. welchen Service könntet ihr in der Cloud deployen?

Was macht ihr aus Security Sicht?

Workout

- **Ziel:** Identifikation eines sinnvollen Anwendungsfall für euer Unternehmen.
- **Output:** Basic Architektur in der Cloud - Wie könnte so etwas ausschauen?
- **Modus:** Alleine oder in Kleingruppen (15-20min anschließende Diskussion)

Cloud Migration – Szenarien und deren Risiken

Was glaubt ihr?

Wie läuft traditionell eine Migration von Cloud Infrastruktur in Unternehmen ab?

Cloud Transition Phases – The Five R's

1. Rehost
2. Revise
3. Rearchitect
4. Rebuild
5. Replace

Lift and Shift
Modification
Cloud Centric
Redesign Cloud Native
Switch to SaaS

1. Rehost – Security Concerns

This approach leads to a misinterpretation of the cloud concepts and thinking that networking, storage, and compute power behave the same in the cloud as used to on-premises.

- IaaS Segmentation
- No clear Perimeter
- Security at Scale Architecture

2. Revise – Security Concerns

This approach refers to altering an infrastructure and apps in a way that allows them to begin enhancing themselves with some public cloud capabilities.

- Segmentation between IaaS and PaaS/CaaS
- Isolation of PaaS/CaaS
- Security at Scale Architecture

3. Rearchitect – Security Concerns

This approach aims at a cloud-native architecture. Therefore, a strong adoption of PaaS, CaaS and FaaS services (wherever possible).
It requires a change of culture and an adoption of the DevOps methodology.

- IAM and Network Controls for IaaS, PaaS, CaaS and FaaS
- Visibility in the Cloud
- Securing of CI/CD (DevSecOps)
- Securing of Legacy Systems
- Cloud Security Architecture

4. Rebuild – Security Concerns

This approach requires a start from scratch. It leads to a new and modern approach, which considers these aspects:

- Newest Capabilities of the Cloud
- Optimization of Operational Excellence
- New Design of Infrastructure

- IAM and Network Controls for IaaS, PaaS, CaaS and FaaS
- Visibility in the Cloud
- Securing of CI/CD (DevSecOps)
- Solid Cloud Security Architecture

5. Replace – Security Concerns

This approach refers to identifying systems, which can be completely outsourced to a SaaS provider. The core of this strategy is to migrate systems, which can be outsourced to a managed service provider.

- Compliance and Law Regulations
- Risk Assessment of a SaaS Provider
- Integration of other Infrastructure and Legacy Systems

The Five R's – Summary

1. Rehost
2. Revise
3. Rearchitect
4. Rebuild
5. Replace

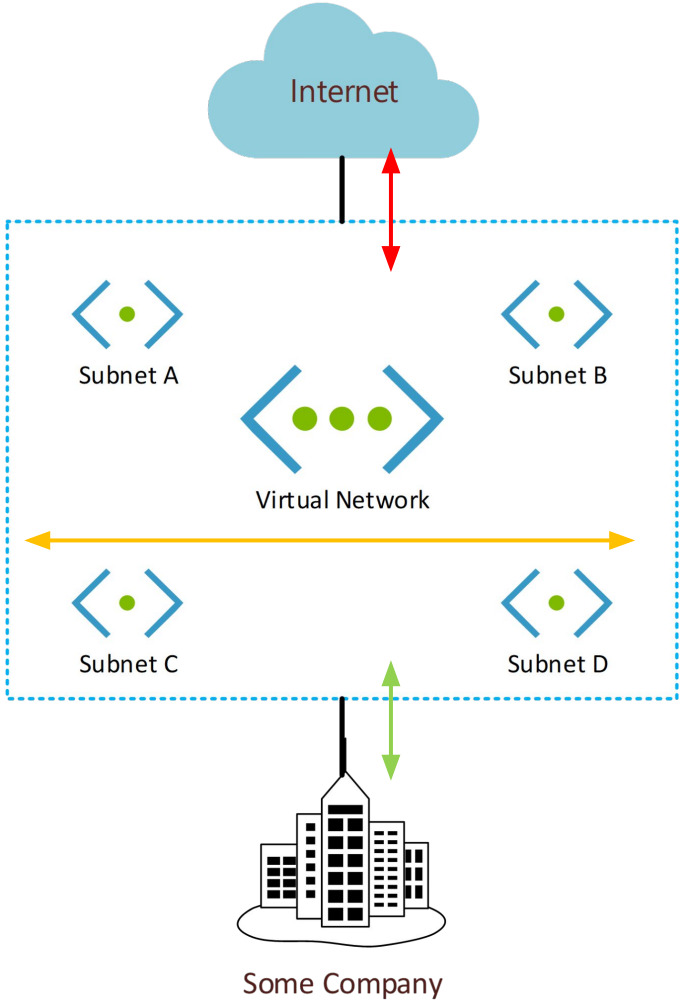
A combination of the strategies is a common approach

Moderne Architekturen für größere Cloud Umgebungen

Infrastructure Basic Traffic Flows

East-West Traffic

North/South Bound Traffic

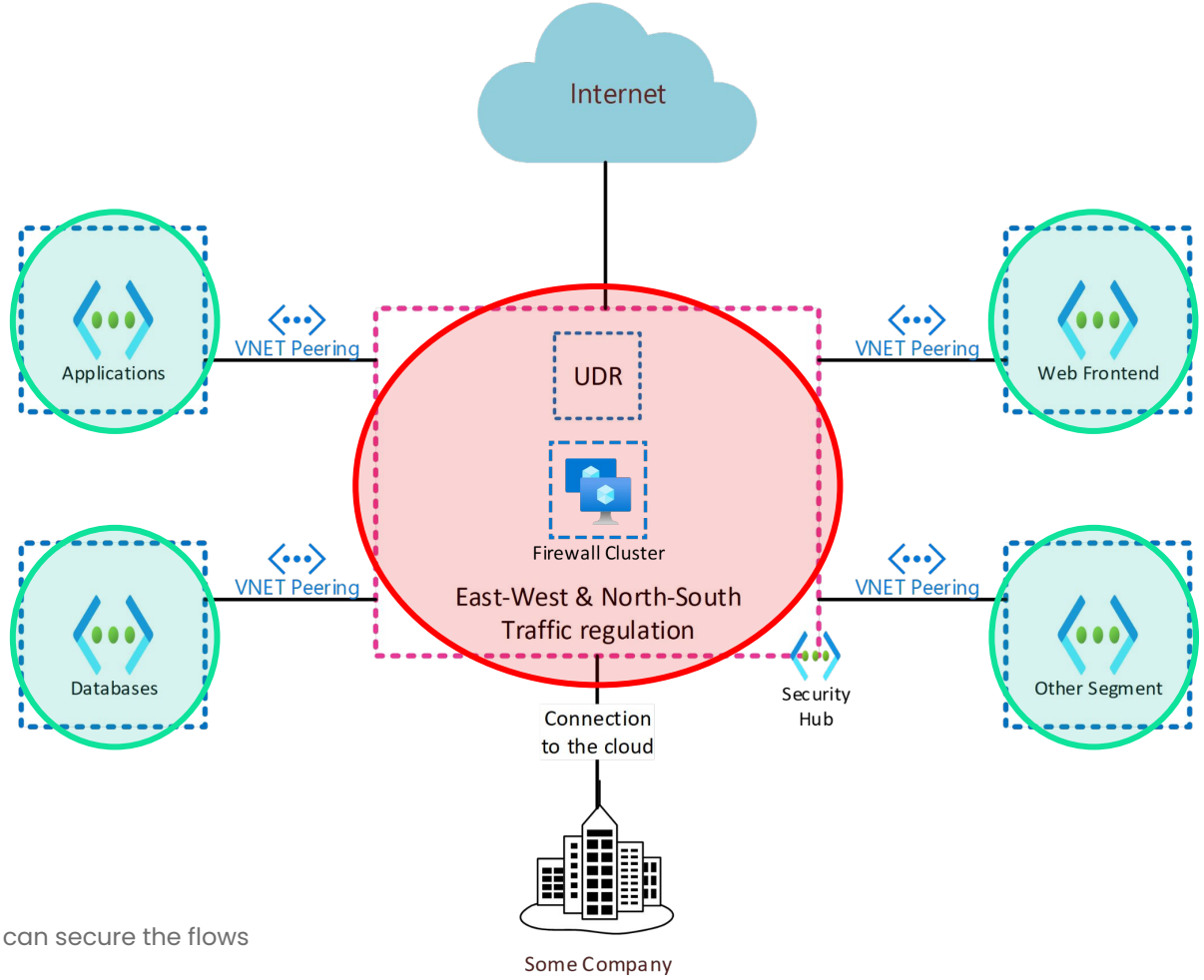


Best Practice: Hub and Spoke Architecture

Keep in mind:

Routing is king &

Segmentation is king



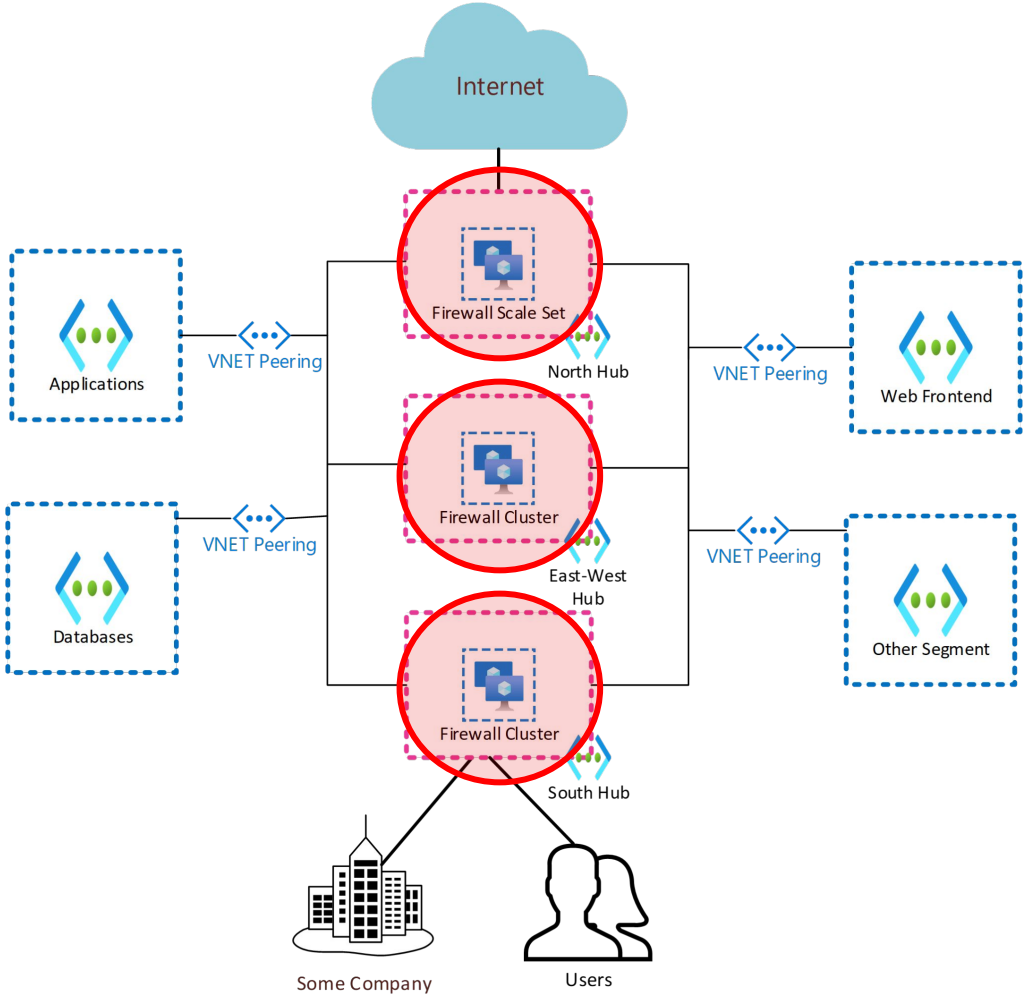
If you understand the flows, you can secure the flows

Hub and Spoke Large scale

Multi-Hub Architecture

Different types

of responsibilities



Wrap Up

Was nehmen wir uns mit?

Die meisten Unternehmen die es gibt verwenden in irgendeiner form Cloud Computing und immer mehr Managed Lösungen

Wir sollten wenn wir Public Cloud Ressourcen verwenden nie den Standardeinstellungen vertrauen. Immer beachten was wir verwenden und wie wir das absichern.

Die zwei wichtigsten Punkte sind: Absichern der Control Plane/Root Accounts und Shared Responsibilities

Security Architekturen für Unternehmensressourcen

Aufbau einer sicheren, praktikablen und skalierbaren IT-Infrastruktur

Lernpfad

FA01: Erweiterte Security Techniken und Tools für Unternehmen

FA02: Security Architekturen für Unternehmens-ressourcen (KMU)

FA03: Cloud and Application Security Strategien

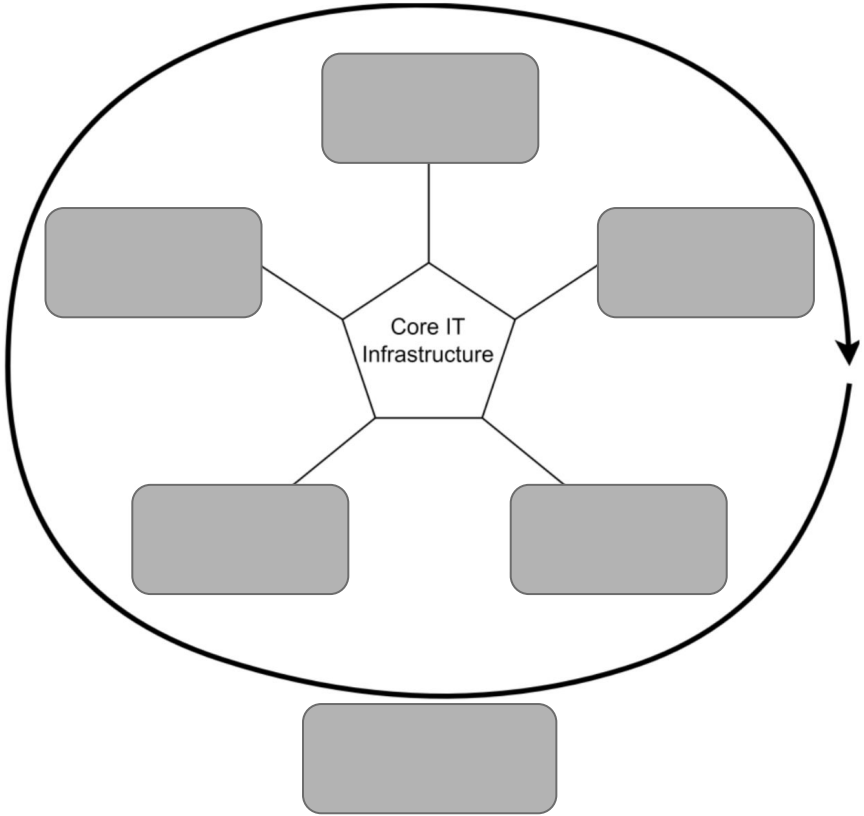
FA04: Compliance - Ganzheitliche Cybersecurity anhand von Cyber Trust Austria

Lernziele

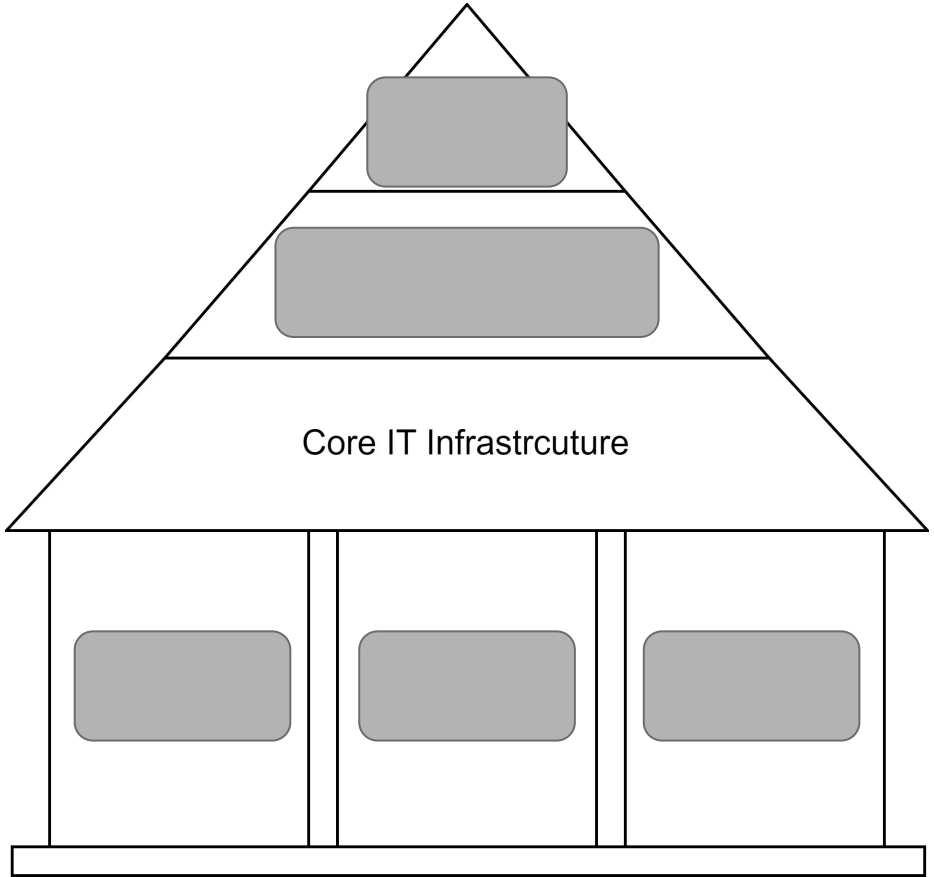
1. Netzwerksicherheit und -architektur: Sichere Netzwerkdesigns für IoT/OT (VLANs, Firewalls, VPNs).
2. Datenmanagement und -architektur: Backup, Verschlüsselung und Disaster-Recovery für Produktions- und Kundendaten
3. Sichere Kommunikation: Integration sicherer E-Mail- und Kollaborationstools.
4. IoT/OT-Sicherheit: Sicherheitsrichtlinien und Updates für IoT/OT-Geräte

PS: Dieses Level sollte min. jeder Umsetzen können

Wichtigste IT Infrastrukturkomponenten?



Abhängigkeiten dieser Komponenten



Design Challenge 🚀

Smart Solutions GmbH

Interaktive Session

Eure Mitarbeit ist gefragt!

Topics

Network | Data | Application

Communication | OT | Business Continuity

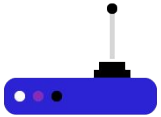
Format

Deduktives Lernen:
ihr versucht das initiale Problem zu Lösen und dann Recap in der großen Runde

Smart Solution

- Hersteller von smarten Temperatursensoren
- 15 Mitarbeiter
- Hat IoT und OT Infra in Verwendung

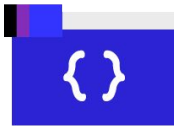
Simple Solution - IT Infrastruktur - Level 0



Einfaches LAN Standard-Router mit WLAN
keine VLANs
Firewall ist deaktiviert

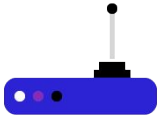
NAS-Server
keine Backups
lokale MySQL-Datenbank
ext. Festplatten, USB Drives

Office 2013 On-Premise
WhatsApp
Zoom Basic
PBX Phone + Private Handys



JTL ERP System (Produktion)
Website
Excel Listen (CRM, BH, Personal ...)

Simple Solution - IT Infrastruktur - Level 0

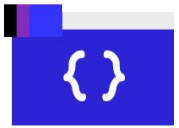


Einfaches LAN Standard-
Router mit WLAN
keine VLANs
Firewall ist

NAS-Server
keine Backups
MySQL-Datenbank
stplatten, USB Drives

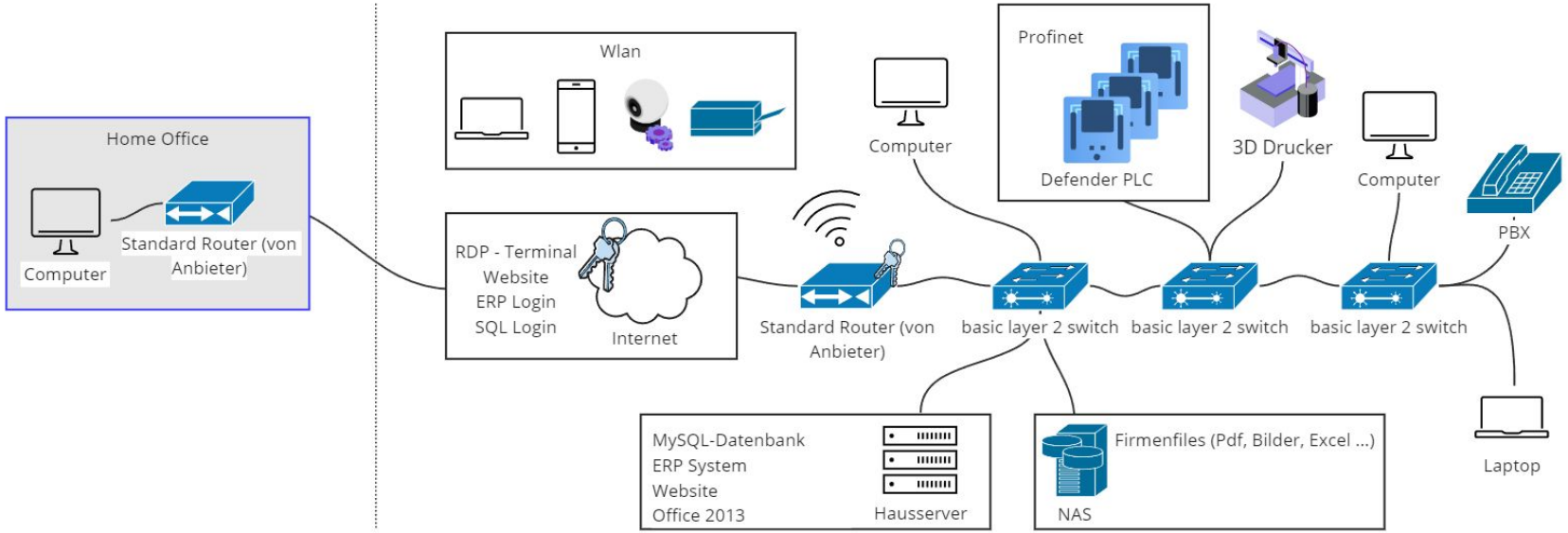
Smart Meters
PLCs
3D Drucker
Profinet

Office 2013 On-Premise
WhatsApp
Zoom Basic
PBX Phone + Private Handys

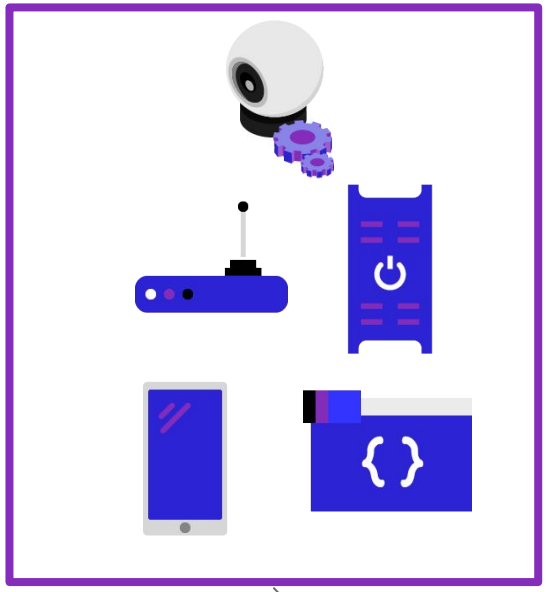


JTL ERP System (Produktion)
Website
Excel Listen (CRM, BH,
Personal ...)

Simple Solution - IT Architektur - Level 0



Level Up - Action Plan

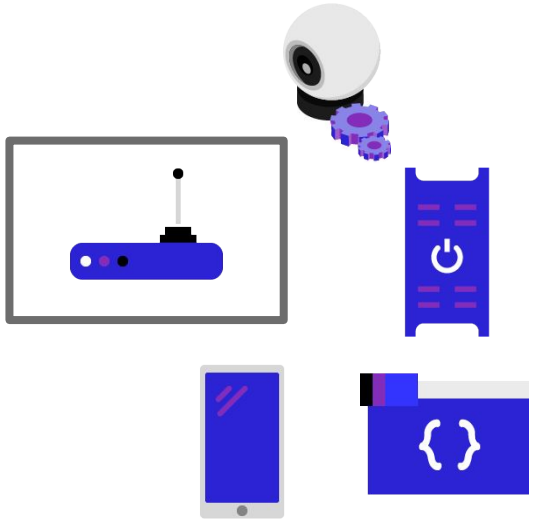


Was müssen wir tun um auf das nächste Level zu kommen ?

1. Ihr bekommt die Problemstellungen
2. Ihr überlegt eine Lösung
3. Wir schauen uns gemeinsam eine Referenz Lösung an

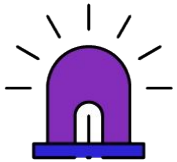
\+ Business Continuity & Disaster Recovery

Level Up - Action Plan



Starten wir mit dem Topic Netzwerk.

Level Up - Netzwerk



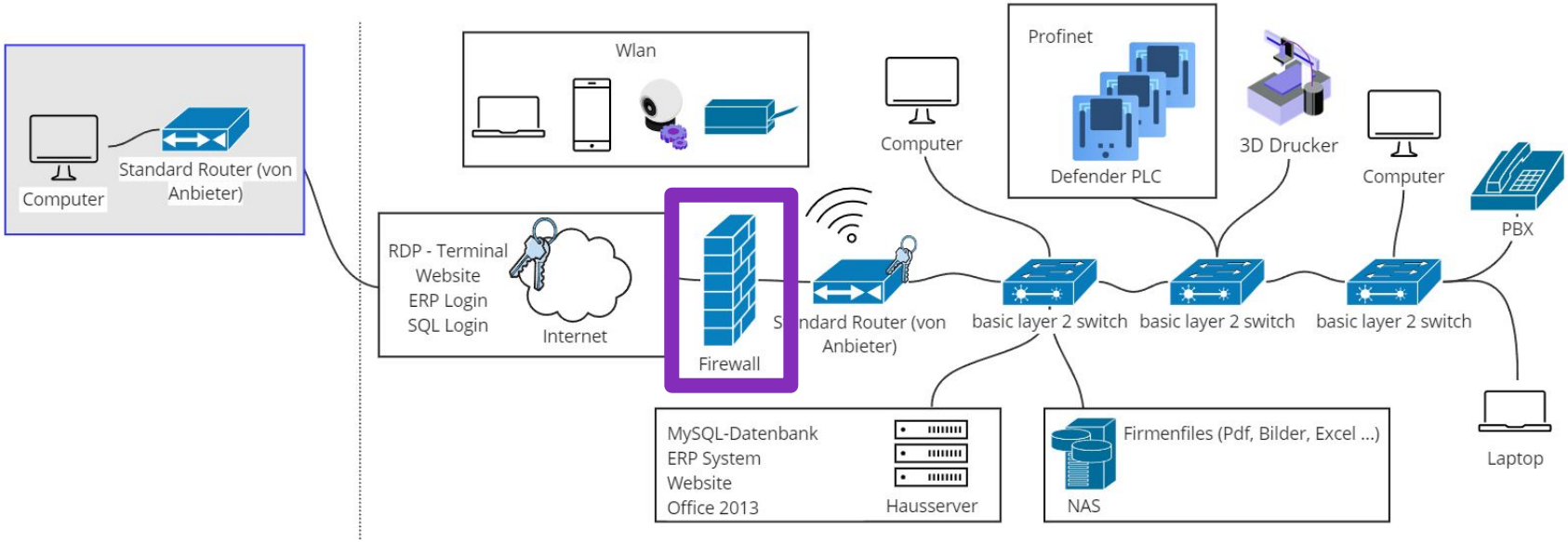
1. Der Zugang zum Internet muss abgesichert werden
2. Der Kommunikationsfluss im Netzwerk muss geregelt werden
3. Die Verbindung vom Home Office in die Firma muss abgesichert werden

Überlegt in Teams

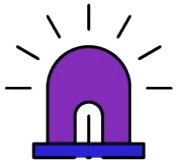
- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Verschlüsselung, Layer 2 vs. Layer 3, VPN, Firewall, Segmentierung

Level 0 – Perimeter absichern



Level Up - Netzwerk



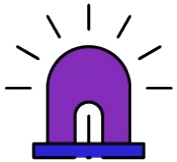
1. Der Zugang zum Internet muss abgesichert werden ✓
2. Der Kommunikationsfluss im Netzwerk muss geregelt werden
3. Die Verbindung vom Home Office in die Firma muss abgesichert werden

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Verschlüsselung, Layer 2 vs. Layer 3, VPN, Firewall, Segmentierung

Level Up - Netzwerk



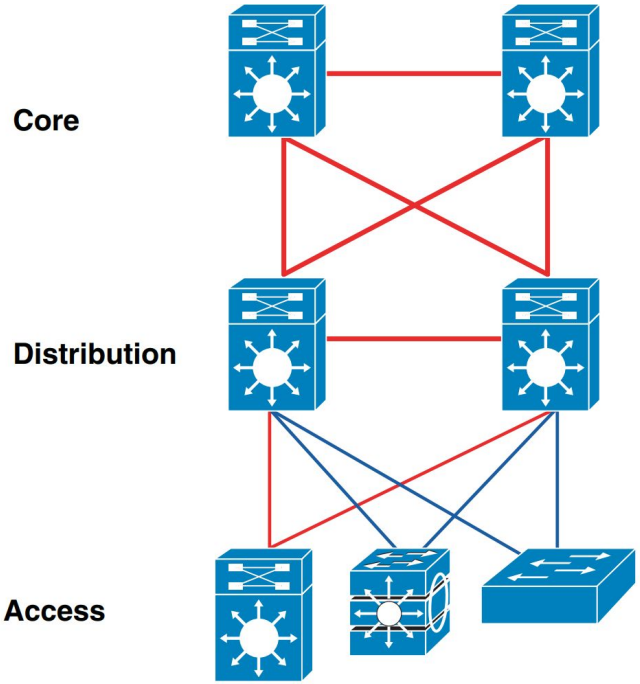
1. Der Zugang zum Internet muss abgesichert werden ✓
2. Der Kommunikationsfluss im Netzwerk muss geregelt werden
3. Die Verbindung vom Home Office in die Firma muss abgesichert werden

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Verschlüsselung, Layer 2 vs. Layer 3, VPN, Firewall, Segmentierung

Level Up - Netzwerk - Hierarchie

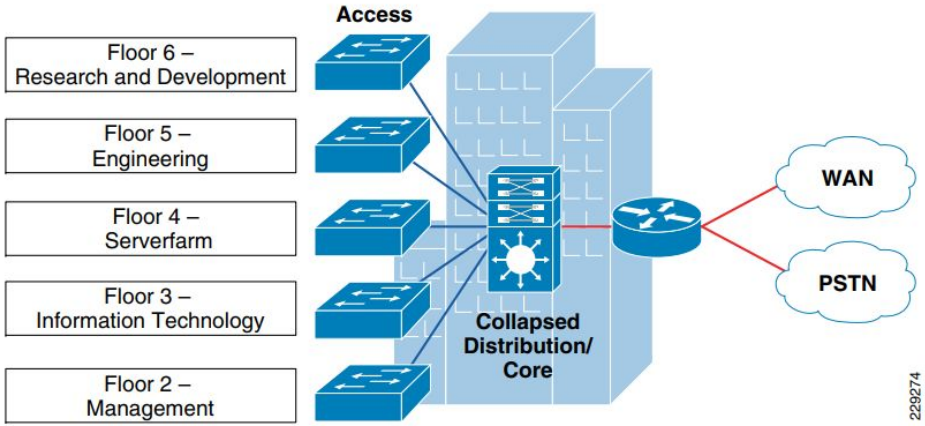


Vorteile einer Tier-Hierarchie

- Verfügbarkeit
- Skalierbarkeit
- Resilienz

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Level Up - Netzwerk - Hierarchie



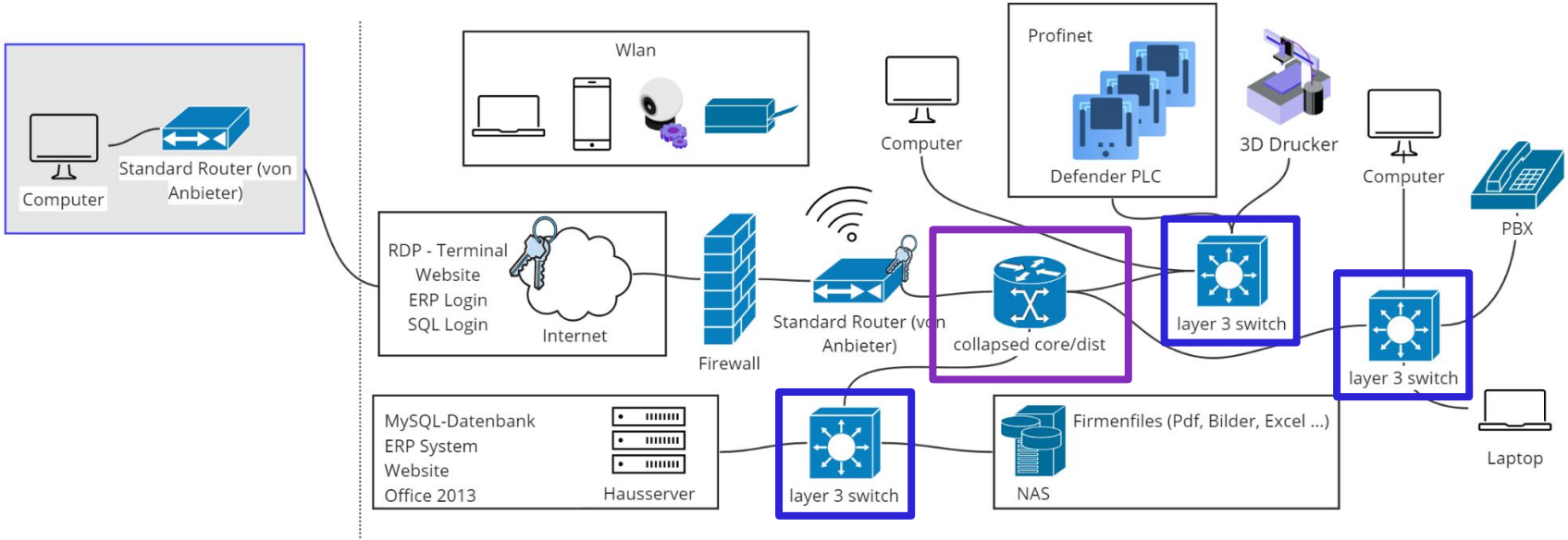
Vorteile einer Tier-Hierarchie

- Verfügbarkeit
- Skalierbarkeit
- Resilienz

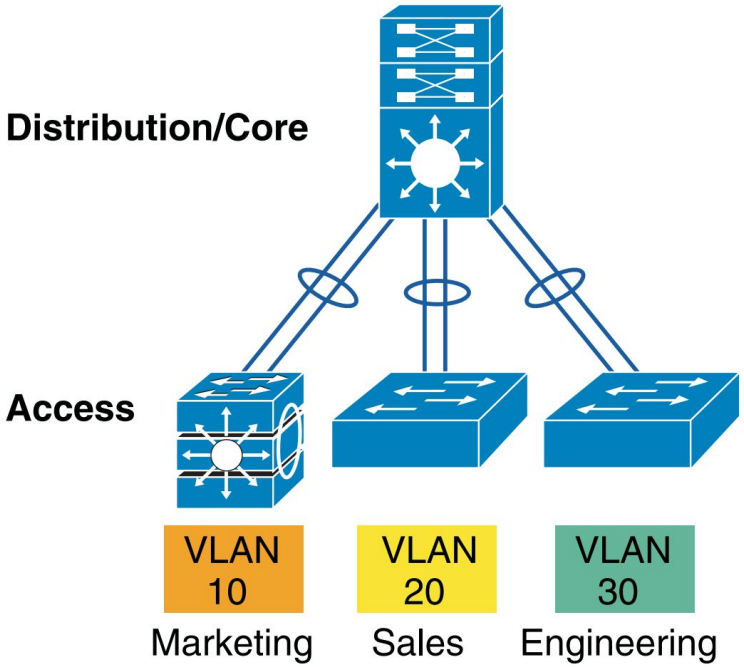
Für ein kleines KMU ist zum start eine 2 - Tier Variante mit Core + Distribution in einem ausreichend

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Level Up - Netzwerk - Hierarchie



Level Up - Netzwerk - Segmentierung



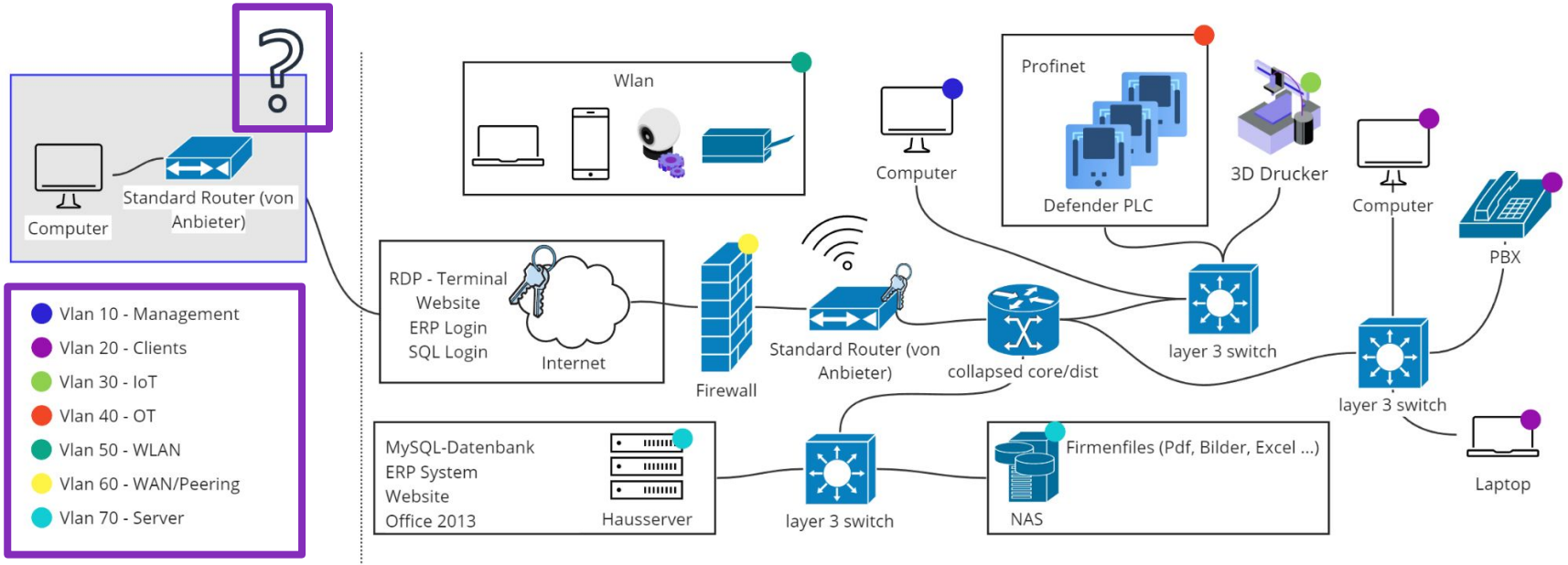
Vorteile einer Segmentierung

- Kontrolle über Kommunikation
- Verbreitung von DoS Angriffen erschwert
- Performance Vorteil (BC Domains)

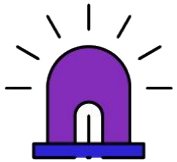
Eine Basisstrategie für die Einteilung der Gruppen ist zu überlegen, welche wesentliche zusammengehörende Nutzerbedürfnisse es gibt.

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Level Up - Netzwerk - Hierarchie



Level Up - Netzwerk



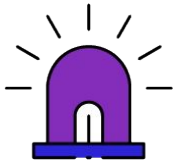
1. Der Zugang zum Internet muss abgesichert werden ✓
2. Der Kommunikationsfluss im Netzwerk muss geregelt werden ✓
3. Die Verbindung vom Home Office in die Firma muss abgesichert werden

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Verschlüsselung, Layer 2 vs. Layer 3, VPN, Firewall, Segmentierung

Level Up - Netzwerk



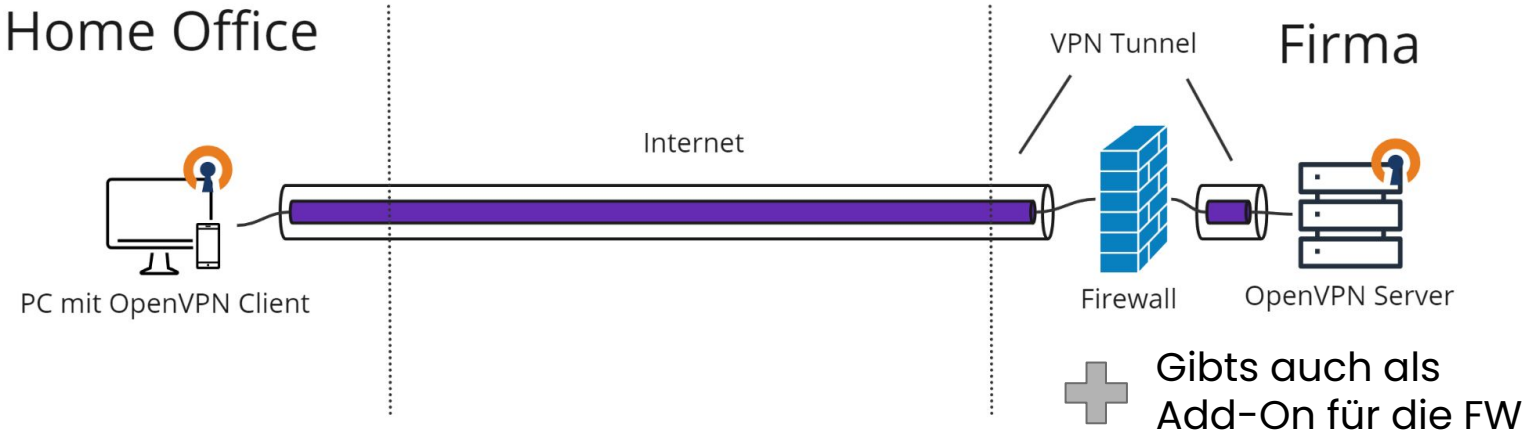
1. Der Zugang zum Internet muss abgesichert werden ✓
2. Der Kommunikationsfluss im Netzwerk muss geregelt werden ✓
3. Die Verbindung vom Home Office in die Firma muss abgesichert werden

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

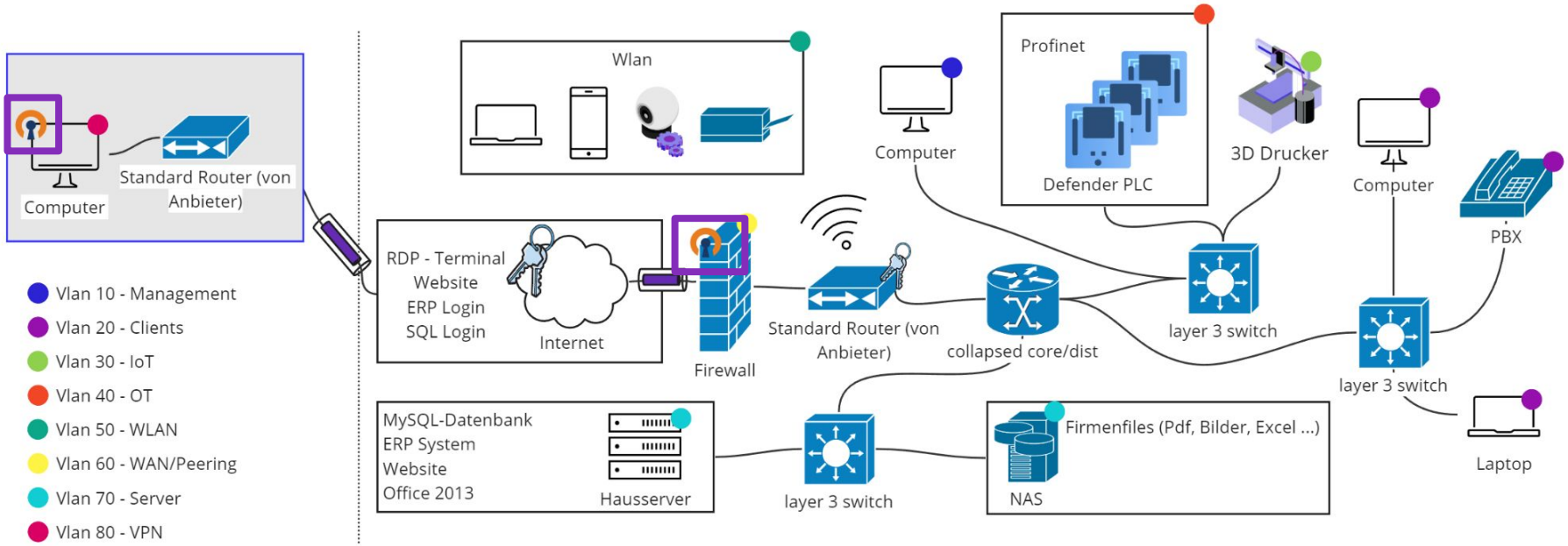
Hinweise: Verschlüsselung, Layer 2 vs. Layer 3, VPN, Firewall, Segmentierung

Level Up - Netzwerk - VPN



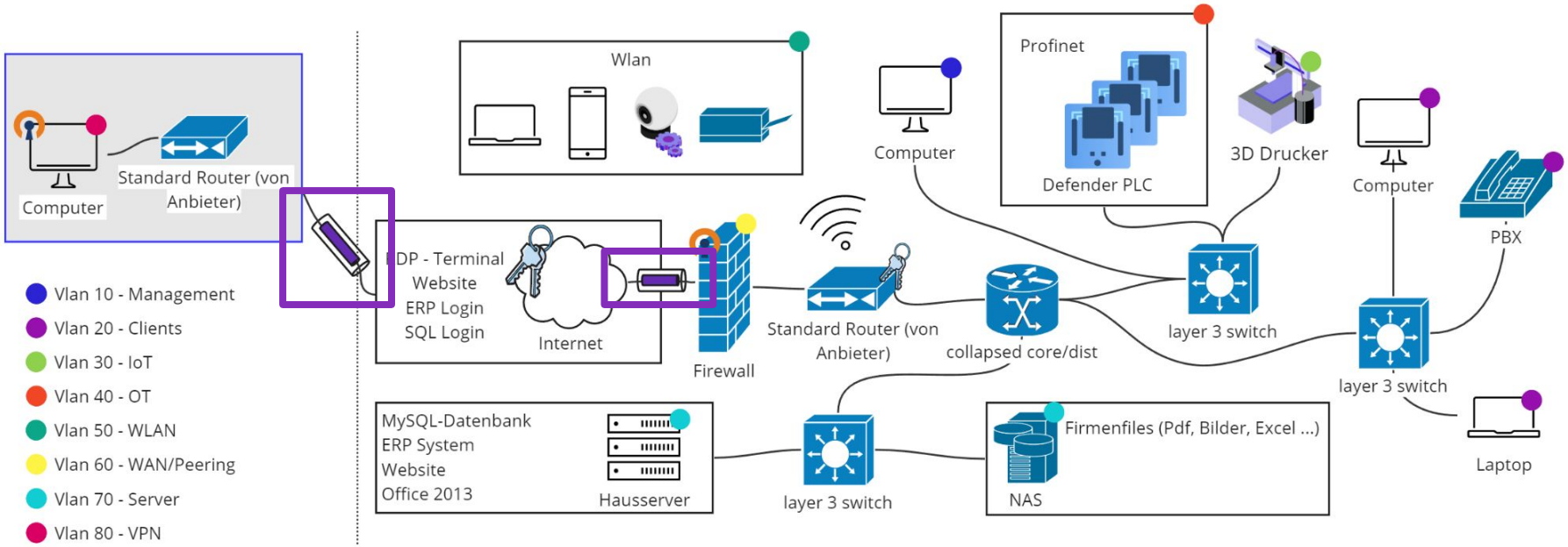
https://openvpn.net/as-docs/network-topology.html

Level Up - Netzwerk - VPN



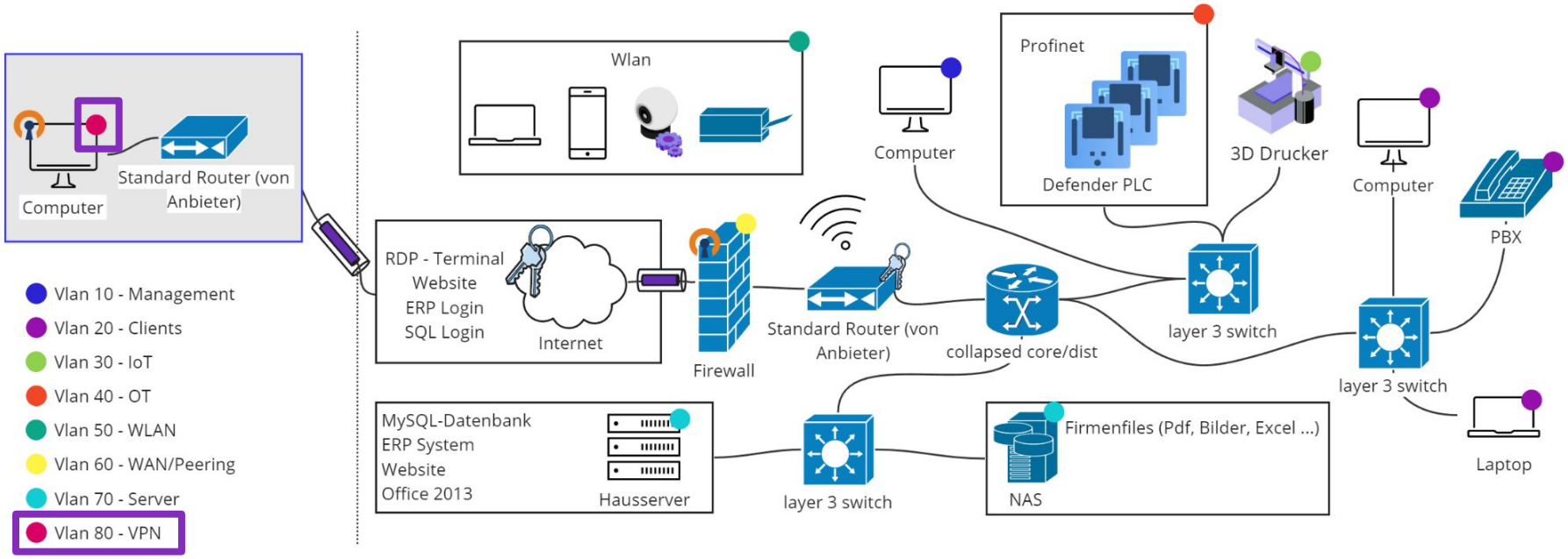
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Level Up - Netzwerk - VPN



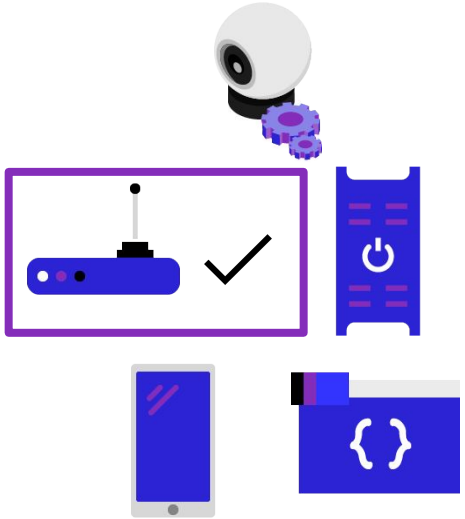
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Level Up - Netzwerk - VPN



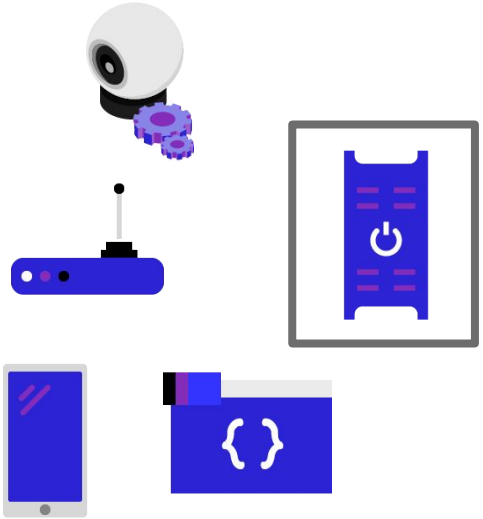
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Level Up - Action Plan



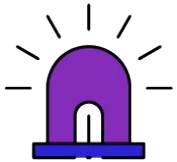
Wir haben unsere Netzwerkarchitektur erfolgreich aufs nächste Level gehoben 🚀

Level Up - Action Plan



Schauen wir uns als nächstes das Topic Data an.

Level Up - Data



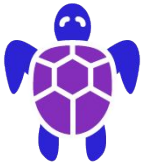
1. Wir brauchen ein vernünftiges Backup
2. Der Zugriff auf unsere Daten muss abgesichert werden
3. Wir brauchen ein Management für unsere Passwörter

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Backup Strategien, Redundanz, Access Management (RBAC), Passwordsafe

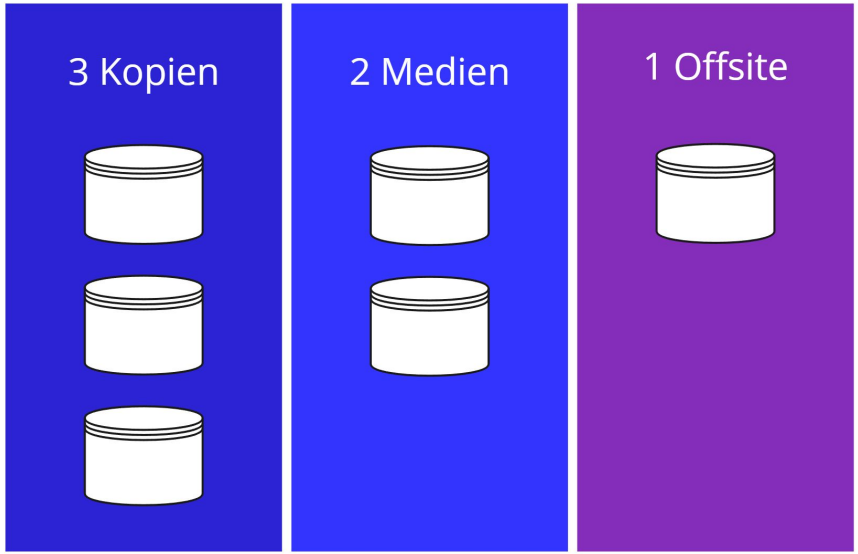
Level Up – Data – Backup



Overarching Goal ist immer Business Continuity !

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Level Up - Data - Backup

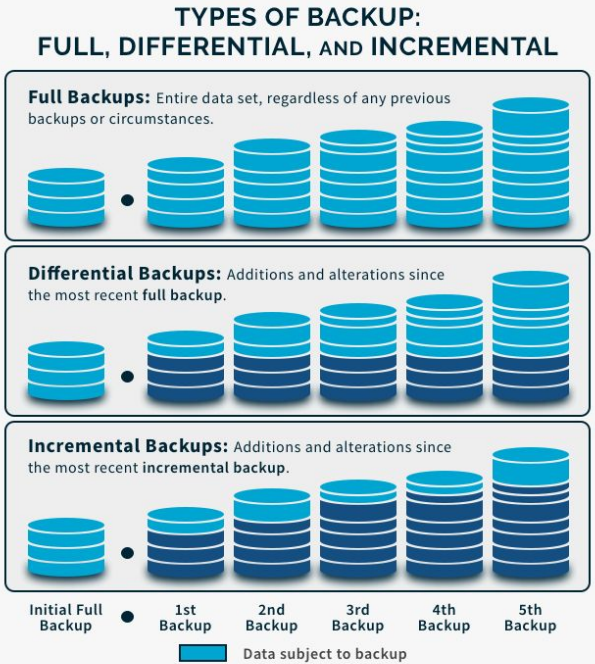


3-2-1 Regel

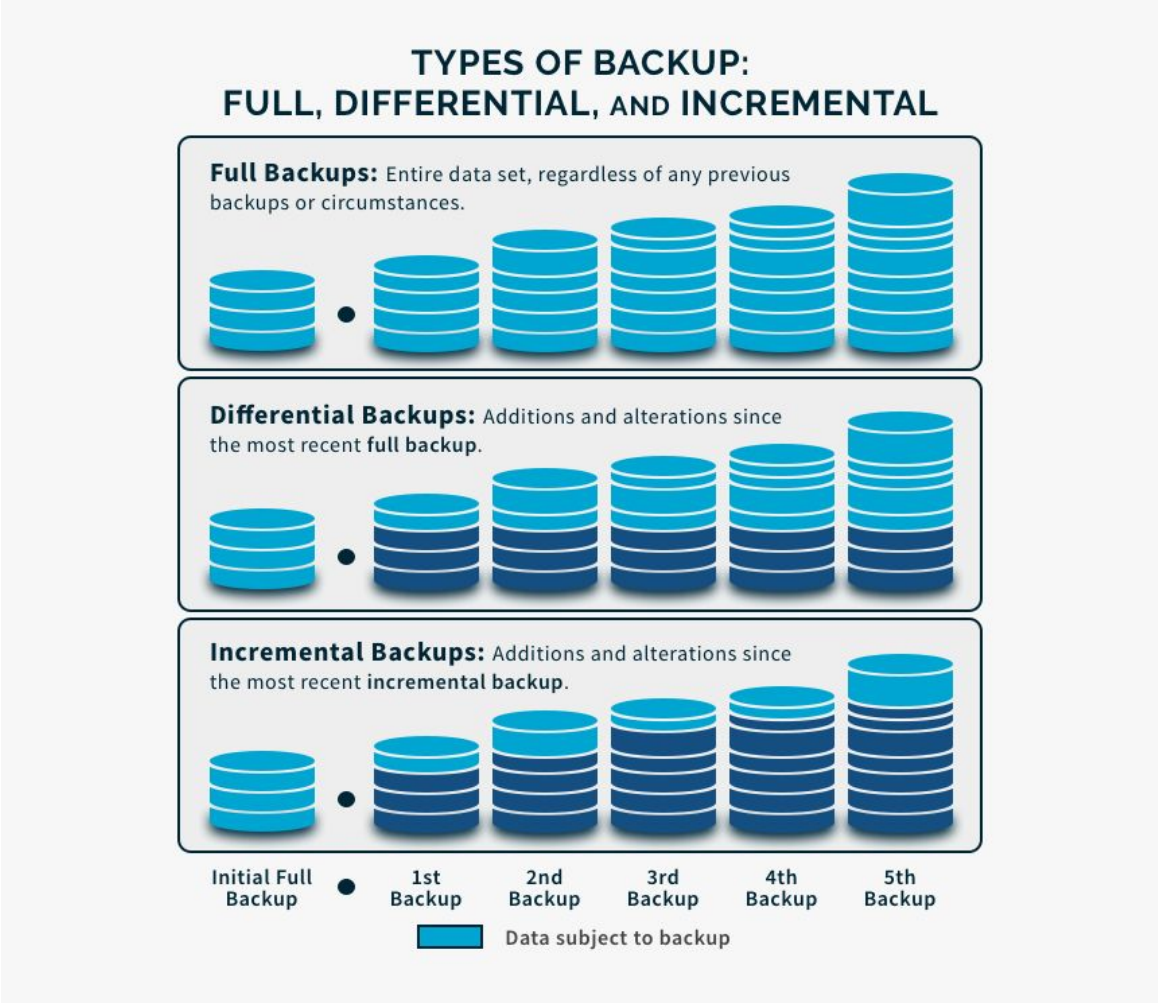
- 1x Daten an denen gearbeitet wird + 2x Kopien
- 2x unterschiedliche Medientypen
- 1x Backup auf externen Standort

https://proton.me/blog/3-2-1-backup#:~:text=The%20idea%20is%20that%20you,of%20something%20than%20you%20need.

Level Up - Data - Backup

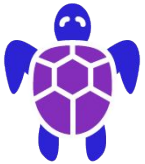


https://www.techtarget.com/searchdatabackup/definition/backup



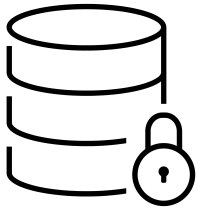
https://www.techtarget.com/searchdatabackup/definition/backup

Level Up - Data - Backup

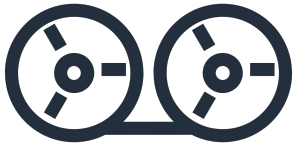


Wie können wir das auf unser Beispiel ummünzen ?

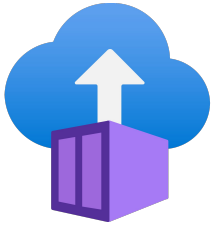
Level Up - Data - Backup



1x Backup Server

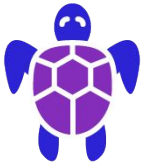


1x Tape Server



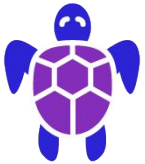
1x Cloud Backup

Level Up - Data - Backup



Wie oft und welche
Art von Backup ?

Level Up - Data - Backup



Backup Server

- 1x pro Woche inkrementell
- 1x pro Monat vollständig

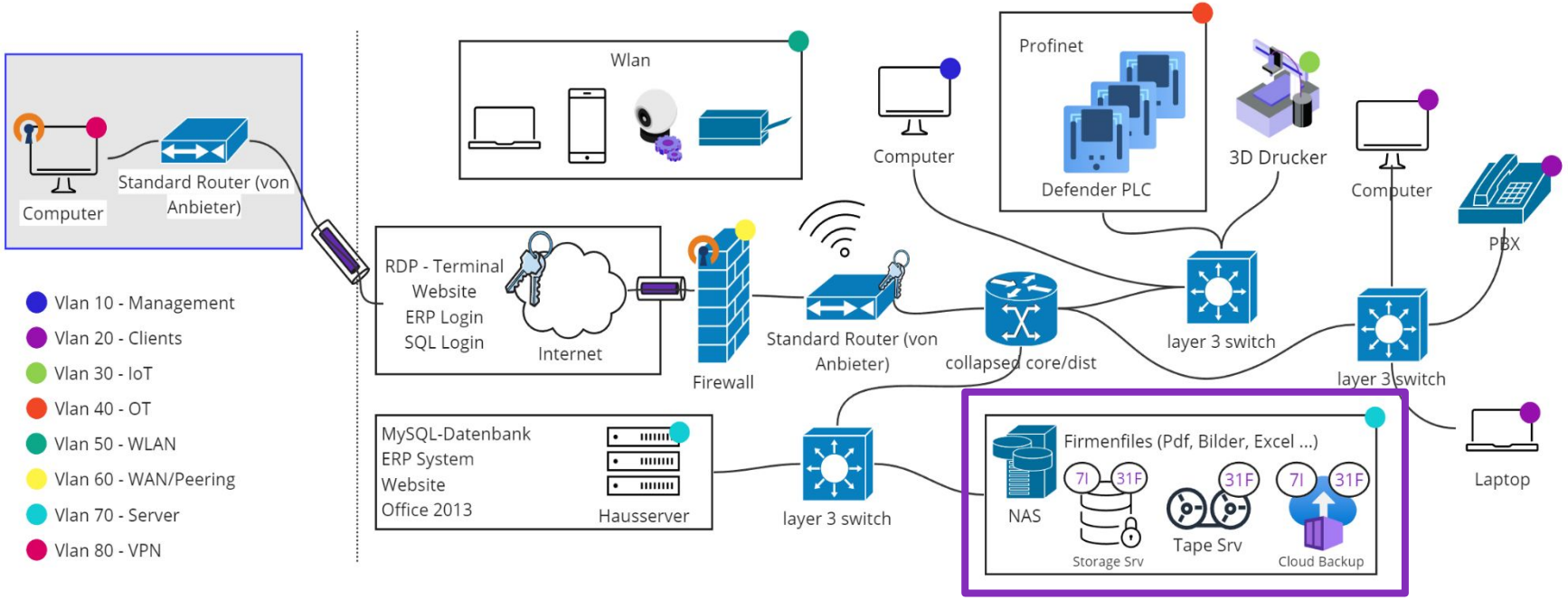
Tape Server

- 1x pro Monat vollständig

Cloud

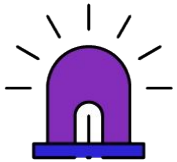
- 1x pro Woche inkrementell
- 1x pro Monat vollständig

Level Up - Data - Backup



http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Level Up - Data



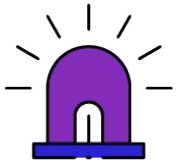
1. Wir brauchen ein vernünftiges Backup ✓
2. Der Zugriff auf unsere Daten muss abgesichert werden
3. Wir brauchen ein Management für unsere Passwörter

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Backup Strategien, Redundanz, Access Management (RBAC), Passwordsafe

Level Up - Data



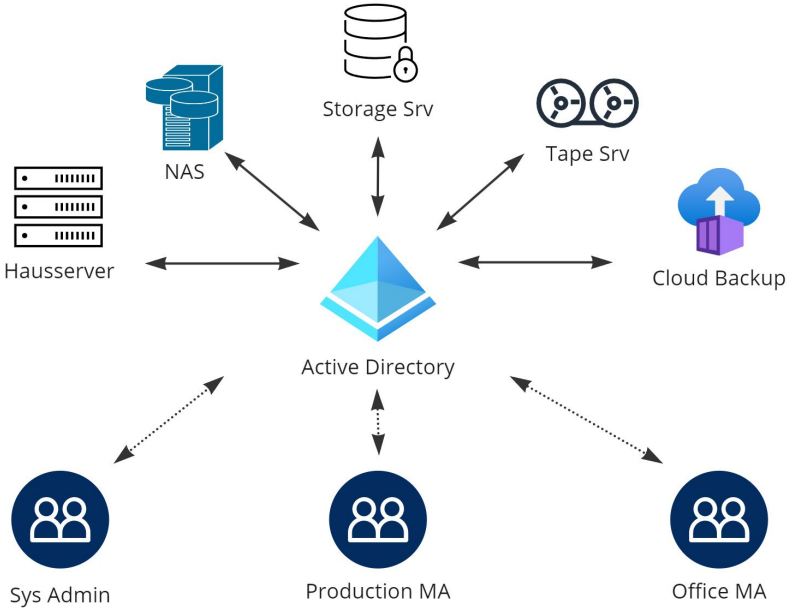
1. Wir brauchen ein vernünftiges Backup ✓
2. Der Zugriff auf unsere Daten muss abgesichert werden
3. Wir brauchen ein Management für unsere Passwörter

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Backup Strategien, Redundanz, Access Management (RBAC), Passwordsafe

Level Up - Data - Access

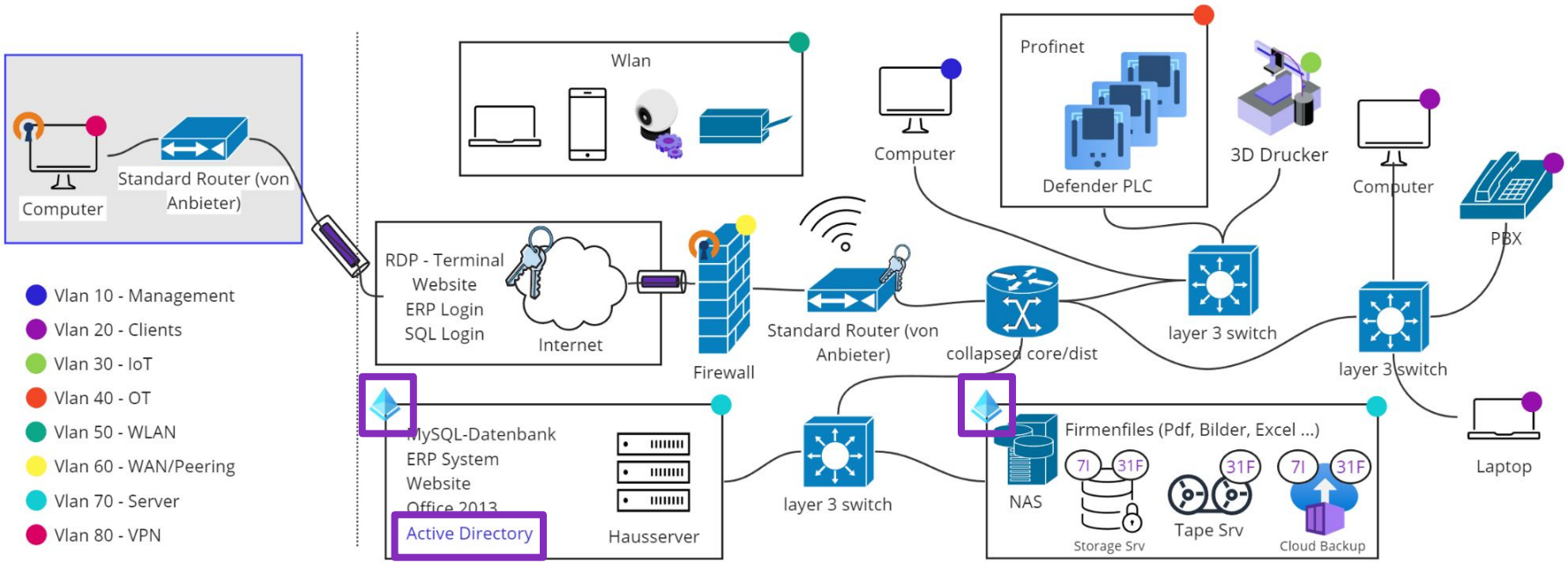


Role Based Access

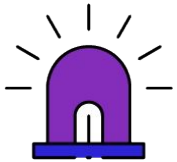
- Für unser Beispiel mit AD als Identity Source
- Kommunikation traditionell über LDAPS
- Besser nur grobe RBAC mit flacher Hierarchie anstatt schlecht gewartete !

https://proton.me/blog/3-2-1-backup#:~:text=The%20idea%20is%20that%20you,of%20something%20than%20you%20need.

Level Up - Data - Access



Level Up - Data



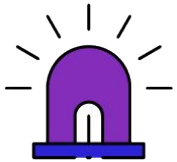
1. Wir brauchen ein vernünftiges Backup ✓
2. Der Zugriff auf unsere Daten muss abgesichert werden ✓
3. Wir brauchen ein Management für unsere Passwörter

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Backup Strategien, Redundanz, Access Management (RBAC), Passwordsafe

Level Up - Data



1. Wir brauchen ein vernünftiges Backup ✓
2. Der Zugriff auf unsere Daten muss abgesichert werden ✓
3. Wir brauchen ein Management für unsere Passwörter

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: Backup Strategien, Redundanz, Access Management (RBAC), Passwordsafe

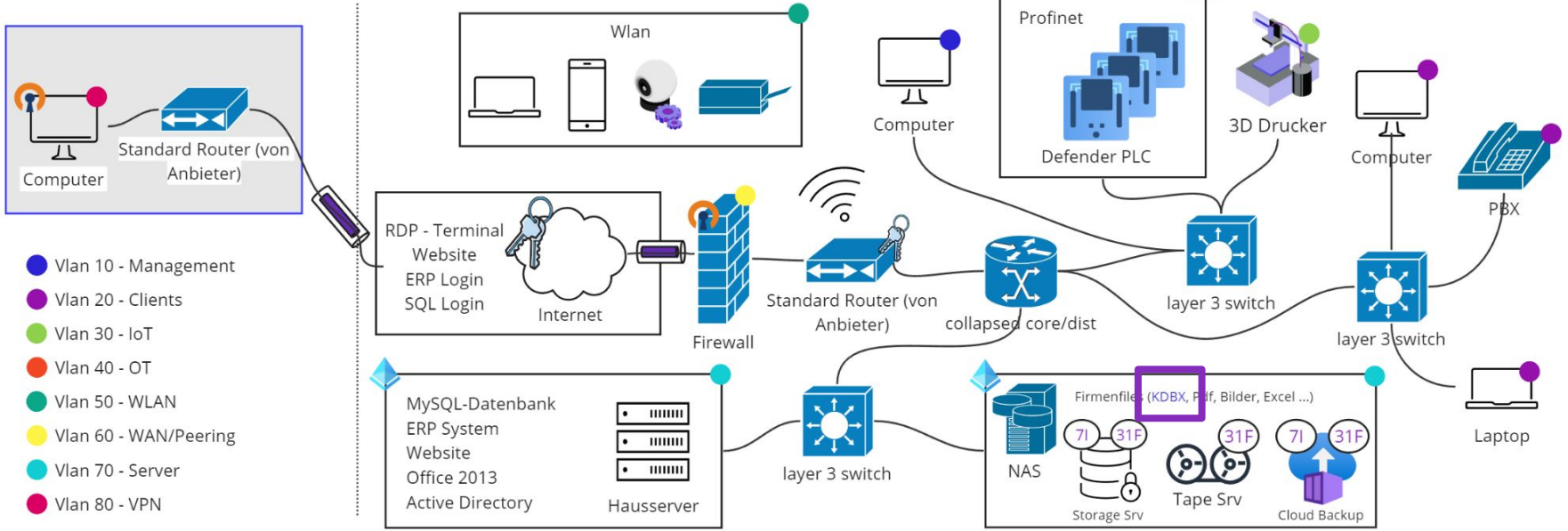
Level Up - Data - Passwordsafe

Password Safe Best Practises

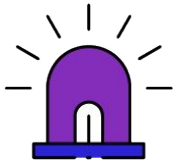
- MFA verwenden
- Passwörter nur verwenden wenn AD Auth nicht möglich
- Trennung zwischen Service und Account Passwörtern

https://proton.me/blog/3-2-1-backup#:~:text=The%20idea%20is%20that%20you,of%20something%20than%20you%20need.

Level Up - Data - Passwordsafe



Level Up - Data



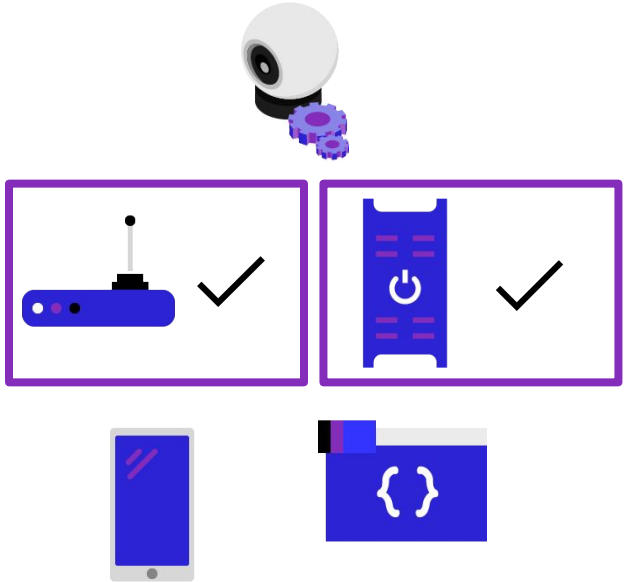
1. Wir brauchen ein vernünftiges Backup ✓
2. Der Zugriff auf unsere Daten muss abgesichert werden ✓
3. Wir brauchen ein Management für unsere Passwörter ✓

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

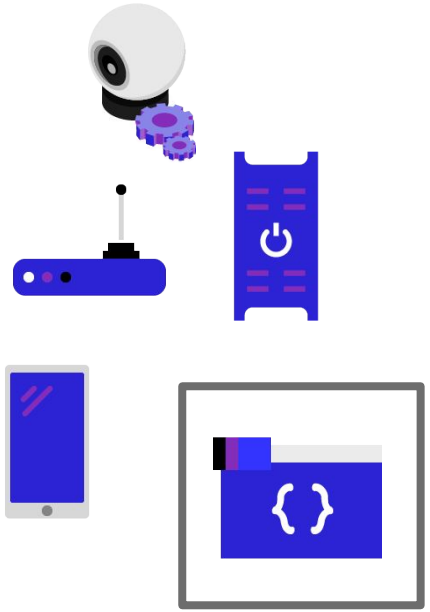
Hinweise: Backup Strategien, Redundanz, Access Management (RBAC), Passwordsafe

Level Up - Action Plan



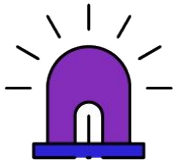
Wir haben unsere Data Architektur erfolgreich aufs nächste Level gehoben 🚀

Level Up - Action Plan



Schauen wir uns als nächstes das Topic Applications an.

Level Up - Applications



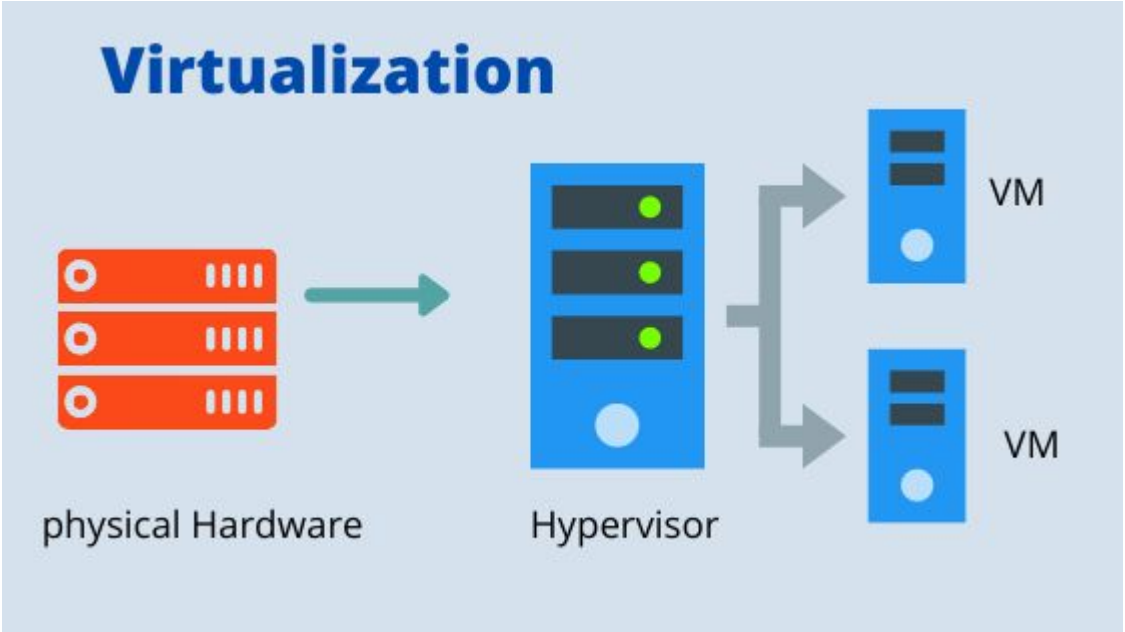
1. Unser Hausserver ist im Moment ein Single Point of Failure - wie können wir das ändern ?
2. Wie können wir unsere Applikationen voneinander isolieren ?

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

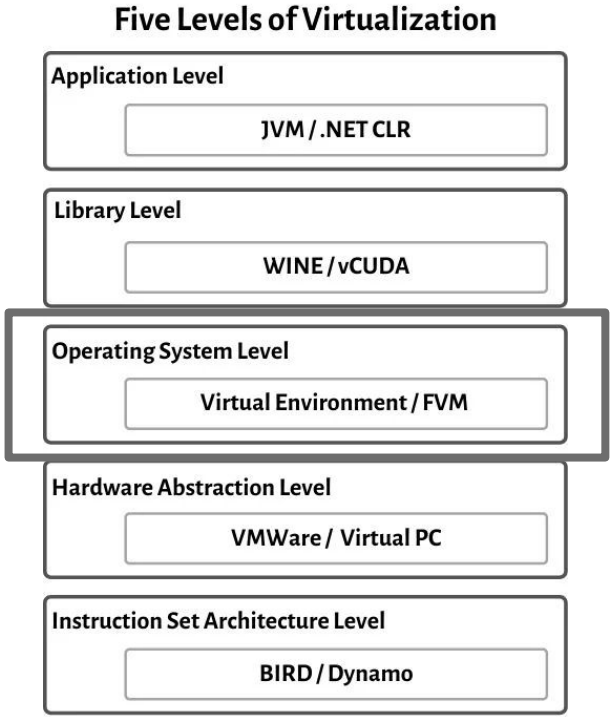
Hinweise: Hochverfügbarkeit, Virtualisierung, Hypervisor

Level Up - Applications - Virtualisierung



https://proton.me/blog/3-2-1-backup#:~:text=The%20idea%20is%20that%20you,of%20something%20than%20you%20need.

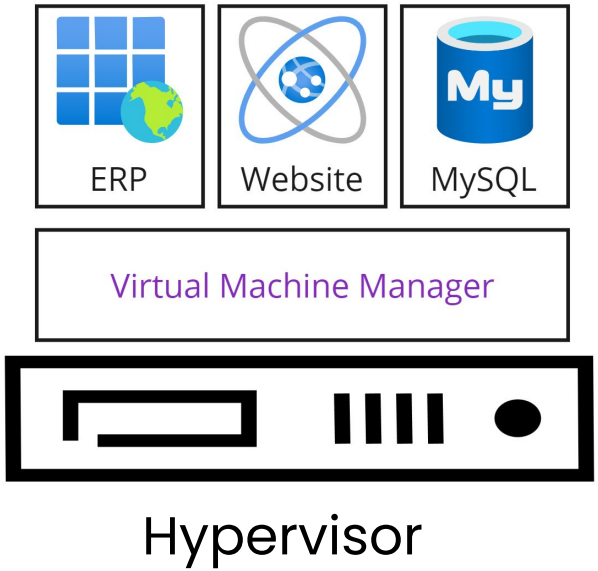
Level Up - Applications - Virtualisierung



https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

OS Level als guter Einstieg

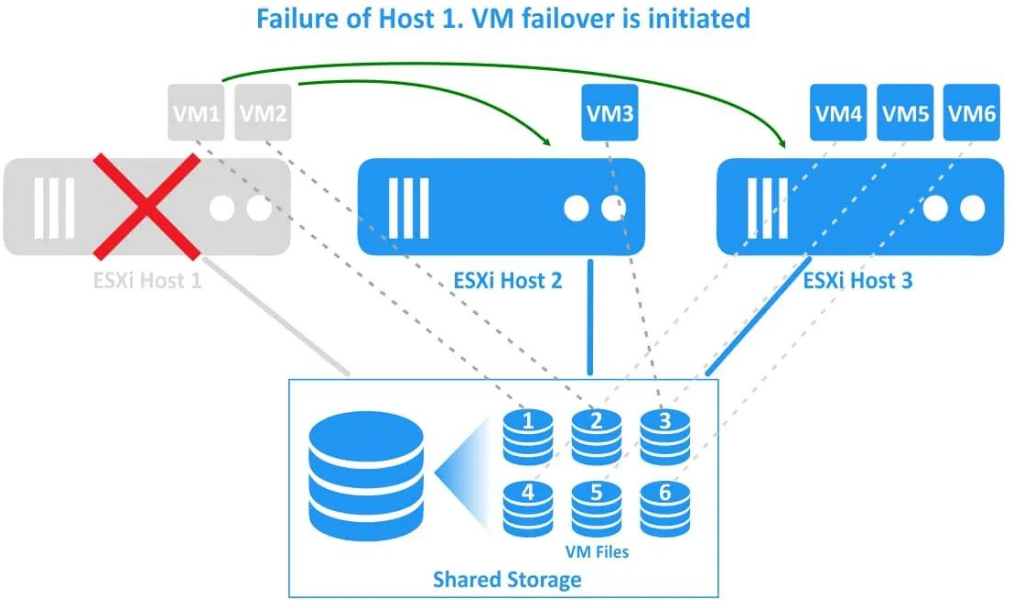
Level Up - Applications - Hypervisor



Angepasst auf unseren Fall z.B. mit Linux und Windows VMs.

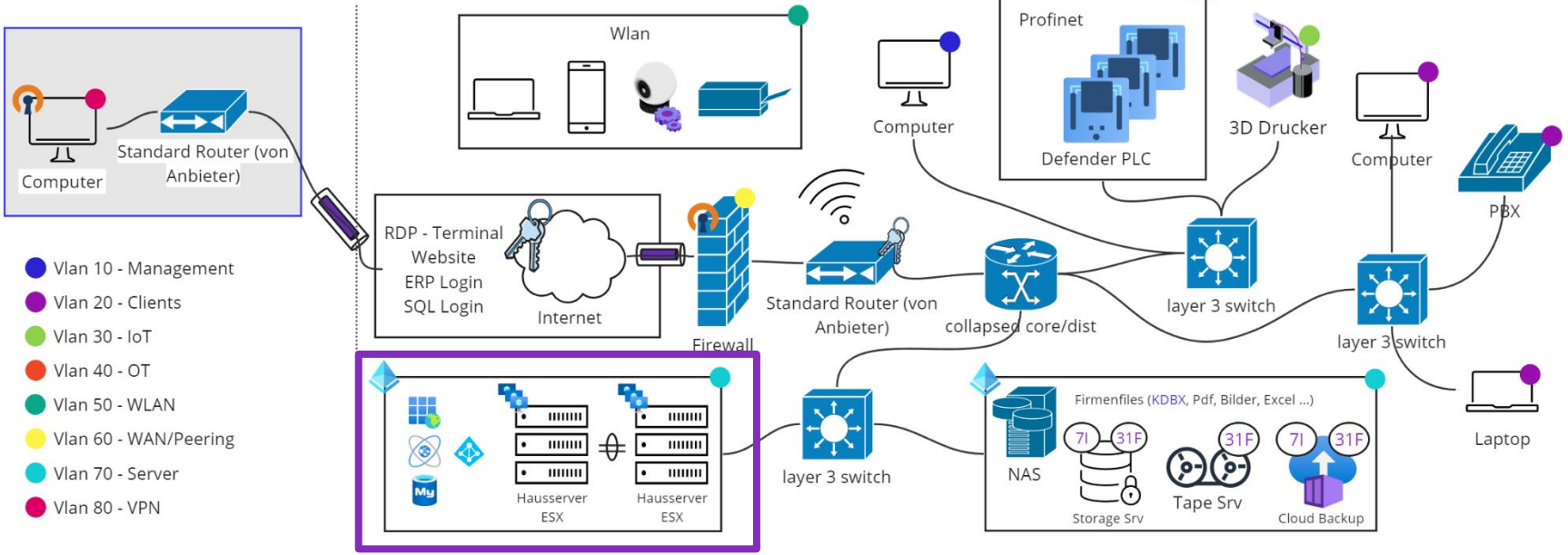
https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up - Applications - High Availability

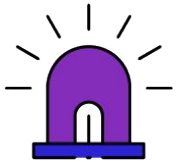


https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up - Applications - Virtualisierung



Level Up - Applications



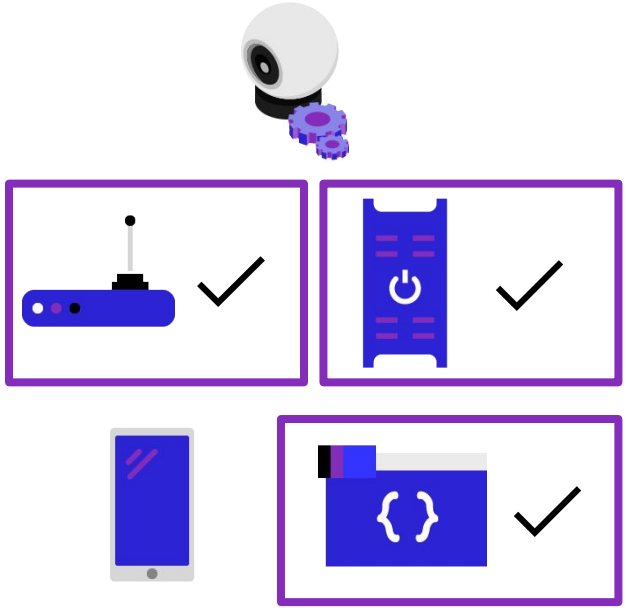
1. Unser Hausserver ist im Moment ein Single Point of Failure - wie können wir das ändern ? ✓
2. Wie können wir unsere Applikationen voneinander isolieren ? ✓

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

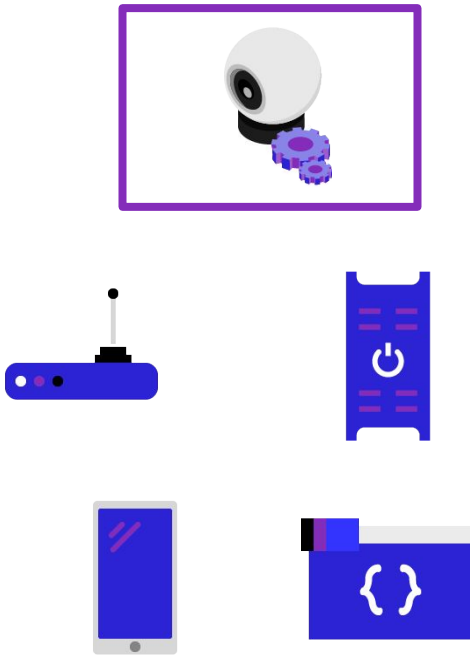
Hinweise: Hochverfügbarkeit, Virtualisierung, Hypervisor

Level Up - Action Plan



Unsere Application Architektur steht nun auch 🚀

Level Up - Action Plan

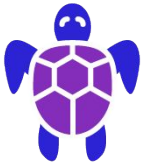


Auf ins nächste Topic OT Security 🚀

Wisst ihr was OT Security ist ?

OT Security - Introduction

Level Up - OT Security



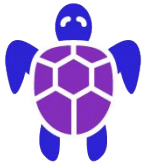
OT Cybersecurity Best Practices

Some of the OT security best practices for implementing a reliable protection system include:

1. Network mapping and connectivity analysis
2. Detection of suspicious activities, exposures, and malware attacks
3. Implementing a zero-trust framework
4. Aligning the right remote access tools
5. Controlling identity and access management (IAM)

https://www.fortinet.com/resources/cyberglossary/ot-security-best-practices

Level Up - OT Security



OT Cybersecurity Best Practices

Some of the OT security best practices for implementing a reliable protection system include:

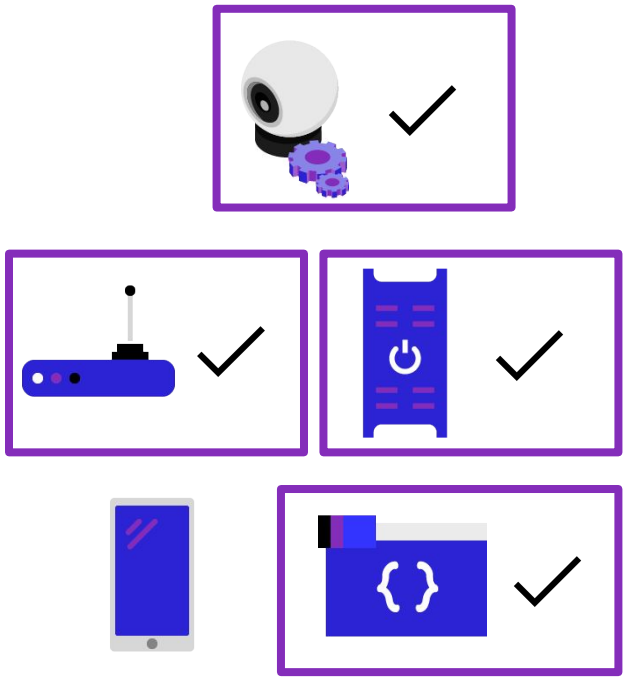
1. Network mapping and connectivity analysis
2. Detection of suspicious activities, exposures, and malware attacks
3. Implementing a zero-trust framework
4. Aligning the right remote access tools
5. Controlling identity and access management (IAM)

Basis haben wir umgesetzt!

Themen wie IAM folgt im nächsten Level.

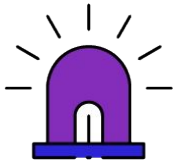
https://www.fortinet.com/resources/cyberglossary/ot-security-best-practices

Level Up - Action Plan



Auf in das letzte Topic um unser Level Up abzuschließen 🚀

Level Up - Communication und Collaboration



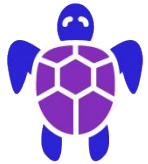
1. Wie gewährleisten wir eine sichere Kommunikation auf privaten Devices?
2. Wie verhindern wie die Nutzung von WhatsApp und Zoom per privaten Accounts ?

Überlegt in Teams

- Welche Komponenten müssen hinzugefügt oder ausgetauscht werden ?
- Welche Technologien können dafür genutzt werden ?
- Skizziert auf dem Papier mögliche Lösungen

Hinweise: SaaS Lösung, Cloud, Migration

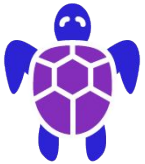
Level Up - Communication und Collaboration



Google Workspace

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

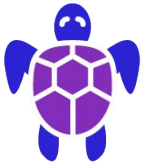
Level Up - Communication und Collaboration



Leider gibt es nur wenige Alternativen zu den gezeigten Lösungen, die mit starken Kompromissen einhergehen!

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

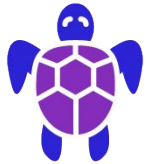
Level Up - Communication und Collaboration



Aus Security Sicht ist ein Umstieg auf ein SaaS Communication Lösung definitiv empfehlenswert.

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

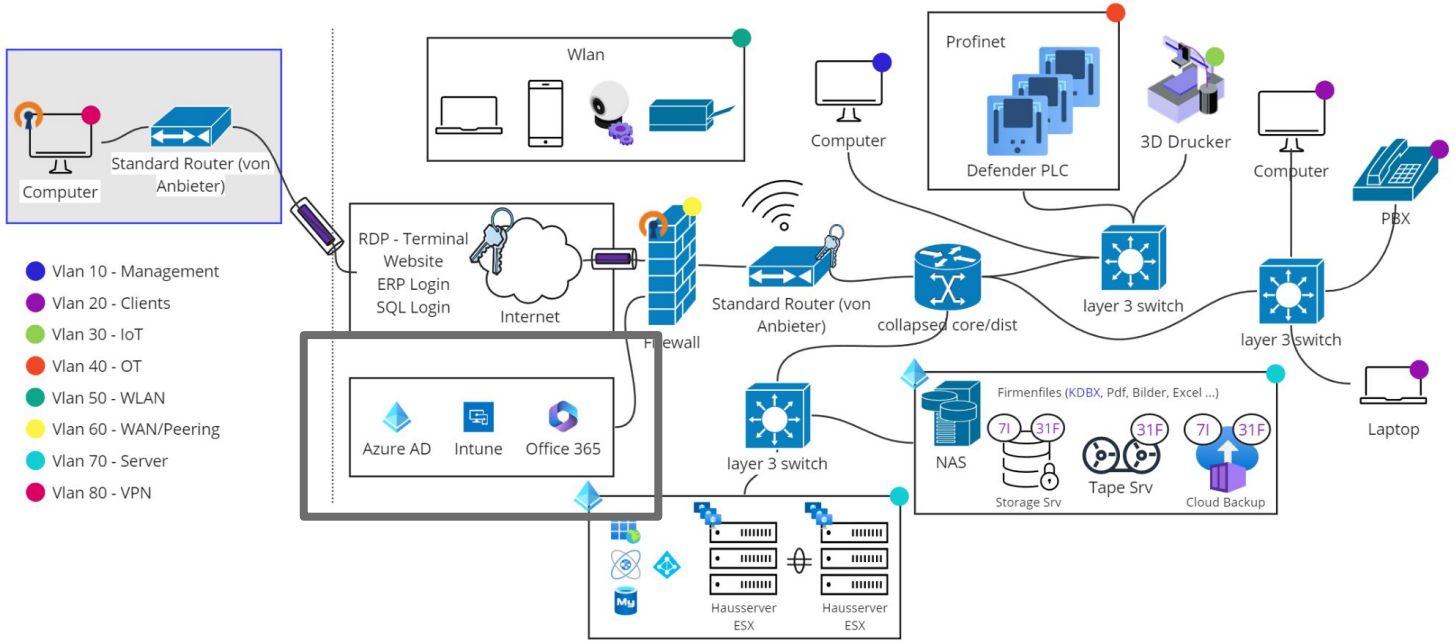
Level Up - Communication und Collaboration

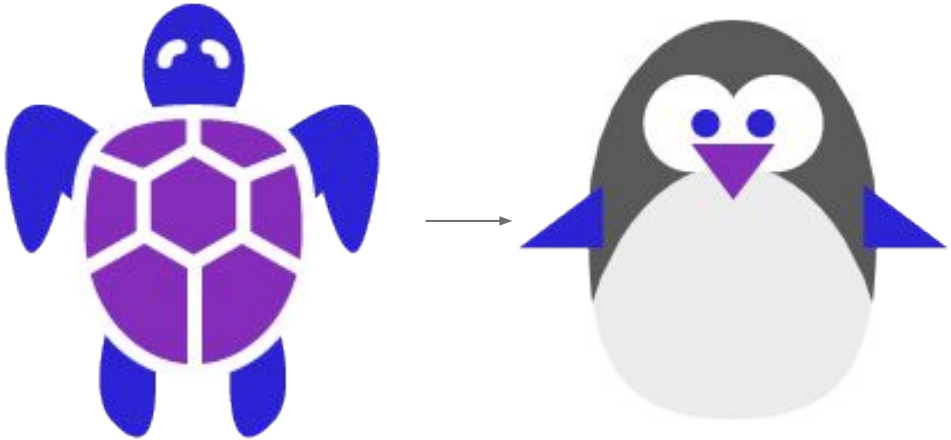


Für unser Beispiel:
Bei richtiger Konfiguration, ist ein sicherer Chat, Kollaboration und VT gegeben.

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

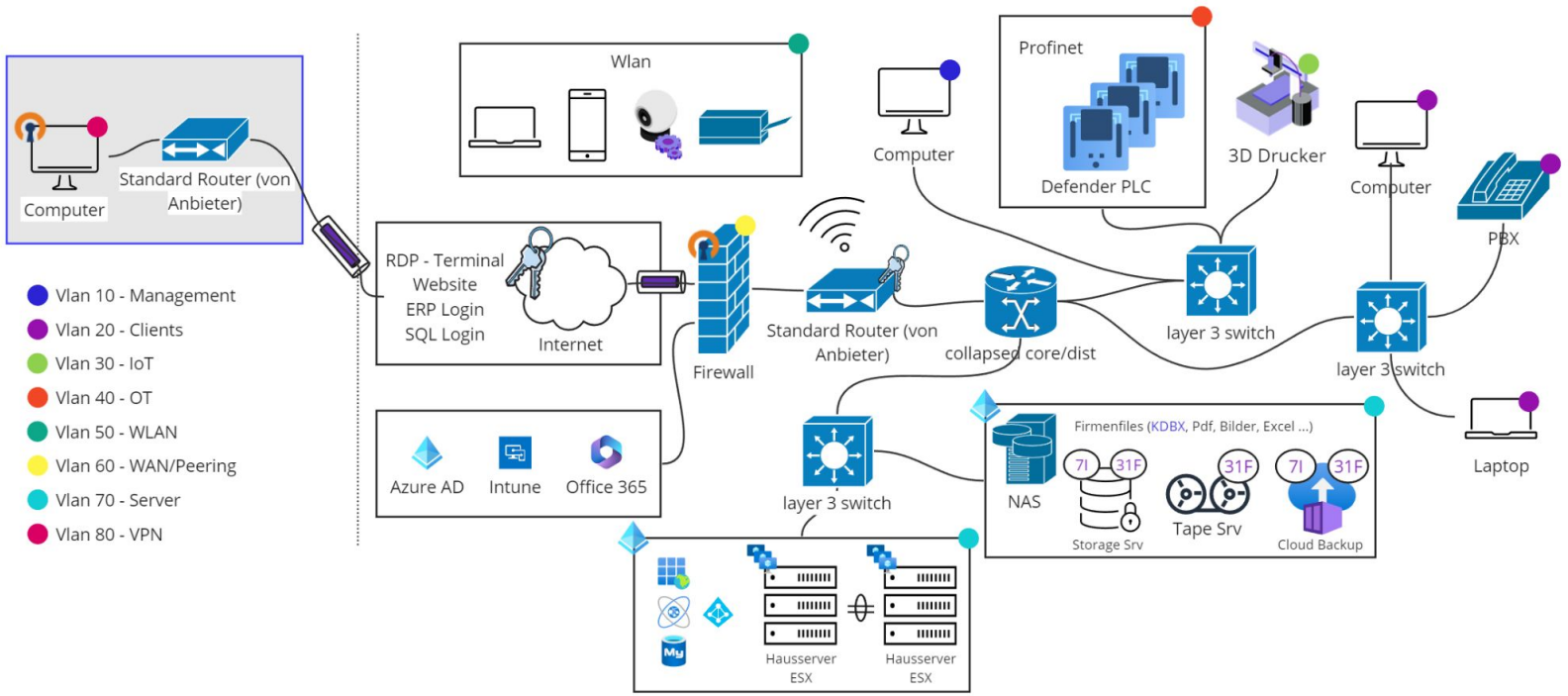
Level Up - Communication und Collaboration





Level Up geschafft! 🚀

Smart Solution – Level 1 – IT Architektur



Level Up

Was denkt ihr, wo gibt es jetzt noch Verbesserungspotential ?

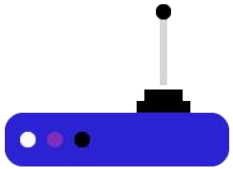
https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up

Gehen wir gemeinsam im Überblick grob ein paar Möglichkeiten durch !

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

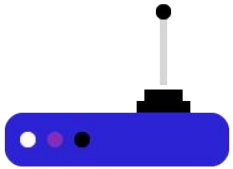
Level Up - Netzwerk



Network Access Control

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up - Netzwerk - NAC

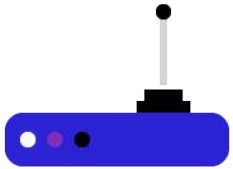


Network Access Control

- Für jeden der sich mit Netzwerk verbindet muss entschieden werden, auf welche Ressourcen er zugreifen darf.

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

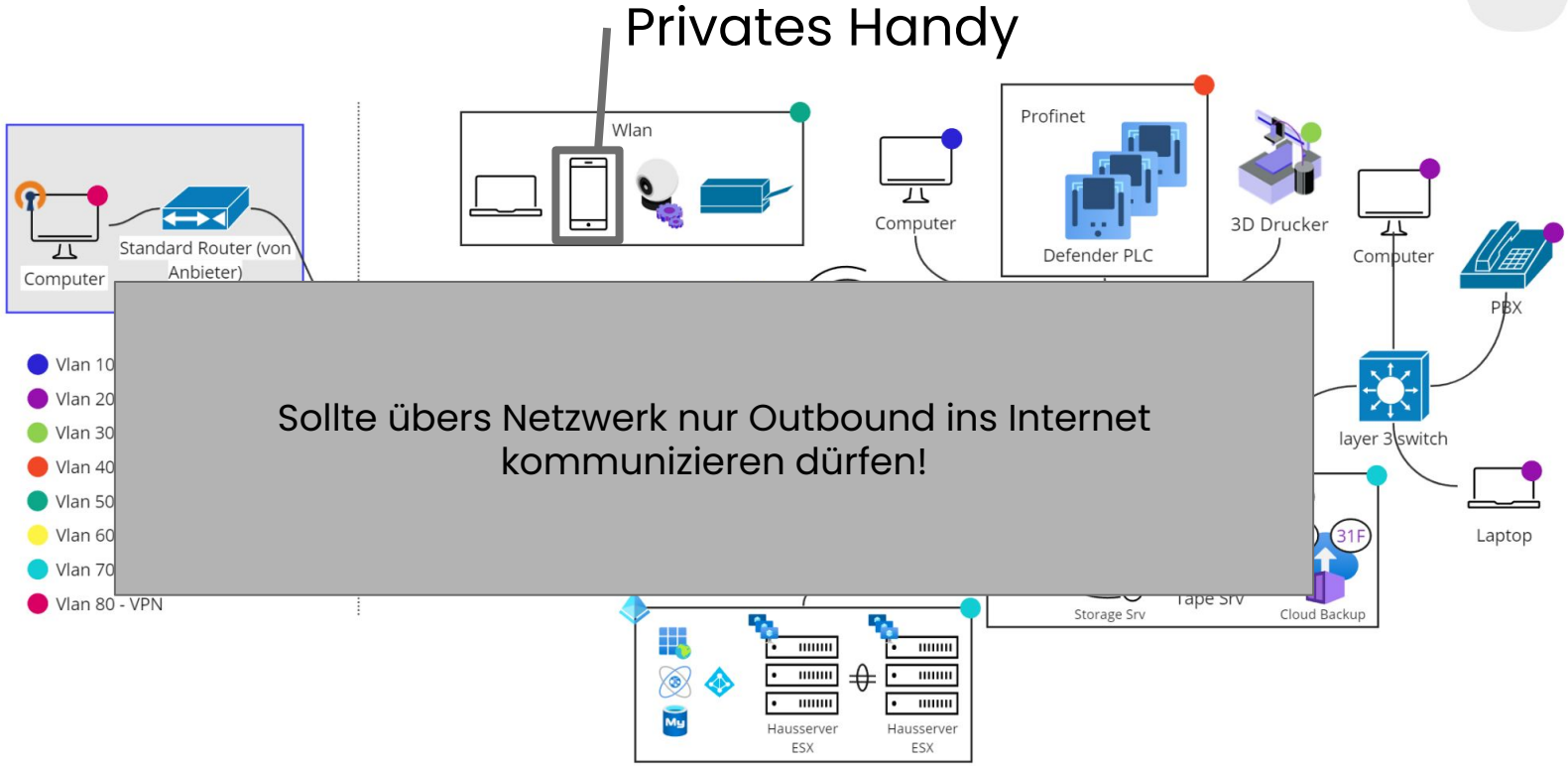
Level Up - Netzwerk - NAC



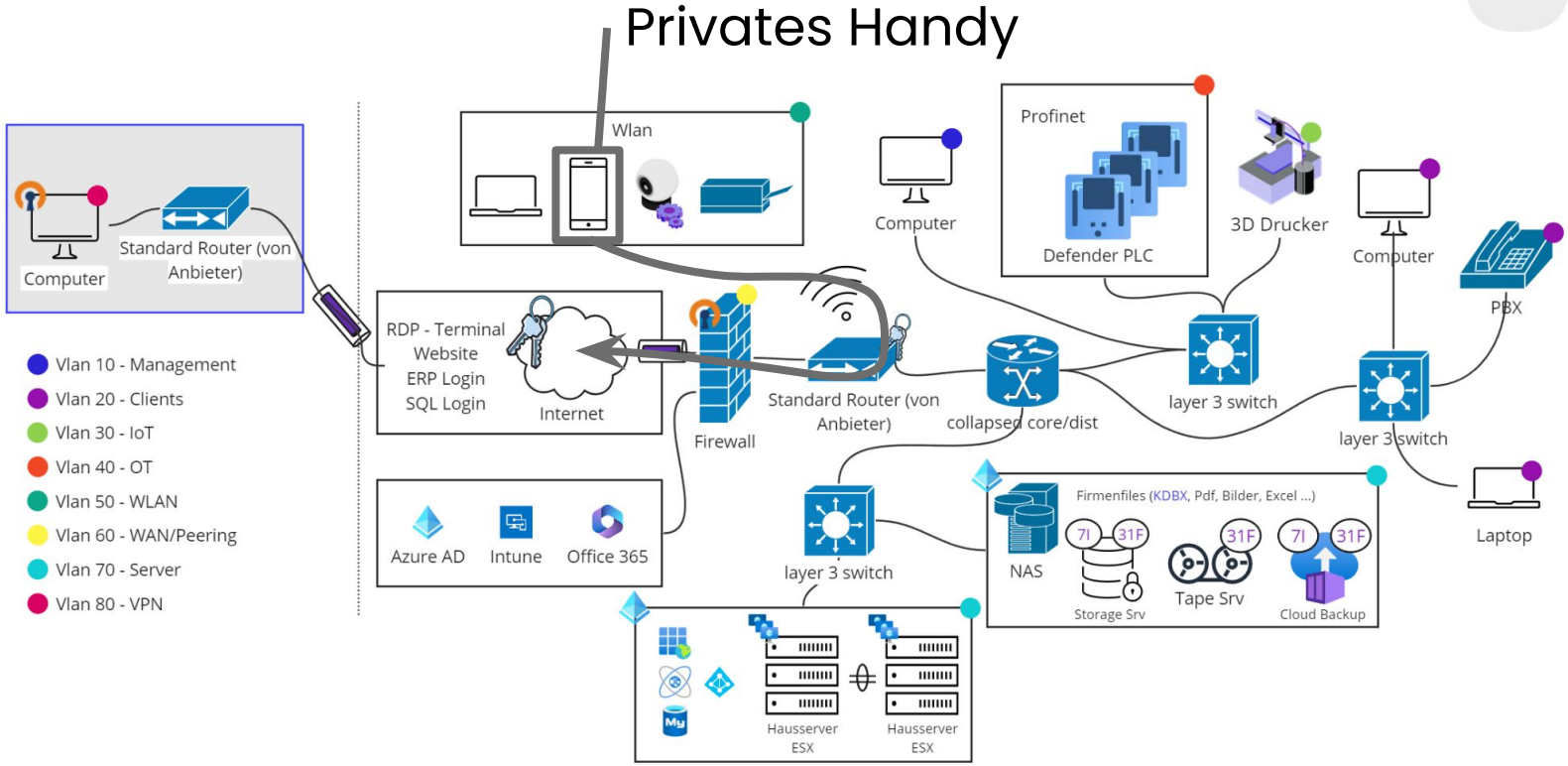
Wie würde das bei unserem Beispiel aussehen ?

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

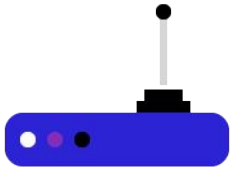
Level Up - Netzwerk - NAC



Level Up - Netzwerk - NAC



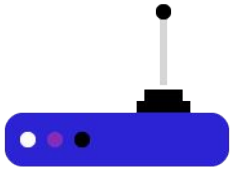
Level Up - Netzwerk - NAC



Woher weiss ich welches Device das ist ?
Wie kann ich bestimmen welchen Zugriff es im Netzwerk hat ?

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

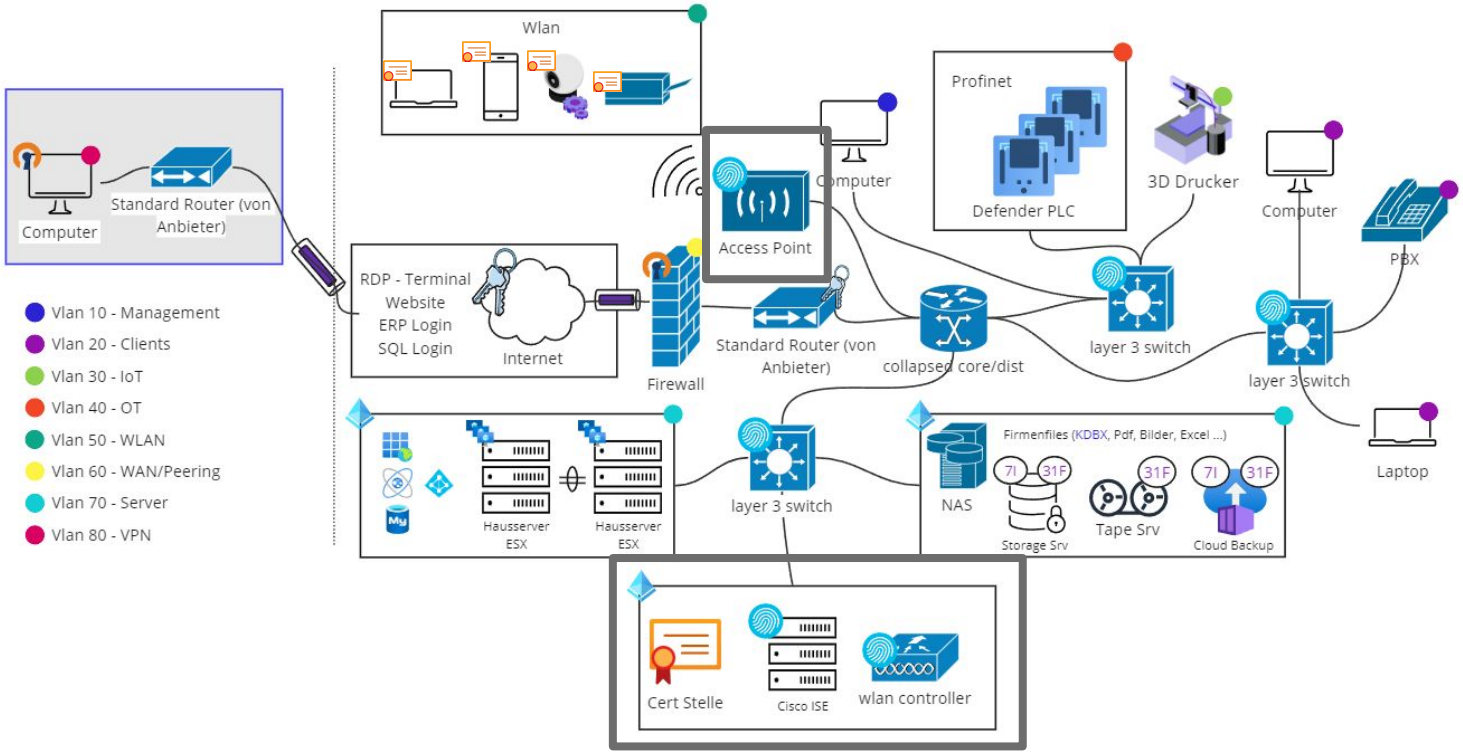
Level Up - Netzwerk - NAC



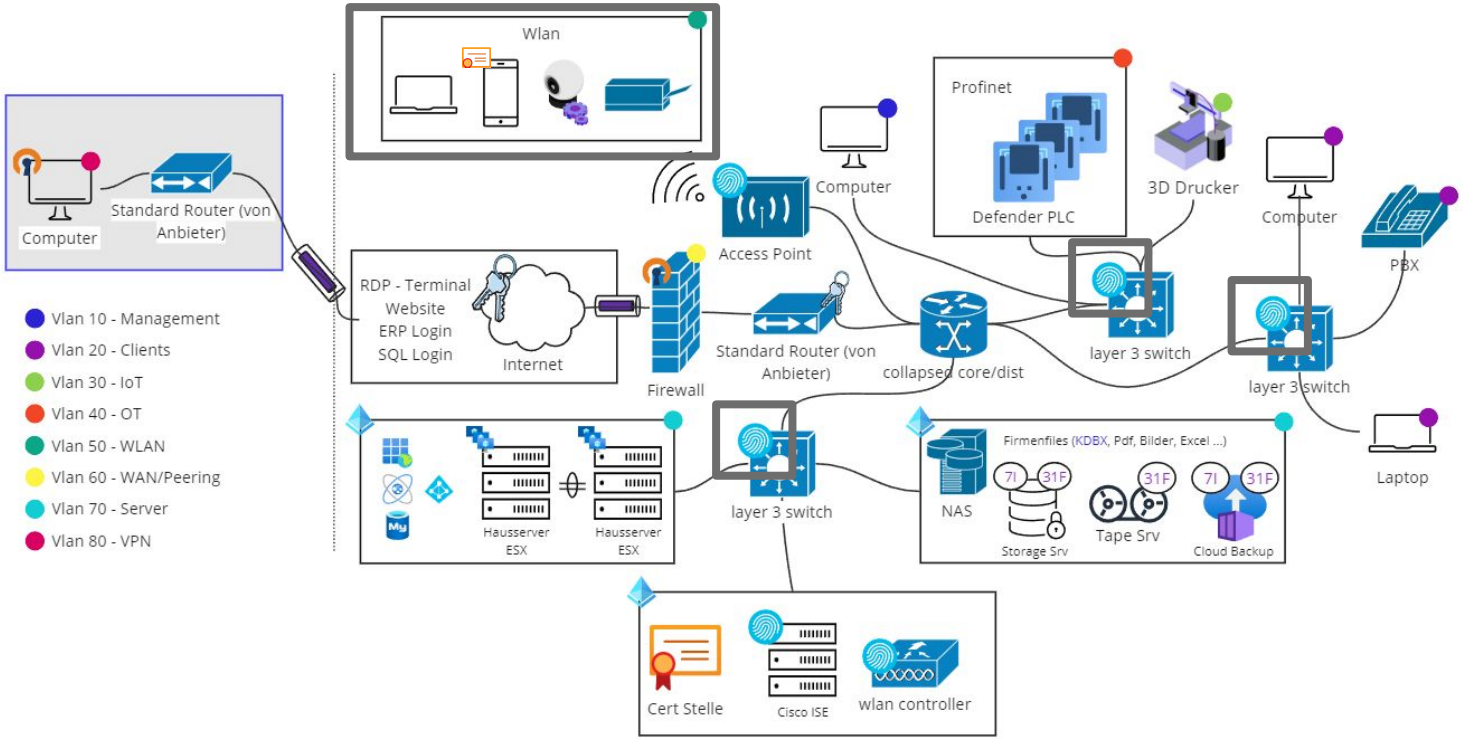
1. Identity Service
   a. Source Pool mit allen Identities (Devices, Benutzer…)
2. Zertifizierungsstelle
   a. Identity Nachweis + Permit Antrag (Was darf die Identity - vgl. mit Reisepass)
3. Zugriff Policies & AAA
4. Enrollment auf SecDevices

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up - Netzwerk - NAC



Level Up - Netzwerk - NAC



Level Up - OT

Threat Detection and Response

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up - OT - TDR

Wisst ihr was TDR ist und wie es funktioniert ?

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up - OT - TDR

Prozess zur Identifizierung, Bewertung und Minderung von Cyber-Bedrohungen und -Vorfällen.

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up - OT - TDR

Bestehend aus:

1. Erkennung: Identifikation von Anomalien und potenziellen Bedrohungen.
2. Untersuchung: Analyse und Bewertung der identifizierten Bedrohungen.
3. Reaktion: Maßnahmen zur Eindämmung und Beseitigung der Bedrohung.

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up – OT – TDR

1. **Erkennung**

- Anomalien: z.B. plötzlicher Datenanstieg zu einer SPS
- Vulnerabilities: Scannen von ICS Devices auf Schwachstellen

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up - OT - TDR

2. Untersuchung

- Vorfallsreaktionspläne: z. B. bei Malware auf einem Controller.
- Forensische Analyse: z. B. durch Log-Analyse im SCADA-System.

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up – OT – TDR

3. **Reaktion**

- Isolation und Segmentierung: z. B. eines infizierten Sensors (unser Smartmeter).
- Restore: z.B. wenn Ransomware Angriff eintritt

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up – OT – TDR

Mit welchen Tools kann man TDR umsetzen ?

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up – OT – TDR

Die Liste ist lange:

- Intrusion Detection Lösung
- SIEM Lösung
- EDR Lösung
- XDR Lösung
- Next Gen. Firewalls
- Vulnerability Scanner

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

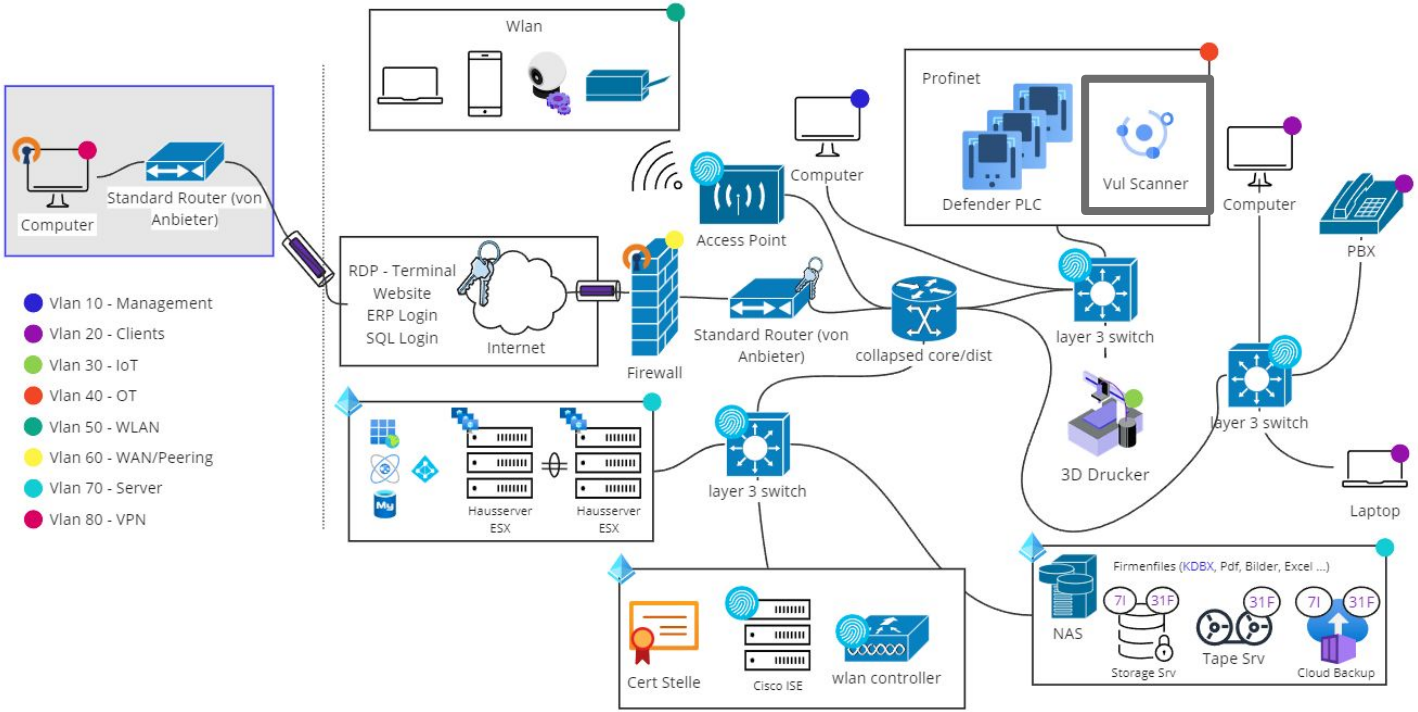
Level Up - OT - TDR

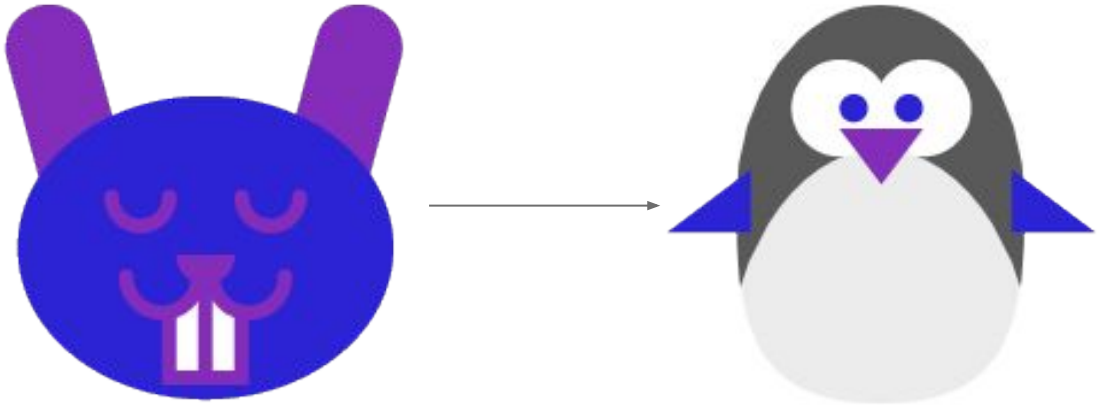
Für unser Use Case ausreichend als kleines Level Up:

- Vulnerability Scanner

https://www.hitechnectar.com/blogs/virtualization-implementation-levels/

Level Up – OT – TDR





Level Up geschafft! 🚀

Mastering Compliance – ein ganzheitliches Security Bild

Erarbeitung einer soliden Grundlage für dein Unternehmen
Anhand der Cyber Trust Austria Maßnahmen

Lernpfad

FA01: Erweiterte Security Techniken und Tools für Unternehmen

FA02: Security Architekturen für Unternehmens-ressourcen (KMU)

FA03: Cloud and Application Security Strategien

FA04: Compliance - Ganzheitliche Cybersecurity anhand von Cyber Trust Austria

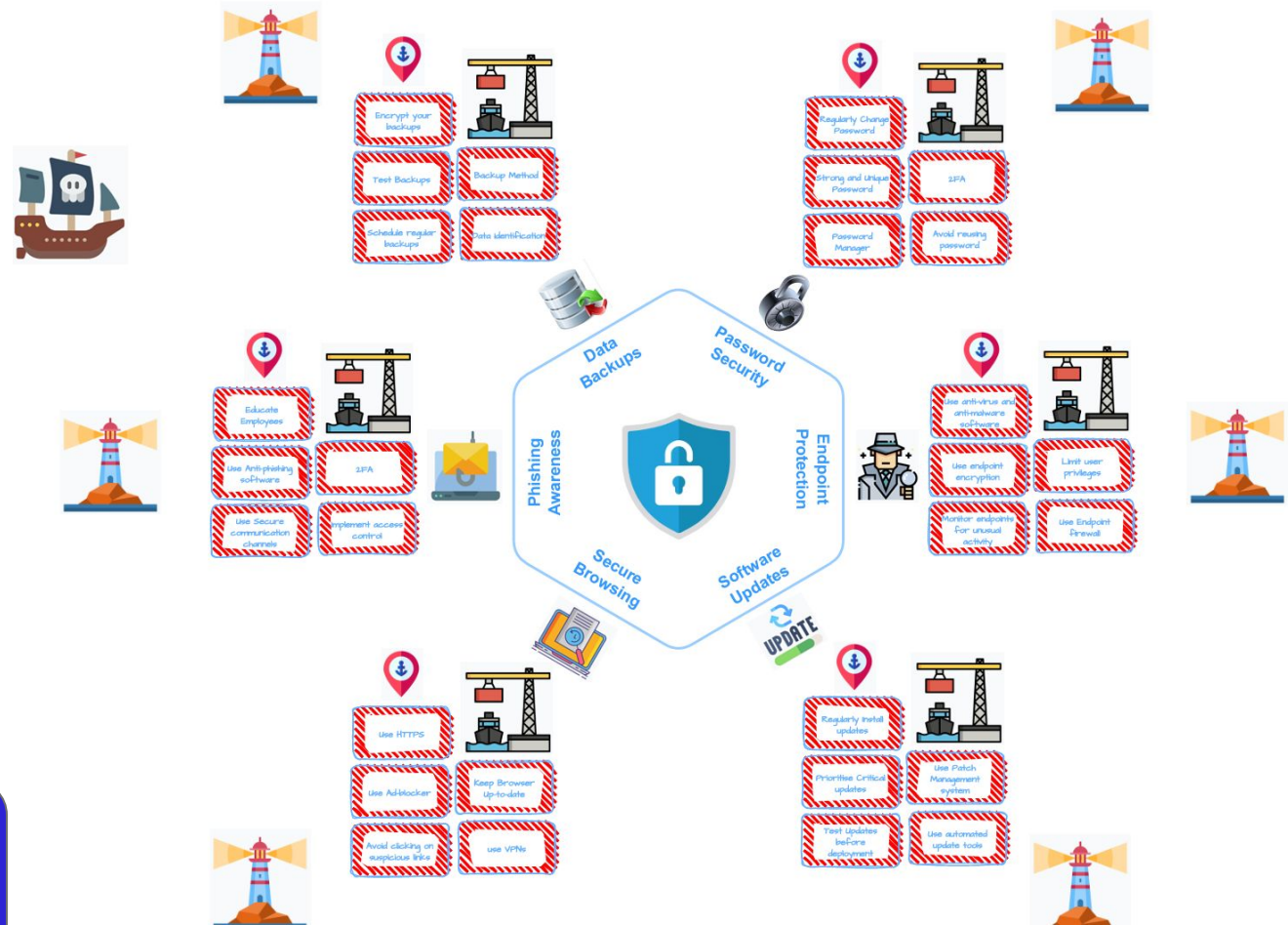
Lernziele

1. Ein Verständnis dafür entwickeln, was ganzheitliche Cybersicherheit ist
2. Verschiedene Anlaufstellen für Security Maßnahmen kennenlernen
3. Das Cyber Trust Austria Zertifizierungsmodell verstehen
4. Maßnahmen des Cyber Risk Rating Schemas für das eigene Unternehmen ableiten können und notwendige Maßnahmen treffen

Recap – Ganzheitlicher Ansatz von Cybersecurity

Security ist eben Überall und kann nicht rein technisch gelöst werden!

Cyber Security 101



Quelle: https://linkedin.com/
Gruppe: Information Security Network

Was nehmen wir uns mit?

Security sollte immer ganzheitlich betrachtet werden und nicht nur Punktuell: Security is Everywhere

Stellt euch das ganze einfach so vor: Security ist wie die Schale einer Banane 🍌 - Wenn die Schale wegfällt hält die Frucht nicht lange

Ein Sicherheitsbewusstsein sollte bei jeder Person eigentlich ein Teil des “Hausverstandes” sein.

Recap – Was können KMUs machen um nach außen hin ihre Security Bemühungen zu zeigen

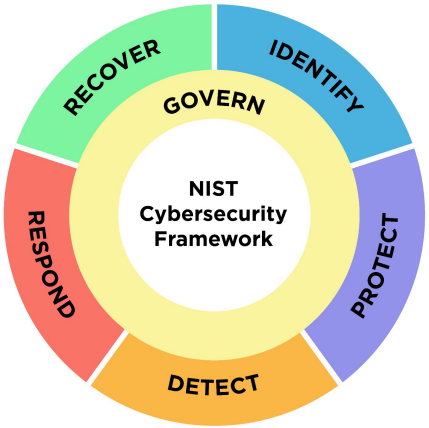
Alternativen zu IEC, TISAX, ISO, etc.

Security Zertifizierungen nach Standards/Normen

Es gibt sehr viele Standards und Normen für Cybersicherheit. Das Problem ist, sie sind für Enterprises ausgelegt!

Beispiele:

- ISO 27001
- IEC 62443
- NIST SP 800 - CSF
- CIS Controls
- etc.



Das kann kein KMU vernünftig Umsetzen

Probleme:

- Know-How Mangel
- Budget für die Umsetzung
- Kauf von Hardware
- Cybersecurity meistens ein neues Thema
- Standards sind viel zu Breit
  - Passt nicht zum KMU scope!
  - Passt auch nicht zu Budget!

Was jetzt wenn wir Kunden oder einer Versicherung etwas zeigen müssen?

Bsp. Indirekte Betroffenheit von NIS-2 durch → Lieferkette

Lösungsansätze und Empfehlungen

Wenn man wirklich betroffen ist durch die Lieferkette bzw. man eine Versicherung etwas vorlegen muss, sollte man sich überlegen wie man belegen kann, dass im Unternehmen gewisse Maßnahmen umgesetzt werden.

Hilfestellungen:

- Förderung https://www.ncc.gv.at/foerderungen.html
- www.it-safe.at → Informationen rund um das Thema Cybersicherheit im Unternehmen
- IT-Sicherheitsexperten (WKÖ)

Zertifizierung → CyberRisk Rating Österreich

Folgende Ratings stehen hierbei zur Auswahl:

- B-Rating:
  Basis-Cyber-Schutzniveau,
  umfasst 14 Anforderungen

- A-Rating: umfasst alle 25 Anforderungen des KSÖ

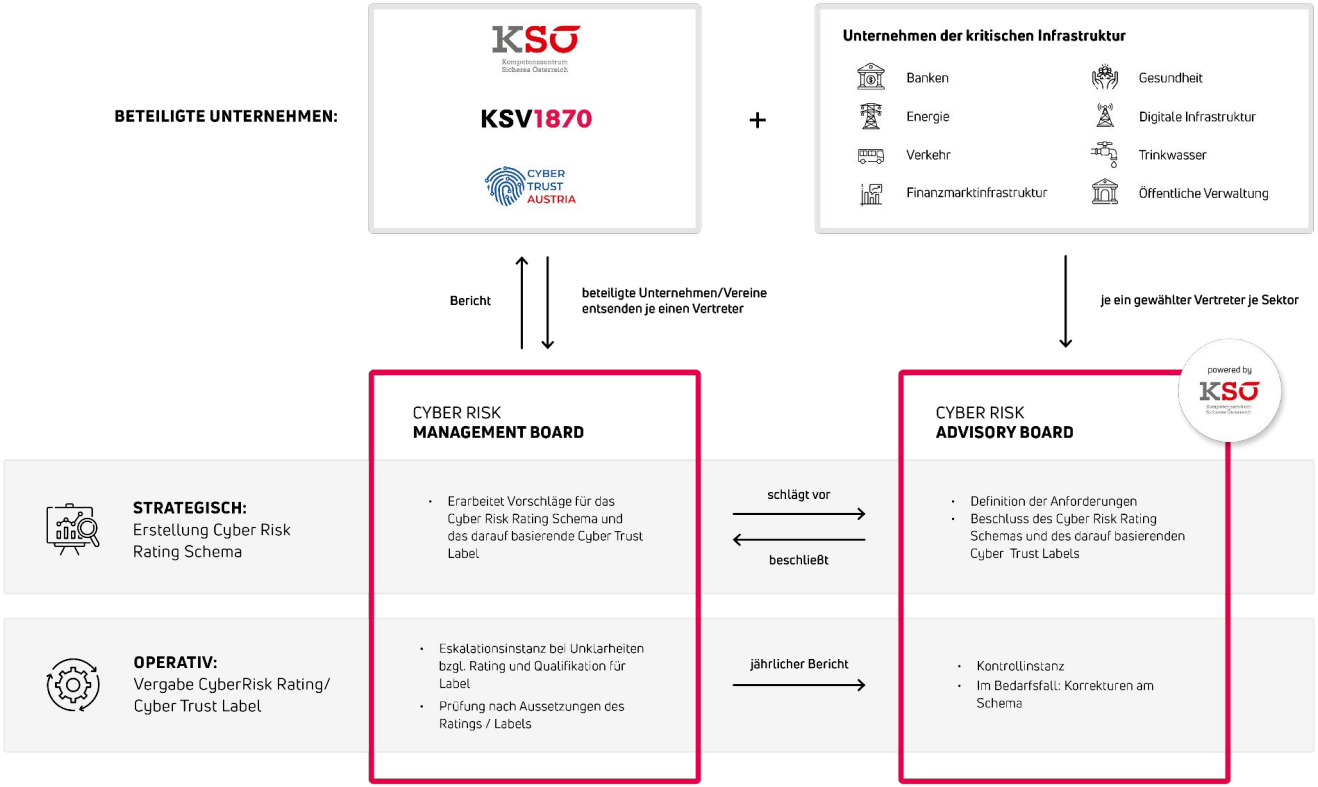
- "A+"-Rating: bietet zusätzlich einen Bericht eines Audit-Partners

KSÖ
Kompetenzzentrum
Sicheres Österreich

CYBER
TRUST
AUSTRIA

KSV1870

CyberRisk Rating Österreich → Qualität?



Blick in das Schema

Kompetenzzentrum Sicheres Österreich

CYBER TRUST AUSTRIA

Cyber Risk Rating & Cyber Trust Label

Schema Policy 2024

Recap Call mit Cyber Trust Austria Vertreter

Ich hatte einen call mit Cyber Trust Austria und mir wurden einige sachen mitgegeben.

Takeaways Meeting CTA

Die Anzahl der ausgestellten Zertifizierungen/Akkreditierungen steigt ständig an.

Die Beantragung erfolgt über ein Online-Formular und gewisse Dokumente die einzureichen sind.

Cyber Trust Austria & KSV1870 checken dann den Antrag und bewerten das Szenario → Es müssen gewisse Punkte erreicht werden.

Überblick und Ablauf der Zertifizierung

- Online-**Beantragung**
- **Beantwortung** des Online Fragebogens
- **Durchführung** des automatisierten Web Scorings (der angegebenen qualifizierten Domäne)
- **Validierung** der Antworten & Errechnung des vorläufigen Cyber Risk Ratings
- **Möglichkeit zur Klärung** offener Punkte & Richtigstellung
- **Erstellung** des finalen Cyber Risk Ratings
- **Ausstellung** des Labels & Eintrag in die Cyber Trust Label Datenbank

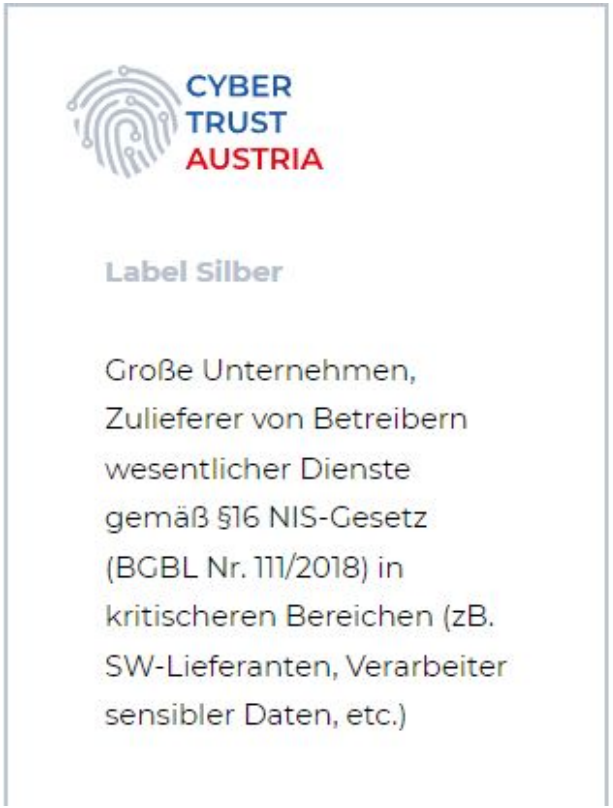
Quelle: https://www.youtube.com/watch?v=h5LhmYimM0Q

B – Rating

- 14 Anforderungen
- Validierte Selbstdeklaration
- 890€
- Vorliegen eines gültigen KSV1870 CyberRisk B-Ratings von 190 oder besser

Quelle: https://www.cyber-trust.at/labeluebersicht/

A - Rating



- 25 Anforderungen
- Validierte Selbstdeklaration
- 1390€
- Vorliegen eines gültigen KSV1870 CyberRisk A-Ratings von 190 oder besser

A+ - Rating

- 25 Anforderungen
- Validierte Selbstdeklaration plus externer Audit
- 1490€ + Auditkosten
- Vorliegen eines gültigen KSV1870 CyberRisk A-Ratings von 190 oder besser

Auditpartner

Anforderungen → Step by Step

Wir gehen jetzt Step by Step das Schema durch

Bitte macht begleitend für euer Unternehmen ein Demo Assessment:
https://demo.cyberrisk-rating.at/

Bzw. schreibt in einem Word mit um das in Zukunft angehen zu können

B1. Informationssicherheitsrichtlinie

Anforderung:
Haben sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für ihr Unternehmen gültig ist?

Anforderungskriterien:
Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (zB. ISO 27001/27002, NIST 800, IT-Grundschutz, IT-Sicherheitshandbuch der WKO u.ä.). Die Richtlinie muss von der Geschäftsführung freigegeben und für alle Mitarbeiter verfügbar sein.

Was ist eine Informations-sicherheits Richtlinie?

Was stellt ihr euch darunter vor und habt ihr sowas in eurem Unternehmen?

B1. Informationssicherheitsrichtlinie - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- ISO 27001 - Control 5.1
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com

B2. Security Schulungen

Anforderung:

Schulen Sie ihre Mitarbeiter regelmäßig in Informationssicherheit?

Anforderungskriterien:

Die Schulung muss die Inhalte der Informationssicherheitsrichtlinie umfassen und auf aktuelle Bedrohungen eingehen. Die Inhalte müssen zumindest folgende Themen umfassen:

- Sicherer Umgang mit Computern und Informationen
- Passwörter richtig auswählen und verwalten
- Sicher im Internet (zB. Nutzung von Firmendaten in KI Diensten und sozialen Netzen)
- E-Mails, Spam und Phishing
- Gefährliche Schadprogramme
- Verhalten und Vorgehen bei Verdacht auf IT-Sicherheitsvorfall

Eine vollständige Schulung muss zumindest beim Eintritt stattfinden und aktualisierte Information muss zumindest alle zwei Jahre kommuniziert werden.

Macht ihr Schulungen bei euch im Unternehmen?

Wenn ja wann, wie oft und mit welchen Unterlagen?

B2. Schulungen - Quellen

- DIN SPEC 27076
- IT-Grundschutz BSI
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com/ratgeber/cybersecurity-schulung-kostenlos/

B3. Security Verantwortung

Anforderung:
Gibt es in ihrem Unternehmen eine oder mehrere benannte Personen, die für das Thema Informationssicherheit zuständig sind?

Anforderungskriterien:
Es muss zumindest eine benannte Person geben, die für das Thema Informationssicherheit zuständig ist, d.h. die Richtlinie erstellt und sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben und sich laufend über Cyberrisken informieren. Diese Tätigkeit kann neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.

Gibt es bei euch einen Security Verantwortlichen?

Wenn ja hat dieser/diese die Notwendigen Ressourcen und das passende Know-How? Das muss nachweisbar sein.

B3. Security Verantwortung

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com/ratgeber/cybersecurity-schulung-kostenlos/ → Ausbildungen in diesem Bereich

B4. Asset Management + Stakeholder

Anforderung:
Pflegen Sie regelmäßig ein Verzeichnis all Ihrer IT-Assets und -Services (inkl. Cloud-Dienste) sowie der damit verbundenen Verantwortlichkeiten?

Anforderungskriterien:

- Es muss ein Verzeichnis aller verwendeten IT-Assets (Systeme, Dienste - Cloud und on premise) geben. Dieses Verzeichnis muss zumindest Name und Version des Systems und den Namen der dafür verantwortlichen Person enthalten.
- Das Verzeichnis muss vollständig und aktuell gehalten werden.

Gibt es bei euch einen Security Verantwortlichen?

Wenn ja hat dieser/diese die Notwendigen Ressourcen und das passende Know-How? Das muss nachweisbar sein.

B4. Asset Management + Stakeholder - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Theoretisch würde hier eine sauber gepflegte Excel Tabelle auch reichen ist jedoch nicht optimal

Short Research: Findet heraus was hier so an tooling verfügbar wäre auch als Open Source Variante.

B5. Permission Konzept + Enforcement

Anforderung:
Verwalten Sie den Zugang zu Ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?

Anforderungskriterien:

- Sowohl der Zugang zu den Anwendungen als auch zu den Dateisystemen muss reglementiert sein und über korrekt gesetzte Berechtigungen sichergestellt werden, dass nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben (Need-to-know).
- Es gibt eine dokumentierte Vorgehensweise zur Vergabe und Entzug von Berechtigungen.

Wie kann man so ein Konzept einfach Umsetzen?

Idee: Anhand einer Matrix der Systeme und “Usergruppen”

B5. Permission Konzept - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Excel → Matrix mit Gruppen und Assets (+ Physischen Access)
- Frage: Welche Technologien haben wir im Einsatz und was supporten diese Technologien im Bezug auf Permission Controls

B6. Passwort Richtlinien & Management

Anforderung:
Verlangen Sie von Ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?

Anforderungskriterien:

Es muss klar beschriebene Mindestkriterien für Passwörter geben, die die Empfehlungen aktueller Standards umsetzen (Passwortstärke, keine Mehrfachverwendung von Passworten, etc.). Referenz: BSI, NIST 800, etc.

Habt ihr hier Regeln definiert?

Wenn ja welche? Rotations? Wiederverwendung? Allgemein?

Was macht hier eigentlich Sinn?

B6. Passwort Richtlinien - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- NIS GV Kennwortsicherheit
- Allgemein wissen wir alle MFA enablen und enforcen wo es geht und bitte Passwort Management Umgebung für Mitarbeiter:innen bereitstellen von Tag 1 an!

B7. Best Practice Security Config

Anforderung:
Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?

Anforderungskriterien:

Es muss ein Dokument geben, das die Anforderungen an die sichere Konfiguration der eingesetzten Systeme beschreibt. Verweise auf Herstellerempfehlungen sind ausreichend. Diese Einstellungen müssen auch auf allen verwendeten Geräten - soweit technisch möglich - tatsächlich umgesetzt sein. Alternativ wird ein Schwachstellenscan vor Inbetriebnahme nachweislich durchgeführt.

Habt ihr alles “vernünftig” konfiguriert?

Habt ihr verwendete Versionen/Betriebssysteme im Überblick?

B7. Best Practice Security Config - Quellen

- Technische Quellen von NIST, CISA, etc.
- Herstellerdokumentation
  - Netzwerk
  - Endgeräte
  - Software
  - etc.
- https://kmusec.com
- Hier sollte zumindest im Asset Management grob hinterlegt sein, welche Security Maßnahmen implementiert sind

B8. Öffentliche Schnittstellen

Anforderung:
Überprüfen Sie - sofern vorhanden - individuell entwickelte, aus dem Internet zugängliche Anwendungen auf Sicherheitslücken vor Inbetriebnahme?

Anforderungskriterien:

Individualsoftware (zB. angepasste Open Source Software, aber nicht Standardsoftware), die aus dem Internet erreichbar ist, muss vor Inbetriebnahme durch einen - auf die Individualsoftware angepassten - Penetration Test auf Schwachstellen geprüft werden.

Habt ihr solche Software im Einsatz?

Wenn ja überlegt ihr über einen Pentest?

B8. Öffentliche Schnittstellen - Quellen

- Technische Quellen von NIST, CISA, etc.
- Pentestinformation Online
- Google: Pentest Österreich
- https://kmusec.com
- Wichtig hierbei handelt es sich um Schnittstellen, auf die im Prinzip “verkauft” werden an Kunden und gleichzeitig

B9. Patch Management

Anforderung:

Aktualisieren Sie alle IT-Systeme und Anwendungen regelmäßig mit Sicherheitsupdates?

Anforderungskriterien:

Regelmäßige Aktualisierung der Systeme mit Updates, die vom Hersteller zur Verfügung gestellt werden. Kein Systemupdate darf länger als ein Quartal überfällig sein (außer es gibt einen dokumentierten Grund, warum ein Update nicht eingesetzt werden kann).

Systeme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden, werden rechtzeitig außer Betrieb genommen bzw. es gibt definierte Ausnahmeprozesse inklusive einer Abweichungsliste.

Wie patcht ihr aktuell Server, Applikationen und Endgeräte?

Was ist euer Intervall bzw. Ansatz?

B9. Patch Management - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Auch wieder Ergänzend zum Thema Asset Management zu sehen.

B10. Network Security

Anforderung:
Sichern Sie Ihr Netzwerk vor unberechtigtem Zugriff von außen ab?

Anforderungskriterien:

Es ist eine Netzwerk-Segmentierungseinrichtung (zB. Firewall, Router, etc.) im Einsatz, die auf Basis möglichst restriktiv gesetzter Regeln den Netzwerkverkehr aus dem Internet in das interne Netzwerk beschränkt.

Wie setzt ihr eure Netzwerk Sicherheit um?

Was wollt ihr ändern in Zukunft?

B10. Network Security - Quellen

- IT-Grundschutz BSI
- NIST/CIS Standards
- Inhalte aus unseren vergangenen Workshops zum Thema Network Security
  - Least Privilege Access
  - Macro and Micros Segmentation
  - Firewall mit VLANs
  - Perimter Absichern
  - Unterschied zwischen Public und Private Zonen

B11. Antivirus auf Assets

Anforderung:
Überwachen Sie Ihre IT-Systeme auf Malware?

Anforderungskriterien:

Es muss zumindest eine Antivirussoftware im Einsatz sein, welche laufend die Systeme und Dateien auf Schadsoftware überprüft. Die Software muss laufend aktualisiert werden und diese Aktualisierung zumindest einmal monatlich zentral geprüft werden. Im Verdachtsfall erfolgt eine Alarmierung im Unternehmen.

Welchen AV habt ihr im Einsatz? Ist dieser mit einem Device Mgmt verknüpft?

Habt ihr das auch auf Servern?

B11. Antivirus auf Assets - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Auch wieder Ergänzend zum Thema Asset Management zu sehen.

B12. Verschlüsselte Kommunikation

Anforderung:
Verschlüsseln Sie sensible Daten bei der Übertragung im Internet?

Anforderungskriterien:

Es muss die Möglichkeit bestehen, Dateien verschlüsselt zu übertragen, entweder per E-Mail (zB. S/MIME, PDF verschlüsselt, mandatory enforced TLS, etc.) oder per verschlüsseltem Upload.

Formulardaten auf der Webseite werden ausschließlich über https hochgeladen.

Wie kommuniziert ihr mit Kunden?

Wie tauscht ihr Nachrichten, Daten und andere Inhalte aus? Betreibt ihr Datenklassifikation?

B12. Verschlüsselte Kommunikation - Quellen

- Sollte eigentlich mittlerweile überall Standard sein!
- Wichtig gilt hier nur bei Austausch von Daten übers Internet!
- Bei E-Mail Provider muss das enabled/supported sein.
- Filesharing über https webplattform ist legitim → Sonst über ssl/tls verschlüsselten Service

B13. Aufbewahrung von Logs jeglicher Art

Anforderung:
Protokollieren Sie die Nutzung Ihrer IT-Systeme, um Sicherheitsvorfälle nachvollziehbar zu machen?

Anforderungskriterien:

Es müssen zumindest die Standardprotokolle der Betriebssysteme aktiviert sein. Die Protokolle müssen dem Unternehmen zur Verfügung stehen.

Es existiert eine Übersicht aller aktiven Systemprotokolle und deren Speicherort.

Die Protokolle werden zumindest drei Monate aufbewahrt.

Habt ihr die möglichkeit zentral Syslog Events zu speichern?

Was könnt bzw. wollt ihr alles loggen?

B13. Aufbewahrung von Logs - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- NIS GV - Log Aufbewahrung

B14. Verhalten im Notfall

Anforderung:
Haben Sie einen Notfallplan, anhand dessen Sie auf einen IT-Sicherheitsvorfall reagieren?

Anforderungskriterien:

Der Notfallplan muss beschreiben, wie auf einen schwerwiegenden IT-Sicherheitsvorfall reagiert wird. Schwerwiegende Sicherheitsvorfälle sind zum Beispiel:

- Ausfall der Systeme,
- Schadsoftware-Befall (inkl. Kryptolocker) sowie
- Data Leakage

Die Pläne müssen mindestens alle zwei Jahre getestet werden. Der Test muss zumindest die Daten- und Service Wiederherstellung umfassen.

Habt ihr nach letzter Session für die wichtigsten Sachen einen Notfallplan?

Wenn ja - habt ihr eine Wiederherstellung getestet?

B14. Verhalten im Notfall - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Das alles bringt nur was mit Testszenarios und Pflege der Notfallpläne

Wrap Up

Was nehmen wir uns mit?

Ganzheitliche Cybersicherheit ist unser großes Ziel da wollen wir hin.

Cyber Trust Austria ist eine gute alternative für ein Sicherheitssiegel nach außen → Auch wichtig für Versicherungen

Es gibt extrem viele und ausreichende Ressourcen für KMUs