Architekturänderungen für mehr Cyber-Sicherheit

Deutscher Nahverkehrstag, 17. April 2024

22.04.24

Beat Stettler

- Professor und > 20 Jahre Dozent für Computernetze, Mobilfunk, Cloud Infrastrukturen, Wireless & IoT
- Gründer mehrerer Startup-Firmen
- Geschäftsführer onway ag

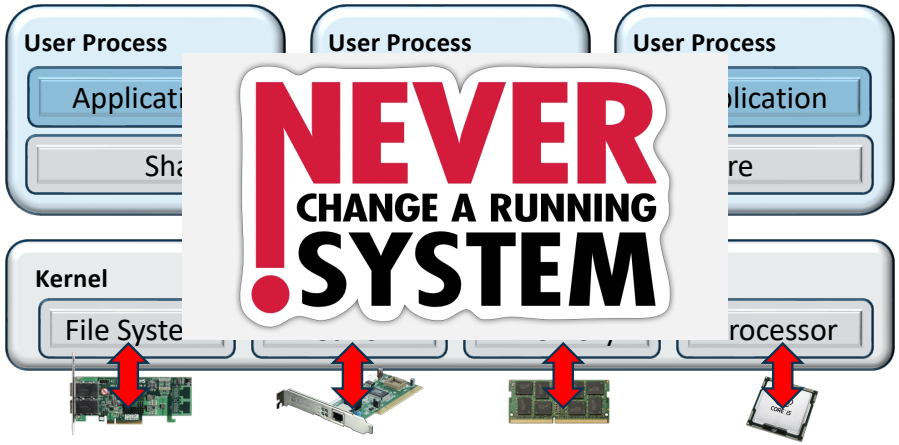
onway

Agenda

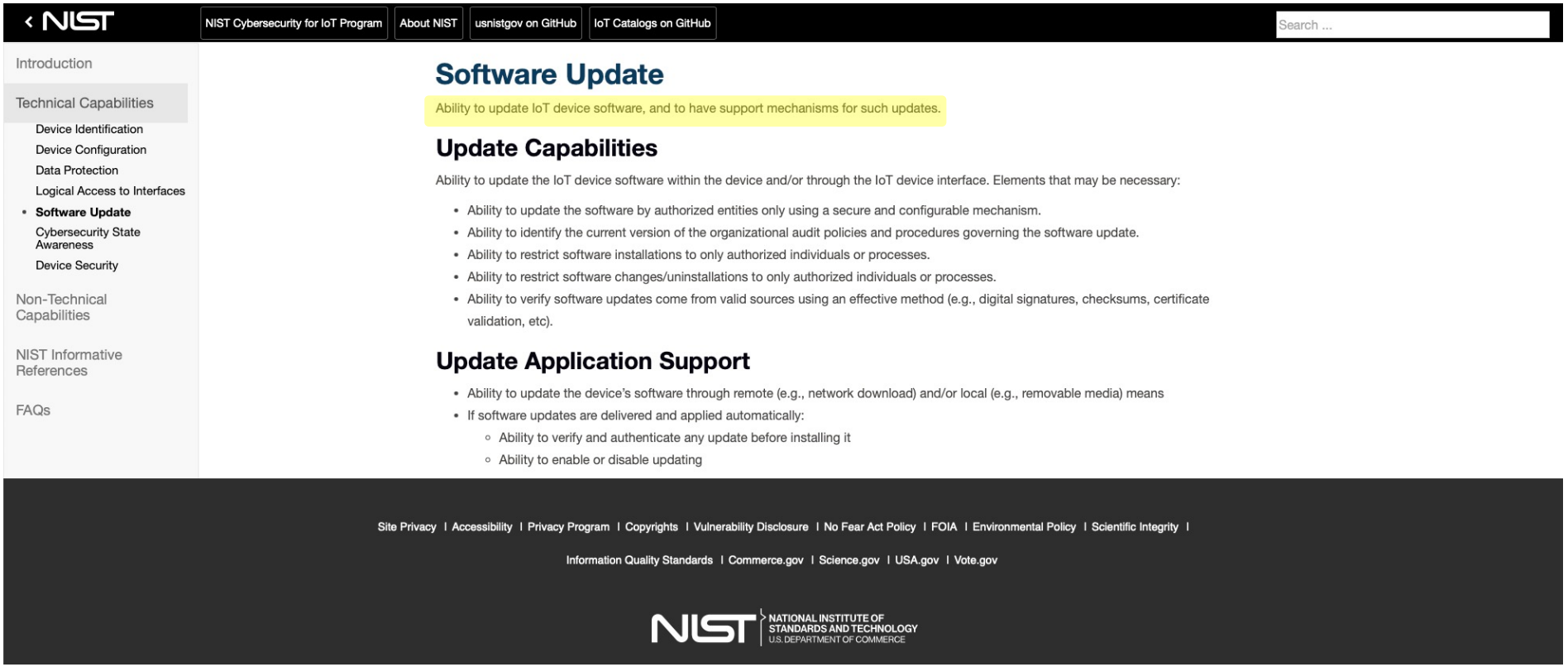
- Trennung von Hard- und Software
- Zentrale Verwaltung aller Komponenten
- End-to-End Security
- Zugriffskontrolle

Klassische (Embedded) PC Architektur

- Praktisch alle elektronischen Geräte basieren auf klassischer PC-Architektur
  - Prozessor, RAM, Speicher, Netzwerk
  - Betriebssytem (Kernel)
  - Applikationen
- Problematiken:
  - Applikationen teilen sich Treiber sowie der Zugang zu Hardware
  - Hardware benötigen eigene Treiber
- Resultat:
  - Hardware und Software sind stark voneinander abhängig
  - Updates einzelner Applikationen führt zu Treiberkonflikten
  - Keine sichere Trennung der verschiedenen Applikationen möglich

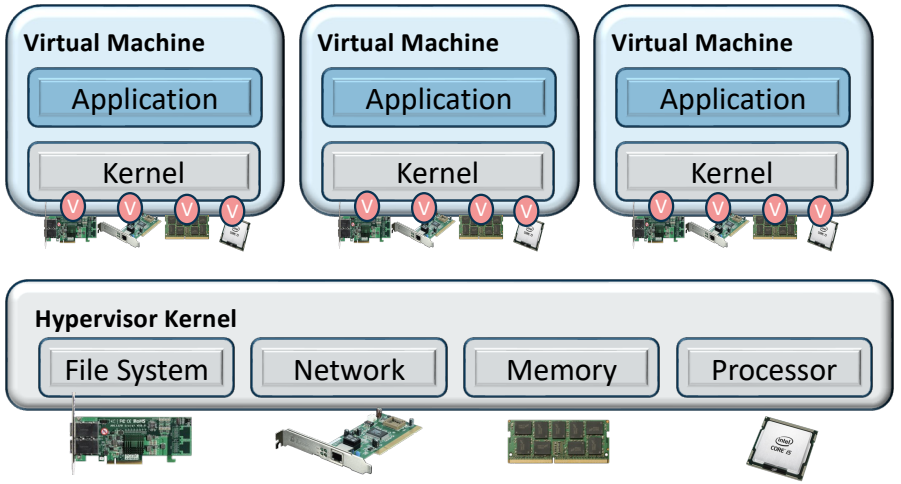


Top Anforderungen für Cyber-Sicherheit:



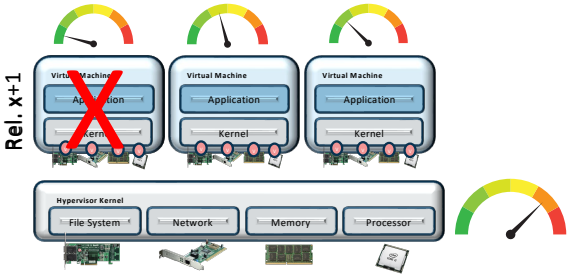
Virtualisierte Architektur

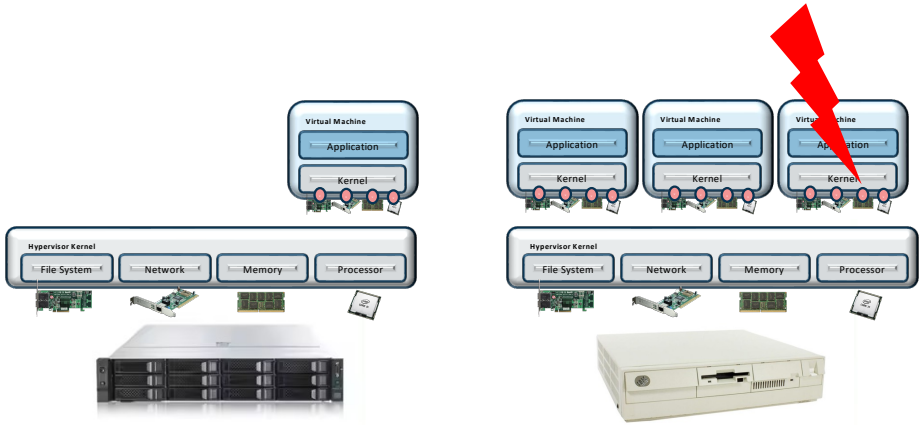
- In Rechenzentren wird seit ca. 2005 “Servervirtualisierung” eingesetzt
- Hypervisor Kernel
  - Emuliert HW über standardisierten Treiber
  - Führt alle priviligierten Aktionen durch
  - Verteilt CPU an Virtuelle Maschinen (VM)
  - Ordnet virtueller zu physischem Speicher zu
- Konsequenzen:
  - Keine Abhängigkeiten mehr zwischen Hardware und Software
  - VM kann auf beliebiger Hardware laufen
  - Sichere Trennung der virtuellen Maschinen über Hipervisor (wissen nichts voneinander)



Vorteile:

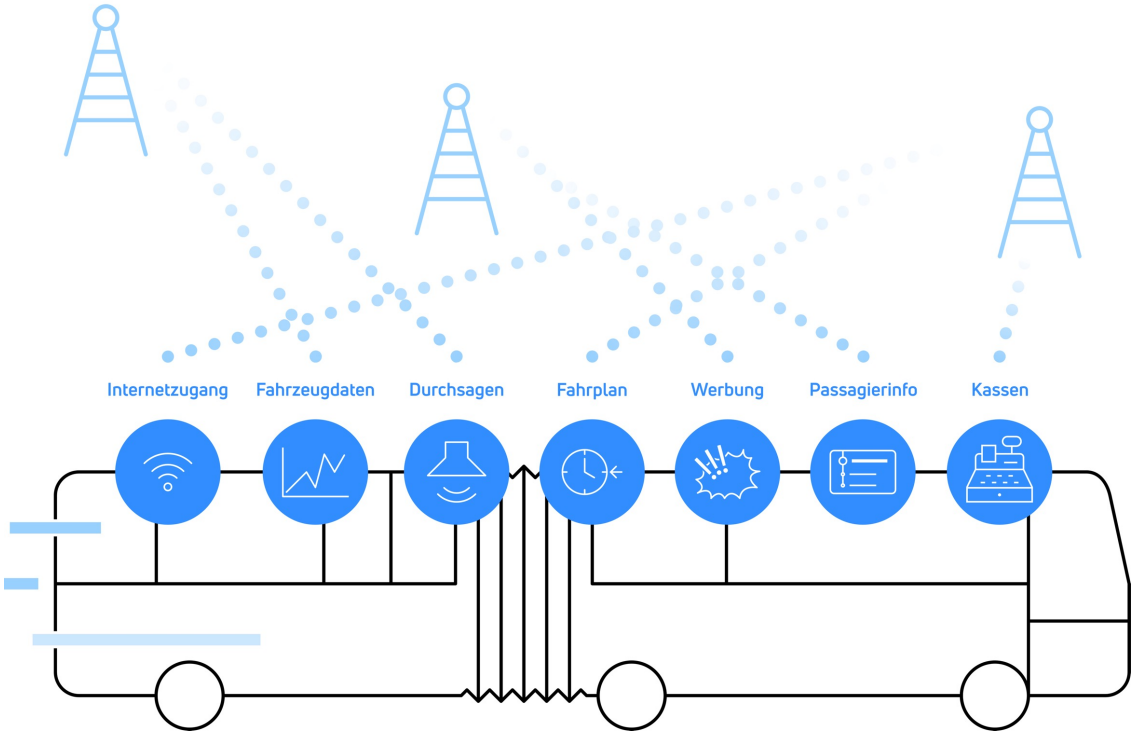
- VMs und Applikationen können jederzeit upgedated und gepached werden -> kein Einfluss auf Andere
- Die Auslastung der HW Ressourcen wird massiv verbessert
- Die gleiche Applikation kann auf unterschiedlicher HW laufen
- Virtuelle Maschinen können “gezügelt” werden
- Redundanz kann sehr einfach durch Hochfahren der gleichen VM auf anderer HW erreicht werden
- Applikationen können auch in die Cloud verschoben werden





Heutige Situation bei vielen Fahrzeugen

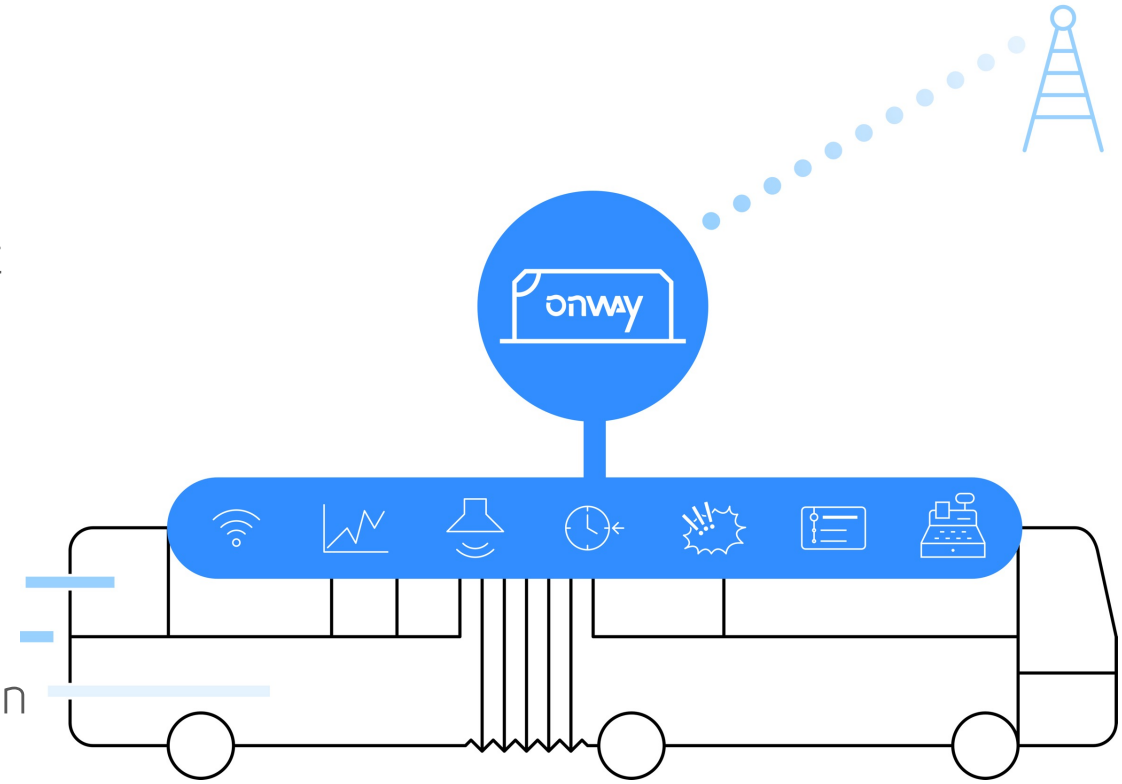
- Viele verschiedene silo-artige Anwendungen von verschiedenen Herstellern
- Unterschiedliche Lebenszyklen der proprietären Systeme
- Systeme kommunizieren nicht miteinander
- Grosse Herstellerabhängigkeit und damit verbunden hohe Kosten



Das Mobile Rechenzentrum

... besteht aus:

- möglichst wenig Hardware
- mind. einem Rechner, der möglichst viele Applikationen hostet
- einem lokalen Netzwerk, über das die Applikationen kommunizieren
- ein oder zwei Uplinks
- den nötigen Security und QoS Funktionen, um jeder Applikation den nötigen Schutz zu gewährleisten

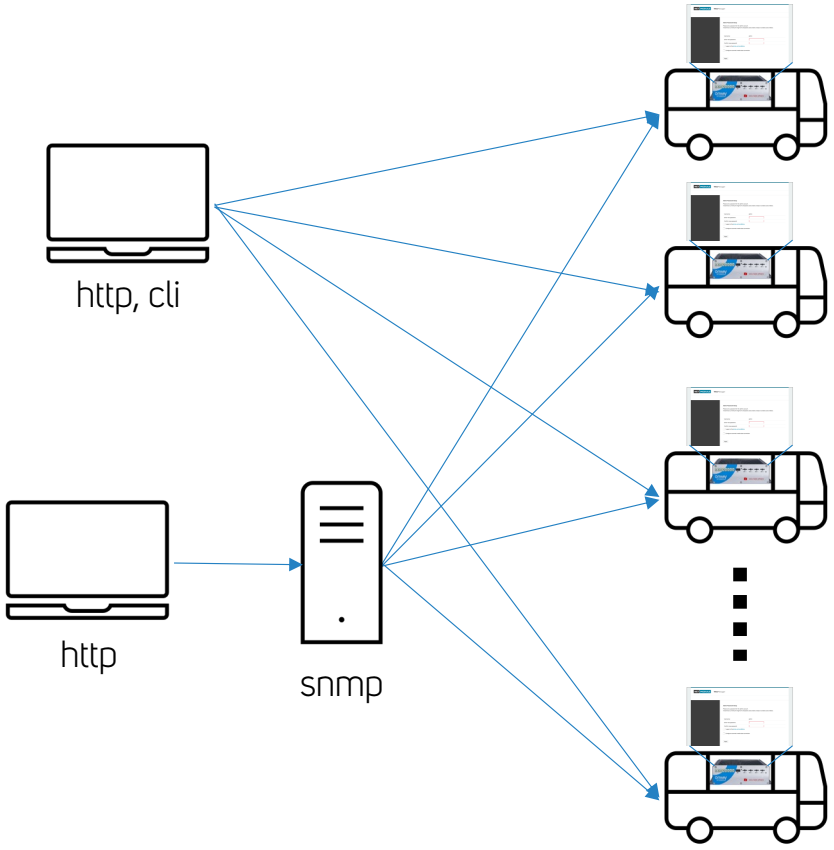


Agenda

- Trennung von Hard- und Software
- Zentrale Verwaltung aller Komponenten
- End-to-End Security
- Zugriffskontrolle

Old-World Konfiguration von Routern

- Konfigurationen werden “Schritt für Schritt” ausgeführt, entweder über Konsole, Web-Interface, snmp etc.
- “Explizite” Konfigurationen, d.h. jeder Router hat eine eigene Konfig
- Router ist “Master”
- Kein “Go-Back to Konfig Version x”
- Keine History (Audit-Log)
- Reale Gefahr, sich “abzuschiessen”, dann Gang vor Ort nötig



Konfigurations-Management

- Was macht ein Rechenzentrum zur Cloud?
  - Standardisierung
  - Automatisierung
  - Orchestrierung
- Zentrale Konfiguration im Backend
  - IT Systeme sind „headless“
  - Reproduzierbarkeit, Templates, Versionierung
  - Integriertes Zertifikates-Management, PKI
- Deployment via Push
  - Auf ganze Flotten
  - Applizierung auf Router in Sekunden(bruchteilen)

Infrastructure-as-Code

Wikipedia: **Infrastructure as code** (IaC) is the process of *managing and provisioning* computer data centers *through machine-readable definition files*, rather than physical hardware configuration or interactive configuration tools. The IT infrastructure managed by this process comprises both physical equipment, such as bare-metal servers, as well as virtual machines, and associated configuration resources. The definitions *may be in a version control system*. It can use *either scripts or declarative definitions*, rather than manual processes, but the term is more often used to promote declarative approaches.

```
- name: SW1234
  id: 10
  vlans:
    10: ITCS
    11: AFZ
    20: CCTV
```

```
hostname {{ name }}

interface Loopback1
ip address 10.1.1.{{ id }} 255.255.255.255

{% for vlan, name in vlans.items() %}
vlan {{ vlan }}
 name {{ name }}
{% endfor %}
```

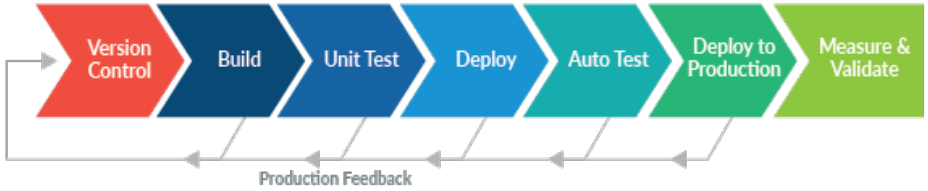
```
hostname SW1234

interface Loopback1
ip address 10.1.1.10 255.255.255.255

vlan 10
 name ITCS
vlan 11
 name AFZ
vlan 20
 name CCTV
```

Daten

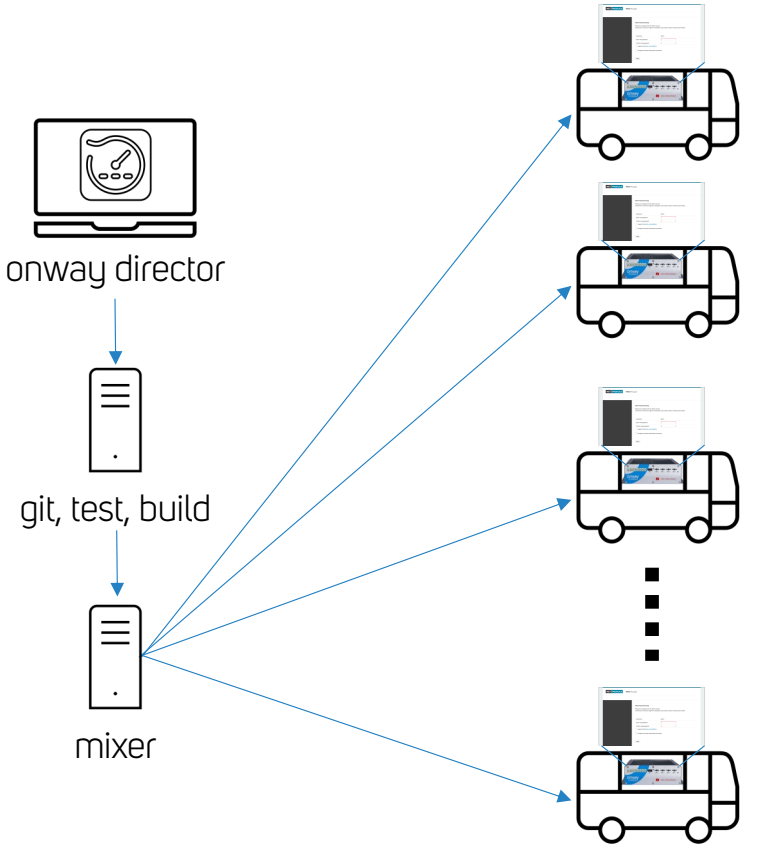
Logik

Automatisierte Konfiguration von Routern

- Konfigurationen erfolgen entweder im onway director oder direkt durch Editieren von Konfig-Files
- Konfigurationen werden im Repository eingecheckt. Dieses ist "Master" aller Konfigversionen, ein "Go back to Version x" ist jederzeit möglich
- 100% Audit Trail (alles wird geloggt)
- New Konfig wird automatisch auf Fehler getestet



- Build/Deployment eines Changes erfolgt "all at once"
- Falls ausgerollte Konfigs/SW-Release fehlerhaft, wird automatisch die letzte Version verwendet



Agenda

- Die grössten IT Revolutionen der letzten 20 Jahre auf der Landseite
- Trennung von Hard- und Software
- Zentrale Verwaltung aller Komponenten
- End-to-End Security
- Zugriffskontrolle

Anforderungen an Netzwerk-Security

Foundational Requirements (FR)

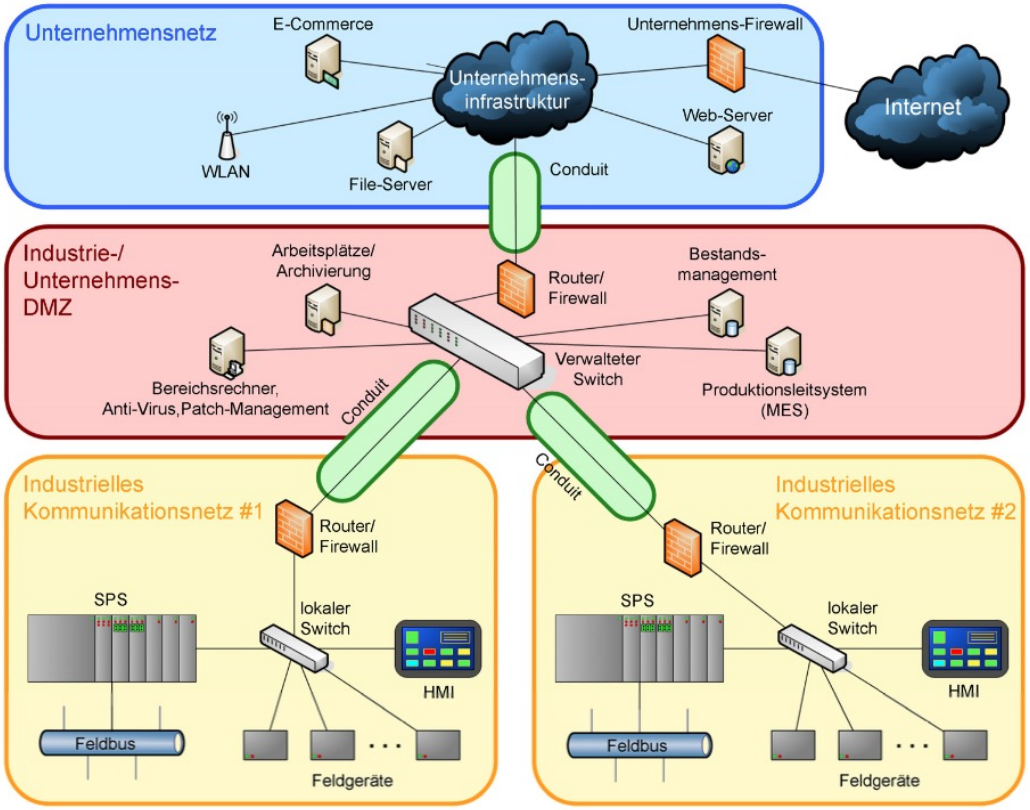
- Access Control (AC)
- Use Control (UC)
- Data Integrity (DI)
- Data Confidentiality (DC)
- Restrict Data Flow (RDF)
- Timely Response to Event (TRE)
- Resource Availability (RA)

Zones:

- Group of logical or physical assets with common security requirements.

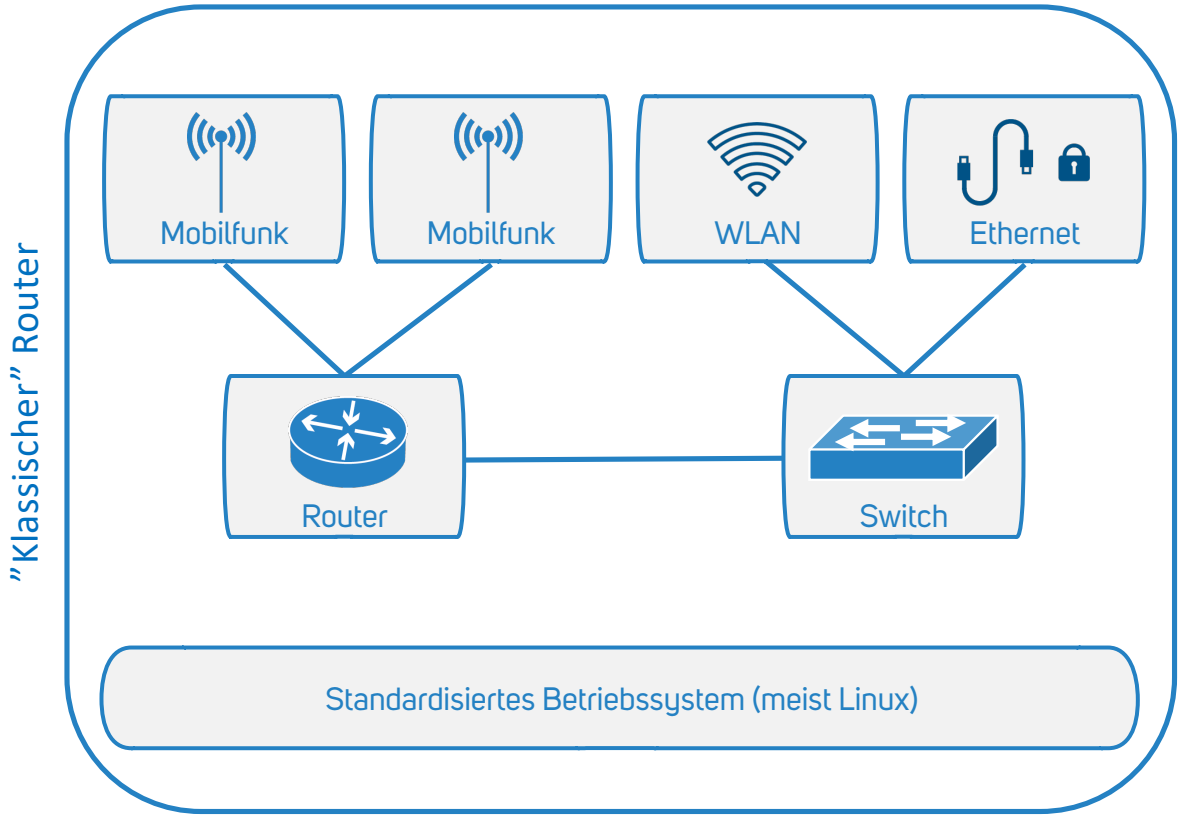
Conduits:

- Logical grouping of communication channels, that share common security requirements and connect two or more zones.



Referenz: EN IEC 62443-3-3

Klassische Router Architektur



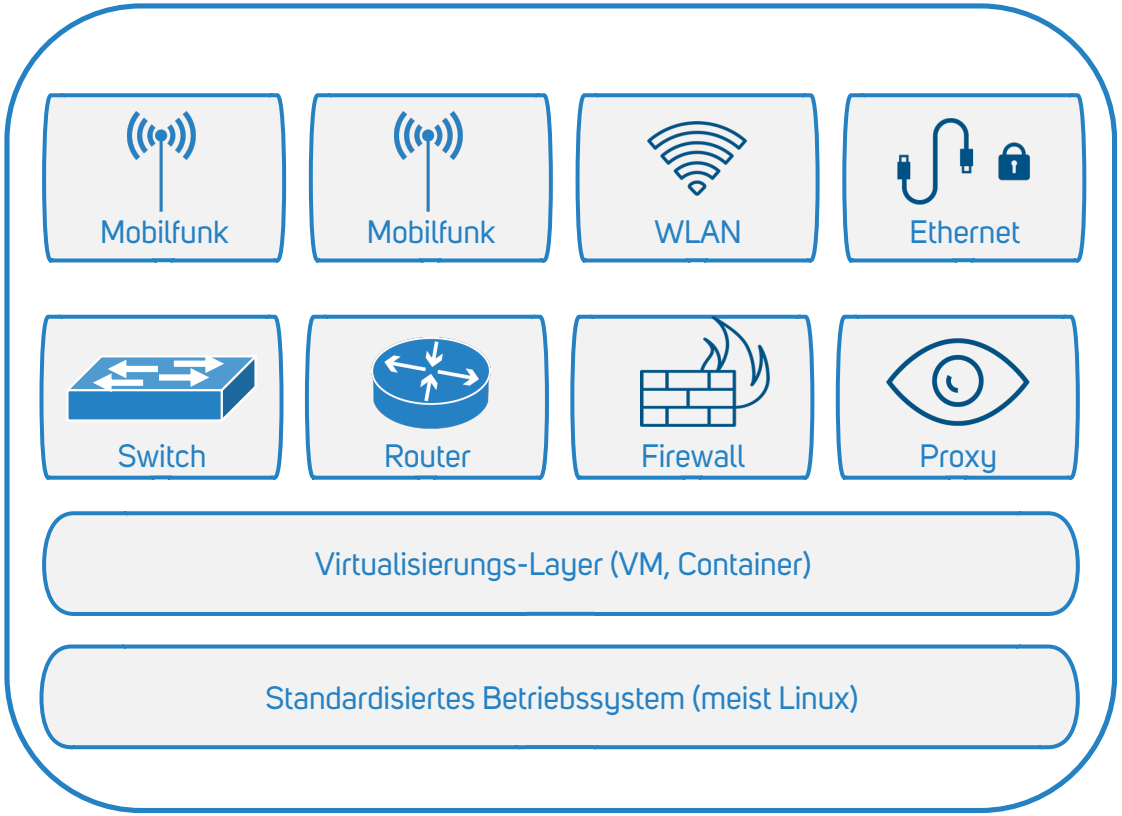
Funktionen des Routers:

- Control-Plane: eine Routing-Tabelle
- Data-Plane: Forwarden von IP-Paketen

Funktionen des integrierten Switches:

- VLAN-Separierung
- Forwarden von Ethernet Frames innerhalb VLAN

Virtualisierte Gatway Architektur



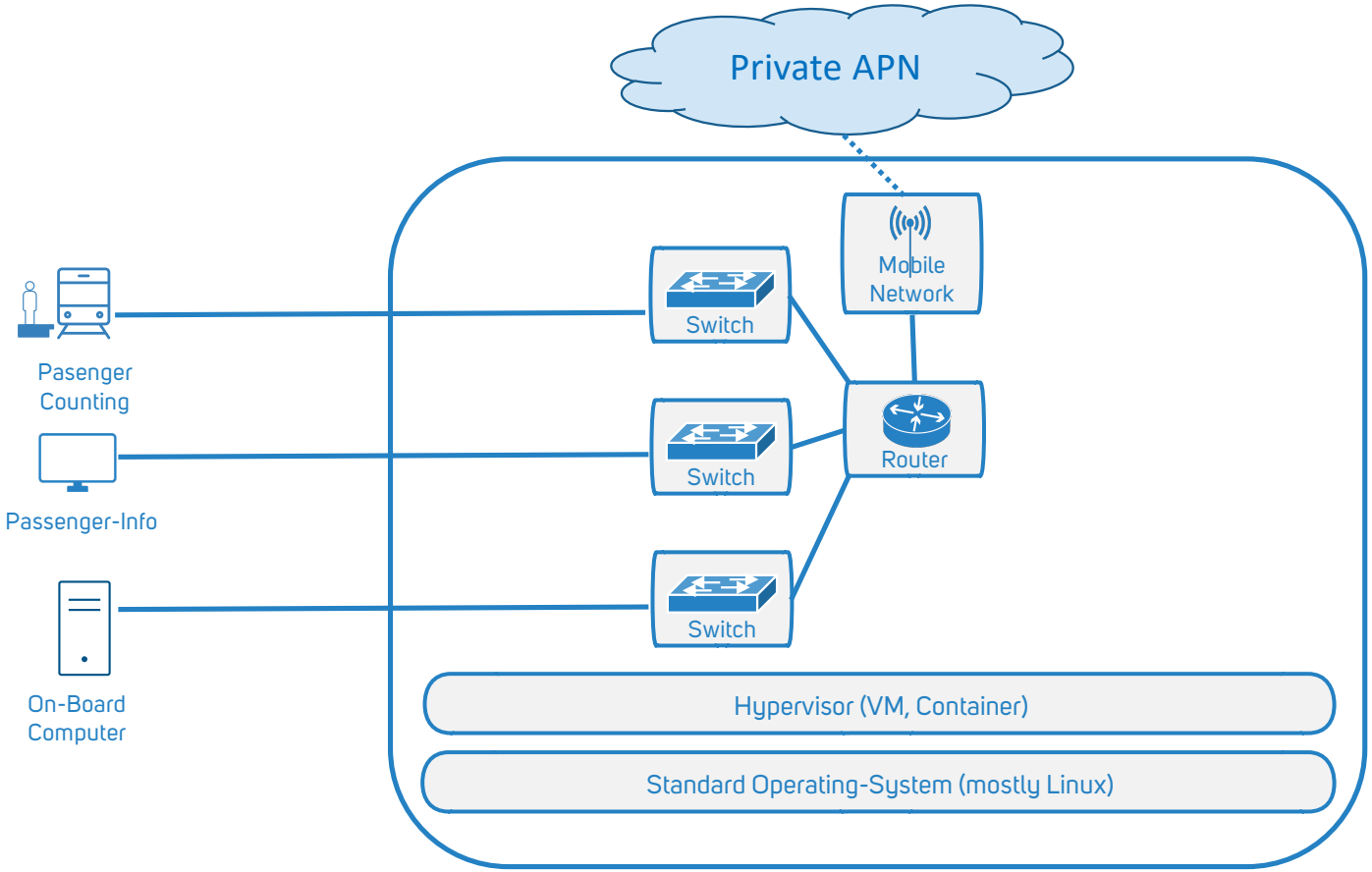
Neu:

- Virtualisierungs-Layer
- Netzwerk-Funktionen als virtualisierte Software

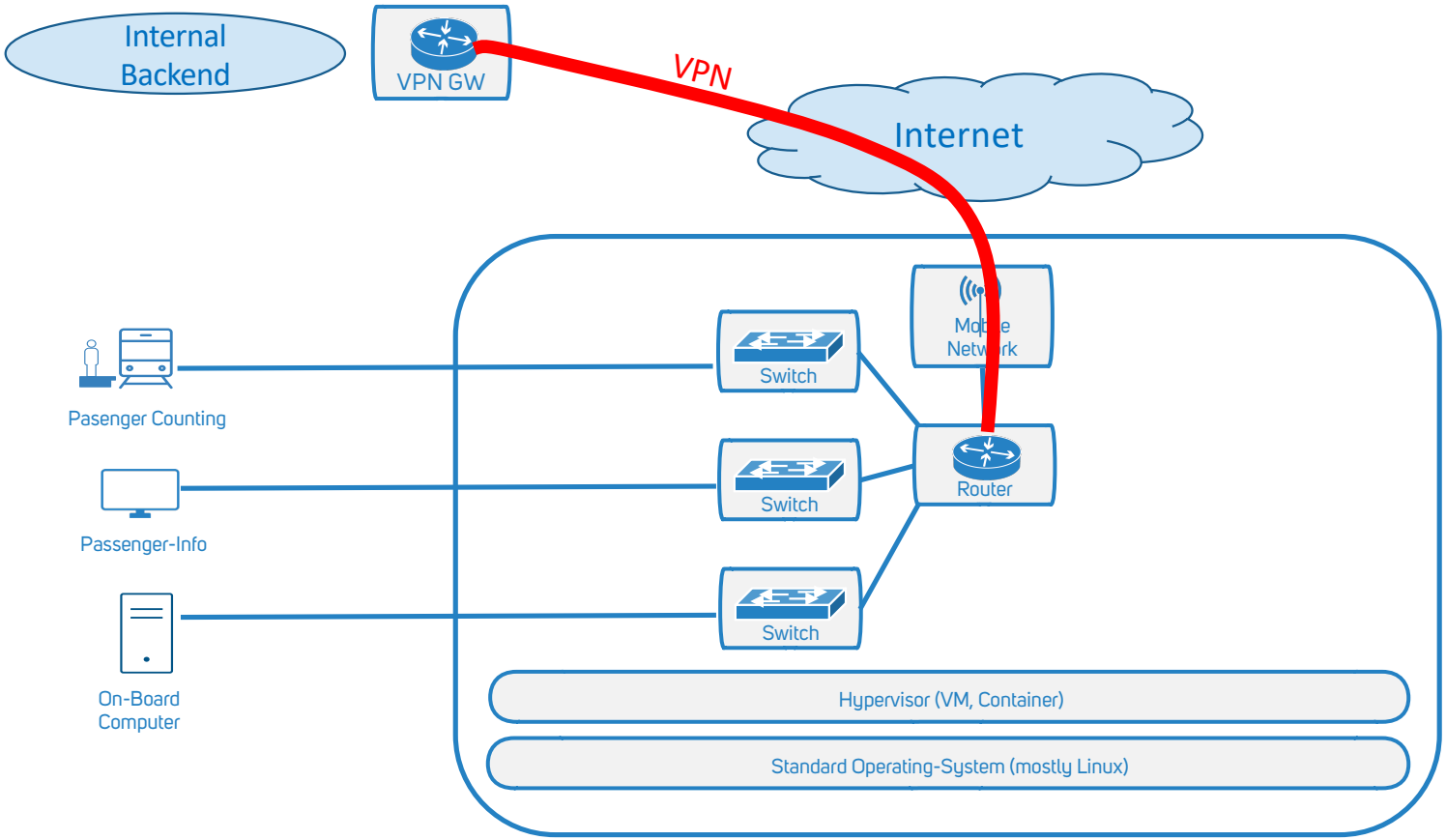
Dadurch:

- Freies "Zusammenstellen" der benötigten Netzwerk-Funktionen möglich
- Weitere Funktionen wie Firewall, Proxy etc. per Software zuladbar

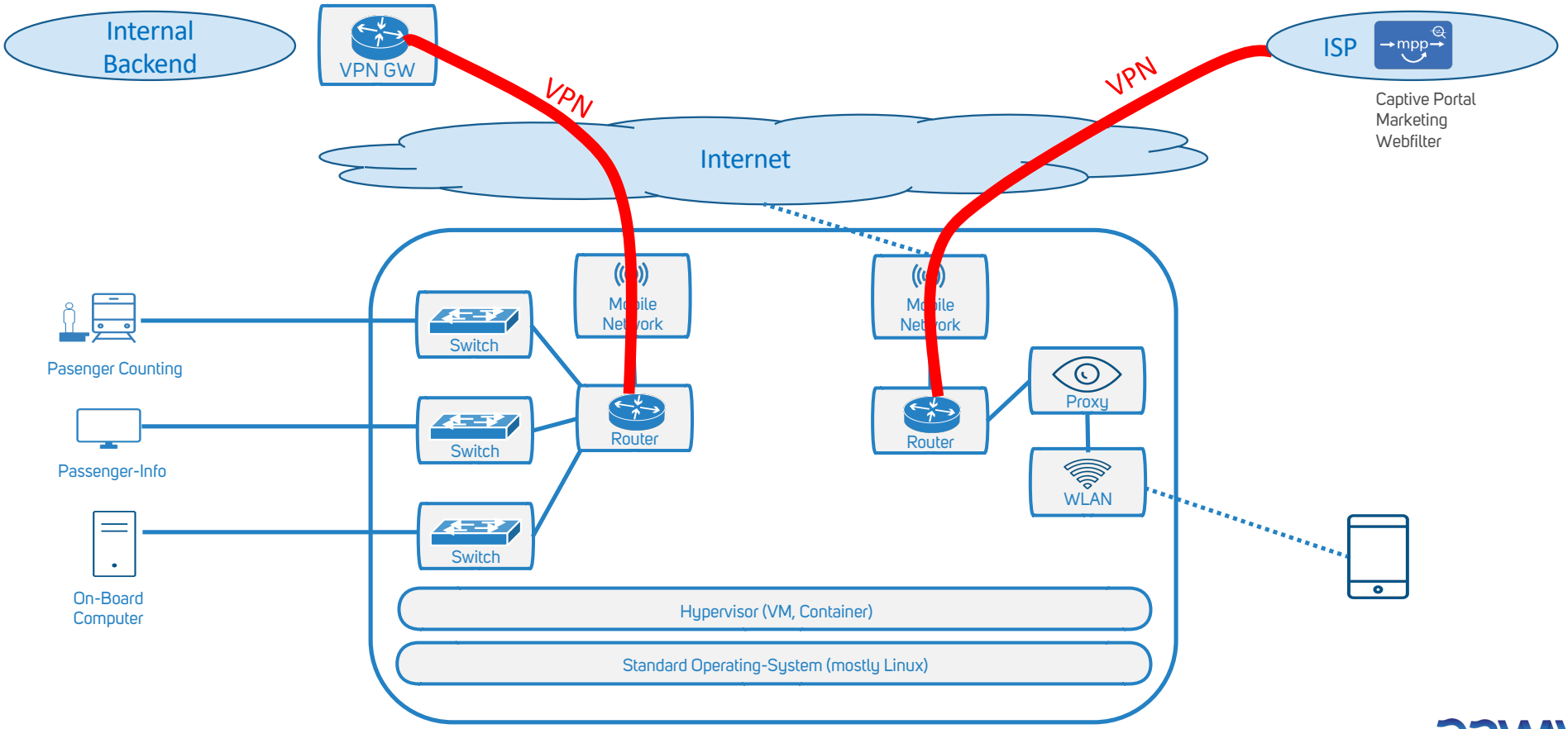
Interne Kommunikation



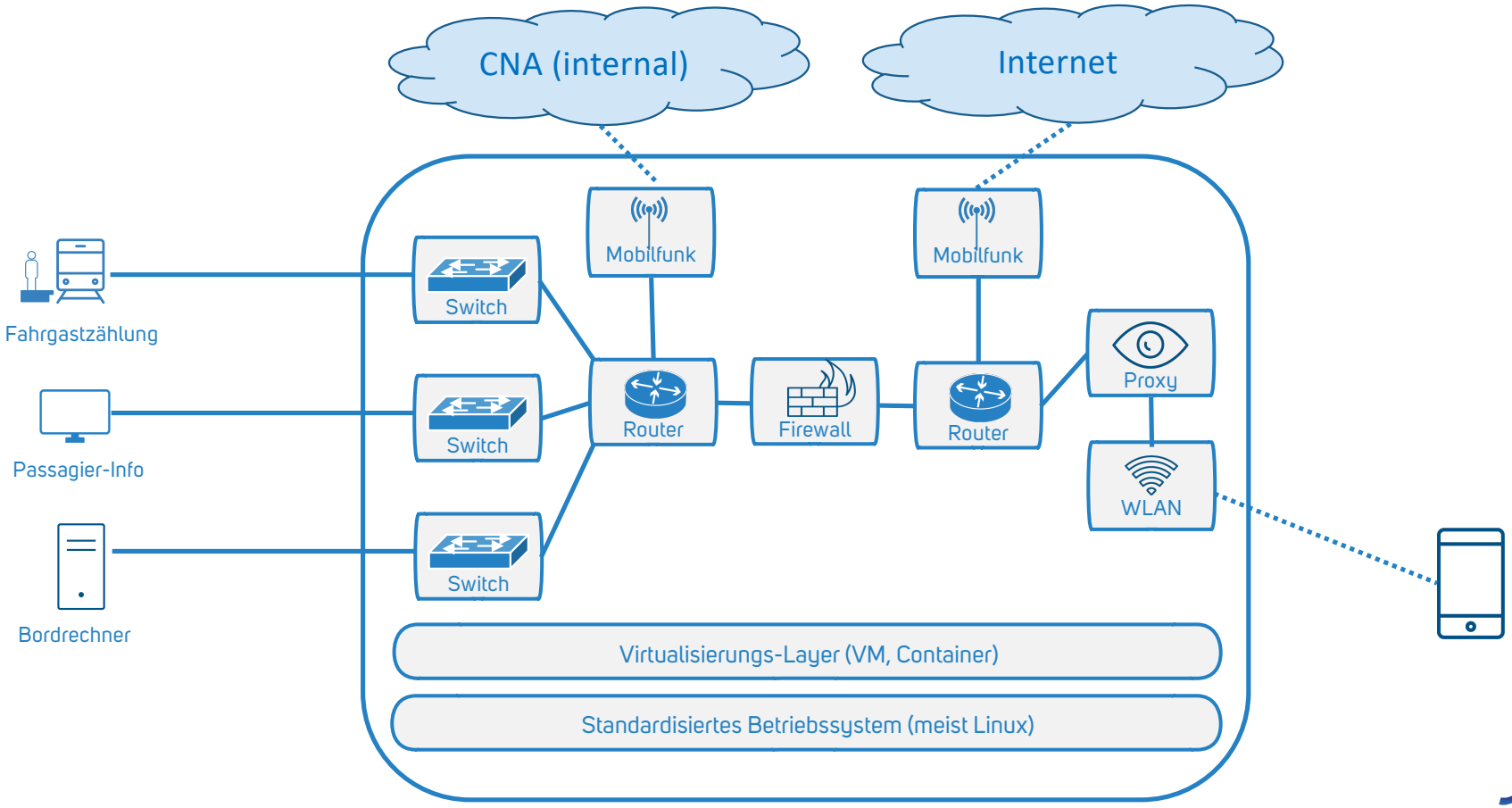
Besser: Verschlüsselte Interne Kommunikation



Sichere Trennung: Two-in-One Router



Firewall zwischen internen und externer Anwendung



Agenda

- Die grössten IT Revolutionen der letzten 20 Jahre auf der Landseite
- Trennung von Hard- und Software
- Zentrale Verwaltung aller Komponenten
- End-to-End Security
- Zugriffskontrolle

Beispiel Zugriffskontrolle nach ISO 27001

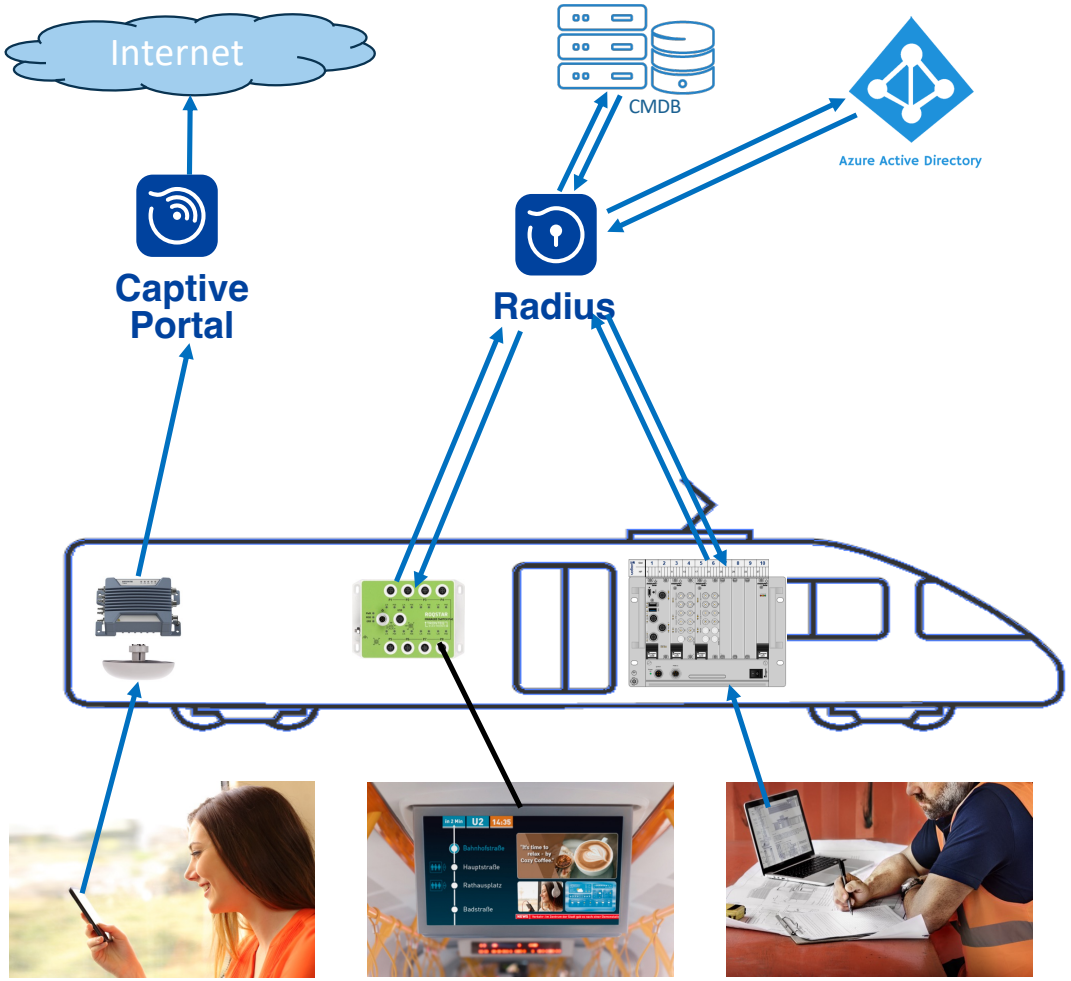
Thema	Beschreibung
Ziel und Zweck	Beschränkung des Zugriffs von Mitarbeitenden, Externen oder Kunden sowie privilegierten Usern auf Informationen und informationsverarbeitende Einrichtungen.
Adressierte Massnahmenziele	A.9.1.1 Leitlinie Zugriffskontrolle A.9.2.1 An- und Abmelden von Benutzern A.9.2.2 Zugangsbereitstellung für Benutzer A.9.2.3 Verwaltung von Sonderzugriffsrechten A.9.2.4 Verwaltung geheimer Authentifizierungsdaten von Benutzern A.9.2.5 Überprüfung von Benutzerberechtigungen A.9.2.6 Entziehung oder Anpassung von Benutzerrechten A.9.3.1 Verwendung geheimer Authentifizierungsdaten von Benutzern A.9.4.1 Beschränkung des Zugriffs auf Informationen A.9.4.2 Sichere Anmeldeverfahren
Mitgeltende Dokumente	43_PasswortManagement 433_Change Management 435_SecurityIncidentManagement

Zugriffkontrolle

1. Zugriff auf Geräte im Fahrzeug
   - Keine unpersönlichen Passwörter
   - Zentrales, userbasiertes Login

2. Zugriff auf internes Netzwerk
   - Keine offenen Ports
   - Authentisierung über Radius (802.1x)
   - Integration in Corporate CMDB

3. Zugriff auf Passagier WLAN
   - Authentisierung über Captive Portal
   - Erfüllung rechtlicher Anforderungen



Zusammenfassung

- Trennen Sie Hardware von Software
  - Ermöglicht regelmässiges Updaten und Patchen
  - Senkt Ihre Live-Cycle Kosten massiv
  - Virtualisierung bildet die Basis für einen sicheren Betrieb
- Denken Sie wie ein Cloud Provider
  - Automatisieren Sie regelmässige Tasks konsequent
  - Bauen Sie ein zentrales Orchestrierungs-Tool
- Trennen Sie Anwendungen / Hersteller im Netzwerk konsequent
  - Fahrzeug-Land übergreifende Netzwerk-Zonierung
  - Übergänge zwischen Zonen nur durch Firewalls
- Schützen Sie den Zugang zu Ihrer Infrastruktur
  - Nutzen Sie die vorhandene Infrastruktur (Radius, Active-Directory usw.)

Besten Dank für Ihre Aufmerksamkeit

Beat.Stettler@onway.ch

22.04.24