OTScan 3

Netzwerk-Check: Geräte und Sicherheit

Version 3.0.0 | 13.11.2026

Netzwerk: Montage_Anlagennetz

GELB - Handlungsbedarf Unsichere Dienste gefunden

Geräte gefunden	Offene Dienste	Unsichere Dienste
22	70	38

SCAN-INFORMATIONEN

Netzwerk:	Montage_Anlagennetz	**Scan gestartet:**	10.11.2026 14:20
CIDR:	192.168.30.0/24	**Dauer:**	1 Std. 28 Min.
Scan-Profil:	Stufenlauf komplett	**Nmap Version:**	7.94
Portset:	ICS_OT_CORE	**Hosts gefunden:**	22

INHALT DIESES BERICHTS

1. **Deckblatt** diese Seite
2. **Auf einen Blick** Ergebnis in einfachen Worten - für alle
3. **Was ist zu tun?** Schritte, unsichere Dienste erklärt, betroffene Geräte
4. **Fachteil: Zusammenfassung** Kennzahlen, Befunde, Empfehlungen für Fachleute
5. **Netzwerk-Heatmap** Übersicht nach Subnetz und Gerätetyp
6. **Kritische Hosts** Detailansicht aller Geräte mit Befund
7. **Host-Inventar** Vollständige Geräteliste
8. **Vergleich** Änderungen seit dem letzten vollständigen Scan (falls vorhanden)
9. **Technische Details** Scan-Parameter und Anhang
10. **ICS/OT-Glossar** Protokoll-Erklärungen und Einordnung

2 AUF EINEN BLICK - DAS ERGEBNIS IN EINFACHEN WORTEN

Netzwerk Montage_Anlagennetz (192.168.30.0/24), gescannt am 10.11.2026 14:20, Dauer: 1 Std. 28 Min.

GELB

Handlungsbedarf

Gesamtbewertung: Handlungsbedarf

Einige Geräte bieten Dienste an, die als unsicher gelten. Das ist kein Angriff, aber eine offene Tür, die geplant geschlossen werden sollte.

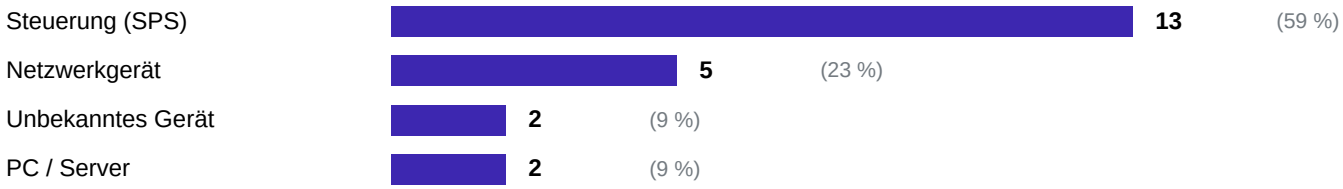
Was jetzt? Die vorgeschlagenen Maßnahmen mit den Verantwortlichen der Anlage abstimmen und einplanen.

Geräte gefunden	Geräte mit Befund	Unsichere Dienste
22	**19**	**38**
haben auf den Scan geantwortet	bieten mind. einen unsicheren Dienst an	offene Dienste, die als unsicher gelten

Das Wichtigste

- Im Netzwerk Montage_Anlagennetz wurden 22 Geräte gefunden.
- 19 von 22 Geräten bieten mindestens einen unsicheren Dienst an.
- 9 Geräte sind laut Herstellermeldung betroffen (Firmware im betroffenen Bereich); bei 2 Geräten passt das Modell zu einer Meldung - Firmware am Gerät prüfen.
- 2 Geräte sind nur im Firewall-Verkehr (Splunk 02.11.2026 - 08.11.2026) sichtbar, nicht im Scan - 2 Geräte davon nicht in der CMDB.
- 38 von 38 unsicheren Diensten hatten im Splunk-Zeitraum 02.11.2026 - 08.11.2026 keinen Verkehr über die Firewall - Kandidaten zum Abschalten.
- Am häufigsten: HTTP auf 15 Geräten, SNMP auf 10 Geräten, Telnet auf 5 Geräten.
- Die meisten Geräte sind: Steuerung (SPS) (13 von 22).

Welche Geräte sind im Netzwerk?



Veränderung seit dem letzten Scan

Kein vollständiger früherer Scan dieses Netzwerks zum Vergleich vorhanden. Beim nächsten vollständigen Scan steht hier, was sich verändert hat.

Gut zu wissen: Dieser Bericht zeigt, welche Dienste im Netzwerk erreichbar sind. Er sagt nicht, ob ein Gerät angegriffen wurde. Steuerungsprotokolle wie S7, Modbus oder OPC UA sind in Produktionsnetzwerken normal und werden nicht als Befund gezählt.

3 WAS IST ZU TUN?

Die wichtigsten Schritte, das Wichtigste zuerst. Bitte mit den Verantwortlichen der Anlage abstimmen - an Steuerungen nichts ohne Absprache abschalten.

1. **HTTP auf 15 Geräten**
   Auf HTTPS umstellen oder abschalten; Anmelden über HTTP ist laut Verkehrsregeln nicht erlaubt.
2. **SNMP auf 10 Geräten**
   SNMPv1/v2c und 'public' sind laut Verkehrsregeln nicht erlaubt: auf SNMPv3 umstellen.
3. **Telnet auf 5 Geräten**
   Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.
4. **FTP auf 2 Geräten**
   Laut Verkehrsregeln nicht erlaubt: abschalten, sonst SFTP oder FTPS nutzen.
5. **Firewall-Regeln prüfen**
   Unsichere Dienste nur für die Rechner freigeben, die sie wirklich brauchen.
6. **2 Geräte nur aus Splunk im Netzwerk suchen (MAC/Switchport) und in die CMDB übernehmen - Vorlage**
   Datei "..._CMDB-Nachtrag.xlsx".

Unsichere Dienste kurz erklärt

Dienst	Was ist das?	Warum riskant?	Was tun?	Geräte
HTTP (Port 80/tcp)	Weboberfläche des Geräts	Anmeldung und Einstellungen gehen unverschlüsselt durchs Netzwerk.	Auf HTTPS umstellen oder abschalten; Anmelden über HTTP ist laut Verkehrsregeln nicht erlaubt.	**15**
SNMP (Port 161/udp)	Abfrage von Gerätedaten	Bei v1/v2c geht das Passwort (Community) unverschlüsselt durchs Netzwerk.	SNMPv1/v2c und 'public' sind laut Verkehrsregeln nicht erlaubt: auf SNMPv3 umstellen.	**10**
Telnet (Port 23/tcp)	Fernzugang auf die Kommandozeile	Passwörter und Befehle gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.	**5**
FTP (Port 21/tcp)	Dateiübertragung	Benutzername, Passwort und Dateien gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten, sonst SFTP oder FTPS nutzen.	**2**
SMB (Port 445/tcp)	Windows-Dateifreigabe	Alte Versionen (SMBv1) sind ein häufiger Weg für Schadsoftware.	SMBv1 abschalten (laut Verkehrsregeln nicht erlaubt), SMBv3 mit Signierung, Zugriff begrenzen.	**2**
VNC (Port 5900/tcp)	Bildschirm-Fernsteuerung	Bild, Eingaben und oft das Passwort gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten oder nur verschlüsselt (TLS, VPN, SSH-Tunnel).	**2**
RPC (Port 135/tcp)	Windows-Fernsteuerdienst	Häufiger Angriffspunkt; zeigt, welche Windows-Dienste laufen.	Nur wenn technisch nötig und nur für freigegebene Rechner; sonst per Firewall sperren.	**2**

Welche Geräte sind betroffen?

IP-Adresse	Gerät	Hersteller	Unsichere Dienste
192.168.30.3	Netzwerkgerät	Cisco Systems	HTTP, SNMP, Telnet
192.168.30.4	Netzwerkgerät	Hirschmann Automation and Control GmbH	HTTP, SNMP, Telnet
192.168.30.20	Steuerung (SPS)	Schneider Electric	FTP, HTTP, SNMP
192.168.30.30	Unbekanntes Gerät	Moxa Technologies	HTTP, SNMP, Telnet
192.168.30.31	Unbekanntes Gerät	Moxa Technologies	HTTP, SNMP, Telnet
192.168.30.102	Netzwerkgerät	Hirschmann Automation and Control GmbH	HTTP, SNMP, Telnet
192.168.30.22	Steuerung (SPS)	Wago Kontakttechnik GmbH	FTP, HTTP
192.168.30.25	Steuerung (SPS)	Siemens AG	HTTP, VNC
192.168.30.26	Steuerung (SPS)	Siemens AG	HTTP, VNC
192.168.30.60	PC / Server	Fujitsu Technology Solutions GmbH	RPC, SMB
192.168.30.61	PC / Server	Fujitsu Technology Solutions GmbH	RPC, SMB
192.168.30.10	Steuerung (SPS)	Siemens AG	HTTP, SNMP
192.168.30.11	Steuerung (SPS)	Siemens AG	HTTP, SNMP
192.168.30.1	Netzwerkgerät	Fortinet	SNMP
192.168.30.2	Netzwerkgerät	Siemens AG	SNMP
192.168.30.15	Steuerung (SPS)	Siemens AG	HTTP
192.168.30.16	Steuerung (SPS)	Siemens AG	HTTP
192.168.30.21	Steuerung (SPS)	OMRON Corporation	HTTP
192.168.30.101	Steuerung (SPS)	Siemens AG, Automations & Drives,	HTTP

Ab der nächsten Seite folgt der Fachteil mit allen Einzelheiten für Fachleute.

4 ZUSAMMENFASSUNG FÜR FACHLEUTE

GELB - Handlungsbedarf - Unsichere Dienste gefunden

WAS BEDEUTET DER RISK-WERT?

OTScan 3 vergleicht die offenen Ports jedes Geraets ausschliesslich gegen die Verkehrsregeln (HanselCraft-Voreinstellung, angelehnt an IEC 62443, vom Anwender anpassbar) - 15 Protokollfamilien wie Telnet, SMB, FTP, HTTP oder SNMP, die nicht verwendet werden sollen oder nur abgesichert. Fuer jedes offene Protokoll aus den Verkehrsregeln addiert das Werkzeug ein Gewicht (3 = verboten und Fernsteuerung/Dateizugriff moeglich, 2 = verboten, Klartext-Anmeldung oder Informationsabfluss, 1 = Zweitport oder mit TLS zulaessig); die Summe ist der "Risk"-Wert dieses Geraets, wie er in Titelzeile, Badge und den Sektionen 6 und 7 dieses Berichts erscheint. OT-Steuerprotokolle wie S7, Modbus, CODESYS oder OPC-UA fliessen NICHT ein - sie sind in OT-Netzwerken erwartete Kommunikation und kein Befund. Ampel: GRUEN = kein Protokoll aus den Verkehrsregeln offen, GELB = mindestens eines offen, INFO = Geraet erreichbar, aber keine Portdaten. Der Risk-Wert ist eine Sortier-/Priorisierungshilfe (hoeher = mehr unsichere IT-Dienste offen), keine genormte Kennzahl wie CVSS. Version und Anmeldeverfahren (z. B. SMBv1/v3, SNMPv1/v3) zeigt ein Portscan nicht; sie sind am Geraet zu pruefen. Vollstaendiger Katalog: Excel-Blatt "Ports", Spalte "Verkehrsregel".

KENNZAHLEN AUF EINEN BLICK

Gescannte Hosts:	**22**	**Offene Ports:**	70
Unsichere Ports offen:	**38**	**Scan-Datum:**	10.11.2026 14:20

KEY FINDINGS

- ⚠ **WARNUNG: 22 Geräte gescannt - MITTLERER Risiko-Level (GELB)**
- ⚠ **38 unsichere Ports laut Verkehrsregeln offen (z. B. Telnet, SMB, FTP, HTTP, SNMP) - OT-Steuerprotokolle wie S7/Modbus/OPC-UA sind darin NICHT enthalten**
- ℹ ***Häufigster Hersteller: Siemens AG (10 von 22)***
- ⚠ **SICHERHEITSRISIKO: 5 Geräte mit Telnet (Port 23) offen**

HANDLUNGSEMPFEHLUNGEN

1. Kritische Ports analysieren und durch Firewall-Regeln absichern
2. Firmware-Updates für alle OT-Geräte prüfen
3. KRITISCH: Telnet (Port 23) auf 5 Geräten deaktivieren -> SSH verwenden
4. Netzwerk-Segmentierung implementieren (OT-Netzwerk vom IT-Netzwerk trennen)
5. FTP (Port 21) auf 2 Geräten durch SFTP/FTPS ersetzen

5 NETZWERK-HEATMAP - RISIKO NACH SUBNETZ & GERÄTETYP

UNSICHER: mindestens ein Protokoll aus den Verkehrsregeln gefunden
EMPFEHLUNG: keine Protokolle aus den Verkehrsregeln offen

Subnetz	Hosts	Unsicher	FW Krit	FW Blk	Top Gerätetyp	Risiko
192.168.30.0/24	22	38	0	0	SPS/PLC (Siemens S7)	UNSICHER

GERÄTETYP-VERTEILUNG

Gerätetyp	Anz.	Anteil	Balken
SPS/PLC (Siemens S7)	10	45%	10
Netzwerk (Firewall/Switch)	4	18%	4
Unbekannt	2	9%	2
Windows-PC / Workstation	2	9%	2
Netzwerk (Siemens SCALANCE)	1	5%	1
SPS/PLC (Schneider Modicon)	1	5%	1
SPS/PLC (Rockwell/Allen-Bradley)	1	5%	1
SPS/PLC (Phoenix/WAGO)	1	5%	1

SPS/PLC HMI/SCADA Netzwerk Windows/Linux Sonstige

6 KRITISCHE HOSTS - DETAILANSICHT (19 GERÄTE)

192.168.30.3 Netzwerk (Firewall/Switch) | Cisco Systems | Risikopunkte: 7

MAC-Adresse:	00:00:0C:1E:18:BD	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Cisco Systems	**OS-Erkennung:**	Cisco IOS 17
TCP-Ports:	22,443,23,80	**UDP-Ports:**	161
Krit. Ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.4 Netzwerk (Firewall/Switch) | Hirschmann Automation and C... | Risikopunkte: 7

MAC-Adresse:	00:80:63:1E:1F:CA	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Hirschmann Automation and Control GmbH	**TCP-Ports:**	23,80
UDP-Ports:	161		
Krit. Ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.20 SPS/PLC (Schneider Modicon) | Schneider Electric | Risikopunkte: 7

MAC-Adresse:	00:00:54:1E:8F:9A	**Gerätetyp:**	SPS/PLC (Schneider Modicon)
Hersteller:	Schneider Electric	**TCP-Ports:**	21,80,502
UDP-Ports:	161		
Krit. Ports:	161/udp, 21/tcp, 80/tcp		

192.168.30.30 - | Moxa Technologies | Risikopunkte: 7

MAC-Adresse:	00:90:E8:1E:D5:1C	**Gerätetyp:**	-
Hersteller:	Moxa Technologies	**TCP-Ports:**	23,80
UDP-Ports:	161		
Krit. Ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.31 - | Moxa Technologies | Risikopunkte: 7

MAC-Adresse:	00:90:E8:1E:DC:29	**Gerätetyp:**	-
Hersteller:	Moxa Technologies	**TCP-Ports:**	23,80
UDP-Ports:	161		
Krit. Ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.102 Netzwerk (Firewall/Switch) | Hirschmann Automation and C... | Risikopunkte: 7

MAC-Adresse:	64:60:38:1E:CD:C4	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Hirschmann Automation and Control GmbH	**TCP-Ports:**	23,80
UDP-Ports:	161		
Krit. Ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.22 SPS/PLC (Phoenix/WAGO) | Wago Kontakttechnik GmbH | Risikopunkte: 5

MAC-Adresse:	00:30:DE:1E:9D:B4	**Gerätetyp:**	SPS/PLC (Phoenix/WAGO)
Hersteller:	Wago Kontakttechnik GmbH	**OS-Erkennung:**	Linux 4.x
TCP-Ports:	21,22,80,443,502,2455		
Krit. Ports:	21/tcp, 80/tcp		

192.168.30.25 SPS/PLC (Siemens S7) | Siemens AG | Risikopunkte: 5

MAC-Adresse:	00:1B:1B:1E:B2:DB	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**TCP-Ports:**	80,5900,102
Krit. Ports:	5900/tcp, 80/tcp		

192.168.30.26 SPS/PLC (Siemens S7) | Siemens AG | Risikopunkte: 5

MAC-Adresse:	00:1B:1B:1E:B9:E8	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**TCP-Ports:**	80,5900,102
Krit. Ports:	5900/tcp, 80/tcp		

192.168.30.60 Windows-PC / Workstation | Fujitsu Technology Solution... | Risikopunkte: 5

MAC-Adresse:	00:19:99:1E:A7:A2	**Gerätetyp:**	Windows-PC / Workstation
Hersteller:	Fujitsu Technology Solutions GmbH	**OS-Erkennung:**	Microsoft Windows 10
TCP-Ports:	135,445,3389		
Krit. Ports:	135/tcp, 445/tcp		

192.168.30.61 Windows-PC / Workstation | Fujitsu Technology Solution... | Risikopunkte: 5

MAC-Adresse:	00:19:99:1E:AE:AF	**Gerätetyp:**	Windows-PC / Workstation
Hersteller:	Fujitsu Technology Solutions GmbH	**OS-Erkennung:**	Microsoft Windows 10
TCP-Ports:	135,445		
Krit. Ports:	135/tcp, 445/tcp		

192.168.30.10 H3-MO-SPS-L1 SPS/PLC (Siemens S7) | Siemens AG | Risikopunkte: 4

Gerätename:	H3-MO-SPS-L1 (S7)	**MAC-Adresse:**	00:1B:1B:1E:49:18
Gerätetyp:	SPS/PLC (Siemens S7)	**Hersteller:**	Siemens AG
S7 System:	H3-MO-SPS-L1	**S7 Modul:**	6ES7 315-2EH14-0AB0 CPU 315-2 PN/DP
TCP-Ports:	80,102	**UDP-Ports:**	161,34964
Krit. Ports:	161/udp, 80/tcp		

192.168.30.11 H3-MO-SPS-L2 SPS/PLC (Siemens S7) | Siemens AG | Risikopunkte: 4

Gerätename:	H3-MO-SPS-L2 (S7)	**MAC-Adresse:**	00:1B:1B:1E:50:25
Gerätetyp:	SPS/PLC (Siemens S7)	**Hersteller:**	Siemens AG
S7 System:	H3-MO-SPS-L2	**S7 Modul:**	6ES7 317-2EK14-0AB0 CPU 317-2 PN/DP
TCP-Ports:	80,102	**UDP-Ports:**	161,34964
Krit. Ports:	161/udp, 80/tcp		

192.168.30.1 Netzwerk (Firewall/Switch) | Fortinet | Risikopunkte: 2

MAC-Adresse:	00:09:0F:1E:0A:A3	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Fortinet	**OS-Erkennung:**	FortiOS 7.2
TCP-Ports:	443	**UDP-Ports:**	161
Krit. Ports:	161/udp		

192.168.30.2 Netzwerk (Siemens SCALANCE) | Siemens AG | Risikopunkte: 2

MAC-Adresse:	00:0E:8C:1E:11:B0	**Gerätetyp:**	Netzwerk (Siemens SCALANCE)
Hersteller:	Siemens AG	**TCP-Ports:**	22,443
UDP-Ports:	161		
Krit. Ports:	161/udp		

192.168.30.15 H3-MO-SPS-ST01 SPS/PLC (Siemens S7) | Siemens AG | Risikopunkte: 2

Gerätename:	H3-MO-SPS-ST01 (S7)	**MAC-Adresse:**	00:1B:1B:1E:6C:59
Gerätetyp:	SPS/PLC (Siemens S7)	**Hersteller:**	Siemens AG
S7 System:	H3-MO-SPS-ST01	**S7 Modul:**	6ES7 214-1AG40-0XB0 CPU 1214C DC/DC/DC
TCP-Ports:	102,80,443		
Krit. Ports:	80/tcp		

192.168.30.16 H3-MO-SPS-ST02 SPS/PLC (Siemens S7) | Siemens AG | Risikopunkte: 2

Gerätename:	H3-MO-SPS-ST02 (S7)	**MAC-Adresse:**	00:1B:1B:1E:73:66
Gerätetyp:	SPS/PLC (Siemens S7)	**Hersteller:**	Siemens AG
S7 System:	H3-MO-SPS-ST02	**S7 Modul:**	6ES7 215-1AG40-0XB0 CPU 1215C DC/DC/DC
TCP-Ports:	102,80,443		
Krit. Ports:	80/tcp		

192.168.30.21 SPS/PLC (Rockwell/Allen-Bradley) | OMRON Corporation | Risikopunkte: 2

MAC-Adresse:	00:00:0A:1E:96:A7	**Gerätetyp:**	SPS/PLC (Rockwell/Allen-Bradley)
Hersteller:	OMRON Corporation	**TCP-Ports:**	80,9600,44818
UDP-Ports:	9600		
Krit. Ports:	80/tcp		

192.168.30.101 SPS/PLC (Siemens S7) | Siemens AG, Automations & D... | Risikopunkte: 2

MAC-Adresse:	30:13:89:1E:C6:B7	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG, Automations & Drives,	**TCP-Ports:**	80,102,443
Krit. Ports:	80/tcp		

7 HOST-INVENTAR - 22 GERÄTE (SORTIERT NACH RISIKOSCORE)

Risikopunkte: Summe der Gewichte aller unsicheren Dienste eines Geräts (0 = unauffällig). Rot ab 6 Punkten.

IP-Adresse	MAC-Adresse	Gerätetyp	Hersteller	Risiko-punkte	Betriebssystem	Name	Offene TCP-Ports
192.168.30.3	00:00:0C:1E:18:BD	Netzwerk (Firewall/Switch)	Cisco Systems	7	Cisco IOS 17		22, 443, 23, 80
192.168.30.4	00:80:63:1E:1F:CA	Netzwerk (Firewall/Switch)	Hirschmann Automation and Control GmbH	7			23, 80
192.168.30.20	00:00:54:1E:8F:9A	SPS/PLC (Schneider Modicon)	Schneider Electric	7			21, 80, 502
192.168.30.30	00:90:E8:1E:D5:1C	-	Moxa Technologies	7			23, 80
192.168.30.31	00:90:E8:1E:DC:29	-	Moxa Technologies	7			23, 80
192.168.30.102	64:60:38:1E:CD:C4	Netzwerk (Firewall/Switch)	Hirschmann Automation and Control GmbH	7			23, 80
192.168.30.22	00:30:DE:1E:9D:B4	SPS/PLC (Phoenix/WAGO)	Wago Kontakttechnik GmbH	5	Linux 4.x		21, 22, 80, 443, 502, 2455
192.168.30.25	00:1B:1B:1E:B2:DB	SPS/PLC (Siemens S7)	Siemens AG	5			80, 5900, 102
192.168.30.26	00:1B:1B:1E:B9:E8	SPS/PLC (Siemens S7)	Siemens AG	5			80, 5900, 102
192.168.30.60	00:19:99:1E:A7:A2	Windows-PC / Workstation	Fujitsu Technology Solutions GmbH	5	Microsoft Windows 10		135, 445, 3389
192.168.30.61	00:19:99:1E:AE:AF	Windows-PC / Workstation	Fujitsu Technology Solutions GmbH	5	Microsoft Windows 10		135, 445
192.168.30.10	00:1B:1B:1E:49:18	SPS/PLC (Siemens S7)	Siemens AG	4		H3-MO-SPS-L1	80, 102
192.168.30.11	00:1B:1B:1E:50:25	SPS/PLC (Siemens S7)	Siemens AG	4		H3-MO-SPS-L2	80, 102
192.168.30.1	00:09:0F:1E:0A:A3	Netzwerk (Firewall/Switch)	Fortinet	2	FortiOS 7.2		443
192.168.30.2	00:0E:8C:1E:11:B0	Netzwerk (Siemens SCALANCE)	Siemens AG	2			22, 443
192.168.30.15	00:1B:1B:1E:6C:59	SPS/PLC (Siemens S7)	Siemens AG	2		H3-MO-SPS-ST 01	102, 80, 443
192.168.30.16	00:1B:1B:1E:73:66	SPS/PLC (Siemens S7)	Siemens AG	2		H3-MO-SPS-ST 02	102, 80, 443
192.168.30.21	00:00:0A:1E:96:A7	SPS/PLC (Rockwell/Allen-Bradley)	OMRON Corporation	2			80, 9600, 44818
192.168.30.101	30:13:89:1E:C6:B7	SPS/PLC (Siemens S7)	Siemens AG, Automations & Drives,	2			80, 102, 443
192.168.30.12	00:1B:1B:1E:57:32	SPS/PLC (Siemens S7)	Siemens AG	0		H3-MO-SPS-L3	102, 443, 4840
192.168.30.17	00:1B:1B:1E:7A:73	SPS/PLC (Siemens S7)	Siemens AG	0		H3-MO-SPS-ST 03	102
192.168.30.100	30:B8:51:1E:BF:AA	SPS/PLC (Siemens S7)	Siemens AG	0			102, 4840

Im Scan gefunden, aber NICHT in CMDB (undokumentiert) - 3 Geraete

Hinweis: undokumentierte Geraete im OT-Netzwerk pruefen (Asset-Erfassung / Segmentierung, IEC 62443).

IP-Adresse	MAC-Adresse	Hersteller	Gerätetyp	TCP-Ports	Risk
192.168.30.1	00:09:0F:1E:0A:A3	Fortinet	Netzwerk (Firewall/Switc	443	2
192.168.30.17	00:1B:1B:1E:7A:73	Siemens AG	SPS/PLC (Siemens S7)	102	0
192.168.30.26	00:1B:1B:1E:B9:E8	Siemens AG	SPS/PLC (Siemens S7)	80,5900,102	5

Nur im Firewall-Verkehr (Splunk), nicht im Scan - 2 Geräte

Splunk-Daten 02.11.2026 - 08.11.2026. Gelb = Gerät ist wahrscheinlich vorhanden (bitte im Netzwerk suchen). Neue und betroffene CMDB-Zeilen stehen in der Datei "..._CMDB-Nachtrag.xlsx". Suchhilfe (MAC, Partner) im Excel-Blatt "Nur in Splunk".

IP-Adresse	Einschätzung	Splunk-Ports	MAC / Hersteller	Zuletzt	CMDB
192.168.30.90	Vorhanden - nur ausgehend	-	00:1B:1B:5A:0E:DE	2026-11-08	nein
192.168.30.91	Vorhanden - nur ausgehend	-	00:30:DE:5A:11:E9	2026-11-08	nein

9 TECHNISCHE DETAILS & ANHANG

KRITISCHE OFFENE PORTS (ÜBERSICHT)

Port/Proto	Dienst (Verkehrsregeln)	Anzahl Hosts	Risikobewertung
80/tcp	HTTP	15	Mittel (Gewicht 2) - prüfen
161/udp	SNMP (v1/v2c?)	10	Mittel (Gewicht 2) - prüfen
23/tcp	Telnet	5	Hoch (Gewicht 3) - zuerst prüfen
21/tcp	FTP	2	Hoch (Gewicht 3) - zuerst prüfen
5900/tcp	VNC (RFB)	2	Hoch (Gewicht 3) - zuerst prüfen
135/tcp	RPC/EPMAP	2	Mittel (Gewicht 2) - prüfen
445/tcp	SMB (Version prüfen)	2	Hoch (Gewicht 3) - zuerst prüfen

Verkehrsregeln 1.0 zu diesen Diensten

HTTP - keine Anmeldung über HTTP / HTTPS empfohlen
HTTPS soll genutzt werden; eine Anmeldung (u. a. HTTP Basic) über unverschlüsseltes HTTP soll nicht verwendet werden. Sichere Alternative: HTTPS (TCP 443) mit aktuellem TLS (1.2 oder neuer).

SNMP - nicht verwenden (v1/v2c, public/private)
SNMPv1/v2c und Standard-Communities (public, private) sollen nicht verwendet werden. Sichere Alternative: SNMPv3 mit authPriv (AES, SHA-2), nur lesend.

Telnet - nicht verwenden
Telnet soll nicht verwendet werden; Dienst und Client abschalten. Sichere Alternative: SSH mit Public-Key-Anmeldung und aktueller Verschlüsselung.

FTP - nicht verwenden
Unverschlüsseltes FTP soll nicht verwendet werden (unsichere Anmeldung, keine Verschlüsselung). Sichere Alternative: SFTP (bevorzugt), FTPS oder HTTPS; SCP nur für Altsysteme.

VNC - nicht verwenden (ohne TLS)
VNC ohne Verschlüsselung soll nicht verwendet werden und nie direkt aus fremden Netzwerken (über Zonengrenzen) erreichbar sein. Sichere Alternative: VNC mit TLS oder über SSH-/VPN-Tunnel, besser zentraler Fernzugang.

RPC/EPMAP - nicht verwenden (außer technisch nötig)
RPC/EPMAP nur, wenn technisch nötig - dann nur für freigegebene interne Systeme, nie über Zonengrenzen aus fremden Netzwerken. Sichere Alternative: Kerberos, RPC-Verschlüsselung (PKT_PRIVACY), Host-Firewall.

SMB - nicht verwenden (SMBv1, NTLMv1, LM)
SMBv1, NTLMv1 und LAN Manager sollen nicht verwendet werden; SMBv3 mit Signierung soll genutzt werden. Sichere Alternative: SMBv3 mit Kerberos, Signierung und Verschlüsselung.

Hinweis: OTScan 3 bewertet offene Ports. Version und Anmeldeverfahren (z. B. SMBv1/v3, SNMPv1/v3, LDAP mit oder ohne TLS, NFS mit oder ohne Kerberos) lassen sich daraus nicht sicher ablesen und sind am Gerät zu prüfen.

NMAP SCAN-ARGUMENTE

Montage_Anlagennetz_20261110_154840_stufenlauf:
(Datei nicht im Ausgabeordner)

Montage_Anlagennetz_20261110_154840_stufenlauf.xml:
nmap -sS -sU -Pn -n -T2 --max-retries 3 --host-timeout 1800s --reason --open -sV --version-intensity 5 -O -p T:21,22,23,80,102,135,443,445,502,1200,2455,3389,4840,5900,8000,9600,44818,U:161,3671,9600,34964,47808 --script banner,http-server-header,http-title,ssl-cert,snmp-sysdescr,s7-info_robust,modbus-identity,codesys-v2-discover,knx-gateway-info,bacnet-info -oX <Ergebnisdatei> 192.168.30.0/24

10 ICS/OT-GLOSSAR - PROTOKOLLE & EINORDNUNG

In diesem Scan wurden Ports gefunden, die auf folgende OT-Protokolle hindeuten. Die Tabelle erklaert jedes Protokoll und seine Sicherheitsrelevanz:

Modbus / Modbus-TCP (502/TCP)

Eines der aeltesten und verbreitetsten OT-Protokolle. Steuert SPSen, Sensoren und Aktoren. Keine eingebaute Authentifizierung - jeder mit Netzwerkzugang kann lesen und schreiben.
Risiko: HOCH - unauthentifizierter Schreibzugriff auf Steuerungen moeglich.

Siemens S7 / S7comm (102/TCP (ISO-TSAP))

Kommunikationsprotokoll fuer Siemens SIMATIC S7-SPSen. Ueber Port 102 werden Programm, Konfiguration und Prozessdaten ausgetauscht.
Risiko: HOCH - Auslesen von CPU-Typ, Firmware, Seriennummer; bei aelteren CPUs auch Manipulation.

CODESYS (1200/TCP, 2455/TCP) [IM SCAN GEFUNDEN]

Laufzeitumgebung fuer SPSen vieler Hersteller (auch Bosch Rexroth, WAGO, Beckhoff). Erlaubt Programmierung und Steuerung der Geraete.
Risiko: HOCH - aeltere CODESYS-V2-Laufzeiten erlauben unauthentifiziertes Stoppen/Starten der SPS.

OPC UA (4840/TCP) [IM SCAN GEFUNDEN]

Moderner, plattformunabhaengiger Industriestandard fuer sichere Maschine-zu-Maschine-Kommunikation. Unterstuetzt Verschluesselung und Authentifizierung (wenn konfiguriert).
Risiko: MITTEL - sicher konfigurierbar, aber oft ohne Verschluesselung im Einsatz.

EtherNet/IP (CIP) (44818/TCP, 2222/UDP)

Industrieprotokoll von Rockwell/Allen-Bradley (ODVA). Verbreitet in der Fabrikautomation, basiert auf dem Common Industrial Protocol (CIP).
Risiko: HOCH - Geraeteidentifikation und teils Konfigurationszugriff ohne Auth.

BACnet (47808/UDP)

Standard fuer Gebaeudeautomation (HLK, Beleuchtung, Zutritt). Findet sich in Heizungs-, Lueftungs- und Klimasteuerungen.
Risiko: MITTEL - Auslesen von Geraete- und Objektinformationen.

KNX / KNXnet-IP (3671/UDP)

Europaeischer Standard fuer Gebaeudeautomation (oft Weinzierl-Gateways). Steuert Licht, Jalousien, Heizung.
Risiko: MITTEL - unauthentifizierter Zugriff auf Gebaeudefunktionen moeglich.

DNP3 (20000/TCP+UDP)

Protokoll fuer SCADA-Systeme, vor allem in Energieversorgung und Wasserwirtschaft.
Risiko: HOCH - kritische Infrastruktur; oft ohne Authentifizierung.

PROFINET (DCP (Layer 2), 34962-34964/UDP)

Echtzeit-Ethernet-Standard von Siemens/PI fuer die Fabrikautomation. Geraetesuche laeuft per Layer-2-Broadcast (DCP).
Risiko: MITTEL - Geraetenamen und IP-Zuweisung manipulierbar.

VxWorks (WDB) (17185/UDP)

Echtzeit-Betriebssystem (Wind River) auf vielen Embedded-OT-Geraeten. Der WDB-Debug-Agent war historisch eine schwere Schwachstelle.
Risiko: HOCH - WDB-Agent erlaubt Speicherzugriff/Codeausfuehrung.

WARUM LIEFERN MANCHE NSE-SKRIPTE KEINE ERGEBNISSE?

Ein NSE-Skript liefert nur dann Ergebnisse, wenn der zugehoerige Port am Zielgeraet tatsaechlich offen ist. Leere Ergebnisse bedeuten meist:

1. Der Port ist geschlossen oder gefiltert (Firewall). Beispiel: laeuft 's7-info' ins Leere, ist Port 102 am Geraet nicht offen - das Geraet spricht also kein S7.

2. Das Geraet spricht ein anderes Protokoll. Viele OT-Geraete (z. B. VxWorks-Embedded, Drucker, Switches) nutzen FTP/Telnet/SNMP statt OT-Protokollen wie Modbus oder S7.

3. Das Geraet hat innerhalb des Zeitlimits (Script-/Host-Timeout) nicht geantwortet. Tote oder sehr langsame Geraete werden bewusst uebersprungen, damit der Scan nicht haengt.

4. UDP-Protokolle (BACnet, KNX, DNP3) antworten nur, wenn das Geraet aktiv lauscht - keine Antwort heisst hier nicht zwingend 'kein Geraet'.

Ein leeres NSE-Ergebnis ist also normalerweise KEIN Fehler des Tools, sondern eine korrekte Aussage: 'dieses Protokoll wurde an diesem Geraet nicht gefunden'.

TIPP - Datensammlung (FORCE): Das Profil 'Voll umfassend FORCE' erzwingt mit dem '+'-Prefix die Ausfuehrung jedes Scripts auf JEDEM offenen Port, unabhaengig von der normalen Port-Regel. Das findet OT-Dienste auch auf untypischen Ports, dauert aber deutlich laenger und erzeugt viele leere Versuche. Sinnvoll in der Lernphase - danach anhand der gesammelten Daten wieder auf die tatsaechlich genutzten Scripts ausduennen.

QUELLEN & VERANKERUNG DER RISIKOBEWERTUNG

Jede Port-Bewertung ist an eine ausgewiesene Quelle gebunden. OT/ICS-Protokolle: Rahmen IEC 62443 (Zonen und Conduits) + technischer Port-Beleg. Unsichere IT-Protokolle: Verkehrsregeln (HanselCraft-Voreinstellung, vom Anwender anpassbar). Gewichte und Ampel sind eine Priorisierungshilfe dieses Werkzeugs, keine Normvorgabe.

VR	Verkehrsregeln 1.0 (HanselCraft-Voreinstellung, Stand 12.11.2026) - unsichere IT-Protokolle in OT-Netzwerken; vom Anwender anpassbar (verkehrsregeln.json)
IEC-62443	IEC 62443 - Zonen und Conduits; Grundanforderungen u. a. Identifizierung/Authentisierung, Vertraulichkeit der Daten, eingeschraenkter Datenfluss
IANA	IANA Service Name and Transport Protocol Port Number Registry
CISA	CISA ICS Advisory (u.a. CVE-2025-7405: MODBUS/TCP ohne Authentisierung)
ODVA	ODVA - EtherNet/IP (CIP) Spezifikation
ITI-PORTS	ITI/ICS-Security-Tools PORTS.md (ICS-Protokoll-Portliste)