OTScan

OT Network Inventory & Risk Report

Version 2.0.1 | 28.09.2026

Netzwerk: Demo-Netz (synthetische Beispieldaten)

HIGH RISK OT-Steuerprotokolle + weitere Risiken offen

Hosts	Offene Ports	Krit. Ports (OT+IT)
5	8	8

SCAN-INFORMATIONEN

Netzwerk:	Demo-Netz (synthetische Beispieldaten)	**Scan gestartet:**	27.09.2026 11:06
Ziel:	192.168.10.0/24	**Dauer:**	200 s
Scan-Profil:	S7/Legacy schonend (NSE, geraeteschonend)	**Nmap Version:**	7.95
Portset:	ICS_OT_CORE	**Hosts gefunden:**	5

INHALT DIESES BERICHTS

2 EXECUTIVE SUMMARY

HIGH RISK - OT-Steuerprotokolle + weitere Risiken offen

KENNZAHLEN AUF EINEN BLICK

Gescannte Hosts:	**5**	**Offene Ports:**	8
Krit. Ports offen:	**8**	**Scan-Datum:**	27.09.2026 11:06

KEY FINDINGS

* KRITISCH: 5 Geräte gescannt - 1 Gerät(e) mit ungeschützten OT-Steuerprotokollen und weiteren Risiken (ROT)
* 5 offene OT-Steuerprotokoll-Port(s) ohne eingebaute Authentisierung/Verschlüsselung: Modbus/TCP (2), S7comm/ISO-TSAP (Siemens S7) (1), OPC UA (Binary) (1), BACnet/IP (1)
* 3 offene unsichere IT-Protokoll-Port(s): HTTP (1), FTP (1), Telnet (1)
* Häufigster Hersteller: Siemens (1 von 5 Geräten)
* SICHERHEITSRISIKO: 1 Gerät(e) mit Telnet (Port 23) offen

HANDLUNGSEMPFEHLUNGEN

1. OT-Steuerprotokolle (S7comm/ISO-TSAP (Siemens S7), Modbus/TCP, OPC UA (Binary), BACnet/IP) nur aus der zuständigen Zone/Leittechnik erreichbar machen - Firewall-Whitelisting und Zonen-/Conduit-Konzept (vgl. IEC 62443-3-2/3-3) prüfen
2. ROT markierte Geräte priorisiert prüfen: Erreichbarkeit einschränken, unnötige Dienste abschalten, Zugriffe protokollieren
3. Telnet (Port 23) auf 1 Gerät(en) deaktivieren -> SSH verwenden
4. FTP (Port 21) auf 1 Gerät(en) durch SFTP/FTPS ersetzen oder abschalten
5. Firmware-Stände der betroffenen Geräte mit Hersteller-Advisories (CERT@VDE, CISA, BSI) abgleichen

3 NETZWERK-HEATMAP - RISIKO NACH SUBNETZ & GERÄTETYP

KRIT-PORTS: mindestens ein bewertetes OT- oder IT-Protokoll offen CLEAN: keine bewerteten Protokolle offen

Subnetz (/24)	Hosts	SEC-BP-Ports	FW Krit	FW Blk	Top Gerätetyp	Risiko
192.168.10.0/24	5	8	0	0	SPS/PLC (Siemens S7)	KRIT-PORTS

GERÄTETYP-VERTEILUNG

Gerätetyp	Anz.	Anteil	Balken
SPS/PLC (Siemens S7)	1	20%	1
OPC-UA-Server (SCADA/DCS)	1	20%	1
Gebäudeautomation (BACnet)	1	20%	1
SPS/PLC (Bosch Rexroth IndraControl/ctrl	1	20%	1
Unbekannt	1	20%	1

SPS/PLC HMI/SCADA Netzwerk Windows/Linux Sonstige

4 KRITISCHE HOSTS - DETAILANSICHT (4 GERÄTE)

192.168.10.21 OPC-UA-Server (SCADA/DCS) | Telemecanique Electrique | Risk: 9

MAC-Adresse:	00:80:F4:44:55:66	**Gerätetyp:**	OPC-UA-Server (SCADA/DCS)
Hersteller:	Telemecanique Electrique	**Krit. Ports:**	21/tcp(FTP), 23/tcp(Telnet), 4840/t
TCP-Ports:	502,4840,21,23	**:**	

192.168.10.11 SPS/PLC (Siemens S7) | Siemens | Risk: 5

MAC-Adresse:	00:1B:1B:11:22:33	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens	**OS-Erkennung:**	Siemens SIMATIC S7-1200
S7 System:	SIMATIC 1200	**S7 Modul:**	6ES7 214-1AG40-0XB0
S7 Seriennr.:	S C-X4U421302016	**Krit. Ports:**	102/tcp(S7comm/ISO-TSAP (Siemens S7
TCP-Ports:	102,80	**:**	

192.168.10.34 SPS/PLC (Bosch Rexroth IndraControl/ctrlX) | Bosch Rexroth | Risk: 3

MAC-Adresse:	00:12:4B:AA:BB:CC	**Gerätetyp:**	SPS/PLC (Bosch Rexroth IndraControl
Hersteller:	Bosch Rexroth	**Krit. Ports:**	502/tcp(Modbus/TCP)
TCP-Ports:	502	**:**	

192.168.10.60 Gebäudeautomation (BACnet) | RuggedCom | Risk: 2

MAC-Adresse:	00:0A:DC:77:88:99	**Gerätetyp:**	Gebäudeautomation (BACnet)
Hersteller:	RuggedCom	**Krit. Ports:**	47808/udp(BACnet/IP)
UDP-Ports:	47808	**:**	

5 HOST-INVENTAR - 5 GERÄTE (SORTIERT NACH RISIKOSCORE)

IP-Adresse	MAC-Adresse	Gerätetyp	Risk	Acc%	OS	TCP-Ports	SNMP-Hostname
192.168.10.21	00:80:F4:44:55:66	OPC-UA-Server (SCA	9			502,4840,21,23	
192.168.10.11	00:1B:1B:11:22:33	SPS/PLC (Siemens S	5	95	Siemens SIMATIC S7-1200	102,80	
192.168.10.34	00:12:4B:AA:BB:CC	SPS/PLC (Bosch Rex	3			502	
192.168.10.60	00:0A:DC:77:88:99	Gebäudeautomation	2				
192.168.10.99	00:11:22:33:44:55		0				

7 TECHNISCHE DETAILS & ANHANG

KRITISCHE OFFENE PORTS (ÜBERSICHT)

Port/Proto	OT-Protokoll	Anzahl Hosts	Risikobewertung
502/tcp	Modbus/TCP	2	KRITISCH - sofort prüfen
102/tcp	S7comm/ISO-TSAP (Siemens S7)	1	Prüfen erforderlich
80/tcp	HTTP	1	Prüfen erforderlich
4840/tcp	OPC UA (Binary)	1	Prüfen erforderlich
21/tcp	FTP	1	Prüfen erforderlich
23/tcp	Telnet	1	Prüfen erforderlich
47808/udp	BACnet/IP	1	Prüfen erforderlich

NMAP SCAN-ARGUMENTE

```
nmap
  -sT
  -sV 192.168.10.0/24
```

8 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 Netzzugang 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)

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) [IM SCAN GEFUNDEN]

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

Die Einstufung, WELCHE Protokolle als unsicher gelten, stuetzt sich auf oeffentliche Quellen (IANA-Portbelegung, NIST SP 800-82, BSI ICS-Security-Kompendium, CISA-Advisories; IEC 62443 als Rahmen fuer Zonen/Conduits). Die GEWICHTE und AMPEL-SCHWELLEN sind eine interne, dokumentierte Heuristik von OTScan - keine Norm schreibt sie vor. Dieser Bericht ist KEINE Konformitaetsbewertung nach IEC 62443 (keine Security-Level-, FR/SR- oder Zonen-/Conduit-Bewertung), sondern eine Bestandsaufnahme offener Dienste als Grundlage dafuer.

SEC-BP	Security Best Practice - unsichere/Klartext- & Legacy-Protokolle (IEC 62443-3-3, NIST SP 800-82 Rev.3, BSI ICS-Security-Kompendium)
IEC62443	IEC 62443-3-3 - System Security Requirements and Security Levels (Zonen/Conduits, Netzsegmentierung)
NIST800-82	NIST SP 800-82 Rev.3 - Guide to Operational Technology (OT) Security (Segmentierung, Schwachstellen-/Scanning-Management)
BSI-ICS	BSI ICS-Security-Kompendium / IT-Grundschutz - Absicherung industrieller Steuerungssysteme
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	ICS-Security-Tools PORTS.md (ICS-Protokoll-Portliste)