OTScan

OT Network Inventory & Risk Report

Version 2.0.0 | 01.07.2026

Netzwerk: Beispiel-Werk Halle 3 / OT-Segment

MEDIUM RISK Kritische Ports gefunden

Hosts	Offene Ports	SEC-BP-krit. Ports
12	26	13

SCAN-INFORMATIONEN

Netzwerk:	Beispiel-Werk Halle 3 / OT-Segment	**Scan gestartet:**	Beispiel-Scan
CIDR:	192.168.10.0/24	**Dauer:**	600.00 s
Scan-Profil:	S7/Legacy schonend (Demo)	**Nmap Version:**	7.95
Portset:	ICS_STANDARD	**Hosts gefunden:**	12

INHALT DIESES BERICHTS

1. **Deckblatt** diese Seite
2. **Executive Summary** Kernaussagen, Key Findings, Empfehlungen
3. **Netzwerk-Heatmap** Risikoübersicht nach Subnetz & Gerätetyp
4. **Kritische Hosts** Detailansicht aller Geräte mit Risiko
5. **Host-Inventar** Vollständige Geräteliste
6. **Delta-Report** Änderungen seit letztem Scan (falls vorhanden)
7. **Technische Details** Scan-Parameter & Anhang
8. **ICS/OT-Glossar** Protokoll-Erklärungen, Links & Einordnung

2 EXECUTIVE SUMMARY

MEDIUM RISK - Kritische Ports gefunden

KENNZAHLEN AUF EINEN BLICK

Gescannte Hosts:	**12**	**Offene Ports:**	26
SEC-BP-krit. Ports offen:	**13**	**Scan-Datum:**	Beispiel-Scan

KEY FINDINGS

* ?? WARNUNG: 12 Geräte gescannt - MITTLERER Risiko-Level (GELB)
* ?? 13 kritische offene Ports gefunden (S7, Modbus, OPC-UA, etc.)
* Mehrheitlich Siemens AG-Geräte (3 von 12)
* ?? SICHERHEITSRISIKO: 2 Geräte mit Telnet (Port 23) offen

HANDLUNGSEMPFEHLUNGEN

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

3 NETZWERK-HEATMAP - RISIKO NACH SUBNETZ & GERÄTETYP

? SEC-BP-Ports: mindestens ein Protokoll aus der Security-Best-Practice-Liste gefunden ? CLEAN: keine SEC-BP-Protokolle offen

Subnetz (/24)	Hosts	SEC-BP-Ports	FW Krit	FW Blk	Top Gerätetyp	Risiko
192.168.10.0/24	12	13	0	0	SPS/PLC (Siemens S7)	SEC-BP-Ports

GERÄTETYP-VERTEILUNG

Gerätetyp	Anz.	Anteil	Balken
SPS/PLC (Siemens S7)	2	17%	2
SPS/PLC (Schneider Modicon)	2	17%	2
SPS/PLC (Phoenix/WAGO)	1	8%	1
OPC-UA-Server (SCADA/DCS)	1	8%	1
Energiemessgeraet	1	8%	1
SPS/PLC (Rockwell/Allen-Bradley)	1	8%	1
HMI / Bedienterminal	1	8%	1
Gebäudeautomation (BACnet)	1	8%	1
Netzwerk (Firewall/Switch)	1	8%	1
SPS/PLC (Bosch Rexroth IndraControl/ctrl	1	8%	1

SPS/PLC HMI/SCADA Netzwerk Windows/Linux Sonstige

4 KRITISCHE HOSTS - DETAILANSICHT (9 GERÄTE)

192.168.10.91 Netzwerk (Firewall/Switch) | Hirschmann | Risk: 7

MAC-Adresse:	00:1C:06:99:91:01	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Hirschmann	**OS-Erkennung:**	Managed Industrial Switch
Krit. Ports:	161/udp(SNMP (v1/v2)), 23/tcp(Telne	**TCP-Ports:**	23,80
UDP-Ports:	161	**:**	

192.168.10.12 SPS/PLC (Siemens S7) | Siemens AG | Risk: 5

MAC-Adresse:	00:1B:1B:2A:11:02	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	Siemens SIMATIC S7-300
S7 System:	SPS_Halle3_02 / Module Type: CPU 31	**S7 Modul:**	6ES7 315-2EH14-0AB0 / Version: 3.2.
Krit. Ports:	21/tcp(FTP), 23/tcp(Telnet)	**TCP-Ports:**	102,21,23

192.168.10.71 HMI / Bedienterminal | Siemens AG | Risk: 5

MAC-Adresse:	00:0E:8C:77:71:04	**Gerätetyp:**	HMI / Bedienterminal
Hersteller:	Siemens AG	**OS-Erkennung:**	Siemens Comfort Panel (HMI)
Krit. Ports:	5900/tcp(VNC (RFB)), 80/tcp(HTTP)	**TCP-Ports:**	5900,80

192.168.10.11 SPS/PLC (Siemens S7) | Siemens AG | Risk: 2

MAC-Adresse:	00:1B:1B:2A:11:01	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	Siemens SIMATIC S7-1500
S7 System:	SPS_Halle3_01 / Module Type: CPU 15	**S7 Modul:**	6ES7 515-2AM01-0AB0 / Basic Hardwar
Krit. Ports:	80/tcp(HTTP)	**TCP-Ports:**	102,80,443

192.168.10.21 SPS/PLC (Schneider Modicon) | Schneider Electric | Risk: 2

MAC-Adresse:	00:80:F4:33:21:05	**Gerätetyp:**	SPS/PLC (Schneider Modicon)
Hersteller:	Schneider Electric	**OS-Erkennung:**	Schneider Modicon M340
Krit. Ports:	80/tcp(HTTP)	**TCP-Ports:**	502,80

192.168.10.31 SPS/PLC (Phoenix/WAGO) | WAGO | Risk: 2

MAC-Adresse:	00:30:DE:44:31:07	**Gerätetyp:**	SPS/PLC (Phoenix/WAGO)
Hersteller:	WAGO	**OS-Erkennung:**	WAGO PFC200 (CODESYS)
Krit. Ports:	80/tcp(HTTP)	**TCP-Ports:**	2455,502,80

192.168.10.51 Energiemessgeraet | Janitza electronics | Risk: 2

MAC-Adresse:	00:1D:9C:55:51:03	**Gerätetyp:**	Energiemessgeraet
Hersteller:	Janitza electronics	**OS-Erkennung:**	Janitza UMG 96-PA (Stromzaehler)
Krit. Ports:	8080/tcp(HTTP (8080))	**TCP-Ports:**	502,8080

192.168.10.61 SPS/PLC (Rockwell/Allen-Bradley) | Rockwell Automation | Risk: 2

MAC-Adresse:	00:00:BC:66:61:09	**Gerätetyp:**	SPS/PLC (Rockwell/Allen-Bradley)
Hersteller:	Rockwell Automation	**OS-Erkennung:**	Allen-Bradley CompactLogix
Krit. Ports:	80/tcp(HTTP)	**TCP-Ports:**	44818,80

192.168.10.101 SPS/PLC (Bosch Rexroth IndraControl/ctrlX) | Bosch Rexroth | Risk: 2

MAC-Adresse:	00:60:34:AA:B1:0C	**Gerätetyp:**	SPS/PLC (Bosch Rexroth IndraControl
Hersteller:	Bosch Rexroth	**OS-Erkennung:**	Bosch Rexroth IndraControl
Krit. Ports:	21/tcp(FTP)	**TCP-Ports:**	1200,21

5 HOST-INVENTAR - 12 GERÄTE (SORTIERT NACH RISIKOSCORE)

IP-Adresse	MAC-Adresse	Gerätetyp	Risk	Acc%	OS	TCP-Ports	SNMP-Hostname
192.168.10.91	00:1C:06:99:91:01	Netzwerk (Firewall	7	94	Managed Industrial Switch	23,80	
192.168.10.12	00:1B:1B:2A:11:02	SPS/PLC (Siemens S	5	94	Siemens SIMATIC S7-300	102,21,23	
192.168.10.71	00:0E:8C:77:71:04	HMI / Bedientermin	5	94	Siemens Comfort Panel (HMI)	5900,80	
192.168.10.11	00:1B:1B:2A:11:01	SPS/PLC (Siemens S	2	94	Siemens SIMATIC S7-1500	102,80,443	
192.168.10.21	00:80:F4:33:21:05	SPS/PLC (Schneider	2	94	Schneider Modicon M340	502,80	
192.168.10.31	00:30:DE:44:31:07	SPS/PLC (Phoenix/W	2	94	WAGO PFC200 (CODESYS)	2455,502,80	
192.168.10.51	00:1D:9C:55:51:03	Energiemessgeraet	2	94	Janitza UMG 96-PA (Stromzaeh	502,8080	
192.168.10.61	00:00:BC:66:61:09	SPS/PLC (Rockwell/	2	94	Allen-Bradley CompactLogix	44818,80	
192.168.10.101	00:60:34:AA:B1:0C	SPS/PLC (Bosch Rex	2	94	Bosch Rexroth IndraControl	1200,21	
192.168.10.22	00:80:F4:33:21:2A	SPS/PLC (Schneider	0	94	Modbus TCP Gateway	502	
192.168.10.41	00:0C:29:41:41:11	OPC-UA-Server (SCA	0	94	OPC-UA Server (Windows)	4840,3389	
192.168.10.81	00:40:9D:88:81:02	Gebäudeautomation	0	94	BACnet Building Controller		

7 TECHNISCHE DETAILS & ANHANG

KRITISCHE OFFENE PORTS (ÜBERSICHT)

Port/Proto	OT-Protokoll	Anzahl Hosts	Risikobewertung
80/tcp	HTTP	6	KRITISCH - sofort prüfen
21/tcp	FTP	2	KRITISCH - sofort prüfen
23/tcp	Telnet	2	KRITISCH - sofort prüfen
8080/tcp	HTTP (8080)	1	Prüfen erforderlich
5900/tcp	VNC (RFB)	1	Prüfen erforderlich
161/udp	SNMP (v1/v2)	1	Prüfen erforderlich

NMAP SCAN-ARGUMENTE

```
nmap
  -sS
  -sU
  -p T:21,23,80,102,443,502,2455,4840,44818,5900,1200,8080 U:161,47808
  --script ot-scan 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) [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) [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

Jede Port-Bewertung ist an einen anerkannten oeffentlichen Standard gebunden. OT/ICS-Protokolle: Rahmen IEC 62443 / NIST SP 800-82 + technischer Port-Beleg. Unsichere IT-Protokolle: Security Best Practice (IEC 62443-3-3, NIST SP 800-82, BSI ICS-Security-Kompendium).

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)