OTScan 3

OT-/ICS-NETZWERKSCANNER · HANSELCRAFT

NETZWERK-CHECK · ALLE NETZWERKE

Standort

6 Netzwerke · Stand 13.11.2026

GELB

NETZWERKE	GERÄTE	INVENTAR	STAND
6 von 6 gescannt	115	126 Einträge	13.11.2026

1 Gesamtbild

GELB **6 von 6 Netzwerken** gescannt (6 GELB).

115 Geräte im Scan	**108** mit unsicheren Diensten	**108** davon ohne Firewall-Verkehr
32 mit Herstellermeldung	**17** neu für die CMDB	**1** in der CMDB, nicht gefunden

INVENTAR ÜBER ALLE QUELLEN (126 EINTRÄGE)



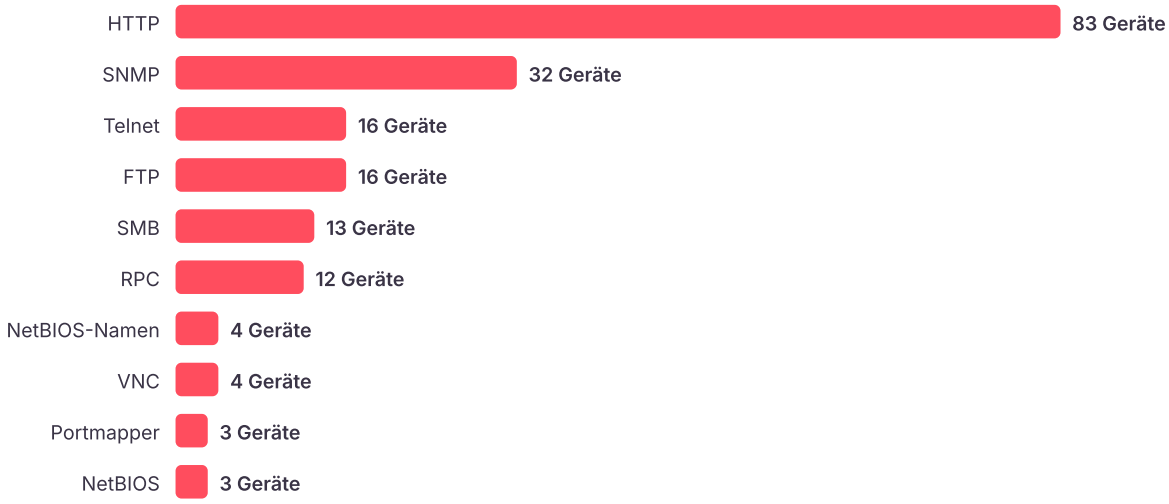
bestätigt (alle Quellen) **98** neu für die CMDB **17** nicht gefunden **1** CMDB ohne IP **1** nur Verkehr, unbekannt **9**

Status	Anzahl	Was tun?
bestätigt (alle Quellen)	98	nichts – durch Scan und Verkehr bestätigt
neu für die CMDB	17	in die CMDB aufnehmen
nicht gefunden	1	vor Ort prüfen: abgebaut, aus, falsche IP?
CMDB ohne IP	1	IP-Adresse in der CMDB nachtragen
nur Verkehr, unbekannt	9	Gerät suchen und in die CMDB aufnehmen

2 Alle Netzwerke im Überblick

	Netzwerk	Geräte	unsicher	Meldung	Maßn. hoch	neu CMDB	nicht gef.	Scan
GELB	Energieverteilung	24	23	5	6	4	0	10.11.2026 11:19
GELB	Halle3_CAM	18	18	0	1	2	1	09.11.2026 11:09
GELB	Lackiererei_Leitstand	15	13	5	8	2	0	10.11.2026 14:07
GELB	Montage_Anlagennetz	22	19	11	17	3	0	10.11.2026 15:48
GELB	Presse_Maschinennetz	20	20	9	22	3	0	10.11.2026 09:26
GELB	Prueffeld	16	15	2	7	3	0	10.11.2026 16:42

3 Unsichere Dienste und Maßnahmen

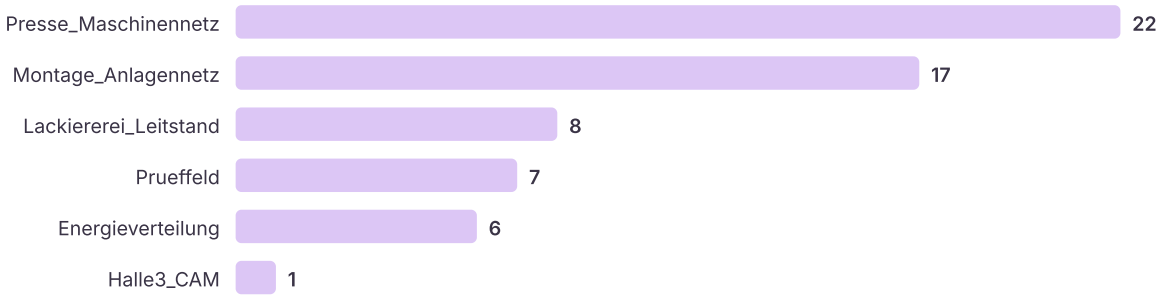


61
Maßnahmen hoch

300
Maßnahmen mittel

30
Maßnahmen niedrig

NETZWERKE MIT DEN MEISTEN DRINGLICHEN MASSNAHMEN



4 Herstellermeldungen

32 Geräte in 5 Netzwerken passen zu Herstellermeldungen. Die häufigsten:

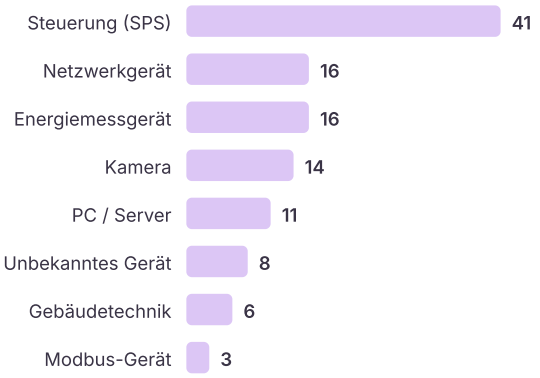
Meldung	Titel	CVSS	Güte	Geräte	Netzw.
SSA-712929	SSA-712929: Denial of Service Vulnerability in OpenSSL (CVE-2022-0778) Affecting Industria	7.5	exakt, modell	12	3
SSA-473245	SSA-473245: Denial of Service Vulnerability in Profinet Devices	7.5	exakt, modell	8	3
SSA-876787	SSA-876787: Open Redirect Vulnerability in SIMATIC S7-1500 and S7-1200 CPUs	4.7	exakt	7	3
SSA-915282	SSA-915282: Denial of service Vulnerability in Interniche IP-Stack based Industrial Device	7.5	exakt	6	3
SSA-725549	SSA-725549: Denial of Service of ICMP in Industrial Devices	5.3	exakt	6	3
BOSCH-SA-741752	Multiple vulnerabilities in Rexroth IndraMotion and IndraLogic series	10.0	modell	5	1
BOSCH-SA-475180	Vulnerabilities in CODESYS V2 runtime systems	9.8	modell	5	1
BOSCH-SA-577411	Vulnerabilities in the communication protocol of the PLC runtime	8.1	modell	5	1
SSA-224824	SSA-224824: Denial of Service Vulnerabilities in SIMATIC S7-1200 CPU Family Before V4.7	7.5	exakt	5	3
SSA-392349	SSA-392349: Denial of Service Vulnerability in Industrial Devices	7.5	exakt	5	3
BOSCH-SA-152060	Denial of Service in PLC Runtime affecting Rexroth IndraMotion Products	7.5	modell	5	1
BOSCH-SA-350374	Vulnerability in the routing protocol of the PLC runtime	7.3	modell	5	1
SSA-717113	SSA-717113: Cross-Site Request Forgery (CSRF) Vulnerability in SIMATIC S7-1200 CPUs before	7.1	exakt	5	3
SSA-478960	SSA-478960: Missing CSRF Protection in the Web Server Login Page of Industrial Controllers	6.5	exakt	5	3
SSA-264814	SSA-264814: Timing Based Side Channel Vulnerability in the OpenSSL RSA Decryption in SIMAT	5.9	exakt	5	3

5 Applikationen und Gerätelandschaft

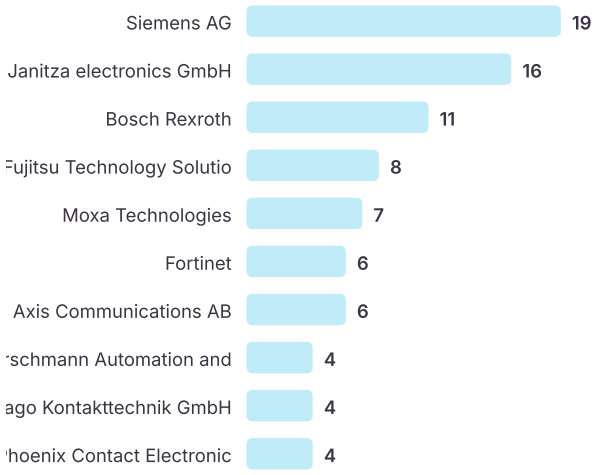
APPLIKATIONEN JE NETZWERK (FIREWALL-VERKEHR, DOKUMENTATIONS-DATENBANK)

Netzwerk	häufigste Applikationen (Verbindungen)
Energieverteilung	Energiemanagement (1.134.312), Zeitdienst und Protokollierung (39.671)
Halle3_CAM	Videomanagement (91.741), Zeitdienst und Protokollierung (30.698)
Lackiererei_Leitstand	MES Produktionsdaten (206.261), Prozessleitsystem (165.909), Zeitdienst und Protokollierung (32.894), Fernwartung (38)
Montage_Anlagennetz	MES Produktionsdaten (928.454), Prozessleitsystem (135.954), Zeitdienst und Protokollierung (42.355), Fernwartung (61)
Presse_Maschinennetz	MES Produktionsdaten (800.793), Zeitdienst und Protokollierung (32.803), Fernwartung (44)
Prueffeld	Qualitätsdaten (53.894), Zeitdienst und Protokollierung (35.614)

GERÄTEKLASSEN



HERSTELLER



6 Begriffe

CMDB	Inventar (CMDB): die selbst gepflegte Geräteliste als Excel (Vorlage aus OTScan 3 oder eigene Liste). Liefert Name, Typ, Hersteller, Ort, Gewerk und Verantwortliche. OTScan 3 liest sie nur.
Gesamtinventar	Eine Excel mit allen Geräten aus CMDB, Scan und Splunk – je Wert mit Quelle. Grundlage der Erstinventarisierung.
Dokumentations-Datenbank	Applikationen, Server, Zonen und Netzwerkbereiche aus der Netzwerk- und Applikationsübersicht und dem Recherche-Register. OTScan 3 ordnet damit Kommunikationspartner Applikationen zu.
Scan / Stufenlauf	Aktive Erkennung durch OTScan 3 in Stufen (Erreichbarkeit, Dienste, Geräteangaben).
Splunk	Auswertung der Firewall-Logs: Adressen, Partner, Ports, Zonen. Verkehr innerhalb eines Netzwerks ist dort nicht sichtbar.
Ampel	GRÜN = keine unsicheren Dienste. GELB = unsichere Dienste – geplant schließen. ROT = besonders gefährliche Dienste – sofort klären.
Unsicherer Dienst	Dienst, den die Verkehrsregeln (HanselCraft-Voreinstellung, anpassbar) verbieten oder nur abgesichert erlauben (z. B. FTP, Telnet, HTTP-Anmeldung, SNMPv1/v2c).
Ohne Firewall-Verkehr	Der Dienst wurde im Splunk-Zeitraum nicht über die Firewall genutzt – Kandidat zum Abschalten.
Herstellermeldung	Sicherheitsmeldung eines Herstellers (CSAF, CISA ICS). Güte exakt / modell / hersteller.
Zone / Service / Policy	Aus dem FortiGate-Log: Sicherheitszone von Quelle und Ziel, Dienstname, Nummer der Firewall-Regel.
Risk (Detailansicht)	2 Punkte je kritischem Port (höchstens 8), +2 bei Herstellermeldung mit CVSS ≥ 7, +1 bei schwächerer Meldung.