Montage_Anlagennetz

192.168.30.0/24 | Stufenlauf komplett | Scan 10.11.2026 14:20, Dauer 1 Std. 28 Min.

Ampel GELB: Handlungsbedarf

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

22	19	38	2
Geräte gefunden	mit unsicherem Dienst	unsichere Dienste	nur im Firewall-Verkehr

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).

Was ist zu tun?

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".

Veränderung seit dem letzten vollständigen Scan

Kein vollständiger früherer Scan dieses Netzwerks zum Vergleich vorhanden.

Unsichere Dienste

Bewertet nach den Verkehrsregeln (HanselCraft-Voreinstellung, anpassbar). Ein unsicherer Dienst ist kein Angriff, aber eine offene Tür, die geplant geschlossen werden sollte.

Dienst	Geräte	Warum riskant	Was tun
HTTP (TCP 80)	15	Anmeldung und Einstellungen gehen unverschlüsselt durchs Netzwerk.	Auf HTTPS umstellen oder abschalten; Anmelden über HTTP ist laut Verkehrsregeln nicht erlaubt.
SNMP (UDP 161)	10	Bei v1/v2c geht das Passwort (Community) unverschlüsselt durchs Netzwerk.	SNMPv1/v2c und 'public' sind laut Verkehrsregeln nicht erlaubt: auf SNMPv3 umstellen.
Telnet (TCP 23)	5	Passwörter und Befehle gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.
FTP (TCP 21)	2	Benutzername, Passwort und Dateien gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten, sonst SFTP oder FTPS nutzen.

Dienst	Geräte	Warum riskant	Was tun
SMB (TCP 445)	2	Alte Versionen (SMBv1) sind ein häufiger Weg für Schadsoftware.	SMBv1 abschalten (laut Verkehrsregeln nicht erlaubt), SMBv3 mit Signierung, Zugriff begrenzen.
VNC (TCP 5900)	2	Bild, Eingaben und oft das Passwort gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten oder nur verschlüsselt (TLS, VPN, SSH-Tunnel).
RPC (TCP 135)	2	Häufiger Angriffspunkt; zeigt, welche Windows-Dienste laufen.	Nur wenn technisch nötig und nur für freigegebene Rechner; sonst per Firewall sperren.

Offen, aber über die Firewall nicht genutzt (Splunk 02.11.2026 - 08.11.2026): 38 unsichere Dienste ohne erlaubten Verkehr. Das sind die ersten Kandidaten zum Abschalten. Splunk sieht nur Verkehr über die Firewall, nicht innerhalb des Netzwerks - vorher mit dem Anlagenverantwortlichen klären.

Dienst	offen	ohne Verkehr	Adressen ohne Verkehr
HTTP (TCP 80)	15	15	192.168.30.3, 192.168.30.4, 192.168.30.10, 192.168.30.11, 192.168.30.15, 192.168.30.16, 192.168.30.20, 192.168.30.21, 192.168.30.22, 192.168.30.25, 192.168.30.26, 192.168.30.30, 192.168.30.31, 192.168.30.101, 192.168.30.102
SNMP (UDP 161)	10	10	192.168.30.1, 192.168.30.2, 192.168.30.3, 192.168.30.4, 192.168.30.10, 192.168.30.11, 192.168.30.20, 192.168.30.30, 192.168.30.31, 192.168.30.102
Telnet (TCP 23)	5	5	192.168.30.3, 192.168.30.4, 192.168.30.30, 192.168.30.31, 192.168.30.102
FTP (TCP 21)	2	2	192.168.30.20, 192.168.30.22
RPC (TCP 135)	2	2	192.168.30.60, 192.168.30.61
SMB (TCP 445)	2	2	192.168.30.60, 192.168.30.61
VNC (TCP 5900)	2	2	192.168.30.25, 192.168.30.26

Bekannte Schwachstellen (Herstellermeldungen)

Abgleich der erkannten Modelle und Firmware-Stände mit den Sicherheitsmeldungen der Hersteller (Siemens, Bosch, CERT@VDE, CISA u. a., Stand 2026-10-27). "exakt" = Firmware liegt im betroffenen Bereich, "Modell" = Modell passt, Firmware nicht bekannt oder nicht vergleichbar - am Gerät prüfen. KEV = laut CISA aktiv ausgenutzt.

Meldung	Modell / Firmware	Geräte	CVSS	KEV	Güte	Maßnahme laut Hersteller
SSA-452276	CPU 1516-3 PN/DP 2.9.4	1	9.6	-	exakt	Update to V2.9.9 or later version
SSA-591731	CPU 1516-3 PN/DP 2.9.4	1	9.6	-	exakt	Disable the webserver if not required on the affected systems. Restrict the access to Port 80/tcp and 443/tcp to trusted IP address only
SSA-688146	CPU 1516-3 PN/DP 2.9.4	1	9.1	-	exakt	Restrict TIA project download to trusted personnel only.
SSA-699386	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.1	-	exakt	Update to V4.5 or later version
SSA-710008	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.1	-	exakt	Update to V4.4 or later version
SSA-723487	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.0	-	exakt	Update to V4.6 or later version
SSA-552702	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	8.8	-	exakt	Update to V4.4 or later version
SSA-224824	CPU 1214C DC/DC/DC 4.2.3; CPU 1214C DC/DC/DC 4.4.1; CPU 1215	3	7.5	-	exakt	Update to V4.7 or later version
SSA-349422	CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN/DP 3.2.15	2	7.5	-	exakt	Update to V3.2.17 or later version
SSA-382653	CPU 1516-3 PN/DP 2.9.4	1	7.5	-	exakt	Update to V2.9.7 or later version
SSA-392349	CPU 1516-3 PN/DP 2.9.4; CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN	3	7.5	-	exakt	As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SSA-473245	CMDB: Siemens TP1200 Comfort V16; CPU 315-2 PN/DP 3.2.14; CP	4	7.5	-	exakt	Restrict network access to affected devices
SSA-480230	CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN/DP 3.2.15; SIMATIC HMI	3	7.5	-	exakt	Update to V3.2.16 or later version

Meldung	Modell / Firmware	Geräte	CVSS	KEV	Güte	Maßnahme laut Hersteller
SSA-592380	CPU 1516-3 PN/DP 2.9.4	1	7.5	-	exakt	Limit access to port 102/tcp to trusted users and systems only
SSA-593272	CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN/DP 3.2.15	2	7.5	-	exakt	Currently no fix is planned

Weitere 35 Meldungen und alle CVE-Nummern: Excel, Blatt "Schwachstellen".

Geräte (22)

Geräte mit unsicherem Dienst stehen oben (Punkt). Alle Details je Gerät - Ports, Versionen, Skriptausgaben - stehen in der Excel-Datei.

IP-Adresse	Gerät	Hersteller	Name / Modell, Firmware	Unsichere Dienste	Offene Ports
192.168.30.3	Netzwerkgerät	Cisco Systems	Cisco IOS Software, IE3x00 Software (IE3x00-UNIVERSALK9-M) FW...	HTTP, SNMP, Telnet	T:22,443,23,80 U:161
192.168.30.4	Netzwerkgerät	Hirschmann Automation and Control	Hirschmann Railswitch Power RSP35 HiOS-3S 08.7.02 FW 08.7.02	HTTP, SNMP, Telnet	T:23,80 U:161
192.168.30.20	Steuerung (SPS)	Schneider Electric	Modicon M340 CPU, Firmware V2.70 FW V2.70	FTP, HTTP, SNMP	T:21,80,502 U:161
192.168.30.30	Unbekanntes Gerät	Moxa Technologies	NPort 5150 Firmware 3.9 Build 20052616 FW 3.9	HTTP, SNMP, Telnet	T:23,80 U:161
192.168.30.31	Unbekanntes Gerät	Moxa Technologies	NPort 5150 Firmware 3.9 Build 20052616 FW 3.9	HTTP, SNMP, Telnet	T:23,80 U:161
192.168.30.102	Netzwerkgerät	Hirschmann Automation and Control	Hirschmann Automation and Control GmbH Hirschmann RSR	HTTP, SNMP, Telnet	T:23,80 U:161
192.168.30.22	Steuerung (SPS)	Wago Kontakttechnik	WAGO 750-8212 PFC200 G2 2ETH RS	FTP, HTTP	T:21,22,80,443,502,2455
192.168.30.25	Steuerung (SPS)	Siemens	SIMATIC HMI Miniweb	HTTP, VNC	T:80,5900,102
192.168.30.26	Steuerung (SPS)	Siemens	SIMATIC HMI Miniweb	HTTP, VNC	T:80,5900,102
192.168.30.60	PC / Server	Fujitsu Technology Solutions	-	RPC, SMB	T:135,445,3389
192.168.30.61	PC / Server	Fujitsu Technology Solutions	-	RPC, SMB	T:135,445
192.168.30.10	Steuerung (SPS)	Siemens	H3-MO-SPS-L1 · CPU 315-2 PN/DP FW 3.2.14	HTTP, SNMP	T:80,102 U:161,34964
192.168.30.11	Steuerung (SPS)	Siemens	H3-MO-SPS-L2 · CPU 317-2 PN/DP FW 3.2.15	HTTP, SNMP	T:80,102 U:161,34964
192.168.30.1	Netzwerkgerät	Fortinet	-	SNMP	T:443 U:161
192.168.30.2	Netzwerkgerät	Siemens	SCALANCE XC208 6GK5 208-0BA00-2AC2 FW V4.3	SNMP	T:22,443 U:161
192.168.30.15	Steuerung (SPS)	Siemens	H3-MO-SPS-ST01 · CPU 1214C DC/DC/DC FW 4.2.3	HTTP	T:102,80,443
192.168.30.16	Steuerung (SPS)	Siemens	H3-MO-SPS-ST02 · CPU 1215C DC/DC/DC FW 4.5.2	HTTP	T:102,80,443
192.168.30.21	Steuerung (SPS)	OMRON	-	HTTP	T:80,9600,44818 U:9600
192.168.30.101	Steuerung (SPS)	Siemens, Automations & Drives	SIMATIC HMI	HTTP	T:80,102,443
192.168.30.12	Steuerung (SPS)	Siemens	H3-MO-SPS-L3 · CPU 1516-3 PN/DP FW 2.9.4	-	T:102,443,4840
192.168.30.17	Steuerung (SPS)	Siemens	H3-MO-SPS-ST03 · CPU 1214C DC/DC/DC FW 4.4.1	-	T:102
192.168.30.100	Steuerung (SPS)	Siemens	-	-	T:102,4840

Firewall-Verkehr und CMDB

Splunk 02.11.2026 - 08.11.2026: 2 Geräte sind nur im Firewall-Verkehr sichtbar, nicht im Scan. Neue und betroffene CMDB-Zeilen stehen in der Datei "..._CMDB-Nachtrag.xlsx", die Suchhilfe (MAC, Ort, Partner) im Excel-Blatt "Nur in Splunk".

IP-Adresse	Einschätzung	In CMDB	Splunk-Ports	Zuletzt
192.168.30.90	Vorhanden - nur ausgehend	nein	-	2026-11-08
192.168.30.91	Vorhanden - nur ausgehend	nein	-	2026-11-08

CMDB (Musterwerk_Halle3_CMDB.xlsx): 19 Einträge in diesem Netzwerk. 3 Geräte im Scan, aber nicht in der CMDB: 192.168.30.1, 192.168.30.17, 192.168.30.26. 0 CMDB-Einträge wurden im Scan nicht gefunden (Liste: Excel, Blatt "CMDB-Ansicht").

Kommunikation über die Firewall

Splunk 02.11.2026 - 08.11.2026: 13 Verbindungsarten mit 7 Partnerzonen. Keine erlaubte Verbindung nutzt ein unsicheres Protokoll. Die vollständige Liste (alle Partner, Ports, Geräte) steht im Excel-Blatt "Kommunikation".

Richtung	Partnerzone / -netz	Port	Dienst	Geräte	Verbindungen	Hinweis
eingehend	Z-Produktion	TCP 102	S7	10	753.530	-
eingehend	Z-Produktion	TCP 4840	OPC-UA	2	151.335	-
eingehend	Z-Leitebene	TCP 502	MODBUS	2	98.695	-
ausgehend	Z-Infrastruktur	UDP 123	NTP	21	30.158	-
ausgehend	Z-Produktion	TCP 102	S7	1	22.140	-
eingehend	Z-Leitebene	UDP 9600	OMRON-FINS	1	21.379	-
ausgehend	Z-Leitebene	TCP 502	MODBUS	1	15.880	-
ausgehend	Z-Infrastruktur	UDP 514	SYSLOG	3	9.745	-
ausgehend	Z-Infrastruktur	TCP 443	HTTPS	2	2.452	-
eingehend	Z-Engineering	TCP 102	S7	10	1.431	-
eingehend	Z-DMZ	TCP 3389	RDP	1	61	-
eingehend	Z-Engineering	TCP 5900	VNC	1	12	nur abgewiesen
eingehend	Z-Engineering	TCP 21	FTP	1	6	nur abgewiesen

Kennzahlen

Kennzahl	Dieser Scan	Letzter vollständiger Scan
Ampel	gelb	-
Geräte gefunden	22	-
Geräte mit unsicherem Dienst	19	-
Unsichere Dienste	38	-
Modell oder Firmware erkannt	17 (77 %)	-
davon mit Firmware-Stand	12	-
Unsichere Dienste ohne Firewall-Verkehr	38	-
Nur im Firewall-Verkehr (Splunk)	2	-
Gefundene Geräte in der CMDB	19 von 22	-
CMDB-Einträge im Scan gefunden	19 von 19	-
Geräte mit Herstellermeldung (Firmware betroffen)	9	-
Geräte mit Herstellermeldung (nur Modell passt)	2	-
davon aktiv ausgenutzte Lücke (KEV)	0	-
Erlaubte unsichere Verbindungen über die Firewall	0	-

Zum Abarbeiten: "..._Massnahmen.xlsx" (unsichere Dienste und Herstellermeldungen je Gerät mit Ort, Priorität und Status-Spalte). Für die CMDB: "..._CMDB-Delta.xlsx" (neu / geändert / fehlt).

Über diesen Scan

Angabe	Wert
Netzwerk	Montage_Anlagennetz
Adressbereich	192.168.30.0/24
Scan-Art	Stufenlauf komplett
Portauswahl	ICS_OT_CORE
Beginn	10.11.2026 14:20
Ende	10.11.2026 15:48
Dauer	1 Std. 28 Min.
Vollständig	ja
nmap-Version	7.94
Bericht erstellt	13.11.2026 01:52

Bewertung: Jeder offene Port wird gegen die Verkehrsregeln (HanselCraft-Voreinstellung, angelehnt an IEC 62443) geprüft. Unerlaubte Protokolle mit Fernsteuerung oder Dateizugriff zählen 3, unerlaubte mit Klartext-Anmeldung 2, Zweitports und mit TLS zulässige 1. Ein Portscan zeigt keine Versionen der Anmeldeverfahren (z. B. SMBv1/v3, SNMPv1/v3); diese sind am Gerät zu prüfen. Der Scan nutzt keine Angriffs-, Brute-Force- oder Schwachstellenskripte.

Scan-Argumente (je Stufe, ohne Ziellisten):

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 192.168.30.0/24