OTScan 3

OT-/ICS-NETZWERKSCANNER · HANSELCRAFT

GERÄTE-DETAILANSICHT

Montage_Anlagennetz

Karten je Gerät mit Firewall-Kommunikation (Zone · Service · Policy)

GERÄTE	NETZWERKE	VERBINDUNGEN	STAND
24	1	5 je Richtung + alle geblockten	13.11.2026

So lesen

Je Gerät: Angaben aus dem Scan, Name und Ort aus der CMDB und die Kommunikation über die Firewall aus Splunk – je Richtung die 5 häufigsten erlaubten Verbindungen und alle geblockten, je mit Quell- und Zielzone, Service, Policy, Aktion und Anzahl. Kritische Ports stehen voll ausgeschrieben mit Klartext-Erklärung. Unter dem Partner steht, soweit bekannt, das System bzw. die Applikation aus der Dokumentations-Datenbank.

	Risk 7–10: mehrere kritische Ports und/oder Herstellermeldung CVSS ≥ 7
	Risk 4–6
	Risk 1–3
	Risk 0: keine kritischen Ports
	nur im Firewall-Verkehr (Splunk), nicht im Scan

Montage_Anlagennetz · 24 Geräte · Scan 10.11.2026 15:48 · Splunk 2026-11-02 – 2026-11-08

192.168.30.20 SPS/PLC (Schneider Modicon) | Schneider Electric | Risk: 8

MAC-Adresse:	00:00:54:1E:8F:9A	**Gerätetyp:**	SPS/PLC (Schneider Modicon)
Hersteller:	Schneider Electric	**OS-Erkennung:**	–
Firmware:	V2.70	**UDP-Ports:**	161
TCP-Ports:	21,80,502	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-FT	**Ort (CMDB):**	Halle 3, Fördertechnik Montage
Meldung:	SEVD-2021-313-05 (CVSS 9.8, Güte modell) +2	**Meldungen:**	3

Kritische Ports:
Port 21/TCP – FTP: Dateiübertragung
Port 80/TCP – HTTP: Weboberfläche des Geräts
Port 161/UDP – SNMP: Abfrage von Gerätedaten

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	192.168.30.20 Z-Montage-Anlagennetz	502/6	MODBUS	31	accept	58.222
Firewall Outbound						
192.168.30.20 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.210

192.168.30.3 Netzwerk (Firewall/Switch) | Cisco Systems | Risk: 6

MAC-Adresse:	00:00:0C:1E:18:BD	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Cisco Systems	**OS-Erkennung:**	Cisco IOS 17
Firmware:	17.9.4	**UDP-Ports:**	161
TCP-Ports:	22,443,23,80	**Lastboot:**	–
CMDB-Name:	H3-MO-SW-02	**Ort (CMDB):**	Halle 3, Montagelinie 2, Schaltschrank +A1

Kritische Ports:
Port 23/TCP – Telnet: Fernzugang auf die Kommandozeile
Port 80/TCP – HTTP: Weboberfläche des Geräts
Port 161/UDP – SNMP: Abfrage von Gerätedaten

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.3 Z-Montage-Anlagennetz	10.20.10.40 Z-Infrastruktur SYSLOG-01 · Zeitdienst und Protokollierung	514/17	SYSLOG	14	accept	3.552
192.168.30.3 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.167

192.168.30.4 Netzwerk (Firewall/Switch) | Hirschmann Automation and Cont | Risk: 6

MAC-Adresse:	00:80:63:1E:1F:CA	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Hirschmann Automation and Control GmbH	**OS-Erkennung:**	–
Firmware:	08.7.02	**UDP-Ports:**	161
TCP-Ports:	23,80	**Lastboot:**	–
CMDB-Name:	H3-MO-SW-03	**Ort (CMDB):**	Halle 3, Montagelinie 3, Schaltschrank +A1
Kritische Ports:	**Port 23/TCP** – Telnet: Fernzugang auf die Kommandozeile **Port 80/TCP** – HTTP: Weboberfläche des Geräts **Port 161/UDP** – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.4 Z-Montage-Anlagennetz	10.20.10.40 Z-Infrastruktur SYSLOG-01 · Zeitdienst und Protokollierung	514/17	SYSLOG	14	accept	3.366
192.168.30.4 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.870

192.168.30.10 SPS/PLC (Siemens S7) | Siemens AG | Risk: 6

MAC-Adresse:	00:1B:1B:1E:49:18	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	3.2.14	**UDP-Ports:**	161,34964
TCP-Ports:	80,102	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-L1	**Ort (CMDB):**	Halle 3, Montagelinie 1
Meldung:	SSA-473245 (CVSS 7.5, Güte exakt) +10	**Meldungen:**	11
Kritische Ports:	**Port 80/TCP** – HTTP: Weboberfläche des Geräts **Port 161/UDP** – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.10 Z-Montage-Anlagennetz	102/6	S7	51	accept	103.421
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.10 Z-Montage-Anlagennetz	102/6	S7	53	accept	212
Firewall Outbound						
192.168.30.10 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.034

192.168.30.11 SPS/PLC (Siemens S7) | Siemens AG | Risk: 6

MAC-Adresse:	00:1B:1B:1E:50:25	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	3.2.15	**UDP-Ports:**	161,34964
TCP-Ports:	80,102	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-L2	**Ort (CMDB):**	Halle 3, Montagelinie 2
Meldung:	SSA-473245 (CVSS 7.5, Güte exakt) +10	**Meldungen:**	11
Kritische Ports:	**Port 80/TCP** – HTTP: Weboberfläche des Geräts **Port 161/UDP** – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.11 Z-Montage-Anlagennetz	102/6	S7	51	accept	53.756
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.11 Z-Montage-Anlagennetz	102/6	S7	53	accept	123
Firewall Outbound						
192.168.30.11 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.860

192.168.30.25 SPS/PLC (Siemens S7) | Siemens AG | Risk: 6

MAC-Adresse:	00:1B:1B:1E:B2:DB	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	Siemens SIMATIC HMI web	**UDP-Ports:**	–
TCP-Ports:	80,5900,102	**Lastboot:**	–
CMDB-Name:	H3-MO-HMI-01	**Ort (CMDB):**	Halle 3, Montagelinie 1, Bedienpult
Meldung:	SSA-941426 (CVSS 9.8, Güte modell) +9	**Meldungen:**	10
Kritische Ports:	**Port 80/TCP** – HTTP: Weboberfläche des Geräts **Port 5900/TCP** – VNC: Bildschirm-Fernsteuerung		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.25 Z-Montage-Anlagennetz	102/6	S7	51	accept	105.986
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.25 Z-Montage-Anlagennetz	102/6	S7	53	accept	100
Geblockt (eingehend) – alle 1 Verbindungen, 12 Versuche						
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.25 Z-Montage-Anlagennetz	5900/6	VNC	0	deny	12
Firewall Outbound						
192.168.30.25 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.031

192.168.30.30 Unbekanntes Gerät | Moxa Technologies | Risk: 6

MAC-Adresse:	00:90:E8:1E:D5:1C	**Gerätetyp:**	Unbekanntes Gerät
Hersteller:	Moxa Technologies	**OS-Erkennung:**	–
Firmware:	3.9	**UDP-Ports:**	161
TCP-Ports:	23,80	**Lastboot:**	–
CMDB-Name:	H3-MO-GW-01	**Ort (CMDB):**	Halle 3, Montagelinie 2, Etikettendrucker seriell
Kritische Ports:	**Port 23/TCP** – Telnet: Fernzugang auf die Kommandozeile **Port 80/TCP** – HTTP: Weboberfläche des Geräts **Port 161/UDP** – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.30 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	963

192.168.30.31 Unbekanntes Gerät | Moxa Technologies | Risk: 6

MAC-Adresse:	00:90:E8:1E:DC:29	**Gerätetyp:**	Unbekanntes Gerät
Hersteller:	Moxa Technologies	**OS-Erkennung:**	–
Firmware:	3.9	**UDP-Ports:**	161
TCP-Ports:	23,80	**Lastboot:**	–
CMDB-Name:	H3-MO-GW-02	**Ort (CMDB):**	Halle 3, Montagelinie 3, Waage seriell
Kritische Ports:	**Port 23/TCP** – Telnet: Fernzugang auf die Kommandozeile **Port 80/TCP** – HTTP: Weboberfläche des Geräts **Port 161/UDP** – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.31 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.451

192.168.30.102 Netzwerk (Firewall/Switch) | Hirschmann Automation and Cont | Risk: 6

MAC-Adresse:	64:60:38:1E:CD:C4	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Hirschmann Automation and Control GmbH	**OS-Erkennung:**	–
Firmware:	–	**UDP-Ports:**	161
TCP-Ports:	23,80	**Lastboot:**	–
CMDB-Name:	H3-MO-GER-52	**Ort (CMDB):**	Halle 3, Montagelinie 3
Kritische Ports:	**Port 23/TCP** – Telnet: Fernzugang auf die Kommandozeile **Port 80/TCP** – HTTP: Weboberfläche des Geräts **Port 161/UDP** – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.102 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.099

192.168.30.2 Netzwerk (Siemens SCALANCE) | Siemens AG | Risk: 4

MAC-Adresse:	00:0E:8C:1E:11:B0	**Gerätetyp:**	Netzwerk (Siemens SCALANCE)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	V4.3	**UDP-Ports:**	161
TCP-Ports:	22,443	**Lastboot:**	–
CMDB-Name:	H3-MO-SW-01	**Ort (CMDB):**	Halle 3, Montagelinie 1, Schaltschrank +A1
Meldung:	SSA-699386 (CVSS 9.1, Güte exakt) +6	**Meldungen:**	7
Kritische Ports:	**Port 161/UDP** – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.2 Z-Montage-Anlagennetz	10.20.10.40 Z-Infrastruktur SYSLOG-01 · Zeitdienst und Protokollierung	514/17	SYSLOG	14	accept	2.827
192.168.30.2 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.387

192.168.30.15 SPS/PLC (Siemens S7) | Siemens AG | Risk: 4

MAC-Adresse:	00:1B:1B:1E:6C:59	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	4.2.3	**UDP-Ports:**	–
TCP-Ports:	102,80,443	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-ST01	**Ort (CMDB):**	Halle 3, Schraubstation
Meldung:	SSA-712929 (CVSS 7.5, Güte exakt) +8	**Meldungen:**	9
Kritische Ports:	**Port 80/TCP** – HTTP: Weboberfläche des Geräts		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.15 Z-Montage-Anlagennetz	102/6	S7	51	accept	77.672
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.15 Z-Montage-Anlagennetz	102/6	S7	53	accept	176
Firewall Outbound						
192.168.30.15 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.863

192.168.30.16 SPS/PLC (Siemens S7) | Siemens AG | Risk: 4

MAC-Adresse:	00:1B:1B:1E:73:66	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	4.5.2	**UDP-Ports:**	–
TCP-Ports:	102,80,443	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-ST02	**Ort (CMDB):**	Halle 3, Klebestation
Meldung:	SSA-712929 (CVSS 7.5, Güte exakt) +4	**Meldungen:**	5
Kritische Ports:	**Port 80/TCP** – HTTP: Weboberfläche des Geräts		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.16 Z-Montage-Anlagennetz	102/6	S7	51	accept	58.317
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.16 Z-Montage-Anlagennetz	102/6	S7	53	accept	287
Firewall Outbound						
192.168.30.16 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	2.025

192.168.30.21 SPS/PLC (Rockwell/Allen-Bradley) | OMRON Corporation | Risk: 4

MAC-Adresse:	00:00:0A:1E:96:A7	**Gerätetyp:**	SPS/PLC (Rockwell/Allen-Bradley)
Hersteller:	OMRON Corporation	**OS-Erkennung:**	–
Firmware:	OMRON NX1P2 web	**UDP-Ports:**	9600
TCP-Ports:	80,9600,44818	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-ZU	**Ort (CMDB):**	Halle 3, Zuführung Kleinteile
Meldung:	ICSA-19-346-02 (CVSS 8.6, Güte modell)	**Meldungen:**	1
Kritische Ports:	**Port 80/TCP** – HTTP: Weboberfläche des Geräts		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	192.168.30.21 Z-Montage-Anlagennetz	9600/17	OMRON-FINS	35	accept	21.379
Firewall Outbound						
192.168.30.21 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.971

192.168.30.22 SPS/PLC (Phoenix/WAGO) | Wago Kontakttechnik GmbH | Risk: 4

MAC-Adresse:	00:30:DE:1E:9D:B4	**Gerätetyp:**	SPS/PLC (Phoenix/WAGO)
Hersteller:	Wago Kontakttechnik GmbH	**OS-Erkennung:**	Linux 4.x
Firmware:	vsftpd 3.0.5	**UDP-Ports:**	–
TCP-Ports:	21,22,80,443,502,2455	**Lastboot:**	–
CMDB-Name:	H3-MO-AS-01	**Ort (CMDB):**	Halle 3, Montagelinie 1, Hilfsantriebe
Kritische Ports:	**Port 21/TCP** – FTP: Dateiübertragung **Port 80/TCP** – HTTP: Weboberfläche des Geräts		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	192.168.30.22 Z-Montage-Anlagennetz	502/6	MODBUS	31	accept	40.473
Geblockt (eingehend) – alle 1 Verbindungen, 6 Versuche						
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.22 Z-Montage-Anlagennetz	21/6	FTP	0	deny	6
Firewall Outbound						
192.168.30.22 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	931

192.168.30.26 SPS/PLC (Siemens S7) | Siemens AG | Risk: 4

MAC-Adresse:	00:1B:1B:1E:B9:E8	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	Siemens SIMATIC HMI web	**UDP-Ports:**	–
TCP-Ports:	80,5900,102	**Lastboot:**	–
CMDB-Name:	– nicht in der CMDB –	**Ort (CMDB):**	–
Kritische Ports:	**Port 80/TCP** – HTTP: Weboberfläche des Geräts **Port 5900/TCP** – VNC: Bildschirm-Fernsteuerung		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.26 Z-Montage-Anlagennetz	102/6	S7	51	accept	55.890
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.26 Z-Montage-Anlagennetz	102/6	S7	53	accept	209
Firewall Outbound						
192.168.30.26 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	987

192.168.30.60 Windows-PC / Workstation | Fujitsu Technology Solutions G | Risk: 4

MAC-Adresse:	00:19:99:1E:A7:A2	**Gerätetyp:**	Windows-PC / Workstation
Hersteller:	Fujitsu Technology Solutions GmbH	**OS-Erkennung:**	Microsoft Windows 10
Firmware:	Microsoft Windows RPC	**UDP-Ports:**	–
TCP-Ports:	135,445,3389	**Lastboot:**	–
CMDB-Name:	H3-MO-ENG-01	**Ort (CMDB):**	Halle 3, Meisterbüro Montage
Kritische Ports:	**Port 135/TCP** – RPC: Windows-Fernsteuerdienst **Port 445/TCP** – SMB: Windows-Dateifreigabe		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.70.8 Z-DMZ FERNWARTUNG-01 · Fernwartung	192.168.30.60 Z-Montage-Anlagennetz	3389/6	RDP	71	accept	61
Firewall Outbound						
192.168.30.60 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.693
192.168.30.60 Z-Montage-Anlagennetz	10.20.50.5 Z-Infrastruktur WSUS-01 · Zeitdienst und Protokollierung	443/6	HTTPS	16	accept	1.262

192.168.30.61 Windows-PC / Workstation | Fujitsu Technology Solutions G | Risk: 4

MAC-Adresse:	00:19:99:1E:AE:AF	**Gerätetyp:**	Windows-PC / Workstation
Hersteller:	Fujitsu Technology Solutions GmbH	**OS-Erkennung:**	Microsoft Windows 10
Firmware:	Microsoft Windows RPC	**UDP-Ports:**	–
TCP-Ports:	135,445	**Lastboot:**	–
CMDB-Name:	H3-MO-BED-01	**Ort (CMDB):**	Halle 3, Linienleitstand Montage
Kritische Ports:	**Port 135/TCP** – RPC: Windows-Fernsteuerdienst **Port 445/TCP** – SMB: Windows-Dateifreigabe		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.61 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.774
192.168.30.61 Z-Montage-Anlagennetz	10.20.50.5 Z-Infrastruktur WSUS-01 · Zeitdienst und Protokollierung	443/6	HTTPS	16	accept	1.190

192.168.30.101 SPS/PLC (Siemens S7) | Siemens AG, Automations & Driv | Risk: 4

MAC-Adresse:	30:13:89:1E:C6:B7	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG, Automations & Drives,	**OS-Erkennung:**	–
Firmware:	–	**UDP-Ports:**	–
TCP-Ports:	80,102,443	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-51	**Ort (CMDB):**	Halle 3, Montagelinie 2
Meldung:	SSA-001536 (CVSS 10.0, Güte hersteller) +26	**Meldungen:**	27
Kritische Ports:	**Port 80/TCP** – HTTP: Weboberfläche des Geräts		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.101 Z-Montage-Anlagennetz	102/6	S7	51	accept	60.088
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.101 Z-Montage-Anlagennetz	102/6	S7	53	accept	56
Firewall Outbound						
192.168.30.101 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.174

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

MAC-Adresse:	00:09:0F:1E:0A:A3	**Gerätetyp:**	Netzwerk (Firewall/Switch)
Hersteller:	Fortinet	**OS-Erkennung:**	FortiOS 7.2
Firmware:	Fortinet FortiGate httpd	**UDP-Ports:**	161
TCP-Ports:	443	**Lastboot:**	–
CMDB-Name:	– nicht in der CMDB –	**Ort (CMDB):**	–
Kritische Ports:	**Port 161/UDP** – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Kein Verkehr über die Firewall im Splunk-Zeitraum.

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

MAC-Adresse:	00:1B:1B:1E:57:32	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	2.9.4	**UDP-Ports:**	–
TCP-Ports:	102,443,4840	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-L3	**Ort (CMDB):**	Halle 3, Montagelinie 3
Meldung:	SSA-452276 (CVSS 9.6, Güte exakt) +15	**Meldungen:**	16

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.12 Z-Montage-Anlagennetz	102/6	S7	51	accept	92.780
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.12 Z-Montage-Anlagennetz	4840/6	OPC-UA	52	accept	82.270
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.12 Z-Montage-Anlagennetz	102/6	S7	53	accept	93
Firewall Outbound						
192.168.30.12 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.379

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

MAC-Adresse:	00:1B:1B:1E:7A:73	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	4.4.1	**UDP-Ports:**	–
TCP-Ports:	102	**Lastboot:**	–
CMDB-Name:	– nicht in der CMDB –	**Ort (CMDB):**	–
Meldung:	SSA-712929 (CVSS 7.5, Güte exakt) +6	**Meldungen:**	7

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.17 Z-Montage-Anlagennetz	102/6	S7	51	accept	58.730
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.17 Z-Montage-Anlagennetz	102/6	S7	51	ip-conn	312
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.17 Z-Montage-Anlagennetz	102/6	S7	53	accept	117
Firewall Outbound						
192.168.30.17 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.208

192.168.30.100 SPS/PLC (Siemens S7) | Siemens AG | Risk: 0

MAC-Adresse:	30:B8:51:1E:BF:AA	**Gerätetyp:**	SPS/PLC (Siemens S7)
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	–	**UDP-Ports:**	–
TCP-Ports:	102,4840	**Lastboot:**	–
CMDB-Name:	H3-MO-SPS-50	**Ort (CMDB):**	Halle 3, Montagelinie 1

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.100 Z-Montage-Anlagennetz	102/6	S7	51	accept	86.578
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.100 Z-Montage-Anlagennetz	4840/6	OPC-UA	52	accept	69.065
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.100 Z-Montage-Anlagennetz	102/6	S7	53	accept	58
Firewall Outbound						
192.168.30.100 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	2.081

192.168.30.90 unbekannt | Siemens AG | nur Firewall-Verkehr

MAC-Adresse:	00:1B:1B:5A:0E:DE	**Gerätetyp:**	unbekannt
Hersteller:	Siemens AG	**OS-Erkennung:**	–
Firmware:	–	**UDP-Ports:**	–
TCP-Ports:	–	**Lastboot:**	–
CMDB-Name:	– nicht in der CMDB –	**Ort (CMDB):**	–

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.90 Z-Montage-Anlagennetz	10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	102/6	S7	51	accept	22.140

192.168.30.91 unbekannt | Wago Kontakttechnik GmbH | nur Firewall-Verkehr

MAC-Adresse:	00:30:DE:5A:11:E9	**Gerätetyp:**	unbekannt
Hersteller:	Wago Kontakttechnik GmbH	**OS-Erkennung:**	–
Firmware:	–	**UDP-Ports:**	–
TCP-Ports:	–	**Lastboot:**	–
CMDB-Name:	– nicht in der CMDB –	**Ort (CMDB):**	–

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.91 Z-Montage-Anlagennetz	10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	502/6	MODBUS	31	accept	15.880