PRAXIS-HILFE

Schritt 2: Netz in Zonen trennen

In fünf Schritten zur sicheren Anlage · nach SANS CC2

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Grundlage	SANS Five ICS Cybersecurity Critical Controls (CC2), BSI, CISA
Stand	11/2026
Notfall 24/7	+49 8031 8603164

Kostenfrei zum Ausdrucken, Ausfüllen und Weitergeben im eigenen Betrieb. Keine Rechtsberatung. Animation, Selbstcheck und Übung: ot-cyber.de/schritte/

1 Schritt 2: Netz in Zonen trennen

In vielen Anlagen hängen Büro, Leitstand und Steuerungen im selben Netz. Dann reicht ein einziger infizierter Rechner. Zonen mit kontrollierten Übergängen halten einen Angreifer dort, wo er hereingekommen ist. Dazu gehört auch: wissen, welche Geräte es gibt, und Stellen schaffen, an denen man den Verkehr mitlesen kann.

IHR ERSTER SCHRITT DIESE WOCHE

Zeichnen Sie Ihr Netz auf ein Blatt: Büro, Technik, Steuerungen, Fernzugänge. Die Vorlage finden Sie unten.

1.1 Checkliste

	Punkt	Wer / bis wann
☐	Es gibt einen aktuellen Netzplan, auf dem Büro und Anlage getrennt zu sehen sind.	
☐	Büro-Rechner können Steuerungen nicht direkt erreichen.	
☐	Zwischen Büro und Anlage gibt es eine Firewall, nicht nur einen Router.	
☐	Es ist bekannt, welche Verbindungen zwischen Büro und Anlage nötig sind, und nur diese sind erlaubt.	
☐	Daten aus der Anlage (zum Beispiel Zählerstände) gehen über einen Zwischenrechner, nicht direkt.	
☐	Kein Gerät der Anlage hat einen direkten Zugang zum Internet.	
☐	WLAN für Gäste oder Mitarbeitende ist von der Anlage getrennt.	
☐	Die Firewall-Regeln werden mindestens einmal im Jahr durchgesehen.	

IEC 62443-3-2 beschreibt Risikobewertung und Einteilung in Zonen und Übergänge (Conduits), IEC 62443-3-3 den Schutz der Zonengrenzen (Grundanforderung 5, eingeschränkter Datenfluss). NIS2 verlangt Sicherheit von Netz- und Informationssystemen nach dem Stand der Technik. Das BSI rät, Steuerungen nie direkt aus dem Internet erreichbar zu machen (BSI-CS 154).

2 Hands-on: Netzskizze in 60 Minuten

1. Vorlage ausdrucken. Vier Kästen: Büro, DMZ, Leitstand oder Technik, Steuerungen und Maschinen.

2. Jedes Gerät, das Ihnen einfällt, in einen Kasten schreiben. Auch Router, WLAN und Fernwartungszugänge.

3. Linien ziehen: Wer spricht mit wem? Fragen Sie die Technik oder den Dienstleister, wenn Sie es nicht wissen.

4. Jede Linie, die direkt vom Büro oder Internet in die Steuerungen geht, rot markieren.

5. Für jede rote Linie klären: Wird sie gebraucht? Wenn ja, über welchen Zwischenrechner? Wenn nein, abschalten lassen.

3 Was Sie tun können, je nach Betrieb

3.1 Kleinstbetrieb (Supermarkt-Filiale, Metzgerei, Bäckerei, Heizungsbauer, Gastronomie)

☐ Kühlung oder Heizung vom Kassen- und Büronetz trennen, bei der Fritzbox zum Beispiel über den Gastzugang am LAN-Anschluss 4. Achtung: Gast-WLAN und LAN-Gastzugang bilden dort ein gemeinsames Gastnetz. Nutzen Kunden das Gast-WLAN, für die Technik lieber einen eigenen kleinen Router vom Techniker einrichten lassen.

☐ Kassen-PC und Technik nicht im selben WLAN wie Gäste oder private Handys.

☐ Im Router alle Portfreigaben ansehen und unbekannte löschen.

3.2 Kleiner Betrieb mit Technik (Handel mit Filialen, Handwerksbetrieb mit Maschinen, kleine Brauerei oder Käserei, Hotel)

☐ Eine kleine Firewall zwischen Büro und Maschinen setzen, auch günstige Geräte können das.

☐ Maschinen in ein eigenes Netz (VLAN), Büro-PCs dürfen nicht hinein.

☐ Liste der nötigen Verbindungen mit dem IT-Dienstleister durchgehen.

3.3 Mittelständische Produktion (Maschinenbau, Lebensmittelhersteller, Brauereigruppe, Kunststoffverarbeitung)

☐ Zonen je Linie oder Halle, Übergänge nur über die DMZ.

☐ Kommunikationsmatrix: welche Verbindung, welches Protokoll, wofür.

☐ Firewall-Regeln jährlich mit Instandhaltung und IT prüfen.

3.4 Kleiner Versorger oder Kommune (Kleine Stadtwerke, Wasser- und Abwasserverband, Fernwärme, Bauhof mit Pumpwerken)

☐ Leitsystem, Außenstationen und Büro in getrennte Zonen, Fernwirkverbindungen nur zur Leitstelle.

☐ Zonen und Übergänge nach IEC 62443-3-2 bewerten.

☐ Mobilfunkrouter der Außenstationen ohne offene Dienste ins Internet.

3.5 Großer Versorger oder Netzbetreiber (Netzbetreiber, große Stadtwerke, Trinkwasserversorger, Kraftwerk)

☐ Zonenmodell nach IEC 62443 für Leitstelle, Stationen und Unternehmens-IT.

☐ Übergänge mit Protokollprüfung, Fernwirkverbindungen verschlüsselt.

☐ Segmentierung regelmäßig mit Angriffstests prüfen lassen.

3.6 Großindustrie und Prozessindustrie (Raffinerie, Chemie, Pharma, Konzern mit vielen Werken)

☐ Konzernweites Zonenmodell mit Standards je Werk, Sicherheitssysteme (SIS) in eigener Zone.

☐ Zentrale Verwaltung der Firewall-Regeln mit Freigabeprozess.

☐ Prüfung der Segmentierung bei jeder größeren Änderung an der Anlage.

4 Vorlage: Netzskizze mit Zonen

Büro-IT	DMZ	Leitstand / Technik	Steuerungen / Maschinen

4.1 Liste der nötigen Verbindungen

Von	Nach	Protokoll / Port	Wofür	Nötig?

5 Muster-Zonenplan und Verbindungsliste: Stadtwerke Musterstadt (fiktiv), Wasser, 12 Beschäftigte

Beispiel, ausgefüllt für einen erfundenen Betrieb. Namen, Nummern und Geräte sind fiktiv.

5.1 Zonen

✓ Z1 Büro-IT: Abrechnung, E-Mail

✓ Z2 DMZ: Historian, Update-Server

✓ Z3 Leitwarte: Leitsystem, Bedienplätze, Engineering-Rechner

✓ Z4 Außenstationen: Brunnen 1 und 2, Hochbehälter, Pumpwerk

✓ Z5 Fernwartung: Sprungserver

5.2 Grundregel

✓ Alles, was nicht in der Liste steht, ist verboten.

✓ Regeln einmal im Jahr mit Wassermeister und IT prüfen.

Von	Nach	Protokoll, Port	Zweck	Regel
Leitsystem (Z3)	Historian (Z2)	OPC UA 4840	Messwerte	FW-12
Büro (Z1)	Historian (Z2)	HTTPS 443, lesen	Zählerstände	FW-07
Leitsystem (Z3)	Stationen (Z4)	IEC 104, VPN	Fernwirken	FW-21
Update-Server (Z2)	Leitsystem (Z3)	HTTPS 443	Updates nach Freigabe	FW-15
Sprungserver (Z5)	Leitsystem (Z3)	RDP 3389	Wartung nach Freigabe	FW-30
alles andere	alles andere	-	verboten	Standard

Geprüft am 20.10.2026 von Wassermeister und IT-Dienstleister. Gefunden: Büro-PC mit direktem Weg zur SPS Brunnen 2, gesperrt.

6 Quellen

SANS Institute: The Five ICS Cybersecurity Critical Controls (Lee, Conway, Oktober 2022): https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

ISA/IEC 62443: Überblick über die Normenreihe: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

BSI-CS 154: Gefährdung durch internet-verbundene OT-Systeme (Oktober 2026): https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_154.pdf?__blob=publicationFile&v=4

BSI-CS 005: ICS-Security, Top 10 Bedrohungen und Gegenmaßnahmen 2022: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=6