PRAXIS-HILFE

Schritt 3: Sehen, was im Netz passiert

In fünf Schritten zur sicheren Anlage · nach SANS CC3

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Grundlage	SANS Five ICS Cybersecurity Critical Controls (CC3), 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 3: Sehen, was im Netz passiert

Viele Angriffe auf Anlagen laufen wochenlang unbemerkt. Wer weiß, was im eigenen Netz normal ist, erkennt das Ungewöhnliche. Dafür reicht am Anfang ein Mitschnitt und ein geübter Blick.

IHR ERSTER SCHRITT DIESE WOCHE

Schreiben Sie auf, welche Geräte in Ihrer Anlage miteinander sprechen sollten. Alles andere ist verdächtig.

1.1 Checkliste

	Punkt	Wer / bis wann
☐	Es ist bekannt, welche Geräte in der Anlage miteinander sprechen sollten.	
☐	Es gibt eine Liste aller Geräte im Anlagennetz.	
☐	Der Netzverkehr der Anlage wurde schon einmal mitgeschnitten und angesehen.	
☐	Ein neues Gerät im Anlagennetz würde auffallen.	
☐	Anmeldungen an Bedienrechnern und Fernzugängen werden protokolliert.	
☐	Jemand schaut sich die Protokolle regelmäßig an.	
☐	Es gibt einen Alarm, wenn Steuerungen ungewöhnlich beschrieben werden.	
☐	Bei einem Alarm ist klar, wer ihn bekommt und was dann passiert.	

In Deutschland müssen Betreiber kritischer Anlagen Systeme zur Angriffserkennung einsetzen (§ 31 Abs. 2 BSIG). Für alle anderen ist das freiwillig und trotzdem sinnvoll. IEC 62443-3-3 fordert die Überwachung von Sicherheitsereignissen (Grundanforderung 6, rechtzeitige Reaktion).

2 Hands-on: Eine Stunde mitschneiden

1. Mit dem IT-Dienstleister einen Spiegelport an einem Switch der Anlage einrichten, oder in der Simulation starten.

2. Eine Stunde Netzverkehr mit Wireshark (kostenlos) mitschneiden.

3. Unter „Statistiken, Konversationen“ ansehen: Welche Geräte sprechen miteinander?

4. Jede Verbindung mit der Liste „Was ist bei uns normal?“ vergleichen.

5. Alles Unbekannte klären. Oft ist es eine vergessene Fernwartung oder ein Gerät, das niemand mehr kennt.

3 Was Sie tun können, je nach Betrieb

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

☐ Im Router die Liste der verbundenen Geräte ansehen: Kennen Sie jedes Gerät?

☐ Temperaturalarm aufs Handy, am besten über einen eigenen Fühler, nicht nur über den Regler.

☐ Mitteilungen des Routers über neue Geräte und Anmeldungen einschalten.

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

☐ Einmal im Quartal die Geräteliste von Router und Firewall mit dem Dienstleister durchgehen.

☐ Protokolle der Fernzugänge aufbewahren und stichprobenartig ansehen.

☐ Einen Mitschnitt der Maschinen machen lassen und mit dem Hersteller besprechen.

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

☐ Spiegelport an den wichtigsten Switches einrichten.

☐ Passive Angriffserkennung für das Anlagennetz einführen, Alarme an eine feste Stelle.

☐ Ein Asset-Inventar aus dem mitgelesenen Verkehr aufbauen.

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

☐ Angriffserkennung für Leitsystem und Fernwirkverbindungen, in Deutschland für KRITIS-Betreiber vorgeschrieben.

☐ Alarme in den Bereitschaftsdienst einbinden.

☐ Monatlich Auffälligkeiten durchgehen, auch kleine.

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

☐ Systeme zur Angriffserkennung (SzA) mit Abdeckung aller Zonen.

☐ Auswertung rund um die Uhr, eigene Spezialisten oder Dienstleister mit OT-Erfahrung.

☐ Regelmäßige Bedrohungssuche (Threat Hunting) mit Szenarien aus der Lage.

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

☐ Monitoring in allen Werken mit zentraler Auswertung.

☐ Erkennungsregeln für die eigenen Prozesse, abgestimmt mit der Prozesstechnik.

☐ Kennzahlen: Zeit bis zur Erkennung, Zeit bis zur Reaktion.

4 Vorlage: Was ist bei uns normal?

Gerät A	Gerät B	Protokoll	Wie oft	Normal?

5 Muster-Blatt „Was ist bei uns normal?“: Stadtwerke Musterstadt (fiktiv)

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

5.1 Messpunkt

✓ TAP am Switch der Leitwarte, Mitschnitt eine Stunde im Normalbetrieb am 22.10.2026

5.2 Alarm schlagen bei

✓ Neues Gerät im Netz der Leitwarte

✓ Verbindung aus der Leitwarte ins Internet

✓ Schreiben auf eine Steuerung außerhalb des Wartungsfensters (Dienstag 8 bis 12 Uhr)

✓ Fernwartung, die nicht über den Sprungserver kommt

5.3 Zusätzlich

✓ Füllstand Hochbehälter mit eigenem Melder per SMS, unabhängig vom Leitsystem

Gerät A	Gerät B	Protokoll	Wie oft	Normal
Leitsystem	SPS Brunnen 1	Modbus/TCP 502	alle 2 s	ja
Leitsystem	Historian	OPC UA 4840	alle 10 s	ja
Engineering-PC	SPS Pumpwerk	Programmierung	Wartungsfenster	ja
Bedienplatz 2	Internet	DNS 53	mehrmals täglich	nein, prüfen

Befund: Bedienplatz 2 fragt Adressen im Internet an. Ursache: automatische Updates eingeschaltet. Abgestellt am 23.10.2026.

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

§ 31 BSIG (Systeme zur Angriffserkennung für Betreiber kritischer Anlagen): https://openlex.de/bsig/31

Wireshark: Statistiken, Konversationen: https://www.wireshark.org/docs/wsug_html_chunked/ChStatConversations.html

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