PRAXIS-HILFE

Schritt 5: Schwachstellen im Griff

In fünf Schritten zur sicheren Anlage · nach SANS CC5

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Grundlage	SANS Five ICS Cybersecurity Critical Controls (CC5), 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 5: Schwachstellen im Griff

Jede Woche werden neue Lücken in Steuerungen und Software bekannt. Nicht jede betrifft Sie, und nicht jede muss sofort gepatcht werden. Wer seine Geräte kennt, kann in Minuten entscheiden: patchen, abschirmen oder beobachten.

IHR ERSTER SCHRITT DIESE WOCHE

Erfassen Sie die zehn wichtigsten Geräte Ihrer Anlage mit Hersteller, Typ und Firmware-Stand.

1.1 Checkliste

	Punkt	Wer / bis wann
☐	Es gibt eine Liste aller wichtigen Geräte mit Hersteller, Typ und Firmware-Stand.	
☐	Jemand verfolgt regelmäßig neue Sicherheitsmeldungen zu diesen Geräten.	
☐	Es ist bekannt, welche Geräte aus dem Internet oder dem Büro erreichbar sind.	
☐	Für jede Meldung wird entschieden: patchen, abschirmen oder beobachten.	
☐	Updates werden für geplante Stillstände eingeplant.	
☐	Router, Firewalls und VPN-Geräte werden zeitnah aktualisiert.	
☐	Entscheidungen zu Lücken werden kurz dokumentiert.	
☐	Hersteller und Dienstleister informieren Sie über Lücken in gelieferter Technik.	

In Deutschland gehört der Umgang mit Schwachstellen zu den Mindestmaßnahmen (§ 30 Abs. 2 Nr. 5 BSIG). Hersteller müssen nach dem Cyber Resilience Act seit 11. September 2026 aktiv ausgenutzte Schwachstellen melden, ab 11. Dezember 2027 gilt die Verordnung vollständig. Die Pflichten treffen Hersteller, nicht Betreiber. Fragen Sie Ihre Hersteller, wie Sie deren Sicherheitsmeldungen bekommen.

2 Hands-on: Das Inventar der zehn wichtigsten Geräte in 60 Minuten

1. Vorlage ausdrucken. Mit der Technik an die Schaltschränke gehen.

2. Die zehn wichtigsten Geräte erfassen: Steuerungen, Bedienrechner, Router, Fernwartungsboxen.

3. Bei jedem Gerät Hersteller, Typ und Firmware-Stand notieren (steht oft auf dem Display oder im Menü).

4. Für jedes Gerät eintragen, von wo es erreichbar ist: nur vor Ort, aus dem Büro, aus dem Internet.

5. Die aktuelle OT-Lage durchgehen: Ist eines Ihrer Geräte dabei? Dann mit dem Entscheidungsbaum weitermachen.

3 Was Sie tun können, je nach Betrieb

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

☐ Automatische Updates im Router einschalten.

☐ Den Kälte- oder Heizungstechniker fragen, ob es für den Regler Updates gibt.

☐ Prüfen lassen, ob Ihre Anlage aus dem Internet erreichbar ist (wir sagen es Ihnen kostenfrei).

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

☐ Geräteliste mit Firmware-Stand anlegen, auch für Router und Fernwartungsboxen.

☐ Sicherheitsmeldungen der eigenen Hersteller abonnieren oder die OT-Lage lesen.

☐ Updates mit dem Dienstleister für ruhige Zeiten einplanen.

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

☐ Asset-Inventar für alle Linien, automatisch abgeglichen mit Sicherheitsmeldungen.

☐ Entscheidungsregeln: was sofort, was beim nächsten Stillstand, was nur mit Absicherung.

☐ Updates gemeinsam mit den Maschinenherstellern testen.

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

☐ Inventar für Leitsystem, Außenstationen und Fernwirktechnik.

☐ Meldungen von CERT@VDE, BSI und Herstellern regelmäßig auswerten.

☐ Erreichbarkeit aus dem Internet regelmäßig prüfen lassen.

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

☐ Schwachstellenmanagement mit Risikobewertung je Zone.

☐ Feste Fristen je Schwere, Ausnahmen dokumentiert und befristet.

☐ Tägliche Auswertung der Lage, Abgleich mit dem Inventar.

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

☐ Konzernweites Inventar und Schwachstellenmanagement, Werke mit lokalen Verantwortlichen.

☐ Absprachen mit Lieferanten zu Updates, Meldepflichten und Lebensdauer.

☐ Kennzahlen: offene Lücken je Kritikalität und Alter.

4 Vorlage: Inventar der wichtigsten Geräte

Gerät	Hersteller / Typ	Firmware	Erreichbar von	Verantwortlich

4.1 Entscheidungsweg bei einer neuen Lücke

1. Ist das Gerät bei uns verbaut, mit betroffener Firmware? Nein: erledigt, kurz notieren.

2. Ist es aus dem Internet oder dem Büro erreichbar? Ja: sofort absichern (Freigabe schließen, Firewall-Regel).

3. Gibt es ein Update? Ja: beim nächsten geplanten Stillstand einspielen, vorher testen.

4. Kein Update? Abschirmen und überwachen, Entscheidung mit Datum notieren.

5 Muster-Inventar und Entscheidung: Stadtwerke Musterstadt (fiktiv)

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

5.1 Neue Meldung, durchgespielt

✓ Meldung: Lücke in Fernwirk-Steuerung „Typ X“ (fiktiv), Firmware vor 3.2

✓ Bei uns verbaut? Ja, Brunnen 1 und 2, Firmware 3.0

✓ Aus dem Internet oder dem Büro erreichbar? Nein, nur aus der Leitwarte über VPN

✓ Aktiv ausgenutzt (KEV-Katalog)? Nein

✓ Entscheidung: abschirmen (Regel FW-21 nur für das Leitsystem), patchen im Wartungsfenster am 3.12.2026

✓ Verantwortlich: Wassermeister. Restrisiko bis dahin akzeptiert von der Werkleitung.

Gerät	Typ (fiktiv)	Firmware	Ort	Erreichbar von
SPS Brunnen 1	Typ X	3.0	Brunnen 1	Leitwarte (VPN)
SPS Brunnen 2	Typ X	3.0	Brunnen 2	Leitwarte (VPN)
SPS Pumpwerk	Typ Y	5.4	Pumpwerk	Leitwarte
Leitsystem	Server	aktuell	Leitwarte	Sprungserver
Firewall	Typ Z	7.2	Leitwarte	IT-Dienstleister

Felder nach der CISA Asset Inventory Guidance (2025), gekürzt. Vollständig wären unter anderem auch Hostname, Adresse, Dienste und Konten.

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

CISA: Known Exploited Vulnerabilities (aktiv ausgenutzte Lücken): https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CISA: Stakeholder-Specific Vulnerability Categorization (Entscheidungsbaum): https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc

CISA: Foundations for OT Cybersecurity, Asset Inventory Guidance (2025): https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators

CERT@VDE: Sicherheitsmeldungen von Automatisierungsherstellern: https://certvde.com/de/

Cyber Resilience Act, Verordnung (EU) 2024/2847: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

§ 30 BSIG (Mindestmaßnahmen, gültig seit 6.12.2025): https://openlex.de/bsig/30