PRAXIS-HILFE

Schritt 1: Für den Notfall vorbereitet

In fünf Schritten zur sicheren Anlage · nach SANS CC1

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Grundlage	SANS Five ICS Cybersecurity Critical Controls (CC1), 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 1: Für den Notfall vorbereitet

Ein Angriff kommt meist dann, wenn keiner damit rechnet: nachts, am Wochenende, im Urlaub. Wer vorher festlegt, wer entscheidet, wen man anruft und wie die Anlage sicher weiterläuft, verliert Stunden statt Wochen. Ein Plan auf einer Seite reicht für den Anfang.

IHR ERSTER SCHRITT DIESE WOCHE

Hängen Sie eine Notfallkarte in Leitwarte, Werkstatt oder Technikraum. Die Vorlage finden Sie unten zum Ausdrucken.

1.1 Checkliste

	Punkt	Wer / bis wann
☐	Es gibt eine Liste mit Telefonnummern für den Notfall (intern, Dienstleister, Hersteller, Behörde).	
☐	Es ist festgelegt, wer im Notfall entscheidet, auch nachts und am Wochenende.	
☐	Alle wissen: Anlage zuerst in einen sicheren Zustand bringen, nichts neu aufsetzen oder löschen.	
☐	Die Anlage lässt sich vor Ort von Hand weiter betreiben oder sicher abschalten.	
☐	Es gibt Sicherungen der Steuerungsprogramme und Konfigurationen, die nicht im Netz hängen.	
☐	Eine Wiederherstellung aus der Sicherung wurde schon einmal ausprobiert.	
☐	Das Team hat den Notfall in den letzten zwölf Monaten einmal durchgespielt.	
☐	Es ist bekannt, ob und wo ein Vorfall gemeldet werden muss.	

NIS2 verlangt die Bewältigung von Sicherheitsvorfällen, Backup, Wiederherstellung und Krisenmanagement (in Deutschland seit 6.12.2025 § 30 Abs. 2 Nr. 2 und 3 BSIG). Erhebliche Vorfälle sind nach § 32 BSIG zu melden: erste Meldung nach spätestens 24 Stunden, dann nach 72 Stunden, Abschluss nach einem Monat. IEC 62443-2-1 verlangt vom Betreiber ein Ereignis- und Vorfallmanagement.

2 Hands-on: Planspiel in 30 Minuten

1. Drei bis fünf Leute an einen Tisch holen: wer entscheidet, wer kennt die Technik, wer spricht mit Kunden.

2. Szenario vorlesen: „Montag, 6 Uhr, die Bildschirme im Leitstand zeigen eine Erpressernachricht."

3. Reihum fragen: Was tun Sie in den ersten 15 Minuten? Wen rufen Sie an? Wie läuft die Anlage weiter?

4. Jede Lücke auf die Notfallkarte schreiben, zum Beispiel eine fehlende Telefonnummer.

5. Notfallkarte fertig machen und aufhängen. Termin für das nächste Planspiel festlegen.

3 Was Sie tun können, je nach Betrieb

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

☐ Notfallnummer des Kälte- oder Heizungstechnikers groß an die Anlage kleben.

☐ Wissen, wie man die Anlage von Hand weiterbetreibt (Handbetrieb am Regler, Notkühlung, Ware umlagern).

☐ Fotos von allen Reglereinstellungen machen und offline aufbewahren.

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

☐ Notfallkarte mit drei Telefonnummern und einer Person, die entscheidet.

☐ Sicherung der Steuerungsprogramme vom Hersteller oder Dienstleister geben lassen und offline lagern.

☐ Einmal im Jahr 30 Minuten Planspiel mit Chef, IT-Dienstleister und Technik.

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

☐ Notfallplan für die Produktion getrennt vom IT-Notfallplan, mit Ansprechpartner je Linie.

☐ Sicherungen aller Steuerungen und Bedienrechner, Wiederherstellung einmal im Jahr testen.

☐ Vertrag mit einem Incident-Response-Dienstleister, der Anlagen kennt.

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

☐ Notfallplan für Leitsystem und Außenstationen, mit Handbetrieb je Anlage.

☐ Meldeweg nach NIS2 klären: wer meldet was bis wann an wen.

☐ Übung mit dem Bereitschaftsdienst, auch die Fahrt zu den Außenstationen planen.

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

☐ Notfall- und Krisenmanagement für Leitstelle und Netz, abgestimmt mit dem Krisenstab.

☐ Regelmäßige Übungen mit Szenarien aus der aktuellen Lage, auch mit Behörden und Nachbarnetzen.

☐ Wiederanlauf aus sauberen Sicherungen für Leitsystem und Schutztechnik planen und testen.

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

☐ Incident Response für jeden Standort, verzahnt mit Prozesssicherheit und Sicherheitssystemen (SIS).

☐ Playbooks für Ransomware, manipulierte Sollwerte und Ausfall der Leittechnik.

☐ Jährliche Übungen über Werke hinweg, mit Lieferanten und Behörden.

4 Notfallkarte: Aushang für Leitwarte, Werkstatt, Technikraum

1. Anlage in einen sicheren Zustand bringen, bei Bedarf von Hand vor Ort.
2. Nichts neu aufsetzen, nichts löschen, Spuren sichern.
3. Netztrennung nur abgestimmt.
4. Sofort anrufen:

Wer	Telefon	Erreichbar wann

Entscheidet im Notfall: _____ Vertretung: _____

OT-NOTFALL RUND UM DIE UHR

+49 8031 8603164

5 Muster-Notfallplan: Brauerei Inntaler (fiktiv), 40 Beschäftigte

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

5.1 Was wir schützen

✓ Sudhaus-Steuerung

✓ Kühlung Gärkeller und Lagerkeller

✓ Abfüllanlage mit Etikettierer

5.2 Szenarien, die wir üben

✓ Ransomware im Büronetz erreicht die Bedienrechner

✓ Solltemperatur im Gärkeller wird von außen verstellt

✓ Fernzugang des Anlagenbauers wird mit gestohlenem Passwort genutzt

5.3 Sicherer Zustand

✓ Sudhaus: laufenden Sud zu Ende fahren, keinen neuen beginnen

✓ Gärkeller: Regler auf Handbetrieb, Temperatur alle 2 Stunden ablesen und notieren

✓ Abfüllung: anhalten, Ware im Kühllager sichern

5.4 Nicht tun

✓ Rechner nicht neu aufsetzen, nichts löschen

✓ Netz nur nach Absprache mit Braumeister und IT trennen

5.5 Meldung

✓ NIS2: nicht meldepflichtig (unter 50 Beschäftigte, Umsatz unter 10 Mio. Euro)

✓ Anzeige bei der Polizei: Zentrale Ansprechstelle Cybercrime (ZAC) Bayern

✓ Versicherung und Kunden nach Rücksprache mit der Geschäftsführung informieren

5.6 Wiederanlauf in dieser Reihenfolge

✓ Kühlung prüfen

✓ Steuerungen aus der Offline-Sicherung prüfen

✓ Bedienrechner sauber aufsetzen

✓ Büro-IT zuletzt

Rolle	Name	Telefon	Entscheidet
Braumeister	A. Beispiel	+49 8031 000 101	Handbetrieb, Anlage stoppen

Rolle	Name	Telefon	Entscheidet
Geschäftsführung	B. Beispiel	+49 8031 000 102	Meldung, Anzeige, Kunden
IT-Dienstleister	Firma C	+49 8031 000 103	Netz trennen (abgestimmt)
Kältetechnik	Firma D	+49 8031 000 104	-
OT-Notfall	OT-Cyber	+49 8031 8603164	-

Planspiel am 14.10.2026: Die Nummer der Kältetechnik fehlte, ergänzt am 15.10.2026. Nächstes Planspiel: Oktober 2027.

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

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

§ 32 BSIG (Meldepflichten 24 Stunden, 72 Stunden, ein Monat): https://openlex.de/bsig/32

CISA Tabletop Exercise Packages (Planspiele, auch für Anlagen): https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

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