PRAXIS-HILFE

Schritt 4: Fernzugang absichern

In fünf Schritten zur sicheren Anlage · nach SANS CC4

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Grundlage	SANS Five ICS Cybersecurity Critical Controls (CC4), 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 4: Fernzugang absichern

Hersteller, Techniker und Dienstleister greifen oft aus der Ferne auf Anlagen zu. Jeder dieser Zugänge ist auch eine Tür für Angreifer. Sicher wird es mit drei Regeln: zweiter Faktor, Freigabe im Einzelfall, Protokoll.

IHR ERSTER SCHRITT DIESE WOCHE

Listen Sie alle Wege auf, über die jemand von außen auf Ihre Anlage kommt. Fragen Sie auch Ihre Techniker.

1.1 Checkliste

	Punkt	Wer / bis wann
☐	Es gibt eine vollständige Liste aller Fernzugänge, auch die der Hersteller.	
☐	Kein Fernzugang ist dauerhaft offen, er wird nur bei Bedarf freigeschaltet.	
☐	Jeder Fernzugang braucht einen zweiten Faktor, zum Beispiel einen Code auf dem Handy.	
☐	Jeder Techniker hat ein eigenes Konto, keine geteilten Passwörter.	
☐	Fernzugänge führen über einen Zwischenrechner, nicht direkt auf Steuerungen.	
☐	Jeder Zugriff wird protokolliert und die Protokolle werden aufbewahrt.	
☐	Konten ehemaliger Mitarbeitender und Dienstleister sind gelöscht.	
☐	Router und VPN-Geräte bekommen ihre Updates zeitnah.	

NIS2 nennt Zugriffskontrolle und Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung ausdrücklich (in Deutschland § 30 Abs. 2 Nr. 9 und 10 BSIG). IEC 62443-3-3 fordert Identifizierung und Anmeldung von Personen sowie den Schutz der Zonengrenzen (Grundanforderungen 1 und 5). Für Fernzugänge nennt das BSI VPN, möglichst mit zweitem Faktor, als Mindeststandard (BSI-CS 154).

2 Hands-on: Alle Türen finden in 45 Minuten

1. Im Router oder in der Firewall alle Portfreigaben und VPN-Konten auflisten.
2. Bei Technik, Herstellern und Dienstleistern nachfragen: Wie kommen Sie auf unsere Anlage?
3. Nach eigenen Boxen für Fernwartung und Mobilfunkroutern in Schaltschränken suchen.
4. Jeden Zugang in die Liste eintragen: wer, wie, mit zweitem Faktor, dauerhaft offen oder nur bei Bedarf.
5. Jeden Zugang ohne zweiten Faktor oder dauerhaft offen als Erstes ändern lassen.

3 Was Sie tun können, je nach Betrieb

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

☐ Im Router alle Portfreigaben für Kühlung oder Heizung löschen.

☐ Für den Techniker die VPN-Funktion des Routers nutzen (die Fritzbox kann das) und nur bei Bedarf einschalten.

☐ Standardpasswörter von Regler, Router und Fernwartung ändern, das Router-Passwort nicht weitergeben.

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

☐ Liste aller Fernwartungen mit Hersteller, Gerät und Ansprechpartner.

☐ Fernwartung nur auf Anruf freischalten, danach wieder aus.

☐ Zweiten Faktor für alle Zugänge einschalten, wo das Gerät es kann.

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

☐ Zentraler Fernzugang für alle Maschinenhersteller statt vieler eigener Boxen.

☐ Freigabe im Einzelfall durch die Instandhaltung, Sitzungen werden aufgezeichnet.

☐ Verträge mit Herstellern um Regeln für Fernwartung ergänzen.

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

☐ Fernzugänge für Bereitschaft und Dienstleister über einen gehärteten Zugang mit zweitem Faktor.

☐ Mobilfunkrouter der Außenstationen ohne Zugang aus dem Internet.

☐ Zugänge jährlich überprüfen und unnötige schließen.

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

☐ Privilegierter Zugang mit Aufzeichnung, Freigabe und zeitlicher Begrenzung.

☐ Getrennte Zugänge für Leitstelle, Stationen und Dienstleister.

☐ Angriffe auf VPN- und Edge-Geräte aus der Lage täglich verfolgen und schnell reagieren.

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

☐ Einheitliche Plattform für Fernzugriff in allen Werken, mit zentraler Steuerung.

☐ Kein direkter Zugriff von Lieferanten auf Sicherheitssysteme.

☐ Regelmäßige Prüfung durch Angriffstests von außen.

4 Vorlage: Liste aller Fernzugänge

Wer (Firma)	Wie	Auf welches Gerät	2. Faktor	Offen

4.1 Freigabe im Einzelfall

Datum	Wer	Grund	Von bis	Freigegeben von

5 Muster-Fernzugangsliste und Freigabe: Brauerei Inntaler (fiktiv)

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

5.1 Regeln

✓ Jeder Zugang hat einen Verantwortlichen und einen zweiten Faktor

✓ Hersteller und Dienstleister nur nach Freigabe im Einzelfall

✓ Jede Sitzung wird protokolliert

5.2 Freigabe im Einzelfall, Beispiel

✓ Datum: 12.11.2026, 9:00 bis 11:00 Uhr

✓ Wer: Hersteller der Abfüllanlage, Techniker E. Beispiel

✓ Grund: Fehleranalyse Etikettierer, Ziel: Steuerung Abfüllung

✓ Freigegeben von: Braumeister, eingeschaltet 9:02, ausgeschaltet 10:41

✓ Protokoll gespeichert, Nachkontrolle: in Ordnung

Wer	Wie	Auf welches Gerät	2. Faktor	Status
Kältetechnik	VPN der Firewall	Kühlregler Gärkeller	ja	bei Bedarf
Hersteller Abfüllung	Sprungserver	Steuerung Abfüllung	ja	Einzelfall
IT-Dienstleister	VPN	Büro-Server	ja	aktiv
Mobilfunk-Router	eigene SIM	Bedienpanel Abfüllung	nein	abgebaut 03.11.

Der Mobilfunk-Router hing seit der Inbetriebnahme 2019 im Schaltschrank der Abfüllung. Niemand wusste mehr davon.

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

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