



EMPFEHLUNG: OT-TECHNIK

Gefährdung durch internet-verbundene OT-Systeme

Einfache Maßnahmen zum Schutz vor Cyberangriffen

Zielgruppe

Diese Cybersicherheitsempfehlung richtet sich vor allem an Betreiber kleiner und kleinster industrieller Anlagen. Sie ist für alle Sektoren anwendbar, dazu gehören Anlagen der Energieerzeugung, z. B. Wasserkraftanlagen, Windenergieanlagen, Müllverbrennung, Solaranlagen beliebiger Größe sowie Kraft-Wärme-Kopplungsanlagen (KWK) und Biogasanlagen ebenso betroffen wie Anlagen der Trinkwasserversorgung, Abwasserbehandlung und -Entsorgung oder sonstigen kleinen und kleinsten Anlagen.

Das Dokument liefert Betreibern einen Leitfaden mit konkreten Maßnahmen, um Gefährdungen durch internet-verbundene OT-Systeme zu prüfen und ihnen entgegenzuwirken. Soweit identifizierte Probleme nicht eigenständig gelöst werden können, dient es als Grundlage, um gegenüber Systemintegratoren oder anderen Dienstleistern erforderliche Maßnahmen einzufordern.

Sachverhalt

Schnell an Informationen über den Zustand der Anlage zu kommen, ist im betrieblichen Alltag essentiell. Zu den Informationen zählen beispielsweise der Wasserstand im Hochbehälter, die Einspeisehistorie des heutigen Tages in das Stromnetz oder der Langtext einer Störung in einer Ereignisliste.

Die benötigten Informationen liegen meist in der Visualisierung (z. B. abgelegt im Supervisory Control and Data Acquisition (SCADA) oder auf einer Human Machine Interface (HMI)) oder direkt auf der Speicherprogrammierbaren Steuerung (SPS). Mit einer Portweiterleitung im Router

können beispielsweise sämtliche Informationen nur mit einem Webbrowser über ein Mobiltelefon abgerufen werden – jederzeit, von überall und schlimmstenfalls von jedem. Automatisierte Dienste und Systeme durchforsten das Internet permanent nach exponierten industriellen Steuerungssystemen. Angreifende nutzen die Ergebnisse immer schneller und bereits teilautomatisiert. Dabei setzen sie unter anderem von Künstlicher Intelligenz (KI) generierte Skripte ein, welche gezielt bekannte, nicht gepatchte Schwachstellen oder Fehlkonfigurationen ausnutzen [1,2].

Beispielhaft sind erfolgreiche Cyberangriffe im August 2026 über auf Wasserversorger in den USA [3,4]. Dabei wurde auf offen im Internet zugängliche SPSEN und SCADA-Systeme zugegriffen. Es wurden Prozesswerte manipuliert und der Zugriff auf die Geräte gesperrt, um eine Wiederherstellung des sicheren Regelbetriebs zu erschweren [5]. In diesem Fall waren mehr als 30 kommunale Betreiber betroffen.

Bereits im Dezember 2025 richteten sich koordinierte Angriffe in Polen [6] gegen zahlreiche Windparks, ein großes und ein kleineres KWK-Kraftwerk sowie ein Unternehmen aus dem produzierenden Gewerbe. In den Windenergieanlagen unterbrachen die Angriffe die Kommunikation zu den Netzbetreibern und störten bzw. blockierten Steuerungs- und Schutzgeräte. Beim kleineren KWK-Kraftwerk wurden Steuerungen gestört und Turbine sowie Wasseraufbereitung abgeschaltet, was dank des schnellen Eingreifens durch den Betreiber nur einen kurzen Ausfall ohne Versorgungsunterbrechung für Kunden zur Folge hatte. Eine Reihe trivialer Schwächen bildete die Basis der Angriffe: Einzelne Geräte waren mit Standard- oder werksseitigen Zugangsdaten ausgestattet, die nicht geändert worden waren. Über verschiedene Anlagen und nachgelagerte Geräte hinweg wurden identische Passwörter wiederverwendet. Dadurch eröffnete ein einzelner kompromittierter Zugang Zugriff auf mehrere, auch räumlich getrennte, Anlagen. Darüber hinaus erlaubte die mobilfunkbasierte Fernanbindung der Anlagen die Kommunikation zwischen beliebigen Geräten innerhalb eines als vertrauenswürdig geltenden privaten Datenübertragungsnetzes (Access Point Name, APN) [7]. Dessen vermeintliche Abschottung erwies sich damit als trügerisch und ermöglichte eine Querbewegung zwischen getrennten Netzbereichen.

Insgesamt handelte es sich um rein destruktive Sabotageakte, die in der Folge glücklicherweise nur begrenzte Auswirkungen auf die reale Versorgung hatten. Die Angriffe waren weder katastrophal noch unerwartet und im Ergebnis einfach vermeidbar – von der Ausnutzung trivialer Zugangsdaten bis hin zur möglichen Verwundbarkeit des zentralen Routers.

Bewertung

In der heutigen hochvolatilen geopolitischen Lage können Anlagen (auch in Deutschland) jederzeit verstärkt in den Fokus geraten. Einfache Ziele versprechen schnelle Erfolge auch in der hybriden Kriegsführung. Fehlender Basisschutz und die Möglichkeit, direkt OT-Geräte (Operational Technology, OT) anzugreifen, anstatt über maliziöse Spam- oder Phishing-E-mails über die IT des Unternehmens gehen zu müssen, senken den Aufwand für die Angreifenden erheblich. Zudem ist durch den Einsatz von KI weniger oder kein Expertenwissen mehr erforderlich. Dies erhöht den Kreis der potentiellen Angreifenden als auch die Skalierbarkeit durch Automation solcher Angriffe.

Jeder Betreiber, der OT-Systeme ohne ausreichende Schutzmaßnahmen offen aus dem Internet zugänglich macht, handelt grundsätzlich pflichtwidrig und nimmt die Gefahr eines unbefugten Zugriffs oder einer Störung zumindest billigend in Kauf. Kompromittierte OT-Systeme stellen außerdem eine ernste Gefahr für Andere dar, da sie als Proxies zur Verschleierung der Infrastruktur von Angreifenden missbraucht werden können und im schlimmsten Fall – durch die Nutzung von Skalierungseffekten – aktive Angriffe auf die Energieerzeugung und die Stabilität des Stromnetzes versucht werden könnten [8].

Allgemeine Maßnahmen

Die nachfolgenden Maßnahmen sollten nach folgender Priorisierung umgesetzt werden. Die Liste der Maßnahmen erhebt keinen Anspruch auf Vollständigkeit und soll erste Ansätze liefern:

1. Direkten Zugriff aus dem Internet unterbinden
2. Zugriffe absichern
3. Systeme aktuell halten
4. Maßnahmen zur Routine machen

Direkten Zugriff aus dem Internet unterbinden

Der wichtigste und zugleich einfachste Schutz ist es, die Anlagen vom Internet zu trennen. Betreiber sollten daher zunächst prüfen, ob ihre Anlagen im Internet exponiert, d. h. aus dem Internet erreichbar sind. Dies gilt unabhängig von Anlagengröße, Rechtsform oder Art der Anlage. Eine direkte Erreichbarkeit ist wirksam zu unterbinden. Dazu gehört es, sämtliche frei zugänglichen SPS- und SCADA-Geräte und Zugriffe auf HMI vom direkten Internetzugang zu trennen und Portweiterleitungen im Router auf Endgeräte zu deaktivieren. Auch OT-Protokolle der Anlagen (z. B. Modbus-TCP, S7Com, Profinet) dürfen keinesfalls über Portweiterleitungen im Internet exponiert werden. Ebenso dürfen keinesfalls Management-Interfaces von Routern und Firewalls aus dem Internet erreichbar sein. Die Verwaltung dieser Geräte darf ausschließlich aus dem lokalen Netz (Local Area Network, LAN) erfolgen.

Zugriffe absichern

Im zweiten Schritt geht es darum, notwendige Zugriffe entsprechend abzusichern und Fernzugriffe zu härten. Benötigte Fernzugriffe sind durch das Vorschalten und Aktivieren von VPN-Lösungen (Virtual Private Network) zu schützen, wobei viele handelsübliche Router diese Funktion bereits anbieten und mindestens ein VPN beim externen Zugriff Pflicht ist.

Betreiber sollten einen Passwort- und idealerweise einen Multifaktor-geschützten Zugriff auf SPS und Geräte etablieren, Default-Zugänge deaktivieren und sichere Passwörter setzen, um unbefugte Zugriffe zu erschweren. Dabei ist zu beachten, dass ein reiner Passwortschutz nicht ausreicht, da Schwachstellen unter Umständen auch ohne Authentifizierung ausgenutzt werden können. Deshalb sollten alle bereits in den Geräten vorhandenen Sicherheitsfunktionen wie Blocklisten und Protokollfilter ausgeschöpft werden. Mit Dienstleistern sollte besprochen werden, welche bereits vorhandenen Sicherheitsfunktionen aktiviert werden können, da oft schon einfache Maßnahmen die Sicherheit deutlich verbessern. Zudem sollte sich ein Betreiber nicht auf eine dynamische IP-Adresse als "Schutz" verlassen.

Bei Anlagen, die mit einer Hersteller-Cloud verbunden sind, sollte geprüft werden, ob diese Verbindung zum Betrieb dauerhaft notwendig ist. Idealerweise stellen Betreiber auf einen rein lokalen Betrieb um, um Risiken durch unzureichend abgesicherte oder nicht vertrauenswürdige Herstellerdienste zu vermeiden. Grundsätzlich sollten Produkte, die für ihre Funktion zwingend auf digitale Herstellerdienste angewiesen sind, nur mit Bedacht beschafft werden, da spätestens bei einer Geschäftsaufgabe oder dem Support-Ende des Herstellers ein Totalverlust drohen kann.

Systeme aktuell halten

Anschließend sollten die Systeme auf aktuellen Software- und Firmwarestand überprüft werden. Soft- und Firmware-Updates sind essenziell, da neue Bedrohungen nur in aktuellen Sicherheitsupdates adressiert werden. Dies gilt besonders für exponierte Systeme wie Router und Fernzugänge. Betreiber sollten regelmäßig - idealerweise automatisiert - prüfen, ob neue Softwareversionen vorliegen, und zumindest

Updates, die Sicherheitslücken beheben, schnellstmöglich und unter Beachtung der jeweiligen Risikoabwägung installieren. Falls der Hersteller eine Autoupdate-Funktion vorsieht, dies betrieblich möglich ist und die Produkte zwingend eine dauerhafte Internetverbindung benötigen, sollte diese Funktion aktiviert werden.

Maßnahmen zur Routine machen

Abschließend sollten diese Schritte zur Gewohnheit werden. Die genannten Maßnahmen sind regelmäßig zu wiederholen. Insbesondere sind eine wiederkehrende Angriffsflächen-Prüfung auf vorhandene Zugriffe und deren Absicherung sowie ein regelmäßiges Update- und Patch-Management durchzuführen. Inventar und Fernzugriffs-Dokumentation sowie Benutzer und Passwörter sind fortlaufend zu pflegen. Alle eingesetzten Sicherheitsmaßnahmen sollten geprüft und solche, die noch nicht im Einsatz sind, hinsichtlich ihrer Verwendungsmöglichkeit evaluiert werden; dies gilt auch für Anlagen, die durch Dritte installiert wurden.

Überprüfung auf eine Exposition und konkrete Gegenmaßnahmen

Insbesondere die Überprüfung auf eine direkte Exposition einer Anlage lässt sich mit geringem bis mittleren Aufwand durch Betreiber eigenständig umsetzen – etwa durch eine Prüfung der Router-Konfiguration auf aktive Portweiterleitungen (Port Forwarding), NAT-Regeln (Network Address Translation) sowie UPnP-Einträge (Universal Plug and Play). Besitzt der Betreiber keinen administrativen Zugriff auf den Router – etwa weil das Gerät vom Systemintegrator verwaltet wird – kann die Prüfung über die Router-Konfiguration nicht direkt erfolgen.

Von außen - Nutzung von etablierten Tools

Mittels Webangeboten wie <https://ivre.rocks>, <https://shodan.io> oder <https://censys.com> lässt sich überprüfen, ob die eigene öffentliche IP-Adresse oder Adressbereiche bereits gelistet sind. Zur Prüfung einzelner IP-Adressen bietet sich die manuelle Suche beispielsweise über die Webseite <https://internetdb.shodan.io/> an. Über den Button "View API Docs" und der dortigen Funktion "Get", kann eine IP-Adresse eingegeben und mit "Try it out" angezeigt werden. Hier werden offene Ports, CPE (Common Platform Enumeration) sowie Tags zurückgegeben. Dies kann auch automatisiert erfolgen.

Nicht immer sind öffentlich erreichbare Systeme bei diesen Suchmaschinen gelistet, da Provider die automatischen Scans teilweise blockieren oder Anlagen nicht permanent erreichbar sind. Daher empfiehlt es sich zusätzlich, die eigene öffentliche IP - soweit bekannt - eigenständig einem Portscan (z. B. mit dem Netzwerk-Tool 'Nmap') zu unterziehen und offene Ports zu identifizieren.

Hinweis

Ein Portscan ist nur am eigenen Anschluss bzw. nach ausdrücklicher Freigabe durch den Anschluss- oder Netzbetreiber zulässig. Da sich bei dynamischen IP-Adressen die Zieladresse ändern kann, sollte vor dem Scan die Zugehörigkeit zur eigenen Anschluss-IP geprüft werden. Bei Anschlüssen oder Netzen, die von Dritten betrieben werden, ist die Erlaubnis vorab einzuholen. Ein Scan muss von außerhalb des eigenen Netzwerks (Internet) gestartet werden, um vergleichbare Ergebnisse und Sichtbarkeit wie sie ein potentieller Angreifer erlangen zu können.

Zum schnellen Scannen gängiger Ports kann folgender Nmap-Befehl verwendet werden:

```
nmap -Pn <target-IP>
```

Die Option -Pn überspringt die Überprüfung, ob die Zieladresse online ist (ARP discovery), da solche Aufrufe von einer Firewall oder IPS (Intrusion Prevention System) normalerweise geblockt werden.

Zum Scannen aller offenen TCP- und UDP-Ports kann der nachfolgende Nmap-Befehl verwendet werden. Dieser Befehl benötigt erhöhte administrative Rechte (unter linux als root oder mittels 'sudo':

```
nmap -n -Pn -sT -sU -p- <target-IP>
```

Die Parameter "-sT" und "-sU" stellen dabei sicher, dass TCP- und UDP-Verbindungen geprüft werden. Der Parameter "-p-" sorgt dafür, dass sämtliche 2^{16} Ports (65536) gescannt werden. Der Betreiber sollte entsprechend mit einer längeren Ausführungszeit rechnen.

Von Innen - Blick ins eigene Netzwerk

Es wird dringend empfohlen, sich einen Überblick über die Netzwerkstruktur und die in der Anlage verbauten Geräte zu verschaffen und diese zu dokumentieren. Nur wer weiß, welche Geräte im Netz vorhanden und wie sie angebunden sind, kann beurteilen, welche Kommunikationsbeziehungen erwartet werden können und welche auffällig sind.

Eine mögliche Exposition lässt sich nicht allein an offenen Ports erkennen. Haben beispielsweise Geräte Zugang zu dem öffentlichen Netz, kann ein Zugriff von außen auch über den Umweg von innen geschehen. Ein zunächst harmlos erscheinendes Gerät baut in diesem Fall eine eigene Verbindung in das öffentliche Netz auf - über einen Kanal, der für das Gerät unter Umständen sogar vorgesehen ist und deshalb nicht auffällt. Pauschale Freigaben sämtlicher ausgehender Verbindungen oder undifferenzierte Firewall-Regeln sind weit verbreitet, weil sie sich schnell einrichten lassen und im Alltag kaum auffallen. Sie hebeln jedoch jeden Schutzgedanken der Netzwerktrennung aus: Bereits ein einziges kompromittiertes Gerät – etwa ein Fernwartungszugang oder ein IIoT-Sensor (Industrial Internet of Things) mit eigener Anbindung – kann dann als Sprungbrett in das gesamte Netz dienen.

Management-Interfaces von Routern und Firewalls

Neben Anlagenkomponenten besitzen auch Router und Firewalls Verwaltungsfunktionen, über die sich das jeweilige Gerät vollständig konfigurieren lässt. Diese Management-Interfaces sind häufig über eine Weboberfläche oder Kommandozeile erreichbar. Sind sie über Portweiterleitungen oder anderweitig aus dem Internet zugänglich, können Angreifende nach einer Kompromittierung beliebige Konfigurationen ändern. Auf diesem Weg lassen sich weitere Systeme der Anlage exponieren oder bestehende Schutzmaßnahmen aushebeln. Management-Interfaces dürfen keinesfalls aus dem Internet erreichbar sein. Die Verwaltung hat ausschließlich lokal zu erfolgen, beispielsweise über einen direkten Anschluss am Gerät. Hierfür sollte die Konfiguration der Netzkomponenten auf aktive Freigaben der Verwaltungsports geprüft und nicht benötigte Fernverwaltung deaktiviert werden.

Ausgehende Verbindungen prüfen

Betreiber sollten sich einen Überblick verschaffen, welche Geräte aktiv Verbindungen ins Internet oder in Dienstleisternetze aufbauen. Ein Monitoring mittels Netzwerkanalysertools wie beispielsweise Wireshark (<https://www.wireshark.org>) oder ganzer Programmsuiten wie Malcolm (<https://malcolm.fyi/>) macht diese ausgehenden Datenströme sichtbar und hilft dabei, sowohl ungewollte Fernwartungsverbindungen als auch verdächtige Kommunikation im Regelbetrieb zu erkennen.

Fernwartungszugänge

Fernwartungszugänge sind nicht immer ausreichend dokumentiert. Solche Zugänge können über ausgehende Verbindungen über einen Router, aber auch über zusätzliche Drahtlosverbindungen wie z. B. WiFi-Gateways oder LTE-Modems implementiert sein. Besonders (I)IoT-Funktionen und Verbindungen zu Cloud-Anwendungen werden der Einfachheit halber häufig mit einer eigenen Anbindung versehen. Es gibt Fälle, bei denen solche Zugänge dem Betreiber überhaupt nicht bekannt sind. Für den Betreiber nicht bekannte oder vom Provider dynamisch vergebenen IP-Adressen ist eine Exposition von außen nicht einfach festzustellen. Um auf solche Zugänge konsequent zu prüfen, kann es erforderlich sein, in jedem Schaltschrank nach Geräten mit entsprechenden Fähigkeiten (oft zu erkennen durch Antennen, eindeutige Bezeichnungen wie "Gateway" auf einem aufgedruckten Typenschild) zu suchen. Bei Vorhandensein eines solchen Geräts muss im Einzelfall die entsprechende Konfiguration überprüft werden. Zur Klärung hilft häufig nur das direkte Gespräch mit dem Dienstleister oder Integrator über aktive oder gegebenenfalls ungenutzte Fernzugänge.

APN-Verbindungen

Oft kommen bei Nutzung von auf Mobilfunk basierten Kommunikationswegen sogenannte private APNs (Access Point Name) zum Einsatz, bei denen mobile Geräte oder Anwendungen mit Fernzugriff direkt mit einem geschützten Firmennetzwerk verbunden werden. Die Idee dahinter entspricht einem VLAN (Virtual Local Area Network), bei dem das Mobilfunknetz den Datenverkehr direkt in ein dediziertes Firmennetz oder eine Cloud leitet. Dies soll unsichtbar für das öffentliche Netz geschehen.

Gleichwohl bietet ein privates APN alleine keinen ausreichenden Schutz. Eine vermeintlich abgeschottete, private Datenübertragung erfolgt häufig unverschlüsselt. Ohne zusätzliche Maßnahmen können Querbewegungen zwischen getrennten Anlagen möglich sein. Auch hier gilt es daher, die APN-Umgebung sorgfältig zu konfigurieren und die Zugriffe eng zu überwachen. Fortschrittliche Angreifer (APT) ist es in der Vergangenheit gelungen, APN Umgebungen von Mobilfunkbetreibern zu übernehmen [9].

Nur benötigte Verbindungen zulassen (Allow-Listing)

Undifferenzierte Firewall-Regeln sollten durch gezielte Freigaben ersetzt werden, die nur die tatsächlich benötigten Kommunikationsbeziehungen erlauben – jeweils mit definierter Quelle, Ziel und Port. Dieses Prinzip wird als Allow-Listing bzw. Positivliste bezeichnet. Was nicht explizit benötigt wird, sollte standardmäßig blockiert sein (Default-Deny). Besonders bei ausgehenden Verbindungen wird dies häufig vernachlässigt: Ausgehender Verkehr wird oft pauschal erlaubt, obwohl nur wenige konkrete Verbindungen benötigt werden. Doch gerade über ausgehende Verbindungen lassen sich kompromittierte Systeme fernsteuern oder können Daten abfließen.

Ein typisches Beispiel: Das Gerät in der Anlage benötigt als einzige Verbindung nach außen den Zugriff auf einen Cloud-Endpunkt bzw. einen Rendezvous-Server, über den der Fernwartungszugriff vermittelt wird. Alle übrige Kommunikation ins Internet wird verworfen. Bei einer linux Firewall mit iptables sähe der Syntax wie folgt aus:

```
iptables -P FORWARD DROP
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -s <DEVICE-IP> -d <CLOUD-SERVICE-IP> -p tcp --dport 443 -j
ACCEPT
```

In gängigen Routern werden solche Firewallregeln häufig nicht per Kommandozeile, sondern über die Weboberfläche eingetragen – etwa unter Menüpunkten wie „Firewall“, „Filterregeln“ oder „Zugriffskontrolle“. Die iptables-Befehle dienen ausschließlich als Beispiel für die Syntax einer solchen

Regel. Die Logik bleibt dabei stets dieselbe: zunächst das grundsätzliche Verwerfen sämtlicher Pakete, anschließend die gezielte Freigabe der jeweils benötigten Verbindung.

Segmentierung konsequent umsetzen und Any-to-Any-Regeln auflösen

Die Netzbereiche einer Anlage – etwa Büro-IT, OT, Fernwartung und IIoT – sollten mit geeigneten Firewall-Funktionen klar voneinander getrennt und wie im vorangegangenen Abschnitt beschrieben per Allow-Listing auf das notwendige Minimum beschränkt werden. Eine so reduzierte Angriffsfläche erschwert es Angreifenden, sich innerhalb des Netzes seitwärts zu bewegen.

Any-to-Any-Regeln – also Freigaben, die zwischen zwei Netzbereichen oder innerhalb eines Netzes sämtliche Kommunikation erlauben – heben diese Trennung faktisch auf und sollten unbedingt aufgelöst werden. Übergänge in ein eigenes VLAN oder ein privates APN (siehe APN-Verbindungen) ersetzen keine echte Segmentierung: Wirkt die Trennung nur in einer Richtung und sind die Zugriffe im Zielbereich wieder pauschal erlaubt, kann sich ein dort kompromittiertes Gerät ungehindert im gesamten Bereich bewegen. Allow-Listing ist daher auch innerhalb dieser Bereiche umzusetzen.

Praktisch lässt sich wie folgt vorgehen: Zuerst die tatsächlich vorhandenen Kommunikationsbeziehungen ermitteln – etwa aus dem Netzwerkinventar, den Projektierungsdaten oder durch zeitweilige Protokollierung am Zonenübergang. Darauf aufbauend werden die Regeln zwischen den Zonen als Positivliste aufgebaut und nicht benötigte Freigaben entfernt.

Weiterführende Literatur und Links

Die in dieser Empfehlung vorgestellten Maßnahmen sind lediglich ein Teil der im ICS-Security-Kompendium [10] aufgeführten Maßnahmen. Detaillierte Informationen zur Etablierung von Fernzugriff oder Fernwartung auf OT-/ICS-Komponenten nach Stand der Technik sind im IT-Grundschutz-Kompendium [11] zu finden. Weitere Informationen rund um die Cybersicherheit der jeweiligen Branche können den Branchenspezifischen Sicherheitsstandards (B3S) entnommen werden [12] sowie weiteren Produkten des Branchenverbandes.

- [1] <https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-231a>
- [2] <https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262788-1032.pdf>
- [3] <https://www.heise.de/news/FBI-und-US-Umweltbehoerde-warnen-Cyberangriffe-auf-US-Wasserwerke-haeufen-sich-11394614.html>
- [4] <https://www.golem.de/news/us-cyberbehoerde-iranische-hacker-stecken-wohl-hinter-angriffen-auf-us-wasserwerke-2608-211519.html>
- [5] <https://www.cisa.gov/news-events/alerts/2026/07/30/cisa-urges-water-and-wastewater-systems-sector-protect-ot-against-activity-targeting-plcs>
- [6] <https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/>
- [7] <https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/>
- [8] <https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.pdf>
- [9] https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Sicherheitshinweis_SALT-TYPHOON_250527.html
- [10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html

[11] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html

[12] https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Branchenspezifische-Sicherheitsstandards-B3S/Uebersicht-der-B3S/uebersicht-der-b3s_node.html

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.