

**WOCHENBERICHT**

# OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 41/2026 · Strom und Energie in DACH

|                         |                                                       |
|-------------------------|-------------------------------------------------------|
| <b>Zielgruppe</b>       | Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger |
| <b>Berichtszeitraum</b> | 02.10.2026-09.10.2026                                 |
| <b>Version</b>          | 1.0                                                   |
| <b>Datum</b>            | 09.10.2026                                            |
| <b>Autor</b>            | Maximilian Gilg, OT-Cyber.de                          |
| <b>Klassifizierung</b>  | TLP:CLEAR – ausschließlich öffentliche Quellen        |

Dieser Bericht fasst öffentlich zugängliche Meldungen zusammen. Die Einstufung der Relevanz bezieht sich auf Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger in Deutschland, Österreich und der Schweiz.

## Management Summary

In KW 41 kam die größte Gefahr für Energieversorger in DACH wieder über Edge-Geräte. Remote-Access-, WAN- und Perimetersysteme vor Leitstelle und Fernwartung wurden gleichzeitig angegriffen. Bei Citrix NetScaler wird eine SAML-Lücke gezielt angegriffen (CVE-2026-88779, laut Citrix Denial of Service). Sie trifft auch Geräte, die schon gegen CVE-2026-88771 bis -88778 gepatcht waren, Neustarts wurden auch auf Build 14.1-73.37 gemeldet. Im Cisco Catalyst SD-WAN Manager wird eine Lücke ausgenutzt, mit der Angreifer die Anmeldung umgehen (CVE-2026-76504, CVSS 9,8). Für einen weiteren Zero-Day in FortiMail (CVE-2026-104286, CVSS 9,8) gibt es seit 05.10. Fixes. FBI und Secret Service warnen außerdem, dass die FortiBleed-Kampagne gegen FortiGate-Firewalls weiterläuft und als Initial Access für Ransomware dient. Über genau diese Systeme laufen bei vielen Netzbetreibern und Stadtwerken die Fernwartung, die Anbindung der Außenstellen und der Remote Access ins Leitnetz. Ein Patch allein reicht deshalb nicht. Die Geräte müssen auch darauf geprüft werden, ob sie schon kompromittiert sind.

In der Leittechnik hat CISA am 06.10. Advisories zu Hitachi Energy nachveröffentlicht. Am schwersten wiegen sechs Lücken in alter RTU500-CMU-Firmware (11.x und älter, End-of-Life, bis CVSS 9,8, gefunden von Dragos). Dazu kommen DoS-Lücken in der IEC-61850-Funktion des Sammelschienenschutzes REB500 und eine ActiveMQ-Lücke in Hitachi Energy SOI. Moxa meldet eine kritische Lücke in MGate-Protokoll-Gateways. NCSC-NL und Modat haben 8.547 offen erreichbare Systeme in europäischen Wind- und Solarparks gefunden, 884 davon in Deutschland. Der Datendiebstahl beim KRITIS-Zertifizierer GUTcert (640 GB Netzpläne und Audit-Berichte) bleibt ein offenes Lieferkettenrisiko. In Österreich gilt seit 01.10. das NISG 2026. Kleine Teams kommen mit den fünf SANS ICS Critical Controls gut durch die Woche, vor allem mit Secure Remote Access (CC4) und Risk-Based Vulnerability Management (CC5).

### GESAMTBEWERTUNG

Die Lage ist hoch. Mehrere Zero-Days und eine Zugangsdaten-Kampagne treffen gleichzeitig Remote-Access-, WAN- und Perimetersysteme, die direkt in die Netzleittechnik führen. Vorrang haben Patch und Compromise Assessment für NetScaler, Cisco SD-WAN, FortiMail und FortiGate (CC4). Danach folgt der Abgleich des Asset-Inventars mit den Hitachi-Energy-Advisories, vor allem RTU500-Firmware 11.x (CC5).

## Trends

- Edge-Geräte für Remote Access, WAN und Perimeter (NetScaler, Cisco SD-WAN, FortiMail, FortiGate, SonicWall SMA1000) bleiben der wichtigste Initial Access. Neue Lücken treffen innerhalb von Tagen auch frisch gepatchte Geräte, wie bei NetScaler 14.1-73.37.
- Patchen allein reicht nicht mehr: Behörden verlangen neben dem Update ausdrücklich eine forensische Prüfung auf Kompromittierung.
- End-of-Life-Firmware in der Fernwirktechnik wird zum eigenen Risiko und zum Ziel für Forscher und Angreifer. Für RTU500 11.x gibt es nur noch das Upgrade, keinen Patch. Ohne Asset-Inventar lässt sich das Risiko nicht bewerten.
- Offene Bibliotheken wie libexpat (REB500), ActiveMQ (Hitachi SOI) und lwIP (ICSA-26-279-02, CVSS 9,8, Sektor Energie) stecken quer durch Schutz-, Leit- und Feldgeräte. Ein SBOM wird damit zur Pflicht.

- Bei den Erneuerbaren wächst die Angriffsfläche schneller als die Absicherung, vor allem über Fernzugänge von Herstellern und Betriebsführern.
- Lieferkettenrisiken verlagern sich zu Dienstleistern mit sensiblen Unterlagen, etwa Zertifizierern, Ingenieurbüros oder Betriebsführern (GUTcert).
- Mit gestohlenen Zugangsdaten statt Exploits (FortiBleed) kommen Angreifer auch an gepatchten Geräten vorbei. Dagegen helfen nur MFA und Kontenkontrolle.

## Lageübersicht

| ID   | Meldung                                                                                                                                   | Relevanz     | Quelle                                                                                                                                                                                                                                                                                                                                      |
|------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L-01 | Citrix NetScaler: SAML-Zero-Day CVE-2026-88779 (DoS) trifft auch bereits gepatchte Geräte                                                 | KRITISCH     | Citrix Security Bulletin CTX697174 ( <a href="https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html">https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html</a> ) / BleepingComputer 04.10. / CISA KEV, 03.10./04.10.                            |
| L-02 | Cisco Catalyst SD-WAN Manager: Auth-Bypass-Zero-Day CVE-2026-76504 (CVSS 9,8) wird aktiv ausgenutzt                                       | KRITISCH     | Cisco Security Advisory / CISA KEV, 30.09.                                                                                                                                                                                                                                                                                                  |
| L-03 | Hitachi Energy RTU500: sechs Schwachstellen in CMU-Firmware 11.x und älter (End-of-Life), bis CVSS 9,8                                    | HOCH         | CISA ICSA-26-279-06 / Hitachi Energy PSIRT, 06.10.                                                                                                                                                                                                                                                                                          |
| L-04 | 8.547 offen erreichbare Steuer- und Login-Systeme in europäischen Wind- und Solarparks, 884 davon in Deutschland                          | HOCH         | Help Net Security (Studie Modat / NCSC-NL), 09.10.                                                                                                                                                                                                                                                                                          |
| L-05 | FortiMail: Zero-Day CVE-2026-104286 (CVSS 9,8) wird ausgenutzt, Fixes seit 05.10. verfügbar                                               | HOCH         | Fortinet PSIRT FG-IR-26-175 / heise / BleepingComputer ( <a href="https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/">https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/</a> ) / CISA KEV, 01.10. |
| L-06 | Datenleck beim KRITIS-Zertifizierer GUTcert: 640 GB Netzpläne und Audit-Berichte von Energieversorgern (Nachtrag, keine neue Entwicklung) | HOCH         | energate messenger / IT-Administrator / Born City, 24.09.                                                                                                                                                                                                                                                                                   |
| L-07 | Hitachi Energy REB500 und SOI: libexpat-Lücken im IEC-61850-Sammelschienenschutz, ActiveMQ-Lücke in SOI                                   | MITTEL       | CISA ICSA-26-279-05 / ICSA-26-279-04 / Hitachi Energy PSIRT, 06.10.                                                                                                                                                                                                                                                                         |
| L-08 | Moxa MGate: Stack Overflow in Protokoll-Gateways, schon mit Leserechten ausnutzbar (CVE-2026-86325)                                       | MITTEL       | SecurityOnline / OpenCVE, 02.10.                                                                                                                                                                                                                                                                                                            |
| L-09 | Österreich: NISG 2026 ist in Kraft, Meldepflicht gilt sofort, Registrierung bis 31.12.                                                    | ORIENTIERUNG | WKO, 01.10.                                                                                                                                                                                                                                                                                                                                 |

## Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 09.10.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt.

| Region      | Gesamt | Top-Protokolle                                  |
|-------------|--------|-------------------------------------------------|
| Deutschland | 138446 | DNP3: 33442, OMRON FINS: 23821, ProConOS: 16426 |
| Österreich  | 4530   | HMI/VNC: 1061, DNP3: 954, IEC-104: 450          |

## Meldungen im Detail

### L-01 Citrix NetScaler: SAML-Zero-Day CVE-2026-88779 (DoS) trifft auch bereits gepatchte Geräte

KRITISCH Citrix Security Bulletin CTX697174

(<https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html>) /

BleepingComputer 04.10. / CISA KEV, 03.10./04.10.

Was ist neu: Laut Citrix-Bulletin CTX697174 (03.10., PST) ist CVE-2026-88779 ein Memory Overflow (CWE-119), der zu Denial of Service führt (CVSS v4 8,7). Betroffen sind nur NetScaler ADC/Gateway, die als SAML-SP oder SAML-IdP konfiguriert sind. Gefixt ist die Lücke in 14.1-73.41, 13.1-64.28, 14.1-73.41 FIPS und 13.1-37.282 FIPS/NDcPP. Das Bulletin selbst nennt keine Ausnutzung. Laut BleepingComputer (04.10.) hat Citrix aber gezielte Angriffe auf ungepatchte Geräte beobachtet, die zu Denial of Service führen können. Erste Berichte über Neustarts kamen am 02.10., auch von Geräten mit Build 14.1-73.37. Citrix fordert alle, die nach den Fixes für CVE-2026-88771 bis -88778 aktualisiert haben, zu einem erneuten Update auf. Die CISA hat die Lücke am 04.10. in den KEV-Katalog aufgenommen, die Frist für US-Bundesbehörden endete am 07.10.

Bedeutung: Bei vielen Stadtwerken und Netzbetreibern ist NetScaler das Gateway für die Fernwartung durch Dienstleister und für den Remote Access ins Leitnetz. Citrix spricht offiziell nur von Denial of Service. Laut BleepingComputer lief auf einem gepatchten Honeypot von Kevin Beaumont aber ein heruntergeladenes Malware-Binary, und ein Admin sah in Logs Benutzernamen mit Shell-Befehlen. Ob die Lücke Codeausführung erlaubt, ist nicht bestätigt. Schon ein Absturz legt die Fernwartung lahm, ein kompromittiertes Gerät öffnet den Weg für Lateral Movement in Richtung OT.

Empfehlung: Sofort auf 14.1-73.41 bzw. 13.1-64.28 aktualisieren (FIPS: 14.1-73.41 FIPS bzw. 13.1-37.282). Danach ein Compromise Assessment machen: nsaaad-Abstürze seit 02.10., verdächtige Benutzernamen, Webshells, neue Konten und aktive Sessions prüfen. Gibt es Spuren, Session-Tokens und Zugangsdaten zurücksetzen und die Incident Response nach Plan starten (CC4, CC1).

Quelle: <https://www.bleepingcomputer.com/news/security/citrix-patches-netscaler-saml-zero-day-exploited-in-attacks/> ✓ geprüft

## **L-02 Cisco Catalyst SD-WAN Manager: Auth-Bypass-Zero-Day CVE-2026-76504 (CVSS 9,8) wird aktiv ausgenutzt**

KRITISCH Cisco Security Advisory / CISA KEV, 30.09.

Was ist neu: Mit einer manipulierten URI-Kodierung (`/%6a\_security\_check`, also kodiert `/j\_security\_check`) erhalten Angreifer ohne Anmeldung Admin-Rechte auf die API. Laut Cisco wird die Lücke seit September ausgenutzt. Es ist der fünfte ausgenutzte Cisco-Zero-Day in diesem Jahr. Das Advisory wurde am 02.10. auf Version 1.1 (Final) aktualisiert. Einen Workaround gibt es nicht, nur ein Live-Protect-Shield, das teilweise und vorübergehend schützt. Gefixt sind 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 und 26.2.1.

Bedeutung: Wer Umspannwerke, Außenstellen oder die Netzleitstelle über Catalyst SD-WAN verbindet, gibt mit dem Manager die Kontrolle über die gesamte Standortvernetzung aus der Hand. Angreifer können dann Routing und Segmentierung ändern und sich per Lateral Movement weiterbewegen.

Empfehlung: Sofort auf eine gefixte Version aktualisieren. Danach serviceproxy-access.log und vmanage-server.log nach `//%6a\_security\_check` durchsuchen und die Admin-Konten prüfen. Den Manager nicht aus dem Internet erreichbar machen, sondern nur aus einem dedizierten Admin-Netz (CC5, CC2).

Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU> ✓ geprüft

## **L-03 Hitachi Energy RTU500: sechs Schwachstellen in CMU-Firmware 11.x und älter (End-of-Life), bis CVSS 9,8**

HOCH CISA ICSA-26-279-06 / Hitachi Energy PSIRT, 06.10.

Was ist neu: Hitachi Energy (29.09.) und CISA (06.10.) melden sechs Schwachstellen in der RTU500-CMU-Firmware 11.x und älter. Darunter sind ein Firmware-Upload ohne Anmeldung bzw. fehlende Authentifizierung (CVE-2026-8065, 9,1), ein Path Traversal (CVE-2026-8066, 9,1), ein Firmware-Download ohne Integritätsprüfung (CVE-2023-46143) und der VxWorks-WDB-Debug-Dienst auf UDP 17185 (CVE-2010-2965, 9,8). Gefunden hat sie Dragos. Für 11.x gibt es keine Updates mehr, Abhilfe ist nur ein Upgrade auf 12.7.8, 13.9.1 oder neuer. Eine Ausnutzung ist nicht bekannt.

Bedeutung: RTU500 ist in DACH in Umspannwerken und in der Fernwirktechnik (IEC 60870-5-101/104, IEC 61850) weit verbreitet. Alte Firmware-Stände laufen dort oft über Jahre weiter. Wer ins Stationsnetz kommt, kann die Firmware tauschen, Befehle ausführen und die RTU neu starten. Das betrifft direkt die Steuerbarkeit des Netzes.

Empfehlung: Im Asset-Inventar alle RTU500 mit CMU-Firmware 11.x oder älter finden und das Upgrade auf 12.7.8/13.9.1 für das nächste Wartungsfenster planen. Bis dahin UDP 17185 sowie die Web-, Update-, Engineering- und Debug-Schnittstellen per Firewall auf das Stationsnetz bzw. die Engineering-Workstation beschränken (CC5, CC2).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-06> ✓ geprüft

## **L-04 8.547 offen erreichbare Steuer- und Login-Systeme in europäischen Wind- und Solarparks, 884 davon in Deutschland**

**HOCH** Help Net Security (Studie Modat / NCSC-NL), 09.10.

Was ist neu: Modat und das niederländische NCSC haben in 35 Ländern 8.547 aus dem Internet erreichbare Systeme in Wind- und Solarparks gefunden. In Deutschland sind es 672 bei PV und 212 bei Wind. Darunter ist eine Steuerseite für Windenergieanlagen mit Start-, Stopp- und Reset-Knöpfen, die auf den Webserver einer Siemens ET 200SP verweist. Für Österreich und die Schweiz nennt die Studie keine Zahlen.

Bedeutung: Erzeuger und Stadtwerke mit eigenen Wind- und PV-Parks sind direkt betroffen. Lassen sich viele Anlagen gleichzeitig steuern, betrifft das die Netzstabilität. Oft hat der Hersteller oder Betriebsführer den Zugang eingerichtet, ohne dass der Betreiber davon weiß.

Empfehlung: Die eigenen öffentlichen IP-Bereiche und die der Betriebsführer auf erreichbare Parkregler, Wechselrichter- und SCADA-Oberflächen prüfen, etwa mit Shodan oder Censys. Admin-Oberflächen nur über einen gesicherten Remote Access mit MFA und Einzelkonten erreichbar machen (CC4, CC3).

Quelle: <https://www.helpnetsecurity.com/2026/10/09/eu-renewable-energy-cybersecurity/> ✓ geprüft

## **L-05 FortiMail: Zero-Day CVE-2026-104286 (CVSS 9,8) wird ausgenutzt, Fixes seit 05.10. verfügbar**

**HOCH** Fortinet PSIRT FG-IR-26-175 / heise / BleepingComputer (<https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/>) / CISA KEV, 01.10.

Was ist neu: Über einen Path Traversal schreiben Angreifer ohne Anmeldung Dateien auf FortiMail und führen so Code aus. Betroffen sind 7.2 bis 7.2.9, 7.4 bis 7.4.8, 7.6 bis 7.6.6 und 8.0.0 bis 8.0.1. CISA hat die Lücke am 01.10. in den KEV-Katalog aufgenommen. Die Fixes 8.0.2, 7.6.7 und 7.4.9 waren zunächst nur angekündigt. Am 05.10. hat Fortinet sie im Advisory FG-IR-26-175 als Lösung ergänzt, für 7.2 gibt es keinen Fix (Migration auf 7.4 oder neuer).

Bedeutung: Viele Stadtwerke betreiben FortiMail als Mail-Gateway. Ein übernommenes Gerät am Perimeter ist ein klassischer Initial Access in die IT, von dort ist Lateral Movement in Richtung OT möglich.

Empfehlung: Auf 8.0.2, 7.6.7 bzw. 7.4.9 aktualisieren, 7.2 auf 7.4 migrieren. Bis dahin IBE abschalten, das Management-Interface vom Internet trennen und nach IOCs suchen (CC5).

Quelle: <https://fortiguard.fortinet.com/psirt/FG-IR-26-175> ✓ geprüft

## **L-06 Datenleck beim KRITIS-Zertifizierer GUTcert: 640 GB Netzpläne und Audit-Berichte von Energieversorgern (Nachtrag, keine neue Entwicklung)**

**HOCH** energate messenger / IT-Administrator / Born City, 24.09.

Was ist neu: Laut GUTcert hatten Unbekannte ab dem 05.09. Zugriff auf die Systeme und haben vom 06. bis 09.09. rund 640 GB gestohlen. Darunter sind Betriebsstättenlisten (Umspannwerke, Ortsnetzstationen, Gas-Druckregelanlagen), Netzstrukturpläne mit IT-/OT-Infrastruktur und Audit-Berichte mit Schwachstellen. GUTcert ist auf die Erpressung nicht eingegangen, Entega hat sich als betroffen gemeldet. In KW 41 gab es keine belegte Veröffentlichung der Daten. Gemeldet wurde der Fall im September, im Briefing tauchte er am 06.10. auf.

Bedeutung: Für Netz- und Kraftwerksbetreiber, die über GUTcert zertifiziert sind, liegen damit womöglich genau die Unterlagen bei Angreifern, die ein gezielter Angriff braucht. Offene Audit-Feststellungen sind dabei besonders heikel, weil sie nicht mehr geheim sind.

Empfehlung: Beim Zertifizierer schriftlich klären, welche Unterlagen dort lagen. Noch offene Schwachstellen aus Audit-Berichten vorrangig schließen und prüfen, ob eine Meldung nötig ist. An den genannten Standorten Threat Hunting und Monitoring verstärken (CC5, CC3, CC1).

Quelle: <https://www.energate-messenger.de/news/267259/cyberattacke-verursacht-grosses-kritis-datenleck>  
✓ geprüft

## **L-07 Hitachi Energy REB500 und SOI: libexpat-Lücken im IEC-61850-Sammelschienenenschutz, ActiveMQ-Lücke in SOI**

**MITTEL** CISA ICSA-26-279-05 / ICSA-26-279-04 / Hitachi Energy PSIRT, 06.10.

Was ist neu: REB500 bis Version 8.3.3.1 enthält zwei libexpat-Schwachstellen (CVE-2024-8176, CVE-2025-59375, jeweils CVSS 6,5). Ein authentifizierter Angreifer kann mit präparierten IEC-61850-Nachrichten einen Denial of Service auslösen, in einzelnen Fällen auch Speicherfehler. Behoben ist das in 8.3.4.0. In Hitachi Energy SOI 2.0.0 bis 2.2.0 ermöglicht eine ActiveMQ-Lücke Codeausführung (CVE-2026-34197, CVSS 8,8, Fix EP2).

Bedeutung: Fällt der Sammelschienenenschutz aus, ist die Selektivität gefährdet und damit die Versorgungssicherheit im Umspannwerk. Ein Angreifer braucht dafür allerdings schon Zugang und Rechte am Stationsbus.

Empfehlung: Das Update auf REB500 8.3.4.0 zusammen mit der Schutzprüfung ins nächste Wartungsfenster legen und SOI auf EP2 aktualisieren. Bis dahin den Zugang zum Stationsbus auf die nötigen Clients beschränken und den MMS-Verkehr überwachen (CC5, CC3).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-05> ✓ geprüft

## **L-08 Moxa MGate: Stack Overflow in Protokoll-Gateways, schon mit Leserechten ausnutzbar (CVE-2026-86325)**

MITTEL SecurityOnline / OpenCVE, 02.10.

Was ist neu: Moxa hat am 02.10. zwei MGate-Lücken veröffentlicht. CVE-2026-86325 (CVSS 4.0: 9,4) ist ein Stack Overflow in der Kontoverwaltung, den schon ein Konto mit reinen Leserechten auslösen kann. Mögliche Folgen sind das Auslesen von Speicher (auch Zugangsdaten), Manipulation und Ausfall. Laut Sekundärquellen sind MB3170/MB3270 bis Firmware 4.7 betroffen. Eine Ausnutzung ist nicht bekannt.

Bedeutung: MGate-Gateways sitzen oft an der Grenze zwischen Feldbus und Leittechnik, etwa in PV-Parks, BHKW oder Ortsnetzstationen. Ein kompromittiertes Gateway kann Messwerte und Befehle verfälschen.

Empfehlung: Den MGate-Bestand im Asset-Inventar erfassen, die Firmware nach dem Moxa-Advisory aktualisieren und die Web-Oberfläche nur aus dem Engineering-Netz erreichbar machen (CC5, CC2).

Quelle: <https://securityonline.info/moxa-mgate-vulnerabilities/> ✓ geprüft

## **L-09 Österreich: NISG 2026 ist in Kraft, Meldepflicht gilt sofort, Registrierung bis 31.12.**

ORIENTIERUNG WKO, 01.10.

Was ist neu: Das NISG 2026 hat am 01.10.2026 das NISG 2018 abgelöst. Erhebliche Cybervorfälle sind ab diesem Tag meldepflichtig. Wesentliche und wichtige Einrichtungen müssen sich bis 31.12.2026 registrieren, die Form regelt noch eine Verordnung. Der Anwendungsbereich umfasst jetzt das ganze Unternehmen.

Bedeutung: Österreichische Netzbetreiber und Erzeuger brauchen jetzt einen funktionierenden Meldeweg und müssen den Geltungsbereich abgrenzen, auch für die OT.

Empfehlung: Meldeprozess und Zuständigkeiten mit dem OT-Incident-Response-Plan abstimmen und die Registrierung vorbereiten (CC1).

Quelle: <https://www.wko.at/it-sicherheit/nis2-uebersicht> ✓ geprüft

## **Fragen für das nächste Jour fixe**

1. Haben wir NetScaler, Cisco SD-WAN, FortiMail und FortiGate nicht nur gepatcht, sondern auch auf Kompromittierung geprüft, und wer hat das dokumentiert?
2. Über welche Systeme erreichen Dienstleister heute unsere Leittechnik, und sind alle auf dem Stand vom 04.10.?
3. Wie viele RTU500 laufen bei uns noch mit CMU-Firmware 11.x oder älter, und wann ist das Upgrade eingeplant?
4. Sind Parkregler, Wechselrichter- oder SCADA-Oberflächen unserer Wind- und PV-Anlagen oder unserer Betriebsführer aus dem Internet erreichbar?
5. Welche Unterlagen (Netzpläne, Audit-Befunde) liegen bei externen Zertifizierern, und wie sind sie dort geschützt?
6. Würden wir eine kompromittierte Firewall oder ein manipuliertes Gateway im OT-Netz überhaupt bemerken (Monitoring, Logs)?
7. Ist unser Meldeweg nach NIS2 (DE: § 5d EnWG / AT: NISG 2026 / CH: 24-h-Meldung an das BACS) mit dem OT-Incident-Response-Plan geübt?

## Maßnahmen dieser Woche

1. NetScaler mit SAML auf 14.1-73.41 bzw. 13.1-64.28 aktualisieren (FIPS: 14.1-73.41 FIPS / 13.1-37.282) und danach ein Compromise Assessment machen: nsaaad-Abstürze seit 02.10., verdächtige Benutzernamen, Webshells, neue Konten und Sessions prüfen (CC4, CC1).
2. Cisco Catalyst SD-WAN Manager auf eine gefixte Version bringen, serviceproxy-access.log und vmanage-server.log nach `%6a\_security\_check` durchsuchen und den Manager nur aus dem Admin-Netz erreichbar machen (CC5, CC2).
3. FortiMail auf 8.0.2/7.6.7/7.4.9 aktualisieren (7.2 auf 7.4 migrieren), bis dahin IBE abschalten, das Management-Interface vom Internet trennen und nach IOCs suchen (CC5).
4. FortiGate: Admin- und VPN-Sessions beenden, Passwörter zurücksetzen, auf PBKDF2 umstellen, phishing-resistente MFA einschalten und die Konten mit dem Soll-Stand abgleichen (CC4).
5. Im Asset-Inventar RTU500 mit CMU-Firmware 11.x oder älter, REB500 bis 8.3.3.1, Hitachi SOI 2.0.0 bis 2.2.0 und Moxa MGate erfassen, Upgrades einplanen und bis dahin UDP 17185 sowie die Management-Schnittstellen abschotten (CC5, CC2).
6. Öffentliche IP-Bereiche, auch die der Betriebsführer, auf erreichbare Steuer- und Login-Oberflächen von Wind- und PV-Anlagen prüfen und diese hinter einen gesicherten Remote Access mit MFA legen (CC4).
7. Beim Zertifizierer klären, ob Unterlagen vom GUTcert-Datenleck betroffen sind, offene Audit-Feststellungen vorrangig schließen und die Meldepflicht prüfen (CC5, CC1).
8. Österreich: Meldeprozess nach NISG 2026 mit dem OT-Incident-Response-Plan abstimmen und die Registrierung bis 31.12.2026 vorbereiten (CC1).

### HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 09.10.2026 automatisch aufgerufen und inhaltlich geprüft. 1 Meldung(en) ohne überprüfbare Originalquelle wurden nicht aufgenommen.