

WOCHENBERICHT

OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 42/2026 · Strom und Energie in DACH

Zielgruppe	Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger
Berichtszeitraum	09.10.2026–16.10.2026
Version	1.0
Datum	16.10.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	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 42/2026 ist kein bestätigter Cyberangriff auf Netzbetreiber, Stadtwerke oder Erzeuger in Deutschland, Österreich oder der Schweiz bekannt geworden. Die größte Gefahr kam trotzdem über die IT/OT-Grenze. Angreifer nutzen bereits zwei Lücken in Edge-Geräten aus: einen Zero-Day in Ivanti Connect Secure (CVE-2026-104935, seit 13.10. im KEV-Katalog der CISA) und eine root-Lücke in der Management-Oberfläche von Palo Alto PAN-OS (CVE-2026-0322, seit 14.10. im KEV-Katalog). Gerade diese VPN-Gateways und Firewalls sichern bei vielen Stadtwerken den Remote Access in die Leitstelle und die Segmentierung zwischen Büro und Netzleittechnik.

Für die Erneuerbaren hat eine Studie von Modat und NCSC-NL 8.547 aus dem Internet erreichbare Steuerungs- und Verwaltungssysteme in Wind- und Solarparks gezählt. 884 davon stehen in Deutschland, und an 181 Standorten in Europa hatten die Forscher volle Kontrolle über die Anlagen. In der Leittechnik kamen wichtige Advisories hinzu: Hitachi Energy RTU500 (Firmware-Upload ohne Anmeldung), openPDC und openHistorian (Remote Code Execution, fest eingebautes Admin-Passwort), die OPC-UA-Bibliothek Eclipse Milo sowie Inductive Automation Ignition. Für diese Lücken ist bisher keine Ausnutzung bekannt. Erzeuger und Stadtwerke sollten die Lage zum Anlass nehmen, ihren Remote Access (CC4) und ihr Asset-Inventar samt Vulnerability Management (CC5) zu prüfen.

GESAMTBEWERTUNG

Die Lage ist erhöht, auch ohne bestätigten Vorfall bei Energieversorgern in DACH, weil Angreifer zwei Lücken in VPN- und Firewall-Gateways an der IT/OT-Grenze aktiv ausnutzen. Vorrang haben Patches und Kompromittierungsprüfung für Ivanti und PAN-OS. Danach folgen die Erreichbarkeit von Parkreglern und Erneuerbaren-Portalen sowie die Patches für Fernwirk-RTUs und Leittechnik-Software.

Trends

- Edge-Geräte an der IT/OT-Grenze (VPN-Gateways, Firewalls) bleiben der wichtigste Einstiegspunkt. Ivanti und PAN-OS landeten innerhalb von zwei Tagen im KEV-Katalog, und die Angreifer umgehen inzwischen auch die Prüfwerkzeuge der Hersteller.
- Die Erneuerbare Erzeugung wächst schneller als ihre Absicherung. Offen erreichbare Parkregler und Portale sind messbar ein Massenproblem, bei Windkraft liegt Deutschland vorn. Oft fehlen diese Systeme im Asset-Inventar.
- End-of-Life-Firmware ist der gemeinsame Nenner bei RTU500, den französischen Kühlsteuerungen und vielen Altgeräten. Ohne Lebenszyklus-Daten im Asset-Inventar bleibt das Risiko unsichtbar.
- Lücken in Bibliotheken wie Eclipse Milo erreichen Betreiber nur über die Hersteller. Ohne SBOM funktioniert Vulnerability Management in der Leittechnik nicht mehr, das wird auch mit Blick auf den CRA praktisch relevant.
- Alte Lücken (ProFTPD, BIND aus 2015) landen wieder im KEV-Katalog. Embedded-Linux-Geräte nahe der OT gehören deshalb in die Patch-Planung.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Ivanti Connect Secure: Zero-Day CVE-2026-104935 wird aktiv ausgenutzt, ein Teil der Angriffskette ist noch ungepatcht	KRITISCH	BleepingComputer / Volexity / Rapid7 / CISA KEV / Canadian Centre for Cyber Security (AV26-1035), 13.10.
L-02	Palo Alto PAN-OS: root-Lücke (RCE) in der Management-Oberfläche wird ausgenutzt (CVE-2026-0322)	HOCH	Palo Alto Networks Security Advisory / CISA KEV, 14.10.
L-03	Studie Modat/NCSC-NL: 8.547 offen erreichbare Systeme in europäischen Wind- und Solarparks, 884 davon in Deutschland	HOCH	heise online / pv magazine (Studie von Modat mit NCSC-NL), 09.10.
L-04	Hitachi Energy RTU500: Firmware-Upload ohne Anmeldung auf der CMU (CVE-2026-8065/-8066, CVSS 9,1)	HOCH	CVE-Einträge (OpenCVE) und CISA-Bulletins vom 06.10. und 08.10., 06.10.
L-05	openPDC und openHistorian (Grid Protection Alliance): Remote Code Execution und fest eingebautes Admin-Passwort (ICSA-26-281-02)	HOCH	CISA ICS Advisory, 08.10.
L-06	Eclipse Milo (OPC UA): Schwachstellen auf der Server-Seite, anonyme Clients können Knoten löschen (ICSA-26-288-01)	MITTEL	CISA ICS Advisory, 15.10.
L-07	Inductive Automation Ignition: Rechteausweitung bis zur Codeausführung auf dem Gateway (CVE-2026-92817, ICSA-26-286-01)	MITTEL	CISA ICS Advisory, 13.10.
L-08	CERT-FR: laufende Angriffe auf aus dem Internet erreichbare Kühlsteuerungen (Danfoss, Copeland xweb, Dixell xweb)	ORIENTIER UNG	CERT-FR (CERTFR-2026-ALE-012), 13.10.
L-09	NSA-Merkblatt: Zero Trust für kritische OT-Umgebungen	ORIENTIER UNG	NSA, 08.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 16.10.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt. Siemens S7 = Port 102 (alle ISO-TSAP-Dienste, nicht nur echte S7-Steuerungen), OPC UA = Standardport 4840.

Region	Gesamt	Top-Protokolle
Deutschland	143086	DNP3: 33392, OMRON FINS: 23267, ProConOS: 16506, Siemens S7: 8211, OPC UA: 5676
Österreich	4649	HMI/VNC: 1053, DNP3: 949, IEC-104: 454, Siemens S7: 357, OPC UA: 139

Meldungen im Detail

L-01 Ivanti Connect Secure: Zero-Day CVE-2026-104935 wird aktiv ausgenutzt, ein Teil der Angriffskette ist noch ungepatcht

KRITISCH BleepingComputer / Volexity / Rapid7 / CISA KEV / Canadian Centre for Cyber Security (AV26-1035), 13.10.

Was ist neu: Ivanti hat am 13.10. eine Authentication-Bypass-Lücke (CWE-290, CVSS 8,6) veröffentlicht. Angreifer können damit ohne Anmeldung Befehle auf dem VPN-Gateway ausführen. Laut Volexity kombiniert der Threat Actor UTA0576 die Lücke seit mindestens 03.10. mit einer Privilege Escalation, für die es noch keinen Patch gibt. Dabei stiehlt er Active-Directory-Zugangsdaten, LAPS-Passwörter und BitLocker-Schlüssel. Betroffen sind die Versionen bis 22.8R2.4, bis 25.1.1.1 und bis 25.1.2.2. Gepatcht sind 22.8R2.5, 25.1.1.2 und 25.1.3.x. Die CISA hat die Lücke am 13.10. in den KEV-Katalog aufgenommen.

Bedeutung: Bei vielen Netzbetreibern und Stadtwerken läuft der Remote Access für Fernwartung, Dienstleister und Bereitschaft über Ivanti. Laut Volexity verändern die Angreifer Logs und setzen keine Webshell ein. Deshalb erkennt das Integrity Checker Tool die Kompromittierung womöglich nicht. Mit gestohlenen AD-Zugangsdaten ist Lateral Movement bis in die Netzleittechnik möglich, wenn die Domänen nicht getrennt sind.

Empfehlung: Sofort auf 22.8R2.5, 25.1.1.2 oder 25.1.3.x aktualisieren und das Gateway so behandeln, als wäre es kompromittiert. Dazu gehören Netzwerk- und Speicherforensik und Threat Hunting in den Logs ab 01.10. Alle Zugangsdaten rotieren, die über das Gateway liefen. OT-Zugänge nur über einen eigenen Jump Host mit eigener Anmeldung und MFA zulassen (CC4 Secure Remote Access).

Quelle: <https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-day-exploited-in-attacks/> ✓ geprüft

L-02 Palo Alto PAN-OS: root-Lücke (RCE) in der Management-Oberfläche wird ausgenutzt (CVE-2026-0322)

HOCH Palo Alto Networks Security Advisory / CISA KEV, 14.10.

Was ist neu: Wer gültige Admin-Zugangsdaten hat und die Management-Oberfläche erreicht, kann Code als root ausführen (CVSS 4.0: 8,6, Status ATTACKED). Betroffen sind PAN-OS 10.2 bis 12.2 auf PA-Series, VM-Series und Panorama. Cloud NGFW und Prisma Access sind nicht betroffen. Palo Alto meldet „very limited exploitation“ und kennt keinen Workaround. Die CISA hat die Lücke am 14.10. in den KEV-Katalog aufgenommen.

Bedeutung: Bei vielen Stadtwerken trennen PAN-OS-Firewalls das Büronetz von der Netzleittechnik. Ein Angreifer mit root auf dieser Firewall kann die Segmentierung zur Netz- und Stationsleittechnik aushebeln und Regeln für den Weg in die OT öffnen. Mit gestohlenen Zugangsdaten, etwa aus der Ivanti-Welle, sinkt die Hürde dafür deutlich.

Empfehlung: Auf die gefixte Version des jeweiligen Zweigs aktualisieren, z. B. 12.2.4, 11.2.16 oder 10.2.18-h12. Die Management-Oberfläche nur aus einem eigenen Admin-Netz oder über einen Jump Host erreichbar machen. Admin-Konten mit MFA schützen und die Konfigurationsänderungen der letzten Wochen prüfen (CC2 Defensible Architecture).

Quelle: <https://security.paloaltonetworks.com/CVE-2026-0322> ✓ geprüft

L-03 Studie Modat/NCSC-NL: 8.547 offen erreichbare Systeme in europäischen Wind- und Solarparks, 884 davon in Deutschland

HOCH heise online / pv magazine (Studie von Modat mit NCSC-NL), 09.10.

Was ist neu: Die Studie „To see the wind and the sun“ wurde am 07.10. vorgestellt. Sie zählt in 35 europäischen Ländern 7.942 Solar- und 605 Windkraft-Systeme, die aus dem Internet erreichbar sind. Für Deutschland sind es 672 Solar- und 212 Windpark-Systeme, bei Wind liegt Deutschland damit europaweit vorn. An 181 Standorten hatten die Forscher weitreichende Kontrolle, etwa um Turbinen zu starten, zu stoppen und zurückzusetzen oder ganze Parks abzuschalten. Die Betreiber werden über die nationalen CERTs informiert.

Bedeutung: Stadtwerke und Erzeuger mit eigenen Erneuerbaren betreiben solche Systeme oft über Dienstleister und Herstellerportale, die nicht im Asset-Inventar stehen. Laut den Forschern sind die Zahlen eine Untergrenze, weil nur eindeutig zugeordnete Systeme gezählt wurden. Für Österreich und die Schweiz nennen die Berichte keine Zahlen. Ein erfolgreicher Angriff ist nicht belegt, aber der Angriff auf polnische Wind- und Solarparks im Dezember 2025 zeigt, dass solche Ziele angegriffen werden.

Empfehlung: Die eigenen öffentlichen IP-Bereiche und Domains sowie die der Betriebsführer auf erreichbare Parkregler, Datenlogger und Web-Oberflächen prüfen, etwa mit Shodan oder Modat. Admin-Oberflächen aus dem Internet nehmen und nur noch über VPN mit MFA erreichbar machen. Die Zugänge von Dienstleistern ins Asset-Inventar aufnehmen (CC4 Secure Remote Access).

Quelle: <https://www.heise.de/news/Tausende-europaeische-Windanlagen-und-Solarparks-offen-im-Internet-11482262.html> ✓ geprüft

L-04 Hitachi Energy RTU500: Firmware-Upload ohne Anmeldung auf der CMU (CVE-2026-8065/-8066, CVSS 9,1)

HOCH CVE-Einträge (OpenCVE) und CISA-Bulletins vom 06.10. und 08.10., 06.10.

Was ist neu: CVE-2026-8065 ist eine Authentication-Bypass-Lücke im Firmware-Update-Endpunkt der RTU500-CMU. Ein Angreifer kann damit ohne Anmeldung beliebige Firmware einspielen. CVE-2026-8066 ist eine Path-Traversal-Lücke beim Datei-Upload. Beide Lücken haben CVSS 9,1. Laut den CVE-Datenbanken betreffen sie Firmware-Versionen, die keinen Support mehr bekommen. Die CISA führt die RTU500-CMU-Firmware im Bulletin vom 06.10. und hat am 08.10. ein Update zu ICSA-25-259-02 veröffentlicht.

Bedeutung: Die RTU500 ist in DACH in der Fernwirktechnik von Verteilnetzbetreibern weit verbreitet. Manipulierte Firmware auf einer RTU kann Schalthandlungen und Messwerte verfälschen und ist nur schwer zu erkennen.

Empfehlung: Im Asset-Inventar alle CMUs mit Firmware bis 11.x finden und auf eine unterstützte Version bringen. Laut Tagesbriefing sind das 12.7.8 bzw. 13.9.1, das sollte mit dem Hitachi-Advisory abgeglichen werden. Bis dahin den Webserver der CMU deaktivieren oder nur aus der Engineering-Zone erreichbar machen (CC5, CC2).

Quelle: <https://app.opencve.io/cve/CVE-2026-8065> ✓ geprüft

L-05 openPDC und openHistorian (Grid Protection Alliance): Remote Code Execution und fest eingebautes Admin-Passwort (ICSA-26-281-02)

HOCH CISA ICS Advisory, 08.10.

Was ist neu: Das Advisory nennt sechs Schwachstellen. Dazu gehören eine Deserialisierung mit Remote Code Execution (CVE-2026-100730, CVSS 3.1: 9,8) und ein fest eingebautes Admin-Passwort im Docker-Image (CVE-2026-105278, 9,8). Die Datenpublisher nehmen standardmäßig Verbindungen ohne Anmeldung an und geben die Geräte- und Messtopologie preis. Behoben ist das in openPDC 2.9.482 und openHistorian 2.8.585. Für das Docker-Image kommt kein Fix.

Bedeutung: Übertragungs- und Verteilnetzbetreiber nutzen openPDC und openHistorian für Phasormessdaten (PMU, IEEE C37.118) und Langzeitarchive. Wer diese Systeme kontrolliert, kann Messdaten manipulieren und Netzzustände falsch darstellen. Das Update ändert die Standardbindung nur bei Neuinstallationen, bestehende Systeme müssen von Hand umgestellt werden.

Empfehlung: Im Asset-Inventar nach openPDC, openHistorian und Docker-Varianten suchen und aktualisieren. Die Bindung der Publisher von Hand auf localhost oder die nötigen Gegenstellen begrenzen und das Docker-Image nicht produktiv nutzen (CC5 Risk-Based Vulnerability Management).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-02> ✓ geprüft

L-06 Eclipse Milo (OPC UA): Schwachstellen auf der Server-Seite, anonyme Clients können Knoten löschen (ICSA-26-288-01)

MITTEL CISA ICS Advisory, 15.10.

Was ist neu: Die CISA meldet für die Java-Bibliothek Eclipse Milo in den Versionen 0.6.0 bis 1.1.4 Schwachstellen auf der Server-Seite (widersprüchlich: A nennt sechs, B sechs CVEs im Advisory, aber nur fünf im Kopf des Advisories). Anonyme oder schwach berechnete Clients können geschützte Methoden aufrufen und Daten löschen (CVE-2026-58080, CVSS 3.1: 8,2). Über ein Padding Oracle lassen sich Passwörter zurückgewinnen (CVE-2026-60007, CVSS 4.0: 9,1). Ein Speicherleck legt den Server ohne Anmeldung lahm (CVE-2026-63252). Der Fix steckt nur in Version 1.1.5, der 0.6.x-Zweig bekommt keinen Patch.

Bedeutung: Milo steckt unsichtbar in Gateways, SCADA- und Edge-Produkten, die OPC UA zwischen Leittechnik, Erzeugungsanlagen und IT-Systemen übersetzen. Betreiber erkennen die Abhängigkeit nur über die SBOM oder über eine Anfrage beim Hersteller. Die CISA nennt ausdrücklich den Energiesektor. (Bewertung widersprüchlich: A HOCH / B MITTEL.)

Empfehlung: Leittechnik-, Gateway- und SCADA-Hersteller schriftlich fragen, ob Milo in ihrer SBOM steckt und wann ein Update kommt. Bis dahin anonyme OPC-UA-Sessions abschalten und OPC-UA-Server nur innerhalb ihrer Zone bzw. aus definierten Zonen erreichbar machen (CC5 Risk-Based Vulnerability Management).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-288-01> ✓ geprüft

L-07 Inductive Automation Ignition: Rechteausweitung bis zur Codeausführung auf dem Gateway (CVE-2026-92817, ICSA-26-286-01)

MITTEL CISA ICS Advisory, 13.10.

Was ist neu: Das Perspective-Modul prüft die Berechtigungen beim Designer-Zugriff nicht ausreichend. Ein angemeldeter Nutzer mit Zugriff auf ein Vision-Projekt kann so Designer-Rechte erlangen und Code im Gateway-Prozess ausführen (CVSS v3.1 8,8). Betroffen sind die Versionen 8.1.0 bis 8.1.54 und 8.3.0 bis 8.3.8. Die CISA kennt keine öffentliche Ausnutzung.

Bedeutung: Ignition läuft bei Stadtwerken und Erzeugern als SCADA und als Datendrehscheibe. Schon ein einfaches Bedienkonto reicht, um den Server zu übernehmen.

Empfehlung: Updaten und prüfen, welche Konten Zugriff auf Vision-Projekte haben. Zugriffe aus der IT auf das Gateway nur über einen Jump Host zulassen (CC5).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-286-01> ✓ geprüft

L-08 CERT-FR: laufende Angriffe auf aus dem Internet erreichbare Kühlsteuerungen (Danfoss, Copeland xweb, Dixell xweb)

ORIENTIERUNG CERT-FR (CERTFR-2026-ALE-012), 13.10.

Was ist neu: CERT-FR hat die Warnung vom 12.10. am 13.10. erweitert und kennt zahlreiche Kompromittierungen. Die Angriffe laufen laut CERT-FR wahrscheinlich noch. Ein Factory Reset allein reicht nicht, weil erreichbare Geräte ohne Patches erneut kompromittiert werden.

Bedeutung: Die Meldung betrifft die Energiewirtschaft nicht direkt. Sie zeigt aber, dass Angreifer gezielt veraltete Hersteller-Steuerungen mit offenem Webinterface und Herstellerfernwartung manipulieren. Dieses Muster lässt sich auf Parkregler, Fernwirktechnik und Stationsperipherie übertragen.

Empfehlung: Alle Steuerungen mit Webinterface aus dem Internet nehmen, auch die der Gebäude- und Klimatechnik in Umspannwerken und Leitstellen. Remote Access nur noch über VPN erlauben und Standardpasswörter ändern (CC4).

Quelle: <https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/> ✓ geprüft

L-09 NSA-Merkblatt: Zero Trust für kritische OT-Umgebungen

ORIENTIERUNG NSA, 08.10.

Was ist neu: Das Cybersecurity Information Sheet „Hardening Critical OT Environments with Zero Trust Principles“ begründet seine Empfehlungen mit Angriffen auf Energie- und Abwasseranlagen. Die Angreifer kamen dort über falsch konfigurierten Remote Access, Altgeräte und Standardpasswörter hinein. Das Merkblatt empfiehlt MFA, Makro- und Mikro-Segmentierung, sicheren Fernzugang und die laufende Prüfung der Machine-to-Machine-Kommunikation entlang der SANS ICS Kill Chain.

Bedeutung: Das Merkblatt richtet sich formal an das US-Verteidigungsumfeld, die Empfehlungen passen aber direkt auf Netz- und Stationsleittechnik. Es hilft, Budget für Segmentierung und Monitoring gegenüber der Geschäftsführung zu begründen, die nach § 5e EnWG persönlich haftet.

Empfehlung: Die Empfehlungen mit dem eigenen Zonenmodell nach IEC 62443 abgleichen und die Lücken als Maßnahmenliste für das nächste Quartal festhalten. Schwerpunkt ist, die Kommunikation zwischen Leitstelle, Umspannwerken und Fernwirktechnik sichtbar zu machen (CC2 Defensible Architecture, CC3 ICS Network Visibility & Monitoring).

Quelle: <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4621936/nsa-releases-zero-trust-guidance-for-protecting-operational-technology-systems/> ✓ geprüft

Fragen für das nächste Jour fixe

1. Läuft bei uns oder bei einem Dienstleister mit OT-Zugang Ivanti Connect Secure oder PAN-OS, und sind Patch und forensische Kompromittierungsprüfung seit 13.10. dokumentiert?
2. Ist die Management-Oberfläche unserer IT/OT-Firewall nur aus einem eigenen Admin-Netz erreichbar?
3. Welche Parkregler, Datenlogger und Portale unserer Wind- und PV-Parks oder unserer Betriebsführer sind aus dem Internet erreichbar, und wer betreibt sie?
4. Welche Firmware läuft auf unseren RTU500-CMUs, und bekommt sie noch Support?
5. Haben wir von unseren Leittechnik- und Gateway-Herstellern eine SBOM, und steckt darin Eclipse Milo?
6. Nutzen wir openPDC, openHistorian oder Ignition, und wer ist dafür verantwortlich?

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 16.10.2026 automatisch aufgerufen und inhaltlich geprüft.