OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 45/2026 · Strom und Energie in DACH

Zielgruppe	Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger
Berichtszeitraum	30.10.2026–06.11.2026
Version	1.0
Datum	06.11.2026
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 45 gab es in DACH keinen öffentlich bekannten Angriff auf Netzleittechnik, Schutztechnik oder Umspannwerke. Die Gefahr liegt weiter an den Rändern des Netzes. Bei Ivanti Connect Secure kamen Angreifer laut Volexity ohne Anmeldung zu Root-Rechten, und das auf vollständig gepatchten Geräten. Bei Siemens SIMATIC IoT2050 Advanced wird eine Node-RED-Lücke mit CVSS 10 ausgenutzt, VulnCheck hat den ersten Angriff am 30. Oktober beobachtet, und bei Zyxel-Switches der Serie GS1900 haben Angreifer laut BleepingComputer Konfigurationen und gehashte Root-Zugangsdaten gestohlen. Jedes dieser Geräte steht bei Stadtwerken oft genau dort, wo Fernwartung und Datenanbindung in die OT führen.

In NRW meldeten die Stadtwerke Waldbröl eine Erpressung mit gestohlenen Kundendaten, die Versorgung lief laut Geschäftsführung ohne Unterbrechung weiter. CISA veröffentlichte ein Advisory zu Subnet Solutions PowerSYSTEM Center (Sektor Energie, CVSS v4 9,4). Mehrere US-Behörden geben nach der Angriffswelle auf Kälteanlagen Härtungsregeln heraus, die sich direkt auf Fernzugänge in der Energietechnik übertragen lassen. Vorrang haben in dieser Woche CC4 (Secure Remote Access) und CC5 (Risk-Based Vulnerability Management).

GESAMTBEWERTUNG

Die Lage ist erhöht, weil mehrere Remote-Access- und Gateway-Produkte aktiv ausgenutzt werden, die in DACH oft vor der Leittechnik stehen. Vorrang haben VPN-Gateways (Ivanti), IoT2050/Node-RED und die Management-Oberflächen von Switches, danach die Prüfung von PowerSYSTEM Center.

Trends

• Angreifer suchen sich weiter Edge-Geräte wie VPN-Gateways, Switches und IoT-Gateways aus, weil diese ohne Anmeldung erreichbar sind und selten überwacht werden.

• Zero-Day-Ketten treffen auch voll gepatchte Systeme, darum zählen Erkennung und das Erneuern von Zugangsdaten so viel wie der Patch selbst.

• Bei kleinen Stadtwerken bleibt Erpressung mit Kundendaten das häufigste öffentlich bekannte Szenario, ohne Folgen für die Versorgung.

• Der Fernzugang von Dienstleistern wird nach der Kälteanlagen-Welle zum Prüfthema, auch Behörden geben dazu jetzt konkrete Härtungsregeln heraus.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Ivanti Connect Secure: zwei weitere Zero-Days, Root-Codeausführung auch auf gepatchten Geräten (CVE-2026-111357, CVE-2026-118527)	KRITISCH	Volexity, 13.10./29.10.
L-02	Subnet Solutions PowerSYSTEM Center: Rechteausweitung und SQL Injection (ICSA-26-307-01)	MITTEL	CISA, 03.11.
L-03	Zyxel GS1900: Zero-Day in Switches ausgenutzt, 996 Geräte kompromittiert (CVE-2026-107441)	MITTEL	BleepingComputer, 04.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 06.11.2026):

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	143185	DNP3: 32440, OMRON FINS: 26119, ProConOS: 16052, Siemens S7: 7764, OPC UA: 5141
Österreich	4790	HMI/VNC: 1046, DNP3: 970, Niagara Fox: 472, Siemens S7: 387, OPC UA: 158

Meldungen im Detail

L-01 Ivanti Connect Secure: zwei weitere Zero-Days, Root-Codeausführung auch auf gepatchten Geräten (CVE-2026-111357, CVE-2026-118527)

KRITISCH Volexity, 13.10./29.10.

Was ist neu: Ivanti hat zwei weitere Lücken in Connect Secure geschlossen. Laut Volexity verkettet der Threat Actor UTA0576 sie mit CVE-2026-104935 und führt so ohne Anmeldung Code mit Root-Rechten aus, auch auf vollständig gepatchten Geräten. Volexity hat die Kette ab dem 3. Oktober beobachtet, und UTA0576 hat dabei weder Malware noch Webshell abgelegt.

Bedeutung: Viele Stadtwerke und Netzbetreiber nutzen Connect Secure als VPN für Fernwartung und Bereitschaft. Weil der Angreifer laut Volexity keine Malware hinterlässt und Spuren in Debug- und Audit-Logs löscht, hat das Integrity Checker Tool von Ivanti bei dieser Angriffskette keine Veränderung erkannt. Ein Patch allein schließt also nicht aus, dass jemand schon im Netz ist.

Empfehlung: Sofort auf die im Ivanti-Advisory genannte Version aktualisieren und alle über das Gateway genutzten Zugangsdaten und Sitzungen erneuern. Zugriffe aus dem VPN-Segment in Richtung Leittechnik seit Anfang Oktober in Firewall- und Jump-Host-Logs nachprüfen (CC1).

Quelle: https://www.volexity.com/blog/2026/10/13/a-series-of-unauthenticated-events-chained-exploitation-of-ivanti-connect-secure-zero-days/ ✓ geprüft

L-02 Subnet Solutions PowerSYSTEM Center: Rechteausweitung und SQL Injection (ICSA-26-307-01)

MITTEL CISA, 03.11.

Was ist neu: Ein angemeldeter Nutzer mit wenigen Rechten kommt an Admin-Ressourcen (CVE-2026-63017) und kann über den Report-Designer eigene SQL-Befehle ausführen (CVE-2026-63774). CISA bewertet beide mit CVSS v3.1 9,0 und v4 9,4 und nennt die Sektoren Critical Manufacturing und Energy. Aus der Ferne ausnutzbar sind die Lücken laut CISA nicht, eine öffentliche Ausnutzung ist nicht bekannt.

Bedeutung: Bei PowerSYSTEM Center geht es um Rechte innerhalb eines Werkzeugs, das im Energiesektor eingesetzt wird. Wer dort schon ein schwaches Konto hat, etwa ein Dienstleister, kann Admin-Rechte erlangen. Die Version 2020 bekommt mit Update 30 nur einen Fix für CVE-2026-63017.

Empfehlung: Version prüfen und auf 2026 Update 1.1 gehen. Falls das nicht geht, den Report-Designer sperren und die Nutzeraktivität überwachen, wie es der Hersteller empfiehlt.

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-307-01 ✓ geprüft

L-03 Zyxel GS1900: Zero-Day in Switches ausgenutzt, 996 Geräte kompromittiert (CVE-2026-107441)

MITTEL BleepingComputer, 04.11.

Was ist neu: Laut BleepingComputer haben Angreifer seit etwa 17. August über eine Out-of-bounds-Write-Lücke in der Weboberfläche 996 Geräte in 48 Ländern kompromittiert. GreyNoise führt die Kampagne als Kapibala und vermutet vorsichtig einen chinesischsprachigen Threat Actor. Zyxel hat am 22. Oktober neue Firmware veröffentlicht, die Juni-Patches für CVE-2026-7273 helfen nicht.

Bedeutung: Günstige Managed Switches stehen oft in Ortsnetzstationen, Pumpwerken und kleinen Leitwarten, dort meist ohne Monitoring. Mit einer gestohlenen Konfiguration lassen sich VLANs und Segmentierung umgehen.

Empfehlung: GS1900 im Asset-Inventar suchen, Firmware vom 22.10. einspielen und die Management-Oberfläche nur aus einem Admin-Netz erreichbar machen. Danach die in der Konfiguration hinterlegten Zugangsdaten tauschen.

Quelle: https://www.bleepingcomputer.com/news/security/zyxel-fixes-zero-day-exploited-to-hack-nearly-1-000-network-switches/ ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Ivanti Connect Secure patchen, Zugangsdaten erneuern und Logs ab Oktober prüfen [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Management-Zugriff auf Switches in Stationen auf ein Admin-Segment beschränken [CC2 Defensible Architecture]	L-03	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Setzen wir oder unsere Dienstleister Ivanti Connect Secure ein, und haben wir nach dem Patch auch Zugangsdaten und Sitzungen erneuert?

2. Wo laufen bei uns Node-RED oder IoT2050-Gateways, und wer hat sie eingerichtet?

3. Welche Switches in Stationen haben eine Weboberfläche, die aus dem Büro- oder VPN-Netz erreichbar ist?

4. Wie lange würden wir bei einer Erpressung mit Kundendaten brauchen, bis Forensik, Behörden und Kundeninfo laufen?

5. Welche Dienstleister haben heute einen Fernzugang in unsere OT, und über welches Gateway läuft er?

Maßnahmen dieser Woche

1. Ivanti Connect Secure auf die Version aus dem aktuellen Advisory bringen, danach alle VPN-Zugangsdaten und Sitzungen erneuern.

2. VPN- und Jump-Host-Logs ab 1. Oktober auf ungewöhnliche Zugriffe in Richtung Leittechnik prüfen.

3. IoT2050 und Node-RED im Asset-Inventar erfassen, auf V4.3.4-1 oder neuer aktualisieren und unbekannte Flows suchen.

4. Zyxel GS1900 suchen, Firmware vom 22.10. einspielen und Management-Zugriff auf ein Admin-Netz beschränken.

5. Version von Subnet PowerSYSTEM Center prüfen und Update planen, bis dahin Report-Designer sperren.

6. Liste aller Dienstleister-Fernzugänge mit Gateway, Freigabeprozess und MFA-Status erstellen.

HINWEIS ZUR QUELLENLAGE

Für den Zeitraum habe ich keinen öffentlichen Vorfall an Netz- oder Stationsleittechnik in DACH gefunden. Ein BSI-Lagebericht 2026 und Wochenmeldungen von NCSC oder CERT.at mit Energiebezug waren ebenfalls nicht auffindbar. Waldbröl ist nur durch eine Quelle (Oberberg-Aktuell) belegt. Knapp vor dem Zeitraum lagen die Advisories zu Hitachi Energy CoreTec und TRO600 (CISA, 29.10.) und zu Sophos UTM CVE-2026-118633 (Sophos, 28.10.), sie sind deshalb nicht aufgenommen. Nicht aufgenommen, weil unbestätigt: das Bekenntnis von NoName057(16) und Z-Pentest zu den Kälteanlagen-Angriffen samt ihrer Drohung gegen Kraftwerke (cybernews nicht abrufbar, ein Forscher zweifelt laut Sekundärquelle) sowie die EU-Frist zum 1. November für Wechselrichter von Hochrisiko-Lieferanten in EU-geförderten Projekten (nur Sekundärquelle, kein Kommissionsdokument gefunden). Alle Quellenlinks wurden am 06.11.2026 automatisch aufgerufen und inhaltlich geprüft. 3 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.