

WOCHENBERICHT

OT-/Cyber-Lagebild Kommunale Versorger und KRITIS

Ausgabe KW 42/2026 · Kommunale Versorger und KRITIS in DACH

Zielgruppe	Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber
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 Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 42 stehen aktiv ausgenutzte Lücken in Edge-Geräten an der Grenze zwischen Internet, IT und OT im Vordergrund. Für Ivanti Connect Secure wird ein Zero-Day (CVE-2026-104935) seit Anfang Oktober aktiv ausgenutzt. Laut Volexity und Ivanti ist er Teil einer Kette aus drei Zero-Days, die ohne Anmeldung zu Root-Rechten und Active-Directory-Zugangsdaten führt. Die Privilege Escalation in dieser Kette ist noch nicht gepatcht. Auch die Management-Oberfläche von Palo Alto PAN-OS (CVE-2026-0322) wird angegriffen. Beide Lücken stehen seit 13. bzw. 14.10. im KEV-Katalog der CISA. Viele Stadtwerke nutzen genau diese VPN-Gateways und Firewalls für Fernwartung und Segmentierung. Ein kompromittiertes Gateway ist deshalb ein direkter Weg Richtung Leitetchnik.

In Frankreich wurden zahlreiche Kühlsteuerungen von Danfoss (AK-SM/AK-SC), Copeland xweb und Dixell xweb kompromittiert. Laut CERT-FR laufen die Angriffe wahrscheinlich noch, und das BSI hat am 13.10. dazu aufgerufen, den direkten Internetzugriff auf solche Steuerungen zu sperren. Das zeigt, wie verwundbar Gebäudeleitetchnik und Kältetechnik mit End-of-Life-Firmware im Internet sind. Bei der Leitetchnik gibt es CISA-Advisories zu Eclipse Milo (OPC UA, Sektoren Energie sowie Wasser und Abwasser) und Inductive Automation Ignition sowie ein Advisory von Rockwell zu 1732E ArmorBlock I/O. Dazu kommt eine Studie zu tausenden offen erreichbaren Systemen von Wind- und Solarparks in Europa. Ein bestätigter OT-Vorfall bei einem Versorger in DACH ist in dieser Woche nicht bekannt. Der Cybervorfall beim Baukonsortium des Fehmarnbelt-Tunnels zeigt, wie stark Angriffe auf die IT eines Dienstleisters den Betrieb eines Infrastrukturprojekts lahmlegen können.

GESAMTBEWERTUNG

Die Lage ist hoch. Zwei Lücken in VPN-Gateways und Firewalls an der IT/OT-Grenze werden aktiv ausgenutzt, und für einen Teil der Ivanti-Kette gibt es noch keinen Patch. Dazu läuft in Europa eine Kampagne gegen Gebäudeleitetchnik. Vorrang haben Patch und Kompromittierungsprüfung von Ivanti und PAN-OS sowie das Abschalten der direkten Internet-Erreichbarkeit von Steuerungen der Gebäude- und Kältetechnik.

Trends

- Angreifer nutzen gezielt VPN-Gateways und Firewalls als Initial Access, also genau die Edge-Geräte, über die Versorger Fernwartung und Segmentierung umsetzen.
- Gebäudeleitetchnik und Kältetechnik mit End-of-Life-Firmware werden in Europa im großen Stil angegriffen. Ohne Netztrennung hilft ein Factory Reset nicht.
- Lücken in Bibliotheken wie Eclipse Milo stecken unsichtbar in vielen OT-Produkten. Ohne SBOM bleibt unklar, wer betroffen ist.
- Dezentrale Erzeugung (Wind, Solar) vergrößert die Angriffsfläche der Stadtwerke, oft über Fernzugänge von Dienstleistern.
- Angriffe auf die IT von Dienstleistern und Generalunternehmern legen Infrastrukturprojekte lahm, auch wenn der Betreiber selbst nicht betroffen ist.
- Ransomware-Gruppen setzen zunehmend auf Datendiebstahl statt auf Verschlüsselung, mit Voice Phishing und MFA-Umgehung über den Helpdesk.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Ivanti Connect Secure: Zero-Day CVE-2026-104935 wird aktiv ausgenutzt, Privilege Escalation in der Angriffskette noch ohne Patch	KRITISCH	BleepingComputer / Volexity / Ivanti / Rapid7 / Canadian Centre for Cyber Security (AV26-1035) / CISA KEV, 13.10.
L-02	Palo Alto PAN-OS: ausgenutzte Lücke in der Management-Oberfläche (CVE-2026-0322)	HOCH	Palo Alto Networks Security Advisory / CISA KEV, 14.10.
L-03	Kühlsteuerungen von Danfoss, Copeland und Dixell: CERT-FR meldet zahlreiche Kompromittierungen, BSI warnt (CERTFR-2026-ALE-012)	HOCH	CERT-FR (ANSSI, CERTFR-2026-ALE-012, auch unter https://www.cert.t.ssi.gouv.fr/alerte/CERTFR-2026-ALE-012/) / BSI, 13.10.
L-04	Eclipse Milo OPC UA: sechs Lücken auf der Server-Seite, Fix nur in Version 1.1.5 (ICSA-26-288-01)	HOCH	CISA ICS Advisory, 15.10.
L-05	Inductive Automation Ignition: Privilege Escalation bis zur Codeausführung im Gateway (ICSA-26-286-01)	MITTEL	CISA ICS Advisory, 13.10.
L-06	Rockwell 1732E ArmorBlock I/O: Webserver-Passwort ohne Anmeldung änderbar (SD1801, CVE-2026-12655)	MITTEL	Rockwell Automation Trust Center / Security Advisory, 13.10.
L-07	Studie: 8.547 Steuer- und Verwaltungssysteme von Wind- und Solarparks in Europa offen im Internet	MITTEL	heise online (Studie Modat / NCSC-NL), 09.10.
L-08	Cybervorfall beim Baukonsortium des Fehmarnbelt-Tunnels (Femern Link Contractors)	ORIENTIERUNG	Ingeniøren (ing.dk) / Femern A/S, 13.10.

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, Privilege Escalation in der Angriffskette noch ohne Patch

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

Was ist neu: Ivanti und Volexity haben am 13.10. eine Kette aus drei Zero-Days gemeldet. Ohne Anmeldung führt sie zu Root-Rechten, auch auf Geräten, die vorher voll gepatcht waren. Kern ist ein Authentication Bypass (CVE-2026-104935, CVSS 8,6), mit dem sich ohne Anmeldung Befehle ausführen lassen. Der Threat Actor UTA0576 kombiniert ihn mit einer noch ungepatchten Privilege Escalation. Er setzt keine Malware und keine Webshell ein, manipuliert die Logs und stiehlt Active-Directory-Zugangsdaten. Ausgenutzt wird die Kette laut Volexity seit dem 03.10., laut Defused schon seit dem 01.10. Die CISA führt CVE-2026-104935 seit 13.10. im KEV-Katalog. Behoben ist die Lücke in 22.8R2.5, 25.1.1.2 und 25.1.3.x.

Bedeutung: Bei vielen Stadtwerken und Wasserbetrieben laufen Fernwartung und Bereitschaft über Ivanti-Gateways. Wer dort Root-Rechte und AD-Zugangsdaten bekommt, hat eine gute Ausgangslage für Lateral Movement bis in die Leittechnik. Laut Volexity umgeht der Angreifer das Integrity Checker Tool von Ivanti, Angriffe im Arbeitsspeicher werden womöglich nicht erkannt. Ein unauffälliges Prüfergebnis ist deshalb keine Entwarnung.

Empfehlung: Sofort auf 22.8R2.5, 25.1.1.2 oder 25.1.3.x aktualisieren. Die Indicators of Compromise von Volexity prüfen und Memory- und Netzwerk-Forensik machen, statt sich nur auf den Integrity Checker zu verlassen. Zugangsdaten, die auf dem Gerät gespeichert sind oder über das Gateway liefen, sowie das Dienstkonto rotieren. Bis die Privilege Escalation gepatcht ist, den OT-Fernzugang hinter dem Gateway zusätzlich über einen eigenen Jump Host mit eigener MFA absichern.

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

L-02 Palo Alto PAN-OS: ausgenutzte Lücke in der Management-Oberfläche (CVE-2026-0322)

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

Was ist neu: Mit gültigen Admin-Zugangsdaten und Zugriff auf die Management-Oberfläche lässt sich Code als root ausführen. Die Lücke hat CVSS 4.0 8,6 (8,5, wenn der Zugriff nur über einen Jump Host möglich ist). Betroffen sind PA-Series, VM-Series und Panorama mit PAN-OS 10.2 bis 12.2, nicht betroffen sind Cloud NGFW und Prisma Access. Palo Alto meldet eine „very limited exploitation“, einen Workaround gibt es nicht. Das Advisory erschien am 14.10. und wurde am 15.10. aktualisiert. Die CISA hat die Lücke am 14.10. in den KEV-Katalog aufgenommen.

Bedeutung: Bei vielen Stadtwerken trennt eine PAN-OS-Firewall die Büro-IT von der Leittechnik. Wer root auf der Firewall hat, kann Regeln ändern und die Segmentierung still aushebeln. Für den Angriff braucht man Admin-Zugangsdaten. Zusammen mit gestohlenen AD- oder VPN-Zugangsdaten, etwa aus der Ivanti-Kampagne, wird daraus ein realistischer Angriffsweg.

Empfehlung: Auf den Fix-Stand des eigenen Zweigs aktualisieren, zum Beispiel 11.2.16, 11.1.16-h3 oder 12.2.4. Die Management-Oberfläche nur aus einem getrennten Admin-Netz erreichbar machen und die Admin-Konten mit MFA absichern. Konfigurationsänderungen der letzten Wochen auf unerklärte Regeln prüfen.

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

L-03 Kühlsteuerungen von Danfoss, Copeland und Dixell: CERT-FR meldet zahlreiche Kompromittierungen, BSI warnt (CERTFR-2026-ALE-012)

HOCH CERT-FR (ANSSI, CERTFR-2026-ALE-012, auch unter <https://www.cert.ssi.gouv.fr/alerte/CERTFR-2026-ALE-012/>) / BSI, 13.10.

Was ist neu: CERT-FR hat die Warnung am 12.10. veröffentlicht und am 13.10. erweitert. Neben Danfoss AK-SC und AK-SM sind jetzt auch die xweb-Steuerungen von Copeland und Dixell betroffen. Die Angriffe laufen laut CERT-FR „wahrscheinlich noch“. Ein Factory Reset allein reicht nicht. Geräte mit End-of-Life-Firmware oder ohne Patch, die weiter im Internet erreichbar sind, werden sehr wahrscheinlich erneut kompromittiert. Wie die Angreifer hineingekommen sind, ist weiter offen. Das BSI hat am 13.10. Betreiber kleiner Anlagen aufgefordert, den direkten Internetzugriff zu sperren. Einen bestätigten Fall in Deutschland gibt es bisher nicht.

Bedeutung: Ähnliche Steuerungen stecken auch in Liegenschaften von Stadtwerken und Kommunen, in Bädern, Rechenzentren, Labors und den Kühlräumen von Kläranlagenlaboren. Oft hat ein Kälte Dienstleister sie eingerichtet und wartet sie aus der Ferne, im Asset-Inventar fehlen sie dann. Die Kampagne zeigt, dass Angreifer gezielt nach solchen Geräten im Internet suchen. CERT-FR empfiehlt ausdrücklich, auch die Abtauzeiten zu prüfen, weil die Konfiguration manipuliert sein kann.

Empfehlung: Alle Danfoss-, Copeland- und Dixell-Steuerungen ins Asset-Inventar aufnehmen. Mit einem externen Scan und über die Dienstleister klären, ob AK-SC, AK-SM oder xweb öffentlich erreichbar sind. Den Remote Access nur noch über VPN mit MFA zulassen und Dienstleister vertraglich darauf verpflichten. Standardpasswörter ändern, die Konfiguration prüfen und bei Verdacht nach dem Ablauf von CERT-FR zurücksetzen. Vor dem Trennen der Datenverbindungen zum Kälte Dienstleister die Versicherungsbedingungen beachten.

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

L-04 Eclipse Milo OPC UA: sechs Lücken auf der Server-Seite, Fix nur in Version 1.1.5 (ICSA-26-288-01)

HOCH CISA ICS Advisory, 15.10.

Was ist neu: Betroffen ist die Server-Seite der Java-Bibliothek in den Versionen 0.6.0 bis 1.1.4, mit sechs CVEs. Ein Speicherleck führt ohne Anmeldung zum Absturz (CVE-2026-63252). Wegen fehlender Autorisierung können anonyme Clients geschützte Methoden aufrufen und Knoten löschen (CVE-2026-58080, CVSS v3.1 8,2). Über ein Padding Oracle lassen sich Passwörter zurückgewinnen (CVE-2026-60007, CVSS v4 9,1). Behoben ist das nur in 1.1.5. Für den 0.6.x-Zweig gibt es keinen Patch. Die CISA nennt ausdrücklich die Sektoren Energie sowie Wasser und Abwasser.

Bedeutung: Milo steckt oft unsichtbar in Produkten anderer Hersteller, etwa in Gateways, Historians, SCADA- und Edge-Plattformen. Betreiber finden es nur über die SBOM oder eine Herstellerankunft. Zwei der Lücken lassen sich ohne Anmeldung ausnutzen und gefährden die Verfügbarkeit von Prozessdaten.

Empfehlung: Die Hersteller von SCADA, Gateways, Leittechnik und Fernwirktechnik schriftlich fragen, ob Eclipse Milo verbaut ist und wann ein Update auf 1.1.5 kommt. Bis dahin anonyme Sessions und den Security-Modus „None“ abschalten und OPC-UA-Server bzw. -Ports nur aus der eigenen Zone erreichbar machen.

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

L-05 Inductive Automation Ignition: Privilege Escalation bis zur Codeausführung im Gateway (ICSA-26-286-01)

MITTEL CISA ICS Advisory, 13.10.

Was ist neu: Das Perspective-Modul prüft die Session-Rechte nicht korrekt. Ein angemeldeter Nutzer mit Zugriff auf ein Vision-Projekt kann so Designer-Rechte erlangen und Code im Ignition-Gateway-Prozess ausführen (CVE-2026-92817, CVSS v3.1 8,8). Betroffen sind 8.1.0 bis 8.1.54 und 8.3.0 bis 8.3.8. Eine öffentliche Ausnutzung ist der CISA nicht bekannt.

Bedeutung: Ignition läuft auch bei Wasser- und Energieversorgern als SCADA- und Visualisierungsplattform. Wer ein normales Bedienerkonto übernimmt, etwa über Phishing oder geteilte Zugangsdaten, kann den Server übernehmen. Die Daten im Advisory sind nicht stimmig, denn die Revisionshistorie nennt den 13.09.2026.

Empfehlung: Ignition-Server ins Inventar aufnehmen und aktualisieren. Bis zum Update die Vision- und Perspective-Konten überprüfen und geteilte Bedienerkonten abschaffen.

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

L-06 Rockwell 1732E ArmorBlock I/O: Webserver-Passwort ohne Anmeldung änderbar (SD1801, CVE-2026-12655)

MITTEL Rockwell Automation Trust Center / Security Advisory, 13.10.

Was ist neu: Mit CVE-2026-12655 (CVSS 3.1 9,1) kann ein Angreifer ohne Anmeldung das Webserver-Passwort von 12 Modellen ändern. Bei CVE-2026-12656 (CVSS 7,5) legt Storm-Traffic die Kommunikation lahm, danach muss das Gerät aus- und wieder eingeschaltet werden. Betroffen ist Firmware bis 3.012, behoben ist beides in 3.013. Einen Workaround gibt es nicht.

Bedeutung: ArmorBlock-Module sind in Wasser- und Abwasseranlagen mit Allen-Bradley-Steuerungen verbreitet. Fällt die I/O-Kommunikation durch Netzlast aus, sind Messwerte und Ausgänge unterbrochen, bis jemand vor Ort eingreift. Das kann Prozesse stoppen. Gefährdet ist vor allem, wer flache Netze ohne Zonen betreibt.

Empfehlung: Die betroffenen Katalognummern im Asset-Inventar suchen und Firmware 3.013 im nächsten Wartungsfenster einspielen. Bis dahin die Module in eine eigene Zone legen, die aus dem Büronetz nicht erreichbar ist, und den Webserver nur aus dem Engineering-Netz zulassen. Broadcast-Stürme begrenzen und im OT-Monitoring alarmieren (CC2, CC3).

Quelle: <https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1801.html> ✓ geprüft

L-07 Studie: 8.547 Steuer- und Verwaltungssysteme von Wind- und Solarparks in Europa offen im Internet

MITTEL heise online (Studie Modat / NCSC-NL), 09.10.

Was ist neu: Laut der Studie „To see the wind and the sun“ (vorgestellt am 07.10.) sind in Deutschland 672 Solar- und 212 Windpark-Systeme aus dem Internet erreichbar. An rund 181 Standorten wären weitreichende Fernsteuerungsfunktionen zugänglich, etwa Turbinen starten, stoppen und zurücksetzen. Ein erfolgreicher Angriff ist bisher nicht belegt.

Bedeutung: Viele Stadtwerke betreiben eigene Wind- und Solarparks oder sind daran beteiligt, die Betriebsführung liegt oft bei Dienstleistern. Offen erreichbare Parkregler sind ein Risiko für die Erzeugung und für die Netzstabilität im Verteilnetz.

Empfehlung: Eigene Anlagen und die der Betriebsführer auf offen erreichbare Parkregler und Portale scannen lassen. Fernzugriff nur über VPN mit MFA zulassen und das vertraglich mit den Betriebsführern regeln.

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

L-08 Cybervorfall beim Baukonsortium des Fehmarnbelt-Tunnels (Femern Link Contractors)

ORIENTIERUNG Ingeniøren (ing.dk) / Femern A/S, 13.10.

Was ist neu: Femern A/S hat am 13.10. bestätigt, dass FLC von einem Cybervorfall betroffen ist. FLC ist ein Konsortium aus acht Firmen aus fünf Ländern. Welche Systeme betroffen sind, ob Ransomware im Spiel war und wer dahintersteckt, ist offiziell nicht bekannt. Laut Presse fielen WLAN, Rechner, E-Mail und Zutrittskarten aus, und Schiffe standen still. Diese Angaben sind nicht amtlich bestätigt.

Bedeutung: Der Fall zeigt, wie ein Angriff auf die IT eines Generalunternehmers ein Infrastrukturprojekt ausbremst, auch wenn der Bauherr selbst nicht betroffen ist. Stadtwerke haben dasselbe Risiko bei Netzbau-Dienstleistern, Betriebsführern und Wartungsfirmen.

Empfehlung: Den Ausfall eines wichtigen Dienstleisters als Szenario in die Incident-Response-Planung aufnehmen und üben. Dazu gehört die Frage, wie dessen Fernzugänge im Ernstfall sofort gesperrt werden.

Quelle: <https://ing.dk/artikel/femern-projektet-ramt-af-hackerangreb> ✓ geprüft

Fragen für das nächste Jour fixe

1. Haben wir Ivanti Connect Secure oder PAN-OS im Einsatz, und sind Patch und Kompromittierungsprüfung nachweislich erledigt?
2. Welche Hersteller-Steuerungen in Gebäudeleittechnik und Kältetechnik sind direkt aus dem Internet erreichbar, und wer hat dort Fernwartungszugang?
3. Welche unserer SCADA-, Gateway- und Leittechnik-Hersteller haben bestätigt, ob Eclipse Milo in ihren Produkten steckt?
4. Laufen bei uns Ignition-Server, und gibt es geteilte Bedienerkonten?
5. Wie setzt unser Helpdesk MFA zurück, und ist dieser Ablauf gegen Voice Phishing abgesichert?
6. Würde unser OT-Monitoring eine geänderte Firewall-Regel oder einen Broadcast-Sturm in der Feldebene erkennen und melden?

7. Wie sperren wir die Fernzugänge eines wichtigen Dienstleisters sofort, wenn er selbst angegriffen wird?

Maßnahmen dieser Woche

1. Ivanti Connect Secure auf 22.8R2.5, 25.1.1.2 oder 25.1.3.x aktualisieren, die Volexity-IoCs prüfen, Memory- und Netzwerk-Forensik machen und die über das Gateway genutzten Zugangsdaten zurücksetzen.
2. PAN-OS auf den Fix-Stand des eigenen Zweigs patchen und die Management-Oberfläche aller Firewalls auf ein getrenntes Admin-Netz mit MFA beschränken.
3. Extern scannen (lassen), ob Danfoss AK-SM/AK-SC, Copeland xweb, Dixell xweb, Parkregler oder andere OT-Geräte aus dem Internet erreichbar sind, und Funde sofort hinter ein VPN legen.
4. Bei allen OT-Herstellern eine SBOM-Auskunft zu Eclipse Milo anfordern und anonyme OPC-UA-Sessions abschalten.
5. Ignition auf 8.1.55 bzw. 8.3.9 aktualisieren und geteilte Bedienerkonten abschaffen.
6. Rockwell ArmorBlock I/O im Asset-Inventar suchen, Firmware 3.013 für das nächste Wartungsfenster einplanen und die Geräte vom Büronetz trennen.
7. Den Incident-Response-Plan um die Szenarien „kompromittiertes VPN-Gateway“ und „Ausfall eines wichtigen Dienstleisters“ ergänzen. Darin klar festlegen, wann der Fernzugang zur Leittechnik getrennt wird.

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 16.10.2026 automatisch aufgerufen und inhaltlich geprüft.