OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Kommunale Versorger und KRITIS

Ausgabe KW 45/2026 · Kommunale Versorger und KRITIS in DACH

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

Management Summary

In KW 45 zeigte sich in Deutschland, wie gefährlich der Fernwartungszugang eines Dienstleisters ist. Laut dpa fielen in Märkten in Wuppertal, Wetter bei Hagen, Niederbayern, dem Münsterland und der Westpfalz die Kühlanlagen aus, vermutlich durch einen Hack. In Wetter-Volmarstein heißt es, der Angriff habe der Firma gegolten, die die Anlagen aus der Ferne wartet. Das BSI kennt einzelne Vorfälle bei Supermärkten und in der Pharmabranche. Es beschreibt die Angreifer als opportunistisch: Sie suchen nach verwundbaren Systemen, ohne vorher eine Branche auszuwählen. Davon sind auch Gebäudeleittechnik und Kältetechnik bei Stadtwerken und Wasserversorgern betroffen.

In der Woche wurden mehrere Schwachstellen in Edge-Geräten aktiv ausgenutzt: Ivanti Connect Secure (zwei CVEs im KEV-Katalog der CISA seit 30.10.), Siemens SIMATIC IoT2050 Advanced mit Node-RED (CVE-2026-58115, CVSS 10, erster Angriff laut VulnCheck am 30.10.) und Zyxel-Switches GS1900 (996 Geräte kompromittiert). Die Stadtwerke Waldbröl wurden laut Geschäftsführung über gestohlene Kundendaten erpresst, die Versorgung lief ohne Unterbrechung weiter (Oberberg-Aktuell, 30.10.).

GESAMTBEWERTUNG

Die Lage ist erhöht, aber nicht kritisch: In DACH ist kein Eingriff in die Leittechnik eines Versorgers belegt, wohl aber in Kältetechnik über die Fernwartung. Zuerst kommen die Fernzugänge von Dienstleistern und die aus dem Internet erreichbaren Edge-Geräte (Ivanti, IoT2050/Node-RED, Sophos UTM, Zyxel) an die Reihe.

Trends

• Angreifer gehen über Fernwartungsdienstleister: Ein kompromittierter Dienstleister öffnet den Weg zu allen seinen Kunden.

• Edge-Geräte (VPN, Gateways, Switches, Firewalls) sind diese Woche der häufigste Angriffsweg, teils mit Zero-Days und monatelanger unbemerkter Ausnutzung.

• Laut BSI wird opportunistisch gescannt: Wer erreichbar und verwundbar ist, wird getroffen, egal in welcher Branche.

• Ransomware-Gruppen erpressen Stadtwerke mit Kundendaten, die Leittechnik bleibt dabei bisher meist unberührt.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Kühlanlagen in deutschen Märkten gehackt, Angriff lief offenbar über den Fernwartungsdienstleister	HOCH	Handelsblatt (dpa), 03.11.
L-02	Siemens SIMATIC IoT2050 Advanced: Node-RED-Lücke CVE-2026-58115 (CVSS 10) wird ausgenutzt (erster Angriff laut VulnCheck am 30.10.)	KRITISCH	VulnCheck, 02.11.
L-03	Ivanti Connect Secure: zwei ausgenutzte Lücken im KEV-Katalog der CISA (30.10.)	HOCH	CISA, 30.10.

ID	Meldung	Relevanz	Quelle
L-04	Stadtwerke Waldbröl (NRW) erpresst, Kundendaten abgeflossen	HOCH	Oberberg-Aktuell, 30.10.
L-05	BSI: Kühlsystem-Angriffe auch in der Pharmabranche, Angreifer gehen opportunistisch vor	MITTEL	CORRECTIV, 05.11.
L-06	Zyxel GS1900: Zero-Day CVE-2026-107441, 996 Switches in 48 Ländern kompromittiert	HOCH	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 Kühlanlagen in deutschen Märkten gehackt, Angriff lief offenbar über den Fernwartungsdienstleister

HOCH Handelsblatt (dpa), 03.11.

Was ist neu: Laut dpa fielen in Wuppertal, Wetter bei Hagen, Niederbayern, dem Münsterland und der Westpfalz Kühlanlagen aus, vermutlich durch einen Hack. Im Markt in Wetter-Volmarstein hieß es, der eigentliche Angriff habe der Firma gegolten, die die Kühlanlagen aus der Ferne wartet. Wer dahintersteckt, ist laut Artikel unklar.

Bedeutung: Stadtwerke, Wasserversorger und Bäder lassen Kälte-, Lüftungs- und Gebäudeleittechnik oft von Dienstleistern fernwarten. Wird so ein Dienstleister kompromittiert, kommen die Angreifer bei allen seinen Kunden an, auch wenn diese selbst gut aufgestellt sind.

Empfehlung: Liste aller Fernwartungszugänge von Dienstleistern anlegen, Dauerverbindungen trennen und den Zugang nur noch über ein eigenes Gateway mit MFA und Freischaltung pro Einsatz erlauben (CC4).

Quelle: https://www.handelsblatt.com/politik/deutschland/hacker-attacke-cyberangriffe-auch-auf-kuehlanlagen-deutscher-supermaerkte/100266999.html ✓ geprüft

L-02 Siemens SIMATIC IoT2050 Advanced: Node-RED-Lücke CVE-2026-58115 (CVSS 10) wird ausgenutzt (erster Angriff laut VulnCheck am 30.10.)

KRITISCH VulnCheck, 02.11.

Was ist neu: Laut VulnCheck wurde die fehlende Authentifizierung an der Node-RED-HTTP-Schnittstelle am 30. Oktober erstmals ausgenutzt, bis 1. November zählte VulnCheck auf seinen Honeypots insgesamt 16 Angriffsversuche von derselben IP. Zuerst wurde ein Linux-Bot nachgeladen, später eine Backdoor über einen Node-RED-Flow, die einen Neustart übersteht. Siemens behebt die Lücke mit V4.3.4-1 (SSA-834709).

Bedeutung: IoT2050-Gateways mit Node-RED binden in Wasser-, Abwasser- und Energieanlagen häufig Messdaten an oder werden für die Fernwartung genutzt. Eine Backdoor auf so einem Gateway ist ein direkter Brückenkopf ins OT-Netz.

Empfehlung: Alle IoT2050 im Asset-Inventar suchen, auf V4.3.4-1 oder neuer bringen und Node-RED nur intern mit aktivierter Anmeldung betreiben. Bei Geräten, die von außen erreichbar waren, nach unbekannten Flows und Webshells suchen und die Geräte im Zweifel neu aufsetzen (CC5, CC3).

Quelle: https://www.vulncheck.com/blog/exploitation-targeting-node-red ✓ geprüft

L-03 Ivanti Connect Secure: zwei ausgenutzte Lücken im KEV-Katalog der CISA (30.10.)

HOCH CISA, 30.10.

Was ist neu: Die CISA hat CVE-2026-111357 (Missing Authentication for Critical Function) und CVE-2026-118527 (Generation of Predictable Numbers or Identifiers) für Ivanti Connect Secure in den KEV-Katalog aufgenommen. Der Eintrag heißt: Beide Lücken werden aktiv ausgenutzt.

Bedeutung: Viele Stadtwerke nutzen Ivanti Connect Secure als VPN für Mitarbeiter und Dienstleister. Wer die Anmeldung umgehen kann, steht direkt im internen Netz und oft auch vor dem Jump Host zur Leittechnik.

Empfehlung: Ivanti-Fixes einspielen und mit dem Integrity Checker prüfen. Bei Verdacht die Zugangsdaten aller VPN- und Domänenkonten zurücksetzen, denn ein Patch macht gestohlene Daten nicht ungültig (CC4, CC1).

Quelle: https://www.cisa.gov/news-events/alerts/2026/10/30/cisa-adds-two-known-exploited-vulnerabilities-catalog ✓ geprüft

L-04 Stadtwerke Waldbröl (NRW) erpresst, Kundendaten abgeflossen

HOCH Oberberg-Aktuell, 30.10.

Was ist neu: Laut Geschäftsführer Mirco Kujbida wurden die Stadtwerke vor rund drei Wochen von einer finanziell motivierten, russischen Hackerbande erpresst. Forensiker haben den Diebstahl von Kundendaten bestätigt, das LKA ermittelt. Die Versorgung war laut Kujbida zu keinem Zeitpunkt unterbrochen oder gefährdet.

Bedeutung: Der Fall folgt dem bekannten Muster bei Stadtwerken: Angegriffen wird die IT, erpresst wird mit Kundendaten, und die Leittechnik bleibt unberührt. Einfallstor und Name der Gruppe sind nicht bekannt.

Empfehlung: Im Incident-Response-Plan den Fall „Erpressung mit Kundendaten“ durchspielen, mit Meldewegen (BSI, Datenschutzbehörde, LKA) und Kundeninformation (CC1).

Quelle: https://www.oberberg-aktuell.de/blaulicht/stadtwerke-wurden-von-russischer-hackerbande-erpresst-a-139763 ✓ geprüft

L-05 BSI: Kühlsystem-Angriffe auch in der Pharmabranche, Angreifer gehen opportunistisch vor

MITTEL CORRECTIV, 05.11.

Was ist neu: Laut CORRECTIV wurde die Medikamentenkühlung eines Pharmahändlers in Deutschland angegriffen. Ein BSI-Sprecher bestätigte einzelne Vorfälle bei Supermärkten und in der Pharmabranche. Laut BSI gehen die Angreifer ungezielt und opportunistisch vor, oft ohne zu wissen, welche Firma sie treffen. Für die Bekenntnisse prorussischer Telegram-Kanäle liegen laut einem BSI-Sprecher gegenüber CORRECTIV keine Belege vor.

Bedeutung: Wenn die Angreifer wahllos scannen, ist die Branche egal: Jede Steuerung, die aus dem Internet erreichbar ist, wird zum Ziel. Das gilt auch für Gebäudeleittechnik in Wasserwerken, Bädern und Verwaltungsgebäuden.

Empfehlung: Die eigenen IP-Bereiche von außen scannen (lassen) und dabei nach erreichbaren HMI-, GLT- und Kälteoberflächen suchen. Was nicht über ein abgesichertes Gateway erreichbar ist, kommt vom Netz (CC2).

Quelle: https://correctiv.org/aktuelles/infrastruktur/2026/11/05/hackerangriffe-auf-kuehlsysteme-auch-pharmahaendler-in-deutschland-betroffen/ ✓ geprüft

L-06 Zyxel GS1900: Zero-Day CVE-2026-107441, 996 Switches in 48 Ländern kompromittiert

HOCH BleepingComputer, 04.11.

Was ist neu: Angreifer nutzten seit etwa 17. August einen Out-of-bounds Write im Web-Management der GS1900 aus und kompromittierten laut GreyNoise 996 Geräte in 48 Ländern. Fixes gibt es seit 22. Oktober, das Advisory folgte am 3. November. Die Juni-Updates für CVE-2026-7273 schützen nicht.

Bedeutung: GS1900 sind günstige Switches, die auch in Außenstationen und kleinen Leitwarten stehen. Gestohlene Konfigurationen und Zugangsdaten erleichtern Lateral Movement.

Empfehlung: GS1900 im Asset-Inventar suchen, die Firmware vom 22.10. einspielen, die Management-Oberfläche nur aus dem Verwaltungsnetz erreichbar machen und gespeicherte Zugangsdaten ändern (CC5).

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	Fernwartung von Dienstleistern nur noch über ein eigenes Gateway mit MFA und Freischaltung pro Einsatz erlauben [CC4 Secure Remote Access]	L-01	HOCH	0 bis 3 Monate
M-02	Ausgenutzte Edge-Geräte (Ivanti, IoT2050/Node-RED, Zyxel GS1900) sofort patchen und auf Kompromittierung prüfen [CC5 Risk-Based Vulnerability Management]	L-02	HOCH	sofort
M-03	Externe Erreichbarkeit von Steuerungen und Gebäudeleittechnik regelmäßig scannen und alles Erreichbare hinter ein Gateway legen [CC2 Defensible Architecture]	L-05	HOCH	sofort
M-04	Szenario „Erpressung mit Kundendaten“ in einer Incident-Response-Übung durchspielen [CC1 ICS Incident Response]	L-04	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Welche Dienstleister haben heute Fernzugang zu unserer Gebäude-, Kälte- oder Leittechnik, und wie ist der Zugang abgesichert?

2. Laufen bei uns Ivanti Connect Secure, Sophos UTM, Siemens IoT2050 oder Zyxel GS1900, und auf welchem Patchstand?

3. Welche unserer Steuerungen sind von außen erreichbar, und wann haben wir das zuletzt selbst gescannt?

4. Ist der Fall „Erpressung mit Kundendaten“ in unserem Incident-Response-Plan geübt, mit Meldewegen und Kundeninformation?

Maßnahmen dieser Woche

1. Ivanti Connect Secure patchen, Integrity Check laufen lassen und VPN-Zugangsdaten bei Verdacht zurücksetzen.

2. Alle Siemens IoT2050 auf V4.3.4-1 bringen und Node-RED nur intern mit aktivierter Anmeldung betreiben, erreichbare Geräte auf unbekannte Flows prüfen.

3. Liste der Fernwartungszugänge von Dienstleistern erstellen und Dauerverbindungen trennen.

4. Eigene öffentliche IP-Bereiche nach erreichbaren HMI-, GLT- und Kälteoberflächen scannen.

5. Zyxel GS1900 auf die Firmware vom 22.10. bringen und Sophos UTM manuell patchen oder den E-Mail-Proxy abschalten.

HINWEIS ZUR QUELLENLAGE

Für alle sechs Meldungen habe ich die Quelle selbst geöffnet und den Beleg geprüft. Das Waldbröl-Material stammt nur aus Oberberg-Aktuell, eine zweite Quelle habe ich nicht gefunden. Nicht aufgenommen, weil unbestätigt oder ohne geprüfte Primärquelle: WABAG als Opfer von „The Gentlemen“ (nur Leak-Site-Tracker, keine Bestätigung von WABAG), die Volexity-Analyse zu Angriffen auf gepatchte Ivanti-Geräte seit 03.10. (Volexity, 13.10., vor dem Zeitraum; steht im Branchenbericht Strom) sowie der Einbruch ins METI-Meldeportal in Japan (Primärquelle nicht abrufbar). Außerdem: CISA ICSA-26-307-01 (Subnet PowerSYSTEM Center, 03.11.) und CERT@VDE VDE-2026-121 (Phoenix Contact PLCnext Engineer bis 2026.6, 04.11.) sind geprüft, aber ohne bekannte Ausnutzung; sie fehlen hier nur, weil die Liste auf sieben Meldungen begrenzt ist. Für Österreich und die Schweiz habe ich im Zeitraum keinen belegten Vorfall bei Versorgern gefunden. Alle Quellenlinks wurden am 06.11.2026 automatisch aufgerufen und inhaltlich geprüft. 1 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.