OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Kommunale Versorger und KRITIS

Ausgabe KW 44/2026 · Kommunale Versorger und KRITIS in DACH

Zielgruppe	Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber
Berichtszeitraum	23.10.2026–30.10.2026
Version	1.0
Datum	30.10.2026
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 44 sind die Edge-Geräte vor dem Leitstellennetz das größte Risiko. Die PHP-Lücken „PHP2Shell“ (CVE-2026-109618/-109619) stehen seit dem 26.10. im KEV-Katalog der CISA. Palo Alto meldet inzwischen aktive Angriffe auf erreichbare PAN-OS-Management-Interfaces und hat bis zum 29.10. Hotfixes für alle Zweige veröffentlicht. Am 28.10. kam ein ausgenutzter Zero-Day in Cisco Secure Firewall ASA/FTD hinzu (CVE-2026-76418), mit dem Angreifer SSL-VPN-Gateways neu starten lassen. Das trifft genau die Geräte, über die Bereitschaft und Fernwartung bei vielen Stadtwerken laufen. Für Siemens S7-1500 und ET 200SP gibt es acht Webserver-Lücken ohne Patch, für ICONICS/MC Works64-Altsysteme wird es nie einen Patch geben.

Bloomberg hat am 27.10. zusammengetragen, wie die russlandnahen Gruppen CARR und Z-Pentest über schlecht gesicherte Steuerungen echten Schaden angerichtet haben. In Dänemark platzten Leitungen und 450 Haushalte hatten kein Wasser, in den USA wurden Trink- und Abwasseranlagen manipuliert. DACH wird im Bericht nicht genannt. Die Methode ist aber banal und überall anwendbar: erreichbare Oberflächen und schwache Passwörter. Für die Daseinsvorsorge in DACH ist in dieser Woche kein neuer, bestätigter Vorfall belegt. Mit Veeam (CVE-2026-108142) wird aber erneut die Backup-Ebene angegriffen, auf die Ransomware-Gruppen vor der Verschlüsselung zielen.

GESAMTBEWERTUNG

Die Lage ist hoch, weil gleich zwei Familien von Remote-Access- und Firewall-Lücken (PHP2Shell bei Palo Alto, Cisco ASA/FTD) aktiv ausgenutzt werden und ein Großteil der Fernwartung in DACH über solche Geräte läuft. Vorrang haben Patchen und Abschotten der Management-Interfaces und VPN-Gateways, danach Steuerungs-Webserver und Backup-Server.

Trends

• Firewalls und VPN-Gateways sind wieder der bevorzugte Einstieg: Mit PHP2Shell, Cisco ASA und den Fortinet-Notfall-Updates waren in einer Woche drei große Hersteller betroffen.

• Lücken in Bibliotheken wie PHP landen über Monate in OT-Edge-Geräten (RUGGEDCOM APE1808, Cisco URWB), deren Patches deutlich später kommen als die der IT-Hersteller.

• Hacktivisten mit Nähe zum russischen Staat verursachen inzwischen über offene HMIs physische Schäden an Wasseranlagen, der Weg dorthin bleibt technisch simpel.

• Ransomware-Leak-Sites führen jede Woche europäische Energiehändler und Engineering-Dienstleister, Bestätigungen der Betroffenen fehlen fast immer.

• Hersteller kündigen für Altprodukte offen keinen Fix mehr an (ICONICS MC Works64, GENESIS32), das Risiko bleibt dann beim Betreiber.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	PHP2Shell: aktiv ausgenutzt, im KEV-Katalog, Palo-Alto-Hotfixes jetzt komplett (CVE-2026-109618/-109619)	KRITISCH	CISA, Palo Alto Networks PSIRT, Siemens ProductCERT, 26.10.

ID	Meldung	Relevanz	Quelle
L-02	Cisco Secure Firewall ASA/FTD: Zero-Day lässt SSL-VPN-Gateways abstürzen (CVE-2026-76418, CVSS 8,6)	HOCH	Cisco PSIRT, 28.10.
L-03	Bloomberg: russlandnahe Gruppen CARR und Z-Pentest verursachen physische Schäden an Wasser- und Industrieanlagen	HOCH	Bloomberg (über Meduza), 27.10.
L-04	Siemens SIMATIC S7-1500 und ET 200SP: acht Webserver-Lücken, 157 Produkte, kein Patch (ICSA-26-295-14)	HOCH	CISA / Siemens ProductCERT, 22.10.
L-05	Veeam Backup & Replication 13: Autorisierung ohne Anmeldung umgehbar (CVE-2026-108142, CVSS v4 9,1)	HOCH	Veeam KB4948, 27.10.
L-06	Mitsubishi Electric ICONICS GENESIS64 und MC Works64: Umgehung der Anmeldung, für Altprodukte kein Fix (ICSA-26-300-02)	MITTEL	CISA, 27.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 30.10.2026):

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	148182	DNP3: 34267, OMRON FINS: 26328, ProConOS: 17131, Siemens S7: 7931, OPC UA: 5265
Österreich	4928	HMI/VNC: 1088, DNP3: 1006, Niagara Fox: 482, Siemens S7: 386, OPC UA: 161

Meldungen im Detail

L-01 PHP2Shell: aktiv ausgenutzt, im KEV-Katalog, Palo-Alto-Hotfixes jetzt komplett (CVE-2026-109618/-109619)

KRITISCH CISA, Palo Alto Networks PSIRT, Siemens ProductCERT, 26.10.

Was ist neu: Am 26.10. hat die CISA beide PHP-Lücken in den KEV-Katalog aufgenommen. Palo Alto führt CVE-2026-109618 seit dem letzten Update am 29.10. als „ATTACKED“: Angegriffen werden Management-Web-UI und XML-API, wenn sie aus dem Internet erreichbar sind. Laut Timeline gibt es Hotfixes für alle Zweige von 10.2 bis 12.2, die letzten kamen am 29.10.

Bedeutung: PAN-OS läuft auch auf Siemens RUGGEDCOM APE1808, der NGFW für Umspannwerke und Fernwirktechnik. Siemens nennt laut SSA-566512 bisher keinen eigenen Fix, sondern verweist auf den Support. Ein übernommenes Management-Interface öffnet den Weg ins OT-Netz.

Empfehlung: Alle PA-Series-, VM-Series- und Panorama-Instanzen auf die Hotfix-Versionen bringen und den Management-Zugang nur über einen Jump Host aus dem internen Netz erlauben. Bei APE1808 Siemens-Support anfragen und die Workarounds von Palo Alto umsetzen. Logs ab dem 20.10. auf Zugriffe von außen prüfen.

Quelle: https://security.paloaltonetworks.com/CVE-2026-109618 ✓ geprüft

L-02 Cisco Secure Firewall ASA/FTD: Zero-Day lässt SSL-VPN-Gateways abstürzen (CVE-2026-76418, CVSS 8,6)

HOCH Cisco PSIRT, 28.10.

Was ist neu: Ohne Anmeldung kann ein Angreifer ASA- und FTD-Geräte mit SSL-VPN neu starten lassen. Betroffen sind nur Konfigurationen mit „secondary-authentication-server-group“ in einer Tunnel-Group, auch in der DefaultWEBVPNGroup. Cisco bestätigt aktive Ausnutzung, einen Workaround gibt es nicht, nur eine Mitigation mit geringerem Schutz.

Bedeutung: Wenn das VPN-Gateway im Störfall wiederholt neu startet, kommt die Bereitschaft nicht an Pumpwerke und Stationen. Ein reiner DoS greift keine Daten ab, er kann aber genau dann treffen, wenn Remote Access am dringendsten gebraucht wird.

Empfehlung: Prüfen, ob in irgendeiner Tunnel-Group eine sekundäre Authentifizierung eingerichtet ist, und auf ASA 9.16.4.104, 9.18.4.96, 9.20.4.50, 9.22.3.200, 9.23.1.48, 9.24.1.27 bzw. FTD 7.0.11 bis 10.1.1 aktualisieren. Einen zweiten, unabhängigen Notfallzugang für die Bereitschaft dokumentieren und testen.

Quelle: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75 ✓ geprüft

L-03 Bloomberg: russlandnahe Gruppen CARR und Z-Pentest verursachen physische Schäden an Wasser- und Industrieanlagen

HOCH Bloomberg (über Meduza), 27.10.

Was ist neu: Bloomberg hat Fälle aus mehreren NATO-Staaten zusammengetragen. In Tureby (Dänemark) wurde im Dezember 2024 der Druck auf null gestellt, 450 Haushalte waren ohne Wasser, am Tag danach platzten Leitungen; das Passwort war laut Betreiber „1234“. In den USA wurden ein Trinkwassersystem in Texas und die Desinfektion einer Abwasseranlage in Pennsylvania manipuliert.

Bedeutung: Die Gruppen brauchen keine Exploits, ihnen reichen offene Oberflächen und Standardpasswörter. Kleine Wasserversorger und Zweckverbände mit Fernzugriff des Integrators sind genau das Ziel. DACH wird im Bericht nicht genannt, die CISA weist außerdem darauf hin, dass die Gruppen ihre Wirkung oft übertreiben.

Empfehlung: Eigene Adressbereiche bei einem externen Scan (Shodan, Censys) auf HMI-, VNC- und Webzugänge prüfen und alles abschalten oder hinter VPN mit MFA legen. Standardpasswörter auf allen Panels tauschen und Sollwertgrenzen in der Steuerung hart begrenzen.

Quelle: https://meduza.io/en/feature/2026/10/28/russia-linked-hackers-are-exploiting-poorly-secured-industrial-systems-to-sabotage-factories-utilities-and-food-production-across-the-west-bloomberg-reports ✓ geprüft

L-04 Siemens SIMATIC S7-1500 und ET 200SP: acht Webserver-Lücken, 157 Produkte, kein Patch (ICSA-26-295-14)

HOCH CISA / Siemens ProductCERT, 22.10.

Was ist neu: Die CVE-2026-63350 bis -63357 betreffen alle Versionen von S7-1500, ET 200SP, Drive Controller, Software Controller, PLCSIM Advanced und SIPLUS, mit CVSS v3 bis 9,6. Ein Angreifer bringt einen Nutzer mit dem Recht „Read diagnostics“ dazu, eine präparierte Trace-Datei zu importieren. Siemens bereitet Fixes vor, liefert aber noch keinen. Das Advisory kam einen Tag vor Beginn des Berichtszeitraums.

Bedeutung: S7-1500 und ET 200SP stehen in vielen Wasser- und Abwasseranlagen. Den Webserver nutzen Instandhaltung und Integratoren gern zur Diagnose, oft auch von außen.

Empfehlung: Im Asset-Inventar alle betroffenen CPUs mit aktivem Webserver markieren, den Webserver wo möglich abschalten und Port 80/443 nur aus dem Engineering-Netz erlauben. Trace-Dateien nur aus eigenen Quellen importieren und Dienstleister darüber informieren.

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-14 ✓ geprüft

L-05 Veeam Backup & Replication 13: Autorisierung ohne Anmeldung umgehbar (CVE-2026-108142, CVSS v4 9,1)

HOCH Veeam KB4948, 27.10.

Was ist neu: Ohne Anmeldung lässt sich die Autorisierung am CDP Coordinator Service umgehen. Betroffen sind Windows-Server und Software Appliance bis 13.1.1.18 bzw. 13.0.2.29, Version 12.x ist nicht betroffen. Dazu kommen zwei Path-Traversal-Lücken (CVSS 5,9) und eine Rechteausweitung im Veeam Agent for Linux (CVSS 7,3).

Bedeutung: Ransomware-Gruppen schalten vor der Verschlüsselung gezielt die Backups aus, laut CISA (AA26-293A) nutzt SafePay dafür Veeam-Lücken. Wer die Leittechnik-Server mit Veeam sichert, verliert sonst im Ernstfall den Wiederanlauf.

Empfehlung: Version 13 auf die Fix-Builds bringen, den Backup-Server aus der Domäne nehmen und eine Kopie offline oder unveränderbar (immutable) halten. Einen Wiederanlauf von HMI- und SCADA-Servern aus dem Backup einmal real üben.

Quelle: https://www.veeam.com/kb4948 ✓ geprüft

L-06 Mitsubishi Electric ICONICS GENESIS64 und MC Works64: Umgehung der Anmeldung, für Altprodukte kein Fix (ICSA-26-300-02)

MITTEL CISA, 27.10.

Was ist neu: Die Passwort-Wiederherstellung nutzt eine feste Challenge-Response, damit lässt sich das System entsperren (CVE-2026-16436, CVSS v4 9,2). Fixes gibt es mit GENESIS 11.04 und GENESIS64/Hyper Historian/AnalytiX/MobileHMI/IoTWorX 10.98. Für MC Works64, GENESIS32 und BizViz plant Mitsubishi keinen Fix.

Bedeutung: Wo GENESIS64 oder MC Works64 als Leitsystem oder Historian läuft, kann ein Angreifer im Netz die Anmeldung umgehen. Altinstallationen ohne Fix bleiben dauerhaft verwundbar, bis sie ersetzt sind.

Empfehlung: Falls im Einsatz: Version im Asset-Inventar erfassen, aktualisieren oder bei Altprodukten die Challenge-Datei ersetzen und ihre Schreibrechte einschränken, wie CISA beschreibt. Diese Systeme vom Remote Access trennen und den Umstieg einplanen.

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-02 ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Management-Interfaces aller Firewalls und Gateways vom Internet nehmen und nur über Jump Host mit MFA erreichbar machen [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Cisco ASA/FTD patchen und einen zweiten, unabhängigen Notfallzugang für die Bereitschaft einrichten und testen [CC4 Secure Remote Access]	L-02	HOCH	sofort
M-03	Monatlicher externer Scan auf offene HMIs und Steuerungs-Webserver, Standardpasswörter tauschen, Sollwertgrenzen in der SPS hart setzen [CC2 Defensible Architecture]	L-03	HOCH	0 bis 3 Monate

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-04	Asset-Inventar um Firmware-Stand, aktive Webserver und Hersteller-Support-Ende ergänzen, Altsysteme ohne Fix (MC Works64, GENESIS32) für Ersatz einplanen [CC5 Risk-Based Vulnerability Management]	L-04	MITTEL	3 bis 6 Monate
M-05	Wiederanlauf von HMI- und SCADA-Servern aus unveränderbarem Backup im Incident-Response-Plan festlegen und einmal üben [CC1 ICS Incident Response]	L-05	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Ist das Management-Interface jeder Firewall vor der Leittechnik aus dem Internet erreichbar, und wer hat das zuletzt nachgeprüft?

2. Läuft unsere Fernwartung über eine Cisco ASA/FTD mit sekundärer Authentifizierung, und welchen Notfallzugang hat die Bereitschaft, wenn das Gateway ausfällt?

3. Bei welchen S7-1500- oder ET-200SP-CPUs ist der Webserver aktiv, und braucht ihn wirklich jemand?

4. Wann haben wir zuletzt einen HMI- oder SCADA-Server aus dem Backup wiederhergestellt, und ist eine Kopie offline?

5. Welche OT-Dokumentation (Netzpläne, Geräteinventare, Firmware-Stände) liegt bei Dienstleistern, und wie ist sie dort geschützt?

Maßnahmen dieser Woche

1. PAN-OS und Panorama auf die PHP2Shell-Hotfixes bringen, Management nur noch über Jump Host, Logs ab 20.10. auswerten.

2. Cisco ASA/FTD auf die Fix-Versionen zu CVE-2026-76418 aktualisieren, vorher Tunnel-Groups auf sekundäre Authentifizierung prüfen.

3. Externen Scan der eigenen IP-Bereiche nach HMI-, VNC- und SPS-Webzugängen durchführen und Treffer sofort schließen.

4. Webserver auf S7-1500 und ET 200SP abschalten oder per Firewall auf das Engineering-Netz begrenzen.

5. Veeam Backup & Replication 13 auf 13.1.2.57 bzw. 13.0.3.63 aktualisieren und eine Offline-Kopie der Leittechnik-Sicherungen prüfen.

6. Bei Integratoren mit Fernzugriff abfragen, welche Remote-Access-Werkzeuge sie nutzen und ob sie gepatcht sind.

HINWEIS ZUR QUELLENLAGE

Gut belegt durch Primärquellen sind PHP2Shell (CISA KEV, Palo Alto PSIRT mit Stand 29.10., Siemens SSA-566512), Cisco ASA/FTD, die Siemens- und Mitsubishi-Advisories, Veeam KB4948 und der Bloomberg-Bericht vom 27.10. (Original hinter Paywall, geprüft über Meduza). Nicht aufgenommen, weil unbestätigt oder nur aus einer Quelle: die Leak-Site-Einträge zu Frommann Energie (Emperador), Ingelectus (N0n), Tema Energy und Hauhinco, für die keine Bestätigung der Betroffenen vorliegt. Das WatchGuard-Paket mit 18 Fireware-Lücken (laut Briefing CERT-Bund WID-SEC-2026-4209) ließ sich nur über eine Sekundärquelle mit abweichenden Zahlen prüfen (https://dailysecurityreview.com/?p=45071) und gehört vor dem Patchen ins WatchGuard PSIRT. Ein bestätigter Cyberangriff auf ein Stadtwerk in DACH im Berichtszeitraum ist nicht belegt: Der Treffer Langenfeld 22./23.10. stammt aus dem Jahr 2019. Alle Quellenlinks wurden am 30.10.2026 automatisch aufgerufen und inhaltlich geprüft.