OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Kommunale Versorger und KRITIS

Ausgabe KW 48/2026 · Kommunale Versorger und KRITIS in DACH

Zielgruppe	Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber
Berichtszeitraum	20.11.2026 bis 27.11.2026
Version	1.0
Datum	27.11.2026
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 48 steht die Grenze zwischen IT und OT im Mittelpunkt. Palo Alto bestätigt Angriffe auf PAN-OS-Firewalls, deren Management-Oberfläche aus dem Internet erreichbar ist. Bei vielen Stadtwerken ist genau diese Firewall der Übergang zur Leittechnik oder zum Remote Access. Siemens meldet für Industrial Edge fünf NGINX-Schwachstellen, für die es noch keinen Patch gibt. WAGO schließt zwei Lücken, über die angemeldete Nutzer mit wenigen Rechten auf Steuerungen der Typen PFC100 G2, PFC200 G2 und CC100 Root-Rechte bekommen. Diese Geräte sind in Pumpwerken und Unterstationen weit verbreitet.

Aus der Schweiz kommt die erste behördliche Bestätigung für Angriffe mit KI-Agenten. Laut BACS-Direktor gibt es fünf Fälle, drei davon bei Betreibern kritischer Infrastrukturen, und in vier Fällen sind die Angreifer in Systeme eingedrungen. Das BACS rät, kritische Updates spätestens 24 Stunden nach Erscheinen einzuspielen. Für kleine Betriebsteams heißt das: zuerst die Systeme am Internet und den Fernzugang absichern (CC4), dann gezielt nach Risiko patchen (CC5). Zusätzlich hat CISA drei Danfoss-Lücken und fünf Lücken in Mitel MiCollab als aktiv ausgenutzt in den KEV-Katalog aufgenommen.

GESAMTBEWERTUNG

Die Lage ist hoch, weil an IT/OT-Firewalls ausgenutzt wird und KI-gestützte Angriffe auf KRITIS-Betreiber in der DACH-Region bestätigt sind. Vorrang haben Management-Oberflächen und Fernzugänge an der Grenze zur Leittechnik.

Trends

• Angreifer zielen weiter auf die Management-Oberflächen von Firewalls und VPN-Gateways, also genau auf den Übergang zwischen IT und Leittechnik.

• KI-Agenten finden ungepatchte Systeme mit Internetanbindung automatisch, deshalb werden Patch-Fenster von Wochen für Edge-Geräte zum Risiko.

• Bei Herstellern von OT- und Edge-Produkten (Siemens Industrial Edge, Danfoss AK-SM8xxA) erscheinen Advisories zunehmend vor dem Patch, sodass Betreiber nur mit Segmentierung reagieren können.

• Engineering-Workstations und Dienstleister-Konten werden selbst zum Angriffsweg, wie CODESYS und WAGO in dieser Woche zeigen.

• Bei Stadtwerken im DACH-Raum trifft Ransomware bisher vor allem Verwaltungs-IT und Kommunikation. Die Versorgung blieb in den öffentlich gemeldeten Fällen stabil.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Palo Alto PAN-OS: Angriffe auf Management-Oberflächen, die aus dem Internet erreichbar sind (CVE-2026-46300, PAN-SA-2026-0015)	KRITISCH	Palo Alto Networks Security Advisory PAN-SA-2026-0015, 24.11.
L-02	Schweiz: BACS bestätigt fünf Angriffe mit KI-Agenten, drei davon auf Betreiber kritischer Infrastrukturen	HOCH	SRF (Aussagen des BACS-Direktors Florian Schütz), 26.11.

ID	Meldung	Relevanz	Quelle
L-03	WAGO PFC100 G2, PFC200 G2, CC100: Rechteausweitung bis Root über das Web-Based Management (VDE-2026-096)	HOCH	CERT@VDE VDE-2026-096, 23.11.
L-04	Siemens Industrial Edge: fünf NGINX-Lücken („NGINX2Root“), noch kein Fix (SSA-935812)	HOCH	Siemens ProductCERT SSA-935812, 20.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 27.11.2026):

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	136005	DNP3: 31017, OMRON FINS: 24583, ProConOS: 15127, Siemens S7: 7537, OPC UA: 4801
Österreich	4553	HMI/VNC: 998, DNP3: 978, Niagara Fox: 435, Siemens S7: 367, OPC UA: 136

Meldungen im Detail

L-01 Palo Alto PAN-OS: Angriffe auf Management-Oberflächen, die aus dem Internet erreichbar sind (CVE-2026-46300, PAN-SA-2026-0015)

KRITISCH Palo Alto Networks Security Advisory PAN-SA-2026-0015, 24.11.

Was ist neu: Palo Alto bestätigt, dass die Linux-Kernel-Lücke CVE-2026-46300 („Fragnesia“) gegen die Management-Oberfläche von PAN-OS ausgenutzt wird. Laut Advisory führt der einzige bekannte Angriffsweg zuerst über PHP2Shell auf einer Management-Oberfläche, die aus dem Internet erreichbar ist. Behoben ist die Lücke unter anderem ab 10.2.7-h41, 11.1.4-h40, 11.2.4-h25, 12.1.4-h15, 12.2.4-h3 und allen späteren Versionen.

Bedeutung: PAN-OS sitzt bei vielen Versorgern an der Grenze zwischen Büro-IT und Leittechnik oder terminiert den VPN-Zugang für Dienstleister. Wer die Management-Oberfläche oder ein Dataplane-Interface mit Management-Profil offen hatte, muss mit einer Kompromittierung rechnen.

Empfehlung: Die Management-Oberfläche nur aus einem internen Admin-Netz erreichbar machen und den Hotfix sofort einspielen. War sie offen, eine Kompromittierung prüfen und den Fall im Incident-Response-Plan durchspielen (CC4, CC1).

Quelle: https://security.paloaltonetworks.com/PAN-SA-2026-0015 ✓ geprüft

L-02 Schweiz: BACS bestätigt fünf Angriffe mit KI-Agenten, drei davon auf Betreiber kritischer Infrastrukturen

HOCH SRF (Aussagen des BACS-Direktors Florian Schütz), 26.11.

Was ist neu: Laut BACS-Direktor gibt es fünf bestätigte Angriffe mit KI-Agenten, alle in den letzten Tagen gemeldet. Betroffen sind drei Betreiber kritischer Infrastrukturen sowie KMU. In vier von fünf Fällen sind die Angreifer in Systeme eingedrungen, größere Ausfälle gab es nicht.

Bedeutung: SRF nennt Strom- und Wasserversorger nur als Beispiele für kritische Infrastrukturen. Welche Sektoren tatsächlich betroffen sind, ist nicht bestätigt. Für Versorger in der Schweiz, in Österreich und in Deutschland heißt das trotzdem: Ungepatchte Systeme mit Internetanbindung werden schneller und automatisiert gefunden.

Empfehlung: Eine Liste aller Systeme mit Internetanbindung erstellen, Unnötiges abschalten und für kritische Updates an Edge-Geräten ein 24-Stunden-Ziel festlegen, wie es das BACS empfiehlt (CC5, CC2).

Quelle: https://www.srf.ch/news/schweiz/fuenf-bestaetigte-faelle-erstmals-cyberangriffe-mit-ki-agenten-in-der-schweiz ✓ geprüft

L-03 WAGO PFC100 G2, PFC200 G2, CC100: Rechteausweitung bis Root über das Web-Based Management (VDE-2026-096)

HOCH CERT@VDE VDE-2026-096, 23.11.

Was ist neu: CVE-2026-80466 (CVSS 8,8) erlaubt angemeldeten Nutzern mit wenigen Rechten eine OS Command Injection über die Routing-Einstellungen. Die Befehle laufen später mit Root-Rechten. Mit CVE-2026-88850 (CVSS 8,1) lassen sich PROFIBUS-Parameter ändern. Betroffen ist wago_os_linux vor 4.10.0 auf CC100, PFC100 G2, PFC200 G2, TP600, Edge Controller und WP400.

Bedeutung: Für einen Angriff genügt ein einfaches Konto, wie es Dienstleister oder Wartungsfirmen oft im WBM haben. Wer dieses Konto übernimmt, kann die Steuerung ganz kontrollieren und in die Feldbus-Parametrierung eingreifen.

Empfehlung: Betroffene Controller im Asset-Inventar identifizieren und auf 4.10.0 aktualisieren. Das WBM nur aus dem Engineering-Netz erreichbar machen und Konten von Dienstleistern prüfen (CC5, CC2).

Quelle: https://certvde.com/en/advisories/VDE-2026-096/ ✓ geprüft

L-04 Siemens Industrial Edge: fünf NGINX-Lücken („NGINX2Root“), noch kein Fix (SSA-935812)

HOCH Siemens ProductCERT SSA-935812, 20.11.

Was ist neu: Betroffen sind alle Versionen von Industrial Edge Cloud Device, Device Kit (arm64, x86-64), Own Device und Virtual Device. Die fünf CVEs (CVE-2026-113425, -121810, -123007, -123633, -123634) haben jeweils CVSS v3.1 8,1 und v4.0 9,2. Siemens bereitet Fixes vor, Hub und Management-Varianten sind nicht betroffen.

Bedeutung: Edge-Geräte verbinden die Steuerungsebene oft mit Cloud- oder Office-Diensten und sind damit eine Brücke zwischen den Zonen. Solange kein Patch verfügbar ist, schützen nur Konfiguration und Segmentierung.

Empfehlung: Die Workarounds aus dem Advisory umsetzen (HTTP/2 und HTTP/3/QUIC deaktivieren, keine SSI- und Mirror-Direktiven). Die Geräte in eine eigene Zone mit eng begrenztem Zugriff stellen (CC2).

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-935812.html ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Alle Management-Oberflächen von Firewalls, VPN und Fernwartung aus dem Internet entfernen und nur über ein Admin-Netz mit MFA erreichbar machen. [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Einen Patch-Prozess für Edge-Geräte mit 24 bis 72 Stunden für aktiv ausgenutzte Lücken festlegen, gestützt auf KEV-Katalog, CERT@VDE und Herstellerportale. [CC5 Risk-Based Vulnerability Management]	L-02	HOCH	0 bis 3 Monate
M-03	Das Asset-Inventar um Firmwarestände von WAGO, CODESYS und Siemens Industrial Edge ergänzen und mit Advisories abgleichen (bei Bedarf KI-gestützt). [CC5 Risk-Based Vulnerability Management]	L-03	MITTEL	0 bis 3 Monate
M-04	Industrial-Edge-Geräte und Engineering-Workstations in eigene Zonen mit eng begrenzten Übergängen verschieben. [CC2 Defensible Architecture]	L-04	MITTEL	3 bis 6 Monate
M-05	Das Szenario „kompromittierte IT/OT-Firewall“ als Tabletop-Übung mit Leitwarte und Dienstleistern durchspielen, inklusive Trennung und Handbetrieb. [CC1 ICS Incident Response]	L-01	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Ist bei unseren Firewalls an der IT/OT-Grenze eine Management-Oberfläche oder ein Interface mit Management-Profil aus dem Internet erreichbar, und wer hat das zuletzt geprüft?

2. Wie lange brauchen wir heute vom Advisory bis zum Patch an Edge-Geräten, und schaffen wir für kritische Fälle 24 bis 72 Stunden?

3. Welche WAGO-, CODESYS- und Siemens-Edge-Systeme haben wir laut Asset-Inventar, und welche Dienstleister haben dort Konten?

4. Mit welchen Laptops greifen Dienstleister auf Engineering und Steuerungen zu, und wer prüft deren Softwarestand?

5. Gibt es einen geübten Ablauf, falls der Fernzugang zur Leittechnik kompromittiert ist, inklusive Handbetrieb?

Maßnahmen dieser Woche

1. PAN-OS: Management-Zugriff auf ein internes Admin-Netz beschränken, Hotfix gemäß PAN-SA-2026-0015 einspielen und Logs auf Zugriffe von außen prüfen.

2. Phoenix Contact FL MGUARD 2xxx/4xxx auf Firmware 10.7.1 bringen (VDE-2026-159 vom 18.11., Nachtrag aus der Vorwoche) und die Management-Schnittstellen per Firewall-Regel einschränken.

3. WAGO-Controller im Asset-Inventar markieren, Firmware 4.10.0 (FW32) planen und WBM-Konten von Dienstleistern prüfen.

4. Siemens Industrial Edge: HTTP/2 und HTTP/3 per Reverse Proxy deaktivieren, Geräte in eine eigene Zone stellen.

5. Mit einem externen Scan oder einer Shodan-Abfrage der eigenen Adressbereiche prüfen, welche Dienste (Fernwartung, Kälte, Telefonie) aus dem Internet erreichbar sind, und alles Unnötige schließen.

6. Engineering-PCs und Dienstleister-Laptops auf CODESYS Visualization 4.11.0.0 aktualisieren.

HINWEIS ZUR QUELLENLAGE

Alle Meldungen sind gegen Primärquellen (Palo Alto, Siemens, CERT@VDE, CISA) bzw. für die Schweiz gegen SRF mit Aussagen des BACS-Direktors geprüft. Eine eigene BACS-Veröffentlichung dazu habe ich nicht gefunden, und welche KRITIS-Sektoren betroffen sind, ist nicht bestätigt (20 Minuten nennt in einer anderen Lesart zwei von drei erfolgreichen KRITIS-Angriffen, das ist widersprüchlich). Beim Palo-Alto-Advisory ist das Datum uneinheitlich: Auf der Seite steht 25.11., in der Timeline 24.11. Vor dem Berichtszeitraum liegen und deshalb nur als Kontext genannt: BSI-Lagebericht 19.11. („angespannt bis kritisch“, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261119_Lagebericht.html), mGuard VDE-2026-159 vom 18.11., der Ransomware-Fall Osaki Electric (17./18.11.) und der Angriff auf Wittenberg-Net (18./19.11., Volksstimme/dpa). Bei Java4Shell ist eine BSI-Aussage zu Ausnutzungsversuchen nicht belegt, ebenso der Danfoss-Eintrag CVE-2026-127057 aus einer Sekundärquelle; beide sind deshalb nicht aufgenommen. Alle Quellenlinks wurden am 27.11.2026 automatisch aufgerufen und inhaltlich geprüft. 2 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.