OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 48/2026 · Strom und Energie in DACH

Zielgruppe	Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger
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 Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 48 gab es keinen öffentlich bestätigten Angriff auf Netzleittechnik, Schutztechnik oder Umspannwerke in DACH. Die Lage im Energiesektor bleibt trotzdem angespannt, und die Angriffe kommen über die Ränder des Betriebs: Palo Alto bestätigt Angriffe auf PAN-OS-Firewalls mit erreichbarer Management-Oberfläche, und das Schweizer BACS meldet die ersten Angriffe mit KI-Agenten. Bei drei Betreiberinnen kritischer Infrastruktur sind die Angreifer in vier von fünf Fällen eingedrungen. In Deutschland traf es WEMAG über den IT-Dienstleister Planet IC. Kundendaten sind abgeflossen, die Strom- und Netzversorgung lief nach Unternehmensangaben ohne Einschränkung weiter.

Für Netzbetreiber und Stadtwerke heißt das: zuerst Firewalls, VPN- und Fernwartungs-Gateways (mGuard, PAN-OS) patchen und deren Management-Zugänge abschotten. Erst danach kommen die Feld- und Stationsgeräte. Der Ransomware-Fall beim japanischen Zählerhersteller Osaki zeigt außerdem, wie verwundbar die Lieferkette für Smart Meter ist. Das BSI misst im zweiten Quartal 2026 nur noch 8 Tage zwischen Veröffentlichung und Ausnutzung einer Lücke. Patch-Zyklen im Quartalstakt reichen deshalb für Edge-Geräte nicht mehr.

GESAMTBEWERTUNG

Die Lage ist erhöht, akute Angriffe auf Leittechnik in DACH sind aber nicht bekannt. Vorrang haben Edge-Geräte an der Grenze zwischen IT und OT, vor allem exponierte Firewall-Management-Oberflächen und Fernwartungs-Gateways.

Trends

• Angreifer nehmen Firewalls und Fernwartungs-Gateways ins Visier, also genau die Geräte an der Grenze zwischen IT und Leittechnik.

• Bei deutschen Versorgern treffen Vorfälle zunehmend IT-Dienstleister, und am Ende fließen Kundendaten ab, während die Netzführung weiterläuft.

• Mit KI-Agenten wird die Zeit zwischen Veröffentlichung einer Lücke und ihrer Ausnutzung kürzer. Das BACS reagiert darauf mit einer Empfehlung von 24 Stunden für kritische Updates.

• Ransomware bei Herstellern von Messtechnik zeigt, dass die Lieferkette des Smart-Meter-Rollouts selbst ein Cyberrisiko ist.

• Advisories zu PLC- und Controller-Firmware (WAGO, Phoenix Contact) erscheinen in dichtem Takt. Ohne aktuelles Asset-Inventar lässt sich kaum entscheiden, was zuerst gepatcht wird.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Palo Alto PAN-OS: Angriffe auf Firewalls mit erreichbarer Management-Oberfläche (PAN-SA-2026-0015, CVE-2026-46300)	KRITISCH	Palo Alto Networks Security Advisory, 24.11.
L-02	Angriff auf IT-Dienstleister Planet IC trifft Energieversorger WEMAG, Kundendaten abgeflossen	MITTEL	Security-Insider, 27.11.

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 Firewalls mit erreichbarer Management-Oberfläche (PAN-SA-2026-0015, CVE-2026-46300)

KRITISCH Palo Alto Networks Security Advisory, 24.11.

Was ist neu: Palo Alto Networks bestätigt, dass die Linux-Kernel-Lücke CVE-2026-46300 (Fragnesia) ausgenutzt wird. Alle beobachteten Angriffe richteten sich gegen PAN-OS-Geräte, deren Management-Oberfläche erreichbar war. Behoben ist die Lücke unter anderem ab 10.2.7-h41, 11.1.4-h40, 11.2.4-h25, 12.1.4-h15 und 12.2.4-h3 sowie in allen späteren Versionen.

Bedeutung: Viele Versorger nutzen PAN-OS an der Grenze zur Leittechnik oder für den Remote Access von Dienstleistern. Wer die Firewall übernimmt, steht direkt vor der OT-Segmentierung. Geräte, deren Management-Oberfläche von außen erreichbar war, gelten als möglicherweise kompromittiert.

Empfehlung: Management-Zugang heute auf ein Admin-Netz oder einen Jump Host beschränken und auf eine gefixte Version gehen. Danach die Logs der letzten Wochen auf Zugriffe von außen prüfen (CC2 Defensible Architecture, CC4 Secure Remote Access).

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

L-02 Angriff auf IT-Dienstleister Planet IC trifft Energieversorger WEMAG, Kundendaten abgeflossen

MITTEL Security-Insider, 27.11.

Was ist neu: Am Abend des 21. November 2026 gab es laut Planet IC einen unbefugten Zugriff auf Server seines Rechenzentrums. WEMAG hat betroffene Systeme vom Netz genommen, ausgelagerte Dienste des Vertriebssystems sind betroffen. Laut NDR sind Kundendaten von WEMAG nach außen gelangt.

Bedeutung: Der Fall folgt dem Muster der letzten Monate: Angreifer kommen über IT-Dienstleister und erbeuten Kundendaten, die Versorgung selbst bleibt laut WEMAG unberührt. Für Stadtwerke heißt das, dass die Lieferkette bei Vertrieb, Abrechnung und Hosting in die eigene Risikoanalyse gehört.

Empfehlung: Liste aller Dienstleister mit Zugriff auf Kundendaten oder Netzsysteme aktualisieren und für jeden klären, wer im Ernstfall meldet, wer abschaltet und wer informiert. Die Meldewege mit dem Dienstleister in der nächsten Notfallübung durchspielen (CC1 ICS Incident Response).

Quelle: https://www.security-insider.de/cyberangriff-planet-ic-kunden-websites-offline-wemag-datenabfluss-a-a12ee7057dc60704e62f5d5203418ffd/ ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Management-Zugänge von PAN-OS-Firewalls auf interne Admin-Netze beschränken, auf gefixte Version aktualisieren und Logs auf Kompromittierung prüfen [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Dienstleister mit Zugriff auf Kundendaten und Netzsysteme erfassen, Meldewege vertraglich festlegen und in einer Notfallübung testen [CC1 ICS Incident Response]	L-02	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Ist bei einer unserer Firewalls oder einem VPN-Gateway die Management-Oberfläche aus dem Internet erreichbar, und wer hat das zuletzt geprüft?

2. Welche mGuard- und WAGO-Geräte laufen bei uns mit betroffener Firmware, und wann ist das Wartungsfenster?

3. Wie schnell können wir einen kritischen Patch an einem Edge-Gerät einspielen: in 24 Stunden, in einer Woche oder erst im Quartal?

4. Welche Dienstleister haben Zugriff auf unsere Kundendaten oder Netzsysteme, und wie melden sie uns einen Vorfall?

5. Was tun wir, wenn unser Zähler- oder Gateway-Lieferant nach einem Cyberangriff wochenlang nicht liefern kann?

Maßnahmen dieser Woche

1. Bei allen PAN-OS-Firewalls prüfen, ob die Management-Oberfläche von außen erreichbar ist. Den Zugang auf interne Admin-Netze beschränken, auf eine gefixte Version aktualisieren

und die Logs auf fremde Zugriffe durchsehen.

2. Phoenix Contact FL MGUARD mit Firmware 10.0.0 bis vor 10.7.1 auf 10.7.1 bringen, Geräte mit Internet-Anbindung zuerst.

3. WAGO-Controller mit wago_os_linux vor 4.10.0 aktualisieren und WBM-Konten von Dienstleistern prüfen und reduzieren.

4. Eine Regel für Notfall-Patches an Edge-Geräten beschließen, mit einem Ziel von 24 Stunden bis wenigen Tagen und einer klaren Freigabe außerhalb des normalen Change-Prozesses.

5. Liste der IT- und Messdienstleister mit Meldewegen und Ansprechpartnern für den Ernstfall aktualisieren.

HINWEIS ZUR QUELLENLAGE

Für KW 48 habe ich keinen öffentlich bestätigten Angriff auf Netzleittechnik, Schutztechnik oder Umspannwerke in DACH gefunden, und auch keine neuen Advisories von Siemens oder Hitachi Energy speziell zu SICAM, SIPROTEC oder RTU500. Nicht aufgenommen habe ich den Angriff auf die Stadtwerke Wittenberg (Telefon und Internet bei Wittenberg-Net, Bericht vom 19.11., also vor dem Zeitraum, Auswirkung auf Strom nicht berichtet). Ebenfalls draußen sind die Danfoss-Kühlanlagen-Lücken (kein Energiebezug), Siemens Industrial Edge SSA-935812 (20.11., noch kein Patch, im Energiebereich selten) und Schneider EcoStruxure Power Build Rapsody (ICSA-26-328-02, nur lokal ausnutzbar, CVSS 5,3). Zur Schweiz: Ob die vom BACS gemeldeten Fälle Energieversorger betreffen, ist nicht bestätigt. Die WEMAG-Meldung stützt sich auf Presseberichte (Security-Insider, NDR), eine Primärmeldung von WEMAG habe ich nicht geöffnet. Alle Quellenlinks wurden am 27.11.2026 automatisch aufgerufen und inhaltlich geprüft. 5 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.