

WOCHENBERICHT

OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 44/2026 · Strom und Energie in DACH

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

Management Summary

In KW 44 gab es keinen bestätigten Angriff auf Netzleittechnik in DACH, aber mehrere aktiv ausgenutzte Lücken in Edge-Geräten, über die Stadtwerke und Netzbetreiber ihre Fernwartung und Außenstellen anbinden. Die PHP2Shell-Lücken (CVE-2026-109618/-109619) stehen seit 26.10. im KEV-Katalog der CISA. Palo Alto hat zwischen 25. und 29.10. Hotfixes für alle unterstützten PAN-OS-Zweige veröffentlicht, auch für die Siemens RUGGEDCOM APE1808 in Umspannwerken. Cisco bestätigt seit 28.10. die Ausnutzung einer DoS-Lücke im SSL-VPN von ASA/FTD. Bei Arista VeloCloud Orchestrator wird die dritte SD-WAN-Lücke seit Juli ausgenutzt.

Direkt die Netztechnik betreffen zwei Advisories von Hitachi Energy (29.10.): Router der Serie TRO600 geben ohne Anmeldung Konfigurations- und Passwortdateien preis, und das Transformator-Monitoring CoreTec erlaubt Command Injection. Ausnutzung ist dort nicht bekannt. Zusammen mit den Altlasten bei Mitsubishi ICONICS GENESIS zeigt die Woche, wie viel von einem vollständigen Asset-Inventar und einem abgeschotteten Remote Access (CC4) abhängt. Mit diesen beiden Grundlagen wird aus einer Patch-Welle eine überschaubare Arbeitsliste.

GESAMTBEWERTUNG

Die Lage ist erhöht bis hoch, weil Angreifer gezielt Firewalls, VPN-Gateways und SD-WAN-Orchestratoren angreifen, also genau den Übergang zwischen Office und Leittechnik. Vorrang haben die PAN-OS-Hotfixes inkl. RUGGEDCOM APE1808, die Cisco-ASA-Fixes und das Abschotten aller Management-Oberflächen.

Trends

- Angreifer nutzen Lücken in Firewalls, VPN und SD-WAN-Orchestratoren inzwischen innerhalb weniger Tage nach der Veröffentlichung aus, das Patch-Fenster für Edge-Geräte ist also eher Tage als Wochen.
- Lücken in Basiskomponenten wie PHP wandern über Lieferketten in OT-Produkte (Siemens, Rockwell, Cisco), und die Hersteller melden ihre Betroffenheit nacheinander über mehrere Tage.
- Ransomware-Gruppen listen vermehrt kleinere Energiehändler und Engineering-Dienstleister der Netzbranche, die meisten Einträge sind aber unbestätigt.
- Hersteller wie Mitsubishi beenden den Support für ältere SCADA-Produkte ohne Fix, Altinstallationen bleiben dadurch dauerhaft ein Risiko.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	PHP2Shell: Hotfixes für PAN-OS da, aktive Ausnutzung bestätigt, RUGGEDCOM APE1808 betroffen	KRITISCH	Palo Alto Networks PSIRT / Siemens ProductCERT / CISA KEV, 29.10.
L-02	Cisco ASA/FTD: ausgenutzte DoS-Lücke im SSL-VPN (CVE-2026-76418, CVSS 8,6)	HOCH	Cisco PSIRT, 28.10.

ID	Meldung	Relevanz	Quelle
L-03	Arista VeloCloud Orchestrator: dritter ausgenutzter Zero-Day seit Juli (CVE-2026-114625), KEV seit 23.10.	HOCH	BleepingComputer / CISA KEV (über Security Affairs), 23.10.
L-04	Hitachi Energy TRO600 und CoreTec: Lücken in Feldnetz-Routern und Transformator-Monitoring	HOCH	CISA ICISA-26-302-02 / ICISA-26-302-03 (Hitachi Energy PSIRT), 29.10.
L-05	Mitsubishi ICONICS GENESIS64/MC Works64: Anmeldung umgehbar, für Altprodukte kein Fix	MITTEL	CISA ICISA-26-300-02, 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: Hotfixes für PAN-OS da, aktive Ausnutzung bestätigt, RUGGEDCOM APE1808 betroffen

KRITISCH Palo Alto Networks PSIRT / Siemens ProductCERT / CISA KEV, 29.10.

Was ist neu: Palo Alto hat zwischen 25. und 29.10. Hotfixes für alle unterstützten PAN-OS-Zweige 10.2 bis 12.2 veröffentlicht, z. B. 11.1.16-h4, 11.2.16-h1 und 12.2.4-h1. Die Ausnutzung über Management-Interfaces, die im Internet erreichbar sind, ist bestätigt (Status „ATTACKED“). Die CISA hat beide CVEs am 26.10. in den KEV-Katalog aufgenommen. Siemens hat SSA-566512 für RUGGEDCOM APE1808 am 28.10. auf V1.1 aktualisiert und verweist auf die verfügbaren PAN-OS-Versionen.

Bedeutung: Die APE1808 ist eine NGFW für Umspannwerke und Fernwirktechnik. Wer dort oder auf einer zentralen Palo-Alto-Firewall noch ungepatcht ist und die Management-Oberfläche erreichbar lässt, bietet einen bestätigt ausgenutzten Einstieg mit CVSS 9,8 direkt vor der Leittechnik.

Empfehlung: Die Hotfixes für die eigenen Zweige aus dem Advisory einspielen und bei der APE1808 den Siemens-Support einbinden. Bis dahin das Management-Interface nur von einem Jump Host aus erreichbar machen und die Threat-IDs aus dem Advisory aktivieren (CC4, CC5).

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

L-02 Cisco ASA/FTD: ausgenutzte DoS-Lücke im SSL-VPN (CVE-2026-76418, CVSS 8,6)

HOCH Cisco PSIRT, 28.10.

Was ist neu: Ohne Anmeldung kann ein Angreifer über den Login-Dienst des SSL-VPN einen Neustart von ASA oder FTD auslösen. Betroffen sind Geräte, bei denen in einer Tunnel-Gruppe eine sekundäre Authentifizierung eingerichtet ist, auch in der DefaultWEBVPNGroup. Cisco bestätigt die aktive Ausnutzung. Einen echten Workaround gibt es nicht, es gibt nur Mitigationen, die die Sicherheit senken.

Bedeutung: Es fließen keine Daten ab, aber ein dauerhaft neu startendes VPN unterbricht den Remote Access der Bereitschaft und von Dienstleistern. Bei einer Störung im Netz kann das die Entstörung verzögern.

Empfehlung: Prüfen, ob irgendwo eine sekundäre Authentifizierung konfiguriert ist, und auf die erste Fix-Version wechseln (z. B. ASA 9.20.4.50, FTD 7.4.9). Für die Bereitschaft einen zweiten, unabhängigen Notzugang dokumentieren und testen (CC4, CC1).

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

L-03 Arista VeloCloud Orchestrator: dritter ausgenutzter Zero-Day seit Juli (CVE-2026-114625), KEV seit 23.10.

HOCH BleepingComputer / CISA KEV (über Security Affairs), 23.10.

Was ist neu: Über eine SQL-Injection wird jeder angemeldete Nutzer, auch mit der Rolle „Enterprise Read Only“, im On-Prem-Orchestrator zum Superuser. Die Fixes stecken in 5.2.3.18, 6.1.3.10 und 6.4.2.12. Die CISA hat die Lücke am 23.10. in den KEV-Katalog aufgenommen. Beim CVSS-Wert gibt es unterschiedliche Angaben, Sekundärquellen nennen 9,9 (v3.1) und 9,4 (v4.0).

Bedeutung: Wer den Orchestrator kontrolliert, kann die Routing- und Segmentierungsregeln aller angebundenen Edges ändern. Für Stadtwerke, die Pumpwerke oder Umspannwerke per VeloCloud anbinden, ist die Segmentierung dann nicht mehr verlässlich.

Empfehlung: Auf die Fix-Versionen aktualisieren und die Logs auf die beiden von Arista genannten Angreifer-IPs (74.82.197.86, 38.54.50.151) prüfen. Dazu alle Konten mit Leserechten am VCO prüfen und die nicht benötigten entfernen (CC2, CC5).

Quelle: <https://www.bleepingcomputer.com/news/security/arista-patches-new-velocloud-orchestrator-zero-day-exploited-in-attacks/> ✓ geprüft

L-04 Hitachi Energy TRO600 und CoreTec: Lücken in Feldnetz-Routern und Transformator-Monitoring

HOCH CISA ICSA-26-302-02 / ICSA-26-302-03 (Hitachi Energy PSIRT), 29.10.

Was ist neu: Auf TRO600 bis 9.2.1.6 kann ein Angreifer ohne Anmeldung beliebige Dateien lesen, auch Konfiguration und Passwortdaten (CVE-2026-106087, CVSS v4 8,7). Mit Anmeldung kommt er per Port-Forwarding an Dienste, die nur für localhost gedacht sind (CVE-2026-10756). Behoben ist das in 9.2.2.1 bzw. 9.1.2.0. In CoreTec4/5 bis 3.4.0 erlaubt die Zeitzone-Einstellung eine Command Injection (CVE-2026-13162), CoreTec5 hat zusätzlich eine Kernel-Lücke zur Rechteausweitung. Der Fix ist CoreTec5 5.0.0, für CoreTec4 empfiehlt Hitachi den Umstieg.

Bedeutung: Die Produkte stecken direkt in der Netzinfrastruktur. Abgegriffene Passwortdaten eines Routers machen oft den Weg zu weiteren Stationen frei. Eine Ausnutzung ist laut CISA nicht bekannt.

Empfehlung: Bestand an TRO600 und CoreTec im Asset-Inventar prüfen, die Firmware aktualisieren und danach die Passwörter der Router wechseln. Bis zum Update die Weboberflächen nur aus dem Stationsleitnetz erreichbar machen (CC5, CC2).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-302-02> ✓ geprüft

L-05 Mitsubishi ICONICS GENESIS64/MC Works64: Anmeldung umgehbar, für Altprodukte kein Fix

MITTEL CISA ICSA-26-300-02, 27.10.

Was ist neu: Die Passwort-Wiederherstellung nutzt eine feste Challenge-Response, die für alle Nutzer gleich ist (CVE-2026-16436, CVSS v4 9,2). Dazu kommt eine Rechteausweitung. Fixes gibt es mit GENESIS 11.04 und GENESIS64 10.98. Für MC Works64, GENESIS32 und BizViz kommt kein Fix.

Bedeutung: GENESIS64 läuft als HMI und Historian auch in Energie- und Wassernetzen. Altinstallationen bleiben dauerhaft verwundbar und gehören deshalb in die Risikobewertung.

Empfehlung: Alle ICONICS- und MC-Works-Installationen erfassen, unterstützte Versionen aktualisieren und Altprodukte vom Remote Access trennen. Den von CISA beschriebenen Workaround (Challenge-Datei leeren) anwenden (CC5).

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

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	PAN-OS-Hotfixes inkl. RUGGEDCOM APE1808 einspielen und Management-Zugang auf Jump Host beschränken [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Cisco ASA/FTD aktualisieren und einen getesteten Notzugang für die Bereitschaft festlegen [CC1 ICS Incident Response]	L-02	HOCH	sofort
M-03	VeloCloud-Orchestrator patchen und Rollen sowie Konten am VCO bereinigen [CC2 Defensible Architecture]	L-03	HOCH	sofort

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-04	Asset-Inventar für Feld- und Stationsgeräte (TRO600, CoreTec, ICONICS) vervollständigen und einen KEV-Abgleich automatisieren [CC5 Risk-Based Vulnerability Management]	L-04	MITTEL	0 bis 3 Monate
M-05	Altinstallationen ohne Herstellersupport (MC Works64, GENESIS32) per Segmentierung isolieren und ihre Ablösung planen [CC2 Defensible Architecture]	L-05	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Sind alle Palo-Alto-Firewalls inkl. RUGGEDCOM APE1808 auf dem Hotfix-Stand, und ist ihr Management-Interface nur über einen Jump Host erreichbar?
2. Haben wir auf irgendeiner Cisco ASA/FTD eine sekundäre Authentifizierung im SSL-VPN, und welchen Notzugang nutzt die Bereitschaft, wenn das VPN ausfällt?
3. Wo im Netz laufen Hitachi TRO600, CoreTec oder ICONICS GENESIS, und steht das vollständig im Asset-Inventar?
4. Welche OT-Dokumentation (Netzpläne, Geräteinventare, Firmware-Stände) liegt bei Engineering-Dienstleistern, und wie ist der Zugriff dort geschützt?
5. Wer erfährt bei uns innerhalb von 24 Stunden von einem KEV-Eintrag, der unsere Edge-Geräte betrifft?

Maßnahmen dieser Woche

1. PAN-OS-Hotfix für CVE-2026-109618/-109619 einspielen, bei RUGGEDCOM APE1808 über den Siemens-Support, und die Management-Logs seit 17.10. prüfen.
2. Cisco ASA/FTD auf die Fix-Version aus cisco-sa-asaftd-tunnel-dos-s6mgkb75 bringen, vorher die Tunnel-Gruppen auf sekundäre Authentifizierung prüfen.
3. On-Prem-VeloCloud-Orchestrator auf 5.2.3.18, 6.1.3.10 oder 6.4.2.12 aktualisieren und die Logs nach den Arista-IOCs durchsuchen.
4. TRO600-Router und CoreTec-Geräte inventarisieren und aktualisieren, danach die Passwörter der Router wechseln.
5. Eine Liste aller Management-Oberflächen anlegen, die aus dem Internet oder dem Office-Netz erreichbar sind, und sie auf Jump-Host-Zugang umstellen.

HINWEIS ZUR QUELLENLAGE

Herstellerseiten und CISA bestätigen die Advisories von Palo Alto, Cisco, Siemens, Hitachi Energy und Mitsubishi. Die VeloCloud-Meldung stützt sich auf BleepingComputer und mehrere Sekundärquellen, die Angaben zum CVSS-Wert gehen auseinander. Nicht aufgenommen, weil unbestätigt oder von mir nicht prüfbar: die Leak-Einträge zu Ingelectus (N0n), Frommann Energie (Emperador) und Tema Energy (nur Angaben der Täter, die Unternehmen haben nichts bestätigt); der Bloomberg-Bericht über physische Schäden durch Russland-nahe Hacktivistinnen und der METI-Vorfall in Japan (Primärquellen nicht abrufbar); die WatchGuard-Meldung WID-SEC-2026-4209 (CERT-Bund-Eintrag nicht auffindbar, nur securityonline.info); die Shadowserver-Zahl von 51.000 ASA-VPNs. Einen Cyberangriff auf ein Stadtwerk in DACH habe ich für KW 44 nicht gefunden. Alle Quellenlinks wurden am 30.10.2026 automatisch aufgerufen und inhaltlich geprüft.