

WOCHENBERICHT

OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 43/2026 · Strom und Energie in DACH

Zielgruppe	Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger
Berichtszeitraum	16.10.2026–23.10.2026
Version	1.0
Datum	23.10.2026
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

Uns ist im Berichtszeitraum (16. bis 23.10.) kein bestätigter Cyberangriff auf Netzleittechnik, Umspannwerke oder Erzeugungsanlagen im DACH-Raum bekannt. Am 15.10. veröffentlicht und am 16.10. in den KEV-Katalog aufgenommen wurde eine Lücke in BeyondTrust Remote Support, die schon vor der Veröffentlichung ausgenutzt wurde; die zwei bekannten Kompromittierungen datiert BeyondTrust auf den 29.08.2026. Laut Rapid7 ordnet Mandiant die Aktivität aus seiner Untersuchung ARMORY CASTLE zu, einem mutmaßlich China-nahen Spionageakteur (früher UNC5221). Bei Palo Alto GlobalProtect beobachtet Unit 42 Ausnutzungsversuche und Angriffe durch Ransomware-Betreiber, darunter Qilin und Inc; seine Untersuchungen seit Anfang Juni umfassen zahlreiche Branchen, darunter Versorgung und Energie. Mit dem SafePay-Advisory vom 20.10. warnen FBI, CISA, US Secret Service, LKA Rheinland-Pfalz sowie die britische National Crime Agency und die North West Regional Organised Crime Unit vor einer Gruppe, von der seit August 2024 mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur betroffen sind. Als Zugangswege nennt das Advisory gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing.

Für die Stations- und Fernwirktechnik hat CISA am 20.10. zwei Advisories von Hitachi Energy neu veröffentlicht. Beim RTU500 lässt eine Lücke die CMU bei Generalabfragen (GI) in kurzen Abständen abstürzen, beim MicroSCADA X SYS600 können Nutzer mit Zugriff auf die Engineering-Tools ihre Rechte bis zum Windows-Administrator ausweiten. Laut CISA-Advisory vom 22.10. gibt es acht CVEs (Typen laut CISA: Eval Injection und Cross-Site Scripting) im Webserver von SIMATIC S7-1500 und ET 200SP, für die es für einen großen Teil der Produkte noch keinen Fix gibt; Siemens bereitet Fixes vor und empfiehlt bis dahin Gegenmaßnahmen. Angreifer können damit SPS-Operationen im Rahmen der Rechte des angemeldeten Nutzers ausführen. Vorrang haben in dieser Woche Fernwartung und VPN. Die Firmware-Updates für Stationstechnik gehören in die nächste Wartungsplanung.

GESAMTBEWERTUNG

Die Lage ist hoch, weil zwei Fernzugangs-Produkte betroffen sind: BeyondTrust Remote Support, dessen Ausnutzung Mandiant laut Rapid7 einem mutmaßlich China-nahen Spionageakteur zuordnet, und Palo Alto GlobalProtect, bei dem Unit 42 Ausnutzungsversuche durch Ransomware-Betreiber beobachtet. Dazu kommt die Ransomware-Gruppe SafePay, die laut Advisory über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing einsteigt. Vorrang hat die Prüfung von BeyondTrust und GlobalProtect auf Kompromittierung, nicht nur das Patchen.

Trends

- Fernzugänge sind derzeit der Haupteinstieg: BeyondTrust, GlobalProtect und FortiGate (PEERSTITCH-Backdoor über gestohlene FortiManager-Konfigurationen, CVE-2025-61624 laut Rescana seit 16.10. im KEV) werden aktiv ausgenutzt (<https://thehackernews.com/2026/10/attackers-exploit-fortios-flaw-to.html>).
- Ein Patch reicht bei Edge Devices oft nicht mehr, weil die Angreifer Zugangsdaten abziehen und Spuren hinterlassen, die Neustarts und Updates überstehen; Rapid7 und Unit 42 raten deshalb ausdrücklich zu einer Prüfung auf Kompromittierung.
- Bei Stationstechnik kommen die Lücken immer häufiger aus Fremdbibliotheken (OpenSSL, libxml2, libcurl in der RTU500, Eclipse Milo in OPC-UA-Produkten), sodass SBOM-Abfragen

beim Hersteller an Bedeutung gewinnen.

- Deutsche Behörden zeichnen internationale Ransomware-Advisories mit (LKA Rheinland-Pfalz bei SafePay); das ist ein direkter Hinweis auf Opfer im DACH-Raum.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	BeyondTrust Remote Support: Zero-Day laut Mandiant von mutmaßlich China-naher Gruppe ausgenutzt, KEV seit 16.10. (CVE-2026-102764)	KRITISCH	Rapid7 / BleepingComputer (Mandiant, CISA KEV), 16.10.
L-02	Palo Alto GlobalProtect (CVE-2026-0257): Unit 42 beobachtet Ausnutzungsversuche durch Ransomware-Betreiber Qilin und Inc	HOCH	Palo Alto Networks Unit 42, 20.10.
L-03	SafePay-Ransomware: FBI, CISA, US Secret Service, LKA Rheinland-Pfalz, NCA und NWROCU warnen gemeinsam (AA26-293A)	HOCH	CISA (govdelivery-Bulletin), BleepingComputer, 20.10.
L-04	Hitachi Energy RTU500: Generalabfragen in kurzen Abständen lassen die CMU abstürzen (ICSA-26-293-05)	HOCH	CISA / Hitachi Energy PSIRT, 20.10.
L-05	Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver, für einen großen Teil der Produkte noch kein Fix (ICSA-26-295-14)	HOCH	CISA / Siemens ProductCERT, 22.10.
L-06	Hitachi Energy MicroSCADA X SYS600: Rechteausweitung bis zum Windows-Administrator (ICSA-26-293-04)	MITTEL	CISA / Hitachi Energy PSIRT, 20.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 23.10.2026):

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	144393	DNP3: 33922, OMRON FINS: 24335, ProConOS: 16607, Siemens S7: 8039, OPC UA: 5548
Österreich	4715	HMI/VNC: 1070, DNP3: 969, IEC-104: 455, Siemens S7: 365, OPC UA: 141

Meldungen im Detail

L-01 BeyondTrust Remote Support: Zero-Day laut Mandiant von mutmaßlich China-naher Gruppe ausgenutzt, KEV seit 16.10. (CVE-2026-102764)

KRITISCH Rapid7 / BleepingComputer (Mandiant, CISA KEV), 16.10.

Was ist neu: Angreifer umgehen ohne Konto die Anmeldung und erhalten Admin-Rechte (CVSS 4.0 9,3). Die Lücke wurde am 15.10. veröffentlicht, am 16.10. in den KEV-Katalog aufgenommen und schon vor der Veröffentlichung ausgenutzt; die zwei bekannten Kompromittierungen datiert BeyondTrust auf den 29.08.2026, eine gehostete Instanz und eine selbst betriebene Appliance. Laut Rapid7 ordnet Mandiant die Aktivität aus seiner Untersuchung ARMORY CASTLE zu, einem mutmaßlich China-nahen Spionageakteur (früher UNC5221). Dieser legt die Webshell SAWFLY und den Tunneler BARECLAW ab, versucht den Credential Vault auszulesen und löscht Logs. CISA hat die Lücke am 16.10. in den KEV aufgenommen und verlangt eine forensische Prüfung.

Bedeutung: Wo BeyondTrust als Fernwartungszugang genutzt wird, liegen im Vault häufig Zugangsdaten für OT-Jump-Hosts. Wer dort eindringt, kann direkt bis zur Netzleittechnik weiterkommen.

Empfehlung: Laut Rapid7 rät Mandiant, vor Änderungen Beweise zu sichern, verdächtige Appliances zu isolieren und sie aus einem sauberen, gepatchten Image neu aufzubauen, wenn eine Kompromittierung bestätigt ist oder sich nicht ausschließen lässt. Alle im Vault gespeicherten Zugangsdaten wechseln (CC4). Danach die Logs der Jump Hosts seit Ende August nach Lateral Movement durchsuchen (CC1).

Quelle: <https://www.rapid7.com/blog/post/etr-cve-2026-102764-critical-beyondtrust-remote-support-authentication-bypass-exploited-in-the-wild/> ✓ geprüft

L-02 Palo Alto GlobalProtect (CVE-2026-0257): Unit 42 beobachtet Ausnutzungsversuche durch Ransomware-Betreiber Qilin und Inc

HOCH Palo Alto Networks Unit 42, 20.10.

Was ist neu: Unit 42 beobachtet Ausnutzungsversuche und Angriffe durch Ransomware-Betreiber, darunter Qilin (Spikey Scorpius) und Inc (Tarnished Scorpius); Settra wird nur in öffentlichen Berichten genannt. Seine Untersuchungen seit Anfang Juni umfassen zahlreiche Branchen, darunter Versorgung und Energie (utilities and energy). Neu ist der Hinweis, dass GlobalProtect-Profile auf dem Management-Interface dieses unbemerkt über die Ports 4443 und 3879 ins Internet stellen können.

Bedeutung: Gelingt eine VPN-Session, stehen Angreifer im Netz hinter dem Gateway. Wo GlobalProtect vor dem Leittechniknetz steht, ist das ein direkter Einstieg.

Empfehlung: Von einem externen Anschluss aus testen, ob das Management-Interface auf 4443/3879 erreichbar ist, und den Zugriff auf das Nötigste beschränken (CC2).

GlobalProtect-Logs nach den Gerätenamen GP-CLIENT und DESKTOP-GP01 sowie nach leerer Domain durchsuchen. Bei Treffern Incident Response auslösen (CC1).

Quelle: <https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/> ✓ geprüft

L-03 SafePay-Ransomware: FBI, CISA, US Secret Service, LKA Rheinland-Pfalz, NCA und NWROCU warnen gemeinsam (AA26-293A)

HOCH CISA (govdelivery-Bulletin), BleepingComputer, 20.10.

Was ist neu: Seit August 2024 sind mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur von SafePay betroffen, auch in Europa. Initial Access läuft laut Advisory über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen, darunter CVE-2020-3259 und CVE-2024-40766, und Phishing. Nach unserer Einordnung betreffen diese CVEs u. a. VPN-Systeme. Die Angreifer schalten Sicherheitsfunktionen ab, um unentdeckt zu bleiben. Herausgeber sind FBI, CISA, US Secret Service, LKA Rheinland-Pfalz sowie die britische National Crime Agency und die North West Regional Organised Crime Unit; die Erkenntnisse stammen aus Ermittlungen von FBI, USSS und LKA Rheinland-Pfalz.

Bedeutung: Das LKA Rheinland-Pfalz hat selbst zu SafePay ermittelt, die Gruppe ist also auch in Deutschland aktiv. Bei Stadtwerken legt ein Angriff auf die IT zwar meist nicht das Netz lahm, aber Abrechnung, Kommunikation und Fernwartung. Fehlen dann die Backups, dauert der Wiederanlauf Wochen.

Empfehlung: VPN-Zugänge ohne MFA abschalten und die im Advisory genannten CVEs im Asset-Inventar abgleichen (CC5). Den Wiederanlauf aus Backups für die Systeme an der Grenze zur Leittechnik üben (CC1).

Quelle: <https://www.bleepingcomputer.com/news/security/cisa-and-fbi-safepay-ransomware-has-hit-over-600-critical-infrastructure-organizations/amp/> ✓ geprüft

L-04 Hitachi Energy RTU500: Generalabfragen in kurzen Abständen lassen die CMU abstürzen (ICSA-26-293-05)

HOCH CISA / Hitachi Energy PSIRT, 20.10.

Was ist neu: CISA hat am 20.10. das Hitachi-Advisory vom 01.09. (Revision 29.09.) veröffentlicht. Betroffen ist die CMU-Firmware 12.7.1 bis 12.7.7 und 13.5.1 bis 13.8.2. Mit CVE-2026-17539 (CVSS v3.1 5,9) lässt eine Lücke die CMU bei Generalabfragen (GI) in kurzen Abständen abstürzen. Dazu kommen Lücken in OpenSSL, libxml2 und libcurl bis CVSS 8,8. Die Kopfzeile nennt 7 Lücken, im Text stehen 9 CVEs.

Bedeutung: Die RTU500 ist in DACH eine verbreitete Fernwirk- und Stationsleiteinheit. Stürzt die CMU ab, sieht die Netzleitstelle die Station nicht mehr und kann nicht mehr schalten. Einen Workaround ohne Firmware-Update gibt es nicht.

Empfehlung: Betroffene Geräte im Asset-Inventar markieren und das Update nach Kritikalität der Station in die Wartungsfenster legen (CC5). Bis dahin prüfen, ob die 104-Verbindungen nur zwischen festen Endpunkten erlaubt sind (CC2).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-05> ✓ geprüft

L-05 Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver, für einen großen Teil der Produkte noch kein Fix (ICSA-26-295-14)

HOCH CISA / Siemens ProductCERT, 22.10.

Was ist neu: CVE-2026-63350 bis -63357 betreffen alle Versionen. Das CISA-Advisory vom 22.10. nennt zahlreiche Produkte, darunter S7-1500, ET 200SP, Drive-, Open- und Software-Controller sowie PLCSIM Advanced. Es sind acht CVEs (Typen laut CISA: Eval Injection und Cross-Site Scripting). Ein Angreifer kann Schadcode in der Browser-Sitzung eines berechtigten Nutzers ausführen und damit SPS-Operationen im Rahmen der Rechte des angemeldeten Nutzers ausführen (CVSS v3 bis 9,6). Siemens rät u. a., nur vertrauenswürdige Trace-Dateien hochzuladen. Siemens bereitet Fixes vor, Energie ist als Sektor genannt.

Bedeutung: Die S7-1500 ist eine weit verbreitete SPS-Familie und steckt nach unserer Einordnung in BHKW, Wasserkraft, Biogas und Nebenanlagen von Umspannwerken. Für den Angriff braucht es einen angemeldeten Nutzer im Browser. Bei Dienstleistern, die Trace-Dateien per Mail austauschen, ist das nach unserer Einschätzung ein realistischer Weg.

Empfehlung: Webserver auf allen CPUs inventarisieren und deaktivieren, wo er nicht gebraucht wird (CC5). Wo er bleiben muss, nur aus dem Engineering-Netz erreichbar machen und Trace-Dateien nur aus bekannter Quelle importieren (CC2).

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

L-06 Hitachi Energy MicroSCADA X SYS600: Rechteausweitung bis zum Windows-Administrator (ICSA-26-293-04)

MITTEL CISA / Hitachi Energy PSIRT, 20.10.

Was ist neu: Betroffen sind die Versionen bis 10.8. Mit CVE-2026-9853 erreichen Nutzer mit Betriebssystem-Zugang Anwendungsobjekte ohne SYS600-Anmeldung. Über CVE-2026-9854 werden Nutzer mit Zugriff auf die Engineering-Tools Windows-Administrator (beide CVSS v4 8,5). Dazu kommt eine CSV Injection im Log-Export (CVE-2026-9852). Hitachi Energy nennt Version 10.8 als Update für CVE-2026-9852; für die übrigen CVEs die Herstellerhinweise im Advisory beachten.

Bedeutung: Ein Angriff von außen ist damit nicht möglich. Wer aber schon im Leittechniknetz ist, etwa über einen kompromittierten Fernwartungs-Zugang wie bei BeyondTrust, kann sich auf dem SYS600-Server vollständige Kontrolle verschaffen. Die Lücken verlängern also eine Angriffskette, die woanders beginnt.

Empfehlung: Prüfen, welche Windows-Konten lokal auf den SYS600-Servern angemeldet sein dürfen, und Engineering-Rechte auf benannte Personen beschränken (CC2). Das Update auf 10.8 mit dem nächsten geplanten Release-Wechsel testen (CC5).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-04> ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Compromise Assessment für BeyondTrust- und GlobalProtect-Systeme durchführen und Zugangsdaten der OT-Jump-Hosts wechseln (CC4)	L-01	HOCH	sofort
M-02	Management-Interfaces aller Firewalls und VPN-Gateways aus dem Internet entfernen und regelmäßig von außen prüfen lassen (CC2)	L-02	HOCH	sofort

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-03	MFA für alle VPN-Zugänge erzwingen und Offline-Backups für Systeme an der Grenze zur Leittechnik einrichten (CC1)	L-03	HOCH	0 bis 3 Monate
M-04	Firmware-Updates RTU500 und SYS600 nach Kritikalität der Stationen planen und den S7-1500-Webserver bis zum Patch abschotten (CC5)	L-04	MITTEL	0 bis 3 Monate
M-05	SBOM-Abfrage an alle Leittechnik- und Gateway-Hersteller als festen Prozess einführen (CC5)	L-06	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Über welche Produkte greifen unsere Dienstleister auf die Leittechnik zu, und ist eines davon BeyondTrust, GlobalProtect oder FortiGate?
2. Wer hat geprüft, ob unsere Firewall-Management-Interfaces aus dem Internet erreichbar sind, und wann zuletzt?
3. Welche RTU500, SYS600 und S7-1500 haben wir im Einsatz, mit welcher Firmware, und haben wir das im Asset-Inventar?
4. Können wir die Netzleitstelle betreiben, wenn die Unternehmens-IT einschließlich VPN und Backups mehrere Tage ausfällt?
5. Haben wir von unseren Leittechnik-Herstellern eine SBOM oder zumindest eine Aussage zu Eclipse Milo und libIEC61850?

Maßnahmen dieser Woche

1. BeyondTrust-Appliances patchen (BT26-05-RS), auf SAWFLY/BARECLAW und gelöschte Logs prüfen und alle im Vault gespeicherten Zugangsdaten wechseln.
2. PAN-OS auf Fixed Release bringen, GlobalProtect-Logs auf Auffälligkeiten durchsuchen und die Ports 4443/3879 des Management-Interfaces von außen testen.
3. VPN-Zugänge ohne MFA sperren und die im SafePay-Advisory genannten Edge-CVEs mit dem Asset-Inventar abgleichen.
4. Webserver auf S7-1500- und ET-200SP-CPUs abschalten oder auf das Engineering-Netz beschränken, bis Siemens Patches liefert.
5. Firmware-Stand aller RTU500-CMUs erfassen und das Update auf die Fix-Version laut Advisory (unter anderem 13.9.1) in die Wartungsplanung der Umspannwerke aufnehmen.

HINWEIS ZUR QUELLENLAGE

Bestätigt sind alle Meldungen über CISA-Primärquellen (ICSA-26-293-04/-05, ICSA-26-295-14, AA26-293A-Bulletin) und Unit 42. Für BeyondTrust stützt sich der Bericht auf Rapid7 und BleepingComputer; der CVSS-Wert ist widersprüchlich (CNA v4 9,3, NVD v3.1 laut Sekundärquelle 9,8, das Tagesbriefing nannte 9,1). Nicht aufgenommen wurden: WAGO OS Linux (ICSA-26-293-02 steht im CISA-Bulletin vom 20.10. (<https://content.govdelivery.com/accounts/USDHSCISA/bulletins/42fd2a7>), die Advisory-Seite liefert aber 404, und CVE-2026-80466/VDE-2026-096 ließen sich nicht an der Primärquelle prüfen), libIEC61850 CVE-2026-68907 (16.10., nur Sekundärquelle, Fix 1.6.2: <https://www.thehackerwire.com/vulnerability/CVE-2026-68907/>), Schneider Sage RTU (AV26-1051 vom 15.10., also vor dem Berichtszeitraum, Details nur im Herstellerdokument: <https://cyber.gc.ca/en/alerts-advisories/control-systems-schneider-electric-security-advisory-av26-1051>) sowie die Leak-Site-Meldungen zu Loxone und Passavant, die nur auf Täterangaben beruhen. Einen bestätigten Cyberangriff auf einen Netzbetreiber oder Energieversorger in DACH habe ich für KW 43 nicht gefunden. Alle Quellenlinks wurden am 23.10.2026 automatisch aufgerufen und inhaltlich geprüft. Am 23.10.2026 nach dem Qualitäts-Tor zusätzlich gegen Primärquellen geprüft (CISA, Rapid7/Mandiant, Unit 42, Loxone, Siemens) und korrigiert; nicht belegte Angaben wurden gestrichen.