

WOCHENBERICHT

OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 40/2026 · Strom und Energie in DACH

Zielgruppe	Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger
Berichtszeitraum	25.09.2026-02.10.2026
Version	1.0
Datum	02.10.2026
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 40/2026 ging das größte Risiko vom Fernzugang aus, also von Edge Devices für Remote Access und Standortvernetzung. In zwei Systemen werden Zero-Days aktiv ausgenutzt: Citrix NetScaler ADC/Gateway (CVE-2026-88771/-88772, CVSS v4.0 9.5, veröffentlicht am 27.09., BSI-Warnstufe 3 von 4) und Cisco Catalyst SD-WAN Manager (CVE-2026-76504, CVSS 9.8, veröffentlicht am 30.09.). CISA hat beide in den KEV-Katalog aufgenommen. Über diese Geräte binden Stadtwerke und Netzbetreiber oft Dienstleister für die Fernwartung, Leitstellen und Außenstellen an, und sie steuern die Segmentierung bis in die OT. Wer ein solches Gerät übernimmt, steht direkt vor der Netzleittechnik. Dazu kommen Lücken in Gateways und Routern, die oft in Ortsnetzstationen und Außenanlagen stecken: Lantronix G520 (Root-Rechte über manipulierte Updates) und MikroTik RouterOS (kritisch, CVSS v3.1 9.8, ohne Anmeldung).

Der Datenabfluss beim Zertifizierer GUTcert betrifft die deutsche Energiewirtschaft direkt. Rund 640 GB Auditunterlagen nach IT-Sicherheitskatalog 1a/1b sollen abgefließen sein, laut Fachpresse auch Netzpläne mit Standorten von Umspann- und Trafostationen. In dieser Woche haben sich weitere Betroffene gemeldet. Für die Schutztechnik meldet ABB zwei Lücken im IED-Engineering-Werkzeug PCM600, für die es bisher nur Workarounds gibt. Außerdem betroffen ist die Ladeplattform Monta. In Österreich gilt seit 01.10. das NISG 2026: Erhebliche Vorfälle sind innerhalb von 24 Stunden als Frühwarnung zu melden, registrieren müssen sich die Einrichtungen bis 31.12. Ransomware bleibt auf dem Jahreshöchststand, die Industrie ist am stärksten betroffen. Der wahrscheinlichste Weg in die OT führt damit weiter über die IT. Unterm Strich: Fernzugänge sofort patchen und forensisch prüfen, danach den Bestand an Gateways und Routern in der Fläche durchgehen.

GESAMTBEWERTUNG

Die Lage ist hoch. Mehrere Remote-Access- und WAN-Komponenten mit Weg in die OT werden aktiv angegriffen, und bei einem Dienstleister sind sensible Netzunterlagen der Branche abgefließen. Zuerst müssen NetScaler und SD-WAN Manager gepatcht und auf Kompromittierung geprüft werden (CC4/CC1/CC2). Danach folgt die Bestandsprüfung von PCM600, G520 und MikroTik (CC5).

Trends

- Edge Devices für Remote Access und WAN (Citrix NetScaler, Cisco SD-WAN) bleiben der wichtigste Weg für den Initial Access. Angegriffen wird schon vor Veröffentlichung der Patches, deshalb gehört zu jedem Patch eine Kompromittierungsprüfung. Allein bei Cisco SD-WAN ist es 2026 laut BleepingComputer der fünfte ausgenutzte Zero-Day.
- Ransomware ist auf dem Jahreshöchststand: Im August zählte Industrial Cyber weltweit 1.073 Angriffe (+12 % zum Juli), 31 % davon trafen die Industrie, Qilin war am aktivsten (Industrial Cyber, 28.09.). Stadtwerke bleiben über die IT unter Druck. Quelle: <https://industrialcyber.co/ransomware/ransomware-activity-hits-2026-high-as-industrial-sector-bears-31-of-attacks-and-qilin-dominates/>
- Angreifer nehmen zunehmend die Supply Chain rund um die OT ins Visier: Zertifizierer, Dienstleister und Partner halten Netzpläne und Zugänge der Betreiber (GUTcert, Adif/Renfe).
- Gateways und Router in der Fläche (LTE-Gateways, MikroTik) und Werkzeuge am Rand der OT (Schutztechnik-Engineering mit PCM600) werden zur Schwachstelle der dezentralen Energiewende, weil sie im Asset-Inventar oft fehlen.

- Ladeinfrastruktur und Cloud-Backends für dezentrale Anlagen rücken als neue OT-nahe Angriffsfläche in den Fokus.
- Die Regulierung wird verbindlich: In Österreich gilt das NISG 2026 seit 01.10., Meldefähigkeit innerhalb von 24 Stunden wird damit Pflicht.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Citrix NetScaler ADC/Gateway: zwei RCE-Zero-Days werden aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772)	KRITISCH	Citrix / CISA / BSI / Rapid7 / Palo Alto Unit 42 / Help Net Security, 27.09.
L-02	Cisco Catalyst SD-WAN Manager: Authentication Bypass wird aktiv ausgenutzt (CVE-2026-76504, CVSS 9.8)	KRITISCH	Cisco PSIRT / CISA KEV, 30.09.
L-03	Datenabfluss bei GUTcert: Auditunterlagen von Netz- und Kraftwerksbetreibern betroffen	HOCH	Borns IT- und Windows-Blog / energate messenger / IT-Administrator, 26.09.
L-04	Lantronix G520 Mobilfunk-Gateway: Root-Codeausführung über den Update-Mechanismus (ICSA-26-272-01)	HOCH	CISA (ICSA-26-272-01), 29.09.
L-05	Österreich: NISG 2026 ist seit 01.10. in Kraft	HOCH	WKO, 01.10.
L-06	ABB PCM600 (Engineering für Schutz- und Stationsleittechnik): Rechteausweitung und Path Traversal (ICSA-26-274-03)	MITTEL	CISA (ICSA-26-274-03) / ABB, 01.10.
L-07	MikroTik RouterOS: Root-Codeausführung ohne Anmeldung (CVE-2026-84411, ICSA-26-272-06, CVSS v3.1 9.8)	MITTEL	CISA (ICSA-26-272-06), 29.09.
L-08	Monta-Ladeplattform: WebSocket-Endpunkte ohne Authentifizierung, Ladestationen übernehmbar (ICSA-26-274-02, CVSS 9.4)	MITTEL	CISA (ICSA-26-274-02), 01.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 02.10.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt.

Region	Gesamt	Top-Protokolle
Deutschland	137008	DNP3: 33014, OMRON FINS: 23241, ProConOS: 16152
Österreich	4567	HMI/VNC: 1082, DNP3: 964, IEC-104: 450

Meldungen im Detail

L-01 Citrix NetScaler ADC/Gateway: zwei RCE-Zero-Days werden aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772)

KRITISCH Citrix / CISA / BSI / Rapid7 / Palo Alto Unit 42 / Help Net Security, 27.09.

Was ist neu: Citrix hat am 27.09. acht Schwachstellen in NetScaler ADC und Gateway veröffentlicht. Zwei davon erlauben Remote Code Execution ohne Anmeldung (CVSS v4.0 9.5). Beide wurden schon vor der Veröffentlichung als Zero-Days ausgenutzt: Laut Palo Alto Unit 42 liefen Scans ab 21.08., die Ausnutzung ab 04.09., und auf ungepatchten Systemen wurden Webshells gefunden. Auch die Standardkonfiguration ist betroffen. CISA hat am 27.09. gewarnt und beide Lücken am selben Tag in den KEV-Katalog aufgenommen, das BSI warnt seit 28.09. mit Stufe 3 von 4.

Bedeutung: NetScaler ist bei Stadtwerken und Netzbetreibern in DACH oft das zentrale VPN- und Remote-Access-Gateway, auch für die Fernwartung durch Dienstleister und Leitstellen. Wer das Gateway übernimmt, kann mit gültigen Sessions und Zugangsdaten per Lateral Movement in Richtung Leitstelle und OT vordringen. Weil die Angriffe schon vor dem Patch liefen, reicht Patchen allein nicht.

Empfehlung: Sofort auf 14.1-73.37 bzw. 13.1-64.23 (FIPS: 13.1-37.279) aktualisieren oder die Appliance bis dahin vom Netz nehmen. Alle Sessions beenden, Speicher und Logs der letzten vier Wochen sichern und die Zugangsdaten tauschen, die über das Gateway genutzt wurden (CC4). Danach per Threat Hunting nach Webshells, ungewöhnlichen Anmeldungen und auffälligen User-Agent-Strings suchen und den Incident-Response-Plan für den Fall einer Kompromittierung bereithalten (CC1).

Quelle: <https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-citrix-netscaler-adc-and-gateway-cve-2026-88771-and-cve-2026-88772/> ✓ geprüft

L-02 Cisco Catalyst SD-WAN Manager: Authentication Bypass wird aktiv ausgenutzt (CVE-2026-76504, CVSS 9.8)

KRITISCH Cisco PSIRT / CISA KEV, 30.09.

Was ist neu: Mit einer URI-kodierten Anfrage (`%6a` statt `j` in `j\_security\_check`) bekommt ein Angreifer ohne Zugangsdaten Admin-Rechte über die API. Die Lücke wird seit September ausgenutzt und betrifft alle Konfigurationen, auch Systeme, die gegen die SD-WAN-Lücken aus Mai und Juni gepatcht sind. Einen Workaround gibt es nicht. Gepatcht sind die Versionen 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 und 26.2.1. CISA hat die Lücke am 30.09. in den KEV-Katalog aufgenommen (Frist für US-Bundesbehörden: 03.10.). Laut BleepingComputer ist es der fünfte ausgenutzte SD-WAN-Zero-Day in diesem Jahr.

Bedeutung: Wer den SD-WAN Manager kontrolliert, kann Routing und Segmentierung zwischen Leitstelle, Stationen und Außenstellen umbauen, bis in die Netze der Netzleittechnik und Fernwirktechnik. Damit wird die Defensible Architecture selbst angreifbar. Betroffen sind vor allem größere Stadtwerke und Netzbetreiber, die ihre Standorte per SD-WAN verbinden.

Empfehlung: Sofort auf eine gefixte Version aktualisieren und den Manager bis dahin nur aus Admin-Netzen bzw. von vertrauenswürdigen Hosts erreichbar machen (CC2). serviceproxy-access.log und vmanage-server.log nach URI-kodierten Anfragen an `j\_security\_check` (/`%6a\_security\_check`) und nach Konten mit dem Präfix „viptela-reserved-“ durchsuchen (CC3).

Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU> ✓ geprüft

L-03 Datenabfluss bei GUTcert: Auditunterlagen von Netz- und Kraftwerksbetreibern betroffen

HOCH Borns IT- und Windows-Blog / energate messenger / IT-Administrator, 26.09.

Was ist neu: Beim Berliner Zertifizierer GUTcert sind seit dem 05.09. rund 640 GB Daten abgeflossen. Laut Fachpresse sind darunter Auditberichte, Anlagenlisten und Netzpläne mit Standorten von Trafostationen und Gas-Druckregelanlagen. In dieser Woche wurden weitere Betroffene bekannt (u. a. Entega, 24.09.). GUTcert hat zwei Erpressungsversuche abgelehnt, eine Veröffentlichung der Daten gilt als wahrscheinlich.

Bedeutung: GUTcert zertifiziert Betreiber nach IT-Sicherheitskatalog 1a (Energienetze) und 1b (Erzeugungsanlagen). Angreifer können so Beschreibungen von Architektur, Segmentierung und Schwachstellen genau der Zielgruppe in die Hand bekommen. Das ist ein Supply-Chain-Risiko, das die Planung von Angriffen auf Umspannwerke und Stationen erleichtert.

Empfehlung: Bei GUTcert schriftlich klären, welche eigenen Unterlagen betroffen sind, und die Meldepflichten nach DSGVO, BSIG und NIS2 prüfen. Die in den Auditunterlagen beschriebenen Zugänge und Schwachstellen so behandeln, als wären sie öffentlich: vorrangig schließen und Zugangsdaten wechseln.

Quelle: <https://borncity.com/blog/2026/09/26/cybervorfaelle-flink-lieferservice-entega-energieversorger-clean-fix-reinigungstechnik/> ✓ geprüft

L-04 Lantronix G520 Mobilfunk-Gateway: Root-Codeausführung über den Update-Mechanismus (ICSA-26-272-01)

HOCH CISA (ICSA-26-272-01), 29.09.

Was ist neu: Die Firmware 2.6.0.4R6_stable hat zwei Schwachstellen (CVE-2026-84409, CVE-2026-91191, jeweils CVSS v3.1 7.5 / v4 7.7). Die Update-Metadaten kommen unverschlüsselt per HTTP, und die Signatur der Firmware ist nicht wirksam abgesichert: Berichten zufolge liegt der private Schlüssel, dem die Firmware vertraut, im öffentlichen SDK bzw. wird die Signatur nicht richtig geprüft. Ein Angreifer kann so eigene Software mit Root-Rechten einspielen. CISA nennt Energie sowie Wasser und Abwasser als betroffene Sektoren. Eine Ausnutzung ist bisher nicht bekannt.

Bedeutung: LTE-Gateways binden in DACH viele Ortsnetzstationen, Erneuerbare-Anlagen und Messstellen an die Fernwirktechnik an. Ein manipuliertes Gateway sitzt direkt vor der RTU bzw. dem Endpunkt für IEC 60870-5-104 und kann den Fernwirkverkehr mitlesen oder verändern.

Empfehlung: Alle G520 im Asset-Inventar erfassen und auf 2.6.0.7R6 aktualisieren. Updates nur über einen geprüften internen Pfad bzw. aus vertrauenswürdigen Quellen zulassen und den Datenverkehr der Gateways auf unerwartete Ziele überwachen (CC5).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-272-01> ✓ geprüft

L-05 Österreich: NISG 2026 ist seit 01.10. in Kraft

HOCH WKO, 01.10.

Was ist neu: Das NISG 2026 (österreichische Umsetzung von NIS2) gilt seit 01.10.2026 vollständig, für die materiellen Pflichten ohne Übergangsfrist. Wesentliche und wichtige Einrichtungen, darunter der Energiesektor, müssen sich bis 31.12.2026 über das USP registrieren. Erhebliche Vorfälle sind innerhalb von 24 Stunden als Frühwarnung an das CSIRT zu melden. Zuständig ist die Cybersicherheitsbehörde im BMI.

Bedeutung: Österreichische Energieversorger und Netzbetreiber sind ab sofort zu Risikomanagement und Meldung verpflichtet. Die Geschäftsleitung hat eine Aufsichts- und Schulungspflicht (§ 31 NISG); eine persönliche Haftung ergibt sich aus GmbHG/AktG. Würden die Zero-Days dieser Woche zu einer Kompromittierung führen, wäre diese bereits meldepflichtig.

Empfehlung: Registrierung einplanen. Meldeweg und Entscheidungskriterien für die 24-Stunden-Frühwarnung im Incident-Response-Plan festlegen und üben (CC1).

Quelle: <https://www.wko.at/it-sicherheit/nis-faq> ✓ geprüft

L-06 ABB PCM600 (Engineering für Schutz- und Stationsleittechnik): Rechteausweitung und Path Traversal (ICSA-26-274-03)

MITTEL CISA (ICSA-26-274-03) / ABB, 01.10.

Was ist neu: PCM600 bis Version 2.14 hat zwei Schwachstellen mit Schweregrad mittel bis hoch (bis 7.1 nach CVSS v4). Bei CVE-2026-15952 läuft der Scheduler Service als LocalSystem, lokale Nutzer können so ihre Rechte ausweiten. Bei CVE-2026-15953 (Path Traversal) können über Archivdateien Dateien außerhalb des Zielordners geschrieben werden. CISA nennt keinen Patch, nur Workarounds, und ordnet die Lücken dem Sektor Energie zu. Eine Ausnutzung ist nicht bekannt.

Bedeutung: Mit PCM600 parametrieren Betreiber ABB-Relion-Schutzgeräte (IEDs) in Umspannwerken. Wer die Engineering-Workstation übernimmt, kann Schutzeinstellungen und IEC-61850-Konfigurationen manipulieren. Ein Angriff setzt lokalen Zugriff voraus, der nach einem Initial Access über die IT aber realistisch ist.

Empfehlung: Den ABBPCMSchedulerService unter demselben Windows-Konto wie PCM600 betreiben, die IED-Authentifizierung aktivieren und das Zertifikatsvertrauen auf die Stationsumgebung begrenzen. Projekt- und Archivdateien nur aus vertrauenswürdigen Quellen öffnen (ABB 2NGA003170/2NGA003179, CC5). Engineering-Workstations nur im Schutztechnik-Netz betreiben und eng segmentieren (CC2), Konfigurationsänderungen an IEDs überwachen (CC3).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-03> ✓ geprüft

L-07 MikroTik RouterOS: Root-Codeausführung ohne Anmeldung (CVE-2026-84411, ICSA-26-272-06, CVSS v3.1 9.8)

MITTEL CISA (ICSA-26-272-06), 29.09.

Was ist neu: Ein Integer-Underflow im Web-Management bei HTTP-Anfragen erlaubt mit einer einzigen Anfrage Root-Codeausführung oder das Lahmlegen des Geräts. Betroffen sind alle Versionen vor 7.24. Laut CISA wird die Lücke bisher nicht ausgenutzt. CISA ordnet sie den Sektoren Kommunikation und IT zu, nicht direkt der Energie.

Bedeutung: MikroTik-Router laufen bei kleineren Versorgern oft unbemerkt in Außenstellen und Stationen, manchmal von Dienstleistern eingebaut. Erfahrungsgemäß werden MikroTik-Lücken schnell massenhaft angegriffen, und die Geräte dienen danach oft als Botnetz- oder C2-Infrastruktur.

Empfehlung: Alle MikroTik-Geräte erfassen, auch die von Dienstleistern, und auf RouterOS 7.24 oder neuer aktualisieren. Das Web-Management aus OT- und Internet-Netzen herausnehmen und nur aus dem Management-Netz erreichbar machen (CC5/CC2).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-272-06> ✓ geprüft

L-08 Monta-Ladeplattform: WebSocket-Endpunkte ohne Authentifizierung, Ladestationen übernehmbar (ICSA-26-274-02, CVSS 9.4)

MITTEL CISA (ICSA-26-274-02), 01.10.

Was ist neu: In allen Versionen von monta.app gibt es vier Schwachstellen. Darunter sind fehlende Authentifizierung an den WebSocket-Endpunkten (CVE-2026-95102, CVSS 9.4), vorhersagbare Session-IDs und öffentlich einsehbare Zugangsdaten. Angreifer könnten sich als Ladestation ausgeben, Ladepunkte administrativ übernehmen oder den Dienst lahmlegen. Eine Ausnutzung ist nicht bekannt. Monta führt OCPP 1.6 Security Profile 2 und Rate Limiting ein.

Bedeutung: Stadtwerke betreiben zunehmend öffentliche Ladeinfrastruktur über Cloud-Backends europäischer Anbieter. Werden viele Ladepunkte gleichzeitig gesteuert, entsteht ein Lastrisiko für die Netzstabilität im Verteilnetz, dazu kommt der Reputationsschaden.

Empfehlung: Klären, ob Monta oder ein vergleichbares Backend direkt oder über Dienstleister genutzt wird. Vom Anbieter den Stand der Fixes, OCPP Security Profile 2 oder höher und einen Nachweis der Behebung verlangen (CC5). OCPP-Backends ins Asset-Inventar aufnehmen und auf auffällige Verbindungen überwachen (CC3).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02> ✓ geprüft

Fragen für das nächste Jour fixe

1. Haben wir NetScaler oder Cisco SD-WAN Manager im Einsatz? Sind alle Instanzen gepatcht, und hat jemand nach einer möglichen Kompromittierung gesucht (nicht nur gepatcht)?
2. Welche Fernwartungszugänge von Dienstleistern laufen über diese Gateways, und können wir im Notfall alle Remote-Access-Pfade in die OT sofort und kontrolliert schließen (Incident-Response-Playbook)?
3. Welche unserer Unterlagen lagen bei GUTcert oder anderen Auditoren, und welche der darin beschriebenen Schwachstellen sind noch offen?

4. Sind PCM600-Arbeitsplätze, LTE-Gateways und MikroTik-Router vollständig im Asset-Inventar erfasst, auch die von Dienstleistern verbauten?
5. Wer darf PCM600 und andere Engineering-Werkzeuge der Schutztechnik nutzen, und würden wir Parameteränderungen an IEDs bemerken?
6. Würden wir einen Incident an der Grenze zwischen IT und OT innerhalb von 24 Stunden erkennen und melden (NISG 2026, NIS2-Umsetzung in DE)?
7. Welche Cloud-Backends steuern unsere Ladeinfrastruktur oder Erzeugungsanlagen, und welche Sicherheitsnachweise haben wir von den Anbietern?

Maßnahmen dieser Woche

1. Citrix NetScaler sofort auf 14.1-73.37/13.1-64.23 (FIPS: 13.1-37.279) patchen. Alle Sessions beenden, Logs der letzten vier Wochen sichern, Zugangsdaten tauschen und nach Webshells oder ungewöhnlichen Anmeldungen suchen.
2. Cisco SD-WAN Manager auf die gefixte Version bringen und bis dahin nur aus Admin-Netzen bzw. von vertrauenswürdigen Hosts erreichbar machen. Die Logs nach `%6a\_security\_check` und nach Konten mit dem Präfix „viptela-reserved-“ durchsuchen.
3. Bei GUTcert die eigene Betroffenheit klären, Meldepflichten nach DSGVO, BSIG und NIS2 prüfen und die in Auditunterlagen dokumentierten Schwachstellen vorrangig schließen.
4. Bestand an Lantronix G520 und MikroTik ermitteln, auch bei Dienstleistern, und auf 2.6.0.7R6 bzw. RouterOS 7.24 oder neuer aktualisieren.
5. Bei PCM600 das Scheduler-Dienstkonto umstellen, die IED-Authentifizierung aktivieren, Engineering-Arbeitsplätze segmentieren und Konfigurationsänderungen an IEDs überwachen.
6. Österreichische Gesellschaften: NISG-Registrierung bis 31.12. einplanen und den 24-Stunden-Meldeweg im Incident-Response-Plan verankern.
7. Fernwartungszugänge im Netzwerk-Monitoring sichtbar machen: Wer greift wann von welchem Gateway auf das OT-Netz zu?

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 02.10.2026 automatisch aufgerufen und inhaltlich geprüft. Am 02.10.2026 zusätzlich per Doppel-Recherche faktengeprüft und korrigiert.