

WOCHENBERICHT

OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 40/2026 · Strom und Energie in DACH

Zielgruppe	Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger
Berichtszeitraum	24.09.2026-01.10.2026
Version	1.0
Datum	01.10.2026
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 waren vor allem Systeme betroffen, über die Dienstleister, Leitstellen und Außenstellen auf das Netz zugreifen. Zwei Zero-Days in Citrix NetScaler ADC/Gateway werden weltweit aktiv ausgenutzt (CISA, 27.09.). Am 30.09. hat CISA außerdem eine Schwachstelle im Cisco Catalyst SD-WAN Manager in den KEV-Katalog aufgenommen, weil sie aktiv angegriffen wird. Mit beiden Produkten binden viele Netzbetreiber und Stadtwerke Standorte und Fernwartung an. Wer sie übernimmt, steht an der Grenze zur Netzleittechnik oder kann die Segmentierung umbauen. Dazu kommen neue Advisories für Mobilfunk-Gateways (Lantronix G520) und MikroTik-Router. Solche Geräte binden in DACH häufig Ortsnetzstationen, Erzeugungsanlagen und Außenstationen an.

Mit Entega gibt es einen Fall in der DACH-Energiebranche: Laut Bericht vom 24.09. sind Daten des Darmstädter Versorgers beim Berliner Zertifizierer GUTcert wohl abgeflossen. Entega selbst wurde nicht angegriffen. Der Fall zeigt, dass Daten bei Dienstleistern, Prüfern und Zertifizierern zum eigenen Risiko gehören. Der Ransomware-Druck bleibt außerdem auf Rekordniveau: Im August gab es laut Industrial Cyber 1.073 Angriffe, 31 % davon auf die Industrie. Kleine Teams sollten sich deshalb nicht verzetteln, sondern Secure Remote Access (CC4) und Risk-Based Vulnerability Management (CC5) zuerst angehen. Mit KI-Unterstützung lassen sich Inventarabgleich und Log-Sichtung auch mit wenig Personal schaffen.

GESAMTBEWERTUNG

Die Lage ist hoch, weil Zero-Days in Remote-Access- und WAN-Komponenten aktiv ausgenutzt werden, die bei der Zielgruppe weit verbreitet sind. Vorrang haben das Patchen von NetScaler und SD-WAN Manager und die Suche nach Spuren einer Kompromittierung, noch vor allen anderen Advisories.

Trends

- Angreifer zielen weiter vor allem auf Edge-Geräte und Remote-Access-Komponenten (NetScaler, SD-WAN, Router, LTE-Gateways), denn sie sind der kürzeste Weg zur OT.
- Die Lieferkette wird breiter angegriffen: Neben Herstellern und Integratoren geraten auch Zertifizierer und Prüfer ins Visier, siehe Entega/GUTcert.
- Kritische Schwachstellen in OT-Umgebungen bleiben laut Holm Security (29.09.) im Schnitt über drei Jahre ungepatcht, deshalb kommt es auf risikobasierte Priorisierung an.
- Der Ransomware-Druck auf Industrie und Versorger steigt weiter und trifft die OT vor allem indirekt über ausfallende IT-Prozesse.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Citrix NetScaler ADC/Gateway: zwei Zero-Days werden aktiv ausgenutzt (CVE-2026-88771, -88772)	KRITISCH	CISA, 27.09.
L-02	Cisco Catalyst SD-WAN Manager: Schwachstelle CVE-2026-76504 wird aktiv ausgenutzt und steht im KEV-Katalog	KRITISCH	CISA, 30.09.

ID	Meldung	Relevanz	Quelle
L-03	Entega: Daten über Hack beim Zertifizierer GUTcert wohl abgeflossen	HOCH	Borns IT- und Windows-Blog (mit Verweis auf Frankfurter Rundschau), 24.09.
L-04	Lantronix G520 Mobilfunk-Gateway: Root-Codeausführung über manipulierte Updates (ICSA-26-272-01)	HOCH	CISA, 29.09.
L-05	MikroTik RouterOS: Codeausführung ohne Anmeldung, CVSS 9.8 (ICSA-26-272-06)	HOCH	CISA, 29.09.
L-06	Ransomware auf 2026-Höchststand, Industrie trägt 31 % der Angriffe	ORIENTIERUNG	Industrial Cyber, 28.09.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 01.10.2026):

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 Zero-Days werden aktiv ausgenutzt (CVE-2026-88771, -88772)

KRITISCH CISA, 27.09.

Was ist neu: Citrix hat acht Schwachstellen in NetScaler ADC und Gateway veröffentlicht (CVE-2026-88771 bis -88778). Zwei davon erlauben jeweils für sich Remote Code Execution und wurden schon als Zero-Day ausgenutzt. CISA meldet aktive Angriffe weltweit.

Bedeutung: Viele Stadtwerke und Netzbetreiber nutzen NetScaler als Gateway für die Fernwartung durch Hersteller und Dienstleister. Ein kompromittiertes Gateway ist ein direkter Initial Access in Richtung Netzleittechnik und Stationsleittechnik.

Empfehlung: Vor dem Patch nach Indicators of Compromise suchen und Beweise sichern, denn ein Update kann die Spuren löschen. Danach patchen, alle aktiven Sessions beenden und die Zugangsdaten der Fernwartungskonten rotieren (CC4, CC1).

Quelle: <https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netScaler-adc-gateway> ✓ geprüft

L-02 Cisco Catalyst SD-WAN Manager: Schwachstelle CVE-2026-76504 wird aktiv ausgenutzt und steht im KEV-Katalog

KRITISCH CISA, 30.09.

Was ist neu: CISA hat CVE-2026-76504 (Cisco Catalyst SD-WAN Manager, „Hex Encoding Vulnerability“) am 30.09. wegen aktiver Ausnutzung in den KEV-Katalog aufgenommen. Laut Tagesbriefing bekommt ein Angreifer damit ohne Anmeldung Admin-Rechte über die API. Einen Workaround gibt es nicht, nur Updates.

Bedeutung: Wer den SD-WAN Manager übernimmt, kann Routing und Segmentierung bis in die OT-Netze ändern. Damit fällt eine zentrale Schutzschicht der Defensible Architecture weg.

Empfehlung: Auf eine gefixte Version aktualisieren und den Manager nur aus einem Management-Netz mit vertrauenswürdigen Hosts erreichbar machen. Außerdem die Logs nach auffälligen, URL-kodierten Anfragen an die Anmeldeschnittstelle durchsuchen (CC2, CC3).

Quelle:

<https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog> ✓ geprüft

L-03 Entega: Daten über Hack beim Zertifizierer GUTcert wohl abgeflossen

HOCH Borns IT- und Windows-Blog (mit Verweis auf Frankfurter Rundschau), 24.09.

Was ist neu: Der Darmstädter Energieversorger Entega wurde über einen Angriff auf den Berliner Zertifizierer GUTcert informiert, der Anfang September stattfand. Daten von Entega, die dort lagen, sind laut Bericht wohl abgeflossen. Entega selbst wurde nicht angegriffen.

Bedeutung: Bei Zertifizierern und Auditoren liegen oft Netzpläne, Asset-Listen und Sicherheitskonzepte. Für Angreifer ist das Material zur Vorbereitung eines Angriffs. Weitere Energieversorger mit Kontakt zu GUTcert könnten ebenfalls betroffen sein.

Empfehlung: Bei GUTcert und anderen Prüfdienstleistern aktiv nachfragen, ob eigene Daten betroffen sind. Prüfen, welche OT-Unterlagen bei Dritten liegen, und künftig nur das Nötigste und das verschlüsselt übergeben (CC1, CC5).

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 manipulierte Updates (ICSA-26-272-01)

HOCH CISA, 29.09.

Was ist neu: Zwei Schwachstellen in der Firmware 2.6.0.4R6_stable (CVE-2026-84409, CVE-2026-91191, CVSS 7.5–7.7) betreffen die unverschlüsselten Update-Metadaten und die fehlerhafte Prüfung der Signatur. Ein Angreifer kann so eigene Software mit Root-Rechten einspielen. CISA nennt ausdrücklich den Energiesektor.

Bedeutung: LTE-Gateways binden häufig Ortsnetzstationen, PV- und Windparks oder Messstellen an die Leittechnik an. Ein manipuliertes Gateway kann die Kommunikation, etwa nach IEC 60870-5-104, mitlesen oder verändern.

Empfehlung: Im Asset-Inventar nach G520 suchen und die Firmware aktualisieren. Updates nur über einen vertrauenswürdigen Pfad beziehen und die Gateways nur per VPN erreichbar machen (CC5, CC4).

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

L-05 MikroTik RouterOS: Codeausführung ohne Anmeldung, CVSS 9.8 (ICSA-26-272-06)

HOCH CISA, 29.09.

Was ist neu: Durch einen Integer-Underflow im Web-Management (CVE-2026-84411) reicht eine präparierte HTTP-Anfrage für Remote Code Execution oder Denial of Service. Betroffen sind alle Versionen unter 7.24. CISA sind bisher keine Angriffe bekannt.

Bedeutung: MikroTik-Router sind bei kleineren Versorgern und Dienstleistern als günstige Edge-Geräte verbreitet. Frühere MikroTik-Schwachstellen wurden schnell für Botnetze und als Sprungbrett genutzt.

Empfehlung: Auf 7.24 aktualisieren und das Web-Management nur aus dem Management-Netz erreichbar machen. Auch MikroTik-Geräte bei Dienstleistern und Errichtern abfragen (CC5, CC2).

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

L-06 Ransomware auf 2026-Höchststand, Industrie trägt 31 % der Angriffe

ORIENTIERUNG Industrial Cyber, 28.09.

Was ist neu: Im August gab es weltweit 1.073 Ransomware-Angriffe, 12 % mehr als im Juli. 329 davon (31 %) trafen die Industrie, Qilin war die aktivste Gruppe.

Bedeutung: Für Stadtwerke bleibt der Druck über die IT hoch. Fallen die IT-Systeme aus, leidet auch der Netzbetrieb, etwa beim Arbeitsmanagement, bei Störungsmeldungen und beim Abrechnungs- und Messwesen.

Empfehlung: Einen ICS-Incident-Response-Plan mit dem Szenario „IT verschlüsselt, Leittechnik läuft“ üben. Dabei klären, wann die IT/OT-Kopplung getrennt wird (CC1).

Quelle: <https://industrialcyber.co/ransomware/ransomware-activity-hits-2026-high-as-industrial-sector-bears-31-of-attacks-and-qilin-dominates/> ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Den gesamten Remote Access von Dienstleistern über einen zentralen, überwachten Jump Host mit MFA und zeitlich begrenzter Freigabe bündeln. Direkte Gateways in die OT abschaffen. [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	SD-WAN- und Firewall-Management in ein getrenntes Management-Netz verlegen und Änderungen an Routing und Segmentierung automatisch melden lassen. [CC2 Defensible Architecture]	L-02	HOCH	0–3 Monate
M-03	Ein Asset-Inventar für Edge-Geräte (LTE-Gateways, Router, APs) aufbauen und die Advisories wöchentlich, KI-gestützt, nach KEV-Status und OT-Nähe abgleichen. [CC5 Risk-Based Vulnerability Management]	L-04	HOCH	0–3 Monate

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-04	Passives Netzwerk-Monitoring an den Übergängen zu Außenstationen einführen (IEC 60870-5-104, IEC 61850), damit neue Verbindungen und Befehle erkannt werden. [CC3 ICS Network Visibility & Monitoring]	L-04	MITTEL	3–6 Monate
M-05	Den ICS-Incident-Response-Plan um die Szenarien „IT verschlüsselt“ und „Dienstleister kompromittiert“ ergänzen und mit der Netzleitstelle als Tabletop üben. [CC1 ICS Incident Response]	L-03	MITTEL	0–3 Monate

Fragen für das nächste Jour fixe

1. Wissen wir vollständig, welche NetScaler-, Cisco-SD-WAN-, MikroTik- und Lantronix-Geräte bei uns und bei unseren Dienstleistern laufen?
2. Haben wir NetScaler und SD-WAN Manager vor dem Patchen auf Kompromittierung geprüft, und wer bewertet das Ergebnis?
3. Welche Netzpläne, Asset-Listen und Sicherheitskonzepte liegen bei Zertifizierern, Auditoren und Errichtern, und wie sind sie geschützt?
4. Würden wir einen unberechtigten Zugriff auf die Fernwirk-Gateways der Außenstationen in unserem OT-Monitoring erkennen?
5. Wann haben wir zuletzt den Betrieb der Netzleitstelle bei vollständig ausgefallener Office-IT geübt?

Maßnahmen dieser Woche

1. NetScaler ADC/Gateway: Indicators of Compromise prüfen, Forensik sichern, patchen, alle Sessions beenden und die Zugangsdaten der Fernwartung rotieren.
2. Cisco Catalyst SD-WAN Manager aktualisieren, nur aus dem Management-Netz erreichbar machen und die API-Logs auf auffällige Anmeldeanfragen prüfen.
3. Im Asset-Inventar nach Lantronix G520 und MikroTik RouterOS suchen und auf Firmware 2.6.0.7R6 bzw. RouterOS 7.24 aktualisieren, Web-Management nicht aus dem Internet erreichbar machen.
4. WatchGuard Access Points in Umspannwerken und Betriebsgebäuden auf Firmware 3.4.8 bringen und ihre Management-Schnittstellen vom OT-Netz trennen.
5. Bei GUTCert und anderen Zertifizierern und Auditoren nachfragen, ob eigene Daten betroffen sind, und erfassen, welche OT-Unterlagen bei Dritten liegen.

HINWEIS ZUR QUELLENLAGE

Die Meldungen zu Citrix, Cisco, Lantronix und MikroTik sind gegen die CISA-Primärquellen geprüft. Die Industrial-Cyber-Zahlen stammen aus dem Tagesbriefing, der Artikel selbst war nicht abrufbar (HTTP 403). Den Entega-Fall belegt nur ein Blog mit Verweis auf die Frankfurter Rundschau, der Umfang der betroffenen Daten ist unbestätigt. Nicht aufgenommen wurden: der CenterPoint-Datenabfluss (USA, Angaben des Angreifers nur teilweise bestätigt), Stadtwerke Landsberg (vor dem Berichtszeitraum, Quellen nennen 01.09. bzw. 08.09.) und die Siemens-Advisories vom 22.09. (vor dem Berichtszeitraum, trotzdem Bestand prüfen). Der Abgleich mit Gemini ist für diesen Bericht nicht erfolgt, in einem Briefing war Gemini ausgefallen. Alle Quellenlinks wurden am 01.10.2026 automatisch aufgerufen und inhaltlich geprüft.