

WOCHENBERICHT

OT-/Cyber-Lagebild Kommunale Versorger und KRITIS

Ausgabe KW 40/2026 · Kommunale Versorger und KRITIS in DACH

Zielgruppe	Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber
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 Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 40/2026 wurden mehrere Edge-Geräte gleichzeitig angegriffen, über die Stadtwerke und Wasserbetriebe Fernwartung, Remote Access und die Anbindung ihrer Standorte betreiben. Citrix hat am 27.09. acht Lücken in NetScaler ADC und Gateway veröffentlicht. Zwei davon (CVE-2026-88771 und -88772, CVSS v4.0 9.5) erlauben Remote Code Execution ohne Anmeldung und wurden schon vor der Veröffentlichung ausgenutzt. CISA hat beide am 27.09. in den KEV-Katalog aufgenommen, und das BSI warnt seit 28.09. mit Stufe 3 von 4 („sehr hoch“). Am 30.09. kam ein Auth-Bypass im Cisco Catalyst SD-WAN Manager dazu (CVE-2026-76504, CVSS 9.8). Er wird aktiv ausgenutzt, und es gibt keinen Workaround. Außerdem hat CISA eine kritische Lücke in MikroTik RouterOS (CVE-2026-84411, CVSS v3.1 9.8) sowie Lücken im Lantronix-Mobilfunk-Gateway G520 gemeldet. Für den G520 nennt CISA Energie sowie Wasser und Abwasser als betroffene Sektoren. Dazu kommen Lücken in WatchGuard Access Points und im ABB PCM600, dem Engineering-Werkzeug für die Schutztechnik.

In DACH wurde in dieser Woche kein Vorfall öffentlich bekannt, der die Versorgung selbst getroffen hat. Kommunale Einrichtungen werden aber konkret angegriffen. Die Webseiten der KVV Kassel haben Schadcode an Besucher verteilt. Die Stadt Wien hat am 30.09. einen Datenabfluss von rund 26.000 Dokumenten bestätigt, und die ausgenutzte Lücke war vorher in einem Forum zum Kauf angeboten worden. Entega ist indirekt über einen Dienstleister betroffen. Ransomware erreichte im August mit 1.073 Angriffen den höchsten Stand des Jahres, 31 % davon trafen die Industrie. Laut Holm Security bleiben kritische OT-Lücken im Schnitt über drei Jahre offen. Vorrang haben diese Woche ein sicherer Remote Access (CC4) mit Patchen, Threat Hunting und dem Beenden laufender Sessions. Danach folgen das Asset-Inventar der Edge-Geräte und ein risikobasiertes Schwachstellenmanagement (CC5). Beides können auch kleine Teams umsetzen.

GESAMTBEWERTUNG

Die Lage ist hoch. Mehrere Zero-Days in Fernzugangs- und WAN-Komponenten an der Grenze zwischen IT und OT werden aktiv ausgenutzt, und genau diese Komponenten sind bei Versorgern verbreitet. Vor allen anderen Patches gilt: Citrix NetScaler und Cisco SD-WAN Manager sofort auf Kompromittierung prüfen, patchen und die Sessions beenden. Danach den Bestand an MikroTik- und Lantronix-Geräten in den Außenstationen prüfen.

Trends

- Angreifer nehmen gezielt Edge-Geräte für Remote Access und WAN an der Grenze zwischen IT und OT ins Visier, etwa Citrix-VPN-Gateways, Cisco-SD-WAN-Controller, MikroTik-Router und Lantronix-Mobilfunk-Gateways. Darüber kommen sie ohne Phishing in die Netze der Versorger.
- Zwischen Ausnutzung und Patch liegen oft Wochen: Bei NetScaler und Cisco SD-WAN begannen die Angriffe vor der Veröffentlichung. Zu jedem Patch gehört deshalb eine Prüfung auf Kompromittierung.
- Für kommunale Versorger bleibt Ransomware über die IT das häufigste Szenario mit spürbaren Folgen. In Landsberg lief die Versorgung weiter, aber Verwaltung und Kundenservice fielen aus.
- Außenstationen mit LTE-Gateways und günstigen Routern (Lantronix, MikroTik) sind ein wachsender Angriffsweg in Wasser- und Stromnetzen, der oft schlecht inventarisiert ist.

- Datenabflüsse bei Kommunen und Dienstleistern (Wien, Entega über GUTcert, Berlin/Rhysida) bringen OT-relevante Planungsunterlagen in Umlauf, auch wenn die Versorgung selbst nicht betroffen ist.
- Initial Access Broker verkaufen Zugänge zu öffentlichen Einrichtungen. Threat Intelligence und Meldewege zu CERT.at, BSI und NCSC gehören deshalb zur Frühwarnung.
- In den USA greifen Angreifer weiter Wasser-SPS an, die direkt aus dem Internet erreichbar sind. Dieses Muster sollten auch kleine Wasserversorger in DACH ernst nehmen.
- Die OT-Patchlage bleibt strukturell schwach. Wer konsequent risikobasiert priorisiert und Lücken mit Segmentierung und Monitoring ausgleicht, ist klar im Vorteil.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Citrix NetScaler ADC/Gateway: zwei Zero-Days mit Remote Code Execution werden aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772)	KRITISCH	CISA / Citrix CTX697096 / BSI, 27.09.
L-02	Cisco Catalyst SD-WAN Manager: Auth-Bypass wird als Zero-Day ausgenutzt (CVE-2026-76504, CVSS 9.8)	KRITISCH	Cisco PSIRT / CISA KEV / BleepingComputer / Help Net Security, 30.09.
L-03	MikroTik RouterOS: Root-Codeausführung ohne Anmeldung mit einer einzigen Anfrage (CVE-2026-84411, CVSS v3.1 9.8)	HOCH	CISA ICSA-26-272-06, 29.09.
L-04	Lantronix G520 Mobilfunk-Gateway: Root-Codeausführung über manipulierte Updates (ICSA-26-272-01, CVE-2026-84409, CVE-2026-91191)	HOCH	CISA ICSA-26-272-01, 29.09.
L-05	Ransomware auf Jahreshöchststand: 1.073 Angriffe im August, 31 % gegen die Industrie	HOCH	Industrial Cyber, 28.09.
L-06	Stadt Wien: rund 26.000 Dokumente abgeflossen, die Lücke wurde vorher in einem Forum angeboten	MITTEL	ORF Wien, 30.09.
L-07	KVV Kassel: Schadcode auf den Webseiten eines kommunalen Versorgers	MITTEL	Security-Insider, 30.09.
L-08	ABB PCM600 (IED-Manager für Schutztechnik): Rechteausweitung und Dateiüberschreibung (CVE-2026-15952, CVE-2026-15953)	MITTEL	CISA ICSA-26-274-03, 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

Region	Gesamt	Top-Protokolle
Österreich	4567	HMI/VNC: 1082, DNP3: 964, IEC-104: 450

Meldungen im Detail

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

KRITISCH CISA / Citrix CTX697096 / BSI, 27.09.

Was ist neu: Citrix hat am 27.09. acht Lücken in NetScaler ADC und Gateway veröffentlicht (CVE-2026-88771 bis -88778). Zwei davon (CVE-2026-88771, CVE-2026-88772, CVSS v4.0 9.5) erlauben jeweils allein und ohne Anmeldung Remote Code Execution. Beide wurden schon vor der Veröffentlichung weltweit ausgenutzt. CISA hat sie am 27.09. in den KEV-Katalog aufgenommen, das BSI warnt seit 28.09. mit Stufe 3 von 4 („sehr hoch“).

Bedeutung: Viele Stadtwerke und Wasserversorger nutzen NetScaler als VPN- und Remote-Access-Zugang für Dienstleister, Bereitschaft und Leitstellen. Wer das Gateway übernimmt, bekommt gültige Sessions und einen direkten Weg für Lateral Movement in die Leittechnik. Bereits installierte Webshells entfernt der Patch nicht.

Empfehlung: Vor dem Update Logs und forensische Spuren sichern und die IoCs von Citrix prüfen, wie CISA empfiehlt. Danach sofort patchen, alle aktiven Sessions beenden und die Zugangsdaten zurücksetzen, die über das Gateway liefen. Nach dem Patch gezielt nach Webshells und neuen Konten suchen. Lässt sich eine Kompromittierung nicht ausschließen, Incident Response einleiten (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: Auth-Bypass wird als Zero-Day ausgenutzt (CVE-2026-76504, CVSS 9.8)

KRITISCH Cisco PSIRT / CISA KEV / BleepingComputer / Help Net Security, 30.09.

Was ist neu: Mit einer URI-kodierten Anfrage (``/%6a_security_check``, ``%6a`` steht für „j“ in ``j_security_check``) bekommen Angreifer ohne Zugangsdaten Admin-Rechte über die API, und zwar unabhängig von der Konfiguration. Cisco hat die Lücke am 30.09. veröffentlicht und meldet Ausnutzung seit September. Betroffen sind auch Systeme, die schon gegen die SD-WAN-Lücken aus Mai und Juni gepatcht sind. CISA hat die Lücke am 30.09. in den KEV-Katalog aufgenommen und US-Bundesbehörden eine Frist bis 03.10. gesetzt. Einen Workaround gibt es nicht.

Bedeutung: Der SD-WAN Manager steuert die gesamte Standortvernetzung. Wer ihn übernimmt, kann Routing und Segmentierung bis in die OT-Netze ändern und so Netzleittechnik und Fernwirktechnik erreichen. Betroffen sind vor allem größere Stadtwerke und Netzbetreiber, die ihre Standorte per SD-WAN vernetzen. Laut BleepingComputer ist es bereits der fünfte ausgenutzte SD-WAN-Zero-Day seit Jahresbeginn.

Empfehlung: Auf eine gepatchte Version aktualisieren: 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 oder 26.2.1. Den Manager nur aus dem Management-Netz bzw. für vertrauenswürdige Hosts erreichbar machen. In `serviceproxy-access.log` und `vmanage-server.log` nach Anfragen mit ``/%6a_security_check`` bzw. verdächtigen ``j_security_check``-Anfragen suchen und die aktuelle Konfiguration mit dem Sollstand vergleichen (CC2, CC3).

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

L-03 MikroTik RouterOS: Root-Codeausführung ohne Anmeldung mit einer einzigen Anfrage (CVE-2026-84411, CVSS v3.1 9.8)

HOCH CISA ICSA-26-272-06, 29.09.

Was ist neu: Ein Integer-Underflow im Web-Management von RouterOS ist schon vor der Anmeldung erreichbar. Eine einzige präparierte Anfrage reicht für Root-Codeausführung oder Denial of Service. Betroffen sind alle Versionen unter 7.24. Ausgenutzt wird die Lücke bisher nicht.

Bedeutung: Kleinere Versorger und Zweckverbände setzen MikroTik-Router oft als günstige Edge-Geräte ein, auch an Pumpwerken und Hochbehältern. Lücken in MikroTik-Geräten werden erfahrungsgemäß schnell ausgenutzt, und die Geräte landen dann in Botnetzen.

Empfehlung: MikroTik-Geräte im Asset-Inventar erfassen und auf 7.24 oder neuer aktualisieren. Die Webfig-Oberfläche auf das Management-Netz beschränken (CC5, CC2).

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

L-04 Lantronix G520 Mobilfunk-Gateway: Root-Codeausführung über manipulierte Updates (ICSA-26-272-01, CVE-2026-84409, CVE-2026-91191)

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

Was ist neu: In Firmware 2.6.0.4R6_stable kommen die Update-Metadaten unverschlüsselt über HTTP, und die Signaturprüfung ist mangelhaft. Berichten zufolge liegt im öffentlichen SDK außerdem der private Schlüssel, dem die Firmware vertraut. Angreifer können so eigene Firmware mit Root-Rechten einspielen (CVSS v3.1 7.5 / v4.0 7.7). CISA nennt Energie sowie Wasser und Abwasser als betroffene Sektoren. Der Fix ist Version 2.6.0.7R6.

Bedeutung: Solche LTE-Gateways binden in DACH häufig entfernte Anlagen an die Fernwirktechnik an. Ein kompromittiertes Gateway ist eine unauffällige, dauerhafte Backdoor direkt im Prozessnetz.

Empfehlung: Alle G520 im Asset-Inventar erfassen und gezielt auf 2.6.0.7R6 aktualisieren. Updates nur aus vertrauenswürdigen, internen Quellen über das Management-Netz einspielen. Den Datenverkehr der Gateways auf unerwartete Ziele überwachen (CC5, CC3).

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

L-05 Ransomware auf Jahreshöchststand: 1.073 Angriffe im August, 31 % gegen die Industrie

HOCH Industrial Cyber, 28.09.

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

Bedeutung: Der Druck auf Stadtwerke läuft weiter über die IT. Das zeigt der Vorfall bei den Stadtwerken Landsberg (verschlüsselt am 01.09.): Die Versorgung lief weiter, aber Verwaltung und Kundenservice fielen aus. Wenn IT und OT nicht sauber getrennt sind, erreicht Ransomware auch Leitsysteme und Planungsdaten.

Empfehlung: Prüfen, ob die Leittechnik bei einem Totalausfall der IT autark weiterläuft, und den manuellen Betrieb üben. Offline-Backups von Projektierungs- und Leitsystemdaten testen (CC1, CC2).

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

L-06 Stadt Wien: rund 26.000 Dokumente abgeflossen, die Lücke wurde vorher in einem Forum angeboten

MITTEL ORF Wien, 30.09.

Was ist neu: Laut ORF sind Angreifer über eine Schwachstelle in eine interne Dokumentationsplattform eingedrungen. Sie haben rund 26.000 Dokumente (9 GB) mit Daten von 5.824 Betroffenen kopiert. Die Stadt erfuhr am 09.09. über CERT.at davon. Die Lücke war zuvor in einem Online-Forum zum Kauf angeboten worden, Phishing wird ausgeschlossen. Laut ORF wurde die Lücke vermutlich per KI-Scan gefunden.

Bedeutung: Der Fall zeigt, dass Initial Access Broker Zugänge zu kommunalen Systemen handeln. Stadtwerke nutzen oft dieselben Plattfortmtypen wie ihre Kommune. Projekt- und Planungsunterlagen können Angreifern Wissen über die OT liefern, das hat das Rhysida-Leak aus Berlin im September gezeigt.

Empfehlung: Extern erreichbare Kollaborations- und Dokumentationsplattformen inventarisieren und patchen. Mit CERT.at bzw. dem BSI oder einem Dienstleister einen Meldeweg vereinbaren, damit Hinweise auf angebotene Zugänge schnell ankommen (CC1).

Quelle: <https://wien.orf.at/stories/3373234/> ✓ geprüft

L-07 KVV Kassel: Schadcode auf den Webseiten eines kommunalen Versorgers

MITTEL Security-Insider, 30.09.

Was ist neu: Unbekannte haben Schadcode in mehrere Webangebote der Kasseler Verkehrs- und Versorgungs-GmbH eingebaut, darunter kvvks.de, kvg.de, netzplusservice.de und die Seiten der Bäder. Besucher wurden aufgefordert, etwas zu installieren oder an ihrem Rechner zu ändern. Laut KVV waren interne Systeme und Kundendaten nicht betroffen. BSI, Ermittlungsbehörden und Datenschutzaufsicht sind eingeschaltet.

Bedeutung: Über die Webseiten von Stadtwerken lassen sich Kunden und Mitarbeitende angreifen, zum Beispiel mit Malware, die sich als Update ausgibt. Betroffen sind auch Bürger und Partner, die den Seiten vertrauen. Das schadet dem Ruf, auch wenn die OT unberührt bleibt.

Empfehlung: CMS, Plugins und Hosting-Zugänge der eigenen Webauftritte auf aktuelle Patches und Multifaktor-Anmeldung prüfen. Eine Integritätsprüfung der Seiten einrichten und eine Ansprechstelle für Meldungen festlegen (CC1).

Quelle: <https://www.security-insider.de/kvv-webseiten-schadcode-besucher-gefaehrdet-a-41f72a70c12fa1e023070fbd72ac6930/> ✓ geprüft

L-08 ABB PCM600 (IED-Manager für Schutztechnik): Rechteauserweiterung und Dateiüberschreibung (CVE-2026-15952, CVE-2026-15953)

MITTEL CISA ICSA-26-274-03, 01.10.

Was ist neu: PCM600 bis Version 2.14 hat zwei Lücken mit dem Schweregrad mittel bis hoch (bis 7.1 nach CVSS v4): eine Privilege Escalation durch fehlerhafte Rechtevergabe und eine Dateiüberschreibung beim Entpacken von Archiven. Das Advisory nennt keinen Patch, ABB empfiehlt Workarounds. Eine Ausnutzung ist nicht bekannt.

Bedeutung: Verteilnetzbetreiber parametrieren mit PCM600 ihre ABB-Schutzgeräte. Über einen kompromittierten Engineering-Rechner lassen sich Schutzeinstellungen ändern.

Empfehlung: Den Scheduler Service mit demselben Windows-Konto betreiben wie PCM600. Projektarchive nur aus vertrauenswürdigen Quellen öffnen. Engineering-Rechner vom Büronetz trennen.

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

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Citrix NetScaler und Cisco SD-WAN Manager patchen, auf Kompromittierung prüfen und Sessions sowie Zugangsdaten erneuern [CC4 Secure Remote Access]	L-01, L-02	HOCH	sofort
M-02	Fernzugänge in die Leittechnik nur noch über einen zentralen Jump Host mit Mehrfaktor-Anmeldung, Freigabe pro Sitzung und Aufzeichnung [CC4 Secure Remote Access]	L-01	HOCH	0–3 Monate
M-03	Asset-Inventar der Edge-Geräte (LTE-Gateways, Router, APs) aufbauen und risikobasiert patchen. Vorrang haben Geräte, die aus dem Internet erreichbar sind oder deren Lücken als ausgenutzt gemeldet sind [CC5 Risk-Based Vulnerability Management]	L-03, L-04	HOCH	0–3 Monate
M-04	Management-Schnittstellen von SD-WAN, Routern, APs und Engineering-Rechnern in ein eigenes Management-Segment verlegen [CC2 Defensible Architecture]	L-02, L-08	MITTEL	0–3 Monate
M-05	Autarken Betrieb der Leittechnik bei einem Totalausfall der IT üben und Offline-Backups von Projektierungs- und Leitsystemdaten testen [CC1 ICS Incident Response]	L-05	MITTEL	0–3 Monate
M-06	Meldewege zu CERT.at, BSI bzw. NCSC und Threat Intelligence zu angebotenen Zugängen sowie zu manipulierten Webauftritten einrichten [CC1 ICS Incident Response]	L-06, L-07	MITTEL	0–3 Monate

Fragen für das nächste Jour fixe

1. Sind unsere Citrix-NetScaler- und Cisco-Systeme vollständig gepatcht? Wurden sie vor dem Patch auf Webshells und IoCs geprüft, und wer hat das dokumentiert?

2. Setzen wir oder unsere Dienstleister Cisco SD-WAN, MikroTik, Lantronix G520 oder WatchGuard-APs ein, an welchen Außenstationen und mit welcher Firmware?
3. Welche Dienstleister haben heute Remote Access auf die Leittechnik, und laufen diese Zugänge über einen kontrollierten Jump Host mit Mehrfaktor-Anmeldung?
4. Welche Fernwartungszugänge von Dienstleistern laufen über Edge-Geräte, und lassen sie sich im Notfall schnell sperren?
5. Wie lange können wir Wasser, Abwasser und Fernwärme ohne die Unternehmens-IT betreiben, und wann haben wir das zuletzt geübt?
6. Würde unsere Angriffserkennung (SzA) eine geänderte Segmentierung oder neue Routen im SD-WAN bemerken?

Maßnahmen dieser Woche

1. Citrix NetScaler ADC/Gateway: Spuren sichern, IoCs prüfen, auf 14.1-73.37 bzw. 13.1-64.23 patchen, alle Sessions beenden und die über das Gateway genutzten Zugangsdaten zurücksetzen.
2. Cisco Catalyst SD-WAN Manager patchen, nur aus dem Management-Netz erreichbar machen, die Logs nach ``/%6a\_security\_check`` durchsuchen und die Konfiguration mit dem Sollstand vergleichen.
3. Asset-Inventar der Edge-Geräte an den Außenstationen ergänzen: Lantronix G520 auf 2.6.0.7R6, MikroTik RouterOS auf 7.24 oder neuer, WatchGuard-APs auf 3.4.8.
4. Management-Schnittstellen von Routern, APs und Gateways aus dem Internet und aus dem OT-Netz entfernen und in ein eigenes Management-Segment legen.
5. Alle aktiven Fernwartungszugänge von Dienstleistern prüfen und nicht benötigte Zugänge sperren.
6. Extern erreichbare Dokumentations- und Kollaborationsplattformen sowie die Webauftritte (CMS, Plugins, Hosting-Zugänge) auf Manipulation, Patchstand und fehlende Mehrfaktor-Anmeldung prüfen.
7. ABB PCM600: Workarounds umsetzen und die Engineering-Rechner vom Büronetz trennen.

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 02.10.2026 automatisch aufgerufen und inhaltlich geprüft. 2 Meldung(en) ohne überprüfbare Originalquelle wurden nicht aufgenommen. Am 02.10.2026 zusätzlich per Doppel-Recherche faktengeprüft und korrigiert.