

BRIEFING

OT-/Cyber-Lagebild

Ausgabe 29.09.2026 · Kommunale Versorger und KRITIS in DACH

Zielgruppe	Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber
Berichtszeitraum	22.09.-29.09.2026
Version	1.0
Datum	29.09.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen

Dieses Briefing fasst öffentlich zugängliche Meldungen zusammen. Die Einstufung der Relevanz bezieht sich auf Betreiber der kommunalen Daseinsvorsorge in Deutschland, Österreich und der Schweiz.

Management Summary

Die Ransomware-Aktivität hat im August 2026 einen neuen Jahreshöchststand erreicht, und fast ein Drittel der Angriffe trifft die Industrie. Die Fälle Landsberg und das Rhysida-Leak zur Berliner Trinkwasserversorgung zeigen, wie schnell ein IT-Vorfall die OT-Planung und die Betriebssicherheit berührt.

Parallel hat die CISA sieben neue Siemens-Advisories veröffentlicht, darunter eine kritische Lücke im Industrial Edge Management. Desigo CC und SIMATIC sind in Stadtwerken sowie Wasser- und Abwasserbetrieben weit verbreitet.

GESAMTBEWERTUNG

Hoher Druck über die IT, konkreter Patchbedarf bei Siemens-Komponenten. Vorrang haben der Abgleich des Siemens-Bestands und eine Prüfung der Trennung von IT und OT.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Ransomware erreicht 2026-Höchststand	HOCH	Industrial Cyber, 28.09.
L-02	Siemens: sieben neue ICS-Advisories	HOCH	CISA, 22.09.
L-03	OpenPLC Runtime v3 verwundbar	MITTEL	CISA ICSA-26-265-09, 22.09.
L-04	Satellitenkommunikation vergrößert die Angriffsfläche	MITTEL	Industrial Cyber, 28.09.
L-05	CISA stellt das CVE-Programm auf Qualität um	MITTEL	Industrial Cyber

Tabelle 1: Meldungen nach Relevanz für Betreiber in DACH

Meldungen im Detail

L-01 Ransomware erreicht 2026-Höchststand

HOCH Industrial Cyber, 28.09.

Im August gab es weltweit 1.073 Ransomware-Angriffe, 12 % mehr als im Juli. 31 % davon (329) trafen die Industrie, Qilin war die aktivste Gruppe. Für Stadtwerke in DACH bleibt der Druck über die IT hoch. Landsberg (verschlüsselt am 01.09.) und das Rhysida-Leak mit Daten zu KRITIS-Anlagen und zur Berliner Trinkwasserversorgung zeigen, wie schnell das die OT-Planung und die Betriebssicherheit berührt.

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

L-02 Siemens: sieben neue ICS-Advisories

HOCH CISA, 22.09.

Betroffen sind Desigo CC, SIPLUS/SIMATIC, Industrial Edge Management (kritisch), SIMOVE Fleetmanager/SIPLANT, Siveillance Control und WTV676/776. Desigo CC und SIMATIC sind in deutschen Stadtwerken sowie Wasser- und Abwasserbetrieben weit verbreitet, deshalb den Bestand prüfen und Patches einplanen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories>

L-03 OpenPLC Runtime v3 verwundbar

MITTEL CISA ICSA-26-265-09, 22.09.

Das Open-Source-SPS-Laufzeitsystem wird in Laboren, Schulungen und kleineren Pilotanlagen genutzt. Für den produktiven Betrieb in der Daseinsvorsorge ist das wenig relevant, für Test- und Ausbildungsumgebungen schon.

Quelle: <https://www.cisa.gov/news-events/ics-advisories>

L-04 Satellitenkommunikation vergrößert die Angriffsfläche

MITTEL Industrial Cyber, 28.09.

Industrial Cyber warnt vor wachsenden Risiken durch Satelliten- und Direct-to-Device-Anbindungen für IoT, Versorger und KRITIS. Das betrifft Versorger, die entlegene Pumpwerke, Hochbehälter oder Umspannstationen per Satellit anbinden.

Quelle: <https://industrialcyber.co/industrial-cyber-attacks/satellite-communications-growth-expands-cybersecurity-attack-surface-across-iot-utilities-critical-infrastructure/>

L-05 CISA stellt das CVE-Programm auf Qualität um

MITTEL Industrial Cyber

Ein Whitepaper beschreibt den Wechsel in eine „Quality Era“ mit besseren Daten, Governance und Infrastruktur. Grund ist ein Anstieg der CVE-Meldungen um 263 % von 2020 bis 2025. Für OT-Betreiber zählt das, weil ihr Schwachstellenmanagement und der Einkauf nach CRA und NIS2 auf verlässlichen CVE-Daten aufbauen.

Quelle: <https://industrialcyber.co/threats-attacks/cisa-launches-cve-quality-era-framework-to-improve-vulnerability-data-quality-infrastructure-program-governance/>

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Siemens-Bestand (Desigo CC, SIMATIC/SIPLUS, Industrial Edge Management) mit den Advisories abgleichen und Patches einplanen	L-02	HOCH	sofort
M-02	Trennung von IT und OT sowie den Wiederanlauf nach einem Ransomware-Vorfall überprüfen	L-01	HOCH	0–3 Monate
M-03	OpenPLC in Labor- und Schulungsumgebungen erfassen und aktualisieren	L-03	MITTEL	0–3 Monate
M-04	Satellitenanbindungen entlegener Anlagen in die Risikoanalyse aufnehmen	L-04	MITTEL	3–6 Monate

HINWEIS ZUR QUELLENLAGE

In den letzten 24 Stunden gab es nur zwei Meldungen mit sicherem Datum (beide 28.09.). Die übrigen Punkte sind bis zu eine Woche alt. Nicht aufgenommen wurden zwei unbestätigte Meldungen vom 28.09.: ein Ransomware-Angriff auf einen Wasserversorger (Originalquelle nicht erreichbar) und neue kritische Lücken in Schneider EcoStruxure (gefundene Meldungen stammen von Anfang September).

Thema für LinkedIn

Ransomware erreicht einen neuen Höchststand, und die Industrie trägt fast ein Drittel der Angriffe. Warum Stadtwerke die Trennung von IT und OT jetzt prüfen sollten, am Beispiel Landsberg und des Berliner Leaks.