

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 05.10.2026, 07:33 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	05.10.2026
Herausgeber	Maximilian Gilg, OT-Cyber.de, Rosenheim
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen
Online	https://ot-cyber.de/ot-lage/

Dieses Lagebild fasst öffentlich zugängliche Meldungen zusammen – automatisch zusammengestellt, ohne Gewähr. Die Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen in Deutschland, Österreich und der Schweiz.

Management Summary

Diese Ausgabe enthält 5 Meldungen, davon 2 mit hoher Relevanz für Betreiber in DACH.

- Iranische Angriffe auf SPS weiten sich von Wasser auf Telekom und Energie aus
- WAGO: CODESYS-Lücken in PLCs der Serien 750/751/752/762 (VDE-2025-081)

GESAMTBEWERTUNG

Hoch – vorrangig die Meldungen mit hoher Relevanz prüfen und umsetzen.

Lageübersicht

ID	Meldung	Relevanz
L-01	Iranische Angriffe auf SPS weiten sich von Wasser auf Telekom und Energie aus	HOCH
L-02	WAGO: CODESYS-Lücken in PLCs der Serien 750/751/752/762 (VDE-2025-081)	HOCH
L-03	Vicksburg (Mississippi): Ransomware legt Stadtverwaltung samt Abrechnung der Versorgung lahm	MITTEL
L-04	WAGO: BACnet-IP-Stack lässt Dateien ohne Anmeldung lesen und überschreiben (VDE-2025-102, CVE-2025-41753, CVSS 9,8)	MITTEL
L-05	Cisco kündigt Advisories für den 07.10. an	MITTEL

Meldungen im Detail

L-01 Iranische Angriffe auf SPS weiten sich von Wasser auf Telekom und Energie aus

Relevanz: HOCH

Die Kampagne gegen offen erreichbare Steuerungen läuft seit Juli und trifft Rockwell MicroLogix 1100/1400, Siemens S7-1200 und Schneider Modicon. Seit September sind laut einer Sekundärquelle auch Telekom- und Energienetze betroffen. Die Angreifer ändern Passwörter, sperren das Bedienpersonal aus und verstellen Parameter. Mehrere US-Versorger mussten auf Handbetrieb umstellen, es gab Druckverlust. Dieselben Gerätetypen hängen in DACH tausendfach offen im Netz.

Quelle: <https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet-facing-programmable-logic-controllers-causing-operational-disruptions>

Quelle: <https://startupfortune.com/iranian-hackers-widen-water-system-attacks-to-telecom-and-energy-grids>

L-02 WAGO: CODESYS-Lücken in PLCs der Serien 750/751/752/762 (VDE-2025-081)

Relevanz: **HOCH**

CERT@VDE meldet am 01.10. drei CODESYS-Control-Lücken für Firmware < 4.10.0. Die schwerste ist CVE-2025-41738 (Type Confusion im Visualisierungsserver, CVSS 8,3), es drohen Denial of Service und Remote Code Execution. Die Lösung ist Firmware 4.10.0 (FW32). Das ist ein anderes Advisory als das schon gemeldete VDE-2026-094. WAGO-PFCs stecken oft in Kläranlagen, Pumpwerken und der Fernwirktechnik.

Quelle: <https://certvde.com/en/advisories/VDE-2025-081/>

L-03 Vicksburg (Mississippi): Ransomware legt Stadtverwaltung samt Abrechnung der Versorgung lahm

Relevanz: **MITTEL**

Seit 02.10. ist die IT der Stadt abgeschaltet und Zahlungen für Versorgungsleistungen sind gestört. Versorgung und Notdienste laufen weiter, die Angreifergruppe ist unbekannt. Das ist das typische Muster im kommunalen Querverbund: Fällt die Verwaltungs-IT aus, trifft es Abrechnung und Kundenservice der Stadtwerke mit.

Quelle: <https://therecord.media/vicksburg-mississippi-government-ransomware-attack>

L-04 WAGO: BACnet-IP-Stack lässt Dateien ohne Anmeldung lesen und überschreiben (VDE-2025-102, CVE-2025-41753, CVSS 9,8)

Relevanz: **MITTEL**

Über Path Traversal in BACnet File Objects lassen sich ohne Anmeldung beliebige Dateien lesen oder überschreiben, auch Zugangsdaten. Betroffen sind rund 11 Produktlinien (u. a. 0750-811x/821x, 0751-9x01, 0762), die Lösung ist Firmware ≥ 4.8.9 (FW30). Relevant ist das für die Gebäudeleittechnik in Stadtwerke-Liegenschaften. Ob die Meldung neu ist, bleibt offen (widersprüchlich: Übersicht von CERT@VDE nennt 01.10.2026 / Detailseite nennt 10.01.2026).

Quelle: <https://certvde.com/en/advisories/VDE-2025-102/>

Quelle: <https://certvde.com/en/advisories/>

L-05 Cisco kündigt Advisories für den 07.10. an

Relevanz: **MITTEL**

Betroffen sind NX-OS (Nexus 3000/7000/9000, MDS 9000, UCS Fabric Interconnects), Meraki, APIC, Finesse und License On-Prem, die Schweregrade sind noch offen. Versorger sollten ein Wartungsfenster einplanen, vor allem für Nexus-Switches in Leitstellen-Rechenzentren.

Quelle:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-fBn58ELx>

Einordnung und Unterstützung: OT-Cyber.de · Am Esbaum 12, 83022 Rosenheim · +49 8031 8603164 · akademie@ot-cyber.de · <https://ot-cyber.de/>