

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 10.10.2026, 16:08 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	10.10.2026
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 4 Meldungen, davon 0 mit hoher Relevanz für Betreiber in DACH.

GESAMTBEWERTUNG
Mittel – keine akute Lage, Meldungen im regulären Schwachstellen-Management bearbeiten.

Lageübersicht

ID	Meldung	Relevanz
L-01	**NSA: Zero-Trust-Leitfaden für OT im US-Verteidigungsumfeld (08.10.)**	MITTEL
L-02	**Anthropic startet „Critical Infrastructure Defense Program“ für OT-Security (08.10.)**	MITTEL
L-03	**Johnson Controls Illustra Standard (L4L China, Windows): Command Injection (CVE-2026-34498, Kanada AV26-1010, 06./07.10.)** Betroffen sind Versionen vor 6.0.0.66394; genannt wird nur die Variante „L4L China“. Eine unzureichende Eingabeprüfung (CWE-20) ermöglicht eine OS Command Injection. CVSS v4 5.1 (mittel), eine Ausnutzung ist nicht bekannt. Unsere Einschätzung: Für DACH nur relevant, wo genau diese Variante der Videotechnik im Einsatz ist	GERING
L-04	**AhsayCBS-Backupserver: zwei Lücken werden aktiv ausgenutzt (CVE-2026-105133/-105134, 08.10.)** Laut Huntress laufen die Angriffe seit dem 07.10. (23:20 UTC); bis zum 08.10. waren fünf Organisationen Ziel. Über einen Authentisierungs-Bypass im Replication Receiver ist Codeausführung ohne Anmeldung möglich; die Angreifer legen JSP-Webshells und XMRig-Miner ab, getarnt als Microsoft Edge. Patch-Stand umstritten: Huntress und SecurityWeek sehen auch Version 10.3.4 als betroffen und ohne Patch, Ahsay erklärt am 09.10., beide Lücken seien im Release vom 04.08.2026 (Version 10.3.4) behoben. Empfehlung: Management-Oberfläche nur für vertrauenswürdige IP-Adressen oder per VPN erreichbar machen, nach den veröffentlichten IoCs suchen und betroffene Server aus einem sauberen Backup neu aufsetzen	MITTEL

Meldungen im Detail

L-01 **NSA: Zero-Trust-Leitfaden für OT im US-Verteidigungsumfeld (08.10.)**

Relevanz: MITTEL

Das neue Cybersecurity Information Sheet richtet sich an National Security Systems, die Netze des US-Verteidigungsministeriums und die Defense Industrial Base. Begründet wird es mit dem KI-Einsatz von Angreifern (automatisierte Aufklärung, schnellere Exploit-Entwicklung) und der zunehmenden KI-Integration in der OT; als mögliche Ziele nennt die NSA etwa Wasser und Energie. Kern ist „never trust, always verify“: Nutzer, Geräte, Abläufe und Kommunikation werden laufend geprüft, um den Schutz vor unbefugtem Zugriff, Lateral Movement und Persistenz zu stärken. Unsere Einschätzung: Auch wenn es ein Leitfaden für das US-Verteidigungsumfeld ist, eignet sich das Merkblatt gut als Argumentationshilfe zu NIS2/KRITIS-DachG bei Stadtwerken.

Quelle: https://media.defense.gov/2026/Oct/08/2004013274/-1/-1/0/CSI_HARDENING_OT_WITH_ZT.PDF
Quelle: <https://www.executivegov.com/articles/nsa-guidance-zero-trust-model-operational-technology>

L-02 **Anthropic startet „Critical Infrastructure Defense Program“ für OT-Security (08.10.)**

Relevanz: MITTEL

Elf Gründungspartner bekommen Zugang zu Frontier-KI-Modellen, Ingenieuren und Threat Research. Laut Anthropic sind das Accenture, Booz Allen, CrowdStrike, Deloitte, Dragos, Hitachi, Insane Cyber, Nozomi Networks, Palo Alto Networks, PwC und Rockwell Automation. Das Programm setzt zunächst bei den Anbietern an – Beratungen, Security-Firmen und Ausrüstern –, die OT-Security für Betreiber kritischer Infrastruktur leisten. Hintergrund laut Anthropic: OT-Systeme können oft nicht für Patches abgeschaltet werden, bekannte Lücken können dort jahrelang offen bleiben. Unsere Einschätzung für DACH: Mehrere große OT-Anbieter setzen beim Schwachstellen-Management auf KI – Betreiber sollten bei ihren Lieferanten nachfragen, wie schnell gefundene Lücken in Patches und Abhilfen umgesetzt werden.

Quelle: <https://www.anthropic.com/news/anthropic-cyber-mission>

Quelle: <https://www.securityweek.com/anthropic-fast-tracks-ai-bug-reports-to-oss-maintainers-taps-11-firms-for-ot-security/>

L-03 **Johnson Controls Illustrate Standard (L4L China, Windows): Command Injection (CVE-2026-34498, Kanada AV26-1010, 06./07.10.). Betroffen sind Versionen vor 6.0.0.66394; genannt wird nur die Variante „L4L China“. Eine unzureichende Eingabeprüfung (CWE-20) ermöglicht eine OS Command Injection. CVSS v4 5.1 (mittel), eine Ausnutzung ist nicht bekannt. Unsere Einschätzung: Für DACH nur relevant, wo genau diese Variante der Videotechnik im Einsatz ist**

Relevanz: GERING

Bestand im Asset-Inventar prüfen.

Quelle:

<https://www.cyber.gc.ca/en/alerts-advisories/control-systems-johnson-controls-security-advisory-av26-1010>

Quelle: <https://app.openCVE.io/cve/CVE-2026-34498>

L-04 **AhsayCBS-Backupserver: zwei Lücken werden aktiv ausgenutzt (CVE-2026-105133/-105134, 08.10.) Laut Huntress laufen die Angriffe seit dem 07.10. (23:20 UTC); bis zum 08.10. waren fünf Organisationen Ziel. Über einen Authentisierungs-Bypass im Replication Receiver ist Codeausführung ohne Anmeldung möglich; die Angreifer legen JSP-Webshells und XMRig-Miner ab, getarnt als Microsoft Edge. Patch-Stand umstritten: Huntress und SecurityWeek sehen auch Version 10.3.4 als betroffen und ohne Patch, Ahsay erklärt am 09.10., beide Lücken seien im Release vom 04.08.2026 (Version 10.3.4) behoben. Empfehlung: Management-Oberfläche nur für vertrauenswürdige IP-Adressen oder per VPN erreichbar machen, nach den veröffentlichten IoCs suchen und betroffene Server aus einem sauberen Backup neu aufsetzen**

Relevanz: MITTEL

ein Update allein repariert einen kompromittierten Server nicht. Das ist kein OT-Produkt. Unsere Einschätzung: Wo solche Backup-Lösungen bei Versorgern im Einsatz sind, ist ein übernommener Backupserver ein gefährlicher Brückenkopf ins Netz.

Quelle: <https://www.huntress.com/blog/ahsaycbs-flaws-exploit>

Quelle: <https://www.securityweek.com/unpatched-ahsaycbs-vulnerabilities-exploited-in-the-wild/>

Quelle: <https://www.ahsay.com/en/company/announcements>

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