

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 11.10.2026, 07:23 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	11.10.2026
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 3 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	**Claroty-Studie: 58 % der CPS-Betreiber melden Cyberangriffe mit Folgen für den Betrieb (08.10.)**	MITTEL
L-02	**Rockwell-Bericht: 46 % der Industrieunternehmen hatten im letzten Jahr einen Cybervorfall (08.10.)**	MITTEL
L-03	**Cisco Nexus 3000/9000: kritische Lücke im MPLS OAM (CVE-2026-76465, CVSS 9.8, 07.10.)** Betroffen sind Switches der Serien Nexus 3000 und Nexus 9000 im Standalone-NX-OS-Modus, und zwar nur, wenn die Funktion MPLS OAM aktiviert ist (Standard: aus). Ein Angreifer kann ohne Anmeldung aus dem Netz Code ausführen. Laut Cisco ist keine Ausnutzung bekannt; es gibt keinen Workaround, aber „no feature mpls oam“ entfernt den Angriffsweg, wenn die Funktion nicht gebraucht wird. Das ist kein OT-Produkt. Unsere Einschätzung: Relevant für Versorger und Industrie, die Nexus-Switches im Rechenzentrum oder an der IT/OT-Grenze betreiben	GERING

Meldungen im Detail

L-01 **Claroty-Studie: 58 % der CPS-Betreiber melden Cyberangriffe mit Folgen für den Betrieb (08.10.)**

Relevanz: MITTEL

Für den Bericht „Global State of Operational Security 2026“ hat Claroty 2.000 Führungskräfte aus Business und Technik in 16 Branchen und mehr als 40 Ländern befragt. 58 % der Betreiber cyber-physischer Systeme (CPS) geben an, dass in den letzten 12 Monaten ein Cyberangriff ihre operativen Umgebungen getroffen hat. Von den Befragten, die Zugänge Dritter als Risiko sehen (53 %), hatten drei von vier mindestens einen Vorfall mit Folgen für den Betrieb, der auf solche Zugänge zurückgeht; 49 % überwachen die Verbindungen von Dienstleistern nur teilweise oder gar nicht. Der Artikel nennt keine Zahlen für DACH. Unsere Einschätzung: Fernwartung und Zugänge von Integratoren und Herstellern gehören bei Betreibern ganz oben auf die Liste – das ist Kern von Secure Remote Access (SANS Critical Control 4).

Quelle: <https://industrialcyber.co/industrial-cyber-attacks/claroty-finds-58-of-cps-operators-faced-operational-cyberattacks-as-third-party-access-and-ai-risks-grow/>

Quelle: <https://claroty.com/resources/reports/the-global-state-of-operational-security-2026>

L-02 **Rockwell-Bericht: 46 % der Industrieunternehmen hatten im letzten Jahr einen Cybervorfall (08.10.)**

Relevanz: MITTEL

Im Bericht „Operational Resilience in the Age of Connectivity“ von Rockwell Automation halten sich zugleich 90 % für fähig, einen Cybervorfall einzudämmen. 62 % haben bereits in Security-Plattformen investiert, zum Beispiel in Asset-Inventar und Angriffserkennung. Wie viele Unternehmen aus welchen Regionen befragt wurden, nennt der Artikel nicht. Unsere Einschätzung: Fast jedes zweite Unternehmen hatte einen Vorfall, aber neun von zehn halten sich für fähig, ihn einzudämmen – diese Lücke zwischen Selbsteinschätzung und geübter Praxis schließt am besten ein getesteter ICS-Incident-Response-Plan (SANS Critical Control 1).

Quelle: <https://industrialcyber.co/industrial-cyber-attacks/rockwell-finds-46-of-industrial-organizations-faced-cyber-incidents-as-ai-adoption-it-ot-convergence-reshape-resilience/>

L-03 **Cisco Nexus 3000/9000: kritische Lücke im MPLS OAM (CVE-2026-76465, CVSS 9.8, 07.10.) Betroffen sind Switches der Serien Nexus 3000 und Nexus 9000 im Standalone-NX-OS-Modus, und zwar nur, wenn die Funktion MPLS OAM aktiviert ist (Standard: aus). Ein Angreifer kann ohne Anmeldung aus dem Netz Code ausführen. Laut Cisco ist keine Ausnutzung bekannt; es gibt keinen Workaround, aber „no feature mpls oam“ entfernt den Angriffsweg, wenn die Funktion nicht gebraucht wird. Das ist kein OT-Produkt. Unsere Einschätzung: Relevant für Versorger und Industrie, die Nexus-Switches im Rechenzentrum oder an der IT/OT-Grenze betreiben**

Relevanz: GERING

Konfiguration prüfen und auf eine korrigierte Version aktualisieren.

Quelle:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-moam-rce-uBTzYV7>

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