OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 18.11.2026, 07:49 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	18.11.2026
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 2 mit hoher Relevanz für Betreiber in DACH.

• □ UPDATE: **Dorsett Controls InfoScan: sechs Lücken in einer Software für die Wasserwirtschaft (ICSA-26-321-01, 17.11.)**: Laut CISA ist InfoScan bis einschließlich Version 1.45.0 betroffen, der Hersteller empfiehlt das Update auf v1.46 oder neuer

• □ UPDATE: **Update Siemens WinCC und PCS 7: CISA veröffentlicht die NTLM-Lücke neu (ICSA-26-321-08, 17.11.)**: Erstmeldung in der OT-Lage vom 10.11

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	□ UPDATE: **Update PHP2Shell: weitere Geräte betroffen, darunter Siemens WTV676 und WTV776 (SSA-166980)**: Siemens nennt die Zählerdaten-Gateways WTV676-HB6035 und WTV776-HB6035 seit dem 16.11. in SSA-166980 zusätzlich als betroffen	MITTEL
L-02	□ UPDATE: **Dorsett Controls InfoScan: sechs Lücken in einer Software für die Wasserwirtschaft (ICSA-26-321-01, 17.11.)**: Laut CISA ist InfoScan bis einschließlich Version 1.45.0 betroffen, der Hersteller empfiehlt das Update auf v1.46 oder neuer	HOCH
L-03	□ UPDATE: **Update Siemens WinCC und PCS 7: CISA veröffentlicht die NTLM-Lücke neu (ICSA-26-321-08, 17.11.)**: Erstmeldung in der OT-Lage vom 10.11	HOCH

Meldungen im Detail

L-01 □ UPDATE: **Update PHP2Shell: weitere Geräte betroffen, darunter Siemens WTV676 und WTV776 (SSA-166980)**: Siemens nennt die Zählerdaten-Gateways WTV676-HB6035 und WTV776-HB6035 seit dem 16.11. in SSA-166980 zusätzlich als betroffen

Relevanz: MITTEL

Betroffen sind dort alle Versionen, es geht um CVE-2026-109618 und CVE-2026-109619, und für beide Geräte steht in der Tabelle „Currently no fix is available“. Siemens empfiehlt allgemein, den Netzwerkzugriff etwa mit Firewalls, Segmentierung und VPN zu schützen. Als weiterer Industrie-PC ist laut CERT@VDE der Pilz IndustrialPI 4 betroffen: Über das Webinterface ist Remote Code Execution möglich. Betroffen sind die IndustrialPI-OS-Stände vom 10.06.2025, 23.06.2025, 25.12.2025 und 15.06.2026, wenn das Paket libapache2-mod-php8.2 in einer Version vor 8.2.35-1 installiert ist. Laut Advisory hilft das Update dieses Pakets auf 8.2.35-1 oder neuer. Unsere Einschätzung: Die Siemens-Gateways sammeln Verbrauchsdaten. Stadtwerke und Wärmeversorger sollten prüfen, ob die Geräte bei ihnen im Einsatz und aus dem Internet erreichbar sind.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-166980.html

Quelle: https://certvde.com/de/advisories/VDE-2026-153

Quelle: https://ot-cyber.de/ot-lage/2026-11-14.html

L-02 □ UPDATE: **Dorsett Controls InfoScan: sechs Lücken in einer Software für die Wasserwirtschaft (ICSA-26-321-01, 17.11.)**: Laut CISA ist InfoScan bis einschließlich Version 1.45.0 betroffen, der Hersteller empfiehlt das Update auf v1.46 oder neuer

Relevanz: HOCH

Zu den sechs CVEs gehören eine fehlerhafte Prüfung von TLS-Zertifikaten (CVE-2026-117659, CVSS v3.1 8,1, CVSS v4.0 8,5) und ein fest eingebauter Schlüssel, über den sich das Datenbank-Passwort wiederherstellen lässt (CVE-2026-120255). CISA nennt als Sektor „Water and Wastewater Systems“ und als Einsatzgebiet weltweit. Eine öffentliche Ausnutzung ist CISA bisher nicht gemeldet. Ob InfoScan in DACH verbreitet ist, haben wir nicht geprüft. Unsere Einschätzung: Der Wassersektor steht seit Wochen im Fokus. Ende Oktober hat Bloomberg beschrieben, wie prorussische Gruppen schlecht gesicherte Steuerungen auch in Wasseranlagen in Europa und den USA manipulieren. Wasser- und Abwasserbetriebe in Bayern, Salzburg und Tirol sollten deshalb wissen, welche Leitsysteme und Fernzugänge bei ihnen aus dem Internet erreichbar sind (Unsere Einordnung: CC4 Secure Remote Access).

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-321-01

Quelle: https://winfuture.de/news

Quelle: https://ot-cyber.de/ot-lage/2026-10-30.html

L-03 □ UPDATE: **Update Siemens WinCC und PCS 7: CISA veröffentlicht die NTLM-Lücke neu (ICSA-26-321-08, 17.11.)**: Erstmeldung in der OT-Lage vom 10.11

Relevanz: HOCH

Die CISA-Advisory vom 17.11. ist eine Neuveröffentlichung von Siemens SSA-970803 vom 10.11. Es geht um CVE-2026-58114 (CVSS v3.1 7,5): Ein Angreifer auf dem Netzwerkpfad kann die Sitzung eines angemeldeten Nutzers übernehmen. Betroffen sind alle Versionen, darunter WinCC V7.5 bis V8.1 und WinCC Runtime Professional V17 bis V21. Für WinCC nennt Siemens bisher nur eine Übergangslösung. Für BATCH V9.1, PCS 7 V9.1, Process Historian und Information Server 2020 und 2022 plant Siemens laut SSA-970803 keinen Fix. Als Übergangslösung empfiehlt Siemens, die Kommunikation des SQL Servers zu verschlüsseln (Supportartikel 109818202). Unsere Einschätzung: PCS 7 und WinCC laufen oft in Leitwarten von Wasser- und Abwasserbetrieben und Stadtwerken in Bayern, Salzburg und Tirol. Diese Betreiber sollten die SQL-Verschlüsselung einplanen und prüfen, ob die Leittechnik sauber segmentiert ist (Unsere Einordnung: CC2 Defensible Architecture).

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-321-08

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-970803.html

Quelle: https://ot-cyber.de/ot-lage/2026-11-10.html

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