OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Gesamt

Ausgabe KW 45/2026 · Gesamt – alle OT-Branchen in DACH

Zielgruppe	Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH
Berichtszeitraum	30.10.2026–06.11.2026
Version	1.0
Datum	06.11.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen

Dieser Bericht fasst öffentlich zugängliche Meldungen zusammen. Die Einstufung der Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 45 sind die Angriffe auf Kühlanlagen in deutschen Supermärkten der wichtigste OT-Vorfall für DACH. Laut dpa/Handelsblatt (03.11.) sind neben Lilienthal auch Märkte in Wuppertal, Wetter bei Hagen, Niederbayern, dem Münsterland und der Westpfalz betroffen. Ein betroffener Markt sagt, der eigentliche Angriff habe die Firma getroffen, die die Kühlanlagen aus der Ferne wartet. Parallel wird eine Lücke mit CVSS 10/10 in Node-RED auf Siemens SIMATIC IoT2050 Advanced seit dem 30.10. aktiv ausgenutzt. Das ist ein typisches Gateway zwischen Anlage und Datenwelt.

Auch an der Grenze zwischen IT und OT stehen Edge-Geräte unter Druck. CISA hat zwei Ivanti-Connect-Secure-Lücken in den KEV-Katalog aufgenommen. Bei Zyxel-GS1900-Switches lief ein Zero-Day, über den 996 Geräte kompromittiert wurden. Für die End-of-Life-Plattform Sophos UTM gibt es seit dem 28.10. eine Root-Lücke ohne Anmeldung (nur bei aktivem E-Mail-Proxy, Ausnutzung laut Sophos nicht bekannt). Die Stadtwerke Waldbröl zeigen das bekannte Muster: Erpressung über Kundendaten, die Versorgung lief laut Geschäftsführung weiter (Oberberg-Aktuell, 30.10.). Vorrang haben in dieser Woche Fernwartung durch Dienstleister (CC4) und das Patchen von Gateways und VPN-Geräten, die aus dem Internet erreichbar sind (CC5).

GESAMTBEWERTUNG

Die Lage ist hoch: Angreifer nutzen OT-nahe Gateways und Fernwartungswege aktiv aus, in Deutschland mit messbarem Schaden. Zuerst Fernwartungszugänge von Dienstleistern prüfen und einschränken, danach IoT2050/Node-RED, Ivanti und Zyxel patchen.

Trends

• Angreifer kommen über die Fernwartung von Dienstleistern und treffen damit viele Betreiber gleichzeitig, wie die Kühlanlagen-Fälle in Deutschland zeigen.

• OT-nahe Edge-Geräte wie IoT2050/Node-RED, Switches und VPN-Gateways werden kurz nach Bekanntwerden einer Lücke ausgenutzt, teils schon als Zero-Day.

• Auch End-of-Life-Geräte wie Sophos UTM bekommen kritische Lücken, und die Patches müssen dann teils von Hand eingespielt werden.

• Bei Stadtwerken bleibt Erpressung über Kundendaten das häufigste Muster, die Leittechnik ist dabei nicht das erste Ziel.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Kühlanlagen deutscher Supermärkte angegriffen, Weg führte offenbar über den Fernwartungsdienstleister	KRITISCH	Handelsblatt (dpa), 03.11.
L-02	Zyxel GS1900: Zero-Day CVE-2026-107441, 996 Switches in 48 Ländern kompromittiert	HOCH	BleepingComputer, 04.11.
L-03	Stadtwerke Waldbröl (NRW) erpresst, Kundendaten gestohlen	MITTEL	Oberberg-Aktuell, 30.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 06.11.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt. Siemens S7 = Port 102 (alle ISO-TSAP-Dienste, nicht nur echte S7-Steuerungen), OPC UA = Standardport 4840.

Region	Gesamt	Top-Protokolle
Deutschland	143185	DNP3: 32440, OMRON FINS: 26119, ProConOS: 16052, Siemens S7: 7764, OPC UA: 5141
Österreich	4790	HMI/VNC: 1046, DNP3: 970, Niagara Fox: 472, Siemens S7: 387, OPC UA: 158
Bayern (München)	1514	OMRON FINS: 836, HMI/VNC: 199, DNP3: 178, Siemens S7: 29, OPC UA: 20
Salzburg	28	HMI/VNC: 8, BACnet: 5, Niagara Fox: 5, Siemens S7: 1, OPC UA: 1
Tirol (Innsbruck)	47	HMI/VNC: 13, DNP3: 9, Niagara Fox: 7, Siemens S7: 2, OPC UA: 2

Meldungen im Detail

L-01 Kühlanlagen deutscher Supermärkte angegriffen, Weg führte offenbar über den Fernwartungsdienstleister

KRITISCH Handelsblatt (dpa), 03.11.

Was ist neu: Neben Lilienthal sind laut dpa auch Märkte in Wuppertal, Wetter bei Hagen, Niederbayern, dem Münsterland und der Westpfalz betroffen. Ein Markt in Wetter-Volmarstein sagt, der Angriff habe die Firma getroffen, die die Kühlanlagen aus der Ferne wartet. Der Inhaber in Lilienthal sagt, er habe Ware im Wert von über 360.000 Euro wegwerfen müssen.

Bedeutung: Ein einzelner Fernwartungsdienstleister reicht als Einfallstor für viele Betreiber gleichzeitig. Für Stadtwerke, Wasserversorger und Produktion gilt das genauso bei Kälte, Klima und anderer Gebäudetechnik, die oft außerhalb der Leittechnik-Verantwortung läuft. Wer hinter den Angriffen steckt, ist bisher unklar.

Empfehlung: Alle Fernzugänge von Dienstleistern auflisten, dauerhafte Verbindungen abschalten und Zugriffe nur auf Anfrage, mit MFA und Protokollierung über einen Jump Host freigeben (CC4). Dienstleister schriftlich fragen, ob sie betroffen sind und welche Zugangsdaten sie für Ihre Anlagen speichern.

Quelle: https://www.handelsblatt.com/politik/deutschland/hacker-attacke-cyberangriffe-auch-auf-kuehlanlagen-deutscher-supermaerkte/100266999.html ✓ geprüft

L-02 Zyxel GS1900: Zero-Day CVE-2026-107441, 996 Switches in 48 Ländern kompromittiert

HOCH BleepingComputer, 04.11.

Was ist neu: Über einen Out-of-bounds Write im Web-Management der GS1900-Serie haben Angreifer 996 Geräte in 48 Ländern kompromittiert. GreyNoise beobachtet das seit etwa dem 17.08. Zyxel hat am 22.10. Updates veröffentlicht.

Bedeutung: Billige Managed Switches stehen oft unbeachtet in Pumpwerken, Umspannstationen oder an Maschinen. Angreifer haben laut BleepingComputer Konfigurationsdateien und gehashte Root-Zugangsdaten abgegriffen, die auch für andere Systeme gelten können.

Empfehlung: GS1900 im Asset-Inventar suchen, Firmware aktualisieren und die Weboberfläche nur aus einem Management-VLAN erreichbar machen (CC2). Passwörter, die in der Switch-Konfiguration standen, überall ändern (CC5).

Quelle: https://www.bleepingcomputer.com/news/security/zyxel-fixes-zero-day-exploited-to-hack-nearly-1-000-network-switches/ ✓ geprüft

L-03 Stadtwerke Waldbröl (NRW) erpresst, Kundendaten gestohlen

MITTEL Oberberg-Aktuell, 30.10.

Was ist neu: Die Stadtwerke wurden vor rund drei Wochen Opfer einer Erpressung, dabei wurden Kundendaten gestohlen. Laut Geschäftsführung war die Versorgung zu keinem Zeitpunkt unterbrochen oder gefährdet, das LKA ermittelt.

Bedeutung: Bei Stadtwerken treffen solche Angriffe meist zuerst die IT mit Kundendaten, nicht die Leittechnik. Ob die Trennung zur OT gehalten hat, zeigt sich nur, wenn es Monitoring und einen geübten Ablauf gibt.

Empfehlung: Den Incident-Response-Plan auf ein Erpressungsszenario mit Datenabfluss durchspielen, mit IT, OT, Datenschutz und NIS2-Meldung (CC1). Mit Netzwerk-Monitoring belegen, dass zwischen IT und OT nur erlaubte Verbindungen laufen (CC3).

Quelle: https://www.oberberg-aktuell.de/blaulicht/stadtwerke-wurden-von-russischer-hackerbande-erpresst-a-139763 ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Fernwartung von Dienstleistern über Jump Host mit MFA, Freigabe auf Anfrage und Protokollierung (CC4)	L-01	HOCH	sofort
M-02	Netzwerk-Monitoring zwischen IT und OT aufbauen, damit Lateral Movement und Webshells auffallen (CC3)	L-03	MITTEL	0 bis 3 Monate
M-03	Incident-Response-Übung zum Szenario Erpressung mit Datenabfluss inkl. NIS2-Meldung (CC1)	L-03	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Welche Dienstleister haben heute einen Fernzugang zu unseren Anlagen, auch zu Kälte, Klima und Gebäudetechnik, und wer gibt ihn frei?

2. Haben wir IoT2050, Zyxel-GS1900, Ivanti oder Sophos UTM im Einsatz, und stehen sie im Asset-Inventar?

3. Würden wir eine Webshell auf einem OT-Gateway überhaupt bemerken?

4. Wann haben wir den Incident-Response-Plan zuletzt mit einem Erpressungsszenario geübt?

Maßnahmen dieser Woche

1. Liste aller Fernwartungszugänge von Dienstleistern erstellen, dauerhafte Verbindungen trennen und Zugriffe nur auf Anfrage freigeben.

2. IoT2050 Advanced auf V4.3.4-1 oder neuer bringen, Node-RED nach unbekannten Flows und Webshells durchsuchen.

3. Ivanti Connect Secure patchen, Logs prüfen und VPN-Zugangsdaten zurücksetzen.

4. Zyxel-GS1900-Firmware vom 22.10. einspielen und gespeicherte Passwörter ändern.

5. Sophos UTM mit aktivem E-Mail-Proxy nach KBA-000049692 patchen und den Ersatz einplanen.

HINWEIS ZUR QUELLENLAGE

Die Kernaussagen habe ich in den verlinkten Quellen selbst nachgelesen (Handelsblatt, SecurityWeek, CISA, BleepingComputer, Sophos, Oberberg-Aktuell). Zu Waldbröl gibt es nur Oberberg-Aktuell, die CVE-Nummer bei Zyxel steht zusätzlich im Zyxel-Advisory vom 03.11. Nicht aufgenommen, weil nicht bestätigt oder nicht geprüft: WABAG als Opfer von „The Gentlemen“ (nur Leak-Site-Tracker, keine Firmenbestätigung), die von Synology ausgenutzten CVEs (Quellen widersprechen sich), das Sophos-EOL-Datum (im Advisory nicht genannt). Phoenix Contact VDE-2026-121 (04.11.) steht im Branchenbericht Maschinenbau, die Volexity-Analyse zu Ivanti (13.10.) im Branchenbericht Strom. Zu NIS2 in Deutschland, Österreich oder der Schweiz habe ich in dieser Woche keine neue Regelung gefunden. Alle Quellenlinks wurden am 06.11.2026 automatisch aufgerufen und inhaltlich geprüft. 4 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.