OT-CYBER.DE

WEEKLY REPORT

# OT-Cyber Situation Report All OT sectors

Edition CW 45/2026 · All OT sectors in DACH

| | |
|---|---|
| **Audience** | Operators of plants and machines, critical infrastructure (KRITIS) and industry in Germany, Austria and Switzerland (DACH) |
| **Reporting period** | 30 October 2026 to 6 November 2026 |
| **Version** | 1.0 |
| **Date** | 6 November 2026 |
| **Author** | Maximilian Gilg, OT-Cyber.de |
| **Classification** | TLP:CLEAR, public sources only |
| **Language** | English edition of the German weekly report |

This report summarises publicly available information. The relevance rating refers to operators of plants and machines in Germany, Austria and Switzerland. Dates are given as DD.MM. as in the sources.

# Executive summary

In calendar week 45 the attacks on refrigeration systems in German supermarkets were the most important OT incident for DACH. According to dpa/Handelsblatt (03.11.), stores in Wuppertal, Wetter near Hagen, Lower Bavaria, the Münsterland and the Western Palatinate were affected in addition to Lilienthal. One affected store says the actual attack hit the company that maintains the refrigeration systems remotely.

Edge devices at the boundary between IT and OT are also under pressure. On Zyxel GS1900 switches a zero-day was exploited, and 996 devices were compromised through it. Stadtwerke Waldbröl, a municipal utility, shows the familiar pattern: extortion with stolen customer data, while supply continued according to its managing director (Oberberg-Aktuell, 30.10.). This week the priorities are remote access by service providers (CC4) and patching gateways and VPN devices that are reachable from the internet (CC5).

**OVERALL ASSESSMENT · THREAT LEVEL HIGH**

The threat level is high: attackers are actively exploiting OT-adjacent gateways and remote maintenance paths, in Germany with measurable damage. First review and restrict remote access for service providers, then patch the affected Zyxel switches and every internet-facing gateway.

### Recommendation to management

This week, management should require that all remote access by service providers is listed and only released under control. This costs little and closes exactly the path that, according to one store owner, led to damage in the six-figure range at the supermarkets.

# Trends

• Attackers come in through the remote maintenance of service providers and so hit many operators at once, as the refrigeration cases in Germany show.

• OT-adjacent edge devices such as switches and VPN gateways are exploited shortly after a vulnerability becomes known, sometimes already as a zero-day.

• At municipal utilities, extortion with customer data remains the most common pattern, and the control systems are not the first target.

# Situation overview

| ID | Item | Relevance | Source |
|---|---|---|---|
| L-01 | Refrigeration systems in German supermarkets attacked, the path apparently led through the remote maintenance provider | **CRITICAL** | Handelsblatt (dpa), 03.11. |
| L-02 | Zyxel GS1900: zero-day CVE-2026-107441, 996 switches in 48 countries compromised | **HIGH** | BleepingComputer, 04.11. |
| L-03 | Stadtwerke Waldbröl (North Rhine-Westphalia) extorted, customer data stolen | **MEDIUM** | Oberberg-Aktuell, 30.10. |

# Exposed OT systems (Shodan, aggregated)

Status: 2026-11-06

We count services of typical OT protocols that are reachable from the internet. The numbers indicate attack surface, they do not prove a vulnerability. No individual systems are named. Siemens S7 = port 102 (all ISO-TSAP services, not only genuine S7 controllers), OPC UA = default port 4840.

| Region | Total | Top protocols |
|---|---|---|
| Germany | 143185 | DNP3: 32440, OMRON FINS: 26119, ProConOS: 16052, Siemens S7: 7764, OPC UA: 5141 |
| Austria | 4790 | HMI/VNC: 1046, DNP3: 970, Niagara Fox: 472, Siemens S7: 387, OPC UA: 158 |
| Bavaria (Munich) | 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 |
| Tyrol (Innsbruck) | 47 | HMI/VNC: 13, DNP3: 9, Niagara Fox: 7, Siemens S7: 2, OPC UA: 2 |

# Items in detail

## L-01 Refrigeration systems in German supermarkets attacked, the path apparently led through the remote maintenance provider

**CRITICAL** Handelsblatt (dpa), 03.11. · Where: Remote maintenance by service providers, refrigeration and building technology · Deadline: immediately

**What is new:** According to dpa, stores in Wuppertal, Wetter near Hagen, Lower Bavaria, the Münsterland and the Western Palatinate are affected in addition to Lilienthal. A store in Wetter-Volmarstein says the attack hit the company that maintains the refrigeration systems remotely. The owner in Lilienthal says he had to throw away goods worth more than 360,000 euros.

**Why it matters:** A single remote maintenance provider is enough as an entry point into many operators at once. For municipal utilities, water suppliers and production the same applies to refrigeration, HVAC and other building technology, which often runs outside the responsibility of the control system team. Who is behind the attacks is still unclear.

**Recommendation:** List all remote access by service providers, switch off permanent connections and grant access only on request, with MFA and logging through a jump host (CC4). Ask your service providers in writing whether they are affected and which credentials for your plants they store.

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

### L-02 Zyxel GS1900: zero-day CVE-2026-107441, 996 switches in 48 countries compromised

**HIGH** BleepingComputer, 04.11. · Where: Switches in small networks, outstations, control rooms · Deadline: 1 week

**What is new:** Through an out-of-bounds write in the web management of the GS1900 series, attackers compromised 996 devices in 48 countries. GreyNoise has been observing this since about 17.08. Zyxel published updates on 22.10.

**Why it matters:** Cheap managed switches often sit unnoticed in pumping stations, substations or on machines. According to BleepingComputer, attackers took configuration files and hashed root credentials, which may also be valid for other systems.

**Recommendation:** Search the asset inventory for GS1900, update the firmware and make the web interface reachable only from a management VLAN (CC2). Change any password that was stored in the switch configuration everywhere it is used (CC5).

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

### L-03 Stadtwerke Waldbröl (North Rhine-Westphalia) extorted, customer data stolen

**MEDIUM** Oberberg-Aktuell, 30.10. · Where: Customer and billing systems of a municipal utility · Deadline: 2 weeks

**What is new:** The municipal utility became the victim of extortion about three weeks earlier, and customer data was stolen. According to its management, supply was never interrupted or at risk. The State Criminal Police Office (LKA) is investigating.

**Why it matters:** At municipal utilities such attacks usually hit IT and customer data first, not the control systems. Whether the separation from OT held can only be shown if there is monitoring and a practised procedure.

**Recommendation:** Run through the incident response plan with an extortion scenario including data theft, with IT, OT, data protection and the NIS2 notification (CC1). Use network monitoring to show that only permitted connections run between IT and OT (CC3).

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

## Recommendations

| No. | Measure | Ref. | Priority | Timeframe |
|---|---|---|---|---|
| M-01 | Remote maintenance by service providers through a jump host with MFA, access on request and logging [CC4 Secure Remote Access] | L-01 | HIGH | immediately |
| M-02 | Build network monitoring between IT and OT so that lateral movement and webshells are noticed [CC3 ICS Network Visibility & Monitoring] | L-03 | MEDIUM | 0 to 3 months |
| M-03 | Incident response exercise for the scenario extortion with data theft, including the NIS2 notification [CC1 ICS Incident Response] | L-03 | MEDIUM | 0 to 3 months |

## Questions for your next team meeting

1. Which service providers have remote access to our plants today, including refrigeration, HVAC and building technology, and who approves it?

2. Do we run Zyxel GS1900 switches, and are they in the asset inventory?

3. Would we even notice a webshell on an OT gateway?

4. When did we last exercise the incident response plan with an extortion scenario?

## Actions for this week

1. Create a list of all remote maintenance access by service providers, disconnect permanent connections and grant access only on request.

2. Install the Zyxel GS1900 firmware of 22.10. and change stored passwords.

3. Check which gateways and VPN devices are reachable from the internet and bring them to the current patch level.

**NOTE ON SOURCES**

We read the core statements in the linked sources ourselves. For Waldbröl, Oberberg-Aktuell is the only source; the CVE number for Zyxel also appears in the Zyxel advisory of 03.11. Further reports of this week were not included because their quote or figures could not be confirmed in the linked source. All source links were opened and checked for content automatically on 06.11.2026. This English edition is a translation of the German weekly report of the same date; items that did not pass the source check are left out here as well.

OT-Cyber.de, Rosenheim (Bavaria). Questions about this report or support for your plants: ot-cyber.de/en