

WOCHENBERICHT

OT-/Cyber-Lagebild Gesamt

Ausgabe KW 42/2026 · Gesamt – alle OT-Branchen in DACH

Zielgruppe	Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH
Berichtszeitraum	09.10.2026–16.10.2026
Version	1.0
Datum	16.10.2026
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 42 standen Angriffe auf Kühlsteuerungen in Frankreich im Mittelpunkt, die direkt aus dem Internet erreichbar waren. In der Nacht vom 11. auf den 12.10. wurden Kühlsteuerungen von Supermärkten manipuliert. CERT-FR nennt Danfoss AK-SM/AK-SC sowie Copeland xweb und Dixell xweb und hält die Kampagne für wahrscheinlich noch aktiv. Das BSI hat am 13.10. die Empfehlung BSI-CS 154 veröffentlicht. Darin warnt es Betreiber kleiner vernetzter Anlagen (Kühlung, PV-Wechselrichter, einzelne Windkraftanlagen, Trinkwasserstellen) und fordert, den direkten Internetzugriff auf Steuerungen zu unterbinden. Laut Handelsverband BVLH gibt es in Deutschland bisher keinen bestätigten Fall, ein bestätigter Fall in DACH ist nicht bekannt. Parallel werden zwei Edge-Geräte aktiv angegriffen, die bei vielen Betreibern die Grenze zwischen IT und OT schützen: Ivanti Connect Secure (Zero-Day CVE-2026-104935, für die Privilege Escalation gibt es noch keinen Patch) und die Management-Oberfläche von Palo Alto PAN-OS (CVE-2026-0322). Beide stehen im KEV-Katalog der CISA.

Bei den Advisories ist für die Leittechnik vor allem Eclipse Milo wichtig (ICSA-26-288-01, sechs CVEs im OPC-UA-Server), außerdem Rockwell 1732E ArmorBlock I/O (SD1801, CVSS 9,1). Die Modat-Studie zählt 884 aus dem Internet erreichbare Steuerungs- und Verwaltungssysteme von Solar- und Windparks in Deutschland. Beim Baukonsortium des Fehmarnbelt-Tunnels hat ein Cybervorfall den Baustellenbetrieb gestört. Der rote Faden der Woche ist der Remote Access: Fernwartungszugänge, VPN-Gateways und Management-Oberflächen sind das Einfallstor. Diese Woche zuerst von außen prüfen, welche Steuerungen, Portale und VPN-Gateways im Internet sichtbar sind. SANS CC4 (Secure Remote Access) und CC2 (Defensible Architecture) gehören ganz nach oben.

GESAMTBEWERTUNG

Die Lage ist hoch: Eine laufende Kampagne richtet sich gegen OT-Steuerungen in Europa, die aus dem Internet erreichbar sind, und kann Nachahmer finden. Gleichzeitig werden Lücken in VPN- und Firewall-Gateways aktiv ausgenutzt. Vorrang haben das Sperren direkter Internetzugriffe auf Steuerungen sowie Patches und Compromise Assessment für Ivanti Connect Secure und PAN-OS.

Trends

- Angreifer zielen auf Herstellerfernwartung und Steuerungen kleiner Anlagen, die direkt aus dem Internet erreichbar sind (Kühlung, PV, Wind). Diese Anlagen laufen oft außerhalb der KRITIS-Regulierung und stehen selten im Asset-Inventar. Behörden in Frankreich und Deutschland warnen deshalb jetzt Betreiber, die bisher kaum im Fokus standen.
- Gateways an der Netzgrenze bleiben der wichtigste Einstieg: Ivanti Connect Secure und Palo Alto PAN-OS wurden in derselben Woche aktiv angegriffen, bei Ivanti ohne Malware auf dem Gerät und damit schwer zu erkennen.
- Ausfälle bei Dienstleistern stoppen den physischen Betrieb, wie der Vorfall beim Fehmarnbelt-Konsortium mit gestörtem Zutritt und gestörter Baulogistik zeigt.
- Lücken in eingebetteten Komponenten wie Eclipse Milo erkennen Betreiber nur noch über die SBOMs ihrer Hersteller. Dadurch wird die SBOM zum Werkzeug im Vulnerability Management.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Angriffswelle auf Kühlsteuerungen in französischen Supermärkten: CERT-FR erweitert Warnung, BSI veröffentlicht BSI-CS 154	KRITISCH	CERT-FR (CERTFR-2026-ALE-012); BSI (BSI-CS 154), über heise, 13.10.
L-02	Ivanti Connect Secure: Zero-Day aktiv ausgenutzt, Privilege Escalation noch ohne Patch (CVE-2026-104935)	KRITISCH	Ivanti / Volexity (via BleepingComputer); Rapid7; CISA KEV, 13.10.
L-03	Palo Alto PAN-OS: Codeausführung als root über die Management-Oberfläche wird ausgenutzt (CVE-2026-0322)	HOCH	Palo Alto Networks PSIRT / CISA KEV, 14.10.
L-04	Eclipse Milo: sechs Lücken im OPC-UA-Server, Fix nur in Version 1.1.5 (ICSA-26-288-01)	HOCH	CISA ICS Advisory, 15.10.
L-05	Rockwell 1732E ArmorBlock I/O: Webserver-Passwort lässt sich ohne Anmeldung ändern (SD1801)	HOCH	Rockwell Automation Trust Center, 13.10.
L-06	Wind- und Solarparks: 8.547 Systeme in Europa offen im Internet, 884 davon in Deutschland	HOCH	heise online (Studie Modat / NCSC-NL), 09.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 16.10.2026):

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	143086	DNP3: 33392, OMRON FINS: 23267, ProConOS: 16506, Siemens S7: 8211, OPC UA: 5676
Österreich	4649	HMI/VNC: 1053, DNP3: 949, IEC-104: 454, Siemens S7: 357, OPC UA: 139
Bayern (München)	1364	OMRON FINS: 694, HMI/VNC: 198, DNP3: 169, Siemens S7: 32, OPC UA: 22
Salzburg	26	HMI/VNC: 7, Niagara Fox: 5, BACnet: 4, Siemens S7: 1, OPC UA: 2
Tirol (Innsbruck)	44	HMI/VNC: 13, DNP3: 7, Niagara Fox: 6, Siemens S7: 3, OPC UA: 1

Meldungen im Detail

L-01 Angriffswelle auf Kühlsteuerungen in französischen Supermärkten: CERT-FR erweitert Warnung, BSI veröffentlicht BSI-CS 154

KRITISCH CERT-FR (CERTFR-2026-ALE-012); BSI (BSI-CS 154), über heise, 13.10.

Was ist neu: CERT-FR hat die Warnung CERTFR-2026-ALE-012 am 12.10. veröffentlicht und am 13.10. erweitert. Betroffen sind Danfoss AK-SC und AK-SM sowie Copeland xweb und Dixell xweb. Laut einer der beiden Recherchen sind rund 700 französische Supermärkte betroffen. Die Angreifer haben unter anderem die Abtauzeiten verändert. CERT-FR weiß von zahlreichen Kompromittierungen und hält die Kampagne wahrscheinlich für noch aktiv. Am 13.10. hat das BSI die Empfehlung BSI-CS 154 „Gefährdung durch internet-verbundene OT-Systeme“ für Betreiber kleiner vernetzter Anlagen veröffentlicht.

Bedeutung: Laut BVLH sind in Deutschland bisher keine Märkte betroffen, ein bestätigter Fall in DACH ist nicht bekannt. Laut heise sind in Deutschland aber einige potenziell verwundbare Systeme aus dem Internet erreichbar, wenn auch in geringer Zahl. Dieselben Steuerungen laufen in DACH in Kühlhäusern, Supermärkten, Kühlketten, in der Lebensmittelproduktion, in Rechenzentren und in kommunalen Gebäuden, oft mit Fernwartung durch den Kältedienstleister direkt über das Internet. Laut CERT-FR reicht ein Factory Reset nicht: End-of-Life-Geräte, die weiter im Internet erreichbar sind, werden sehr wahrscheinlich wieder kompromittiert.

Empfehlung: Alle Danfoss-, Copeland- und Dixell-Steuerungen sowie andere Kühl- und Gebäudesteuerungen mit öffentlicher IP vom Internet trennen und den Zugang für Dienstleister nur noch über VPN mit MFA freigeben (CC4). Sollwerte, Konfiguration und Abtauzeiten prüfen, Standardpasswörter ändern, bei Danfoss-Geräten den Sicherheitsmodus „Strict“ setzen und End-of-Life-Geräte für den Austausch einplanen (CC5).

Quelle: <https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/> ✓ geprüft

L-02 Ivanti Connect Secure: Zero-Day aktiv ausgenutzt, Privilege Escalation noch ohne Patch (CVE-2026-104935)

KRITISCH Ivanti / Volexity (via BleepingComputer); Rapid7; CISA KEV, 13.10.

Was ist neu: Ivanti hat am 13.10. die Authentication-Bypass-Lücke CVE-2026-104935 (CVSS 8,6) gepatcht. Über sie können Angreifer ohne Anmeldung Befehle auf dem Gateway ausführen. Laut Volexity kombiniert der Threat Actor UTA0576 sie mit einer Privilege Escalation, für die es noch keinen Patch gibt. So erlangt er Root-Rechte, auch auf voll gepatchten Geräten, und stiehlt Active-Directory-Zugangsdaten. Die CISA hat die Lücke am 13.10. in den KEV-Katalog aufgenommen. Zum Beginn der Ausnutzung gibt es zwei Angaben (widersprüchlich: ab 01.10. laut BleepingComputer / ab 03.10. laut Volexity). Gesichert ist: seit Anfang Oktober.

Bedeutung: Ivanti-VPNs sind bei Stadtwerken, Versorgern und Industriebetrieben ein typischer Zugangsweg für Fernwartung durch Dienstleister und eigene Techniker. Laut Berichten hinterlässt der Angreifer weder Malware noch Webshell und manipuliert die Logs. Das Integrity Checker Tool erkennt den Angriff daher womöglich nicht. Mit gestohlenen AD-Zugangsdaten beginnt Lateral Movement bis zu den Jump Hosts vor der OT.

Empfehlung: Sofort auf 22.8R2.5, 25.1.1.2 bzw. 25.1.3.x aktualisieren und sich nicht allein auf das Integrity Checker Tool verlassen. IoCs von Volexity, Logs und Netzwerkverkehr des Gateways prüfen und Konten und Dienstkonten zurücksetzen, die über das VPN genutzt wurden (CC1, CC4). Bis die Privilege Escalation behoben ist, den OT-Zugang hinter dem VPN zusätzlich über einen Jump Host mit eigener MFA absichern.

Quelle: <https://www.volexity.com/blog/2026/10/13/a-series-of-unauthenticated-events-chained-exploitation-of-ivanti-connect-secure-zero-days/> ✓ geprüft

L-03 Palo Alto PAN-OS: Codeausführung als root über die Management-Oberfläche wird ausgenutzt (CVE-2026-0322)

HOCH Palo Alto Networks PSIRT / CISA KEV, 14.10.

Was ist neu: Palo Alto hat die Lücke CVE-2026-0322 (CVSS 4.0: 8,6) am 14.10. veröffentlicht und das Advisory am 15.10. aktualisiert. Wer gültige Admin-Zugangsdaten hat und die Management-Oberfläche erreicht, kann Code als root ausführen. Betroffen sind PA-Series, VM-Series und Panorama mit PAN-OS 10.2 bis 12.2, einen Workaround gibt es nicht. Palo Alto meldet eine sehr begrenzte Ausnutzung und nennt drei Angreifer-IPs. Die CISA hat die Lücke am 14.10. in den KEV-Katalog aufgenommen.

Bedeutung: Viele Betreiber in DACH trennen Büronetz und Produktion mit PAN-OS-Firewalls. Wer diese Firewall übernimmt, kann die Segmentierung aushebeln. Die nötigen Admin-Zugangsdaten können zum Beispiel aus Angriffen wie dem auf Ivanti stammen.

Empfehlung: Patches einspielen und die Management-Oberfläche nur aus einem eigenen Admin-Netz oder über einen Jump Host erreichbar machen (CC2). Admin-Konten mit MFA absichern. Admin-Logins der letzten Wochen auf ungewöhnliche Quellen prüfen und Logs nach Zugriffen von 66.42.72.14, 208.83.239.114 und 149.248.47.234 durchsuchen (CC3).

Quelle: <https://security.paloaltonetworks.com/CVE-2026-0322> ✓ geprüft

L-04 Eclipse Milo: sechs Lücken im OPC-UA-Server, Fix nur in Version 1.1.5 (ICSA-26-288-01)

HOCH CISA ICS Advisory, 15.10.

Was ist neu: CISA meldet sechs CVEs im Server-Teil der Java-Bibliothek Eclipse Milo (Versionen 0.6.0 bis 1.1.4). Darunter sind fehlende Autorisierung für anonyme Clients (CVE-2026-58080, CVSS 3.1: 8,2), ein Padding Oracle, über das sich Passwörter zurückgewinnen lassen (CVE-2026-60007, CVSS 4.0: 9,1), und ein Speicherverlust, der einen Absturz auslösen kann (CVE-2026-63252). Behoben ist das nur in 1.1.5, für den 0.6.x-Zweig gibt es keinen Fix.

Bedeutung: Milo steckt als Komponente in Produkten anderer Hersteller und taucht deshalb selten im eigenen Asset-Inventar auf. Betreiber brauchen Angaben ihrer Hersteller. Die CISA nennt ausdrücklich die Sektoren Energie, Wasser und Abwasser, Chemie und kritische Fertigung.

Empfehlung: Bei Herstellern von SCADA, Gateways und Leittechnik nachfragen, ob Milo in ihrer SBOM steckt, und ihren Patchplan einfordern (CC5). Bis dahin anonyme OPC-UA-Sessions abschalten und OPC-UA-Server nur aus der OT-Zone erreichbar machen (CC2).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-288-01> ✓ geprüft

L-05 Rockwell 1732E ArmorBlock I/O: Webserver-Passwort lässt sich ohne Anmeldung ändern (SD1801)

HOCH Rockwell Automation Trust Center, 13.10.

Was ist neu: Über CVE-2026-12655 (CVSS 3.1: 9,1) können Angreifer ohne Konto das Webserver-Passwort der 1732E ArmorBlock I/O ändern und so die Administration übernehmen. CVE-2026-12656 (CVSS 3.1: 7,5) legt die Kommunikation per Storm-Traffic lahm, danach muss das Gerät neu gestartet werden. Betroffen ist Firmware bis 3.012, Version 3.013 behebt beide Lücken, einen Workaround gibt es nicht. (Relevanz widersprüchlich: A MITTEL / B HOCH, wegen CVSS 9,1 als HOCH übernommen.)

Bedeutung: Allen-Bradley-Peripherie ist in DACH in Wasser, Abwasser und Fertigung verbreitet. ArmorBlock-I/O sitzt direkt an Prozess und Maschine. Ein Ausfall stoppt Signale an die Steuerung und damit den Prozess, auch wenn die SPS selbst nicht betroffen ist. Eine Übernahme ermöglicht Manipulation am Feldgerät.

Empfehlung: Betroffene Module im Asset-Inventar suchen und Firmware 3.013 im nächsten Wartungsfenster einspielen. Bis dahin die Geräte in eine eigene Zone legen und den Webserver aus Büronetz und Fernwartung unerreichbar machen (CC2, CC5).

Quelle: <https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1801.html> ✓ geprüft

L-06 Wind- und Solarparks: 8.547 Systeme in Europa offen im Internet, 884 davon in Deutschland

HOCH heise online (Studie Modat / NCSC-NL), 09.10.

Was ist neu: Die Studie „To see the wind and the sun“ von Modat und dem niederländischen NCSC zählt in 35 Ländern 8.547 Steuerungs- und Verwaltungssysteme von Wind- und Solarparks, die aus dem Internet erreichbar sind (7.942 Solar, 605 Wind). Die Forscher nennen die Zahl eine Untergrenze. In Deutschland sind es 672 Solar- und 212 Windpark-Systeme, bei Wind liegt Deutschland vorn. An rund 181 Standorten wären Fernsteuerfunktionen erreichbar, etwa Turbinen starten, stoppen und zurücksetzen. (Relevanz widersprüchlich: A HOCH / B MITTEL, laut Tagesbriefing hoch.)

Bedeutung: Ein erfolgreicher Angriff ist nicht belegt. Stadtwerke und Direktvermarkter mit eigenen Parks haben aber dasselbe Muster wie bei den Kühlsteuerungen in Frankreich: Herstellerportale und Regler, die direkt erreichbar sind. Das BSI zählt in BSI-CS 154 die Stromerzeugung, einzelne Windkraftanlagen und PV-Wechselrichter ausdrücklich zu den gefährdeten Anlagen.

Empfehlung: Eigene öffentliche IP-Bereiche und die der Betriebsführer und Parkbetreiber scannen lassen, etwa mit Shodan oder Censys, und erreichbare Parkregler und Portale hinter VPN legen (CC4). Verträge mit Betriebsführern und Dienstleistern um Vorgaben zum Remote Access ergänzen.

Quelle: <https://www.heise.de/news/Tausende-europaeische-Windanlagen-und-Solarparks-offen-im-Internet-11482262.html> ✓ geprüft

Fragen für das nächste Jour fixe

1. Welche unserer Steuerungen, Portale und Fernwartungszugänge sind heute aus dem Internet erreichbar, und wer hat darauf Zugriff?
2. Betreiben wir oder unsere Dienstleister Kühl- und Gebäudesteuerungen von Danfoss, Copeland oder Dixell, und sind diese nur über VPN mit MFA erreichbar?
3. Sind unsere Ivanti-Connect-Secure-Gateways gepatcht und auf Kompromittierung geprüft, und ist der OT-Zugang zusätzlich über einen Jump Host mit eigener MFA abgesichert?
4. Ist die Management-Oberfläche unserer PAN-OS-Firewalls nur aus einem eigenen Admin-Netz erreichbar?
5. Haben unsere Hersteller von SCADA, Gateways und Leittechnik bestätigt, ob Eclipse Milo in ihrer SBOM steckt?
6. Was läuft weiter, wenn die IT eines kritischen Dienstleisters ausfällt, und steht dieses Szenario in unserem Incident-Response-Plan?

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 16.10.2026 automatisch aufgerufen und inhaltlich geprüft. 1 Meldung(en) ohne überprüfbare Originalquelle wurden nicht aufgenommen.