OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Gesamt: alle OT-Branchen

Ausgabe KW 46/2026 · Gesamt: alle OT-Branchen in DACH

Zielgruppe	Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH
Berichtszeitraum	06.11.2026 bis 13.11.2026
Version	1.0
Datum	13.11.2026
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

Im Berichtszeitraum (06. bis 13.11.) lag der Schwerpunkt auf zwei Themen: Kälteanlagen und Fernwartungszugänge. Laut BleepingComputer (09.11.) schreibt Frankreich die Oktober-Angriffe auf Danfoss-Kühlsteuerungen in rund 700 angegriffenen Geschäften einer Einheit zu, die den iranischen Revolutionsgarden nahesteht. Die spätere Welle im November in sechs europäischen Ländern ist nicht zugeordnet. Unsere Einschätzung: Geräte dieser Hersteller dürften auch in DACH im Einsatz sein, fernwartbare Kältetechnik gehört deshalb ins OT-Asset-Inventar.

Die zweite Baustelle ist der Remote Access. Am 10.11. hat MB connect line über CERT@VDE zwei PHP-Lücken im Fernwartungsportal mbCONNECT24 veröffentlicht (Remote Code Execution ohne Anmeldung, CVSS 3.1: 9,8 und 8,1). Die CISA führt eine SonicWall-SSL-VPN-Lücke seit dem 06.11. als aktiv ausgenutzt. Siemens hat für den WinCC Graphics Designer noch keinen Fix. Für OpenSSH auf Linux-Systemen mit musl libc ohne PAM gibt es den Fix in OpenSSH 10.6p2. Wer diese Woche nur eine Sache schafft: Fernwartungsportale und VPN-Gateways patchen und Kälteregler vom Internet trennen.

GESAMTBEWERTUNG

Die Lage ist erhöht: Frankreich schreibt die Oktober-Angriffe auf Kühlanlagen in französischen Geschäften einem staatlichen Akteur zu, und das Fernwartungsportal mbCONNECT24 hat eine kritische Lücke ohne Anmeldung. Vorrang haben Secure Remote Access (CC4) und das Abschotten erreichbarer Kälteregler.

Trends

• Kältetechnik wird zum festen OT-Angriffsziel: Nach den Angriffen in Frankreich, der Zuordnung der Oktober-Angriffe und dem US-Fact-Sheet (05.11.) geht es jetzt um die Geräte, die nach unserer Einschätzung auch in DACH-Betrieben stehen.

• Eine einzelne PHP-Lücke (CVE-2026-109618) taucht über Komponenten von Drittanbietern in mehreren DACH-Produkten auf, von mbCONNECT24 bis zu Routern von Weidmüller und ads-tec, und das mit sehr unterschiedlicher Schwere.

• Fernwartungsportale und VPN-Gateways bleiben der wichtigste Initial Access in die OT, diese Woche mit Lücken bei MB connect line, Helmholz und SonicWall.

• Embedded-Linux in Edge-Geräten bringt Lücken aus der IT-Welt in die Anlage, und der Patch hängt am Hersteller (OpenSSH SSHole).

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	MB connect line mbCONNECT24: Remote Code Execution ohne Anmeldung über gebündeltes PHP (VDE-2026-128, CVSS 9,8)	KRITISCH	MB connect line, koordiniert von CERT@VDE, 10.11.
L-02	Kühlanlagen-Angriffe: Frankreich macht IRGC-nahe Einheit „Shahid Kaveh“ verantwortlich	HOCH	BleepingComputer, 09.11.
L-03	SonicWall SonicOS SSL-VPN: CVE-2026-19868 aktiv ausgenutzt (CISA KEV)	HOCH	CISA, 06.11.

ID	Meldung	Relevanz	Quelle
L-04	OpenSSH „SSHole“: Login ohne gültiges Passwort auf Linux mit musl libc ohne PAM (behoben in OpenSSH 10.6p2)	HOCH	OpenSSH (oss-security) / SecurityWeek, 06.11.
L-05	Siemens SIMATIC WinCC Graphics Designer: Code-Ausführung über präparierte Datei, noch kein Fix (SSA-979641)	MITTEL	Siemens ProductCERT, 10.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 13.11.2026):

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	139840	DNP3: 31446, OMRON FINS: 26419, ProConOS: 15503, Siemens S7: 7574, OPC UA: 4952
Österreich	4663	HMI/VNC: 1007, DNP3: 959, Niagara Fox: 456, Siemens S7: 381, OPC UA: 149
Bayern (München)	1525	OMRON FINS: 849, HMI/VNC: 200, DNP3: 183, Siemens S7: 28, OPC UA: 24
Salzburg	29	HMI/VNC: 8, Niagara Fox: 7, BACnet: 5, Siemens S7: 1, OPC UA: 1
Tirol (Innsbruck)	41	HMI/VNC: 11, DNP3: 9, Niagara Fox: 6, Siemens S7: 2, OPC UA: 1

Meldungen im Detail

L-01 MB connect line mbCONNECT24: Remote Code Execution ohne Anmeldung über gebündeltes PHP (VDE-2026-128, CVSS 9,8)

KRITISCH MB connect line, koordiniert von CERT@VDE, 10.11.

Was ist neu: mbCONNECT24 und mymbCONNECT24 ab Version 2.0.0 und vor 2.21.6 enthalten ein PHP mit CVE-2026-109618 (CVSS 3.1: 9,8) und CVE-2026-109619 (CVSS 3.1: 8,1). Laut Advisory können beide Lücken zu Remote Code Execution ohne Anmeldung führen. Behoben ist das in Version 2.21.6. Eine Ausnutzung meldet das Advisory nicht.

Bedeutung: Über so ein Portal laufen die Fernwartungsverbindungen zu vielen Maschinen und Anlagen gleichzeitig. Wer das Portal übernimmt, hat damit einen Initial Access zu allen angebundenen Anlagen. Nach unserer Erfahrung haben viele Betreiber das Portal nicht selbst im Betrieb, es läuft beim Maschinenbauer.

Empfehlung: Selbst betriebene Instanzen sofort auf 2.21.6 bringen. Bei gehosteten Instanzen den Maschinenbauer schriftlich nach Patchstand und Datum fragen und bis dahin die Verbindungen nur bei Bedarf aufbauen.

Quelle: https://certvde.com/en/advisories/VDE-2026-128/ ✓ geprüft

L-02 Kühlanlagen-Angriffe: Frankreich macht IRGC-nahe Einheit „Shahid Kaveh“ verantwortlich

HOCH BleepingComputer, 09.11.

Was ist neu: Laut BleepingComputer schreibt Frankreich die Angriffe vom Oktober auf Kühlsysteme in rund 700 angegriffenen Supermärkten und anderen Geschäften der Einheit Shahid Kaveh zu, die den iranischen Revolutionsgarden nahesteht. Dabei wurden kompromittierte Danfoss-Kühlregler genutzt, es gab mindestens 15 Brände. Frankreich will neue EU-Sanktionen vorschlagen. Die spätere Welle im November mit über 115 Geschäften in sechs europäischen Ländern ist nicht zugeordnet.

Bedeutung: Damit sind die Oktober-Angriffe in Frankreich einem Staat zugeordnet, die November-Welle nicht. Unsere Einschätzung für Betreiber in DACH: Dieselben Gerätetypen sind hier im Einsatz, und eine EU-Sanktionsdebatte kann weitere Angriffe auslösen.

Empfehlung: Für Kühl- und Kälteanlagen festlegen, wer im Ernstfall abschaltet und wie der Betrieb ohne Fernsteuerung läuft (CC1). Bei Sollwerten Plausibilitätsgrenzen mit Alarm einrichten.

Quelle: https://www.bleepingcomputer.com/news/security/france-blames-iranian-hackers-for-supermarket-attacks-that-sparked-fires/ ✓ geprüft

L-03 SonicWall SonicOS SSL-VPN: CVE-2026-19868 aktiv ausgenutzt (CISA KEV)

HOCH CISA, 06.11.

Was ist neu: Die CISA hat CVE-2026-19868 in SonicOS SSLVPN (Use of Single-factor Authentication) in den KEV-Katalog aufgenommen, weil es Belege für aktive Ausnutzung gibt.

Bedeutung: SonicWall-Firewalls sind bei kleineren Stadtwerken, Zweckverbänden und im Mittelstand oft das einzige Tor in die OT. Ein übernommener VPN-Zugang ist ein direkter Initial Access ins Anlagennetz.

Empfehlung: Herstellerhinweis zu CVE-2026-19868 lesen und patchen, phishing-resistente MFA am SSL-VPN erzwingen und die VPN-Logs der letzten Wochen auf Anmeldungen zu ungewöhnlichen Zeiten oder aus fremden Ländern prüfen.

Quelle: https://www.cisa.gov/news-events/alerts/2026/11/06/cisa-adds-one-known-exploited-vulnerability-catalog ✓ geprüft

L-04 OpenSSH „SSHole“: Login ohne gültiges Passwort auf Linux mit musl libc ohne PAM (behoben in OpenSSH 10.6p2)

HOCH OpenSSH (oss-security) / SecurityWeek, 06.11.

Was ist neu: Die Lücke betrifft sshd auf Linux-Systemen mit musl libc und abgeschaltetem PAM, laut SecurityWeek unter anderem Alpine, OpenWrt, Buildroot und Yocto. Mit einem Passwort von 257 bis 1.024 Zeichen ist unter bestimmten Bedingungen eine Anmeldung möglich. Behoben ist das in OpenSSH 10.6p2, Alpine hat am 05.11. zum Patchen aufgerufen. Eine Ausnutzung ist laut Detectify noch nicht bekannt, die Details sind aber öffentlich.

Bedeutung: Viele Industrie-Router, Fernwirk-Gateways und Edge-Geräte bauen auf genau diesen Embedded-Distributionen auf. Ob ein Produkt betroffen ist, kann nur der Hersteller sagen, deshalb kommt der Fix hier oft erst Wochen später.

Empfehlung: Im Asset-Inventar Geräte mit SSH-Zugang auf Embedded-Linux-Basis markieren und bei den Herstellern nach der Betroffenheit fragen. Bis zum Update Passwort-Logins abschalten oder SSH nur aus dem Verwaltungsnetz zulassen.

Quelle: https://www.securityweek.com/openssh-rushes-patches-for-sshole-authentication-bypass/ ✓ geprüft

L-05 Siemens SIMATIC WinCC Graphics Designer: Code-Ausführung über präparierte Datei, noch kein Fix (SSA-979641)

MITTEL Siemens ProductCERT, 10.11.

Was ist neu: CVE-2026-59082 (CVSS 3.1: 7,8) betrifft den Graphics Designer in WinCC V7.5, V8.0 und V8.1, jeweils alle Versionen. Wer eine präparierte Datei öffnet, kann Code ausführen. Einen Fix gibt es noch nicht, Siemens bereitet ihn vor.

Bedeutung: WinCC ist in der DACH-Industrie und bei Versorgern weit verbreitet. Projektdateien kommen oft per Mail oder USB vom Integrator. Damit kann eine einzige manipulierte Datei die Engineering-Station übernehmen.

Empfehlung: Projektdateien von außen nur nach Prüfung und aus bekannten Quellen öffnen. Engineering-Stationen vom Büronetz trennen (CC2) und den Fix einplanen, sobald Siemens ihn veröffentlicht.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-979641.html ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Fernwartungsportale (mbCONNECT24, myREX24) beim Dienstleister patchen lassen und Verbindungen nur bei Bedarf freischalten [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Notfallplan für Kälte- und Kühlanlagen mit Abschaltweg und Handbetrieb erstellen und üben [CC1 ICS Incident Response]	L-02	MITTEL	0 bis 3 Monate
M-03	Risikobasiertes Schwachstellenmanagement für Edge-Geräte und Router: Herstelleranfragen zu OpenSSH und PHP2Shell nachverfolgen [CC5 Risk-Based Vulnerability Management]	L-04	MITTEL	0 bis 3 Monate
M-04	Engineering-Stationen (WinCC) segmentieren und Dateiannahme über eine Prüfstation führen [CC2 Defensible Architecture]	L-05	NIEDRIG	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Welche Kälte- und Kühlregler (Danfoss AK-SM und andere) haben wir, und wer hat darauf Fernzugriff?

2. Laufen bei unseren Maschinenbauern Fernwartungsportale wie mbCONNECT24 oder myREX24, und wann sind sie gepatcht?

3. Ist unser VPN-Gateway mit phishing-resistenter MFA abgesichert, und wer prüft die Logs?

4. Welche Edge-Geräte und Router haben SSH offen, und was sagen die Hersteller zu SSHole (OpenSSH 10.6p2)?

5. Wie öffnen wir WinCC-Projektdateien vom Integrator, und gibt es dafür eine Prüfstation?

Maßnahmen dieser Woche

1. Kälteregler (laut CERT-FR unter anderem Danfoss AK-SM und AK-SC, Copeland und Dixell XWEB) im Asset-Inventar suchen, Erreichbarkeit aus dem Internet prüfen und den Firmware-Stand beim Hersteller abfragen.

2. Bei allen Maschinen- und Anlagenbauern den Patchstand von mbCONNECT24 (2.21.6) und myREX24V2 (ab 2.21.0) schriftlich abfragen.

3. SonicWall-SSL-VPN patchen und die VPN-Logs der letzten 30 Tage auf ungewöhnliche Anmeldungen prüfen.

4. Weboberflächen von Weidmüller IE-SR und ads-tec-Routern nur aus dem Verwaltungsnetz erreichbar machen und Updates planen.

5. Für Kühl- und Kälteanlagen einen Notbetrieb ohne Fernsteuerung festlegen und mit dem Dienstleister abstimmen.

HINWEIS ZUR QUELLENLAGE

Geprüft haben wir die Primärquellen CISA, CERT@VDE und Siemens sowie die OpenSSH-Meldung auf oss-security (05.11., ohne CVE-Kennung; eine in der Presse genannte CVE-Nummer haben wir nicht bestätigt und deshalb weggelassen). Eine BSI-Warnung zum Danfoss AK-SM 800A vom 13.11. haben wir in keiner Primärquelle gefunden, sie ist gestrichen. Die französische Zuordnung ist nur über BleepingComputer belegt, die Erklärung des Außenministeriums selbst haben wir nicht gefunden. Nicht aufgenommen, weil nicht ausreichend belegt: die Meldung eines Blogs (shattered.io), das BSI habe Vorfälle bei Supermärkten in Deutschland bestätigt; die Fix-Versionen zu SonicWall CVE-2026-19868; konkrete OT-Vorfälle in Österreich und der Schweiz in KW 46 (keine gefunden). Das US-Fact-Sheet zu Kühlanlagen vom 05.11. liegt vor dem Berichtszeitraum. Alle Quellenlinks wurden am 13.11.2026 automatisch aufgerufen und inhaltlich geprüft. 2 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.