OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Maschinen- und Anlagenbau

Ausgabe KW 46/2026 · Maschinen- und Anlagenbau in DACH

Zielgruppe	Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren
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 Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren in Deutschland, Österreich und der Schweiz.

Management Summary

Die Woche brachte vor allem Schwachstellen in Fernwartungsportalen und Edge-Software. Am 10.11. hat MB connect line über CERT@VDE das Advisory VDE-2026-128 zu mbCONNECT24/mymbCONNECT24 veröffentlicht: Zwei PHP2Shell-Lücken erlauben dort Remote Code Execution ohne Anmeldung (CVSS 3.1: 9,8 und 8,1), behoben ist das in 2.21.6. Zum Fernwartungsserver myREX24V2 von Helmholz kamen am selben Tag 12 CVEs (VDE-2026-141). Siemens meldet für den WinCC Graphics Designer eine Lücke beim Öffnen von Dateien, für die es noch keinen Fix gibt (SSA-979641). Bei Siemens Industrial Edge Management sind mehrere Configurator-Apps über eine Brotli-Lücke angreifbar (CVE-2026-111497, CVSS 3.1: 9,8), für den Common Configurator gibt es noch keinen Fix.

Für die Produkt-Security unter dem Cyber Resilience Act ist die OpenSSH-Lücke „SSHole“ wichtig, behoben in OpenSSH 10.6p2. Betroffen sind Linux-Systeme mit musl libc und abgeschaltetem PAM, laut SecurityWeek unter anderem Alpine, OpenWrt, Buildroot und Yocto. Nach unserer Einschätzung bauen viele Hersteller solche Distributionen in eigene Steuerungen, HMIs und Gateways ein. Wer solche Produkte ausliefert, braucht eine aktuelle SBOM, sonst kann er nicht schnell sagen, welche Firmware-Stände betroffen sind. Zu CRA-Normen und Maschinenverordnung haben wir in dieser Woche keine belegte neue Entscheidung gefunden.

GESAMTBEWERTUNG

Die Lage ist erhöht, weil das Fernwartungsportal mbCONNECT24 Lücken ohne Anmeldung hat und der Fernwartungsserver myREX24V2 12 Schwachstellen. Vorrang haben die Updates von mbCONNECT24 auf 2.21.6 und von myREX24V2 auf mindestens 2.21.0 sowie eine Prüfung eigener Embedded-Linux-Produkte auf SSHole.

Trends

• Die PHP2Shell-Lücken (CVE-2026-109618/-109619) tauchen Woche für Woche in weiteren OT-Produkten auf, diese Woche bei MB connect line, Weidmüller, ads-tec und Siemens.

• Fernwartungsportale und Industrie-Router der Hersteller selbst sind das häufigste Thema in den Advisories von CERT@VDE.

• Embedded-Linux-Bausteine wie OpenSSH, PHP und Brotli machen Drittkomponenten zum größten Patch-Aufwand für Komponentenhersteller, ohne SBOM ist das kaum zu überblicken.

• Bei Kälte- und Gebäudetechnik ist mit Frankreichs Zuordnung der Oktober-Angriffe jetzt ein staatlicher Akteur benannt.

• Für die Cybersecurity-Anforderungen der Maschinenverordnung (Anwendung ab 20.01.2027) haben wir weiter keine Entscheidung über eine Verschiebung gefunden.

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.

ID	Meldung	Relevanz	Quelle
L-02	Helmholz myREX24V2 / myREX24V2.virtual: 12 Schwachstellen im Fernwartungsserver (VDE-2026-141)	HOCH	CERT@VDE, 10.11.
L-03	Siemens SIMATIC WinCC Graphics Designer: Code-Ausführung über präparierte Datei, noch kein Fix (SSA-979641)	MITTEL	Siemens ProductCERT, 10.11.
L-04	Siemens Industrial Edge Management: Brotli-Lücke in Configurator-Apps, CVSS 9,8, teils ohne Fix (ICSA-26-316-03)	HOCH	CISA / Siemens ProductCERT, 12.11.
L-05	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-06	SonicWall SonicOS SSLVPN: aktiv ausgenutzte Lücke im CISA-KEV (CVE-2026-19868)	HOCH	CISA, 06.11.
L-07	Kühlanlagen-Angriffe: Frankreich macht IRGC-Einheit „Shahid Kaveh“ verantwortlich	MITTEL	BleepingComputer, 09.11.

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

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: Viele Maschinenbauer betreiben mbCONNECT24 als eigenes Portal für die Fernwartung beim Kunden. Wer das Portal übernimmt, kommt im schlimmsten Fall an alle angebundenen Kundenanlagen, und die Haftungsfrage landet beim Hersteller.

Empfehlung: Eigene Instanzen sofort auf 2.21.6 bringen, danach die Zugriffslogs prüfen und betroffene Kunden informieren (CC4).

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

L-02 Helmholz myREX24V2 / myREX24V2.virtual: 12 Schwachstellen im Fernwartungsserver (VDE-2026-141)

HOCH CERT@VDE, 10.11.

Was ist neu: Firmware unter 2.21.0 von myREX24V2 und myREX24V2.virtual hat 12 Schwachstellen (CVE-2026-60035 bis CVE-2026-60046). Die höchste Bewertung nach CVSS 4.0 ist 8,7. Das Cross-Site Scripting CVE-2026-60043 bewertet das Advisory nach CVSS 3.1 mit 9,3, im CVE-Eintrag steht dafür CVSS 4.0 6,4. Laut Advisory können die Lücken zum vollständigen Verlust von Vertraulichkeit, Integrität und Verfügbarkeit führen.

Bedeutung: myREX24 ist bei Maschinenbauern als eigener Fernwartungsserver verbreitet. Fällt er, gehen Vertraulichkeit, Integrität und Verfügbarkeit des gesamten Remote Access verloren.

Empfehlung: Auf 2.21.0 oder neuer aktualisieren. Die Admin-Oberfläche nur aus dem Verwaltungsnetz erreichbar machen und die Admin-Konten prüfen.

Quelle: https://certvde.com/en/advisories/VDE-2026-141/ ✓ geprüft

L-03 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 SIMATIC WinCC V7.5, V8.0 und V8.1, jeweils alle Versionen. Wer eine präparierte Datei öffnet, kann Code ausführen. Laut Siemens gibt es derzeit keinen Fix, er ist in Vorbereitung.

Bedeutung: Maschinenbauer tauschen WinCC-Projektdateien laufend mit Kunden und Unterlieferanten aus. Eine präparierte Datei auf diesem Weg kann die Engineering-Station übernehmen und von dort weitere Projekte erreichen.

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

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

L-04 Siemens Industrial Edge Management: Brotli-Lücke in Configurator-Apps, CVSS 9,8, teils ohne Fix (ICSA-26-316-03)

HOCH CISA / Siemens ProductCERT, 12.11.

Was ist neu: CISA hat am 12.11. das Siemens-Advisory zu CVE-2026-111497 (CVSS 3.1: 9,8) neu veröffentlicht, Siemens hatte es am 30.10. herausgegeben. Updates gibt es unter anderem für Cloud Connector Configurator (V1.24.3), Databus Configurator (V4.0.1) und Edge OPC UA Server Configurator (V2.3.10). Für den Common Configurator auf IEM und auf dem Edge-Gerät gibt es noch keinen Fix, Siemens rät, die Management-Apps zu deinstallieren bzw. CC on Edge zu stoppen.

Bedeutung: Industrial Edge verbindet Maschinen mit IT und Cloud. Nach unserer Einschätzung ist eine Lücke ohne Anmeldung in dieser Schicht ein direkter Weg zu Maschinendaten und Konfigurationen.

Empfehlung: Configurator-Apps auf die genannten Versionen bringen, Common Configurator nach Siemens-Vorgabe entfernen und IEM-Instanzen per Firewall oder WAF schützen (CC5, CC2).

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-316-03 ✓ geprüft

L-05 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 Komponentenhersteller bauen Firmware auf Alpine, OpenWrt, Buildroot oder Yocto. Unter dem CRA müssen sie solche Lücken in ihren Produkten erkennen und beheben, ohne SBOM ist die Frage nach der Betroffenheit kaum schnell zu beantworten.

Empfehlung: Firmware-SBOMs nach OpenSSH, musl und deaktiviertem PAM durchsuchen, betroffene Produkte mit OpenSSH 10.6p2 neu bauen und Kunden per Advisory informieren (CC5).

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

L-06 SonicWall SonicOS SSLVPN: aktiv ausgenutzte Lücke im CISA-KEV (CVE-2026-19868)

HOCH CISA, 06.11.

Was ist neu: CISA hat CVE-2026-19868 in SonicOS SSLVPN („Use of Single-factor Authentication“) wegen aktiver Ausnutzung in den KEV-Katalog aufgenommen. Betroffene Versionen nennt die Meldung nicht.

Bedeutung: Viele Mittelständler im Anlagenbau nutzen SonicWall als VPN-Gateway, auch für Servicetechniker beim Kunden. Ein übernommenes VPN-Konto ist ein direkter Initial Access ins Firmennetz und oft weiter in Testfelder und Fernwartungssysteme.

Empfehlung: Das SonicWall-Advisory prüfen und patchen. Phishing-resistente MFA für SSL-VPN erzwingen und die Anmeldungen der letzten Wochen auf fremde Quellen und ungewöhnliche Zeiten durchsehen.

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

L-07 Kühlanlagen-Angriffe: Frankreich macht IRGC-Einheit „Shahid Kaveh“ verantwortlich

MITTEL BleepingComputer, 09.11.

Was ist neu: Frankreich führt die Oktober-Angriffe auf Kühlsysteme in rund 700 angegriffenen Supermärkten auf die IRGC-nahe Einheit Shahid Kaveh zurück. Angreifer hatten Danfoss-Kühlsteuerungen kompromittiert und die Abtau-Einstellungen geändert, mindestens 15 Brände werden genannt. Frankreich will neue EU-Sanktionen vorschlagen. Die spätere Welle im November mit über 115 Geschäften in sechs europäischen Ländern ist nicht zugeordnet.

Bedeutung: Laut französischer Zuordnung hat ein staatlicher Threat Actor Steuerungen eines Komponentenherstellers über deren Erreichbarkeit angegriffen. Für Hersteller und Integratoren von Kälte- und Gebäudetechnik wird die Frage nach sicheren Werkseinstellungen und Fernzugängen damit auch zur Haftungsfrage.

Empfehlung: Ausgelieferte Steuerungen mit Internet- oder Fernzugang inventarisieren. Kunden auf Standardpasswörter und offene Ports hinweisen und Sollwertgrenzen mit Alarm vorsehen.

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

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Phishing-resistente MFA auf allen VPN-Zugängen und Logging der Anmeldungen mit Alarm bei ungewöhnlichen Quellen [CC3 ICS Network Visibility & Monitoring]	L-06	HOCH	sofort
M-02	Incident-Response-Ablauf für kompromittierte Fernwartung üben, inklusive Information der Kunden und CRA-Meldeweg [CC1 ICS Incident Response]	L-07	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Welche unserer Fernwartungsportale (mbCONNECT24, myREX24, eigene) laufen noch unter 2.21.6 bzw. 2.21.0, und wer ist dafür verantwortlich?

2. Können wir für jedes ausgelieferte Produkt per SBOM in einer Stunde sagen, ob OpenSSH mit musl ohne PAM oder ein betroffenes PHP drin ist?

3. Wie tauschen wir WinCC-Projektdateien mit Kunden und Unterlieferanten aus, und wird dabei auf Malware geprüft?

4. Ist auf allen VPN-Zugängen für Servicetechniker phishing-resistente MFA aktiv?

5. Wer schreibt bei uns Advisories an Kunden, und wie schnell könnten wir eine CRA-Meldung abgeben?

Maßnahmen dieser Woche

1. mbCONNECT24/mymbCONNECT24 auf 2.21.6 und myREX24V2 auf 2.21.0 oder neuer aktualisieren, danach die Zugriffslogs prüfen.

2. Firmware-SBOMs nach OpenSSH, musl und deaktiviertem PAM durchsuchen und für betroffene Produkte Builds mit OpenSSH 10.6p2 einplanen.

3. Bis zum WinCC-Fix eine Regel einführen: Graphics-Designer-Dateien nur aus geprüften Quellen und nur auf getrennten Engineering-Rechnern öffnen.

4. Bei Industrial Edge die Configurator-Apps aktualisieren und Common Configurator nach Siemens-Vorgabe einschränken.

5. SonicWall-SSLVPN patchen und die Anmeldungen der letzten Wochen auf fremde Quellen durchsehen.

6. Weidmüller IE-SR-Router auf Firmware 2.3.4 bringen und die Weboberfläche nur aus vertrauenswürdigen Netzen erreichbar lassen.

HINWEIS ZUR QUELLENLAGE

Advisories von CERT@VDE, Siemens und CISA haben wir direkt geöffnet. SSHole stützt sich auf die OpenSSH-Meldung auf oss-security (05.11., ohne CVE-Kennung) und SecurityWeek; eine in der Presse genannte CVE-Nummer haben wir nicht bestätigt und deshalb weggelassen. Die Zuordnung durch Frankreich stützt sich auf BleepingComputer, die Erklärung des französischen Ministeriums haben wir nicht gefunden. Laut BleepingComputer (26.10.) wird PHP2Shell allgemein schon ausgenutzt, für mbCONNECT24 meldet das Advisory aber keine Ausnutzung. Nicht aufgenommen: Welotec TK-Router (VDE-2026-119, schon am 03.11.), Welotec egOS (VDE-2026-138, CVSS 5,4), ads-tec (VDE-2026-131, nur DoS). Zu CRA und Maschinenverordnung haben wir nur Sekundärquellen gefunden: Die Ratifizierung von EN 40000-1-1/-1-2 war für 02.11. geplant (ibf-solutions, Stand 06.10.). Bestätigt haben wir sie nicht, eine Verschiebung der Cybersecurity-Pflichten der Maschinenverordnung ebenfalls nicht. Alle Quellenlinks wurden am 13.11.2026 automatisch aufgerufen und inhaltlich geprüft. Die vier zunächst aussortierten Meldungen (mbCONNECT24, SSHole, WinCC, Industrial Edge) haben wir am 13.11. an den Quellen nachgeprüft und aufgenommen.