OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Maschinen- und Anlagenbau

Ausgabe KW 48/2026 · Maschinen- und Anlagenbau in DACH

Zielgruppe	Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren
Berichtszeitraum	20.11.2026 bis 27.11.2026
Version	1.0
Datum	27.11.2026
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

In KW 48 kamen für Maschinen- und Anlagenbauer vor allem Advisories zu Komponenten, die sie selbst in Maschinen einbauen. Am schwersten wiegt die Lücke im TCP-Stack der Phoenix Contact FL MGUARD 2xxx/4xxx (VDE-2026-159, CVSS 9,8, ausnutzbar ohne Login). Diese Geräte stecken oft als Fernwartungs-Gateway im Schaltschrank. Siemens meldet fünf NGINX-Lücken in Industrial Edge (SSA-935812), für die es noch keinen Patch gibt. Dazu kommen CODESYS Visualization (VDE-2026-154): Hier kann eine manipulierte Runtime Code auf dem Engineering-PC ausführen, was Inbetriebnehmer und Systemintegratoren direkt trifft. Bei WAGO-Controllern mit wago_os_linux vor 4.10.0 (VDE-2026-096) kann ein angemeldeter Nutzer mit wenigen Rechten Root werden.

Die PHP-Lücke „PHP2Shell“ (CVE-2026-109618) zieht weiter durch die Lieferkette. Diese Woche hat Wiesemann & Theis Advisories für mehrere Geräte veröffentlicht (VDE-2026-135), vorher schon Phoenix Contact, Weidmüller und Festo. Eine aktive Ausnutzung von Komponenten aus der Industrie ist diese Woche nur für die Kühlstellen-Manager Danfoss AK-SM 800A belegt: CISA hat am 25.11. drei Lücken in den KEV-Katalog aufgenommen. Beim CRA hat CEN-CENELEC am 19.11. mit EN 40000-1-1 und EN 40000-1-2 die ersten Normen zu Begriffen und zum Risikomanagement über den Produktlebenszyklus veröffentlicht. Die Meldepflichten laufen schon seit September, damit wird das eigene PSIRT-Verfahren jetzt praktisch geprüft.

GESAMTBEWERTUNG

Die Lage ist erhöht: Mehrere kritische Lücken betreffen Komponenten, die Maschinenbauer selbst verbauen, für Industrial Edge und Danfoss AK-SM 8xxA fehlt der Patch noch. Zuerst sollten Fernwartungs-Gateways (mGuard) und Engineering-PCs (CODESYS) aktualisiert und die Kunden informiert werden.

Trends

• Open-Source-Bausteine wie PHP, NGINX und der Linux-Kernel sorgen für Advisories bei vielen Herstellern auf einmal (Phoenix Contact, Siemens, Wiesemann & Theis, Weidmüller, Festo), wer seine SBOM nicht kennt, kommt kaum hinterher.

• Fernwartungs- und Gateway-Geräte (mGuard, Edge-Geräte, Firewalls wie PAN-OS mit PAN-SA-2026-0015) sind weiter das bevorzugte Ziel, auch die Management-Oberflächen werden aktiv angegriffen.

• Angriffe richten sich zunehmend gegen den Engineering-Arbeitsplatz selbst, die CODESYS-Lücken zeigen den Weg von der Runtime zurück zum Laptop des Technikers.

• Ransomware beim Hersteller stoppt die Lieferkette: Osaki Electric hat am 17.11. Produktion und Auslieferung von Smart Metern an drei Standorten angehalten (https://www.osaki.co.jp/ja/notice/20261118.html).

• Beim CRA kommen die Normen jetzt Stück für Stück, wer erst auf die vollständige Normenreihe wartet, verliert Zeit für den Prozessaufbau.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Siemens Industrial Edge: fünf NGINX-Lücken („NGINX2Root“), noch kein Patch (SSA-935812)	HOCH	Siemens ProductCERT, 20.11.
L-02	PHP2Shell in der Lieferkette: Wiesemann & Theis meldet betroffene Geräte (VDE-2026-135)	HOCH	CERT@VDE / Wiesemann & Theis, 23.11.
L-03	CRA: CEN-CENELEC veröffentlicht EN 40000-1-1 und EN 40000-1-2	ORIENTIERUNG	CEN-CENELEC, 19.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 27.11.2026):

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	136005	DNP3: 31017, OMRON FINS: 24583, ProConOS: 15127, Siemens S7: 7537, OPC UA: 4801
Österreich	4553	HMI/VNC: 998, DNP3: 978, Niagara Fox: 435, Siemens S7: 367, OPC UA: 136

Meldungen im Detail

L-01 Siemens Industrial Edge: fünf NGINX-Lücken („NGINX2Root“), noch kein Patch (SSA-935812)

HOCH Siemens ProductCERT, 20.11.

Was ist neu: Siemens meldet fünf NGINX-Lücken (CVE-2026-113425, CVE-2026-121810, CVE-2026-123007, CVE-2026-123633, CVE-2026-123634) mit CVSS v3.1 8,1 bzw. v4.0 9,2. Betroffen sind alle Versionen von Industrial Edge Cloud Device, Device Kit (arm64/x86-64), Own Device und Virtual Device. Einen Fix gibt es noch nicht. Industrial Edge Hub und die Management-Varianten sind nicht betroffen.

Bedeutung: Wer Industrial Edge als Teil eines Retrofit- oder Datenerfassungspakets an Kunden liefert, hat jetzt verwundbare Geräte im Feld und keinen Patch, den er verteilen kann. Ausnutzbar sind die Lücken ohne Anmeldung über das Netz, allerdings mit hoher Komplexität. Möglich sind Denial of Service, Speicherkorruption oder Codeausführung.

Empfehlung: Edge-Geräte nur aus einer eigenen Zone erreichbar machen und HTTP/3/QUIC sowie HTTP/2 über WAF oder Reverse Proxy abschalten. Die Kunden mit einer kurzen Handlungsanweisung informieren und den Siemens-Fix fest einplanen (CC2 Defensible Architecture).

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-935812.html ✓ geprüft

L-02 PHP2Shell in der Lieferkette: Wiesemann & Theis meldet betroffene Geräte (VDE-2026-135)

HOCH CERT@VDE / Wiesemann & Theis, 23.11.

Was ist neu: Die PHP-Lücken CVE-2026-109618 und CVE-2026-109619 (CVSS 4.0 jeweils 9,2) betreffen FTP Data Station 3, Motherbox 4 sowie pure.box 3 und pure.box 5 von Wiesemann & Theis. Laut Advisory kann ein entfernter Angreifer beliebigen Code ausführen. Die Updates liegen auf wut.de, und bis zum Update rät der Hersteller, den Webserver im Web-Based Management abzuschalten.

Bedeutung: Hier steckt eine Open-Source-Komponente in fremden Geräten, und der Maschinenbauer erfährt davon nur, wenn seine Zulieferer Advisories veröffentlichen. Genau diesen Fall soll das eigene Schwachstellenmanagement für Komponenten von Dritten abdecken. In der Advisory heißt das Produkt einmal Motherbox 4 und einmal Motherbox 3, das sollte man beim Hersteller klären.

Empfehlung: In der SBOM bzw. Stückliste nach Geräten mit eingebettetem PHP suchen und alle Zulieferer-Advisories zu CVE-2026-109618 abgleichen. Betroffene Geräte aktualisieren oder ihren Webserver abschalten (CC5).

Quelle: https://certvde.com/de/advisories/VDE-2026-135/ ✓ geprüft

L-03 CRA: CEN-CENELEC veröffentlicht EN 40000-1-1 und EN 40000-1-2

ORIENTIERUNG CEN-CENELEC, 19.11.

Was ist neu: CEN und CENELEC haben im Rahmen des Normungsauftrags M/606 zum Cyber Resilience Act die ersten zwei Normen veröffentlicht. EN 40000-1-1 legt die Begriffe fest, EN 40000-1-2 regelt Grundsätze, Produkt-Risikomanagement und Aktivitäten über den Lebenszyklus. FprEN 40000-1-3 zum Schwachstellenmanagement soll bald folgen.

Bedeutung: Damit gibt es erstmals einen europäischen Normrahmen, an dem Hersteller ihr Security-Risikomanagement über den Produktlebenszyklus ausrichten können. Die Normen gibt es über die nationalen Normenkataloge. Die eigentlichen Anforderungen an Schwachstellenmanagement und Produktkategorien fehlen aber noch.

Empfehlung: EN 40000-1-2 über DIN, ASI bzw. SNV beschaffen und gegen das bestehende Vorgehen nach IEC 62443-4-1 abgleichen. Die Ergebnisse in die technische Dokumentation übernehmen, damit sie später für den CRA und die Maschinenverordnung genutzt werden können (CC5).

Quelle: https://www.cencenelec.eu/news-events/news/2026/en-in-the-spotlight/2026-11-19-cra-standards-en-40000-1-1-and-en-40000-1-2/ ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Industrial-Edge-Geräte in eine eigene Zone legen, HTTP/2 und HTTP/3 per Reverse Proxy abschalten und den Siemens-Fix einplanen [CC2 Defensible Architecture]	L-01	HOCH	sofort
M-02	Advisory-Abgleich gegen SBOM automatisieren (CERT@VDE, Siemens ProductCERT, CISA) und eine Kundenwarnung als Vorlage vorbereiten [CC5 Risk-Based Vulnerability Management]	L-02	MITTEL	0 bis 3 Monate

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-03	Produkt-Risikomanagement mit EN 40000-1-2 abgleichen und die Ergebnisse in die technische Dokumentation übernehmen [CC5 Risk-Based Vulnerability Management]	L-03	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Wissen wir für jede ausgelieferte Maschine, welche mGuard-, WAGO- und Industrial-Edge-Firmware verbaut ist, und wie schnell erreichen wir die Kunden?

2. Wer bei uns liest die Advisories von CERT@VDE und Siemens ProductCERT und gleicht sie mit unseren Stücklisten ab, und wie lange dauert das heute?

3. Sind unsere Service-Laptops von den Kundenanlagen getrennt, oder kann eine kompromittierte Steuerung über sie ins eigene Netz gelangen?

4. Wäre unser PSIRT in der Lage, eine aktiv ausgenutzte Lücke in unserem Produkt innerhalb der CRA-Meldefrist zu bewerten und zu melden?

5. Welche Zulieferer würden uns bei einem Ransomware-Ausfall wie bei Osaki die Produktion stoppen, und haben wir dafür einen Plan B?

Maßnahmen dieser Woche

1. Installed Base nach FL MGUARD mit Firmware unter 10.7.1 durchsuchen und den Kunden das Update auf 10.7.1 anbieten.

2. Kunden mit Siemens Industrial Edge eine kurze Handlungsanweisung schicken: Netzzugang einschränken, HTTP/2 und HTTP/3 per Reverse Proxy abschalten.

3. Alle Engineering- und Service-Laptops auf CODESYS Visualization 4.11.0.0 aktualisieren.

4. WAGO-Steuerungen im Feld auf wago_os_linux 4.10.0 bringen und überflüssige WBM-Konten löschen.

5. SBOM und Stücklisten auf PHP-basierte Webserver in Zukaufteilen prüfen (CVE-2026-109618) und offene Herstelleraussagen nachfordern.

6. Fernwartungszugänge zu Danfoss-Kühlstellen-Managern prüfen und ausschließlich über VPN zulassen.

HINWEIS ZUR QUELLENLAGE

Alle Meldungen beruhen auf Primärquellen (CERT@VDE, Siemens ProductCERT, CISA, CEN-CENELEC), die ich geöffnet habe. Nicht aufgenommen habe ich drei Dinge: die aktive Ausnutzung von PHP2Shell (nur über BleepingComputer, Bestätigung durch CISA nicht selbst geprüft), die Änderung von M/606 vom 10.11. und den Stand der harmonisierten Normen zur Maschinenverordnung (nur Blogs, nicht im Amtsblatt geprüft). Ein Suchtreffer zu einem Cyberangriff auf KraussMaffei ließ sich keinem Jahr sicher zuordnen und ist deshalb nicht im Bericht. In der W&T-Advisory heißt dasselbe Produkt einmal Motherbox 4 und einmal Motherbox 3. Alle Quellenlinks wurden am 27.11.2026 automatisch aufgerufen und inhaltlich geprüft. 4 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.