

WOCHENBERICHT

OT-/Cyber-Lagebild Maschinen- und Anlagenbau

Ausgabe KW 44/2026 · Maschinen- und Anlagenbau in DACH

Zielgruppe	Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren
Berichtszeitraum	23.10.2026–30.10.2026
Version	1.0
Datum	30.10.2026
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 Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 44 geht es vor allem um zwei Dinge. Siemens hat acht Schwachstellen im Webserver von S7-1500, ET 200SP, ET 200pro, Drive Controllern und Software Controllern veröffentlicht (ICSA-26-295-14, CVSS bis 9,6). Betroffen sind alle Versionen, und einen Patch gibt es noch nicht. Diese Steuerungen sind in unzähligen Maschinen verbaut, die beim Kunden laufen. Das zweite Thema sind die PHP-Lücken „PHP2Shell“ (CVE-2026-109618/-109619). Die CISA führt sie seit dem 26.10. als aktiv ausgenutzt. Sie stecken in OT-Produkten von Schneider Electric, B&R (APROL), Belden (NetModule, ohne Patch), HMS (Netbiter, Talk2M), Wibu-Systems (CodeMeter License Central) und Siemens (RUGGEDCOM APE1808).

Für Komponentenhersteller ist PHP2Shell der erste große Prüffall seit dem Start der CRA-Meldepflicht am 11.09.2026. Wer PHP in eigenen Produkten mit digitalen Elementen ausliefert, muss jetzt prüfen, ob eine Meldung an ENISA fällig ist. Beim Fernzugang wird außerdem ein Zero-Day in Cisco ASA/FTD ausgenutzt (CVE-2026-76418), mit dem sich SSL-VPN-Geräte zum Absturz bringen lassen. Für Integratoren kommt die Anmeldeumgehung in Mitsubishi ICONICS GENESIS64 dazu. Für MC Works64, GENESIS32 und BizViz wird es keinen Fix geben.

GESAMTBEWERTUNG

Die Lage ist hoch: Die PHP2Shell-Lücken werden aktiv ausgenutzt, in OT-Produkten und Fernwartungs-Komponenten fehlen noch Patches, und im Siemens-Webserver gibt es bisher keinen Fix. Vorrang haben drei Punkte: die eigenen Produkte auf PHP prüfen und eine CRA-Meldung bewerten, den Webserver an ausgelieferten S7-1500/ET-200SP-Steuerungen abschalten oder einschränken und die Fernwartungswege patchen.

Trends

- Lücken in Basiskomponenten wie PHP schlagen breit auf OT-Produkte durch, und Hersteller brauchen Tage bis Monate für eine Bewertung (Rockwell und Hitachi Energy prüfen noch, Belden hat keinen Patch).
- Edge-Geräte für den Fernzugang (Cisco ASA, WatchGuard, NetModule, Netbiter) stehen weiter im Fokus von Angreifern, gerade die Systeme, über die Maschinenbauer ihre Kundenanlagen warten.
- Hersteller wie Siemens und Mitsubishi veröffentlichen kritische Steuerungs- und HMI-Lücken ohne Patch oder mit „Fix nur durch Umstieg“, die Abwehr hängt damit an Architektur und Konfiguration beim Betreiber.
- Immer mehr Lücken werden mit KI-Werkzeugen gefunden (WatchGuard: 13 von 18 aus eigener KI-Forschung), dadurch kommen mehr Patches in kürzerer Folge.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	PHP2Shell in OT-Produkten: aktiv ausgenutzt, CISA-KEV seit 26.10., Patches teils offen	KRITISCH	CISA KEV / SecurityWeek, 26.10.
L-02	Siemens S7-1500, ET 200SP und Drive Controller: acht Webserver-Lücken, kein Patch (ICSA-26-295-14)	HOCH	CISA / Siemens ProductCERT, 22.10.

ID	Meldung	Relevanz	Quelle
L-03	Cisco ASA/FTD: Zero-Day bringt SSL-VPN-Geräte zum Absturz (CVE-2026-76418)	HOCH	Cisco PSIRT, 28.10.
L-04	Mitsubishi ICONICS GENESIS64/GENESIS: Anmeldeumgehung, für MC Works64, GENESIS32 und BizViz kein Fix (ICSA-26-300-02)	HOCH	CISA / Mitsubishi Electric PSIRT, 27.10.
L-05	CRA und Maschinenverordnung: Normen kommen später, die Pflichten bleiben	ORIENTIERUNG	cyberresilienceact.eu / Swissmem, 11.09.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 30.10.2026):

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	148182	DNP3: 34267, OMRON FINS: 26328, ProConOS: 17131, Siemens S7: 7931, OPC UA: 5265
Österreich	4928	HMI/VNC: 1088, DNP3: 1006, Niagara Fox: 482, Siemens S7: 386, OPC UA: 161

Meldungen im Detail

L-01 PHP2Shell in OT-Produkten: aktiv ausgenutzt, CISA-KEV seit 26.10., Patches teils offen

KRITISCH CISA KEV / SecurityWeek, 26.10.

Was ist neu: Die CISA hat CVE-2026-109618 und CVE-2026-109619 am 26.10. in den KEV-Katalog aufgenommen. Laut SecurityWeek (26.10.) sind Produkte von Schneider Electric (EcoStruxure Security Expert, ProLeiT LINEoptimize, EcoStruxure Control Engineering), B&R APROL bis R 4.4-65, Belden NetModule NRSW (alle Versionen, noch kein Patch), HMS Netbiter, Wibu CodeMeter License Central und Siemens RUGGEDCOM APE1808 betroffen. Rockwell prüft noch, Moxa meldet keine Betroffenheit.

Bedeutung: Viele Maschinen und Fernwartungsboxen haben eine Weboberfläche auf PHP-Basis, auch bei kleineren Herstellern. Seit dem 11.09.2026 müssen Hersteller aktiv ausgenutzte Schwachstellen in eigenen Produkten innerhalb von 24 Stunden über die ENISA-Plattform melden. Damit wird PHP2Shell für viele Komponentenhersteller zum ersten echten CRA-Meldefall.

Empfehlung: Per SBOM oder Firmware-Analyse feststellen, ob eigene Produkte eine verwundbare PHP-Version enthalten. Behoben ist das in PHP 8.5.12, 8.4.27, 8.3.36 und 8.2.35. Bis zum Patch rät PHP zu session.upload_progress.enabled=0. Fällt die Prüfung positiv aus, die CRA-Meldung vorbereiten und die Kunden aktiv informieren (CC5).

Quelle: <https://www.securityweek.com/industrial-vendors-check-products-for-php2shell-vulnerabilities/> ✓ geprüft

L-02 Siemens S7-1500, ET 200SP und Drive Controller: acht Webserver-Lücken, kein Patch (ICSA-26-295-14)

HOCH CISA / Siemens ProductCERT, 22.10.

Was ist neu: CVE-2026-63350 bis -63357 betreffen alle Versionen von S7-1500-CPU, ET 200SP-CPU und Open Controllern, ET 200pro, Drive Controllern 1504D/1507D TF, Software Controllern und S7-PLCSIM Advanced (CVSS v3 bis 9,6). Wer eine präparierte Trace-Datei importiert, kann im Webserver Skriptcode ausführen lassen, der dann mit dessen Rechten auf der Steuerung arbeitet. Siemens bereitet Fixes vor, verfügbar ist noch keiner.

Bedeutung: Maschinenbauer nutzen den Webserver und Trace-Dateien oft für Diagnose und Service. Gerade der Austausch von Trace-Dateien zwischen Service, Kunde und Integrator ist hier der Angriffsweg. Als Hersteller der Maschine sind Sie für Ihre Kunden der erste Ansprechpartner.

Empfehlung: Den Webserver in Standardprojekten abschalten, wo er nicht gebraucht wird, sonst 80/tcp und 443/tcp auf vertrauenswürdige IPs begrenzen. Trace-Dateien nur aus bekannter Quelle importieren. Den Kunden einen kurzen Service-Hinweis schicken und den Patch-Termin von Siemens beobachten (CC2).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-14> ✓ geprüft

L-03 Cisco ASA/FTD: Zero-Day bringt SSL-VPN-Geräte zum Absturz (CVE-2026-76418)

HOCH Cisco PSIRT, 28.10.

Was ist neu: Cisco bestätigt, dass die Lücke ausgenutzt wird (CVSS 8,6). Ohne Anmeldung lässt sich ein ASA/FTD mit SSL-Remote-Access-VPN neu starten, wenn in einer Tunnel-Gruppe eine sekundäre Authentifizierung eingerichtet ist. Behoben ist das u. a. in ASA 9.20.4.50, 9.22.3.200 und FTD 7.4.9, 7.6.7. Einen vollständigen Workaround gibt es nicht.

Bedeutung: Viele Maschinenbauer erreichen Kundenanlagen und eigene Service-Netze über ASA-VPNs. Fällt das Gateway aus, ist die Fernwartung weg, im Störfall genau dann, wenn sie gebraucht wird.

Empfehlung: Das Update einspielen. Bis dahin die Mitigation von Cisco anwenden (no tunnel-group-list enable, wenn DefaultWEBVPNGroup keine sekundäre Authentifizierung nutzt). Für Notfälle einen zweiten Fernzugang festlegen, der unabhängig davon funktioniert (CC4).

Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafld-tunnel-dos-s6mgkb75> ✓ geprüft

L-04 Mitsubishi ICONICS GENESIS64/GENESIS: Anmeldeumgehung, für MC Works64, GENESIS32 und BizViz kein Fix (ICSA-26-300-02)

HOCH CISA / Mitsubishi Electric PSIRT, 27.10.

Was ist neu: Die Passwort-Wiederherstellung nutzt eine feste Challenge-Response, die für alle Benutzer gleich ist. Damit lässt sich das System aus der Ferne entsperren (CVE-2026-16436, CVSS v4 9,2). Fixes gibt es in GENESIS 11.04 und GENESIS64/Hyper Historian/AnalytiX/MobileHMI/IoTWorX 10.98. Für MC Works64, GENESIS32 und BizViz ist kein Fix geplant.

Bedeutung: Integratoren, die solche Systeme ausgeliefert haben, sollten ihre Kunden aktiv informieren. Für die Altprodukte bleibt nur der Umstieg, das wird zum Wartungs- und Vertriebsthema.

Empfehlung: Ausgelieferte Installationen aus der Projektliste herausuchen. Den Workaround der CISA umsetzen: die Challenge-Datei durch eine leere Datei ersetzen und die Schreibrechte darauf beschränken. Remote Access auf diese Systeme nur für Administratoren erlauben (CC5).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-02> ✓ geprüft

L-05 CRA und Maschinenverordnung: Normen kommen später, die Pflichten bleiben

ORIENTIERUNG cyberresilienceact.eu / Swissmem, 11.09.

Was ist neu: Laut einem Entwurf der Kommission sollen die Fristen für die CRA-Normen um zwei Monate verschoben werden: für die Schwachstellenbehandlung (prEN 40000-1-3) auf den 31.10.2026, für vertikale OT-Normen (prEN 50770) auf den 31.12.2026. Der Beschluss ist laut dieser Quelle noch nicht im Amtsblatt erschienen, und es ist noch keine CRA-Norm gelistet. Swissmem erwartet die erste Liste harmonisierter Normen zur Maschinenverordnung bis Ende 2026, gelten wird die Verordnung ab dem 20.01.2027.

Bedeutung: Ohne gelistete Normen gibt es keine Konformitätsvermutung, die Pflichten gelten trotzdem. Die Meldepflicht nach CRA läuft seit dem 11.09.2026, und die Maschinenverordnung verlangt ab dem 20.01.2027 Schutz gegen Korruption.

Empfehlung: Entwicklung und Dokumentation an prEN 40000-1-3 und IEC 62443-4-1/-4-2 ausrichten. PSIRT, Meldeweg an ENISA und SBOM-Pflege jetzt fest besetzen, damit ein Fall wie PHP2Shell nicht improvisiert werden muss (CC1).

Quelle: <https://www.cyberresilienceact.eu/de/news/cra-standardisation-deadlines-pushed-back-two-months.html> ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	PHP-Prüfung aller eigenen Produkte per SBOM, Entscheidung über CRA-Meldung und Kundeninformation [CC5 Risk-Based Vulnerability Management]	L-01	HOCH	sofort
M-02	Webserver an S7-1500/ET 200SP in Standardprojekten abschalten, sonst per Firewall auf Service-IPs begrenzen [CC2 Defensible Architecture]	L-02	HOCH	sofort

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-03	Fernwartungs-Gateways (ASA, WatchGuard, NetModule, Netbiter) inventarisieren, patchen und über einen Jump Host mit MFA bündeln [CC4 Secure Remote Access]	L-03	HOCH	0 bis 3 Monate
M-04	Für Bestandsanlagen mit ICONICS/GENESIS64 Update- und Migrationspaket anbieten, Altprodukte im Asset-Inventar kennzeichnen [CC5 Risk-Based Vulnerability Management]	L-04	MITTEL	0 bis 3 Monate
M-05	Entwicklungsprozess an prEN 40000-1-3 und IEC 62443-4-1 ausrichten, Nachweise für Anhang III Nr. 1.1.9 Maschinenverordnung bis Januar 2027 erstellen [CC1 ICS Incident Response]	L-05	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Enthält eines unserer Produkte PHP, und wer entscheidet bis wann, ob wir nach CRA an ENISA melden?
2. In welchen ausgelieferten Maschinen ist der Webserver der S7-1500/ET 200SP aktiv, und wie informieren wir diese Kunden?
3. Über welche Gateways (ASA, WatchGuard, NetModule, Netbiter/Talk2M) läuft unsere Fernwartung, und sind alle auf dem aktuellen Stand?
4. Haben wir für jedes Produkt eine aktuelle SBOM, mit der wir eine Lücke wie PHP2Shell in Stunden statt Wochen zuordnen können?
5. Welche Anforderungen aus Anhang III Nr. 1.1.9 der Maschinenverordnung (Schutz gegen Korruption) sind für Maschinen ab dem 20.01.2027 noch offen?

Maßnahmen dieser Woche

1. Eigene Produkte per SBOM auf PHP prüfen und das Ergebnis mit Datum dokumentieren. Bei Betroffenheit die CRA-Meldung über die ENISA-Plattform vorbereiten.
2. In Standard-TIA-Projekten den Webserver der S7-1500/ET 200SP standardmäßig deaktivieren und einen Service-Hinweis an Bestandskunden schicken.
3. Cisco ASA/FTD für das Service-VPN auf die Fix-Version heben. Bis dahin prüfen, ob in DefaultWEBVPNGroup eine sekundäre Authentifizierung aktiv ist.
4. WatchGuard Firebox auf Fireware 2026.4, 12.12.4 oder 12.5.22 updaten und die Advisories von Belden (NetModule) und HMS (Netbiter) für eingesetzte Fernwartungsrouter abgleichen.
5. Ausgelieferte ICONICS/GENESIS64-Installationen aus der Projektliste herausuchen, Updates anbieten und für MC Works64/GENESIS32 ein Migrationsangebot vorbereiten.

HINWEIS ZUR QUELLENLAGE

Siemens, Cisco, Mitsubishi und die KEV-Aufnahme sind über die Seiten von CISA und Hersteller belegt. Die Liste der PHP2Shell-Hersteller stammt aus SecurityWeek (26.10.), Rockwells eigenes Advisory habe ich nicht gefunden. Bei WatchGuard nennen die Quellen sieben oder acht kritische Lücken, und die CERT-Bund-Kennung WID-SEC-2026-4209 ließ sich nicht verifizieren. Die CRA-Normungsfristen beruhen auf einem unabhängigen Leitfaden und einem noch nicht veröffentlichten Kommissionsentwurf. Nicht aufgenommen, weil unbestätigt: die Leak-Site-Einträge zu Hauhinco (Payload, 28.10.) und Phoenix S&S (Emperador), die Daten-Behauptungen von N0n zu Ingelectus, die Forescout-Zahlen zu offenen Kühlsteuerungen (keine Primärquelle gefunden) und der Bloomberg-Bericht zu Hacktivisten (nicht abrufbar). Für Phoenix Contact, WAGO und Beckhoff habe ich bei CERT@VDE keine Advisories aus dem Zeitraum gefunden. Alle Quellenlinks wurden am 30.10.2026 automatisch aufgerufen und inhaltlich geprüft. 1 Meldung(en) ohne überprüfbare Originalquelle wurden nicht aufgenommen.