

WOCHENBERICHT

OT-/Cyber-Lagebild Maschinen- und Anlagenbau

Ausgabe KW 41/2026 · Maschinen- und Anlagenbau in DACH

Zielgruppe	Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren
Berichtszeitraum	02.10.2026-09.10.2026
Version	1.0
Datum	09.10.2026
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 41 wurden vor allem die Zugänge angegriffen, über die Maschinenbauer und Systemintegratoren ihre Fernwartung betreiben. Beim Citrix NetScaler Gateway mit SAML-Konfiguration greifen Angreifer die Lücke CVE-2026-88779 gezielt an (laut Citrix Denial of Service). Sie trifft auch Geräte, die schon gegen CVE-2026-88771 bis -88778 gepatcht waren. Der Patch kam am 03.10. (PST). Bei FortiMail wird ein Zero-Day mit CVSS 9,8 ausgenutzt, Fixes nennt Fortinet seit 05.10. Beim Cisco Catalyst SD-WAN Manager umgehen Angreifer die Anmeldung (Zero-Day, CVSS 9,8). FBI und US Secret Service warnen außerdem vor der Kampagne „FortiBleed“: Mit gestohlenen Zugangsdaten werden FortiGate-Firewalls und SSL-VPNs übernommen, den Zugang verkaufen Initial Access Broker an Ransomware-Gruppen weiter. Wer Remote Access zu Kundenanlagen über solche Edge Devices anbietet, muss diese Woche patchen, Zugangsdaten rotieren und nach einer Kompromittierung suchen. Ein Patch allein reicht nicht.

Auf der Produktseite kamen mehrere Advisories zu Komponenten, die direkt in Maschinen verbaut werden. Betroffen sind Red Lion N-Tron 700 (Industrial-Ethernet-Switches), Moxa MGate (Modbus-Gateways) und CODESYS-Runtimes bei KEB COMBIVIS (VDE-2026-105) und WAGO-SPS (VDE-2025-081). Der aas-edge-client von Murrelektronik für die Verwaltungsschale hat eine Lücke mit CVSS 9,8 und bekommt keinen Patch. Im SMTP-Client des eingebetteten TCP/IP-Stacks lwIP steckt ein Buffer Overflow. Für Hersteller ist das ein Praxistest für den Cyber Resilience Act: Seit dem 11.09.2026 gelten die Meldepflichten für aktiv ausgenutzte Schwachstellen. Ohne SBOM und Asset-Inventar lässt sich nicht innerhalb von 24 Stunden sagen, ob das eigene Produkt betroffen ist. Mit KI-Unterstützung schaffen das auch kleine Teams.

GESAMTBEWERTUNG

Die Lage ist hoch. Mehrere ausgenutzte Zero-Days und eine Kampagne mit gestohlenen Zugangsdaten treffen Edge Devices für Remote Access und Mail-Gateways. Dazu kommen kritische Lücken in verbreiteten Steuerungs-, Switch- und Gateway-Komponenten. Vorrang haben die Fernwartungszugänge (NetScaler, FortiMail, FortiGate, SD-WAN; CC4). Danach folgt die Zuordnung der Advisories zur eigenen Produkt-SBOM (CC5), die Steuerungs-Patches werden gezielt im Wartungsfenster eingespielt.

Trends

- Edge Devices für Remote Access (NetScaler, FortiMail, FortiGate, Cisco SD-WAN CVE-2026-76504, SonicWall SMA1000) bleiben das wichtigste Einfallstor. Frisch gepatchte Geräte sind nach Tagen wieder verwundbar, und Zugangsdaten werden missbraucht. Deshalb müssen neben dem Patch auch Zugangsdaten und Kompromittierung geprüft werden, und die Fernwartung muss so gebaut sein, dass ein kompromittiertes Gateway nicht automatisch Zugriff auf Kundenanlagen bedeutet.
- Advisories betreffen zunehmend Bibliotheken und Runtimes, die bei vielen OEMs verbaut sind (CODESYS bei KEB und WAGO, lwIP-SMTP-Client CVE-2026-15340). Ohne SBOM lassen sie sich den eigenen Produkten kaum zuordnen.
- Mehrere Advisories betreffen eine fehlende Integritätsprüfung der Firmware (Moxa CVE-2026-86326, Red Lion, Hitachi Energy RTU500 CVE-2026-8065). Das ist ein Kernthema der CRA-Anforderungen.

- Für End-of-Life-Software und Demonstratoren kündigen Hersteller keine Fixes mehr an (Murrelektronik AAS, RTU500 Firmware 11.x) und raten zum Entfernen oder Upgrade. Referenzcode wird zum Produktrisiko, wenn er ohne Security-Review in Industrie-4.0-Projekte gelangt.
- Seit dem 11.09.2026 gelten die CRA-Meldepflichten über die ENISA-Plattform CRA-SRP mit Frühwarnung binnen 24 Stunden. Advisories wie zu lwIP oder CODESYS werden damit zum Prüffall für die Meldefähigkeit der Hersteller.
- Die Maschinenverordnung gilt ab 20.01.2027 und verlangt mit Anhang III 1.1.9 Schutz gegen Korruption. Harmonisierte Normen dafür sind noch nicht im Amtsblatt, und ob die Cybersecurity-Norm prEN 50742 bis dahin harmonisiert ist, bleibt offen.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Citrix NetScaler: SAML-Zero-Day CVE-2026-88779 (DoS) trifft auch bereits gepatchte Geräte	KRITISCH	Citrix Security Bulletin CTX697174 (https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html) / BleepingComputer 04.10. / CISA KEV, 03.10.
L-02	FortiMail: Zero-Day CVE-2026-104286 (CVSS 9,8) wird ausgenutzt, Fixes seit 05.10. verfügbar	KRITISCH	Fortinet PSIRT FG-IR-26-175 / heise / BleepingComputer (https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/) / CISA KEV, 01.10.
L-03	Cisco Catalyst SD-WAN Manager: Zero-Day mit Auth-Bypass (CVE-2026-76504, CVSS 9,8)	HOCH	Cisco Security Advisory / CISA KEV, 30.09.
L-04	FortiBleed: FBI und Secret Service warnen vor Übernahme von FortiGate-Firewalls über gestohlene Zugangsdaten	HOCH	The Hacker News (Warnung von FBI/USSS), 07.10.
L-05	Red Lion N-Tron 700: sieben Lücken in Industrial-Ethernet-Switches (ICSA-26-281-01)	HOCH	CISA ICS Advisory, 08.10.
L-06	Moxa MGate: Stack Overflow schon mit Leserechten (CVE-2026-86325, CVSS4 9,4, MP5A-269540)	HOCH	Moxa MP5A-269540 (über SecurityOnline, OpenCVE), 02.10.
L-07	CODESYS-Lücken bei weiteren OEMs: KEB COMBIVIS Control Runtime (VDE-2026-105) und WAGO-SPS (VDE-2025-081)	HOCH	CERT@VDE (VDE-2026-105, VDE-2025-081: https://cert.vde.com/en/advisories/VDE-2025-081/), 08.10.
L-08	Murrelektronik aas-edge-client (Verwaltungsschale): CVSS 9,8 ohne Patch, Hersteller rät zum Entfernen (VDE-2026-108)	HOCH	CERT@VDE (VDE-2026-108), 06.10.
L-09	lwIP-SMTP-Client: kritischer Buffer Overflow im eingebetteten TCP/IP-Stack (ICSA-26-279-02)	MITTEL	CISA ICS Advisory, 06.10.

ID	Meldung	Relevanz	Quelle
L-10	Cyber Resilience Act: Meldepflicht für ausgenutzte Schwachstellen gilt seit 11.09.2026	ORIENTIER UNG	BSI, 11.09.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 09.10.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt.

Region	Gesamt	Top-Protokolle
Deutschland	138446	DNP3: 33442, OMRON FINS: 23821, ProConOS: 16426
Österreich	4530	HMI/VNC: 1061, DNP3: 954, IEC-104: 450

Meldungen im Detail

L-01 Citrix NetScaler: SAML-Zero-Day CVE-2026-88779 (DoS) trifft auch bereits gepatchte Geräte

KRITISCH Citrix Security Bulletin CTX697174

(<https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html>) /

BleepingComputer 04.10. / CISA KEV, 03.10.

Was ist neu: Laut Citrix-Bulletin CTX697174 (03.10., PST) ist CVE-2026-88779 ein Memory Overflow (CWE-119), der zu Denial of Service führt (CVSS v4 8,7). Betroffen sind nur NetScaler ADC/Gateway, die als SAML-SP oder SAML-IdP konfiguriert sind. Gefixt ist die Lücke in 14.1-73.41, 13.1-64.28, 14.1-73.41 FIPS und 13.1-37.282 FIPS/NDcPP. Das Bulletin selbst nennt keine Ausnutzung. Laut BleepingComputer (04.10.) hat Citrix aber gezielte Angriffe auf ungepatchte Geräte beobachtet, die zu Denial of Service führen können. Erste Berichte über Neustarts kamen am 02.10., auch von Geräten mit Build 14.1-73.37. Citrix fordert alle, die nach den Fixes für CVE-2026-88771 bis -88778 aktualisiert haben, zu einem erneuten Update auf. Die CISA hat die Lücke am 04.10. in den KEV-Katalog aufgenommen, die Frist für US-Bundesbehörden endete am 07.10.

Bedeutung: Viele Maschinenbauer und Integratoren betreiben NetScaler mit SSO/SAML als zentralen Remote Access für Service-Techniker und Kundenanlagen. Wird das Gateway kompromittiert, können Angreifer den Fernwartungskanal per Lateral Movement in die OT-Netze vieler Kunden gleichzeitig nutzen. Daraus entsteht ein Haftungs- und Lieferkettenrisiko.

Empfehlung: Sofort auf die gefixten Builds aktualisieren. Danach nach Webshells, neuen Konten und verdächtigen Sessions suchen, denn Patchen allein reicht nicht (CC1). Wer nicht sofort patchen kann, nimmt den SAML-Zugang vom Netz. Fernwartungs-Sessions nur mit MFA und Freigabe durch den Kunden aufbauen (CC4).

Quelle: <https://www.bleepingcomputer.com/news/security/citrix-patches-netscaler-saml-zero-day-exploited-in-attacks/> ✓ geprüft

L-02 FortiMail: Zero-Day CVE-2026-104286 (CVSS 9,8) wird ausgenutzt, Fixes seit 05.10. verfügbar

KRITISCH Fortinet PSIRT FG-IR-26-175 / heise / BleepingComputer (<https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/>) / CISA KEV, 01.10.

Was ist neu: Über eine Path-Traversal-Lücke können Angreifer ohne Anmeldung Dateien auf das Gerät schreiben und Code ausführen. Betroffen sind FortiMail 7.2 bis 7.2.9, 7.4 bis 7.4.8, 7.6 bis 7.6.6 und 8.0.0 bis 8.0.1. Die CISA führt die Lücke seit dem 01.10. im KEV-Katalog. Die Fixes 8.0.2, 7.6.7 und 7.4.9 waren zunächst nur angekündigt. Am 05.10. hat Fortinet sie im Advisory FG-IR-26-175 als Lösung ergänzt, für 7.2 gibt es keinen Fix (Migration auf 7.4 oder neuer).

Bedeutung: Mail-Gateways sind ein häufiger Einstieg für Ransomware bei mittelständischen Maschinenbauern. Von dort führt Lateral Movement zu Konstruktionsdaten, Build-Servern und zur Firmware-Signierung.

Empfehlung: Sofort auf 8.0.2, 7.6.7 bzw. 7.4.9 aktualisieren und bis dahin die Workarounds umsetzen. Das Mail-Gateway vom internen Netz und von Entwicklungsumgebungen trennen (CC2) und auf IOCs prüfen (CC1).

Quelle: <https://fortiguard.fortinet.com/psirt/FG-IR-26-175> ✓ geprüft

L-03 Cisco Catalyst SD-WAN Manager: Zero-Day mit Auth-Bypass (CVE-2026-76504, CVSS 9,8)

HOCH Cisco Security Advisory / CISA KEV, 30.09.

Was ist neu: Mit einer speziell kodierte URL am Endpunkt /j_security_check (als /%6a_security_check) bekommt ein Angreifer ohne Anmeldung Admin-Rechte auf der API. Die Lücke wird seit September ausgenutzt, die CISA hat sie am 30.09. in den KEV-Katalog aufgenommen. Einen Workaround gibt es nicht. Gefixt ist sie in 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 und 26.2.1.

Bedeutung: Wer Werke, Montagestandorte oder Inbetriebnahme-Netze über SD-WAN verbindet, riskiert, dass Angreifer die Netzsteuerung übernehmen und die Segmentierungsregeln aushebeln.

Empfehlung: Sofort patchen. Danach serviceproxy-access.log und vmanage-server.log nach '/%6a_security_check' durchsuchen (CC1). Außerdem prüfen, ob die OT-Segmente auch ohne SD-WAN-Policy getrennt bleiben (CC2).

Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU> ✓ geprüft

L-04 FortiBleed: FBI und Secret Service warnen vor Übernahme von FortiGate-Firewalls über gestohlene Zugangsdaten

HOCH The Hacker News (Warnung von FBI/USSS), 07.10.

Was ist neu: Laut The Hacker News warnen FBI und US Secret Service vor einer laufenden Kampagne. Sie nutzt Credential Stuffing und Password Spraying, mit dem Tool „FortigateSniffer“ greifen die Angreifer weitere Zugangsdaten ab. Genannt werden über 86.644 kompromittierte Geräte in 194 Ländern (Stand 19.06.2026). Der Zugang geht an Ransomware wie INC und Lynx.

Bedeutung: Hinter der Kampagne steckt keine CVE, ein Patch allein schützt also nicht. Gefährdet sind vor allem FortiGate-VPNs mit Passwort-Anmeldung, wie sie im Mittelstand und bei Service-Zugängen zu Maschinen üblich sind. Die Angreifer legen eigene Admin-Konten an und sperren die echten Admins aus.

Empfehlung: Alle VPN- und Admin-Zugangsdaten zurücksetzen und für jeden Remote Access phishing-resistente MFA erzwingen. Die Admin-Oberfläche nicht aus dem Internet erreichbar machen und nach unbekannten lokalen Konten und API-Konten suchen.

Quelle: <https://thehackernews.com/2026/10/fbi-warns-fortibleed-remains-active.html> ✓ geprüft

L-05 Red Lion N-Tron 700: sieben Lücken in Industrial-Ethernet-Switches (ICSA-26-281-01)

HOCH CISA ICS Advisory, 08.10.

Was ist neu: Betroffen sind Firmware $\leq 3.11.0$ und Bootloader $\leq 2.0.6.1$. Zu den Lücken gehören fest einprogrammierte Zugangsdaten, fehlende Authentifizierung und Firmware ohne Integritätsprüfung (CVSS4 bis 9,3). Angreifer können damit Admin-Zugriff erlangen, die Konfiguration ändern und per URL dauernde Reboots auslösen. Eine Ausnutzung ist laut CISA nicht bekannt.

Bedeutung: N-Tron-Switches stecken in vielen Maschinen und Anlagen. Wer sie verbaut, ist nach CRA-Logik verpflichtet, Kunden zu informieren und Updates bereitzustellen. Startet der Switch dauernd neu, steht die Maschine still.

Empfehlung: In der SBOM bzw. Stückliste nach N-Tron 700 suchen und das Firmware-Update 3.11.1 an die Kunden ausrollen. Bis dahin die SNMP-Communities ändern oder SNMP abschalten und den Zugriff auf die Web-GUI sperren.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-01> ✓ geprüft

L-06 Moxa MGate: Stack Overflow schon mit Leserechten (CVE-2026-86325, CVSS4 9,4, MPSA-269540)

HOCH Moxa MPSA-269540 (über SecurityOnline, OpenCVE), 02.10.

Was ist neu: CVE-2026-86325 ist ein Stack Overflow im Parameter `account_name` der Kontoverwaltung. Schon ein Konto mit reinen Leserechten reicht, um Speicher zu korrumpieren, Zugangsdaten auszulesen und das Gerät lahmzulegen. Fixes gibt es für MB3170/MB3270 (v4.7.1), MB3180 (v2.7.1), MB3280 (v4.6.3), MB3480 (v4.5.1), MB3660 (v3.4.5) und 5217 (v1.5.5). Die zweite Lücke CVE-2026-86326 (fehlende Signaturprüfung der Firmware, CVSS4 8,6) erlaubt manipulierte Firmware und hat noch keinen Fix. Eine Ausnutzung ist nicht bekannt.

Bedeutung: MGate-Gateways sind in Retrofit-Projekten und bei der Anbindung von Altsteuerungen weit verbreitet. Sie werden oft in Schaltschränke eingebaut und bleiben jahrelang auf altem Firmware-Stand. Weil die Signaturprüfung der Firmware fehlt, lässt sich manipulierte Firmware dauerhaft verankern. Das ist ein Lieferkettenrisiko für jeden Integrator und Maschinenhersteller.

Empfehlung: Verbaute MGate-Serien in Stücklisten und Asset-Inventar finden und die Firmware nur aus offiziellen Moxa-Quellen aktualisieren (CC5). Das Web-Management nur aus dem Engineering- bzw. Wartungssegment erreichbar machen (CC2) und überflüssige Konten mit Leserechten entfernen.

Quelle: <https://securityonline.info/moxa-mgate-vulnerabilities/> ✓ geprüft

L-07 CODESYS-Lücken bei weiteren OEMs: KEB COMBIVIS Control Runtime (VDE-2026-105) und WAGO-SPS (VDE-2025-081)

HOCH CERT@VDE (VDE-2026-105, VDE-2025-081: <https://certvde.com/en/advisories/VDE-2025-081/>), 08.10.

Was ist neu: Betroffen ist die KEB COMBIVIS Control Runtime (arm64) ab 2.0.0 und vor 2.1.0 auf Basis von CODESYS 3.5.21.10. Über CVE-2025-41659 (CVSS 8,3) kann ein Angreifer mit wenigen Rechten den PKI-Ordner mit Zertifikaten und privaten Schlüsseln lesen und überschreiben. Drei weitere CVEs (CVSS 7,5/7,5/5,9) erlauben einen DoS ohne Anmeldung. Der Fix ist Version 2.1.0 mit CODESYS 3.5.21.50. WAGO meldet für mehrere SPS (`wago_os_linux` unter 4.10.0) CODESYS-Lücken mit DoS (bis CVSS 7,5) und Codeausführung über manipulierte Projektdateien. Der Fix ist Firmware 4.10.0.

Bedeutung: CODESYS steckt in den Steuerungen vieler OEMs, die die Runtime lizenzieren. Wer KEB oder WAGO verbaut, muss als Maschinenhersteller die Advisories seinen eigenen Maschinen zuordnen können und Updates bereitstellen. Unter dem CRA wird das zur Pflicht.

Empfehlung: Die SBOM nach dem CODESYS Runtime Toolkit durchsuchen, ausgelieferte Maschinen ermitteln und Updates nach Risiko priorisieren (CC5). Bei KEB über den App Manager oder das NOA Cloud Portal auf 2.1.0 aktualisieren und danach Zertifikate und Schlüssel neu ausstellen. Den Kunden ein kurzes Advisory mit dem Update-Weg schicken.

Quelle: <https://certvde.com/en/advisories/VDE-2026-105/> ✓ geprüft

L-08 Murrelektronik aas-edge-client (Verwaltungsschale): CVSS 9,8 ohne Patch, Hersteller rät zum Entfernen (VDE-2026-108)

HOCH CERT@VDE (VDE-2026-108), 06.10.

Was ist neu: Die REST-API (TCP 18000) der Referenz-Implementierung für das LNI-4.0-Testbed (alle Versionen) verlangt keine Anmeldung und nimmt Anfragen von jeder Herkunft an (CORS). Angreifer können die Daten der Verwaltungsschale lesen und ändern, auch über eine präparierte Webseite. Die falschen Daten können an AAS-Server weitergehen (CVE-2026-94293). Murrelektronik liefert keinen Fix, weil die Software als Messe-Demonstrator gedacht war, und rät, alle Installationen, Kopien und Container-Images zu entfernen.

Bedeutung: Demonstratoren und Referenzcode landen oft unbemerkt in Produkten oder Kundenprojekten. Manipulierte AAS-Daten wandern an zentrale AAS-Server und nachgelagerte Systeme weiter. Damit werden digitale Typenschilder und Produktdaten angreifbar, die künftig auch für den CRA und den Digitalen Produktpass zählen.

Empfehlung: Repositories, Container-Registries, Asset-Inventar und Kundenprojekte nach dem aas-edge-client durchsuchen und die Funde entfernen (CC5). Bis dahin den Zugriff auf TCP 18000 per Segmentierung sperren (CC2). Intern festlegen, dass Demo- und Referenzcode nie ohne Security-Review in ausgelieferte Produkte gelangt.

Quelle: <https://certvde.com/en/advisories/VDE-2026-108/> ✓ geprüft

L-09 lwIP-SMTP-Client: kritischer Buffer Overflow im eingebetteten TCP/IP-Stack (ICSA-26-279-02)

MITTEL CISA ICS Advisory, 06.10.

Was ist neu: Die CISA meldet einen kritischen Buffer Overflow im SMTP-Client von lwIP (CVE-2026-15340, CVSS 9,8). Betroffen ist der SMTP-Client in lwIP 2.2.1, der Hersteller hat einen Patch veröffentlicht (patch_125_smtp_txbuf.diff). lwIP ist ein Open-Source-Netzwerkstack, der in vielen Mikrocontroller-Produkten steckt.

Bedeutung: Für Komponentenhersteller ist das ein typischer Fall für den CRA, denn eine Lücke in einer Fremdkomponente muss bewertet werden. Wird sie aktiv ausgenutzt, muss der Endhersteller sie melden, sobald er weiß, dass sein Produkt betroffen ist.

Empfehlung: In den SBOMs der eigenen Produkte prüfen, ob lwIP mit aktiviertem SMTP-Client verbaut ist (laut CISA betroffen: SMTP-Client in lwIP 2.2.1, Fix per Patch patch_125_smtp_txbuf.diff). Die Betroffenheit dokumentieren und ein Update einplanen (CC5).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-02> ✓ geprüft

L-10 Cyber Resilience Act: Meldepflicht für ausgenutzte Schwachstellen gilt seit 11.09.2026

ORIENTIERUNG BSI, 11.09.

Was ist neu: Hersteller müssen aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle innerhalb von 24 Stunden als Frühwarnung melden. Nach 72 Stunden folgen weitere Informationen, spätestens 14 Tage nach dem Update der Abschlussbericht. Gemeldet wird über die zentrale ENISA-Plattform (CRA Single Reporting Platform, CRA-SRP). Die übrigen Pflichten gelten ab 11.12.2027.

Bedeutung: Die Advisories dieser Woche zu verbauten Komponenten (Switches, Gateways, Runtimes, Netzwerkstacks) zeigen, wie schnell eine Lücke beim Zulieferer zur Lücke im eigenen Produkt wird. Wird sie aktiv ausgenutzt, läuft für den Maschinenhersteller die 24-Stunden-Frist.

Empfehlung: Klare Zuständigkeiten im PSIRT festlegen und eine Meldevorlage vorbereiten. Den Ablauf an einem Fall dieser Woche als Übung durchspielen.

Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html ✓ geprüft

Fragen für das nächste Jour fixe

1. Welche Remote-Access-Gateways nutzen wir und unsere Service-Partner für die Fernwartung beim Kunden? Sind sie mit MFA abgesichert, gegen CVE-2026-88779 und die übrigen Lücken dieser Woche gepatcht und auf Kompromittierung geprüft?
2. Können wir innerhalb von 24 Stunden per SBOM sagen, in welchen ausgelieferten Maschinen N-Tron-Switches, Moxa MGate, CODESYS-Runtimes oder lwIP stecken (CRA-Frühwarnung)?
3. Wer meldet bei uns nach CRA eine aktiv ausgenutzte Schwachstelle an die ENISA-Plattform, und haben wir das schon geübt?
4. Liegt in unseren Projekten noch Demo- oder Referenzcode ohne Wartung, z. B. AAS-Clients?
5. Wie weit ist die Bewertung unserer Maschinen nach Anhang III 1.1.9/1.2.1 der Maschinenverordnung für den 20.01.2027?

Maßnahmen dieser Woche

1. Citrix NetScaler mit SAML auf 14.1-73.41 bzw. 13.1-64.28 (FIPS: 14.1-73.41 FIPS, 13.1-37.282 FIPS/NDcPP) bringen und auf Webshells und neue Konten prüfen.
2. FortiMail: IBE abschalten, das Management-Interface vom Internet trennen, IOCs prüfen und 8.0.2, 7.6.7 bzw. 7.4.9 einspielen (seit 05.10. verfügbar).
3. Cisco Catalyst SD-WAN Manager auf die gefixten Versionen patchen und serviceproxy-access.log und vmanage-server.log nach '/%6a_security_check' durchsuchen.
4. Bei allen FortiGate- und VPN-Zugängen für die Fernwartung die Zugangsdaten rotieren, MFA erzwingen und die Admin-Oberfläche vom Internet nehmen.
5. SBOMs und Stücklisten nach Red Lion N-Tron 700, Moxa MGate, KEB COMBIVIS/CODESYS, WAGO-SPS und lwIP 2.2.1 durchsuchen und betroffene Kunden informieren.
6. Den Murrelektronik aas-edge-client in Repositories, Container-Registries und Kundenprojekten suchen und entfernen.

7. Den CRA-Meldeablauf (24 h/72 h/14 Tage) an einem der Advisories dieser Woche als Übung durchspielen.
8. Für den ICS Patch Tuesday am 13.10. Zeit einplanen, um die neuen Advisories von Siemens und Schneider Electric zu bewerten.

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 09.10.2026 automatisch aufgerufen und inhaltlich geprüft.