

WOCHENBERICHT

OT-/Cyber-Lagebild Maschinen- und Anlagenbau

Ausgabe KW 42/2026 · Maschinen- und Anlagenbau in DACH

Zielgruppe	Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren
Berichtszeitraum	09.10.2026–16.10.2026
Version	1.0
Datum	16.10.2026
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 42 standen Fernwartung und Schwachstellen in Standardkomponenten im Mittelpunkt. Ivanti Connect Secure hat einen aktiv ausgenutzten Zero-Day (CVE-2026-104935). Für die nachgelagerte Privilege Escalation gibt es noch keinen Patch, und laut Volexity waren auch voll gepatchte Geräte betroffen. Bei PAN-OS wird eine Lücke in der Management-Oberfläche bereits ausgenutzt (CVE-2026-0322). In Frankreich läuft laut CERT-FR weiter eine Kampagne gegen Kühlsteuerungen von Danfoss, Copeland und Dixell, die aus dem Internet erreichbar sind. Geräte ohne Patch (End-of-Life) werden laut CERT-FR auch nach einem Factory Reset sehr wahrscheinlich wieder kompromittiert. Das BSI hat am 13.10. dringend gefordert, Steuerungen nicht direkt aus dem Internet erreichbar zu machen (BSI-CS 154). Für Maschinenbauer ist das ein Lehrstück über Fernwartungszugänge, die sie selbst ausliefern, und über den Umgang mit ihrer installierten Basis.

Auf Produktseite brachte der Patchday 17 Siemens-Advisories. Darunter sind über 400 Lücken im GNU/Linux-Subsystem einzelner S7-1500-CPU's und SSA-591731 mit Webserver-Lücken bis CVSS 9,6 in S7-1500, ET 200SP und Drive Controllern, für die es noch keinen Fix gibt. Hinzu kommen das Bulletin SSB-091449 zu Zugriffsattributen in TIA-Portal-Projekten, sechs Lücken in der OPC-UA-Bibliothek Eclipse Milo (für den 0.6.x-Zweig gibt es keinen Patch), eine Privilege Escalation in Ignition und eine kritische Lücke im Rockwell ArmorBlock I/O. Wer Milo in eigenen Gateways oder Edge-Produkten verbaut, sollte das jetzt im SBOM prüfen. Seit dem 11.09.2026 gilt die Meldepflicht nach dem Cyber Resilience Act: Aktiv ausgenutzte Schwachstellen in eigenen Produkten müssen innerhalb von 24 Stunden über die ENISA Single Reporting Platform gemeldet werden.

GESAMTBEWERTUNG

Die Lage ist hoch (widersprüchlich: A „hoch“ / B „erhöht“). Übernommen ist „hoch“, weil Fernwartungs-Gateways und Firewalls (Ivanti, PAN-OS) aktiv angegriffen werden und eine Kampagne gegen Steuerungen am Internet läuft. Gleichzeitig sind mehrere Lücken in Standardkomponenten (S7-1500, OPC UA, Edge, I/O) noch nicht behoben. Vorrang haben Patch und Kompromittierungsprüfung bei Ivanti und PAN-OS, danach die Webserver-Mitigation bei S7-1500, die SBOM-Prüfung auf Eclipse Milo und das Abschalten direkt erreichbarer Fernwartungszugänge.

Trends

- Fernwartungs-Gateways und Firewalls (Ivanti, PAN-OS) bleiben der bevorzugte Initial Access, auch auf voll gepatchten Geräten.
- Angreifer nutzen gezielt Herstellersteuerungen mit Webportal, die für den Service ins Internet gestellt wurden, darunter EoL-Geräte (Kühltechnik Frankreich). Das BSI erwartet Nachahmer. Damit wächst der Druck auf Hersteller, ihre installierte Basis aktiv zu betreuen.
- Siemens und CISA melden immer öfter Lücken in eingebetteten Komponenten (Linux-Subsystem der S7-1500 MFP, OpenSSL, SQLite, Eclipse Milo). Ohne SBOM lässt sich kaum beurteilen, ob das eigene Produkt betroffen ist. Das SBOM wird damit zur Pflichtaufgabe der Produkt-Security.
- Für mehrere kritische Lücken gibt es zunächst nur Mitigations und keinen Fix (SSA-591731, Teile der MFP-Advisories). Hersteller müssen ihre Kunden über eigene Zwischenmaßnahmen informieren.

- Seit dem 11.09.2026 gilt die CRA-Meldepflicht über die ENISA Single Reporting Platform. Damit wird Produkt-Security zu einem Prozess mit Fristen von 24 und 72 Stunden.
- Ab dem 20.01.2027 verlangt die Maschinenverordnung Cybersecurity-Nachweise in der technischen Dokumentation. Die harmonisierten Normen zu CRA und Maschinenverordnung sind aber noch offen.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Ivanti Connect Secure: aktiv ausgenutzter Zero-Day, Privilege Escalation noch ohne Patch (CVE-2026-104935)	KRITISCH	BleepingComputer / Rapid7 (mit Bezug auf Ivanti und Volexity), 13.10.
L-02	BSI und CERT-FR nach den Angriffen auf Kühlsteuerungen von Danfoss, Copeland und Dixell: Steuerungen nicht direkt ans Internet (BSI-CS 154, CERTFR-2026-ALE-012)	HOCH	BSI / CERT-FR (CERTFR-2026-ALE-012), 13.10.
L-03	Siemens SIMATIC S7-1500, ET 200SP und Drive Controller: Webserver-Lücken bis CVSS 9,6, noch kein Fix (SSA-591731)	HOCH	Siemens ProductCERT, 13.10.
L-04	Eclipse Milo (OPC UA): sechs Lücken im Server, kein Patch für den 0.6.x-Zweig (ICSA-26-288-01)	HOCH	CISA ICS Advisory, 15.10.
L-05	Palo Alto PAN-OS: Lücke in der Management-Oberfläche wird ausgenutzt (CVE-2026-0322)	HOCH	Palo Alto Networks Security Advisory, 14.10.
L-06	Siemens-Bulletin SSB-091449: Variablenattribute „Accessible/Writable from HMI/OPC UA/Web API“ schützen PG/HMI-Zugriffe nicht	HOCH	Siemens ProductCERT, 13.10.
L-07	ICS-Patchday Oktober: 17 Siemens-Advisories, über 400 Lücken im Linux-Subsystem der S7-1500, dazu Schneider und CERT@VDE	HOCH	SecurityWeek, 14.10.
L-08	Rockwell 1732E ArmorBlock I/O: Passwortänderung ohne Anmeldung (CVE-2026-12655, CVSS 9,1; SD1801)	HOCH	Rockwell Automation Security Advisory, 13.10.
L-09	Inductive Automation Ignition: Privilege Escalation bis zur Codeausführung im Gateway (CVE-2026-92817, CVSS 8,8; ICSA-26-286-01)	MITTEL	CISA, 13.10.
L-10	Cyberangriff auf das Baukonsortium des Fehmarnbelt-Tunnels (Femern Link Contractors)	MITTEL	Ingeniøren (ing.dk), 13.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 16.10.2026):

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	143086	DNP3: 33392, OMRON FINS: 23267, ProConOS: 16506, Siemens S7: 8211, OPC UA: 5676
Österreich	4649	HMI/VNC: 1053, DNP3: 949, IEC-104: 454, Siemens S7: 357, OPC UA: 139

Meldungen im Detail

L-01 Ivanti Connect Secure: aktiv ausgenutzter Zero-Day, Privilege Escalation noch ohne Patch (CVE-2026-104935)

KRITISCH BleepingComputer / Rapid7 (mit Bezug auf Ivanti und Volexity), 13.10.

Was ist neu: Ivanti hat am 13.10. eine aktiv ausgenutzte Lücke bestätigt (Authentication Bypass und Remote Code Execution, CVSS 8,6). Betroffen sind die Versionen bis 22.8R2.4, bis 25.1.1.1 und bis 25.1.2.2. Gepatcht sind 22.8R2.5, 25.1.1.2 und 25.1.3.x. Laut Volexity kommt der Threat Actor UTA0576 über eine weitere Privilege Escalation, für die es noch keinen Patch gibt, an Root-Rechte. Beim Opfer hat er Active-Directory-Zugangsdaten, LAPS-Passwörter und BitLocker-Schlüssel abgegriffen.

Bedeutung: Viele Maschinenbauer und Integratoren nutzen Ivanti-Gateways als Zugang für die Fernwartung von Kundenanlagen. Ein kompromittiertes Gateway öffnet den Weg ins eigene AD und von dort per Lateral Movement in die Service-Zugänge zu Kunden. Laut Volexity hat der Angreifer Logs manipuliert und das Integrity Checker Tool umgangen.

Empfehlung: Sofort auf eine gepatchte Version gehen und die Kompromittierung mit Netzwerk- und Speicheranalyse prüfen, denn der Integrity Checker allein genügt nicht. AD-Zugangsdaten, die über das Gateway liefen, rotieren und die Service-Zugänge zu Kunden prüfen.

Quelle: <https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-day-exploited-in-attacks/> ✓ geprüft

L-02 BSI und CERT-FR nach den Angriffen auf Kühlsteuerungen von Danfoss, Copeland und Dixell: Steuerungen nicht direkt ans Internet (BSI-CS 154, CERTFR-2026-ALE-012)

HOCH BSI / CERT-FR (CERTFR-2026-ALE-012), 13.10.

Was ist neu: Das CERT-FR hat seine Warnung vom 12.10. am 13.10. erweitert. Außer Danfoss AK-SM und AK-SC sind jetzt auch Copeland xweb und Dixell xweb betroffen. Laut CERT-FR laufen die Angriffe wahrscheinlich noch. Geräte ohne Patch (End-of-Life), die aus dem Internet erreichbar bleiben, werden auch nach einem Factory Reset sehr wahrscheinlich wieder kompromittiert. Einen Angriffsvektor oder eine CVE nennt das CERT-FR nicht. Das BSI fordert Betreiber kleinerer Anlagen (Lebensmittelkühlung, Stromerzeugung) eindringlich auf, Steuerungen nicht direkt ins Internet zu stellen und VPN, MFA und Updates zu nutzen.

Bedeutung: Hier richten Angriffe auf Steuerungen eines Komponentenherstellers beim Betreiber Schaden an. Die betroffenen Geräte sind Herstellersteuerungen mit Webportal, die für den Service ins Internet gestellt wurden. Dasselbe Muster findet sich bei vielen Maschinen mit eigenem Fernwartungsportal. EoL-Geräte mit öffentlicher IP bleiben für Hersteller ein Haftungs- und Reputationsrisiko. Wird eine Schwachstelle in einem eigenen Produkt aktiv ausgenutzt, gilt seit dem 11.09.2026 die CRA-Meldepflicht mit Frühwarnung binnen 24 Stunden. Für neue Produkte verlangt der CRA ab Dezember 2027 einen festgelegten Support-Zeitraum und sichere Voreinstellungen.

Empfehlung: Prüfen, welche eigenen Steuerungen und Web-Oberflächen beim Kunden direkt aus dem Internet erreichbar sind, und betroffene Kunden aktiv anschreiben. Remote Access nur noch über einen gesicherten Zugang anbieten (VPN oder Fernwartungs-Gateway mit MFA). Standardpasswörter ab Werk abschaffen bzw. bei der Auslieferung eine Änderung erzwingen. End-of-Life-Produkte im Feld ermitteln und die Kunden informieren (CC4 Secure Remote Access).

Quelle: <https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/> ✓ geprüft

L-03 Siemens SIMATIC S7-1500, ET 200SP und Drive Controller: Webserver-Lücken bis CVSS 9,6, noch kein Fix (SSA-591731)

HOCH Siemens ProductCERT, 13.10.

Was ist neu: Siemens meldet acht CVEs (CVE-2026-63350 bis -63357, Eval Injection und XSS) im Webserver mehrerer Produkte: S7-1500-CPU's einschließlich F-, T- und MFP-Varianten, ET 200SP CPU's und Open Controller, Drive Controller 1504D/1507D TF, S7-1500 Software Controller, PLCSIM Advanced und SIPLUS. Für alle Produkte gilt: „Currently no fix is available“. Siemens bereitet Fixes vor. Für einen Angriff muss ein Nutzer mit dem Recht „Read diagnostics“ eine präparierte Trace- oder Signaldatei importieren.

Bedeutung: Die S7-1500 ist in Maschinen aus DACH Standard. Wer Maschinen mit aktivem Webserver ausgeliefert hat, braucht bis zum Fix eine Kundeninformation zur Mitigation. Der Angriff läuft über Social Engineering. Deshalb sind auch Servicetechniker ein Einfallstor, wenn sie Trace-Dateien austauschen.

Empfehlung: Den Webserver abschalten, wo er nicht gebraucht wird. Sonst den Zugriff auf 80/tcp und 443/tcp auf feste Engineering-IPs begrenzen. Trace-Dateien nur aus vertrauenswürdigen Quellen importieren und die Kunden über das Advisory informieren (CC5 Risk-Based Vulnerability Management).

Quelle: <https://cert-portal.siemens.com/productcert/html/ssa-591731.html> ✓ geprüft

L-04 Eclipse Milo (OPC UA): sechs Lücken im Server, kein Patch für den 0.6.x-Zweig (ICSA-26-288-01)

HOCH CISA ICS Advisory, 15.10.

Was ist neu: Die CISA meldet sechs CVEs in der Java-Bibliothek Eclipse Milo (Server-Seite, Versionen 0.6.0 bis 1.1.4). Der Kopf des Advisories nennt fünf. Anonyme Clients können geschützte Methoden aufrufen (fehlende Autorisierung, CVE-2026-58080, CVSS v3.1 8,2). Über ein Padding Oracle lassen sich Passwörter zurückgewinnen (CVE-2026-60007, CVSS v4 9,1). Dazu kommt ein Speicherleck mit DoS (CVE-2026-63252). Behoben ist das nur in 1.1.5, für 0.6.x gibt es keinen Fix. Unter den genannten Sektoren ist auch Critical Manufacturing.

Bedeutung: Milo steckt als Open-Source-Komponente unsichtbar in vielen Gateways, MES-Anbindungen und Edge-Apps von Komponentenherstellern und Integratoren. Wer Milo verbaut, ist Hersteller im Sinne des CRA und muss die Lücken in seinen Produkten bewerten und beheben. Wird eine davon aktiv ausgenutzt, gilt die Meldepflicht.

Empfehlung: In den SBOMs und Build-Abhängigkeiten aller ausgelieferten Produkte nach org.eclipse.milo suchen, auf 1.1.5 umstellen und ein eigenes Advisory für die Kunden herausgeben. Bis dahin anonyme OPC-UA-Sessions im Auslieferungszustand abschalten (CC5 Risk-Based Vulnerability Management).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-288-01> ✓ geprüft

L-05 Palo Alto PAN-OS: Lücke in der Management-Oberfläche wird ausgenutzt (CVE-2026-0322)

HOCH Palo Alto Networks Security Advisory, 14.10.

Was ist neu: Wer gültige Admin-Zugangsdaten hat und die Management-Oberfläche erreicht, kann Code als root ausführen (CVSS 4.0: 8,6). Betroffen sind PA-Series, VM-Series und Panorama mit PAN-OS 10.2 bis 12.2, nicht betroffen sind Cloud NGFW und Prisma Access. Palo Alto meldet „very limited exploitation“. Fixes gibt es für alle Zweige.

Bedeutung: In vielen Produktionsnetzen und an Fernwartungszugängen sichern PAN-OS-Firewalls die Segmentierung. Ist die Firewall übernommen, ist die Trennung zwischen IT, OT und Dienstleistern aufgehoben.

Empfehlung: Auf eine gepatchte Version gehen und die Management-Oberfläche nur über einen Jump Host aus dem Admin-Netz erreichbar machen. Admin-Konten mit MFA absichern und ihre Anmeldungen prüfen.

Quelle: <https://security.paloaltonetworks.com/CVE-2026-0322> ✓ geprüft

L-06 Siemens-Bulletin SSB-091449: Variablenattribute „Accessible/Writable from HMI/OPC UA/Web API“ schützen PG/HMI-Zugriffe nicht

HOCH Siemens ProductCERT, 13.10.

Was ist neu: Siemens stellt klar, dass die Attribute je Variable nur bei OPC UA und Web API greifen. Bei PG/HMI-Kommunikation werden sie nicht durchgesetzt. Laut Siemens ist das so gewollt, die Dokumentation im TIA Portal war aber missverständlich. Betroffen sind S7-1500/ET 200MP, S7-1200 G2 und SINUMERIK ONE.

Bedeutung: Möglicherweise verlassen sich viele Steuerungsprojekte auf diese Attribute als Schreibschutz für sicherheitsrelevante Parameter. Für Maschinenbauer betrifft das die eigene Security-Architektur und die Risikobeurteilung nach Maschinenverordnung und IEC 62443.

Empfehlung: Standardprojekte und Bibliotheken darauf prüfen, ob die Attribute als Zugriffsschutz gedacht waren. PG/HMI-Zugriffe über Schutzstufen und Function Rights absichern und das Ergebnis in der Security-Dokumentation der Maschine festhalten (CC2 Defensible Architecture).

Quelle: <https://cert-portal.siemens.com/productcert/html/ssb-091449.html> ✓ geprüft

L-07 ICS-Patchday Oktober: 17 Siemens-Advisories, über 400 Lücken im Linux-Subsystem der S7-1500, dazu Schneider und CERT@VDE

HOCH SecurityWeek, 14.10.

Was ist neu: Siemens hat 17 neue Advisories veröffentlicht. Kritisch eingestuft sind einzelne Simatic S7-1500-CPU's mit über 400 Lücken im GNU/Linux-Subsystem, Industrial Edge und Ruggedcom Crossbow SAC. Weitere Advisories betreffen Deserialisierungslücken in Engineering-Plattformen vor V20, Path Traversal in Industrial Edge, einen hart codierten Testschlüssel in SIMATIC IPCs (Umgehung von Secure Boot) und Lücken in LOGO! 8. Schneider Electric meldet unter anderem eine Lücke in Sage RTUs, über die ein privilegierter Nutzer Schad-Firmware installieren kann. CERT@VDE hat VDE-2026-109 (Bender) veröffentlicht.

Bedeutung: Maschinenbauer und Integratoren, die diese Komponenten verbauen, müssen ihren Kunden sagen, welche Anlagen betroffen sind und wann ein Update möglich ist. Für einige Siemens-Lücken gibt es bisher nur Mitigations.

Empfehlung: Die Advisories mit der Stückliste ausgelieferter Maschinen abgleichen und die Kunden mit betroffenen Anlagen informieren. Updates nach Erreichbarkeit und Kritikalität priorisieren. Wo es keinen Patch gibt, die Mitigations umsetzen.

Quelle: <https://www.securityweek.com/ics-patch-tuesday-siemens-issues-17-advisories-rockwell-fixes-armorblcock-takeover-flaw/> ✓ geprüft

L-08 Rockwell 1732E ArmorBlock I/O: Passwortänderung ohne Anmeldung (CVE-2026-12655, CVSS 9,1; SD1801)

HOCH Rockwell Automation Security Advisory, 13.10.

Was ist neu: Angreifer ohne Konto können das Webserver-Passwort ändern und so das Admin-Konto übernehmen (CVE-2026-12655, CVSS 3.1 9,1). Eine zweite Lücke (CVE-2026-12656, CVSS 3.1 7,5) legt die Kommunikation bei Storm-Traffic lahm, danach muss das Gerät aus- und wieder eingeschaltet werden. Betroffen ist Firmware bis 3.012, Version 3.013 behebt beide Lücken. Einen Workaround gibt es nicht.

Bedeutung: ArmorBlock-Module sitzen direkt an Maschinen und Fördertechnik. Ein Ausfall durch Netzlast führt zum Stillstand, der nur mit einem Eingriff vor Ort behoben werden kann. Das betrifft vor allem die installierte Basis von Maschinenbauern, die nach Nordamerika exportieren oder Rockwell-Ausrüstung auf Kundenwunsch verbauen.

Empfehlung: Ausgelieferte Maschinen mit 1732E im Asset-Inventar ermitteln, die Firmware-Stände prüfen und das Update mit den Kunden abstimmen, etwa beim nächsten Serviceeinsatz. Die I/O-Ebene in eine eigene Zone legen, damit sie aus dem Büronetz nicht erreichbar ist (CC2 Defensible Architecture).

Quelle: <https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1801.html> ✓ geprüft

L-09 Inductive Automation Ignition: Privilege Escalation bis zur Codeausführung im Gateway (CVE-2026-92817, CVSS 8,8; ICSA-26-286-01)

MITTEL CISA, 13.10.

Was ist neu: Ein angemeldeter Nutzer mit Zugriff auf ein Vision-Projekt kann über seine Session-ID Designer-Rechte erlangen und Code im Ignition-Gateway ausführen. Betroffen sind 8.1.0 bis 8.1.54 und 8.3.0 bis 8.3.8. Laut CISA ist keine öffentliche Ausnutzung bekannt.

Bedeutung: Ignition ist bei Systemintegratoren in DACH beliebt, vor allem für Visualisierung und MES-Anbindung. Ein kompromittiertes Gateway eignet sich als Ausgangspunkt für Lateral Movement in die Steuerungsebene.

Empfehlung: Kundeninstallationen über die Wartungsverträge ermitteln und Updates einplanen. Bis dahin die Vision-Nutzerkonten auf das Nötige begrenzen (CC5 Risk-Based Vulnerability Management).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-286-01> ✓ geprüft

L-10 Cyberangriff auf das Baukonsortium des Fehmarnbelt-Tunnels (Femern Link Contractors)

MITTEL Ingenieuren (ing.dk), 13.10.

Was ist neu: Femern A/S hat bestätigt, dass das Konsortium FLC von einem Cyberangriff betroffen ist. Ob Ransomware im Spiel war und wer dahintersteckt, ist offiziell nicht bekannt. Berichte über stillstehende Kräne, Schiffe und Zugangskarten stammen nur aus der Presse.

Bedeutung: Anlagenbauer und Zulieferer in Großprojekten hängen an der IT des Konsortiums (Zugänge, Projektdaten, Logistik). Fällt sie aus, sind Termine betroffen, und auch Unterauftragnehmern drohen Vertragsstrafen.

Empfehlung: In laufenden Großprojekten klären, wer bei einem Incident meldet, wer entscheidet und wie Projektdaten offline verfügbar bleiben. Diese Absprachen in den eigenen IR-Plan aufnehmen (CC1 ICS Incident Response).

Quelle: <https://ing.dk/artikel/fehmarbelt-tunnel-project-hit-cyber-attack> ✓ geprüft

Fragen für das nächste Jour fixe

1. In welchen unserer ausgelieferten Produkte steckt Eclipse Milo oder ein anderer OPC-UA-Stack, und wer pflegt das SBOM?
2. Ist unser CRA-Meldeweg für die 24-Stunden-Frühwarnung über die ENISA-Plattform eingerichtet und getestet, und wer ist als Vertreter registriert?
3. Welche Ivanti- und PAN-OS-Geräte nutzen wir oder unsere Kunden für die Fernwartung, und sind sie gepatcht und auf Kompromittierung geprüft?
4. Wie erfahren wir, welche unserer Geräte beim Kunden direkt aus dem Internet erreichbar sind, und wie informieren wir die Kunden bei EoL?
5. Sind die Cybersecurity-Nachweise nach Maschinenverordnung für Maschinen, die ab dem 20.01.2027 in Verkehr gebracht werden, in der technischen Dokumentation eingeplant?

Maßnahmen dieser Woche

1. Ivanti Connect Secure auf 22.8R2.5, 25.1.1.2 oder 25.1.3.x bringen, auf Kompromittierung prüfen und AD-Zugangsdaten rotieren.
2. PAN-OS auf die gefixte Version aktualisieren und die Management-Oberfläche nur über einen Jump Host im Admin-Netz zulassen.
3. Bei S7-1500, ET 200SP und Drive Controllern den Webserver abschalten oder 80/443 auf feste Engineering-IPs begrenzen, bis Siemens einen Fix für SSA-591731 liefert.
4. Das SBOM aller Gateway-, Edge- und SCADA-Produkte nach Eclipse Milo durchsuchen und den Umstieg auf 1.1.5 einplanen.
5. Steuerungsprojekte und Bibliotheken auf die Nutzung der HMI/OPC UA/Web API-Attribute als Schreibschutz prüfen (SSB-091449).
6. Siemens-, Schneider-, Rockwell- und Ignition-Advisories vom Patchday mit der Stückliste ausgelieferter Maschinen abgleichen und die Kunden informieren.
7. Per Shodan oder Censys prüfen, ob eigene Steuerungen mit öffentlicher IP erreichbar sind, und die betroffenen Kunden anschreiben.

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 16.10.2026 automatisch aufgerufen und inhaltlich geprüft.