

WOCHENBERICHT

OT-/Cyber-Lagebild Kommunale Versorger und KRITIS

Ausgabe KW 41/2026 · Kommunale Versorger und KRITIS in DACH

Zielgruppe	Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber
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 Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 41 kamen die größten Risiken für kommunale Versorger und KRITIS-Betreiber in DACH wieder über die IT und über die Edge Devices am Netzrand. Über diese Geräte wickeln Stadtwerke und Wasserbetriebe den Remote Access für Leitstellen und Dienstleister ab. Fünf Produktgruppen werden aktiv angegriffen. Die NetScaler-SAML-Lücke CVE-2026-88779 (laut Citrix Denial of Service) wird gezielt angegriffen und trifft auch Geräte, die schon gegen CVE-2026-88771 bis -88778 gepatcht waren. Bei Cisco Catalyst SD-WAN Manager (CVE-2026-76504, CVSS 9,8) und FortiMail (CVE-2026-104286, CVSS 9,8) gibt es inzwischen Patches, bei FortiMail seit 05.10. Laut FBI und Secret Service läuft die FortiBleed-Kampagne gegen FortiGate-Firewalls und VPNs weiter: Die Angreifer sperren Administratoren aus und verkaufen die Zugänge an Ransomware-Gruppen. Außerdem steht Zammad seit 02.10. im KEV-Katalog. Laut Symantec hat die Warlock-Gruppe Longlegs (Storm-2603) unter anderem einen Wasserversorger angegriffen, ToolShell-Lücken in on-prem SharePoint gehören zu ihrem Arsenal. Im ausführlich beschriebenen Fall eines KRITIS-Betreibers vergingen von der ersten Aktivität bis zur Ransomware etwa neun Tage.

Auf OT-Ebene gab es mehrere kritische Advisories für Komponenten, die in DACH weit verbreitet sind. Hitachi Energy RTU500 hat Lücken bis CVSS 9,8 in der End-of-Life-Firmware 11.x der Fernwirktechnik (ICSA-26-279-06). Dazu kommen Moxa-MGate-Protokoll-Gateways, CODESYS-Runtimes bei KEB und am 08.10. Advisories zu openPDC/openHistorian und Red Lion N-Tron-Switches. Das Datenleck beim Zertifizierer GUTcert zeigt ein Risiko in der Lieferkette: Netzpläne und Audit-Berichte deutscher Energieversorger liegen vermutlich bei den Angreifern. Für kleine Teams gilt: Statt Einzelmeldungen abzuarbeiten, sollten sie die SANS Five ICS Critical Controls umsetzen, vor allem Secure Remote Access (CC4) und Risk-Based Vulnerability Management (CC5). Mit KI-Unterstützung ist das auch personell machbar.

GESAMTBEWERTUNG

Die Lage ist hoch. Mehrere aktiv ausgenutzte Zero-Days und eine Credential-Kampagne treffen genau die Remote-Access- und Edge-Geräte, über die Fernwartung und Leittechnik erreichbar sind. Vorrang haben Patches und eine Kompromittierungsprüfung für NetScaler, FortiGate/FortiMail und Cisco SD-WAN. Danach folgt die Prüfung des Asset-Inventars auf RTU500-, MGate- und CODESYS-Geräte mit altem Firmware-Stand.

Trends

- Edge Devices für Remote Access (NetScaler, FortiGate, SD-WAN, SonicWall SMA1000) bleiben das Haupteinfallstor. Neue Lücken treffen inzwischen auch frisch gepatchte Geräte (NetScaler), deshalb reicht Patchen allein ohne Kompromittierungsprüfung nicht mehr.
- Ransomware kommt weiter über die IT: Alte, ungepatchte Lücken wie in on-prem SharePoint reichen Threat Actors, um KRITIS-Betreiber in wenigen Tagen zu verschlüsseln.
- Initial Access Broker verkaufen kompromittierte Firewall- und VPN-Zugänge im großen Stil an Ransomware-Gruppen (FortiBleed → INC/Lynx/Payload). Gegen Credential-Kampagnen helfen keine Patches, nur saubere Zugangsdaten und MFA.
- Das Lieferkettenrisiko verschiebt sich auf Dienstleister mit sensiblen Betreiberdaten (Zertifizierer, Helpdesk-Software wie Zammad, Atlassian).

- In der OT häufen sich Advisories für EoL-Firmware und OEM-Runtimes (RTU500, CODESYS, openPDC). Ohne Asset-Inventar ist keine Priorisierung möglich.

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	Cisco Catalyst SD-WAN Manager: Auth-Bypass-Zero-Day CVE-2026-76504 (CVSS 9,8) aktiv ausgenutzt	HOCH	Cisco Security Advisory / CISA KEV / Help Net Security (weitere Quellen: https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog , https://helpnetsecurity.com/2026/10/01/new-cisco-sd-wan-zero-day-exploited-in-the-wild-cve-2026-76504/), 30.09.
L-03	Update FortiMail CVE-2026-104286 (CVSS 9,8): Patches seit 05.10. verfügbar, 7.2 ohne Fix	HOCH	Fortinet PSIRT FG-IR-26-175 / CISA KEV / heise / BleepingComputer (weitere Quellen: https://www.heise.de/en/news/FortiMail-Attacks-on-zero-day-vulnerability-underway-work-around-available-11473685.html , https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/), 05.10.
L-04	Hitachi Energy RTU500: kritische Lücken bis CVSS 9,8 in End-of-Life-Firmware 11.x (ICSA-26-279-06)	HOCH	CISA ICS Advisory ICSA-26-279-06 / Hitachi Energy PSIRT, 06.10.
L-05	Warlock-Ransomware (Longlegs/Storm-2603) trifft Wasserversorger über on-prem SharePoint	HOCH	Symantec Threat Intelligence (Broadcom), bestätigt durch BleepingComputer/SecurityWeek/The Record (weitere Quelle: https://www.bleepingcomputer.com/news/security/warlock-ransomware-breach-sharepoint-in-water-telecom-operator-attacks/), 01.10.

ID	Meldung	Relevanz	Quelle
L-06	Datenleck beim Zertifizierer GUTcert: Netzpläne und Audit-Berichte deutscher Energieversorger betroffen	HOCH	IT-Administrator / energate messenger / GUTcert, 06.10.
L-07	Feldebene: Moxa MGate (CVE-2026-86325) und KEB COMBIVIS/CODESYS (VDE-2026-105) mit kritischen Lücken	MITTEL	Moxa MPSA-269540 (über SecurityOnline: https://securityonline.info/moxa-mgate-vulnerabilities/) / CERT@VDE VDE-2026-105, 08.10.
L-08	Neue ICS-Advisories 08.10.: openPDC/openHistorian (Energie) und Red Lion N-Tron 700	MITTEL	CISA ICS Advisories ICSA-26-281-01 (Red Lion N-Tron 700) / ICSA-26-281-02 (openPDC/openHistorian, https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-02), 08.10.

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. Ob auch Codeausführung möglich ist, ist nicht bestätigt: Citrix spricht nur von DoS, Kevin Beaumont berichtet von einem heruntergeladenen Malware-Binary auf einem gepatchten Honeypot, watchTowr hat die Lücke reproduziert.

Bedeutung: Bei vielen Stadtwerken läuft der Remote Access für Dienstleister und Bereitschaft über NetScaler. Beaumont verweist auf CVE-2025-6543: Diese Lücke war anfangs ebenfalls nur als DoS eingestuft und wurde später für Codeausführung genutzt. Schon ein Absturz des Gateways legt die Fernwartung lahm, ein übernommenes Gateway könnte den Weg in die Leittechnik öffnen. Patchen allein schließt einen bereits erfolgten Zugriff nicht aus.

Empfehlung: In der Konfiguration nach 'add authentication samlAction' bzw. 'samlIdPProfile' suchen und betroffene Geräte sofort auf 14.1-73.41 bzw. 13.1-64.28 aktualisieren. Danach nach Webshells, neuen Konten und auffälligen Sessions suchen und die Session-Tokens invalidieren. Bei Verdacht den Zugang vom Netz nehmen und den Incident-Response-Plan auslösen. Für die Fernwartung einen Fallback-Zugang über einen Jump Host vorbereiten.

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

L-02 Cisco Catalyst SD-WAN Manager: Auth-Bypass-Zero-Day CVE-2026-76504 (CVSS 9,8) aktiv ausgenutzt

HOCH Cisco Security Advisory / CISA KEV / Help Net Security (weitere Quellen:

<https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog>,
<https://helpnetsecurity.com/2026/10/01/new-cisco-sd-wan-zero-day-exploited-in-the-wild-cve-2026-76504/>,
30.09.

Was ist neu: Über eine kodierte URL (/%6a_security_check, also ein kodierte 'j_security_check') umgehen Angreifer die Anmeldung und bekommen Admin-Rechte auf die API. Laut Cisco wird die Lücke seit September ausgenutzt, es ist der fünfte ausgenutzte Cisco-Zero-Day 2026. 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. Advisory-Version 1.1 erschien am 02.10. (Relevanz widersprüchlich: A KRITISCH / B HOCH)

Bedeutung: Wer Außenstellen, Pumpwerke oder die Netzleittechnik per SD-WAN anbindet, gibt Angreifern mit dem Manager die zentrale Steuerung der gesamten Standortvernetzung, inklusive der Routen in OT-Segmente. Das ist ein klassischer Ausgangspunkt für Lateral Movement.

Empfehlung: Sofort auf eine gefixte Version aktualisieren und Versionen vor 20.9 auf ein gefixtes Release migrieren. Danach serviceproxy-access.log und vmanage-server.log nach /%6a_security_check bzw. kodierte Zugriffen auf 'j_security_check' durchsuchen. Den Manager nur aus einem dedizierten Management-Netz bzw. hinter einer filternden Firewall erreichbar machen.

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

L-03 Update FortiMail CVE-2026-104286 (CVSS 9,8): Patches seit 05.10. verfügbar, 7.2 ohne Fix

HOCH Fortinet PSIRT FG-IR-26-175 / CISA KEV / heise / BleepingComputer (weitere Quellen: <https://www.heise.de/en/news/FortiMail-Attacks-on-zero-day-vulnerability-underway-workaround-available-11473685.html>, <https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/>), 05.10.

Was ist neu: Die Path-Traversal-Lücke wird ohne Anmeldung ausgenutzt, die CISA führt sie seit 01.10. im KEV-Katalog. 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. Zum Patch-Stand gibt es eine Abweichung (widersprüchlich: A die Fixes sind nur angekündigt / B Fortinet hat das Advisory am 05.10. um die Lösung ergänzt). B ist durch das PSIRT-Advisory besser belegt. Die Fixes sind 8.0.2, 7.6.7 und 7.4.9. Für den Zweig 7.2 gibt es keinen eigenen Fix, er muss auf 7.4 oder neuer migriert werden. FortiMail Cloud wurde am 05.10. serverseitig behoben.

Bedeutung: Die Lücke erlaubt ohne Anmeldung das Schreiben von Dateien und damit Codeausführung auf dem Mail-Gateway. Das Gateway steht bei Stadtwerken direkt am Internet und ist ein bequemer Einstieg ins IT-Netz, von wo aus Ransomware in Richtung OT vordringen kann.

Empfehlung: Sofort aktualisieren. Bis dahin den IBE-Dienst abschalten, das Management-Interface vom Internet trennen und Webmail auf vertrauenswürdige Netze beschränken. In den Logs nach den von Fortinet genannten IOCs suchen, etwa dem Konto 'archive234'.

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

L-04 Hitachi Energy RTU500: kritische Lücken bis CVSS 9,8 in End-of-Life-Firmware 11.x (ICSA-26-279-06)

HOCH CISA ICS Advisory ICSA-26-279-06 / Hitachi Energy PSIRT, 06.10.

Was ist neu: Die CISA hat das Advisory am 06.10. veröffentlicht. Die Hitachi-Meldung stammt vom 29.09., gefunden hat die Lücken Dragos. Betroffen ist die CMU-Firmware 11.x und älter (End-of-Life) mit insgesamt sechs Lücken, darunter: ein Firmware-Upload ohne Anmeldung bzw. ohne Integritätsprüfung (CVE-2026-8065, CVSS 9,1), ein Path Traversal zum Schreiben beliebiger Dateien (CVE-2026-8066, 9,1), ein Reboot ohne Berechtigung, die alte VxWorks-WDB-Debug-Lücke CVE-2010-2965 (9,8, UDP 17185) und eine Befehlsausführung ohne Anmeldung (CVE-2014-9195). Für die EoL-Versionen gibt es keine Patches. Abhilfe ist nur das Upgrade auf 12.7.8 oder 13.9.1.

Bedeutung: RTU500 sind in DACH in der Fernwirktechnik von Stadtwerken und Verteilnetzbetreibern weit verbreitet, oft noch mit altem Firmware-Stand. Wer im Fernwirknetz ist, könnte Firmware manipulieren, Stationen steuern oder unberechtigte Reboots auslösen. Das betrifft direkt die Versorgung.

Empfehlung: Im Asset-Inventar alle RTU500 mit ihrem Firmware-Stand erfassen und die Geräte mit Version 11.x oder älter priorisiert und mit dem Hersteller auf 12.7.8 oder 13.9.1 migrieren. Bis dahin per Segmentierung UDP 17185, die Web-Endpunkte sowie die Engineering- und Debug-Schnittstellen sperren und den Zugriff nur aus der Leitstelle zulassen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-279-06> ✓ geprüft

L-05 Warlock-Ransomware (Longlegs/Storm-2603) trifft Wasserversorger über on-prem SharePoint

HOCH Symantec Threat Intelligence (Broadcom), bestätigt durch BleepingComputer/SecurityWeek/The Record (weitere Quelle: <https://www.bleepingcomputer.com/news/security/warlock-ransomware-breach-sharepoint-in-water-telecom-operator-attacks/>), 01.10.

Was ist neu: Der China-nahe Threat Actor Storm-2603 (Longlegs) hat in rund zwei Monaten mindestens vier Organisationen angegriffen, darunter einen Wasserversorger, einen Telekom-Anbieter und Behörden. Die Opfer liegen laut Symantec in portugiesisch- und spanischsprachigen Ländern in Europa, Afrika und Lateinamerika. Zum Arsenal der Gruppe zählt Symantec die ToolShell-Kette in on-premises SharePoint (CVE-2025-49704, -49706, -53770, -53771). Danach folgten Webshells und VS-Code-Tunnel als versteckter Remote Access. Den Endpoint-Schutz schalten die Angreifer per BYOVD ab, in anderen Angriffen mit dem K7RKScan-Treiber (CVE-2025-1055); im ausführlich beschriebenen Fall ist der Treiber unbekannt. Dort verteilten sie ihr Störwerkzeug in etwa zwei Stunden auf mindestens 40 Hosts, Warlock wurde auf mindestens 33 Hosts gefunden. Zwischen der ersten Aktivität (22.07.) und der Ransomware-Phase (31.07.) lagen etwa neun Tage.

Bedeutung: Das ist ein Musterfall für Ransomware über die IT: Ein vergessener oder ungepatchter SharePoint-Server im Büronetz reicht als Einstieg. Wer nicht segmentiert hat, riskiert Lateral Movement und eine Verschlüsselung über die Domäne bis zu HMI und Engineering-Stationen.

Empfehlung: On-prem SharePoint auf den aktuellen Stand bringen (inkl. der Patches von 2025) oder vom Internet nehmen und im Verzeichnis LAYOUTS nach Webshells suchen. Ausgehende Tunnel (z. B. VS Code, devtunnels) überwachen bzw. blockieren. Prüfen, ob OT-Systeme in derselben AD-Domäne hängen, und falls ja, eine Trennung planen. Einen Incident-Response-Plan für den Fall 'Domäne verschlüsselt, OT im Handbetrieb' üben.

Quelle: <https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure> ✓ geprüft

L-06 Datenleck beim Zertifizierer GUTcert: Netzpläne und Audit-Berichte deutscher Energieversorger betroffen

HOCH IT-Administrator / energate messenger / GUTcert, 06.10.

Was ist neu: Angreifer waren ab 05.09. in den Systemen der GUTcert GmbH und haben rund 640 GB gestohlen. Darunter sind Anlagenlisten, Netzstrukturpläne mit IT/OT-Infrastruktur und Audit-Berichte mit Schwachstellen. Die Erpressungsversuche wurden abgelehnt. Entega hat seine Betroffenheit gemeldet. Eine Veröffentlichung der Daten ist noch nicht belegt.

Bedeutung: Audit-Befunde und Netzpläne sind für Angreifer eine fertige Zielplanung. Das betrifft Netzbetreiber, die nach IT-Sicherheitskatalog 1a/1b zertifiziert wurden, auch wenn ihre eigenen Systeme nicht kompromittiert sind.

Empfehlung: Beim Zertifizierer klären, welche Unterlagen dort vorliegen. Die dort dokumentierten Schwachstellen vorrangig schließen und künftig weniger Daten an Auditoren weitergeben.

Quelle: <https://www.it-administrator.de/datenleck-gutcert-kritische-infrastruktur-energienetz> ✓ geprüft

L-07 Feldebene: Moxa MGate (CVE-2026-86325) und KEB COMBIVIS/CODESYS (VDE-2026-105) mit kritischen Lücken

MITTEL Moxa MPSA-269540 (über SecurityOnline: <https://securityonline.info/moxa-mgate-vulnerabilities/>) / CERT@VDE VDE-2026-105, 08.10.

Was ist neu: In den Modbus-Gateways MGate MB3170/MB3270 bis Firmware 4.7 reicht ein Konto mit Leserechten für einen Stack Overflow (CVSS4 9,4). Bei der KEB COMBIVIS Control Runtime (CODESYS 3.5.21.10) lassen sich PKI-Zertifikate und Schlüssel lesen und überschreiben, dazu kommen DoS-Lücken. Behoben ist das in Version 2.1.0.

Bedeutung: Beide Produktgruppen sind in der Wasser- und Abwassertechnik in DACH verbreitet. CODESYS-Lücken tauchen bei immer mehr OEMs auf, nicht nur bei WAGO.

Empfehlung: Das Asset-Inventar nach MGate und CODESYS-basierten Runtimes durchsuchen und die Firmware aktualisieren. Standard- und Lesekonten bereinigen und die Webverwaltung nur aus dem Engineering-Netz erlauben.

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

L-08 Neue ICS-Advisories 08.10.: openPDC/openHistorian (Energie) und Red Lion N-Tron 700

MITTEL CISA ICS Advisories ICSA-26-281-01 (Red Lion N-Tron 700) / ICSA-26-281-02 (openPDC/openHistorian, <https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-02>), 08.10.

Was ist neu: Für openPDC und openHistorian nennt die CISA eine Deserialisierung mit Remote Code Execution (CVE-2026-100730, CVSS 9,8) und feste Admin-Zugangsdaten im Docker-Image (CVSS 9,8, kein Fix geplant). Dazu kommen Datenpublisher, die in der Standardkonfiguration ohne Anmeldung erreichbar sind. Bei den Red Lion N-Tron-700-Switches lassen sich über SNMP ohne Anmeldung Konfiguration und Firmware tauschen, und die Zugangsdaten liegen im Klartext. Behoben ist das in Firmware 3.11.1. Eine Ausnutzung ist bei beiden nicht bekannt.

Bedeutung: openPDC/openHistorian wird für Synchrophasor- und Messdaten im Netzbetrieb eingesetzt, N-Tron-Switches dienen als Industrial Ethernet in Anlagen. Über beide kann ein Angreifer die Netztopologie auslesen oder die Kommunikation stören. Bei openPDC gilt die neue Bindung nur an localhost lediglich für Neuinstallationen.

Empfehlung: Den Bestand prüfen und auf openPDC 2.9.482, openHistorian 2.8.585 bzw. N-Tron-Firmware 3.11.1 aktualisieren.

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

Fragen für das nächste Jour fixe

1. Welche Remote-Access-Gateways (NetScaler, FortiGate, SMA1000) nutzen wir oder unsere Dienstleister? Sind sie auf aktuellem Stand und auf Kompromittierung geprüft?
2. Läuft unsere Standortvernetzung über Cisco SD-WAN, und ist der Manager nur aus einem Management-Netz erreichbar?
3. Welche RTU500-, MGate-, CODESYS-, openPDC- und N-Tron-Geräte haben wir mit welchem Firmware-Stand im Asset-Inventar?
4. Welche Netzpläne und Audit-Berichte liegen bei Zertifizierern und Dienstleistern, und wie schnell schließen wir die darin dokumentierten Befunde?
5. Würden wir Lateral Movement von SharePoint oder dem Büronetz Richtung Leittechnik heute erkennen, und hängen OT-Systeme in derselben AD-Domäne?

Maßnahmen dieser Woche

1. NetScaler mit SAML-Konfiguration auf 14.1-73.41 bzw. 13.1-64.28 patchen, auf Webshells, neue Konten und Sessions prüfen und die Session-Tokens invalidieren.
2. Cisco SD-WAN Manager aktualisieren und die Logs nach `/%6a_security_check` durchsuchen.
3. FortiGate- und FortiMail-Admin-Oberflächen aus dem Internet nehmen, VPN- und Admin-Passwörter zurücksetzen, phishing-resistente MFA erzwingen und die Konten prüfen.
4. FortiMail auf 8.0.2, 7.6.7 bzw. 7.4.9 aktualisieren, den Zweig 7.2 migrieren und nach IOCs wie dem Konto 'archive234' suchen.
5. On-prem SharePoint patchen oder vom Internet nehmen, LAYOUTS nach Webshells durchsuchen und ausgehende VS-Code-Tunnel blockieren.
6. RTU500 mit CMU-Firmware 11.x oder älter inventarisieren, das Upgrade auf 12.7.8 oder 13.9.1 planen und bis dahin UDP 17185 sowie die Web-Endpunkte sperren.

7. Asset-Inventar nach Moxa MGate, CODESYS-Runtimes, openPDC/openHistorian und N-Tron-Switches durchsuchen und die Firmware aktualisieren.

8. Beim Zertifizierer die Betroffenheit durch das GUTcert-Leck klären und die dort dokumentierten Schwachstellen vorrangig schließen.

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 09.10.2026 automatisch aufgerufen und inhaltlich geprüft. 1 Meldung(en) ohne überprüfbare Originalquelle wurden nicht aufgenommen.