

**WOCHENBERICHT**

# OT-/Cyber-Lagebild Gesamt

Ausgabe KW 40/2026 · Gesamt – alle OT-Branchen in DACH

|                         |                                                                |
|-------------------------|----------------------------------------------------------------|
| <b>Zielgruppe</b>       | Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH |
| <b>Berichtszeitraum</b> | 25.09.2026-02.10.2026                                          |
| <b>Version</b>          | 1.0                                                            |
| <b>Datum</b>            | 02.10.2026                                                     |
| <b>Autor</b>            | Maximilian Gilg, OT-Cyber.de                                   |
| <b>Klassifizierung</b>  | TLP:CLEAR – ausschließlich öffentliche Quellen                 |

Dieser Bericht fasst öffentlich zugängliche Meldungen zusammen. Die Einstufung der Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH in Deutschland, Österreich und der Schweiz.

## Management Summary

In KW 40/2026 kamen die größten Risiken für OT-Betreiber in DACH wieder über Edge-Geräte im Remote Access und in der Standortvernetzung. Bei Citrix NetScaler ADC/Gateway werden zwei Zero-Days mit Remote Code Execution ohne Anmeldung aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772, CVSS v4.0 9.5). Laut Unit 42 wurde schon ab dem 21.08. gezielt nach verwundbaren Systemen gesucht, ab dem 04.09. wurden die Lücken bereits vor der Veröffentlichung ausgenutzt. Laut Fachpresse wurden die Lücken wochenlang vor dem Patch ausgenutzt, auch mit Webshells. CISA führt beide seit dem 27.09. im KEV-Katalog, das BSI warnt seit 28.09. mit Stufe 3 von 4 (<https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>). Seit dem 30.09. kommt ein ebenfalls aktiv ausgenutzter Zero-Day im Cisco Catalyst SD-WAN Manager hinzu (CVE-2026-76504, CVSS v3.1 9.8). Damit lässt sich die Anmeldung umgehen, und einen Workaround gibt es nicht (<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>). Beide Produkte sind in Stadtwerken, Netzbetrieben und der Industrie typische Zugänge für Fernwartung und die Anbindung von Standorten. Wer sie übernimmt, kommt also bis vor die Leittechnik.

Dazu kommen Advisories für Gateways an Außenstationen: das LTE-Gateway Lantronix G520 (Root-Codeausführung über das Update, CVSS v3.1 7.5) sowie kritische Lücken in MikroTik RouterOS (CVSS v3.1 9.8, ohne Anmeldung) und WatchGuard Access Points (CVSS 9.3). Für Engineering-Arbeitsplätze in der Schutztechnik gibt es außerdem ein Advisory zu ABB PCM600. Ransomware erreichte im August laut NCC Group mit 1.073 Angriffen den Höchststand des Jahres, 31 % trafen die Industrie, die aktivste Gruppe war Qilin (<https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of-august/>). Die Stadt Wien hat am 30.09. einen Abfluss von rund 26.000 internen Dokumenten öffentlich gemacht. Laut ORF wurde die Lücke vermutlich per KI-Scan gefunden (<https://wien.orf.at/stories/3373234/>).

Auch die Regulierung zieht an: In Österreich gilt seit dem 01.10. das NISG 2026, mit Meldepflichten, Registrierung bis 31.12.2026 und einer Aufsichts- und Schulungspflicht der Geschäftsleitung (§ 31 NISG). Seit dem 11.09. gelten die CRA-Meldepflichten für Hersteller. In der Schweiz ist der BACS-Fachbericht zur Cyberresilienz von Störfallbetrieben (28.09.) erschienen. Vorrang haben CC4 Secure Remote Access und CC5 Risk-Based Vulnerability Management, unterstützt durch CC1 ICS Incident Response. Dabei gilt: erst nach Kompromittierung suchen, dann patchen.

### GESAMTBEWERTUNG

Die Lage ist hoch, weil zwei Zero-Days in verbreiteten Fernzugangs- und WAN-Systemen bereits aktiv ausgenutzt werden. Sie treffen genau die Gateways, über die Dienstleister, Leitstellen und Standorte in die OT kommen. Vorrang haben in dieser Woche NetScaler und SD-WAN Manager: nach Kompromittierung suchen, patchen bzw. abschalten und Sessions und Zugangsdaten erneuern. Danach folgen die Gateways an Außenstationen.

## Trends

- Angreifer nutzen gezielt Edge-Geräte für Remote Access und WAN (NetScaler, SD-WAN, VPN-Gateways) als Einstieg. Oft suchen sie wochenlang nach verwundbaren Systemen und nutzen die Lücken schon aus, bevor sie bekannt werden. Beim Cisco SD-WAN ist es laut BleepingComputer der fünfte ausgenutzte Zero-Day seit Jahresbeginn.

- Gateways an Außenstationen (LTE-Router, MikroTik, WLAN-APs) häufen sich in den CISA-Advisories, sind aber im Asset-Inventar vieler Betreiber kaum erfasst.
- Laut Holm Security (29.09.) ist die typische ungepatchte kritische Lücke in SCADA- und Industrieumgebungen seit mehr als drei Jahren öffentlich bekannt. Gepatcht werden muss also nach Risiko, nicht vollständig.
- Ransomware bleibt auf Rekordniveau, Qilin ist am aktivsten. Wer vorbereitet ist, kann die OT bei einem Angriff auf die IT weiterbetreiben. Leaks wie in Berlin zeigen, dass KRITIS-Unterlagen bei Dritten zum Risiko werden.
- KI-gestütztes Scannen findet Lücken in Randanwendungen wie Doku-Plattformen und Wikis schneller (Stadt Wien, dort laut ORF vermutlich per KI-Scan).
- Die Regulierung zieht in DACH an: Österreich hat mit dem NISG 2026 nachgezogen, seit dem 11.09. gelten die CRA-Meldepflichten für Hersteller, und in der Schweiz ist der BACS-Fachbericht zur Cyberresilienz von Störfallbetrieben (28.09.) erschienen. In Deutschland führt das BSI eine Personenzertifizierung für KRITIS-Prüfer ein.

## Lageübersicht

| ID   | Meldung                                                                                                                         | Relevanz | Quelle                                                        |
|------|---------------------------------------------------------------------------------------------------------------------------------|----------|---------------------------------------------------------------|
| L-01 | Citrix NetScaler ADC/Gateway: zwei Zero-Days mit Remote Code Execution werden aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772) | KRITISCH | CISA / BSI / Citrix / Unit 42, 27.09.                         |
| L-02 | Cisco Catalyst SD-WAN Manager: aktiv ausgenutzter Zero-Day gibt Admin-Rechte ohne Anmeldung (CVE-2026-76504, CVSS 9.8)          | KRITISCH | Cisco PSIRT / CISA / Rapid7, 30.09.                           |
| L-03 | Lantronix G520 LTE-Gateway: Root-Codeausführung über unsicheres Firmware-Update (ICSA-26-272-01)                                | HOCH     | CISA ICS Advisory ICSA-26-272-01, 29.09.                      |
| L-04 | MikroTik RouterOS: Codeausführung ohne Anmeldung (CVE-2026-84411, CVSS v3.1 9.8, ICSA-26-272-06)                                | HOCH     | CISA ICS Advisory ICSA-26-272-06, 29.09.                      |
| L-05 | Ransomware erreicht im August 2026 den Jahreshöchststand, 31 % der Angriffe treffen die Industrie                               | HOCH     | NCC Group Monthly Threat Pulse (via Industrial Cyber), 28.09. |
| L-06 | Österreich: NISG 2026 seit 01.10. in Kraft – Registrierung bis 31.12.2026                                                       | HOCH     | Börse Express / WKO, 01.10.                                   |
| L-07 | Stadt Wien: rund 26.000 interne Dokumente abgeflossen, Lücke laut ORF vermutlich per KI-Scan gefunden                           | MITTEL   | ORF Wien / Stadt Wien, 30.09.                                 |
| L-08 | WatchGuard Access Points: Command Injection ohne Anmeldung (CVE-2026-86102, CVSS 9.3)                                           | MITTEL   | SecurityOnline / WatchGuard, 28.09.                           |
| L-09 | ABB PCM600 (Schutz- und Leittechnik): Rechteauserweiterung und Path Traversal (ICSA-26-274-03)                                  | MITTEL   | CISA ICS Advisory, 01.10.                                     |

## Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 02.10.2026):

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       | 137008 | DNP3: 33014, OMRON FINS: 23241, ProConOS: 16152 |
| Österreich        | 4567   | HMI/VNC: 1082, DNP3: 964, IEC-104: 450          |
| Bayern (München)  | 1324   | OMRON FINS: 675, HMI/VNC: 203, DNP3: 173        |
| Salzburg          | 29     | HMI/VNC: 8, DNP3: 6, BACnet: 5                  |
| Tirol (Innsbruck) | 42     | HMI/VNC: 13, DNP3: 6, Niagara Fox: 6            |

## Meldungen im Detail

### L-01 Citrix NetScaler ADC/Gateway: zwei Zero-Days mit Remote Code Execution werden aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772)

KRITISCH CISA / BSI / Citrix / Unit 42, 27.09.

Was ist neu: Citrix hat ein Advisory zu acht Lücken in NetScaler ADC und Gateway veröffentlicht (CVE-2026-88771 bis -88778). Zwei davon erlauben Remote Code Execution ohne Anmeldung (CVSS v4.0 9.5), auch in der Standardkonfiguration. Laut Unit 42 wurde schon ab dem 21.08. nach verwundbaren Systemen gesucht, ab dem 04.09. wurden die Lücken bereits vor der Veröffentlichung ausgenutzt. CISA bestätigt die weltweite aktive Ausnutzung und hat beide CVEs am 27.09. in den KEV-Katalog aufgenommen. Das BSI warnt seit 28.09. mit Stufe 3 von 4 (orange). Die CISA-Meldung stammt vom 27.09., am 28.09. folgte nur eine Überarbeitung.

Bedeutung: NetScaler ist bei Stadtwerken, Versorgern und in der Industrie oft das zentrale VPN- bzw. Remote-Access-Gateway für Fernwartung und Leitstellen. Ein übernommenes Gateway steht direkt vor der Segmentierung zur OT und ist der Einstieg für Lateral Movement. Weil die Lücken wochenlang vor dem Patch ausgenutzt wurden, entfernt das Patchen allein keine Backdoor oder Webshell, die schon eingerichtet wurde.

Empfehlung: Nach dem Hinweis von CISA zuerst Logs und Snapshots sichern und nach IoCs suchen (u. a. von Unit 42). Dann sofort auf die gepatchten Versionen laut Citrix-Bulletin CTX697096 aktualisieren (u. a. 14.1-73.37 bzw. 13.1-64.23). Danach alle Sessions beenden, die über das Gateway genutzten Zugangsdaten rotieren, nach Webshells und ungeklärten Lücken in der Protokollierung suchen. Gibt es Hinweise auf eine Kompromittierung, die Meldepflicht nach NIS2/BSIG prüfen (CC4, CC1).

Quelle: <https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netScaler-adc-gateway> ✓ geprüft

## **L-02 Cisco Catalyst SD-WAN Manager: aktiv ausgenutzter Zero-Day gibt Admin-Rechte ohne Anmeldung (CVE-2026-76504, CVSS 9.8)**

KRITISCH Cisco PSIRT / CISA / Rapid7, 30.09.

Was ist neu: Mit einer URI-kodierten Anfrage (``/%6a_security_check``, also ``%6a`` statt ``j`` in ``j_security_check``) umgehen Angreifer die API-Anmeldung und bekommen Admin-Rechte. Die Lücke wird seit September ausgenutzt und betrifft alle Konfigurationen, auch Systeme, die schon gegen die SD-WAN-Lücken aus Mai und Juni gepatcht sind. CISA hat sie am 30.09. in den KEV-Katalog aufgenommen. Einen Workaround gibt es nicht. Gefixt sind u. a. 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 den SD-WAN Manager kontrolliert, kann Routing und Segmentierung zwischen Leitstelle, Außenstellen und OT-Netzen umbauen. Für Netzbetreiber und Stadtwerke, die Netzleittechnik oder Außenstellen per SD-WAN anbinden, ist das ein Risiko für den Betrieb. Laut BleepingComputer ist es der fünfte ausgenutzte SD-WAN-Zero-Day seit Jahresbeginn. Diese Produktlinie sollte also als Hochrisiko-Asset gelten.

Empfehlung: Sofort patchen und den Manager nur aus einem Admin-Netz erreichbar machen. Danach ``/var/log/nms/containers/service-proxy/serviceproxy-access.log`` und `vmanage-server.log` nach ``j_security_check``-Anfragen mit ``%6a`` und nach Zugriffen auf ``viptela-reserved``-Konten durchsuchen. Bei Treffern Incident Response starten und die SD-WAN-Konfiguration gegen eine bekannte gute Version auf ungeplante Änderungen am Routing prüfen (CC2, CC3, CC1).

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

## **L-03 Lantronix G520 LTE-Gateway: Root-Codeausführung über unsicheres Firmware-Update (ICSA-26-272-01)**

HOCH CISA ICS Advisory ICSA-26-272-01, 29.09.

Was ist neu: Zwei Lücken betreffen Firmware 2.6.0.4R6 (CVE-2026-84409, CVE-2026-91191, je CVSS v3.1 7.5 / v4 7.7). Die Update-Metadaten kommen unverschlüsselt über HTTP, die Signaturprüfung ist deaktiviert, und der produktive private Schlüssel, dem die Firmware vertraut, liegt im öffentlichen SDK. Ein Angreifer kann so eigene Software mit Root-Rechten einspielen. CISA nennt Energie sowie Wasser und Abwasser als betroffene Sektoren. Ausgenutzt wird bisher nichts.

Bedeutung: Mit diesen LTE-Gateways ist Fernwirktechnik in der Fläche angebunden, oft unbeaufsichtigt. Wer sie übernimmt, kann die Kommunikation zu Außenstationen manipulieren oder das Gateway als dauerhaften Brückenkopf ins Leit- und Fernwirknetz nutzen.

Empfehlung: Alle G520 im Asset-Inventar erfassen, nach Kritikalität der Station priorisieren und auf 2.6.0.7R6 aktualisieren. Firmware-Updates nur über einen geprüften Pfad aus vertrauenswürdiger Quelle einspielen, nicht direkt aus dem Internet. Das Management-Interface nur aus einem eigenen Management-Netz erreichbar machen (CC5).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-272-01> ✓ geprüft

## **L-04 MikroTik RouterOS: Codeausführung ohne Anmeldung (CVE-2026-84411, CVSS v3.1 9.8, ICSA-26-272-06)**

**HOCH** CISA ICS Advisory ICSA-26-272-06, 29.09.

Was ist neu: Ein Integer-Underflow im Web-Management erlaubt mit einer einzigen Anfrage ohne Anmeldung Root-Codeausführung oder das Lahmlegen des Geräts (CVSS v3.1 9.8, v4: 9.3). Betroffen sind alle Versionen unter 7.24. Laut CISA wird die Lücke bisher nicht ausgenutzt.

Bedeutung: MikroTik-Lücken werden erfahrungsgemäß schnell angegriffen und für Botnetze genutzt. Die günstigen Router stehen oft ohne zentrale Verwaltung an Außenstellen der Wasser- und Energieversorgung und fehlen im Asset-Inventar. Ein übernommener Router ist ein dauerhafter Brückenkopf ins Fernwirknetz.

Empfehlung: Das Web-Management nur aus dem Admin-Netz erreichbar machen und auf 7.24 oder neuer aktualisieren. Geräte, die nicht im Inventar stehen, per Netzwerk-Scan finden und nach Kritikalität der Station priorisieren (CC5).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-272-06> ✓ geprüft

## **L-05 Ransomware erreicht im August 2026 den Jahreshöchststand, 31 % der Angriffe treffen die Industrie**

**HOCH** NCC Group Monthly Threat Pulse (via Industrial Cyber), 28.09.

Was ist neu: Laut NCC Group gab es im August 2026 weltweit 1.073 Ransomware-Angriffe, 12 % mehr als im Juli (960). Die Industrie war mit 31 % der Angriffe der meistgetroffene Sektor. Qilin war mit 15 % der Fälle die aktivste Gruppe, vor The Gentlemen. Auf Europa entfielen 26 % der Angriffe.

Bedeutung: Ransomware trifft die OT meist indirekt: Die IT fällt aus, die Leittechnik wird vorsorglich getrennt oder Planungsdaten sind weg. Ein Beispiel ist der Angriff auf die Stadtwerke Landsberg (verschlüsselt am 01.09.), bei dem die Versorgung laut Berichten dank der Trennung von IT und OT weiterlief. Das Rhysida-Leak aus dem Berliner Landesnetz (Veröffentlichung am 04.09.) hat Risikoanalysen zu Anlagen der Wasserversorgung und KRITIS-Notfallpapiere öffentlich gemacht.

Empfehlung: Prüfen, ob sich die Anlagen bei verschlüsselter IT sicher im Inselbetrieb fahren lassen, und das im Rahmen eines OT-spezifischen Incident-Response-Plans üben.

Offline-Backups von Projektierung und Konfiguration testen. Auch prüfen, wo Dokumente zu OT und Sicherheit außerhalb der eigenen geschützten Ablage liegen, etwa bei Behörden oder Dienstleistern (CC1, CC2).

Quelle: <https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of-august/> ✓ geprüft

## **L-06 Österreich: NISG 2026 seit 01.10. in Kraft - Registrierung bis 31.12.2026**

**HOCH** Börse Express / WKO, 01.10.

Was ist neu: Österreich setzt NIS2 mit dem NISG 2026 um. Es betrifft Unternehmen ab 50 Beschäftigten oder über 10 Mio. € Umsatz und über 10 Mio. € Bilanzsumme in 18 Sektoren. Erhebliche Sicherheitsvorfälle müssen innerhalb von 24 bis 72 Stunden an das zuständige CSIRT gemeldet werden. Registrierung bis 31.12.2026, Selbstdokumentation bis 30.09.2027.

Bedeutung: Für Betreiber und Zulieferer in Österreich wird OT-Sicherheit damit zur Aufgabe der Geschäftsleitung: Sie hat eine Aufsichts- und Schulungspflicht (§ 31 NISG), eine persönliche Haftung ergibt sich aus GmbHG/AktG. Auch deutsche und Schweizer Unternehmen mit österreichischen Standorten oder Kunden sind betroffen.

Empfehlung: Betroffenheit je Gesellschaft prüfen und die Registrierung planen. Meldewege mit 24-Stunden-Frist in den Incident-Response-Plan aufnehmen und einmal durchspielen (CC1).

Quelle: <https://www.boerse-express.com/news/articles/nis-2-umsetzung-oesterreich-schaerft-cybersicherheit-ab-oktober-937040> ✓ geprüft

## **L-07 Stadt Wien: rund 26.000 interne Dokumente abgeflossen, Lücke laut ORF vermutlich per KI-Scan gefunden**

**MITTEL** ORF Wien / Stadt Wien, 30.09.

Was ist neu: Zwischen 03. und 11.09. hat ein Angreifer über einen Webzugang auf eine interne Dokumentationsplattform des Magistrats zugegriffen und rund 26.000 Dokumente (ca. 9 GB) kopiert. Betroffen sind 5.824 Personen. Laut Bericht waren auch Geschäfts- und Infrastrukturinformationen dabei. CERT.at meldete am 09.09. ein Angebot zu der Schwachstelle in einem Online-Forum. Laut ORF wurde die Lücke vermutlich per KI-Scan gefunden. Phishing schließen die Behörden aus.

Bedeutung: Laut Stadt gab es keine Kontrolle über Systeme und keine Erpressung. Der Fall zeigt aber, dass Lücken in Randanwendungen wie Wikis oder Projektablagen schnell gefunden werden, laut ORF hier vermutlich per KI-gestütztem Scannen. Gerade dort liegen bei Versorgern oft Netzpläne, Anlagendokumentationen und Zugangsinformationen zur OT.

Empfehlung: Die externe Angriffsfläche einschließlich der Doku-Plattformen erfassen und prüfen. OT-Dokumentation (Netzpläne, IP-Listen, Zugangsdaten) nur in geschützten, protokollierten Ablagen führen.

Quelle: <https://wien.orf.at/stories/3373234/> ✓ geprüft

## L-08 WatchGuard Access Points: Command Injection ohne Anmeldung (CVE-2026-86102, CVSS 9.3)

MITTEL SecurityOnline / WatchGuard, 28.09.

Was ist neu: WatchGuard hat drei Lücken in der AP-Firmware 1.0 bis 3.4.7 veröffentlicht, darunter Command Injection in der internen Management-API (CVE-2026-86102) und ein Auth-Bypass (CVE-2026-101891). Ausgenutzt werden sie laut Hersteller bisher nicht.

Bedeutung: WatchGuard ist bei Stadtwerken und Zweckverbänden verbreitet. WLAN-APs in Betriebsgebäuden hängen oft im selben Netz wie Bedienstationen. Ein übernommener AP ermöglicht dann Lateral Movement in die OT.

Empfehlung: Auf 3.4.8 aktualisieren und die Management-Schnittstellen vom OT-Netz trennen. Prüfen, ob WLAN im OT-Bereich überhaupt nötig ist (CC2).

Quelle: <https://securityonline.info/watchguard-ap-vulnerabilities-patch/> ✓ geprüft

## L-09 ABB PCM600 (Schutz- und Leittechnik): Rechteausweitung und Path Traversal (ICSA-26-274-03)

MITTEL CISA ICS Advisory, 01.10.

Was ist neu: In ABB PCM600 bis Version 2.14 läuft der Scheduler-Dienst als LocalSystem und gibt Standardnutzern zu weitgehende Rechte (CVE-2026-15952). Dazu kommt ein Path Traversal beim Entpacken von Archiven (CVE-2026-15953). Der Schweregrad ist mittel bis hoch (bis 7.1 nach CVSS v4). Ausgenutzt wird bisher nichts. CISA nennt als Sektor Energie mit weltweitem Einsatz. Am selben Tag hat CISA unter anderem auch Advisories zu Johnson Controls EasyIO-Gebäudereglern veröffentlicht (CVE-2026-64892, niedrig).

Bedeutung: PCM600 wird zum Parametrieren von Schutzgeräten im Energiesektor genutzt. Lücken auf diesen Engineering-Arbeitsplätzen betreffen damit unmittelbar die Schutz- und Leittechnik.

Empfehlung: PCM600-Installationen  $\leq 2.14$  erfassen, den Scheduler-Dienst unter dem PCM600-Konto statt als LocalSystem betreiben und die IED-Authentifizierung aktivieren (CC5).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-03> ✓ geprüft

## Fragen für das nächste Jour fixe

1. Setzen wir oder unsere Dienstleister Citrix NetScaler oder Cisco SD-WAN ein, sind die Systeme gepatcht, und hat jemand nach Spuren einer Kompromittierung gesucht?
2. Welche LTE-Gateways, MikroTik-Router und WLAN-APs stehen an unseren Außenstationen, und wer ist für ihre Updates zuständig?
3. Kann unsere Leittechnik mindestens 72 Stunden ohne IT weiterlaufen, und wann haben wir das zuletzt getestet?
4. Wo liegen Netzpläne, IP-Listen und Zugangsdaten zur OT, und ist die Ablage aus dem Internet erreichbar?
5. Falls Standorte in Österreich bestehen: Sind wir vom NISG 2026 betroffen, und wer übernimmt die Registrierung bis 31.12.?
6. Haben wir eine Liste der Fernwartungszugänge mit Verantwortlichen und Ablaufdatum?

## Maßnahmen dieser Woche

1. NetScaler ADC/Gateway: zuerst Forensik sichern und nach IoCs (u. a. Unit 42) und Webshells suchen, dann nach CTX697096 patchen, alle Sessions beenden und Zugangsdaten rotieren (CC4, CC1).
2. Cisco SD-WAN Manager auf eine gepatchte Version bringen und nur aus dem Admin-Netz erreichbar machen. Die Logs nach `%6a\_security\_check` und nach Zugriffen auf `viptela-reserved`-Konten durchsuchen, die Konfiguration gegen einen bekannten guten Stand prüfen (CC2/CC3).
3. Lantronix G520 auf 2.6.0.7R6 und MikroTik RouterOS auf  $\geq 7.24$  aktualisieren und das Web-Management vom Internet und vom OT-Netz trennen (CC5).
4. Bei Dienstleistern mit Fernwartung abfragen, ob ihre eigenen NetScaler-/SD-WAN-Zugänge gepatcht sind (CC4).
5. WatchGuard-APs in Betriebsgebäuden auf 3.4.8 aktualisieren und prüfen, ob WLAN im OT-Bereich nötig ist (CC2).
6. ABB PCM600  $\leq 2.14$  erfassen, den Scheduler-Dienst unter dem PCM600-Konto betreiben und die IED-Authentifizierung aktivieren (CC5).
7. Den Inselbetrieb der Leittechnik bei IT-Ausfall üben und Offline-Backups von Projektierung und Konfiguration testen (CC1).
8. Mit Standorten in Österreich: Betroffenheit nach NISG 2026 klären und eine Meldekette mit 24-Stunden-Frist festlegen (CC1).

#### **HINWEIS ZUR QUELLENLAGE**

Alle Quellenlinks wurden am 02.10.2026 automatisch aufgerufen und inhaltlich geprüft. Am 02.10.2026 zusätzlich per Doppel-Recherche faktengeprüft und korrigiert.