

WOCHENBERICHT

OT-/Cyber-Lagebild Maschinen- und Anlagenbau

Ausgabe KW 40/2026 · Maschinen- und Anlagenbau in DACH

Zielgruppe	Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren
Berichtszeitraum	25.09.2026-02.10.2026
Version	1.0
Datum	02.10.2026
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 40/2026 waren vor allem Edge-Geräte an der Grenze zwischen Internet und Unternehmensnetz das Ziel. Über genau diese Geräte leisten Maschinen- und Anlagenbauer Fernwartung oder verbinden ihre Standorte. In Citrix NetScaler ADC/Gateway werden zwei Zero-Days weltweit aktiv ausgenutzt (CVE-2026-88771/-88772, CISA 27.09.). Im Cisco Catalyst SD-WAN Manager wird eine Lücke ausgenutzt, über die Angreifer ohne Anmeldung Admin-Rechte bekommen (CVE-2026-76504, CVSS 9.8, KEV seit 30.09.). Für die Fernwartung sind außerdem wichtig: fünf Schwachstellen in TeamViewer (bis CVSS 8.8, Fix 15.82), eine Pre-Auth-RCE in MikroTik RouterOS (CVSS v3.1 9.8) und eine manipulierbare Firmware-Update-Kette im LTE-Gateway Lantronix G520. Solche Geräte stecken häufig in Fernwartungsboxen, Schaltschränken und auf Industrie-PCs ausgelieferter Anlagen. Laut Hersteller bzw. CISA werden TeamViewer, MikroTik und Lantronix bisher nicht ausgenutzt.

Der Druck durch Ransomware bleibt hoch: Laut NCC Group gab es im August 1.073 Angriffe, den Höchststand 2026. 31 % davon trafen die Industrie, Qilin war die aktivste Gruppe. Der Angriff auf Adif/Renfe zeigt, wie Angreifer über die Systeme eines verbundenen Partners eindringen. Seit dem 11.09.2026 gilt die Meldepflicht des Cyber Resilience Act. Wer ein betroffenes Gateway, einen Router oder TeamViewer in die eigene Maschine einbaut und darin eine aktiv ausgenutzte Schwachstelle feststellt, muss prüfen, ob eine 24-Stunden-Frühwarnung über die ENISA Single Reporting Platform fällig ist. Lantronix zeigt außerdem, was CRA und Maschinenverordnung (ab 20.01.2027) verhindern sollen: eine unsichere Update-Kette. Vorrang haben diese Woche drei Dinge: Remote Access absichern (CC4), Asset-Inventar und SBOM der verbauten Komponenten abgleichen (CC5) und den PSIRT-/CRA-Meldeprozess an einem echten Fall durchspielen (CC1).

GESAMTBEWERTUNG

Die Lage ist hoch: Zwei Plattformen für Remote Access und WAN (Citrix NetScaler, Cisco SD-WAN) werden aktiv ausgenutzt, und in weiteren Fernwartungs-Komponenten in Maschinen gibt es schwerwiegende Lücken, während die CRA-Meldepflicht bereits läuft. Zuerst kommen Patch und Kompromittierungsprüfung bei Citrix NetScaler und Cisco SD-WAN. Danach folgen die Fernwartungs-Werkzeuge (TeamViewer, MikroTik, LTE-Gateways) im eigenen Haus und in ausgelieferten Maschinen, inklusive Abgleich mit den aktuellen Advisories.

Trends

- Angreifer nutzen gezielt Edge-Geräte für Remote Access (SD-WAN, NetScaler, Router, LTE-Gateways), um in Produktionsnetze zu gelangen. Genau darüber laufen die Service-Zugänge der Maschinenbauer (CISA, 27.09./29.09./30.09.).
- Laut Holm Security (29.09.) bleiben kritische Schwachstellen in der OT typischerweise über drei Jahre offen. In der IT derselben Unternehmen gibt es oft zugleich Lücken, die Ransomware ausnutzt (<https://www.globenewswire.com/news-release/2026/09/29/3370430/0/en/three-years-and-counting-how-long-critical-vulnerabilities-survive-in-industrial-systems.html>).
- Seit dem 11.09. gilt die Meldepflicht des CRA (24 h / 72 h / 14 Tage über die Single Reporting Platform der ENISA). Aktiv ausgenutzte Schwachstellen in Fremdkomponenten (LTE-Gateways, Router, TeamViewer, OpenSSL) werden damit zum Meldefall für Hersteller, SBOM und Komponenten-Monitoring sind keine Kür mehr

(<https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>).

- Unsichere Update-Ketten wie bei Lantronix sind ein typisches Muster, das die Maschinenverordnung (Schutz gegen Korruption, ab 20.01.2027) und der CRA künftig ausschließen sollen.
- Bei den harmonisierten Normen bleibt es knapp: Die harmonisierte Norm zur Cybersecurity unter der Maschinenverordnung (prEN 50742, gilt ab 20.01.2027) fehlt weiterhin, deshalb müssen Hersteller die Anforderungen vorerst selbst begründen.
- Ransomware gegen die Industrie bleibt auf Rekordniveau, und Angriffe über verbundene Partner (Adif/Renfe) zeigen das Risiko in der Lieferkette. Mit KI-Unterstützung können auch kleine Teams Advisories schneller dem eigenen Asset-Inventar zuordnen. Deshalb lohnt der Fokus auf die fünf Critical Controls statt auf Einzellösungen.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Citrix NetScaler ADC/Gateway: zwei RCE-Zero-Days werden weltweit aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772, CVSS v4.0 9.5)	KRITISCH	Citrix / CISA / BSI, 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 KEV / Rapid7 / Help Net Security, 30.09.
L-03	Lantronix G520 LTE-Gateway: eingeschleuste Firmware mit Root-Rechten über manipulierbare Update-Kette (ICSA-26-272-01)	HOCH	CISA ICS Advisory, 29.09.
L-04	MikroTik RouterOS: Pre-Auth-RCE im Web-Management mit einer einzigen Anfrage (CVE-2026-84411, CVSS v3.1 9.8, ICSA-26-272-06)	HOCH	CISA ICS Advisory, 29.09.
L-05	TeamViewer: fünf Schwachstellen, darunter Umgehung der Session-Rechte (CVE-2026-92370, CVSS 8.8)	HOCH	TeamViewer Security Bulletin TV-2026-1010 / BleepingComputer, 29.09.
L-06	Ransomware auf Jahreshöchststand: 31 % der Angriffe treffen die Industrie	HOCH	Industrial Cyber / NCC Group Threat Pulse / Infosecurity Magazine, 28.09.
L-07	CRA-Meldepflicht läuft: ENISA Single Reporting Platform nur per Web-Oberfläche und auf Englisch	ORIENTIERUNG	ENISA / BSI / EU-Kommission / Help Net Security, 11.09.
L-08	Adif/Renfe: Bahnbetreiber über die kompromittierten Server eines verbundenen Partners angegriffen	ORIENTIERUNG	El Español / Telemadrid / The Cyber Express, 25.09.

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

Meldungen im Detail

L-01 Citrix NetScaler ADC/Gateway: zwei RCE-Zero-Days werden weltweit aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772, CVSS v4.0 9.5)

KRITISCH Citrix / CISA / BSI, 27.09.

Was ist neu: Citrix hat acht Schwachstellen in NetScaler ADC und Gateway veröffentlicht (CVE-2026-88771 bis -88778). Zwei davon erlauben jeweils für sich Remote Code Execution ohne Anmeldung und wurden schon vor der Veröffentlichung angegriffen. Beide stehen im KEV-Katalog der CISA. Laut CISA sollte man vor dem Patch nach Spuren einer Kompromittierung suchen und forensische Daten sichern, weil das Update Spuren zerstören kann. Das BSI warnt seit 28.09. mit Stufe 3 von 4.

Bedeutung: Viele Maschinenbauer und Integratoren nutzen NetScaler Gateway für den Service-Zugriff auf Kundenanlagen, für die eigenen Techniker oder für externe Dienstleister. Wer das Gateway übernimmt, bekommt Zugangsdaten und einen Ausgangspunkt für Lateral Movement in Fernwartungs-Sessions, Engineering- und Servicenetze und auf Jump Hosts mit Zugangsdaten zu Kundenanlagen. Ein solcher Vorfall trifft deshalb auch die Kunden.

Empfehlung: Vor dem Patch die IoCs prüfen und forensische Daten sichern. Danach die Builds aus Bulletin CTX697096 einspielen, alle aktiven Sessions beenden und die Zugangsdaten der Fernwartungs-Konten rotieren. Prüfen, welche Kundenanlagen über dieses Gateway erreichbar waren. Mittelfristig den Fernzugang zur OT über einen eigenen Jump Host mit MFA führen statt direkt über das Gateway (CC4).

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 KEV / Rapid7 / Help Net Security, 30.09.

Was ist neu: Weil eine URI-Kodierung falsch behandelt wird, lässt sich mit einer speziell kodierten URL (`/%6a\_security\_check`) die Anmeldung umgehen. Danach steht die API des Managers mit Admin-Rechten offen, unabhängig von der Konfiguration. Die Lücke wird seit September ausgenutzt. Sie betrifft auch Systeme, die gegen die SD-WAN-Lücken aus Mai und Juni gepatcht sind. Laut BleepingComputer ist sie der fünfte ausgenutzte SD-WAN-Zero-Day in diesem Jahr. Cisco hat sie am 30.09. veröffentlicht, CISA hat sie am selben Tag in den KEV-Katalog aufgenommen. Einen Workaround gibt es nicht. Gefixt sind 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: Hersteller mit mehreren Werken, Servicestandorten oder einem zentralen Remote-Service-Netz verbinden diese oft per SD-WAN. Wer den Manager übernimmt, kann Routing und Segmentierung zwischen Büro-IT, Fertigungsnetz und Service-Zugängen umbauen und so Wege in Produktions- und Servicenetze öffnen.

Empfehlung: Sofort auf eine gefixte Version gehen und den Manager nur für vertrauenswürdige Hosts erreichbar machen. Danach serviceproxy-access.log und vmanage-server.log nach Anfragen an `/%6a\_security\_check` durchsuchen und die Konfigurationsänderungen der letzten Wochen prüfen (CC2, CC5, CC1).

Quelle:

<https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog> ✓
geprüft

L-03 Lantronix G520 LTE-Gateway: eingeschleuste Firmware mit Root-Rechten über manipulierbare Update-Kette (ICSA-26-272-01)

HOCH CISA ICS Advisory, 29.09.

Was ist neu: Die Firmware 2.6.0.4R6_stable hat zwei Lücken (CVE-2026-84409, CVE-2026-91191). Die Bewertung liegt bei CVSS v3.1 7.5 bzw. CVSS v4 7.7. Das Gerät holt seine Update-Metadaten unverschlüsselt per HTTP, und die Signatur wird nicht wirksam geprüft. Berichten zufolge liegt der private Schlüssel, dem die Firmware vertraut, im öffentlichen SDK. Ein Angreifer kann so eigene Software mit Root-Rechten einspielen. Laut CISA sind Energie sowie Wasser und Abwasser betroffen, eine Ausnutzung ist bisher nicht bekannt. Lantronix hat die Fix-Version 2.6.0.7R6 am 18.09. veröffentlicht.

Bedeutung: Viele Maschinen werden über mitgelieferte LTE-Gateways aus der Ferne gewartet, ohne dass das Kundennetz beteiligt ist. Für den Maschinenbauer ist das eine verbaute Komponente mit Schwachstelle und damit ein Thema für die Lieferkette und das CRA-Schwachstellenmanagement. Der Fall zeigt typische Konstruktionsfehler, die CRA und Maschinenverordnung (Schutz gegen Korruption) künftig ausschließen sollen: eine unsichere Update-Kette und einen offengelegten Schlüssel.

Empfehlung: Im Asset-Inventar und in den SBOMs der Produkte nach G520 suchen, das Update auf 2.6.0.7R6 ausrollen und die Kunden mit einem Update-Hinweis informieren. Bei eigenen Produkten prüfen, ob Updates nur über TLS und mit verifizierter Signatur laufen. Lieferanten von Kommunikationsmodulen vertraglich zu signierten Updates und gesicherter Schlüsselverwaltung verpflichten (CC5, CC4).

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

L-04 MikroTik RouterOS: Pre-Auth-RCE im Web-Management mit einer einzigen Anfrage (CVE-2026-84411, CVSS v3.1 9.8, ICSA-26-272-06)

HOCH CISA ICS Advisory, 29.09.

Was ist neu: Ein Integer-Underflow beim Verarbeiten von HTTP-Anfragen im Web-Management erlaubt mit einer einzigen Anfrage ohne Anmeldung Codeausführung als root oder einen Denial of Service. Betroffen sind alle Versionen vor 7.24. CISA sind bisher keine Angriffe bekannt.

Bedeutung: MikroTik-Router sind günstig und werden deshalb oft als Router oder VPN-Endpunkt in Anlagen, selbst gebaute Fernwartungslösungen, Inbetriebnahme-Netze oder Prüfstände eingebaut. Damit sind sie Teil des eigenen Produkts und fallen unter die CRA-Pflichten zum Schwachstellenmanagement. MikroTik-Lücken werden erfahrungsgemäß schnell angegriffen. Sobald ein Exploit kursiert, wird ein verbautes Gerät zum CRA-Meldefall.

Empfehlung: Alle MikroTik-Geräte in Produkten, ausgelieferten Anlagen, Prüffeld und Service erfassen, auf 7.24 aktualisieren und das Web-Management nur aus dem Management-Netz erreichbar machen (CC5, CC2).

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

L-05 TeamViewer: fünf Schwachstellen, darunter Umgehung der Session-Rechte (CVE-2026-92370, CVSS 8.8)

HOCH TeamViewer Security Bulletin TV-2026-1010 / BleepingComputer, 29.09.

Was ist neu: TeamViewer hat fünf Schwachstellen in Remote, Tensor und ONE behoben. Mit CVE-2026-92370 kann ein entfernter Angreifer die eingestellten Session-Rechte umgehen, bis hin zu Remote Code Execution. Die übrigen Schwachstellen erlauben Rechteauserweiterung bis SYSTEM, und eine präparierte .tvs-Datei kann Code ausführen. Laut TeamViewer wird bisher nichts davon ausgenutzt.

Bedeutung: Im DACH-Maschinenbau läuft TeamViewer oft fest installiert auf Bedien-PCs und Industrie-PCs ausgelieferter Anlagen, und diese Installationen werden selten aktualisiert. Für Hersteller ist das zugleich eine Frage der Produkt-Security und der SBOM: Wer TeamViewer mitliefert, muss die Updates auch beim Kunden ermöglichen.

Empfehlung: Alle eigenen und mitgelieferten TeamViewer-Installationen im Asset-Inventar erfassen, auf 15.82 heben und Kunden mit Anlagen im Feld informieren. Mittelfristig die Fernwartung über ein zentrales, protokolliertes Gateway führen (CC4, CC5).

Quelle: <https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2026-1010/> ✓ geprüft

L-06 Ransomware auf Jahreshöchststand: 31 % der Angriffe treffen die Industrie

HOCH Industrial Cyber / NCC Group Threat Pulse / Infosecurity Magazine, 28.09.

Was ist neu: NCC Group zählt für August weltweit 1.073 Ransomware-Angriffe, 12 % mehr als im Juli (960) und so viele wie in keinem anderen Monat 2026. Der Anteil der Industrie stieg von 28 % auf 31 %. Qilin war mit 164 Fällen (15 %) die aktivste Gruppe. Auf Europa entfielen 26 % der Angriffe.

Bedeutung: Die Industrie, zu der der Maschinen- und Anlagenbau gehört, ist weiterhin das häufigste Ziel, und mittelständische Hersteller gehören zu den häufigsten Opfern. Meist kommen die Angreifer über die IT und Edge-Geräte. Fallen ERP, PDM oder die Software-Build-Umgebung aus, stehen Auslieferung, Service und oft auch die Produktion still. Kompromittierte Build-Systeme werden außerdem zum Lieferketten-Risiko für die Kunden.

Empfehlung: Offline-Backups von Konstruktionsdaten, Steuerungsprojekten und Build-Umgebung prüfen und eine Wiederherstellung testen. Fertigung und Inbetriebnahme-Netze von der Büro-IT segmentieren und prüfen, ob die OT bei einem IT-Ausfall getrennt weiterarbeiten kann. Einen ICS-spezifischen Incident-Response-Plan mit Wiederanlauf der Produktion als Tabletop üben (CC1, CC2).

Quelle: <https://industrialcyber.co/ransomware/ransomware-activity-hits-2026-high-as-industrial-sector-bears-31-of-attacks-and-qilin-dominates/> ✓ geprüft

L-07 CRA-Meldepflicht läuft: ENISA Single Reporting Platform nur per Web-Oberfläche und auf Englisch

ORIENTIERUNG ENISA / BSI / EU-Kommission / Help Net Security, 11.09.

Was ist neu: Seit dem 11.09.2026 müssen Hersteller aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle über die Single Reporting Platform der ENISA melden. Die Fristen: Frühwarnung in 24 Stunden, Meldung in 72 Stunden, Abschlussbericht nach 14 Tagen bzw. einem Monat. ENISA hat die Plattform erst am Morgen des Stichtags freigeschaltet, zunächst ohne API und nur auf Englisch.

Bedeutung: Die Pflicht gilt ausdrücklich auch für Maschinenbauer, Hersteller von Steuerungen und Sensoren sowie für Importeure vernetzter Geräte. Die Advisories dieser Woche (Lantronix, MikroTik, TeamViewer) zeigen, wie schnell eine verbaute Fremdkomponente zum Meldefall werden kann, sobald eine Ausnutzung bekannt wird.

Empfehlung: Prüfen, ob das Unternehmen in der SRP registriert ist (EU Login) und wer am Wochenende meldet. Den Ablauf von der Erkennung bis zur Frühwarnung einmal mit einem echten Advisory dieser Woche durchspielen (CC1).

Quelle: <https://www.enisa.europa.eu/news/the-cra-single-reporting-platform-is-launched> ✓ geprüft

L-08 Adif/Renfe: Bahnbetreiber über die kompromittierten Server eines verbundenen Partners angegriffen

ORIENTIERUNG El Español / Telemadrid / The Cyber Express, 25.09.

Was ist neu: Renfe meldet einen Angriff, der von bereits kompromittierten Servern des Infrastrukturbetreibers Adif ausging. Diese Server waren mit den Systemen von Renfe verbunden. Laut Medienberichten setzten die Angreifer KI für automatisiertes Scannen und Fuzzing ein. Abgeflossen sind vor allem Namen und E-Mail-Adressen von Kunden, Berichte nennen rund 500 GB Daten.

Bedeutung: Maschinenbauer sind über Serviceportale, Fernwartung und Datenaustausch eng mit Kunden und Zulieferern verbunden. Der Fall zeigt, dass ein kompromittierter Partner direkt zum Einfallstor werden kann.

Empfehlung: Verbindungen zu Partnern und Kunden in einer Netzübersicht erfassen und die Zugänge mit den geringsten nötigen Rechten und mit Monitoring absichern (CC2, CC3).

Quelle: https://www.lespanol.com/invertia/economia/macroeconomia/20260925/adif-sufre-ataque-sofisticado-ia-robado-informacion-accedido-proveedores/1003744397822_0.html ✓ geprüft

Fragen für das nächste Jour fixe

1. Über welche Gateways (NetScaler, SD-WAN, LTE-Boxen) laufen unsere Fernwartungszugänge zu Kunden, und sind alle auf dem aktuellen Stand?
2. Welche unserer ausgelieferten Maschinen enthalten Lantronix- oder MikroTik-Geräte oder TeamViewer-Installationen, und wie erreichen wir die Betreiber mit einem Update-Hinweis?
3. Wer meldet eine aktiv ausgenutzte Schwachstelle innerhalb von 24 Stunden an die ENISA-Plattform, auch am Wochenende?
4. Sind unsere Firmware-Updates durchgehend signiert und nur über TLS erreichbar, und wo liegen die Signierschlüssel?
5. Wie weit sind wir mit dem Nachweis zum Schutz gegen Korrumpierung für Maschinen, die ab dem 20.01.2027 in Verkehr gehen?

Maßnahmen dieser Woche

1. Citrix NetScaler: vor dem Patch auf Kompromittierung prüfen und Spuren sichern, dann die Builds aus CTX697096 einspielen, Sessions beenden und die Zugangsdaten der Fernwartungs-Konten rotieren.
2. Cisco SD-WAN Manager auf eine gefixte Version bringen, nur noch für vertrauenswürdige Hosts erreichbar machen und die Logs (serviceproxy-access.log, vmanage-server.log) nach /%6a_security_check durchsuchen.
3. Lantronix G520, MikroTik RouterOS und TeamViewer in Asset-Inventar und SBOMs suchen, auf 2.6.0.7R6, 7.24 bzw. 15.82 aktualisieren und die Kunden mit Anlagen im Feld informieren.
4. Registrierung bei der ENISA Single Reporting Platform prüfen und den 24-Stunden-Meldeablauf mit einem echten Advisory dieser Woche durchspielen.
5. Offline-Backups von Konstruktionsdaten, Steuerungsprojekten und Build-Umgebung prüfen, die Wiederherstellung testen und die Segmentierung zwischen IT und OT kontrollieren.

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.