

WOCHENBERICHT

OT-/Cyber-Lagebild Gesamt

Ausgabe KW 41/2026 · Gesamt – alle OT-Branchen in DACH

Zielgruppe	Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH
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 Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 41 kamen die größten Risiken für OT-Betreiber in DACH wieder über die Edge-Geräte und den Remote Access vor dem Leitnetz, nicht über die Steuerungen. Aktiv ausgenutzt wurden drei Lücken: Citrix NetScaler (SAML-Zero-Day CVE-2026-88779, laut Citrix Denial of Service), Cisco Catalyst SD-WAN Manager (Auth-Bypass CVE-2026-76504, CVSS 9,8) und FortiMail (CVE-2026-104286, CVSS 9,8; Fixes sind seit dem 05.10. gelistet). Die neue NetScaler-Lücke trifft auch Geräte, die erst kurz zuvor gegen CVE-2026-88771 bis -88778 gepatcht wurden. Dazu kommt die laufende FortiBleed-Kampagne: Angreifer melden sich mit gestohlenen Zugangsdaten an FortiGate-Firewalls und SSL-VPN an, sperren die Admins aus und verkaufen den Zugang an Ransomware-Gruppen. Patchen allein reicht deshalb nicht. Wer nicht auch nach einer Kompromittierung sucht, übersieht möglicherweise Webshells und Backdoors, die schon gesetzt sind.

Auf der Feldebene gab es kritische Advisories zu Hitachi Energy RTU500 (Fernwirktechnik, CMU-Firmware 11.x und älter, End-of-Life, bis CVSS 9,8) und Moxa MGate (Modbus-Gateways, CVSS 9,4). Dazu kommen zwei Advisories von CERT@VDE: Für den Murrelektronik aas-edge-client gibt es keinen Patch, und KEB COMBIVIS ist von CODESYS-Lücken betroffen. Für die deutsche Energiewirtschaft besonders wichtig ist das Datenleck beim Zertifizierer GUTcert. Rund 640 GB mit Anlagenlisten, Netzstrukturplänen und Audit-Befunden sind abgeflossen; ob die Daten veröffentlicht werden, ist noch nicht belegt. In Österreich gilt seit 01.10.2026 das NISG 2026. Einen bestätigten OT-Vorfall mit Auswirkung auf den Betrieb in DACH haben wir für diese Woche nicht gefunden. Unsere Kernbotschaft: Wer Secure Remote Access (CC4) und Risk-Based Vulnerability Management (CC5) im Griff hat, deckt den Großteil dieser Woche ab.

GESAMTBEWERTUNG

Die Lage ist hoch. Mehrere Lücken in Remote-Access- und Netz-Gateways werden gleichzeitig ausgenutzt, ein Initial Access Broker verkauft gezielt Zugänge über FortiGate, und Daten über die Netzstrukturen deutscher Versorger sind abgeflossen. Vorrang haben Patch und Kompromittierungsprüfung bei NetScaler, Cisco SD-WAN, FortiGate und FortiMail. Danach kommt die Bereinigung der OT-Asset-Inventare (RTU500, MGate, CODESYS, aas-edge-client).

Trends

- Edge-Geräte und Remote-Access-Gateways bleiben der wichtigste Initial-Access-Vektor: NetScaler, Cisco SD-WAN, FortiMail, FortiGate und SonicWall SMA1000 hatten in derselben Woche kritische oder ausgenutzte Lücken. Bei SMA1000 ist es CVE-2026-102255 mit CVSS 10, den Hotfix gab es laut Help Net Security am 06.10. (<https://www.helpnetsecurity.com/?p=387130>). Frisch gepatchte Geräte sind teils nach Tagen wieder verwundbar.
- Patchen allein reicht nicht mehr: Bei NetScaler trifft die neue Lücke auch frisch gepatchte Geräte, und bei FortiBleed kommen die Angreifer mit gültigen Zugangsdaten herein. Behörden verlangen ausdrücklich eine forensische Prüfung. Kompromittierungsprüfung und Konten-Hygiene werden zur Pflichtaufgabe.
- Das Lieferkettenrisiko verlagert sich zu Prüfern und Dienstleistern: Der GUTcert-Fall zeigt, dass Audit-Unterlagen Angreifern eine fertige Karte der Infrastruktur liefern.

- Lücken in Komponenten wie CODESYS, lwIP oder ActiveMQ ziehen sich durch viele OEM-Produkte. Ohne ein SBOM-gestütztes Asset-Inventar bleiben sie unsichtbar.
- Ransomware-Gruppen greifen Versorger über alte IT-Lücken an: Symantec beschrieb am 01.10., dass die Gruppe Longlegs/Storm-2603 unter anderem einen Wasserversorger angriff, ToolShell-Lücken in SharePoint gehören zu ihrem Arsenal. Im ausführlich beschriebenen Fall eines KRITIS-Betreibers vergingen bis zur Warlock-Ransomware etwa neun Tage (<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>).
- Bei Fernwirktechnik und Gateways bleiben End-of-Life-Firmware und schwache Konten das Grundproblem (RTU500 11.x mit CVE-2010-2965, Moxa MGate).
- Die Regulierung zieht an: In Österreich gilt seit 01.10.2026 das NISG 2026 mit gestuften Meldefristen von 24 h, 72 h und einem Monat (laut Beratungsquellen, z. B. <https://www.secjur.com/blog/nisg-2026>). Seit 11.09.2026 greifen zudem die Meldepflichten des CRA für Hersteller.

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./04.10.
L-02	Cisco Catalyst SD-WAN Manager: Auth-Bypass CVE-2026-76504 (CVSS 9,8) aktiv ausgenutzt	KRITISCH	Cisco PSIRT cisco-sa-sdwan-webauth-xr8beuuU / CISA KEV / Help Net Security, 30.09./02.10.
L-03	FortiBleed: FBI und Secret Service warnen vor Aussperrung von FortiGate-Admins und Weiterverkauf an Ransomware	KRITISCH	FBI / U.S. Secret Service (über The Record, Help Net Security), 06.10.
L-04	FortiMail: Zero-Day CVE-2026-104286 (CVSS 9,8) ausgenutzt, Fixes jetzt gelistet	HOCH	Fortinet PSIRT FG-IR-26-175 / heise / BleepingComputer / CISA KEV, 01.10./05.10.
L-05	Datenleck bei Zertifizierer GUTcert: Netzpläne und Audit-Befunde deutscher Energieversorger abgeflossen	HOCH	IT-Administrator / energate messenger / Pressebox, 06.10.
L-06	Hitachi Energy RTU500: sechs Lücken in CMU-Firmware 11.x und älter (ICSA-26-279-06)	HOCH	CISA ICS Advisory / Hitachi Energy, 06.10.
L-07	Moxa MGate MB3170/MB3270: Stack Overflow CVE-2026-86325 (CVSS 9,4) schon mit Leserechten	HOCH	Moxa MPESA-269540 / OpenCVE / SecurityOnline, 02.10.
L-08	CERT@VDE: Murrelektronik aas-edge-client ohne Patch (CVSS 9,8) und CODESYS-Lücken bei KEB COMBIVIS	MITTEL	CERT@VDE VDE-2026-108 / VDE-2026-105, 06.10./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
Bayern (München)	1378	OMRON FINS: 724, HMI/VNC: 199, DNP3: 172
Salzburg	27	HMI/VNC: 8, BACnet: 5, DNP3: 5
Tirol (Innsbruck)	43	HMI/VNC: 14, DNP3: 6, Niagara Fox: 6

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./04.10.

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: NetScaler ist in DACH ein verbreitetes Gateway, über das Dienstleister in die Fernwartung und Leitstellenbediener ins Netz kommen. Wie schwer die Lücke wiegt, ist offen: Citrix stuft sie als Denial of Service ein, Kevin Beaumont meldet ein heruntergeladenes Malware-Binary auf einem gepatchten Honeypot, Codeausführung ist nicht bestätigt. watchTowr hat die Lücke reproduziert. Gepatchte Honeypots von Beaumont stürzten nach Anfragen mehrerer Quell-IPs ab. Fällt die SAML-Anmeldung aus, kommt niemand mehr per VPN/SSO in die Fernwartung. Ein gepatchter Stand heißt nicht, dass das Gerät sauber ist.

Empfehlung: Die Konfiguration auf 'add authentication samlAction' bzw. 'samIIdPProfile' prüfen und sofort auf 14.1-73.41 bzw. 13.1-64.28 aktualisieren. Danach nach Webshells, neuen lokalen Konten und fremden Sessions suchen und Sessions sowie Zugangsdaten zurücksetzen. Bei Hinweisen auf eine Kompromittierung das Gerät neu aufsetzen und den Zugang zur Leittechnik bis dahin trennen (CC4, CC1).

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 CVE-2026-76504 (CVSS 9,8) aktiv ausgenutzt

KRITISCH Cisco PSIRT cisco-sa-sdwan-webauth-xr8beuuU / CISA KEV / Help Net Security, 30.09./02.10.

Was ist neu: Über eine kodierte URL (/j_security_check, also ein kodierter Aufruf von /j_security_check) bekommen Angreifer ohne Anmeldung Admin-Rechte auf die API. Cisco bestätigt Angriffe seit September 2026. Es ist die fünfte ausgenutzte Cisco-Zero-Day-Lücke in diesem Jahr. CISA hat sie am 30.09. in den KEV-Katalog aufgenommen. Einen Workaround gibt es nicht. Am 02.10. kam ein Live-Protect-Shield als vorübergehender Teilschutz dazu.

Bedeutung: Wer den SD-WAN Manager übernimmt, steuert die WAN-Verbindungen zu allen Standorten. Damit wird Lateral Movement bis in die Leittechnik möglich.

Empfehlung: Auf 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 oder 26.2.1 aktualisieren. In serviceproxy-access.log und vmanage-server.log nach /j_security_check suchen. Die Management-Oberfläche aus dem Internet nehmen und nur aus einem Management-Netz erreichbar machen (CC2, CC5).

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

L-03 FortiBleed: FBI und Secret Service warnen vor Aussperrung von FortiGate-Admins und Weiterverkauf an Ransomware

KRITISCH FBI / U.S. Secret Service (über The Record, Help Net Security), 06.10.

Was ist neu: Die Angreifer melden sich mit geleakten oder geknackten Zugangsdaten an FortiGate-Firewalls und SSL-VPN an, die aus dem Internet erreichbar sind. Sie legen eigene Admin-Konten an und löschen oder ändern die echten, sodass die Admins ausgesperrt sind. Den Zugang geben sie laut Bericht an Affiliates von INC/Lynx und Payload weiter. Wie viele Geräte betroffen sind, ist uneinheitlich: 86.644 laut SOCRadar, früher ca. 74.000 laut CISA.

Bedeutung: Bei vielen Stadtwerken, Wasserverbänden und Mittelständlern steht FortiGate direkt vor dem Netz für Fernwartung und Leittechnik. Ein Patch schließt diesen Weg nicht, weil die Angreifer gültige Zugangsdaten nutzen.

Empfehlung: Alle VPN- und Admin-Sessions beenden und die Passwörter zurücksetzen. Phishing-resistente MFA einführen, die Admin-Passwörter auf PBKDF2 umstellen und unbekannte Konten löschen. Das Management-Interface darf nicht aus dem Internet erreichbar sein (CC4, CC2).

Quelle: <https://therecord.media/fortibleed-warning-fbi-secret-service> ✓ geprüft

L-04 FortiMail: Zero-Day CVE-2026-104286 (CVSS 9,8) ausgenutzt, Fixes jetzt gelistet

HOCH Fortinet PSIRT FG-IR-26-175 / heise / BleepingComputer / CISA KEV, 01.10./05.10.

Was ist neu: Über eine Path-Traversal-Lücke schreiben Angreifer ohne Anmeldung Dateien auf das Gerät und führen Code aus. 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. CISA hat die Lücke am 01.10. in den KEV-Katalog aufgenommen. Am 04.10. waren die Fixes nur angekündigt. Am 05.10. hat Fortinet das Advisory um die Lösung ergänzt und nennt jetzt 8.0.2, 7.6.7 und 7.4.9. FortiMail Cloud ist seit dem 05.10. gepatcht, am 07.10. folgte dazu eine Klarstellung im Advisory.

Bedeutung: Ein übernommenes Mail-Gateway ist ein direkter Einstieg ins Unternehmensnetz. Von dort erreichen Angreifer oft auch Jump Hosts und schlecht segmentierte OT-Netze.

Empfehlung: Im Download-Portal prüfen, ob die Builds für on-premises verfügbar sind, und sofort aktualisieren. Bis dahin IBE abschalten, das Management-Interface vom Internet trennen und die IOC's aus dem Advisory prüfen (CC5, CC1).

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

L-05 Datenleck bei Zertifizierer GUTcert: Netzpläne und Audit-Befunde deutscher Energieversorger abgeflossen

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

Was ist neu: Angreifer waren ab dem 05.09. in den Systemen der GUTcert GmbH und haben rund 640 GB gestohlen. Darunter sind Anlagenlisten (Umspannwerke, Ortsnetzstationen, Gas-Druckregelanlagen), Netzstrukturpläne und Audit-Berichte mit Schwachstellen. GUTcert ist auf mehrere Erpressungsversuche nicht eingegangen, Entega hat Betroffenheit gemeldet.

Bedeutung: Angreifer kennen damit unter Umständen die Netzarchitektur und offene Audit-Befunde, was ihre Aufklärung deutlich einfacher macht. Der Fall zeigt, wie groß das Lieferkettenrisiko bei Prüfern und Dienstleistern ist.

Empfehlung: Bei GUTcert erfragen, welche eigenen Unterlagen dort lagen, und davon ausgehen, dass diese Dokumentation offenliegt. Die darin genannten Schwachstellen vorrangig schließen. Die Datenweitergabe an Dienstleister vertraglich begrenzen.

Quelle: <https://www.energate-messenger.de/news/267259/cyberattacke-verursacht-grosses-kritis-datenleck>
✓ geprüft

L-06 Hitachi Energy RTU500: sechs Lücken in CMU-Firmware 11.x und älter (ICSA-26-279-06)

HOCH CISA ICS Advisory / Hitachi Energy, 06.10.

Was ist neu: Hitachi Energy hat das Advisory am 29.09. veröffentlicht, CISA hat es am 06.10. übernommen. Betroffen ist die End-of-Life-Firmware 11.x und älter. Zu den Lücken gehören ein Firmware-Update-Endpunkt ohne Anmeldung und ohne Integritätsprüfung (CVE-2026-8065, 9,1), Directory Traversal (CVE-2026-8066, 9,1), ein Reboot ohne Berechtigung (6,5) und der VxWorks-WDB-Debugdienst auf UDP 17185 (CVE-2010-2965, 9,8). Abhilfe bringt nur das Upgrade auf 12.7.8 oder 13.9.1.

Bedeutung: RTU500 sind in den Netzbetrieben in DACH weit verbreitet und laufen oft noch mit alter Firmware. Wer das Netz erreicht, kann Firmware tauschen, Befehle ausführen und Geräte neu starten. Das greift direkt in die Steuerung der Netze ein.

Empfehlung: Alle RTU500 mit Firmware-Stand im Asset-Inventar erfassen und Geräte mit 11.x oder älter für ein Upgrade einplanen. Bis dahin UDP 17185 und die Webdienste an der Zonengrenze sperren und streng segmentieren. Engineering- und Update-Zugriffe auf definierte Jump Hosts beschränken und überwachen (CC5, CC3).

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

L-07 Moxa MGate MB3170/MB3270: Stack Overflow CVE-2026-86325 (CVSS 9,4) schon mit Leserechten

HOCH Moxa MPSA-269540 / OpenCVE / SecurityOnline, 02.10.

Was ist neu: Ein Stack Overflow im Parameter `account_name` der Kontoverwaltung (CVSS 4.0: 9,4) lässt sich schon mit einem reinen Lesekonto ausnutzen. Angreifer können dann Zugangsdaten auslesen, Speicher ändern und das Gerät lahmlegen. Am selben Tag kam CVE-2026-86326 dazu (fehlende Signaturprüfung der Firmware, CVSS 8,6). Eine Ausnutzung ist nicht bekannt. Welche Versionen betroffen sind, unterscheidet sich je nach Quelle (v4.7 und älter laut SecurityOnline). Bei der Frist sind sich die Quellen nicht einig (widersprüchlich: A 2 Wochen / B 1 Woche).

Bedeutung: MGate-Gateways übersetzen Feldbusprotokolle und sitzen genau an der Grenze zwischen Leittechnik und Feldebene. Ein Lesekonto für Wartung oder Monitoring reicht für die Übernahme. Ein übernommenes Gateway kann Prozessdaten verfälschen.

Empfehlung: Die betroffenen Geräte im Asset-Inventar suchen, die Firmware-Stände mit dem Moxa-Advisory abgleichen und die Fixes einspielen. Lesekonten aufräumen und die Weboberfläche nur aus dem Management-Netz erreichbar machen (CC5, CC2).

Quelle: <https://app.opencve.io/cve/CVE-2026-86325> ✓ geprüft

L-08 CERT@VDE: Murrelektronik aas-edge-client ohne Patch (CVSS 9,8) und CODESYS-Lücken bei KEB COMBIVIS

MITTEL CERT@VDE VDE-2026-108 / VDE-2026-105, 06.10./08.10.

Was ist neu: Die REST-API des Murrelektronik aas-edge-client hat keine Anmeldung (CWE-306, CVSS 9,8). Einen Fix gibt es nicht, der Hersteller rät dazu, die Software vollständig zu entfernen. Bei der KEB COMBIVIS Control Runtime 2.0.0 bis vor 2.1.0 kann ein Angreifer mit wenigen Rechten aus der Ferne den PKI-Ordner mit privaten Schlüsseln lesen und überschreiben (CVE-2025-41659, 8,3). Drei weitere CVEs erlauben ohne Anmeldung einen Denial of Service. Der Fix ist Version 2.1.0 mit CODESYS 3.5.21.50.

Bedeutung: Die Lücken stecken in Software für die Verwaltungsschale und in CODESYS-Runtimes, also auch in OEM-Komponenten von DACH-Herstellern. Solche Software taucht in Pilotprojekten und Maschinen oft gar nicht im Asset-Inventar auf.

Empfehlung: Das Asset-Inventar nach dem aas-edge-client und nach CODESYS-Runtimes aller Hersteller durchsuchen. Den Client entfernen. COMBIVIS über den App Manager oder das NOA Cloud Portal auf 2.1.0 bringen und anschließend die Zertifikate erneuern (CC5).

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

Fragen für das nächste Jour fixe

1. Welche unserer Remote-Access-Gateways (NetScaler, FortiGate, Cisco, SonicWall SMA1000) sind aus dem Internet erreichbar, und wer prüft sie diese Woche nach dem Patch auch auf Kompromittierung?
2. Sind alle VPN- und Admin-Konten an der FortiGate bekannt und mit MFA abgesichert, und wann wurden die Passwörter zuletzt gewechselt?
3. Welche Netz- und Audit-Unterlagen liegen bei Zertifizierern, Prüfern und Dienstleistern, und was folgt daraus, falls sie veröffentlicht werden?
4. Wie viele RTU500 mit CMU-Firmware 11.x, Moxa MGate und CODESYS-basierte Steuerungen haben wir im Feld, und mit welchem Firmware-Stand?
5. Ist unser Incident-Response-Plan für einen kompromittierten Fernzugang geübt, inklusive der Entscheidung, die Fernwartung zu trennen?
6. Wie schnell kommen KEV-Meldungen zu unseren Produkten heute bei den Verantwortlichen an?

Maßnahmen dieser Woche

1. NetScaler auf 14.1-73.41 bzw. 13.1-64.28 aktualisieren, dann nach Webshells und neuen Konten suchen und Sessions sowie Zugangsdaten zurücksetzen.
2. Cisco SD-WAN Manager patchen, aus dem Internet nehmen und die Logs nach /%6a_security_check durchsuchen.
3. Bei FortiGate alle VPN- und Admin-Sessions beenden, Passwörter zurücksetzen, unbekannte Konten löschen und phishing-resistente MFA einführen.
4. FortiMail auf 8.0.2, 7.6.7 bzw. 7.4.9 aktualisieren und bis dahin IBE deaktivieren, das Management vom Internet trennen und auf IOCs prüfen.
5. Bei GUTcert und anderen Prüfern abfragen, welche eigenen Unterlagen dort liegen, und die dort genannten Audit-Befunde vorziehen.

6. Das Asset-Inventar nach RTU500 (CMU $\leq$ 11.x), Moxa MGate MB3170/MB3270, CODESYS-Runtimes und dem Murrelektronik aas-edge-client durchsuchen und die Upgrades bzw. die Entfernung einplanen.

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 09.10.2026 automatisch aufgerufen und inhaltlich geprüft.