

WOCHENBERICHT

OT-/Cyber-Lagebild Lebensmittel und Getränke

Ausgabe KW 40/2026 · Lebensmittel und Getränke in DACH

Zielgruppe	Lebensmittel- und Getränkehersteller, Abfüller, Molkereien, Brauereien
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 Lebensmittel- und Getränkehersteller, Abfüller, Molkereien, Brauereien in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 40 kam die größte Gefahr für Lebensmittel- und Getränkehersteller über Edge Devices und Remote Access. In Citrix NetScaler ADC/Gateway werden zwei Zero-Days weltweit aktiv ausgenutzt (CVE-2026-88771/-88772, CVSS v4.0 9.5). Im Cisco Catalyst SD-WAN Manager wird eine Lücke ausgenutzt, mit der Angreifer ohne Anmeldung Admin-Rechte bekommen (CVE-2026-76504, CVSS 9.8). Für beide gibt es Patches, für Cisco aber keinen Workaround. Genau über diese Systeme laufen in vielen Betrieben die Fernwartung der Anlagenbauer für Abfüll-, Verpackungs- und Kälteanlagen und die Vernetzung von Werken, Abfüllstandorten, Lagern und Kühlhäusern. Dazu kommen kritische Lücken in MikroTik-Routern und WatchGuard Access Points sowie hoch eingestufte Lücken in Lantronix-Mobilfunk-Gateways. Solche Edge-Geräte stehen oft unbemerkt in Außenlagern, Kühlhäusern, an Sammelstellen und an Maschinen.

Der Ransomware-Druck bleibt hoch. Im August gab es weltweit 1.073 Angriffe, so viele wie noch in keinem Monat 2026. 31 % davon trafen die Industrie, Qilin war die aktivste Gruppe. Für den Lebensmittelsektor meldet der Food and Ag-ISAC bis Juli 62 % mehr Ransomware-Fälle als im Vorjahr. Wie schnell ein solcher Angriff die Produktion trifft, zeigt der Fall Fairlife (Coca-Cola) aus dem Juli: Dort stand die Molkereiproduktion in den USA rund zehn Tage still. Für verderbliche Ware und Kühlketten ist das ein unmittelbares Risiko. Im Zeitraum wurde kein öffentlich bestätigter neuer Produktionsausfall bei einem Lebensmittelhersteller in DACH gefunden. In Österreich gilt seit 01.10. das NISG 2026, das auch die Herstellung, Verarbeitung und den Vertrieb von Lebensmitteln erfasst. Damit gelten dort ab sofort Meldepflichten (24 h / 72 h / 1 Monat). Vorrang haben jetzt ein sicherer Remote Access (CC4), eine belastbare Segmentierung zwischen IT und Produktion (CC2) und ein geübter Notfallplan für die Produktion (CC1). Mit KI-Unterstützung schaffen das auch kleine Teams.

GESAMTBEWERTUNG

Die Lage ist hoch, weil zwei aktiv ausgenutzte Lücken genau die Fernzugänge und die Standortvernetzung betreffen, über die Ransomware die Produktion erreicht, und weil Ransomware auf Rekordniveau steht. Vorrang hat in dieser Woche, NetScaler und SD-WAN Manager zu patchen, auf Kompromittierung zu prüfen und alle Fernwartungswege in die Produktion zu überprüfen.

Trends

- Edge-Geräte wie VPN- und Remote-Access-Gateways, SD-WAN, Router und Mobilfunk-Gateways bleiben der wichtigste Weg in die Produktion. Zero-Days werden dort oft schon vor der Veröffentlichung ausgenutzt.
- Ransomware erreicht 2026 Höchststände und trifft am häufigsten die Industrie. Der Food and Ag-ISAC meldet für den Lebensmittelsektor bis Juli 62 % mehr Fälle als im Vorjahr. In der Lebensmittelbranche entsteht der Schaden vor allem durch Stillstand und verdorbene Ware, weniger durch den Datenabfluss.
- Die Fernwartung der Anlagenbauer läuft häufig über Mobilfunk-Gateways und Kleinrouter, die in keinem Asset-Inventar stehen. Diese Schatten-Zugänge werden zum Risiko.
- Durch KI liegen zwischen Veröffentlichung und Ausnutzung einer Lücke oft nur noch Stunden (auch laut Food and Ag-ISAC „State of the Threat 2026“). Patchen nach Risiko anhand von KEV-Katalog und Erreichbarkeit (CC5) und eine schnelle Erkennung (CC3) werden

damit wichtiger als lange Wartungsfenster.

- Laut Food and Ag-ISAC bereiten sich staatliche Akteure in OT-Umgebungen vor. Dazu kommen Hacktivismus, Typosquatting und BEC in der Lieferkette sowie ClickFix-Social-Engineering (+108 % im ersten Halbjahr). Die Zahlen sind US-lastig, die Muster gelten aber auch für DACH.
- Regulierung zieht an: Mit dem NISG 2026 gelten in Österreich seit 01.10. NIS2-Pflichten auch für Lebensmittelhersteller ab mittlerer Größe.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Citrix NetScaler ADC/Gateway: zwei Zero-Days werden aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772)	KRITISCH	CISA / Citrix (Cloud Software Group), 27.09.
L-02	Cisco Catalyst SD-WAN Manager: aktiv ausgenutzte Lücke gibt Admin-Rechte ohne Anmeldung (CVE-2026-76504, CVSS 9.8)	KRITISCH	Cisco Security Advisory / CISA KEV (https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog), 30.09.
L-03	Ransomware auf Jahreshöchststand: 1.073 Fälle im August, Industrie mit 31 % am stärksten betroffen	HOCH	Industrial Cyber / Infosecurity Magazine (Daten: NCC Group), 28.09.
L-04	Österreich: NISG 2026 seit 01.10. in Kraft, auch für Lebensmittelhersteller	HOCH	KPMG Austria (OTS) / NISG 2026, 30.09.
L-05	MikroTik RouterOS: Codeausführung ohne Anmeldung, CVSS v3.1 9.8 (ICSA-26-272-06)	MITTEL	CISA ICS Advisory ICSA-26-272-06, 29.09.
L-06	Lantronix G520 Mobilfunk-Gateway: Root-Codeausführung über das Update (ICSA-26-272-01)	MITTEL	CISA ICS Advisory ICSA-26-272-01, 29.09.
L-07	WatchGuard Access Points: Befehlsausführung ohne Anmeldung, CVSS 9.3	MITTEL	SecurityOnline, 28.09.
L-08	Lebensmittel-Lieferdienst Flink: Datenabfluss über kompromittierte Zugangsdaten, Kunden werden erpresst	NIEDRIG	Borns IT- und Windows-Blog, 26.09.

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 Zero-Days werden aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772)

KRITISCH CISA / Citrix (Cloud Software Group), 27.09.

Was ist neu: Citrix hat am 27.09. acht Lücken in NetScaler ADC und Gateway veröffentlicht (CVE-2026-88771 bis -88778). Zwei davon erlauben Remote Code Execution ohne Anmeldung, schon in der Standardkonfiguration (CVSS v4.0 9.5). CISA hat beide am 27.09. in den KEV-Katalog aufgenommen und meldet weltweite Ausnutzung. CISA rät, vor dem Update nach Indicators of Compromise zu suchen, weil das Update forensische Spuren löschen kann.

Bedeutung: Viele Molkereien, Brauereien und Abfüller geben Maschinen- und Abfüllanlagenbauern sowie Dienstleistern für MES und Kühltechnik über NetScaler Gateway Zugriff auf Werksnetze, SPS/HMI und MES. Ein kompromittiertes Gateway ist ein direkter Initial-Access-Weg Richtung Produktionsnetz, und typische Ransomware-Ketten beginnen genau hier.

Empfehlung: Alle NetScaler-Instanzen erfassen. Vor dem Patch Logs und Spuren sichern und nach den Vorgaben von CISA und Citrix mit den Citrix-Werkzeugen auf IoC prüfen, dann auf die gefixten Versionen aktualisieren. Danach alle aktiven Sessions beenden, Konten von Dienstleistern prüfen und deren Zugangsdaten erneuern. Fernwartung in die OT nur noch über einen Jump Host mit MFA und Freigabe pro Sitzung erlauben (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 ausgenutzte Lücke gibt Admin-Rechte ohne Anmeldung (CVE-2026-76504, CVSS 9.8)

KRITISCH Cisco Security Advisory / CISA KEV

(<https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog>), 30.09.

Was ist neu: Über eine falsch verarbeitete URI-Kodierung, also eine speziell kodierte Anfrage an `/api/v20/management/security_check`, bekommen Angreifer ohne Zugangsdaten Admin-Rechte über die API. Cisco bestätigt die Ausnutzung seit September. Betroffen sind auch Systeme, die gegen die SD-WAN-Lücken aus Mai und Juni gepatcht sind. Einen Workaround gibt es nicht, nur Updates (20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1, 26.2.1). CISA hat die Lücke am 30.09. in den KEV-Katalog aufgenommen.

Bedeutung: Hersteller mit mehreren Werken, Molkereien mit Sammelstellen und Getränkegruppen mit mehreren Abfüllstandorten verbinden ihre Standorte oft per SD-WAN. Wer den Manager kontrolliert, kann Routing und Segmentierung ändern und so Wege bis in die Produktionsnetze öffnen.

Empfehlung: Sofort auf eine gefixte Version aktualisieren und den Manager nur für vertrauenswürdige Admin-Hosts aus einem dedizierten Management-Segment erreichbar machen. Danach `serviceproxy-access.log` und `vmanage-server.log` nach Anfragen an `/api/v20/management/security_check` durchsuchen und unerwartete Änderungen an Konfiguration und Routing prüfen (CC2, CC5).

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

L-03 Ransomware auf Jahreshöchststand: 1.073 Fälle im August, Industrie mit 31 % am stärksten betroffen

HOCH Industrial Cyber / Infosecurity Magazine (Daten: NCC Group), 28.09.

Was ist neu: Laut NCC Group gab es im August weltweit 1.073 Ransomware-Fälle, 12 % mehr als im Juli. Auf die Industrie entfielen 31 % der Fälle, auf Konsumgüter 18 %. Europa kam auf 26 % der Fälle. Am aktivsten waren Qilin (164 Fälle, 15 %), The Gentlemen (116) und Clop (89).

Bedeutung: Lebensmittel- und Getränkehersteller zählen statistisch zu Industrie und Konsumgütern und werden häufig getroffen. Sie sind besonders verwundbar, weil Produktion und Kühlkette kaum Stillstand vertragen und verderbliche Ware den Druck zu zahlen erhöht. Fällt die IT aus, stehen Abfüllung, Rezepturverwaltung und Rückverfolgbarkeit oft mit still. Im Fall Fairlife (Juli 2026) stand die Produktion etwa zehn Tage, weil Planung, MES und Logistik an der IT hingen. Der Food and Ag-ISAC meldet für den Sektor bis Juli 2026 ein Plus von 62 % gegenüber dem Vorjahr.

Empfehlung: Ein OT-spezifisches Incident-Response-Playbook festlegen und üben: Wer entscheidet über das Abschalten, wie laufen Abfüllung und Kühlung im Inselbetrieb, und wie lange läuft die Produktion ohne MES und ERP weiter (Rezepturen, Chargen, Etiketten offline, manuelle Chargendokumentation)? Die Wiederherstellung von SPS-Programmen, HMI-Projekten und MES-Datenbanken aus Offline-Backups mindestens einmal pro Quartal testen (CC1).

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

L-04 Österreich: NISG 2026 seit 01.10. in Kraft, auch für Lebensmittelhersteller

HOCH KPMG Austria (OTS) / NISG 2026, 30.09.

Was ist neu: Das NISG 2026 gilt seit 01.10.2026. Ab dann müssen erhebliche Sicherheitsvorfälle gemeldet werden. Die Registrierung läuft bis zum Jahresende 2026, die Selbstdeklaration bis 30.09.2027 (laut KPMG). Der Sektor Lebensmittel (Herstellung, Verarbeitung, Vertrieb) fällt unter das Gesetz, die Schwelle liegt ab 50 Beschäftigten oder über 10 Mio. € Umsatz und über 10 Mio. € Bilanzsumme. Laut der KPMG-Umfrage unter 1.396 österreichischen Unternehmen ist jeder achte Angriff erfolgreich, Lieferketten-Sicherheit erreicht im Schnitt nur 2,03 von 5 Punkten.

Bedeutung: Mittelständische Molkereien, Brauereien und Lebensmittelhersteller in Österreich sind jetzt rechtlich verpflichtet, Cyber-Risiken zu managen und Vorfälle fristgerecht zu melden. Die Geschäftsleitung hat eine Aufsichts- und Schulungspflicht (§ 31 NISG); eine persönliche Haftung ergibt sich aus GmbHG/AktG. Ein Ransomware-Vorfall in der Produktion wird damit auch zum Meldefall.

Empfehlung: Klären, ob das Unternehmen betroffen ist, und die Registrierung beim Bundesamt für Cybersicherheit vorbereiten. Den Meldeweg für OT-Vorfälle im Incident-Response-Plan verankern, also festlegen, wer innerhalb von 24 h die Frühwarnung abgibt (CC1). Lieferanten und Fernwartungs-Dienstleister in die Risikobewertung aufnehmen.

Quelle: https://www.ots.at/presseaussendung/OTS_20260930_OTS0028/nisg-2026-jeder-achte-cyberangriff-ist-erfolgreich-neues-gesetz-soll-unternehmen-besser-schuetzen ✓ geprüft

L-05 MikroTik RouterOS: Codeausführung ohne Anmeldung, CVSS v3.1 9.8 (ICSA-26-272-06)

MITTEL CISA ICS Advisory ICSA-26-272-06, 29.09.

Was ist neu: Ein Integer-Underflow im Web-Management (CVE-2026-84411, CVSS v3.1 9.8, v4: 9.3) erlaubt mit einer einzigen Anfrage ohne Anmeldung Root-Codeausführung oder das Lahmlegen des Geräts (DoS). Betroffen sind alle Versionen unter 7.24. Laut CISA wird die Lücke bisher nicht ausgenutzt.

Bedeutung: Günstige MikroTik-Router stecken oft unbemerkt in Außenlagern, Getränkelagern, Kühlcontainern, an Mineralbrunnen-Quellen und Milchsammelstellen oder in Schaltschränken von Anlagenbauern. Sie werden selten gepatcht. MikroTik-Lücken werden erfahrungsgemäß schnell ausgenutzt, und betroffene Geräte landen in Botnetzen oder dienen als Einstieg.

Empfehlung: Alle MikroTik-Geräte im Asset-Inventar erfassen, auch die der Dienstleister. Priorisiert nach Erreichbarkeit aus dem Internet auf 7.24 aktualisieren (CC5) und das Web-Management vom Internet und vom OT-Netz trennen bzw. nur über VPN zugänglich machen.

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

L-06 Lantronix G520 Mobilfunk-Gateway: Root-Codeausführung über das Update (ICSA-26-272-01)

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

Was ist neu: Firmware 2.6.0.4R6 holt die Update-Metadaten unverschlüsselt über HTTP, und im öffentlichen SDK liegt der private Schlüssel, dem die Firmware vertraut, sodass die Signaturprüfung nicht schützt (CVE-2026-84409, CVE-2026-91191, CVSS v3.1 7.5 / v4 7.7). So lässt sich eigene Software mit Root-Rechten einspielen. Laut CISA wird bisher nichts davon ausgenutzt.

Bedeutung: Mobilfunk-Gateways laufen oft am Firmennetz und an der Firewall vorbei und werden für die Fernwartung von Kältezentralen, Tanks, Silos, Kühlcontainern oder Kläranlagen der Werke und für die Temperaturüberwachung der Kühlkette genutzt. Ein manipuliertes Gateway ist eine Backdoor direkt in die Steuerung.

Empfehlung: Alle Mobilfunk-Gateways einschließlich der Geräte der Anlagenbauer erfassen, auf 2.6.0.7R6 aktualisieren und Updates nur aus vertrauenswürdigen Quellen zulassen. Mittelfristig die Fernwartung über einen zentralen Remote-Access-Weg mit Protokollierung führen.

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

L-07 WatchGuard Access Points: Befehlsausführung ohne Anmeldung, CVSS 9.3

MITTEL SecurityOnline, 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 einen Auth-Bypass (CVE-2026-101891). Laut WatchGuard werden sie bisher nicht ausgenutzt.

Bedeutung: Im WLAN von Lager und Halle hängen Scanner, Staplerterminals, Tablets mit HMI-Zugriff und teils auch Maschinen. Ein übernommener Access Point kann zum Einstieg für Lateral Movement in das Produktionsnetz werden.

Empfehlung: Auf 3.4.8 aktualisieren und die Management-Schnittstellen in ein eigenes Admin-Netz verlegen. Außerdem prüfen, ob Produktions-WLAN und Büro-WLAN wirklich getrennt sind.

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

L-08 Lebensmittel-Lieferdienst Flink: Datenabfluss über kompromittierte Zugangsdaten, Kunden werden erpresst

NIEDRIG Borns IT- und Windows-Blog, 26.09.

Was ist neu: Laut Bericht hat sich ein Unbefugter am 25.09. mit kompromittierten Zugangsdaten Zugang zu internen Systemen von Flink verschafft. Betroffen sind Namen, E-Mail- und Postadressen und Telefonnummern, möglicherweise auch Lieferhinweise und Bestellhistorie. Passwörter und Zahlungsdaten sind laut Flink nicht betroffen. Kunden werden Berichten zufolge erpresst.

Bedeutung: Der Fall liegt nicht in der Produktion. Er zeigt aber das Muster, das auch Hersteller trifft: Gültige Zugangsdaten ohne starke Absicherung reichen für den Einstieg. Für Hersteller mit eigenem Online-Shop oder Direktvertrieb drohen zudem DSGVO-Folgen.

Empfehlung: Alle extern nutzbaren Konten (Dienstleister, Shop-Backends, Fernwartung) auf MFA umstellen, ungenutzte Konten sperren und auf Credential Stuffing überwachen (CC4).

Quelle: <https://borncity.com/blog/2026/09/26/cybervorfaelle-flink-lieferservice-entega-energieversorger-clean-fix-reinigungstechnik/> ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	NetScaler und SD-WAN Manager patchen, auf Kompromittierung prüfen und nur noch für definierte Hosts erreichbar machen [CC4 Secure Remote Access]	L-01, L-02	HOCH	sofort
M-02	Fernwartung der Anlagenbauer auf einen zentralen, protokollierten Zugang (Jump Host mit MFA, Freigabe pro Sitzung) umstellen und Schatten-Zugänge über LTE-Router abbauen [CC4 Secure Remote Access]	L-01, L-06	HOCH	mittelfristig
M-03	OT-Incident-Response-Playbook für Notbetrieb ohne MES/ERP festlegen und üben, Wiederherstellung von SPS-, HMI- und MES-Backups testen [CC1 ICS Incident Response]	L-03	HOCH	1 Woche

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-04	Betroffenheit nach NISG 2026 prüfen, Registrierung vorbereiten und Meldeweg für OT-Vorfälle im Incident-Response-Plan verankern [CC1 ICS Incident Response]	L-04	HOCH	1 Woche
M-05	Edge-Router, LTE-Gateways und Access Points im Asset-Inventar erfassen und nach Erreichbarkeit priorisiert patchen, Management-Schnittstellen vom Internet und OT-Netz trennen [CC5 Risk-Based Vulnerability Management]	L-05, L-06, L-07	MITTEL	1 Woche
M-06	Alle extern nutzbaren Konten auf MFA umstellen, ungenutzte Konten sperren und auf Credential Stuffing überwachen [CC4 Secure Remote Access]	L-08	MITTEL	2 Wochen

Fragen für das nächste Jour fixe

1. Über welche Wege greifen unsere Anlagenbauer heute auf Abfüllung, Verpackung und Kälte zu, und hängt davon etwas an NetScaler, SD-WAN oder einem eigenen LTE-Router?
2. Wie lange können wir ohne MES, ERP und Etikettendruck weiterproduzieren, und wer entscheidet im Ernstfall über das Herunterfahren?
3. Sind die SPS-Programme, HMI-Projekte und Rezepturen offline gesichert, und wann haben wir zuletzt eine Wiederherstellung getestet?
4. Würden wir es bemerken, wenn sich jemand nachts über die Fernwartung an einer SPS anmeldet (CC3)?
5. Sind NetScaler und SD-WAN Manager gepatcht und auf Kompromittierung geprüft, und wer bestätigt das bis Freitag?
6. Fallen unsere österreichischen Standorte unter das NISG 2026, und wer gibt im Ernstfall innerhalb von 24 h die Frühwarnung ab?

Maßnahmen dieser Woche

1. Citrix NetScaler ADC/Gateway patchen. Vorher Spuren sichern und auf Indicators of Compromise prüfen, danach alle Sessions beenden und die Zugangsdaten der Dienstleister erneuern.
2. Cisco Catalyst SD-WAN Manager auf eine gefixte Version bringen, nur für Admin-Hosts erreichbar machen und die Logs nach /%6a_security_check durchsuchen.
3. Alle MikroTik-Router, Lantronix-Gateways und WatchGuard-APs in Werken, Lagern, Kühlhäusern und an Außenstandorten erfassen, auch die Geräte der Anlagenbauer, und aktualisieren.
4. Liste aller Fernwartungszugänge in die Produktion erstellen. Unbekannte oder ungenutzte Zugänge abschalten.
5. Notfall-Checkliste für die Produktion prüfen: manuelle Chargendokumentation, Kühlketten-Überwachung ohne IT, Kontaktliste der Anlagenbauer.
6. Für österreichische Standorte die Betroffenheit nach NISG 2026 klären, Registrierung vorbereiten und den Meldeweg (24 h / 72 h / 1 Monat) festlegen.

7. Alle extern nutzbaren Konten (Dienstleister, Shop-Backends, Fernwartung) auf MFA umstellen und ungenutzte Konten sperren.

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.