

WOCHENBERICHT

OT-/Cyber-Lagebild Lebensmittel und Getränke

Ausgabe KW 41/2026 · Lebensmittel und Getränke in DACH

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

Management Summary

In KW 41/2026 haben wir keinen öffentlich bestätigten Cyberangriff auf einen Lebensmittel- oder Getränkehersteller in Deutschland, Österreich oder der Schweiz gefunden. Für die Branche bleibt die Lage trotzdem angespannt. Angreifer nutzen gerade massenhaft die Edge-Geräte, über die auch Molkereien, Brauereien und Abfüller ihre Fernwartung, Standortvernetzung, Mail und Remote Access betreiben. Das FBI und der US Secret Service warnen am 06.10., dass die FortiBleed-Kampagne gegen FortiGate-Firewalls und SSL-VPN weiterläuft. Die erbeuteten Zugänge werden laut Berichten an Ransomware-Gruppen weitergegeben. Bei FortiMail wird ein Zero-Day ausgenutzt, Fixes gibt es laut Fortinet seit 05.10. Die NetScaler-SAML-Lücke CVE-2026-88779 (laut Citrix Denial of Service) wird gezielt angegriffen und trifft auch Geräte, die gegen frühere NetScaler-Lücken schon gepatcht waren. Für den Cisco SD-WAN Manager ist ein Zero-Day ohne Workaround im Umlauf. Für SonicWall SMA1000 gibt es Hotfixes gegen eine kritische Lücke.

Auf der OT-Seite sind Advisories für Komponenten erschienen, die in Abfüll- und Verpackungslinien, Kälte- und Prozessanlagen häufig verbaut sind: Moxa-MGate-Protokoll-Gateways (Modbus) und CODESYS-basierte Steuerungen von KEB. Das Beispiel aus der Branche kommt aus Japan. Am 07.10. hat Ransomware die IDCf Cloud lahmgelegt, betroffen sind 495 Unternehmen und Kommunen. Am selben Tag hat die Logistiktochter des Lebensmittelkonzerns Nissui den Wareneingang und die Auslieferung eingestellt, nach einem mutmaßlichen unbefugten Zugriff auf das Rechenzentrum eines Dienstleisters. Ob beides zusammenhängt, ist offen. Für Molkereien, Abfüller und Brauereien heißt das: Ihre Verfügbarkeit hängt zunehmend an Cloud- und Logistikdienstleistern. Vorrang haben diese Woche Secure Remote Access (CC4): Fernzugänge patchen, auf Kompromittierung prüfen und Zugangsdaten absichern. Danach kommen eine Defensible Architecture zwischen IT, Cloud und Produktion (CC2) und ein erprobter Incident-Response-Plan für den Ausfall von Logistik- und Dienstleister-IT (CC1). Mit KI-Unterstützung schafft das auch ein kleines Team.

GESAMTBEWERTUNG

Die Lage ist erhöht bis hoch, ohne bestätigten Branchenvorfall in DACH. Mehrere Zero-Days in Edge-Geräten für Fernwartung, Mail und Standortvernetzung werden aktiv ausgenutzt (FortiMail, NetScaler, Cisco SD-WAN), dazu läuft die FortiBleed-Kampagne mit gestohlenen Zugangsdaten gegen FortiGate. Zugänge werden gezielt an Ransomware-Gruppen weitergegeben. Vorrang vor allem anderen hat, diese Gateways zu härten und zu prüfen, ob dort schon jemand eingedrungen ist.

Trends

- Edge-Geräte für Remote Access, Mail und Standortvernetzung (FortiGate, FortiMail, NetScaler, Cisco SD-WAN, SonicWall) sind derzeit der wichtigste Weg ins Netz. Ein Patch allein reicht nicht mehr, danach gehört immer eine Prüfung auf Kompromittierung dazu.
- Patch-Zyklen werden kürzer: Beim NetScaler mussten Geräte, die gerade erst gegen CVE-2026-88771 bis -88778 gepatcht waren, wegen einer neuen Lücke innerhalb weniger Tage erneut aktualisiert werden.
- Gestohlene Zugangsdaten statt Exploits: FortiBleed zeigt, dass Credential Stuffing gegen VPNs in großem Stil funktioniert, wenn MFA fehlt. Die Zugänge gehen über Initial Access Broker an Ransomware-Gruppen (INC, Lynx, Payload).

- Schwachstellen in der Lieferkette der Steuerungssoftware (CODESYS bei mehreren OEMs, Protokoll-Gateways) treffen Maschinen, die Betreiber oft gar nicht im Asset-Inventar führen.
- Ausfälle bei Cloud- und Logistikdienstleistern (IDCF/Nissui im Oktober, Nichirei im Juli 2026) treffen viele Kunden gleichzeitig und unterbrechen Kühlketten, auch wenn der Hersteller selbst nicht angegriffen wurde.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Japan: Ransomware legt die IDCF Cloud lahm (495 Kunden), Logistiktochter von Nissui kann keine Ware mehr annehmen oder ausliefern	HOCH	BleepingComputer; nippon.com (Jiji Press) / IDC Frontier – https://www.nippon.com/en/news/yjj2026100700867/ , 07.10.–08.10.
L-02	Citrix NetScaler: SAML-Zero-Day CVE-2026-88779 (DoS) trifft auch bereits gepatchte Geräte	HOCH	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-03	FortiMail: Zero-Day CVE-2026-104286 (CVSS 9,8) wird ausgenutzt, Fixes seit 05.10. verfügbar	HOCH	Fortinet PSIRT FG-IR-26-175 (https://fortiguard.fortinet.com/psirt/FG-IR-26-175) / BleepingComputer / heise – https://www.heise.de/en/news/FortiMail-Attacks-on-zero-day-vulnerability-underway-workaround-available-11473685.html , 01.10.
L-04	Cisco Catalyst SD-WAN Manager: Zero-Day CVE-2026-76504 (CVSS 9,8) umgeht die Anmeldung, kein Workaround	HOCH	Cisco Security Advisory / CISA KEV, 30.09.
L-05	Moxa MGate: kritische Lücke in Modbus-Protokoll-Gateways (CVE-2026-86325, CVSS4 9,4)	HOCH	Moxa / OpenCVE, 02.10.
L-06	SonicWall SMA1000: kritische SSRF-Lücke im Remote-Access-Gateway (CVE-2026-102255)	HOCH	BleepingComputer / SonicWall, 07.10.
L-07	KEB COMBIVIS Control Runtime: CODESYS-Lücken legen Zertifikate und Schlüssel offen und ermöglichen DoS (VDE-2026-105)	MITTEL	CERT@VDE, 08.10.
L-08	Qilin-Ransomware: Japan liefert mutmaßlichen Entwickler an Deutschland aus (Qilin hatte sich 2025 zum Angriff auf Asahi bekannt)	ORIENTIERUNG	heise online / BleepingComputer (https://www.bleepingcomputer.com/news/security/qilin-ransomware-claims-asahi-brewery-attack-leaks-data/), 06.10.

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 Japan: Ransomware legt die IDCf Cloud lahm (495 Kunden), Logistiktochter von Nissui kann keine Ware mehr annehmen oder ausliefern

HOCH BleepingComputer; nippon.com (Jiji Press) / IDC Frontier – <https://www.nippon.com/en/news/yjj2026100700867/>, 07.10.–08.10.

Was ist neu: Am 07.10. gegen 03:40 Uhr Ortszeit hat Ransomware einen Teil der IDCf Cloud von IDC Frontier (SoftBank-Gruppe) getroffen. Die Region „East Japan Region 1“ wurde vom Netz genommen, betroffen sind 495 Unternehmen und Kommunen. Einen Termin für die Wiederherstellung gab es zunächst nicht. Nissui meldet, dass Nissui Logistics nach einem mutmaßlichen unbefugten Zugriff auf das Rechenzentrum eines Dienstleisters keine Waren mehr annimmt oder ausliefert. Ob beide Fälle zusammenhängen, ist laut BleepingComputer unklar.

Bedeutung: Der Fall folgt einem bekannten Muster (Nichirei im Juli 2026, Peter Green Chilled): Fällt die IT eines Logistik- oder Cloud-Dienstleisters aus, steht die Kühltette, auch wenn die eigene Produktion gar nicht angegriffen wurde. Viele Hersteller lagern ERP, MES, Etikettierdaten oder Tourenplanung aus. Fehlen Aufträge, Chargendaten oder Lieferscheine, steht das Werk. Hersteller mit kurzen Mindesthaltbarkeiten (Molkerei, Frischfleisch, Feinkost) trifft das am schnellsten.

Empfehlung: In der Business-Impact-Analyse und im Notfallplan festlegen, wie Produktion und Versand bei einem Ausfall von Cloud-, ERP- oder Logistik-IT für 3–7 Tage weiterlaufen (Offline-Rezepte, Chargenlisten, manuelle Lieferscheine, Kühlhaus-Notprozesse), und das üben (CC1). Mit den Dienstleistern Meldewege, Wiederanlaufzeiten und Backups vertraglich klären.

Quelle: <https://www.bleepingcomputer.com/news/security/ransomware-attack-disrupts-japans-idcf-cloud-used-by-govt-clients/> ✓ geprüft

L-02 Citrix NetScaler: SAML-Zero-Day CVE-2026-88779 (DoS) trifft auch bereits gepatchte Geräte

HOCH 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. 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: Viele Lebensmittelhersteller lassen Lieferanten, Instandhalter, Maschinenbauer und Außendienst über NetScaler herein, oft mit SAML-Anmeldung. Ein Patch allein reicht hier nicht. Wer schon kompromittiert ist, behält eine Backdoor im Netz, die bis in die Produktion reichen kann.

Empfehlung: Auf 14.1-73.41 bzw. 13.1-64.28 aktualisieren. Anschließend per Threat Hunting nach Webshells, neuen Konten und auffälligen Sessions suchen und bei Verdacht den Incident-Response-Plan auslösen (CC3/CC1). Fernwartung für die OT nur über einen getrennten Jump Host mit MFA zulassen (CC4).

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

L-03 FortiMail: Zero-Day CVE-2026-104286 (CVSS 9,8) wird ausgenutzt, Fixes seit 05.10. verfügbar

HOCH Fortinet PSIRT FG-IR-26-175 (<https://fortiguard.fortinet.com/psirt/FG-IR-26-175>) / BleepingComputer / heise – <https://www.heise.de/en/news/FortiMail-Attacks-on-zero-day-vulnerability-underway-workaround-available-11473685.html>, 01.10.

Was ist neu: Über eine Path-Traversal-Lücke können Angreifer ohne Anmeldung Dateien auf FortiMail schreiben und Code ausführen. Betroffen sind 7.2.0–7.2.9, 7.4.0–7.4.8, 7.6.0–7.6.6 und 8.0.0–8.0.1. Die Fixes 7.4.9, 7.6.7 und 8.0.2 waren beim Erscheinen nur angekündigt, am 05.10. hat Fortinet sie im Advisory FG-IR-26-175 als Lösung ergänzt. Wer 7.2 nutzt, soll auf 7.4 oder neuer wechseln. Die CISA hat die Lücke in den KEV-Katalog aufgenommen.

Bedeutung: Über das Mail-Gateway laufen Bestellungen, Lieferavis und die Kommunikation mit dem Handel. Wer es übernimmt, kann glaubwürdiges Phishing verschicken und kommt ins Netz.

Empfehlung: Den Workaround aus FG-IR-26-175 sofort umsetzen: IBE abschalten und das Management-Interface vom Internet trennen. Auf 7.4.9, 7.6.7 bzw. 8.0.2 aktualisieren und das Gerät nach IOCs durchsuchen (CC5).

Quelle: <https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/> ✓ geprüft

L-04 Cisco Catalyst SD-WAN Manager: Zero-Day CVE-2026-76504 (CVSS 9,8) umgeht die Anmeldung, kein Workaround

HOCH Cisco Security Advisory / CISA KEV, 30.09.

Was ist neu: Mit einer speziell kodierten URL umgehen Angreifer ohne Anmeldung die Authentifizierung und bekommen Admin-Zugriff auf die API. Cisco weiß seit September von Angriffen. CISA hat die Lücke am 30.09. in den KEV-Katalog aufgenommen. Einen Workaround gibt es nicht. Gefixt ist die Lücke 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. Die von Cisco verwaltete Cloud ist bereits gepatcht.

Bedeutung: Mehrwerk-Gruppen und Getränkekonzerne verbinden Werke, Abfüllstandorte und Kühllager oft per SD-WAN. Wer den SD-WAN Manager kontrolliert, kann Routen und Richtlinien zwischen den Standorten ändern und damit die Segmentierung zur Produktion aushebeln.

Empfehlung: Sofort auf eine gepatchte Version gehen und den Manager nur aus einem Management-Netz erreichbar machen (CC2/CC5). Danach serviceproxy-access.log und vmanage-server.log nach „/%6a_security_check“ durchsuchen (CC3).

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

L-05 Moxa MGate: kritische Lücke in Modbus-Protokoll-Gateways (CVE-2026-86325, CVSS4 9,4)

HOCH Moxa / OpenCVE, 02.10.

Was ist neu: Ein Stack-Overflow in der Kontoverwaltung lässt sich schon mit einem Konto mit reinen Leserechten ausnutzen. Ein Angreifer kann so Speicher auslesen (auch Zugangsdaten), Speicher verändern und das Gerät lahmlegen. Laut OpenCVE sind die Serien MB3170 und MB3270 bis v4.7 betroffen. Dazu kommt CVE-2026-86326 (manipulierte Firmware, CVSS 8,6). Eine aktive Ausnutzung ist bisher nicht bekannt.

Bedeutung: MGate-Gateways koppeln in Molkereien, Brauereien und Abfüllanlagen häufig ältere Modbus-Geräte wie Kälteanlagen, CIP-Dosierung oder Zähler an SPS, SCADA und MES. Fällt so ein Gateway aus oder wird es manipuliert, sind die Prozessdaten falsch oder fehlen ganz. Im schlimmsten Fall steht die Kühlkette.

Empfehlung: Im Asset-Inventar nach MGate MB3170/MB3270 suchen und die Firmware nach dem Moxa-Advisory aktualisieren. Die Web-Oberfläche nur aus dem Engineering-Netz erreichbar machen und unnötige Lesekonten löschen (CC5).

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

L-06 SonicWall SMA1000: kritische SSRF-Lücke im Remote-Access-Gateway (CVE-2026-102255)

HOCH BleepingComputer / SonicWall, 07.10.

Was ist neu: Ohne Anmeldung lassen sich SMA1000 6210, 7210 und 8200v über die WorkPlace-Oberfläche dazu bringen, Anfragen an interne Funktionen zu schicken. Hotfixes gibt es seit dem 06.10. Eine Ausnutzung ist noch nicht bekannt. Shadowserver zählt über 400 offen erreichbare Geräte.

Bedeutung: Ransomware-Gruppen haben SMA-Gateways 2026 schon mehrfach angegriffen. Läuft die Fernwartung der Anlagenbauer für Abfüll- oder Verpackungslinien über SMA1000, ist das ein direkter Weg Richtung Produktion.

Empfehlung: Den Hotfix sofort einspielen und prüfen, ob die WorkPlace-Oberfläche aus dem Internet erreichbar sein muss. Fernwartung nur über einen Jump Host mit MFA und zeitlich begrenzter Freigabe erlauben (CC4).

Quelle: <https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-max-severity-ssrf-flaw-in-sma1000-gateways/> ✓ geprüft

L-07 KEB COMBIVIS Control Runtime: CODESYS-Lücken legen Zertifikate und Schlüssel offen und ermöglichen DoS (VDE-2026-105)

MITTEL CERT@VDE, 08.10.

Was ist neu: Über CVE-2025-41659 (CVSS 8,3) kann ein Angreifer mit wenigen Rechten aus der Ferne den PKI-Ordner mit Zertifikaten und privaten Schlüsseln lesen und überschreiben. Werden die Zertifikate gelöscht, läuft die Kommunikation nur noch unverschlüsselt. Drei weitere CVEs (7,5/7,5/5,9) erlauben ohne Anmeldung einen Denial of Service. Betroffen ist die arm64-Runtime ab 2.0.0 bis vor 2.1.0 (CODESYS 3.5.21.10). Behoben ist das in 2.1.0 mit CODESYS 3.5.21.50.

Bedeutung: KEB-Antriebe und andere CODESYS-basierte Steuerungen stecken häufig in Förderbändern, Abfüll-, Verpackungs- und Palettieranlagen, also oft in Maschinen von Zulieferern. Ein DoS auf der Runtime stoppt die Linie. CODESYS-Lücken tauchen bei immer mehr OEMs auf. Die Lieferkette der Steuerungssoftware gehört deshalb ins Schwachstellenmanagement.

Empfehlung: Beim Maschinenbauer eine SBOM bzw. die Liste der eingesetzten CODESYS-Versionen anfordern und im Asset-Inventar erfassen, wo CODESYS-Runtimes laufen. KEB COMBIVIS im nächsten Wartungsfenster auf 2.1.0 aktualisieren (CC5). Bis dahin die Runtimes per Segmentierung nur aus der Zelle erreichbar machen (CC2).

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

L-08 Qilin-Ransomware: Japan liefert mutmaßlichen Entwickler an Deutschland aus (Qilin hatte sich 2025 zum Angriff auf Asahi bekannt)

ORIENTIERUNG heise online / BleepingComputer (<https://www.bleepingcomputer.com/news/security/qilin-ransomware-claims-asahi-brewery-attack-leaks-data/>), 06.10.

Was ist neu: Ein 28-jähriger Russe, der die Qilin-Ransomware programmiert haben soll, wurde im Mai in Osaka festgenommen und Anfang Oktober nach Deutschland ausgeliefert (heise, nach einem Bericht der Asahi Shimbun). Der Haftbefehl beruht auf der Erpressung eines deutschen Logistikunternehmens im September 2024, bei der Lösegeld gezahlt wurde. Wegen des Angriffs auf die Brauerei Asahi, zu dem sich Qilin 2025 bekannt hatte (BleepingComputer), klagt Japan ihn laut heise bisher nicht an.

Bedeutung: Der Asahi-Fall zeigt, wie Ransomware einen Getränkehersteller samt Produktion lahmlegen kann: Asahi stoppte Ende September 2025 den Betrieb in japanischen Werken, die Konkurrenz konnte den Ausfall laut heise nicht auffangen. Festnahmen schwächen solche Gruppen nur kurz, die Bedrohung bleibt.

Empfehlung: Den Incident-Response-Plan für einen kompletten ERP-/MES-Ausfall mit Produktion und Logistik als Tabletop üben (CC1).

Quelle: <https://www.heise.de/news/Seltene-Sache-Japan-liefert-Ransomware-Verdaechtigen-an-Deutschland-aus-11478517.html> ✓ geprüft

Fragen für das nächste Jour fixe

1. Welche Fernzugänge (FortiGate-VPN, NetScaler, SonicWall SMA) führen bei uns in die Produktion? Sind alle mit MFA abgesichert und auf dem aktuellen Patch-Stand?
2. Haben wir nach den NetScaler- und FortiGate-Warnungen nicht nur gepatcht, sondern auch auf Webshells, fremde Admin-Konten und unbekannte VPN-Benutzer geprüft?
3. Wissen wir, in welchen Maschinen und Linien Moxa-Gateways oder CODESYS-Runtimes stecken, und fragen wir das bei den Maschinenbauern ab?
4. Wie lange können Abfüllung, Kühlkette und Versand laufen, wenn ERP, MES, unser Cloud-Dienstleister oder unser Logistikdienstleister mehrere Tage ausfallen?
5. Wer entscheidet nachts und am Wochenende, ob ein kompromittierter Fernzugang vom Netz genommen wird, und ist das im Incident-Response-Plan geregelt?

Maßnahmen dieser Woche

1. FortiGate: alle VPN- und Admin-Passwörter zurücksetzen, aktive Sessions beenden und MFA erzwingen. Admin-Konten auf Fremdkonten prüfen und die Admin-Oberfläche vom Internet trennen (CC4).
2. Citrix NetScaler mit SAML auf 14.1-73.41 bzw. 13.1-64.28 aktualisieren und anschließend auf Webshells, neue Konten und fremde Sessions prüfen (CC4/CC1).
3. FortiMail: den Workaround aus FG-IR-26-175 umsetzen (IBE abschalten, Management-Interface vom Internet trennen), nach IOCs suchen und auf 7.4.9/7.6.7/8.0.2 aktualisieren (CC5).
4. Cisco SD-WAN Manager patchen und die Logs nach „/%6a_security_check“ durchsuchen; SonicWall SMA1000 mit dem Hotfix versorgen (CC5).
5. Asset-Inventar nach Moxa MGate MB3170/MB3270 und CODESYS-basierten Runtimes (u. a. KEB COMBIVIS) durchsuchen, bei Maschinenbauern SBOM bzw. CODESYS-Versionen

anfordern und die Updates einplanen (CC5).

6. Notbetrieb für den Ausfall von Cloud-, ERP- und Logistikdienstleistern festlegen und üben (manuelle Lieferscheine, Chargenlisten, Kühlhaus-Notprozesse). Meldewege und Wiederanlaufzeiten mit den Dienstleistern vertraglich klären (CC1).

HINWEIS ZUR QUELLENLAGE

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