

WOCHENBERICHT

OT-/Cyber-Lagebild Lebensmittel und Getränke

Ausgabe KW 42/2026 · Lebensmittel und Getränke in DACH

Zielgruppe	Lebensmittel- und Getränkehersteller, Abfüller, Molkereien, Brauereien
Berichtszeitraum	09.10.2026–16.10.2026
Version	1.0
Datum	16.10.2026
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 42 standen Angriffe auf die Kühlkette im Mittelpunkt. In der Nacht vom 11. auf den 12.10. haben Unbekannte in mehreren hundert französischen Supermärkten Kühl- und Tiefkühlschränke über Fernsteuerungen manipuliert, die aus dem Internet erreichbar waren. Sie haben Temperaturen und Abtauzeiten verstellt, und Ware verdarb in großer Menge. CERT-FR hat am 12.10. zahlreiche kompromittierte Steuerungen vom Typ Danfoss AK-SM und AK-SC bestätigt und die Warnung am 13.10. auf Copeland xweb und Dixell xweb erweitert. Die Angriffe laufen laut CERT-FR wahrscheinlich noch. Laut Reuters waren am 13.10. mindestens 4.500 Danfoss-Oberflächen online sichtbar. Das BSI warnt vor Nachahmern und nennt ausdrücklich kleine vernetzte Anlagen wie Kühlsysteme. In Deutschland und der Schweiz melden die großen Händler bisher keinen Befall, und behördlich bestätigte Fälle in DACH gibt es nicht. Dieselben Steuerungen laufen aber auch in Kühlhäusern, Kühlzellen und Tiefkühlagern von Molkereien, Fleischverarbeitern und Getränkeabfüllern.

Am 12.10. hat Ahold Delhaize nach einem Sicherheitsvorfall Systeme in den USA, den Niederlanden und Belgien vom Netz genommen. Bestell- und Übergabeprozesse waren gestört, und in den Niederlanden blieben Frischeregale leer. Am Werksrand gab es zwei aktiv ausgenutzte Lücken: Ivanti Connect Secure (Zero-Day, für die Privilege Escalation fehlt noch ein Patch) und PAN-OS, also Firewalls, die oft IT und OT trennen. Dazu kamen Advisories mit direktem Bezug zur Produktion: Rockwell ArmorBlock I/O (CVSS 9,1), kritische Siemens-Updates für S7-1500 und Industrial Edge, ein HMI-Advisory von Schneider und Eclipse Milo im OPC-UA-Umfeld. Vorrang hat in dieser Woche Secure Remote Access (CC4): Keine Steuerung für Kälte, Abfüllung oder Prozess darf direkt aus dem Internet erreichbar sein.

GESAMTBEWERTUNG

Die Lage ist hoch. In einem Nachbarland läuft eine aktive Kampagne gegen Kühlsteuerungen, die aus dem Internet erreichbar sind, mit realen Warenschäden. Dieselben Gerätetypen sind in der DACH-Lebensmittelbranche verbreitet, und das BSI erwartet Nachahmer. Vorrang hat, alle Kälte- und Fernwartungszugänge vom Internet zu trennen, ihre Konfiguration zu prüfen und VPN-Gateways und Firewalls an der IT/OT-Grenze abzusichern (CC4, CC2).

Trends

- Kältetechnik rückt als OT-Ziel in den Vordergrund. Sie liegt oft außerhalb der OT-Verantwortung und wird von Dienstleistern direkt über das Internet gewartet. Angreifer manipulieren Sollwerte und Abtauzeiten, statt Daten zu verschlüsseln.
- Sabotage ohne Lösegeldforderung: Beim Angriff in Frankreich gab es weder ein Bekennerschreiben noch eine Forderung. Der Schaden entstand allein durch verdorbene Ware.
- Fernwartungszugänge von Dienstleistern (Kälte, Gebäudetechnik, Maschinenbauer) bleiben die häufigste offene Tür, weil sie oft nicht im eigenen Asset-Inventar stehen.
- Altgeräte ohne Patches (End-of-Life) werden zum Hauptrisiko, weil ein Reset sie nicht dauerhaft schützt.
- Edge-Geräte am Übergang zwischen IT und OT (VPN-Gateways, Firewalls) werden weiter aktiv ausgenutzt. Zero-Days wie bei Ivanti treffen auch voll gepatchte Geräte.

- Cybervorfälle bei großen Handelskunden treffen Hersteller von Frischware über Bestellung, Logistik und Kühlkette, auch ohne Angriff auf die eigene Produktion.
- Lücken in Bibliotheken wie Eclipse Milo machen SBOM-Abfragen bei OT-Lieferanten zur Pflichtaufgabe.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	CERT-FR: aktive Angriffswelle auf Kühlsteuerungen von Danfoss AK-SC/AK-SM, Copeland xweb und Dixell xweb (CERTFR-2026-ALE-012)	KRITISCH	CERT-FR (ANSSI), 12.10.
L-02	BSI warnt Betreiber kleiner Anlagen vor Nachahmern des Kühlanlagen-Angriffs (BSI-CS 154)	HOCH	heise online / BSI, 13.10.
L-03	Ivanti Connect Secure: Zero-Day wird aktiv ausgenutzt, Privilege Escalation noch ohne Patch (CVE-2026-104935)	HOCH	BleepingComputer / Volexity / CISA KEV, 13.10.
L-04	Palo Alto PAN-OS: Lücke in der Management-Oberfläche aktiv ausgenutzt (CVE-2026-0322)	HOCH	Palo Alto Networks; CISA KEV, 14.10.
L-05	Tausende Kühlsteuerungen weiter offen im Internet, bekannte Lücken in Danfoss AK-SM 800A	HOCH	Reuters via Euronews; Claroty Team82, 14.10.
L-06	Rockwell 1732E ArmorBlock I/O: Passwort ohne Anmeldung änderbar (SD1801, CVE-2026-12655)	HOCH	Rockwell Automation; SecurityWeek, 13.10.
L-07	ICS-Patchday: kritische Lücken in Siemens S7-1500 und Industrial Edge, Schneider-HMI betroffen	HOCH	SecurityWeek, 14.10.
L-08	Cybervorfall bei Ahold Delhaize: Bestellungen und Belieferung von Albert Heijn, Delhaize und Food Lion gestört	MITTEL	BleepingComputer / NL Times, 12.10.
L-09	Eclipse Milo: Lücken in OPC-UA-Server-Bibliothek (ICSA-26-288-01)	MITTEL	CISA, 15.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 16.10.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt. Siemens S7 = Port 102 (alle ISO-TSAP-Dienste, nicht nur echte S7-Steuerungen), OPC UA = Standardport 4840.

Region	Gesamt	Top-Protokolle
Deutschland	143086	DNP3: 33392, OMRON FINS: 23267, ProConOS: 16506, Siemens S7: 8211, OPC UA: 5676
Österreich	4649	HMI/VNC: 1053, DNP3: 949, IEC-104: 454, Siemens S7: 357, OPC UA: 139

Meldungen im Detail

L-01 CERT-FR: aktive Angriffswelle auf Kühlsteuerungen von Danfoss AK-SC/AK-SM, Copeland xweb und Dixell xweb (CERTFR-2026-ALE-012)

KRITISCH CERT-FR (ANSSI), 12.10.

Was ist neu: CERT-FR hat die Warnung am 12.10. veröffentlicht. Am 13.10. kamen zu Danfoss AK-SM und AK-SC auch Copeland xweb und Dixell xweb hinzu. Laut CERT-FR sind zahlreiche Geräte kompromittiert, und die Kampagnen laufen „wahrscheinlich noch“. Ein Factory Reset allein reicht nicht: End-of-Life-Geräte, die weiter erreichbar sind, werden sehr wahrscheinlich erneut kompromittiert. Den Angriffsweg nennt die Behörde nicht (widersprüchlich: A sagt, der Zugang lief nach bisherigem Stand über die Fernwartung des Kältedienstleisters / B sagt, CERT-FR nennt keinen Angriffsweg).

Bedeutung: Diese Steuerungen regeln nicht nur Kühlschränke im Handel. Sie laufen auch in Molkereien, Fleisch- und Feinkostbetrieben, Brauereien, Getränkelagern und Logistikzentren, und Kältefirmen warten sie oft per Fernwartung. Diese Verbindung steht häufig nicht im Asset-Inventar. Wird ein Sollwert oder eine Abtauzzeit manipuliert, reißt die Kühlkette und damit die HACCP-Kette. Die Folgen sind Warenverlust, Rückrufisiko und Ärger mit der Lebensmittelüberwachung.

Empfehlung: Heute mit dem Kältedienstleister klären, welche Steuerungen eine öffentliche IP haben oder per Portweiterleitung erreichbar sind, und diese Erreichbarkeit beenden. Danach Zugriff nur noch per VPN oder über ein geschütztes Netz (CC4). Als Notlösung gilt eine Firewall-Freigabe nur für die IP-Adressen des Dienstleisters. Standardpasswörter ändern und Konfiguration, Abtaupläne und Alarmgrenzen mit dem Soll abgleichen. Kompromittierte Geräte auf Werkseinstellungen zurücksetzen und neu einrichten. End-of-Life-Geräte vom Netz nehmen oder ersetzen. Vorher die Versicherungsbedingungen zur Datenübertragung an den Dienstleister prüfen.

Quelle: <https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/> ✓ geprüft

L-02 BSI warnt Betreiber kleiner Anlagen vor Nachahmern des Kühlanlagen-Angriffs (BSI-CS 154)

HOCH heise online / BSI, 13.10.

Was ist neu: Das BSI hat eine Empfehlung für Betreiber kleiner und kleinster industrieller Anlagen veröffentlicht und nennt darin ausdrücklich Kühlsysteme. BSI-Präsidentin Claudia Plattner sagt, der Angriff hätte jedes Land treffen können und könne jederzeit Nachahmer finden. Laut BSI waren die Passwörter offenbar schon bei Auslieferung unzureichend gesichert. Ein bestätigter Fall in Deutschland ist nicht bekannt.

Bedeutung: Viele Hersteller sehen Kältetechnik, PV-Wechselrichter oder Druckluft als Haustechnik außerhalb der OT-Verantwortung. Genau diese Anlagen sind oft direkt mit dem Internet verbunden und werden von externen Dienstleistern betreut. Mit der Prüfliste des BSI lässt sich das ohne großes Projekt klären.

Empfehlung: Die Fragen aus BSI-CS 154 für jede vernetzte Kälte- und Energieanlage beantworten: Internet-Erreichbarkeit, VPN, zweiter Faktor, Update-Status. Das Ergebnis ins Asset-Inventar übernehmen. Temperaturalarmlen so einstellen, dass sie auch bei absichtlich geänderten Sollwerten auslösen.

Quelle: <https://www.heise.de/news/BSI-gemahnt-auch-Betreiber-kleiner-vernetzter-Anlagen-11487069.html> ✓ geprüft

L-03 Ivanti Connect Secure: Zero-Day wird aktiv ausgenutzt, Privilege Escalation noch ohne Patch (CVE-2026-104935)

HOCH BleepingComputer / Volexity / CISA KEV, 13.10.

Was ist neu: Die Lücke (CVSS 8,6) erlaubt ohne Anmeldung die Ausführung von Befehlen auf dem VPN-Gateway. Volexity beobachtet die Ausnutzung durch den Threat Actor UTA0576 seit Anfang Oktober. Zusammen mit einer Privilege Escalation, für die Ivanti noch keinen Patch hat, erreichen die Angreifer Root-Rechte auch auf gepatchten Geräten und stehlen Active-Directory-Zugangsdaten. CISA hat die Lücke am 13.10. in den KEV-Katalog aufgenommen.

Bedeutung: Viele Produktionsbetriebe öffnen über Ivanti Connect Secure den Fernzugang für Maschinenbauer, Anlagenbauer und Kältedienstleister. Wer das Gateway übernimmt, kommt mit gestohlenen AD-Zugangsdaten per Lateral Movement bis an MES, SCADA und Abfüllanlagen.

Empfehlung: Sofort auf die gepatchten Versionen gehen und das Gerät auf Kompromittierung untersuchen. Der Integrity Checker allein reicht laut CISA womöglich nicht. Bei Verdacht alle Konten zurücksetzen, die über das Gateway genutzt werden, und den OT-Zugang vorübergehend über einen separaten Jump Host führen.

Quelle: <https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-day-exploited-in-attacks/> ✓ geprüft

L-04 Palo Alto PAN-OS: Lücke in der Management-Oberfläche aktiv ausgenutzt (CVE-2026-0322)

HOCH Palo Alto Networks; CISA KEV, 14.10.

Was ist neu: Wer gültige Admin-Zugangsdaten hat und die Management-Oberfläche erreicht, kann Code als root ausführen. Betroffen sind PA-Series, VM-Series und Panorama mit PAN-OS 10.2 bis 12.2. Palo Alto meldet „very limited exploitation“. Die CISA hat die Lücke am 14.10. in den KEV-Katalog aufgenommen.

Bedeutung: In vielen Produktionsstätten trennt eine PAN-OS-Firewall das Büronetz von Produktion und Abfüllung. Wird sie übernommen, ist der Weg für Lateral Movement in die OT frei.

Empfehlung: Patch einspielen und die Management-Oberfläche nur aus einem eigenen Admin-Netz erreichbar machen (CC2). Admin-Konten mit MFA absichern und die Logins der letzten Wochen prüfen.

Quelle: <https://security.paloaltonetworks.com/CVE-2026-0322> ✓ geprüft

L-05 Tausende Kühlsteuerungen weiter offen im Internet, bekannte Lücken in Danfoss AK-SM 800A

HOCH Reuters via Euronews; Claroty Team82, 14.10.

Was ist neu: Laut Reuters waren am Dienstag vor dem 14.10. mindestens 4.500 Danfoss-Oberflächen online sichtbar. Der Scan-Anbieter Onyphe meldet, dass darunter noch viele veraltete Versionen sind. Claroty Team82 hatte schon vorher eine Authentifizierungsumgehung, Command Injection und DoS in der Weboberfläche des AK-SM 800A beschrieben. Behoben ist das in Firmware R4.3.1.

Bedeutung: Keine Behörde hat bestätigt, dass genau diese Lücken für die Angriffe in Frankreich genutzt wurden. Klar ist aber: Weboberflächen der Kältetechnik sind ein bekanntes Ziel. Oft fehlen sie im Asset-Inventar, weil die Kältefirma sie betreut und nicht die eigene IT oder OT.

Empfehlung: Die eigenen öffentlichen IP-Bereiche nach Weboberflächen von Kälte- und Gebäudesteuerungen absuchen oder einen Dienstleister damit beauftragen. Alle Kältesteuern mit Firmware-Stand ins Asset-Inventar aufnehmen und nach Risiko patchen (CC5). Bei Danfoss den Sicherheitsmodus „Strict“ setzen und Standardpasswörter ändern.

Quelle:

<https://www.euronews.com/2026/10/14/thousands-of-supermarket-fridges-still-exposed-after-cyberattack> ✓
geprüft

L-06 Rockwell 1732E ArmorBlock I/O: Passwort ohne Anmeldung änderbar (SD1801, CVE-2026-12655)

HOCH Rockwell Automation; SecurityWeek, 13.10.

Was ist neu: Mit CVE-2026-12655 (CVSS 3.1: 9,1) kann ein Angreifer ohne Konto das Webserver-Passwort ändern. CVE-2026-12656 (7,5) legt die Kommunikation per Storm-Traffic lahm, danach muss das Gerät aus- und wieder eingeschaltet werden. Betroffen ist Firmware bis 3.012, behoben ist das in 3.013. Einen Workaround gibt es nicht. SecurityWeek führt das Advisory im ICS-Patchday vom 14.10.

Bedeutung: ArmorBlock-I/O-Module sitzen direkt an Abfüll-, Verpackungs- und Förderanlagen mit Allen-Bradley-Steuerung. Fällt ein Modul aus, steht die Linie, bis jemand vor Ort das Gerät neu startet.

Empfehlung: Betroffene Artikelnummern im Asset-Inventar suchen und das Update im nächsten Wartungsfenster einspielen (CC5). Bis dahin die Geräte in eine eigene Zelle legen, ohne Zugriff aus dem Büronetz (CC2).

Quelle: <https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1801.html> ✓
geprüft

L-07 ICS-Patchday: kritische Lücken in Siemens S7-1500 und Industrial Edge, Schneider-HMI betroffen

HOCH SecurityWeek, 14.10.

Was ist neu: Siemens hat 17 Advisories veröffentlicht. Kritisch sind Lücken in einigen Simatic-S7-1500-CPU's (über 400 Schwachstellen im GNU/Linux-Subsystem), in Industrial Edge und in Ruggedcom Crossbow SAC. Dazu kommen Updates für Simatic WinCC und Simatic IPC. Schneider meldet eine Lücke in Pro-face STW6000 und Harmony STW6, über die ein präparierter Link zur Geräteübernahme führen kann. Rockwell ArmorBlock siehe eigene Meldung.

Bedeutung: S7-1500 und WinCC sind in DACH Standard in Abfüllung, Verpackung, Prozesstechnik und Reinigung (CIP). Eine Ausnutzung ist laut SecurityWeek nicht bekannt. Deshalb zählt hier Planung nach Risiko statt Notfall-Patch.

Empfehlung: Betroffene Geräte über das Asset-Inventar ermitteln und nach Erreichbarkeit priorisieren: zuerst alles, was aus dem Büronetz oder per Fernwartung erreichbar ist. Patches im nächsten geplanten Linienstillstand einspielen und bis dahin die Workarounds der Hersteller und Segmentierung nutzen.

Quelle: <https://www.securityweek.com/ics-patch-tuesday-siemens-issues-17-advisories-rockwell-fixes-armorblock-takeover-flaw/> ✓ geprüft

L-08 Cybervorfall bei Ahold Delhaize: Bestellungen und Belieferung von Albert Heijn, Delhaize und Food Lion gestört

MITTEL BleepingComputer / NL Times, 12.10.

Was ist neu: Ahold Delhaize hat am 12.10. ein „security issue within its network“ bestätigt und vorsorglich Systeme vom Netz genommen. Betroffen waren Websites, Apps und Kundenservice von Albert Heijn, Etos, Gall & Gall und Delhaize sowie Systeme bei Stop & Shop und Food Lion in den USA, den Niederlanden und Belgien. Die Filialen blieben offen. Ein internes Memo von Food Lion warnt, dass Bestellungen eventuell nicht übergeben werden können. Laut NL Times waren am 14.10. Frischeregale leer und der Regalnachschub gestört. Frischware, die nicht an die Filialen ging, wurde gespendet. Ursache und Täter sind unbekannt, Ransomware ist nicht bestätigt, und eine Gruppe hat sich bisher nicht bekannt (Relevanz widersprüchlich: A hoch / B mittel).

Bedeutung: Für Hersteller und Abfüller, die an Albert Heijn oder Delhaize liefern, kann so ein Ausfall heißen: Bestellte Frischware wird nicht abgerufen, und Lieferscheine, Abrechnung, Disposition und Kühlkettenlogistik stocken. Bei kurzen Haltbarkeiten wie bei Molkereiprodukten, Frischfleisch oder Backwaren wird daraus schnell Warenverlust. Dazu kommen Phishing-Mails im Namen des betroffenen Händlers.

Empfehlung: Im Incident-Response-Plan (CC1) einen Ablauf für den Ausfall großer Abnehmer festlegen: manuelle Bestellannahme, Ansprechpartner beim Händler, Lager- und Kühlkapazität für zurückgehaltene Ware, Umleitung von Frischware. Schnittstellen zu Handelskunden (EDI, Portale) auf ungewöhnliche Aktivität überwachen. Vertrieb und Buchhaltung vor gefälschten Zahlungs- und Bankdatenänderungen im Namen betroffener Händler warnen.

Quelle: <https://www.bleepingcomputer.com/news/security/retail-giant-ahold-delhaize-takes-systems-offline-after-cyberattack/> ✓ geprüft

L-09 Eclipse Milo: Lücken in OPC-UA-Server-Bibliothek (ICSA-26-288-01)

MITTEL CISA, 15.10.

Was ist neu: Die Java-Bibliothek Eclipse Milo hat in den Versionen 0.6.0 bis 1.1.4 Lücken auf der Serverseite. Möglich sind ein Absturz ohne Anmeldung (CVE-2026-63252), der Zugriff anonymer Clients auf geschützte Methoden (CVE-2026-58080, CVSS 3.1: 8,2) und das Zurückgewinnen von Passwörtern über ein Padding Oracle (CVE-2026-60007, CVSS 4.0: 9,1). Behoben ist das nur in 1.1.5, für den 0.6.x-Zweig gibt es keinen Patch. Der Kopf des Advisories nennt fünf Schwachstellen, der Text sechs CVEs (Frist widersprüchlich: A Quartal / B 2 Wochen).

Bedeutung: OPC UA verbindet in vielen Betrieben SPS und Linien mit MES, Rückverfolgung und Energiemonitoring. Milo steckt als Bibliothek in Gateways, MES-Konnektoren und Edge-Produkten, ohne dass der Betreiber es sieht. Stürzt der OPC-UA-Server ab, können Chargendaten und Rückverfolgbarkeit unterbrochen werden. CISA nennt die Lebensmittelbranche nicht ausdrücklich, betroffen ist aber jeder, der solche Produkte nutzt.

Empfehlung: Lieferanten von MES, Gateways, Leittechnik und Edge-Software schriftlich fragen, ob Milo in ihrer SBOM steckt und wann ein Update kommt (CC5). Anonyme OPC-UA-Sessions abschalten, wo der Betrieb es erlaubt, und OPC-UA-Verkehr im Monitoring sichtbar machen (CC3).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-288-01> ✓ geprüft

Fragen für das nächste Jour fixe

1. Welche Kälte-, Energie- und Haustechnik-Steuerungen haben wir (Danfoss, Copeland, Dixell, andere), wer wartet sie, ist eine davon aus dem Internet erreichbar, und wer hat das zuletzt geprüft?
2. Welche Dienstleister haben Fernzugang zu unseren Anlagen, über welchen Weg, und wird jede Sitzung protokolliert?
3. Wie lange dauert es, bis wir eine manipulierte Abtauzeit oder Solltemperatur bemerken, lösen unsere Temperaturalarme auch bei absichtlichen Änderungen aus, und wer bekommt den Alarm?
4. Wie schnell können wir eine aktiv ausgenutzte Lücke im VPN-Gateway schließen, und gibt es einen Ersatzweg für die Fernwartung?
5. Ist die Management-Oberfläche unserer Firewall zwischen IT und OT nur aus dem Admin-Netz erreichbar, und ist der PAN-OS-Patch eingespielt?
6. Was tun wir, wenn ein großer Handelskunde wie Ahold Delhaize mehrere Tage oder eine Woche lang keine Bestellungen abrufen?
7. Welche Lieferanten von MES, Gateways und Edge-Software haben uns eine SBOM geliefert?

Maßnahmen dieser Woche

1. Mit allen Kältedienstleistern klären, ob Danfoss AK-SC/AK-SM, Copeland xweb oder Dixell xweb im Einsatz sind. Alle Kälte- und Gebäudesteuerungen mit öffentlicher IP noch diese Woche vom Internet trennen. Zugriff des Dienstleisters nur noch per VPN mit MFA (CC4).
2. Die Prüfliste BSI-CS 154 für jede vernetzte Kälte- und Energieanlage durchgehen und die Ergebnisse mit Firmware-Stand ins Asset-Inventar übernehmen.

3. Konfiguration, Sollwerte, Alarmgrenzen und Abtaupläne der Kälteanlagen mit dem dokumentierten Soll abgleichen und Abweichungen klären.
4. Ivanti Connect Secure patchen, auf Kompromittierung prüfen und die Zugangsdaten tauschen, die über das Gateway genutzt werden.
5. PAN-OS-Firewalls an der IT/OT-Grenze patchen und die Management-Oberfläche auf ein Admin-Netz beschränken (CC2).
6. Rockwell 1732E ArmorBlock I/O sowie betroffene Siemens-S7-1500-, Industrial-Edge- und Schneider-HMI-Geräte im Asset-Inventar suchen und die Updates für das nächste Wartungsfenster einplanen (CC5).
7. Eine unabhängige Temperaturüberwachung mit eigenem Alarmweg für kritische Kühlräume prüfen, damit eine manipulierte Steuerung nicht unbemerkt bleibt (CC3).
8. Den Incident-Response-Plan um die Szenarien „Kühlkette manipuliert“ (Qualitätssicherung, Sperrung der Ware, Meldewege) und „Ausfall eines Großkunden“ ergänzen (CC1).

HINWEIS ZUR QUELLENLAGE

Alle Quellenlinks wurden am 16.10.2026 automatisch aufgerufen und inhaltlich geprüft.