OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Lebensmittel und Getränke

Ausgabe KW 45/2026 · Lebensmittel und Getränke in DACH

Zielgruppe	Lebensmittel- und Getränkehersteller, Abfüller, Molkereien, Brauereien
Berichtszeitraum	30.10.2026–06.11.2026
Version	1.0
Datum	06.11.2026
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 45 geht es um die Kühlkette. In der Nacht zum 2. November haben Angreifer zum zweiten Mal Kühlsteuerungen in Supermärkten in mehreren europäischen Ländern verstellt. In Deutschland sind laut dpa unter anderem Märkte in Wuppertal, Wetter bei Hagen und im Münsterland betroffen. Ein Markt in Lilienthal musste nach eigenen Angaben Ware im Wert von über 360.000 Euro wegwerfen. Mindestens ein deutscher Markt sagt, angegriffen worden sei eigentlich die Firma, die seine Kühlanlagen aus der Ferne wartet. In Italien meldet die Cyberbehörde ACN einen Angriff auf einen Hersteller von Tiefkühlkost in der Emilia-Romagna. Damit sind nicht mehr nur Händler betroffen, sondern auch Hersteller.

Am 5. November haben CISA, FBI, USDA, HHS und DOT eine gemeinsame Warnung veröffentlicht. Danach greifen Angreifer weltweit Kühlsteuerungen und Systeme zur Überwachung der Kühlkette an, die ungepatcht oder aus dem Internet erreichbar sind. Gemeint sind ausdrücklich auch Kühllager. Für Molkereien, Fleischverarbeiter, Tiefkühlhersteller und Getränkeabfüller mit eigener Kältetechnik heißt das: Diese Woche klären, welche Kältesteuerungen und Fernwartungszugänge von außen erreichbar sind und welche Dienstleister darauf zugreifen. Parallel dazu wird in Siemens-IoT2050-Gateways eine Node-RED-Lücke ausgenutzt, und Ivanti Connect Secure hat zwei ausgenutzte Lücken. Beides betrifft die Anbindung und den Fernzugang der Produktion.

GESAMTBEWERTUNG

Die Lage ist hoch: Angriffe auf Kältetechnik laufen weiter, reichen über Ländergrenzen und Branchen hinweg und laufen teilweise über Fernwartungsdienstleister. Vorrang hat, dass keine Kältesteuerung und kein Fernwartungszugang mehr direkt aus dem Internet erreichbar ist (CC4) und dass die Kühlkette unabhängig überwacht wird (CC3).

Trends

• Angriffe auf Kältetechnik weiten sich vom Handel auf Hersteller und Kühllager aus, Italien meldet einen Tiefkühlhersteller als Opfer.

• Fernwartungsdienstleister werden zum Einfallstor, über deren Zugang mehrere Kunden gleichzeitig erreichbar sind.

• Ausgenutzt werden meist einfache Fehler wie Erreichbarkeit aus dem Internet, Standardpasswörter und Geräte ohne Herstellersupport, kaum neue Zero-Days.

• Behörden in den USA, Frankreich und Italien geben nahezu gleiche Empfehlungen: vom Internet trennen, Fernzugriff nur über VPN mit MFA, Altgeräte ersetzen.

• Edge-Geräte zur Datenanbindung (IoT2050/Node-RED) und VPN-Gateways bleiben bevorzugte Ziele für den Erstzugriff.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	USA: Gemeinsame Behördenwarnung vor Angriffen auf Kühlsteuerungen und Kühlketten-Überwachung	KRITISCH	CISA (mit FBI, HHS, USDA, DOT), 05.11.

ID	Meldung	Relevanz	Quelle
L-02	Deutschland: Kühlanlagen in mehreren Supermärkten manipuliert, Angriff lief offenbar über den Fernwartungsdienstleister	HOCH	Tageskarte (dpa), 03.11.
L-03	Italien: ACN meldet Angriff auf Tiefkühl-Hersteller und Großküchen-Betreiber	HOCH	AGI, 02.11.
L-04	Zweite Angriffswelle auf Kühlsteuerungen in Europa: Danfoss nennt ungesicherte Netze und Standardpasswörter	HOCH	The Hacker News, 03.11.
L-05	Ivanti Connect Secure: Zwei ausgenutzte Lücken im KEV-Katalog (CVE-2026-111357, CVE-2026-118527)	MITTEL	CISA, 30.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 06.11.2026):

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	143185	DNP3: 32440, OMRON FINS: 26119, ProConOS: 16052, Siemens S7: 7764, OPC UA: 5141
Österreich	4790	HMI/VNC: 1046, DNP3: 970, Niagara Fox: 472, Siemens S7: 387, OPC UA: 158

Meldungen im Detail

L-01 USA: Gemeinsame Behördenwarnung vor Angriffen auf Kühlsteuerungen und Kühlketten-Überwachung

KRITISCH CISA (mit FBI, HHS, USDA, DOT), 05.11.

Was ist neu: CISA, FBI und drei Ministerien warnen gemeinsam, dass Angreifer weltweit ungepatchte oder aus dem Internet erreichbare elektronische Temperaturregler und gewerbliche Kühlsteuerungen angreifen. Genannt werden Lebensmittelhandel und Kühllager, als Folgen Brandgefahr, Warenverlust und eine kürzere Lebensdauer der Anlagen. Hersteller, Täter oder Vorfälle in den USA nennt die Warnung nicht, auch keinen Bezug zu den Angriffen in Europa.

Bedeutung: Die Warnung nennt ausdrücklich den Sektor Ernährung und Landwirtschaft und Kühllager. Damit betrifft sie Molkereien, Fleischverarbeiter, Tiefkühlhersteller und Getränkelogistik direkt. Fällt die Kühlung aus, muss Ware vernichtet werden, und es drohen Lieferausfälle beim Handel.

Empfehlung: Die Maßnahmen der Behörden umsetzen, vor allem: Geräte vom Internet trennen, OT in ein eigenes VLAN legen, Standardpasswörter ändern, patchen, Geräte ohne Herstellersupport ersetzen und Grenzwerte für Sollwerte mit Alarm festlegen. Fernzugriff nur über einen gesicherten Zugang mit MFA erlauben (CC4).

Quelle: https://www.cisa.gov/resources-tools/resources/us-government-partners-urge-hardening-industrial-refrigeration-and-cold-chain-monitoring-systems ✓ geprüft

L-02 Deutschland: Kühlanlagen in mehreren Supermärkten manipuliert, Angriff lief offenbar über den Fernwartungsdienstleister

HOCH Tageskarte (dpa), 03.11.

Was ist neu: Laut dpa wurden Kühlanlagen in Wuppertal, Wetter bei Hagen und im Münsterland vermutlich per Hackerangriff lahmgelegt. In Lilienthal bei Bremen fiel die Kühlkette zeitweise aus, laut Inhaber mussten Waren im Wert von über 360.000 Euro weggeworfen werden. Ein Markt in Wetter-Volmarstein sagt, eigentlich sei die Firma angegriffen worden, die die Anlagen aus der Ferne wartet.

Bedeutung: Hersteller und Abfüller lassen Kältetechnik, Verpackungslinien und Abfüllanlagen oft vom selben Typ Dienstleister fernwarten. Wird ein Dienstleister kompromittiert, kann der Angreifer über dessen Zugang mehrere Kunden gleichzeitig erreichen.

Empfehlung: Alle Fernwartungszugänge von Dienstleistern auflisten (Kälte, Abfüllung, Gebäudetechnik). Dauerverbindungen beenden und Zugriffe nur noch auf Freigabe, mit MFA und Protokoll erlauben (CC4).

Quelle: https://www.tageskarte.io/industrie/detail/cyberangriffe-auch-auf-kuehlanlagen-deutscher-supermaerkte.html ✓ geprüft

L-03 Italien: ACN meldet Angriff auf Tiefkühl-Hersteller und Großküchen-Betreiber

HOCH AGI, 02.11.

Was ist neu: Die italienische Cyberbehörde ACN hat einen Angriff auf ein Unternehmen in der Emilia-Romagna festgestellt, das Tiefkühlkost herstellt. Ein Unternehmen der Gemeinschaftsverpflegung aus der Toskana hat einen Vorfall nach NIS gemeldet. Die ACN fordert, Steuerungs- und Fernwartungssysteme auf Erreichbarkeit aus dem Internet zu prüfen und getrennt vom Firmennetz zu betreiben.

Bedeutung: Damit ist erstmals ein Lebensmittelhersteller in dieser Welle öffentlich als Ziel genannt. Wer Kältetechnik in der Produktion oder im Kühllager betreibt, gehört zum Ziel, nicht nur der Handel.

Empfehlung: Kältesteuerungen und Fernwartungs-Gateways in eine eigene Zone legen, getrennt vom Büronetz (CC2). Fernzugriff nur über VPN mit MFA, privilegierte Konten prüfen und nicht mehr unterstützte Geräte ersetzen.

Quelle: https://www.agi.it/cronaca/news/2026-11-02/cybersicurezza-allerta-acn-attacchi-filiera-39837420/ ✓ geprüft

L-04 Zweite Angriffswelle auf Kühlsteuerungen in Europa: Danfoss nennt ungesicherte Netze und Standardpasswörter

HOCH The Hacker News, 03.11.

Was ist neu: In der Nacht zum 2. November haben Angreifer Kühlsteuerungen in Supermärkten unter anderem in Belgien, Schweden und Estland aus der Ferne verstellt. Laut Danfoss lagen die betroffenen Systeme in den Niederlanden nicht in einem gesicherten Netz und liefen noch mit Standardpasswörtern. Am 3. November gab es laut The Hacker News noch kein Danfoss-Advisory zu den Angriffen.

Bedeutung: Danfoss-Systemmanager stehen auch in Kühlhäusern und Produktionsbetrieben. Ein fehlendes Herstelleradvisory bedeutet nicht, dass keine Gefahr besteht, denn ausgenutzt werden einfache Fehler: Erreichbarkeit aus dem Internet und Standardpasswörter.

Empfehlung: Alle Kältesteuerungen im Asset-Inventar erfassen, mit Firmware-Stand und Supportstatus. Standardpasswörter ersetzen und bei Danfoss-Geräten das Security Level auf Strict stellen, wie es CERT-FR empfiehlt (CC5).

Quelle: https://thehackernews.com/2026/11/second-wave-of-cyberattacks-hits.html ✓ geprüft

L-05 Ivanti Connect Secure: Zwei ausgenutzte Lücken im KEV-Katalog (CVE-2026-111357, CVE-2026-118527)

MITTEL CISA, 30.10.

Was ist neu: CISA hat am 30. Oktober CVE-2026-111357 und CVE-2026-118527 in Ivanti Connect Secure als aktiv ausgenutzt in den KEV-Katalog aufgenommen.

Bedeutung: Viele Hersteller nutzen Ivanti Connect Secure als VPN für Mitarbeitende und Dienstleister. Wird das VPN-Gateway übernommen, ist der Weg zu Fernwartungssystemen in der Produktion offen.

Empfehlung: Herstellerpatch einspielen, VPN-Logs auf Auffälligkeiten prüfen und die über das Gerät genutzten Zugangsdaten zurücksetzen (CC4, CC1).

Quelle: https://www.cisa.gov/news-events/alerts/2026/10/30/cisa-adds-two-known-exploited-vulnerabilities-catalog ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Kältesteuerungen und Fernwartung vom Internet trennen, Zugriff nur über gesicherten Fernzugang mit MFA [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Dienstleisterzugänge (Kälte, Abfüllung, Verpackung) inventarisieren, auf Freigabe umstellen und protokollieren [CC4 Secure Remote Access]	L-02	HOCH	sofort
M-03	Kälte- und Fernwartungssysteme in eigene Netzzone getrennt vom Büronetz legen [CC2 Defensible Architecture]	L-03	HOCH	0 bis 3 Monate
M-04	Asset-Inventar für Kältesteuerungen und Edge-Gateways mit Firmware- und Supportstatus aufbauen, Altgeräte ersetzen [CC5 Risk-Based Vulnerability Management]	L-04	MITTEL	0 bis 3 Monate
M-05	Unabhängige Temperaturüberwachung und Notfallablauf für Kühlausfall einrichten und üben [CC1 ICS Incident Response]	L-01	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Welche Kältesteuerungen und Temperaturüberwachungen haben wir, und ist eine davon aus dem Internet erreichbar?

2. Welche Dienstleister können per Fernwartung auf Kälte, Abfüllung oder Verpackung zugreifen, und wie ist das abgesichert?

3. Merken wir einen Temperaturanstieg im Kühllager auch dann, wenn die Steuerung selbst manipuliert ist (unabhängige Fühler, Alarm per SMS)?

4. Wie viele Stunden Ware können wir bei Kühlausfall retten, und wer entscheidet nachts über Notbetrieb und Vernichtung?

5. Sind IoT2050-Gateways und Ivanti-VPN im Einsatz, und sind sie gepatcht?

Maßnahmen dieser Woche

1. Externen Scan der eigenen IP-Bereiche auf Kältesteuerungen, Node-RED und Fernwartungsports durchführen, Treffer sofort sperren.

2. Standardpasswörter an Kältesteuerungen und Systemmanagern ersetzen, bei Danfoss das Security Level auf Strict stellen.

3. Kälte- und Anlagendienstleister schriftlich fragen, wie sie zugreifen, ob ihnen ein Vorfall bekannt ist und ob sie MFA nutzen. Dauerzugänge abschalten.

4. Unabhängige Temperaturalarmierung (separater Fühler, Meldung außerhalb der Steuerung) für Kühllager und Tiefkühlzellen prüfen.

5. IoT2050 auf V4.3.4-1 aktualisieren und Ivanti Connect Secure patchen, danach Logs und Zugangsdaten prüfen.

6. Notfallablauf für Kühlausfall üben: wer wird nachts gerufen, wie wird manuell auf sichere Werte zurückgestellt.

HINWEIS ZUR QUELLENLAGE

Primärquellen für die US-Behördenwarnung (CISA, 05.11.) und den KEV-Eintrag (CISA, 30.10.). Die Vorfälle in Deutschland und Italien stützen sich auf Agenturmeldungen (dpa, AGI), Täter und genauer Angriffsweg sind offen; die Zuschreibung an Iran (NPR, TechCrunch) ist laut US-Regierung nicht bestätigt und wurde nicht übernommen. Nicht aufgenommen, weil nicht prüfbar oder ohne Bestätigung: ein Danfoss-Advisory zur Welle (am 03.11. keines gefunden), eine Warnung von BSI oder NCSC Schweiz aus dieser Woche (nicht gefunden), Angriffe in Österreich (Spar Österreich erklärte am 03.11. nur, man rechne damit, ohne Fälle zu bestätigen) sowie Ransomware-Fälle bei Lebensmittelherstellern in DACH (keiner im Zeitraum gefunden); Phoenix Contact VDE-2026-121 (04.11.) betrifft Engineering-Software und steht im Branchenbericht Maschinenbau. Alle Quellenlinks wurden am 06.11.2026 automatisch aufgerufen und inhaltlich geprüft. 1 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.