OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Lebensmittel und Getränke

Ausgabe KW 48/2026 · Lebensmittel und Getränke in DACH

Zielgruppe	Lebensmittel- und Getränkehersteller, Abfüller, Molkereien, Brauereien
Berichtszeitraum	20.11.2026 bis 27.11.2026
Version	1.0
Datum	27.11.2026
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 48/2026 standen die Kühlanlagen der Lebensmittelkette im Mittelpunkt. Die CISA hat am 25.11.2026 drei Lücken in den Danfoss-Kühlstellen-Managern AK-SM 800A in ihren KEV-Katalog aufgenommen. Damit gelten sie als aktiv ausgenutzt. Schon am 24.11. hatte die CISA für dieselbe Gerätereihe eine weitere Lücke gemeldet, die sich ohne Login ausnutzen lässt (CVE-2026-129713, CVSS v3.1 9,8) und für die es noch keinen Patch gibt. Aus der Schweiz kommt ein Beispiel, das zeigt, was ein solcher Angriff anrichtet: In einer Berner Metzgerei stieg die Temperatur im Tiefkühler auf 50 bis 70 Grad. Wer bei sich Kühlräume, Tiefkühllager oder Abfüllkühlung über Fernwartung betreuen lässt, ist damit unmittelbar betroffen.

Auch an der Grenze zwischen IT und OT gibt es Handlungsbedarf. Palo Alto bestätigt Angriffe auf PAN-OS-Firewalls, deren Management-Oberfläche aus dem Internet erreichbar ist. Bei Siemens Industrial Edge sind fünf NGINX-Lücken offen, ein Fix fehlt noch. CODESYS Visualization ermöglicht Codeausführung auf dem Engineering-PC. Die Zahlen von Dragos für das dritte Quartal 2026 zeigen, wie sich die Lage verschärft: Die Ransomware-Fälle bei Lebensmittel- und Getränkeherstellern stiegen das dritte Quartal in Folge (57, 70, 90). Deutschland bleibt weltweit das am zweitstärksten betroffene Land.

GESAMTBEWERTUNG

Die Lage ist hoch, weil Kühlstellen-Manager nachweislich angegriffen werden und für eine neue Lücke noch kein Patch vorliegt. Vorrang hat in dieser Woche, alle aus dem Internet erreichbaren Kühlsteuerungen und Firewall-Managementzugänge zu finden und abzuschotten (CC4 Secure Remote Access).

Trends

• Kühlsteuerungen werden zum eigenen Angriffsziel: Nach den Wellen auf Supermärkte im Oktober und November führt die CISA jetzt Danfoss-Lücken als aktiv ausgenutzt.

• Mehrere Hersteller veröffentlichen kritische Lücken, bevor ein Patch da ist (Danfoss 5.5.x, Siemens Industrial Edge), deshalb schützen oft nur Abschottung und Segmentierung.

• Angreifer gehen über Edge-Geräte wie Firewall-Managementzugänge und VPN in die Unternehmen, und das führt bei Ransomware zum Stillstand der Produktion.

• Die Ransomware-Fälle bei Lebensmittel- und Getränkeherstellern steigen seit drei Quartalen, Deutschland ist überdurchschnittlich stark betroffen.

• Engineering-PCs und Laptops von Dienstleistern geraten selbst ins Visier, wie die CODESYS-Lücken zeigen.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Palo Alto PAN-OS: Angriffe auf Management-Oberflächen, die aus dem Internet erreichbar sind (PAN-SA-2026-0015)	HOCH	Palo Alto Networks, 25.11.
L-02	Danfoss AK-SM 8xxA: Lücke ohne Login, Patch erst mit Version 5.5.x (ICSA-26-328-03, CVE-2026-129713)	HOCH	CISA ICS Advisory, 24.11.

ID	Meldung	Relevanz	Quelle
L-03	Schweiz: Berner Metzgerei nach Angriff auf Kühlanlage, BACS sieht deutlichen Anstieg bei KRITIS-Angriffen	ORIENTIERUNG	watson.ch, 27.11.
L-04	Dragos Q3 2026: Ransomware bei Lebensmittel- und Getränkeherstellern steigt das dritte Quartal in Folge	ORIENTIERUNG	Dragos, 16.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 27.11.2026):

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	136005	DNP3: 31017, OMRON FINS: 24583, ProConOS: 15127, Siemens S7: 7537, OPC UA: 4801
Österreich	4553	HMI/VNC: 998, DNP3: 978, Niagara Fox: 435, Siemens S7: 367, OPC UA: 136

Meldungen im Detail

L-01 Palo Alto PAN-OS: Angriffe auf Management-Oberflächen, die aus dem Internet erreichbar sind (PAN-SA-2026-0015)

HOCH Palo Alto Networks, 25.11.

Was ist neu: Palo Alto bestätigt, dass die Kernel-Lücke CVE-2026-46300 („Fragnesia“) gegen die Management-Oberfläche von PAN-OS ausgenutzt wird. Behoben ist sie unter anderem in 10.2.7-h41, 11.1.4-h40, 12.1.4-h15, 12.2.4-h3 und allen späteren Versionen.

Bedeutung: Viele Lebensmittel- und Getränkehersteller trennen Büronetz und Produktion mit einer Firewall oder bieten darüber Remote Access für Maschinenbauer an. Wird diese Firewall übernommen, steht der Weg in die Produktion offen.

Empfehlung: Management-Zugriff nur von vertrauenswürdigen internen IP-Adressen erlauben und sofort auf eine behobene Version aktualisieren (CC2). War die Oberfläche offen, Logs auf Angriffsspuren durchsehen (CC1).

Quelle: https://security.paloaltonetworks.com/PAN-SA-2026-0015 ✓ geprüft

L-02 Danfoss AK-SM 8xxA: Lücke ohne Login, Patch erst mit Version 5.5.x (ICSA-26-328-03, CVE-2026-129713)

HOCH CISA ICS Advisory, 24.11.

Was ist neu: Die CISA meldet für AK-SM8xxA bis Version 5.4.0 die Lücke CVE-2026-129713 mit CVSS v3.1 9,8 und v4 9,3. Danfoss will sie mit Version 5.5.x beheben. Eine öffentliche Ausnutzung ist der CISA bisher nicht bekannt.

Bedeutung: Damit ist auch die aktuelle Firmware 5.4.0 betroffen, die das BSI Mitte November noch als Ausweg genannt hatte (laut Presseberichten, siehe Quellenlage). Bis zum Patch hilft nur Abschottung.

Empfehlung: Alle AK-SM-Geräte im Strict Mode betreiben, aus dem Internet nehmen und Zugriffe von Kältedienstleistern nur über ein VPN zulassen (CC4). Den Patch 5.5.x vormerken und gleich nach Erscheinen einspielen (CC5).

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-328-03 ✓ geprüft

L-03 Schweiz: Berner Metzgerei nach Angriff auf Kühlanlage, BACS sieht deutlichen Anstieg bei KRITIS-Angriffen

ORIENTIERUNG watson.ch, 27.11.

Was ist neu: Laut watson herrschten nach dem Angriff Anfang November im Tiefkühler einer Berner Metzgerei 50 bis 70 Grad. Der Betrieb meldete am 18. November auf seiner Webseite, dass er wieder geöffnet hat. Das BACS verzeichnet insgesamt einen deutlichen Anstieg meldepflichtiger Angriffe auf kritische Infrastrukturen.

Bedeutung: Der Fall zeigt, dass eine manipulierte Kühlsteuerung nicht nur zu Ausfällen führt, sondern gezielt Hitze erzeugen und so die ganze Ware zerstören kann. Für Molkereien und Fleischverarbeiter heißt das Totalverlust der gekühlten Ware und unter Umständen Fragen zur Lebensmittelsicherheit.

Empfehlung: Einen Temperaturalarm einrichten, der unabhängig von der Kühlsteuerung arbeitet (eigener Fühler, eigene Meldung), und einen Notfallablauf für den Kühlausfall üben (CC1, CC3).

Quelle: https://www.watson.ch/wirtschaft/digital/710558028-nach-cyberangriffen-gefahr-fuer-industrieanlagen-haelt-an ✓ geprüft

L-04 Dragos Q3 2026: Ransomware bei Lebensmittel- und Getränkeherstellern steigt das dritte Quartal in Folge

ORIENTIERUNG Dragos, 16.11.

Was ist neu: Dragos zählt im dritten Quartal 2026 weltweit 1.266 Ransomware-Fälle bei Industrieunternehmen. 876 davon (69 %) entfallen auf die Fertigung, davon 90 auf Lebensmittel und Getränke (nach 57 und 70 in den Vorquartalen). Deutschland ist mit 66 Fällen weiterhin das am zweitstärksten betroffene Land.

Bedeutung: Die Branche wird immer häufiger getroffen, und Deutschland steht weit oben. Nach Dragos erreichte im dritten Quartal kein Ransomware-Angreifer direkt die Steuerungen. Stillstände entstehen also meist über die IT.

Empfehlung: Im Notfallplan festlegen, ob und wie Abfüllung und Kühlung weiterlaufen, wenn ERP und Büro-IT ausfallen. Diesen Plan einmal pro Quartal durchspielen (CC1).

Quelle: https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3-2026 ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Firewall-Managementzugang zwischen IT und OT absichern und PAN-OS patchen (CC2)	L-01	HOCH	sofort
M-02	Danfoss-Patch 5.5.x und Siemens-Edge-Fixes vormerken und nach Risiko einplanen (CC5)	L-02	HOCH	0 bis 3 Monate
M-03	Unabhängiges Temperatur-Monitoring und Alarmierung für Kühl- und Tiefkühlräume aufbauen (CC3)	L-03	MITTEL	0 bis 3 Monate
M-04	Notfallplan für den Ausfall von Kühlung und ERP schreiben und einmal üben (CC1)	L-04	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Welche Kühlstellen-Manager (Danfoss oder andere) haben wir, und welcher Kältedienstleister erreicht sie auf welchem Weg?

2. Ist die Management-Oberfläche unserer Firewall zwischen IT und Produktion aus dem Internet erreichbar, und auf welchem Stand ist die Firmware?

3. Merken wir einen Temperaturanstieg im Kühl- oder Tiefkühlraum auch dann, wenn die Kühlsteuerung selbst manipuliert ist?

4. Welche Abfüll- und Verpackungsanlagen nutzen CODESYS, und wer pflegt die Engineering-PCs der Maschinenbauer?

5. Wie lange können wir abfüllen und ausliefern, wenn ERP und Büro-IT eine Woche ausfallen?

Maßnahmen dieser Woche

1. Alle Danfoss-AK-SM-Geräte und andere Kühlsteuerungen erfassen, Firmwarestand notieren und von außen auf Erreichbarkeit prüfen.

2. Direkte Portfreigaben für Kühlsteuerungen schließen und Fernwartung nur noch über ein VPN mit eigenem Konto pro Dienstleister erlauben.

3. Die PAN-OS-Management-Oberfläche auf interne IP-Adressen begrenzen, auf eine behobene Version aktualisieren und die Logs auf Auffälligkeiten prüfen.

4. Auf Siemens-Industrial-Edge-Geräten HTTP/2 und HTTP/3 per Reverse Proxy abschalten und den Netzzugang einschränken.

5. CODESYS Visualization auf 4.11.0.0 aktualisieren und von den Maschinenbauern bestätigen lassen, dass sie es auch tun.

6. Einen von der Kühlsteuerung unabhängigen Temperaturalarm für kritische Kühl- und Tiefkühlräume testen.

HINWEIS ZUR QUELLENLAGE

Leak-Site-Einträge aus dem Zeitraum zu HLB Tropical Food (Kelsterbach) und Meisterbäckerei Steinecke (je 23.11.), The Neil Jones Food Company und Fuji Food Products (je 25.11.) sowie Lowell Foods (23.11.) sind nicht bestätigt und wurden deshalb nicht aufgenommen. Die Danfoss-Lücke CVE-2026-127057 (Standard-Passwörter, 20.11.) ist nur über eine Sekundärquelle belegt, die Danfoss-Advisory war nicht abrufbar. Die BSI-Warnung zu Danfoss (13.11.) kenne ich nur aus der Presse, und der Dragos-Bericht (16.11.) erschien vor dem Berichtszeitraum. Er ist nur zur Orientierung aufgenommen. Ein Artikel von thedrinksbusiness.com zu Angriffen auf Lebensmittel- und Getränkebetriebe blockierte den Abruf (HTTP 403). Alle Quellenlinks wurden am 27.11.2026 automatisch aufgerufen und inhaltlich geprüft. 3 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.