OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Lebensmittel und Getränke

Ausgabe KW 46/2026 · Lebensmittel und Getränke in DACH

Zielgruppe	Lebensmittel- und Getränkehersteller, Abfüller, Molkereien, Brauereien
Berichtszeitraum	06.11.2026 bis 13.11.2026
Version	1.0
Datum	13.11.2026
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

Seit dem 06.11. drehte sich fast alles um die Kühlkette. Laut BleepingComputer (09.11.) ordnet Frankreich die Angriffe vom Oktober auf Danfoss-Kühlsteuerungen in rund 700 angegriffenen Supermärkten und anderen Geschäften einer Einheit zu, die den iranischen Revolutionsgarden nahesteht. Die spätere Welle im November in sechs europäischen Ländern ist nicht zugeordnet. Unit 42 hat am 5. und 6.11. über 5.000 aus dem Internet erreichbare Geräte der Hersteller gezählt, die CERT-FR im Oktober genannt hat (Bericht vom 06.11.). Unsere Einschätzung: Wer Kältetechnik fernwartbar betreibt, muss auch mit staatlichen Akteuren rechnen. Für Molkereien, Fleischverarbeiter und Kühlhäuser ist das die wichtigste Meldung der Woche. Einen bestätigten Ransomware-Fall mit Produktionsstillstand bei einem Lebensmittel- oder Getränkehersteller in DACH haben wir für den Zeitraum nicht gefunden.

Bei der Fernwartung kamen mehrere Lücken zusammen: Die CISA führt seit dem 06.11. eine SonicWall-SSL-VPN-Lücke als aktiv ausgenutzt (CVE-2026-19868). Das Fernwartungsportal mbCONNECT24 hat zwei PHP-Lücken mit Remote Code Execution ohne Anmeldung (CVSS 3.1: 9,8 und 8,1). Für den Graphics Designer in Siemens WinCC V7.5 bis V8.1 gibt es eine Lücke, die beim Öffnen präparierter Dateien Code ausführt, und noch keinen Fix.

GESAMTBEWERTUNG

Die Lage ist erhöht: Frankreich schreibt die Oktober-Angriffe auf Kühlsteuerungen in französischen Geschäften einem staatlichen Akteur zu, und mehrere Fernwartungszugänge (SonicWall-VPN, Portal mbCONNECT24) haben kritische Lücken. Vorrang haben Remote Access (CC4) und das Abschotten der Kältetechnik vom Internet (CC2).

Trends

• Angriffe auf Kältetechnik werden jetzt einem staatlichen Akteur zugeordnet, die Kühlkette wird damit ein geopolitisches Ziel.

• Fernwartungsportale der Maschinenbauer (mbCONNECT24, myREX24) häufen kritische Lücken, das Risiko liegt oft beim Lieferanten und nicht im eigenen Netz.

• Alte Bibliotheken in Industrieprodukten, hier PHP2Shell, kommen über Wochen bei immer mehr Herstellern als eigene Advisories an.

• Nach unserer Einschätzung kommen Angreifer eher über Dienstleister und VPN-Zugänge als direkt über die SPS, diese Woche zeigt das die SonicWall-Meldung der CISA.

• Nach öffentlichen Warnungen sinkt die Zahl der offenen Geräte schnell, wie Frankreich zeigt. Abschalten wirkt also.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Kühlanlagen-Angriffe: Frankreich macht eine IRGC-nahe Einheit verantwortlich	HOCH	BleepingComputer, 09.11.
L-02	Unit 42: über 5.000 Geräte der in der CERT-FR-Warnung genannten Hersteller offen im Internet	HOCH	Unit 42 (Palo Alto Networks), 06.11.

ID	Meldung	Relevanz	Quelle
L-03	SonicWall SonicOS SSL-VPN: CVE-2026-19868 aktiv ausgenutzt (CISA KEV)	HOCH	CISA, 06.11.
L-04	MB connect line mbCONNECT24: Remote Code Execution ohne Anmeldung über gebündeltes PHP (VDE-2026-128, CVSS 9,8)	KRITISCH	MB connect line, koordiniert von CERT@VDE, 10.11.
L-05	Siemens SIMATIC WinCC Graphics Designer: Code-Ausführung über präparierte Datei, noch kein Fix (SSA-979641)	MITTEL	Siemens ProductCERT, 10.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 13.11.2026):

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	139840	DNP3: 31446, OMRON FINS: 26419, ProConOS: 15503, Siemens S7: 7574, OPC UA: 4952
Österreich	4663	HMI/VNC: 1007, DNP3: 959, Niagara Fox: 456, Siemens S7: 381, OPC UA: 149

Meldungen im Detail

L-01 Kühlanlagen-Angriffe: Frankreich macht eine IRGC-nahe Einheit verantwortlich

HOCH BleepingComputer, 09.11.

Was ist neu: Frankreich ordnet die Angriffe vom Oktober auf Danfoss-Kühlsteuerungen in rund 700 angegriffenen Supermärkten und anderen Geschäften der Einheit Shahid Kaveh zu, die den iranischen Revolutionsgarden nahesteht. Den Angriffen werden mindestens 15 Brände zugeschrieben. Frankreich will den iranischen Botschafter einbestellen und neue EU-Sanktionen vorschlagen. Die spätere Welle im November mit über 115 Geschäften in sechs europäischen Ländern ist nicht zugeordnet.

Bedeutung: Laut französischer Zuordnung hat ein staatlicher Akteur gezeigt, dass er Kühlsteuerungen aus der Ferne umstellen kann. Diese Steuerungen sitzen nicht nur im Handel, sondern auch in Kühlräumen von Molkereien, Fleischbetrieben und Logistikern. Ein manipulierter Abtauzyklus über Nacht kann eine ganze Charge vernichten.

Empfehlung: Alle Kühlsteuerungen mit Fernzugang erfassen, öffentliche IP-Adressen abschalten und den Zugang nur noch über ein abgesichertes VPN mit MFA erlauben. Temperaturalarme so einstellen, dass auch nachts jemand reagiert.

Quelle: https://www.bleepingcomputer.com/news/security/france-blames-iranian-hackers-for-supermarket-attacks-that-sparked-fires/ ✓ geprüft

L-02 Unit 42: über 5.000 Geräte der in der CERT-FR-Warnung genannten Hersteller offen im Internet

HOCH Unit 42 (Palo Alto Networks), 06.11.

Was ist neu: Unit 42 hat am 5. und 6.11. über 5.000 aus dem Internet erreichbare Geräte der Hersteller gezählt, die CERT-FR im Vormonat genannt hat. Erreichbar heißt laut Unit 42 nicht automatisch, dass verwundbare Software läuft. Die Zählung liegt zum Teil vor dem Berichtszeitraum, der Bericht erschien am 06.11.

Bedeutung: Jede dieser Steuerungen ist ein mögliches Ziel für dieselbe Methode, egal wer hinter der Kampagne steht. Nach unserer Einschätzung stehen solche Geräte auch in Kühlräumen von Lebensmittelbetrieben in DACH.

Empfehlung: Öffentliche IP-Adressen der Standorte auf erreichbare Kälte-Weboberflächen prüfen lassen und gefundene Geräte hinter ein VPN mit MFA legen (CC2, CC4).

Quelle: https://unit42.paloaltonetworks.com/europes-refrigeration-systems-attacks/ ✓ geprüft

L-03 SonicWall SonicOS SSL-VPN: CVE-2026-19868 aktiv ausgenutzt (CISA KEV)

HOCH CISA, 06.11.

Was ist neu: Die CISA hat am 06.11. CVE-2026-19868 in SonicOS SSLVPN („Use of Single-factor Authentication“) in den KEV-Katalog aufgenommen, weil es Belege für aktive Ausnutzung gibt. Betroffene Versionen nennt die Meldung nicht.

Bedeutung: Viele Lebensmittelbetriebe nutzen SonicWall als VPN-Gateway, auch für Maschinenlieferanten. Ein übernommener VPN-Zugang ist ein direkter Initial Access ins Firmennetz und je nach Segmentierung bis in die Produktion.

Empfehlung: Herstellerhinweis zu CVE-2026-19868 lesen und patchen, phishing-resistente MFA am SSL-VPN erzwingen und die VPN-Logs der letzten Wochen auf Anmeldungen zu ungewöhnlichen Zeiten oder aus fremden Ländern prüfen (CC4).

Quelle: https://www.cisa.gov/news-events/alerts/2026/11/06/cisa-adds-one-known-exploited-vulnerability-catalog ✓ geprüft

L-04 MB connect line mbCONNECT24: Remote Code Execution ohne Anmeldung über gebündeltes PHP (VDE-2026-128, CVSS 9,8)

KRITISCH MB connect line, koordiniert von CERT@VDE, 10.11.

Was ist neu: mbCONNECT24 und mymbCONNECT24 ab Version 2.0.0 und vor 2.21.6 enthalten ein PHP mit CVE-2026-109618 (CVSS 3.1: 9,8) und CVE-2026-109619 (CVSS 3.1: 8,1). Laut Advisory können beide Lücken zu Remote Code Execution ohne Anmeldung führen. Behoben ist das in Version 2.21.6. Eine Ausnutzung meldet das Advisory nicht.

Bedeutung: Über so ein Portal warten Maschinenlieferanten Abfüllanlagen, Verpackungsmaschinen und Kältetechnik. Wer das Portal übernimmt, kommt im schlimmsten Fall an alle angebundenen Anlagen.

Empfehlung: Maschinenlieferanten mit Fernzugang schriftlich nach Portal und Version fragen und 2.21.6 bestätigen lassen. Bis dahin die Verbindung nur bei Bedarf freischalten (CC4).

Quelle: https://certvde.com/en/advisories/VDE-2026-128/ ✓ geprüft

L-05 Siemens SIMATIC WinCC Graphics Designer: Code-Ausführung über präparierte Datei, noch kein Fix (SSA-979641)

MITTEL Siemens ProductCERT, 10.11.

Was ist neu: CVE-2026-59082 (CVSS 3.1: 7,8) betrifft den Graphics Designer in SIMATIC WinCC V7.5, V8.0 und V8.1, jeweils alle Versionen. Wer eine präparierte Datei öffnet, kann Code ausführen. Laut Siemens gibt es derzeit keinen Fix, er ist in Vorbereitung.

Bedeutung: WinCC steuert in vielen Molkereien, Brauereien und Abfüllbetrieben die Visualisierung. Projektdateien kommen oft per Mail oder USB vom Integrator, eine einzige manipulierte Datei reicht dann für die Code-Ausführung auf dem Engineering-PC.

Empfehlung: Projektdateien von außen nur aus bekannten Quellen und nach Prüfung öffnen. Engineering-Stationen ohne Mail- und Internetzugang betreiben (CC2) und den Fix einplanen, sobald Siemens ihn veröffentlicht.

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-979641.html ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Kühlsteuerungen vom Internet trennen und Zugang nur über VPN mit MFA erlauben, Sollwert-Alarme scharf schalten [CC2 Defensible Architecture]	L-01	HOCH	sofort
M-02	SonicWall-SSL-VPN patchen, phishing-resistente MFA erzwingen und Patchstand der Fernwartungsportale (mbCONNECT24 2.21.6) bei den Lieferanten abfragen [CC4 Secure Remote Access]	L-03	HOCH	sofort
M-03	Engineering-PCs mit WinCC von Mail und Internet trennen und Projektdateien nur über einen festen Übergabeweg annehmen [CC2 Defensible Architecture]	L-05	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Welche Kühlsteuerungen haben wir, wer kommt von außen darauf, und läuft das über VPN mit MFA?

2. Über welche Portale (mbCONNECT24, myREX24, andere) warten unsere Maschinenlieferanten, und sind diese Portale aktualisiert?

3. Setzen wir SonicWall-SSL-VPN ein, und hat jemand die Anmeldungen der letzten 30 Tage angesehen?

4. Wie kommen Projektdateien für WinCC zu uns, und wer darf sie auf dem Engineering-PC öffnen?

5. Wer wird nachts alarmiert, wenn ein Kühlraum über den Grenzwert steigt, und was tut diese Person dann?

Maßnahmen dieser Woche

1. Öffentliche IP-Adressen des Werks von außen auf erreichbare Weboberflächen von Kälte-, Gebäude- und Fernwartungstechnik prüfen lassen.

2. SonicWall-Firewalls patchen und SSL-VPN nur mit zweitem Faktor zulassen.

3. Allen Maschinenlieferanten mit Fernzugang eine kurze Abfrage schicken: Portal, Version, Update-Stand mbCONNECT24 2.21.6 bzw. myREX24 2.21.0.

4. Sollwert-Grenzen und Temperaturalarme an Kühlräumen prüfen und eine Nachtalarmierung testen.

5. Engineering-PCs mit WinCC V7.5 bis V8.1 von Mail und Internet trennen und einen festen Übergabeweg für Projektdateien festlegen.

6. Dienstleister mit Kundendaten (Reservierung, Webshop) auflisten und Meldewege für Vorfälle abfragen.

HINWEIS ZUR QUELLENLAGE

Primärquellen liegen vor für CISA, Siemens, CERT@VDE und MB connect line. Die Zuordnung Frankreichs ist nur über die Presse (BleepingComputer) belegt, die Erklärung des Außenministeriums haben wir nicht gefunden. Das US-Fact-Sheet zu Kühlanlagen (CISA u. a., 05.11.) und die Kühlanlagen-Fälle in deutschen Supermärkten (Bericht vom 03.11.) liegen vor dem Zeitraum und fehlen deshalb. Nicht bestätigt und nicht aufgenommen: der Eintrag zum Gräflichen Hofbrauhaus Freising (Gruppe Lamashtu, 22.10.) auf einer Angriffsliste, Opferlisten auf ransomware.live mit widersprüchlichen Daten, die Schließung einer Metzgerei-Filiale in Köniz (ohne klares Datum). Alle Quellenlinks wurden am 13.11.2026 automatisch aufgerufen und inhaltlich geprüft. Vier zunächst aussortierte Meldungen (SonicWall, mbCONNECT24, Unit 42, WinCC) haben wir am 13.11. an den Primärquellen nachgeprüft und aufgenommen. Helmholz myREX24V2 steht im Bericht für Maschinenbau. Den Fall Union Brauerei Bremen haben wir nicht in einer Primärquelle gefunden, er ist gestrichen.