

WOCHENBERICHT

OT-/Cyber-Lagebild Lebensmittel und Getränke

Ausgabe KW 43/2026 · Lebensmittel und Getränke in DACH

Zielgruppe	Lebensmittel- und Getränkehersteller, Abfüller, Molkereien, Brauereien
Berichtszeitraum	16.10.2026–23.10.2026
Version	1.0
Datum	23.10.2026
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

Die Woche stand im Zeichen der Nachwirkungen des Angriffs auf Kühlsteuerungen in Hunderten französischer Supermärkte. Laut AP (16.10.) hielt die französische Cybersicherheitsbehörde die Angriffe für wahrscheinlich noch andauernd; Europol steht mit Behörden in den betroffenen Ländern in Kontakt. Ein bestätigter Fall in Deutschland ist uns nicht bekannt. Das Risiko betrifft ältere, nicht mehr gepflegte oder offen aus dem Internet erreichbare Fernwartungsmodule von Kälteanlagen; nach unserer Einschätzung kann das auch Kühllhäuser, Tiefkühlager, Molkereien und Brauereien betreffen. Danfoss zufolge waren in Frankreich vor allem ältere Produkte ohne Updates betroffen.

Für die Produktion ist ein CISA-Advisory vom 22.10. zu Siemens am wichtigsten: Acht CVEs im Webserver von SIMATIC S7-1500 und ET 200SP (Typen laut CISA: Eval Injection und Cross-Site Scripting), betroffen sind zahlreiche Produkte in allen Versionen, und für einen großen Teil der Produkte gibt es noch keinen Fix; Siemens bereitet Fixes vor und empfiehlt bis dahin Gegenmaßnahmen. Angreifer können damit SPS-Operationen im Rahmen der Rechte des angemeldeten Nutzers ausführen. Am 20.10. haben FBI, CISA, US Secret Service, LKA Rheinland-Pfalz sowie die britische National Crime Agency und die North West Regional Organised Crime Unit vor der Ransomware-Gruppe SafePay gewarnt (seit August 2024 mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur betroffen). SafePay kommt laut Advisory über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing herein.

Ahold Delhaize hat nach einem Cyberangriff Systeme in den USA und Europa vorsorglich vom Netz genommen; die Läden blieben geöffnet (The Register, 19.10.). Einen Täter nennt die Quelle nicht.

GESAMTBEWERTUNG

Die Lage ist erhöht. Kühlketten mit offen erreichbarer Fernwartung werden nach Einschätzung der französischen Behörde wahrscheinlich weiter angegriffen, und für einen großen Teil einer weit verbreiteten SPS-Familie gibt es noch keinen Fix. Vorrang haben das Abschotten von Kälte- und SPS-Webzugängen und MFA auf allen VPN-Zugängen.

Trends

- Angreifer zielen auf die Kühlkette und nicht auf Daten: In Frankreich wurden Sollwerte manipuliert, ohne Lösegeldforderung und ohne Bekennerschreiben (<https://www.euronews.com/2026/10/14/thousands-of-supermarket-fridges-still-exposed-after-cyberattack>).
- Offen erreichbare Fernwartung von Altgeräten ohne Sicherheitsupdates ist nach unserer Einordnung ein häufiger Einstieg; laut AP sagt Danfoss, betroffen seien in Frankreich vor allem ältere Produkte ohne Updates.
- Ransomware-Gruppen wie SafePay kommen laut Advisory über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing herein; nach unserer Einordnung betreffen die genannten CVEs u. a. VPN-Systeme und Veeam Backup, also Systeme, die in vielen Mittelständlern niemand überwacht.
- Die Branche bleibt im Fokus: Für das erste Halbjahr 2026 meldet das Food and Ag-ISAC laut Fachpresse 227 Ransomware-Vorfälle gegen 140 im Vorjahreszeitraum, Fairlife (Coca-Cola) musste im Juli die US-Produktion stoppen (<https://www.foodnavigator.com/Article/2026/08/03/cybercrime-escalates-across-the-food-and-beverage-industry/>).

- Für SPS-Schwachstellen gibt es oft erst Wochen später einen Patch, daher hängt der Schutz in der Zwischenzeit an der Segmentierung.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver, für viele Produkte noch kein Fix (ICSA-26-295-14)	HOCH	CISA ICS Advisory / Siemens, 22.10.
L-02	Angriffe auf Kühlsteuerungen: französische Behörde hält sie für wahrscheinlich andauernd, Europol in Kontakt mit Behörden	HOCH	Insurance Journal (Agenturmeldung), Euronews, 16.10.
L-03	Behörden aus den USA, Deutschland und Großbritannien warnen vor SafePay-Ransomware (AA26-293A)	HOCH	CISA Joint Cybersecurity Advisory, 20.10.
L-04	Ahold Delhaize: Systeme in Europa und den USA nach Cyberangriff vorsorglich vom Netz genommen	MITTEL	The Register, 19.10.
L-05	BeyondTrust Remote Support: Zero-Day vor der Veröffentlichung ausgenutzt, Mandiant sieht mutmaßlich China-nahen Spionageakteur	MITTEL	The Record, 18.10.
L-06	Eclipse Milo: sechs CVEs (der Kopf des CISA-Advisorys nennt fünf) in der OPC-UA-Bibliothek, für 0.6.x keine Releases mit Fix (ICSA-26-288-01)	ORIENTIERUNG	CISA ICS Advisory, 15.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 23.10.2026):

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	144393	DNP3: 33922, OMRON FINS: 24335, ProConOS: 16607, Siemens S7: 8039, OPC UA: 5548
Österreich	4715	HMI/VNC: 1070, DNP3: 969, IEC-104: 455, Siemens S7: 365, OPC UA: 141

Meldungen im Detail

L-01 Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver, für viele Produkte noch kein Fix (ICSA-26-295-14)

HOCH CISA ICS Advisory / Siemens, 22.10.

Was ist neu: CVE-2026-63350 bis CVE-2026-63357, acht CVEs (Typen laut CISA: Eval Injection und Cross-Site Scripting), betreffen zahlreiche Produkte aus den Familien S7-1500, ET 200SP, ET 200pro, Drive Controller und S7-PLCSIM Advanced, jeweils in allen Versionen. CISA nennt CVSS v3 bis 9,6. Möglich sind Angriffe im Browser des Nutzers (Cross-Site Scripting); der Angreifer kann danach SPS-Operationen im Rahmen der Rechte dieses Nutzers ausführen. Siemens rät u. a., nur vertrauenswürdige Trace-Dateien hochzuladen.

Bedeutung: Die S7-1500 steckt in vielen Abfüllanlagen, Molkereien und Brauhäusern in DACH. Ein Fix ist laut Siemens in Arbeit, ein Datum gibt es nicht; bis dahin empfiehlt Siemens Mitigations. Nach unserer Einordnung betrifft das typischerweise Engineering- und Service-PCs, deren Browser auf den SPS-Webserver zugreifen.

Empfehlung: Im Asset-Inventar alle S7-1500/ET 200SP mit aktivem Webserver erfassen, den Webserver abschalten, wo er nicht gebraucht wird, und sonst den Zugriff auf Ports 80/443 auf feste Engineering-IPs begrenzen (CC2). Trace-Dateien nur aus eigener, geprüfter Quelle importieren, auch nicht von Servicetechnikern per USB.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-14> ✓ geprüft

L-02 Angriffe auf Kühlsteuerungen: französische Behörde hält sie für wahrscheinlich andauernd, Europol in Kontakt mit Behörden

HOCH Insurance Journal (Agenturmeldung), Euronews, 16.10.

Was ist neu: Laut AP (16.10.) hielt die französische Cybersicherheitsbehörde die Angriffe für wahrscheinlich noch andauernd; Europol steht mit Behörden in den betroffenen Ländern in Kontakt, nennt aber keine Details. Laut AP meldete die französische Cybersicherheitsbehörde zahlreiche Kompromittierungen von Fernsteuermodulen für Kälteanlagen von Danfoss und Copeland; Danfoss zufolge waren in Frankreich vor allem ältere Produkte ohne Updates betroffen.

Bedeutung: Gefährdet sind ältere, nicht mehr gepflegte oder offen aus dem Internet erreichbare Fernwartungsmodule von Kälteanlagen. Nach unserer Einschätzung kann das auch Kühlhäuser, Reifekeller, Tiefkühlager und die Kälte von Molkereien betreffen. Oft hat der Kältedienstleister die Fernwartung eingerichtet, und der Betreiber weiß nichts davon. In Frankreich verdarb Ware in Millionenhöhe, weil die Sollwerte nachts auf bis zu 50 °C gesetzt wurden.

Empfehlung: Beim Kältedienstleister schriftlich abfragen, welche Steuerungen aus dem Internet erreichbar sind. Direkte Zugänge schließen und durch VPN mit MFA ersetzen (CC4). Bei Danfoss den Strict Security Mode aktivieren und Standardpasswörter ändern, für Altgeräte ohne Updates den Austausch planen.

Quelle: <https://www.insurancejournal.com/news/international/2026/10/16/889220.htm> ✓ geprüft

L-03 Behörden aus den USA, Deutschland und Großbritannien warnen vor SafePay-Ransomware (AA26-293A)

HOCH CISA Joint Cybersecurity Advisory, 20.10.

Was ist neu: Laut Advisory sind seit August 2024 mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur von SafePay betroffen. Der Initial Access läuft laut Advisory über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing. Genannt werden CVE-2020-3259, CVE-2023-20269, CVE-2023-27532, CVE-2024-40711 und CVE-2024-40766; nach unserer Einordnung betreffen sie u. a. VPN-Systeme und Veeam Backup. Die Ermittlungen führten FBI, USSS und das LKA Rheinland-Pfalz. Herausgeber sind FBI, CISA, US Secret Service, LKA Rheinland-Pfalz sowie die britische National Crime Agency und die North West Regional Organised Crime Unit.

Bedeutung: Mittelständische Hersteller mit einer Firewall, einem VPN-Zugang für Wartungsfirmen und einem Veeam-Backup passen nach unserer Einordnung in dieses Muster. Lebensmittel nennt das Advisory nicht ausdrücklich. Dass ein deutsches LKA mitzeichnet, zeigt aber den DACH-Bezug. Ein Ransomware-Angriff auf IT-Systeme legt in der Lebensmittelproduktion oft auch die Produktion still, weil Rezepturen, Chargenrückverfolgung und Etiketten am MES und ERP hängen.

Empfehlung: VPN-Konten ohne MFA heute auflisten und abstellen, Veeam (CVE-2023-27532, CVE-2024-40711) und die Firewall auf den Patchstand prüfen (CC5). Offline-Backup der Rezeptur- und MES-Daten testen.

Quelle: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a> ✓ geprüft

L-04 Ahold Delhaize: Systeme in Europa und den USA nach Cyberangriff vorsorglich vom Netz genommen

MITTEL The Register, 19.10.

Was ist neu: Ahold Delhaize hat nach einem Cyberangriff Systeme in den USA und Europa vorsorglich vom Netz genommen; die Läden blieben geöffnet (The Register, 19.10.). Einen Täter nennt die Quelle nicht.

Bedeutung: Für Lieferanten des Handels zeigt der Fall, dass ein Angriff beim Abnehmer Bestellungen und Abrufe stören kann. Ob Lieferanten-Schnittstellen betroffen waren, nennt der Bericht nicht. Bei Frischware und kurzen MHD wirkt jede Verzögerung sofort.

Empfehlung: Im Incident-Response-Plan festlegen, wie bei Ausfall eines großen Handelskunden Bestellungen manuell abgewickelt und Frischware umgeleitet werden (CC1). Kontaktwege zum Einkauf des Kunden außerhalb von E-Mail und Portal hinterlegen.

Quelle: <https://www.theregister.com/security/2026/10/19/grocery-giant-ahold-delhaize-confirms-cyberattack-forced-us-and-european-systems-offline/5303970> ✓ geprüft

L-05 BeyondTrust Remote Support: Zero-Day vor der Veröffentlichung ausgenutzt, Mandiant sieht mutmaßlich China-nahen Spionageakteur

MITTEL The Record, 18.10.

Was ist neu: Laut The Record ordnet Mandiant die Angriffe der Gruppe Armory Castle (UNC5221) zu, einem mutmaßlich China-nahen Spionageakteur. Die Lücke wurde vor der Veröffentlichung ausgenutzt. Sie wurde am 15.10. veröffentlicht, am 16.10. in den KEV-Katalog aufgenommen, CVSS 4.0 9,3. Mandiant beobachtete den Versuch, den Credential Vault auszulesen; die Angreifer bleiben auch nach Neustart oder Zurücksetzen der Konfiguration im System. Mandiant rät laut Rapid7, vor Änderungen Beweise zu sichern, verdächtige Appliances zu isolieren und sie aus einem sauberen, gepatchten Image neu aufzubauen, wenn eine Kompromittierung bestätigt ist oder sich nicht ausschließen lässt. Rapid7 empfiehlt, auch nach dem Patch auf Kompromittierung zu prüfen.

Bedeutung: Wo BeyondTrust als Fernwartungszugang genutzt wird, liegen dort oft Zugangsdaten zu Jump Hosts oder HMI. Laut The Record konnten die Angreifer auf der Appliance gespeicherte Zugangsdaten abgreifen; nach unserer Einschätzung sollten diese nach dem Patch gewechselt werden.

Empfehlung: Klären, ob die eigene Firma oder ein Dienstleister BeyondTrust selbst betreibt. Falls ja, alle dort gespeicherten Zugangsdaten wechseln, auch die zu OT-Jump-Hosts (CC4).

Quelle: <https://therecord.media/beyond-trust-cyberattack-china> ✓ geprüft

L-06 Eclipse Milo: sechs CVEs (der Kopf des CISA-Advisorys nennt fünf) in der OPC-UA-Bibliothek, für 0.6.x keine Releases mit Fix (ICSA-26-288-01)

ORIENTIERUNG CISA ICS Advisory, 15.10.

Was ist neu: Die Java-Bibliothek Eclipse Milo ist in den Versionen 0.6.0 bis 1.1.4 von sechs CVEs betroffen (der Kopf des CISA-Advisorys nennt fünf): Der Server kann nicht mehr antworten (Denial of Service), außerdem können Angreifer laut CISA geschützte Daten löschen, Zugangsdaten auslesen und sich als legitime Nutzer ausgeben. Behoben ab Version 1.1.5; für 0.6.x gibt es keinen Fix, nötig ist der Umstieg auf 1.1.5 oder neuer. CISA nennt die Sektoren Chemie, kritische Fertigung, Energie sowie Wasser und Abwasser. Das Advisory wurde am 15.10. veröffentlicht.

Bedeutung: OPC UA verbindet in vielen Betrieben Linien mit MES und Chargenrückverfolgung. Steckt Milo in einem Gateway, kann ein Denial of Service die Datenerfassung einer Linie unterbrechen.

Empfehlung: Lieferanten von MES-Konnektoren und Edge-Gateways nach Milo in der SBOM fragen und anonyme OPC-UA-Sessions abschalten (CC5).

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

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Webserver der S7-1500/ET 200SP abschalten oder per Firewall auf Engineering-IPs begrenzen, bis Siemens den Patch liefert [CC2 Defensible Architecture]	L-01	HOCH	sofort

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-02	Fernzugänge zu Kälteanlagen inventarisieren, direkte Internetzugänge schließen und über VPN mit MFA führen [CC4 Secure Remote Access]	L-02	HOCH	sofort
M-03	MFA auf allen VPN-Zugängen erzwingen und Edge Devices sowie Backup-Server nach KEV-Liste patchen [CC5 Risk-Based Vulnerability Management]	L-03	HOCH	0 bis 3 Monate
M-04	Incident-Response-Plan um Szenarien für Ausfall des Großkunden und Manipulation der Kühltemperatur ergänzen und einmal üben [CC1 ICS Incident Response]	L-04	MITTEL	0 bis 3 Monate
M-05	Temperatur- und Sollwertänderungen an Kälte und SPS zentral protokollieren und nachts alarmieren [CC3 ICS Network Visibility & Monitoring]	L-02	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Welche Kälteanlagen und Kühlhäuser sind heute direkt oder über den Kältedienstleister aus dem Internet erreichbar, und wer hat die Zugänge eingerichtet?
2. Bei welchen S7-1500/ET 200SP in Abfüllung und Prozess ist der Webserver aktiv, und wer braucht ihn wirklich?
3. Haben alle VPN-Zugänge, auch die von Maschinenbauern und Wartungsfirmen, MFA?
4. Wie lange können wir ohne MES und ERP produzieren und chargengenau etikettieren?
5. Was tun wir, wenn ein großer Handelskunde drei Tage keine Bestellungen übermitteln kann?

Maßnahmen dieser Woche

1. Mit Shodan oder dem eigenen Dienstleister prüfen, ob Kältesteuern (Danfoss AK-SM/AK-SC, Copeland xweb) aus dem Internet erreichbar sind, und diese Zugänge schließen.
2. Liste aller S7-1500/ET 200SP mit aktivem Webserver erstellen, Webserver abschalten oder auf Engineering-IPs begrenzen.
3. Alle VPN-Konten ohne MFA sperren oder nachrüsten, Firewall und Veeam auf die im SafePay-Advisory genannten CVEs prüfen.
4. Bei Maschinenbauern und IT-Dienstleistern abfragen, ob sie BeyondTrust nutzen und ob dort eigene Zugangsdaten gespeichert sind.
5. Temperaturalarmlinien der Kühlräume auf einen zweiten, von der Fernwartung unabhängigen Weg legen (SMS oder Datenlogger), damit nächtliche Sollwertänderungen auffallen.
6. Notfallablauf für den Ausfall eines Großkunden und für MES-Ausfall mit Produktion und Vertrieb kurz durchsprechen.

HINWEIS ZUR QUELLENLAGE

Für den Berichtszeitraum habe ich keinen bestätigten Cyberangriff auf einen Lebensmittel- oder Getränkehersteller in DACH gefunden. Die Angaben zu Europol und ANSSI stammen aus einem Agenturtext. Die zum Kälteangriff genannten Opferzahlen in Spanien, Portugal, Polen, Deutschland und Belgien beruhen nur auf Angaben von Sekoia und sind nicht von Händlern bestätigt. Einen Zusammenhang mit Ahold Delhaize sieht das niederländische NCSC nicht. Das BSI-Dokument BSI-CS 154 (gemeldet am 14.10.) kenne ich nur aus der Fachpresse. Nicht aufgenommen habe ich die WAGO-Meldung ICSA-26-293-02, weil die CISA-Seite bei der Prüfung nicht erreichbar war (HTTP 404), sowie die Berichte zum Siemens Software Center und zu PAN-OS CVE-2026-0257, die ich nicht gegen eine Primärquelle prüfen konnte. Alle Quellenlinks wurden am 23.10.2026 automatisch aufgerufen und inhaltlich geprüft. Am 23.10.2026 nach dem Qualitäts-Tor zusätzlich gegen Primärquellen geprüft (CISA, Rapid7/Mandiant, Unit 42, Loxone, Siemens) und korrigiert; nicht belegte Angaben wurden gestrichen.