

WOCHENBERICHT

OT-/Cyber-Lagebild Lebensmittel und Getränke

Ausgabe KW 44/2026 · Lebensmittel und Getränke in DACH

Zielgruppe	Lebensmittel- und Getränkehersteller, Abfüller, Molkereien, Brauereien
Berichtszeitraum	23.10.2026–30.10.2026
Version	1.0
Datum	30.10.2026
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

Diese Woche ging es vor allem um die Kühlung. Forescout hat am 22.10. weltweit 12.976 offen im Internet erreichbare Dienste von Kühlsteuerungen gezählt, auf 6.017 IP-Adressen in 99 Ländern. Den größten Teil machen Copeland/Dixell XWEB und Danfoss StoreView aus. Anlass sind die Angriffe auf Kühlanlagen französischer Supermärkte Mitte Oktober, bei denen Sollwerte und Abtauzyklen verstellt wurden. Bloomberg hat am 27.10. ähnliche Fälle aus der Lebensmittelproduktion veröffentlicht: In einem Fleischbetrieb bei Los Angeles schalteten pro-russische Hacktivist*innen die Kühlung ab, rund 900 kg Fleisch verdarben und Ammoniak trat aus. In Spanien standen zwei Weingüter still, nachdem Heizung und Lüftung manipuliert worden waren. Wer Kühlhäuser, Gärkeller oder Tanklager über ein Web-HMI fernwartet, ist damit direkt im Visier.

Auf der Ebene von SPS und Remote Access gibt es drei Baustellen. Für den Webserver der Siemens S7-1500 und ET 200SP sind acht Lücken offen, für die es noch keinen Patch gibt. Cisco ASA/FTD hat einen aktiv ausgenutzten Zero-Day, mit dem sich SSL-VPN-Zugänge zum Absturz bringen lassen. PHP2Shell steht seit dem 26.10. im KEV-Katalog der CISA. Für die Wiederherstellung nach Ransomware zählt Veeam: Version 13 hat eine Lücke, die ohne Anmeldung ausnutzbar ist. Im Branchenumfeld gab es Leak-Einträge zu Brauereien, darunter AB InBev. Bestätigt ist davon bisher keiner, deshalb stehen sie unter Quellenlage.

GESAMTBEWERTUNG

Die Lage ist hoch: Hacktivist*innen verstellen gezielt Kühl- und Klimasteuerungen, die offen im Internet stehen, und mehrere Zugänge für Remote Access werden aktiv angegriffen. Vorrang hat diese Woche, alle Kühl-, Tank- und Gärsteuerungen mit Web-HMI vom Internet zu nehmen und die Fernwartung nur noch über einen abgesicherten Zugang zu erlauben.

Trends

- Kühlung ist zum bevorzugten Ziel geworden: Nach Frankreich zeigen Forescout und Bloomberg, dass offen erreichbare Kälte- und Klimasteuerungen gezielt verstellt werden.
- Hacktivist*innen ohne tiefes OT-Wissen richten physischen Schaden an, weil ihnen ein offenes HMI mit Standardpasswort reicht.
- Edge-Geräte für Remote Access (Cisco ASA, Palo Alto, Fortinet) bleiben das Haupteinfallstor, mehrere Lücken wurden diese Woche aktiv ausgenutzt.
- Ransomware-Gruppen nehmen gezielt die Backups ins Visier, bevor sie verschlüsseln, und gefährden damit den Wiederanlauf der Produktion.
- Brauereien und Lebensmittelhersteller tauchen regelmäßig auf Leak-Sites auf, oft lange bevor die Unternehmen selbst etwas bestätigen.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Forescout: 12.976 Kühlsteuerungen offen im Internet, Frankreich-Kampagne laut CERT-FR vermutlich noch aktiv	KRITISCH	Forescout Vedere Labs; Industrial Cyber; CERT-FR (über Refindustry), 22.10.

ID	Meldung	Relevanz	Quelle
L-02	Siemens S7-1500 und ET 200SP: acht Lücken im SPS-Webserver, noch kein Patch (ICSA-26-295-14)	HOCH	CISA / Siemens ProductCERT, 22.10.
L-03	Cisco ASA/FTD: Zero-Day bringt SSL-VPN zum Absturz, Ausnutzung bestätigt (CVE-2026-76418)	HOCH	Cisco PSIRT; BleepingComputer, 28./29.10.
L-04	Veeam Backup & Replication 13: Lücke ohne Anmeldung (CVE-2026-108142, CVSS v4 9,1)	HOCH	Veeam KB4948; heise, 27.10.
L-05	Mitsubishi Electric ICONICS GENESIS64 und MC Works64: Umgehung der Anmeldung, für Altprodukte kein Fix (ICSA-26-300-02)	MITTEL	CISA, 27.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 30.10.2026):

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	148182	DNP3: 34267, OMRON FINS: 26328, ProConOS: 17131, Siemens S7: 7931, OPC UA: 5265
Österreich	4928	HMI/VNC: 1088, DNP3: 1006, Niagara Fox: 482, Siemens S7: 386, OPC UA: 161

Meldungen im Detail

L-01 Forescout: 12.976 Kühlsteuerungen offen im Internet, Frankreich-Kampagne laut CERT-FR vermutlich noch aktiv

KRITISCH Forescout Vedere Labs; Industrial Cyber; CERT-FR (über Refindustry), 22.10.

Was ist neu: Forescout zählt 12.976 erreichbare Dienste auf 6.017 IP-Adressen in 99 Ländern. Davon entfallen 7.075 auf Copeland/Dixell XWEB, 4.697 auf Danfoss StoreView, 551 auf Copeland Site Supervisor und 513 auf Carel pCOWeb. Rund 80 % der Danfoss-StoreView-Instanzen (3.762) laufen mit Firmware vor 4.3.1. CERT-FR hatte am 12./13.10. vor Angriffen auf Danfoss AK-SM/AK-SC sowie Copeland und Dixell XWEB gewarnt und hält die Kampagnen für wahrscheinlich noch aktiv.

Bedeutung: Die betroffenen Steuerungen laufen auch in Kühlhäusern von Molkereien, Fleischbetrieben, Brauereien und Logistikern, häufig mit Fernzugang für den Kältebauer. Wer die Sollwerte oder Abtauzyklen verstellt, löst Warenverlust, Rückrufrisiken und Lieferausfälle aus, ohne dass die IT etwas davon merkt. Laut Forescout könnten nach Frankreich weitere europäische Länder folgen. Zahlen für Deutschland, Österreich und die Schweiz nennt der Bericht im Text nicht.

Empfehlung: Mit Shodan oder einem externen Scan die eigenen öffentlichen IP-Adressen auf XWEB, StoreView, Site Supervisor und pCOWeb prüfen. Portweiterleitungen schließen und den Zugang des Kältebauers nur noch über einen Remote-Access-Gateway mit MFA und persönlichen Konten erlauben. Gemeinsam genutzte Zugangsdaten von Dienstleistern abschaffen und Temperaturalarme unabhängig von der Steuerung auswerten.

Quelle:

<https://www.forescout.com/blog/cold-chain-open-control-exposed-refrigeration-systems-reveal-global-risk/> ✓
geprüft

L-02 Siemens S7-1500 und ET 200SP: acht Lücken im SPS-Webserver, noch kein Patch (ICSA-26-295-14)

HOCH CISA / Siemens ProductCERT, 22.10.

Was ist neu: CVE-2026-63350 bis -63357 betreffen den Webserver von S7-1500, ET 200SP, Software Controllern und S7-PLCSIM Advanced, und zwar in allen Versionen. Der höchste Wert ist CVSS v3 9,6. Ein Angreifer bringt einen Nutzer mit Diagnoserechten dazu, eine präparierte Trace-Datei zu importieren. Siemens arbeitet an Fixes, bisher gibt es für die gelisteten Produkte keinen.

Bedeutung: S7-1500 und ET 200SP stecken in vielen Abfüll-, Misch- und Verpackungslinien. Der Webserver wird oft für die Diagnose durch Instandhaltung oder Maschinenbauer eingeschaltet und dann vergessen. Die Lebensmittelbranche steht nicht in der Sektorliste der CISA, betroffen ist sie über die Produkte trotzdem.

Empfehlung: Im Asset-Inventar alle S7-1500 und ET 200SP mit aktivem Webserver markieren. Trace-Dateien nur aus bekannter Quelle importieren lassen und die Instandhaltung darauf hinweisen. Die Patches einplanen, sobald Siemens sie veröffentlicht.

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

L-03 Cisco ASA/FTD: Zero-Day bringt SSL-VPN zum Absturz, Ausnutzung bestätigt (CVE-2026-76418)

HOCH Cisco PSIRT; BleepingComputer, 28./29.10.

Was ist neu: Ohne Anmeldung lässt eine präparierte Anfrage ASA- oder FTD-Geräte mit aktivem SSL-VPN neu starten. Voraussetzung ist eine sekundäre Authentifizierung in einer Tunnel-Gruppe. Cisco bestätigt die Ausnutzung und nennt keinen vollständigen Workaround. Shadowserver zählt über 51.000 erreichbare ASA-SSL-VPNs. Den CVSS-Wert 8,6 nennt das Cisco-Advisory, BleepingComputer spricht nur von „high“.

Bedeutung: Viele Betriebe lassen den Remote Access des Bereitschaftsdienstes und der Linienlieferanten über die ASA laufen. Fällt das VPN in der Nachtschicht aus, kommt bei einer Störung niemand mehr von außen auf die Anlage. Das ist ein Verfügbarkeitsrisiko, auch wenn kein Datenabfluss droht.

Empfehlung: Patchen und prüfen, ob es für die Fernwartung einen zweiten, unabhängigen Weg gibt, etwa einen Jump Host mit eigenem Zugang. Neustarts der ASA im SIEM oder Syslog überwachen.

Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75> ✓ geprüft

L-04 Veeam Backup & Replication 13: Lücke ohne Anmeldung (CVE-2026-108142, CVSS v4 9,1)

HOCH Veeam KB4948; heise, 27.10.

Was ist neu: Ohne Anmeldung lässt sich die Autorisierung am CDP Coordinator Service umgehen. Betroffen sind Windows-Backup-Server und die Veeam Software Appliance bis 13.1.1.18 bzw. 13.0.2.29, Version 12.x laut Veeam nicht. Eine Ausnutzung ist bisher nicht bekannt.

Bedeutung: Nach einem Ransomware-Angriff hängt der Wiederanlauf von MES, Chargenrückverfolgung und Rezepturdaten am Backup. Laut CISA schalten Gruppen wie SafePay über Veeam-Lücken gezielt die Backups aus, bevor sie verschlüsseln.

Empfehlung: Patchen und den Backup-Server aus der Office-Domäne herausnehmen. Mindestens eine Kopie offline oder unveränderbar halten und im Incident-Response-Plan die Wiederherstellung der Produktionssysteme einmal testen.

Quelle: <https://www.veeam.com/kb4948> ✓ geprüft

L-05 Mitsubishi Electric ICONICS GENESIS64 und MC Works64: Umgehung der Anmeldung, für Altprodukte kein Fix (ICSA-26-300-02)

MITTEL CISA, 27.10.

Was ist neu: Die Passwort-Wiederherstellung nutzt eine feste Challenge-Response, die für alle Benutzer gleich ist (CVE-2026-16436, CVSS v4 9,2). Hinzu kommt eine Rechteauserweiterung (CVE-2026-16438). Für MC Works64, GENESIS32 und BizViz plant Mitsubishi keinen Fix. Eine Ausnutzung ist laut Hersteller nicht bekannt.

Bedeutung: Als HMI und Historian wird ICONICS auch in der Prozess- und Energieüberwachung von Produktionsbetrieben eingesetzt. Ältere Installationen laufen dort oft jahrelang unverändert weiter.

Empfehlung: Prüfen, ob ICONICS im Haus oder beim Maschinenbauer im Einsatz ist. Den von CISA beschriebenen Workaround mit der leeren Challenge-Datei umsetzen, den Ersatz der Altprodukte ins Budget aufnehmen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-02> ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Alle Kühl- und Klimasteuerungen vom Internet trennen und die Fernwartung über einen Remote-Access-Gateway mit MFA und persönlichen Konten bündeln [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Asset-Inventar um SPS-Webserver, Edge-Geräte und SCADA-Altinstallationen ergänzen und Patches nach Ausnutzung (KEV) und Erreichbarkeit priorisieren [CC5 Risk-Based Vulnerability Management]	L-02	HOCH	0 bis 3 Monate
M-03	Veeam patchen, eine Backup-Kopie offline oder unveränderbar halten und die Wiederherstellung von MES und Rezepturdaten im Incident-Response-Plan testen [CC1 ICS Incident Response]	L-04	HOCH	sofort
M-04	Temperaturdaten und Anmeldungen am Remote Access zentral überwachen, damit verstellte Sollwerte und ungewöhnliche Sitzungen auffallen [CC3 ICS Network Visibility & Monitoring]	L-01	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Welche Kühl-, Gär- oder Tanksteuerungen bei uns haben eine Weboberfläche, und ist eine davon aus dem Internet erreichbar?
2. Wie greifen Kältebauer und Maschinenbauer heute auf unsere Anlagen zu, mit persönlichen Konten und MFA oder mit gemeinsam genutzten Zugangsdaten?
3. Merken wir eine verstellte Solltemperatur rechtzeitig, auch nachts und am Wochenende, unabhängig von der Steuerung selbst?
4. Bei welchen S7-1500-Steuerungen ist der Webserver aktiv, und wer braucht ihn tatsächlich?

5. Wann haben wir zuletzt getestet, ob sich MES und Rezepturdaten nach einem Ransomware-Angriff aus dem Backup wiederherstellen lassen?

Maßnahmen dieser Woche

1. Die eigenen öffentlichen IP-Adressen mit Shodan oder einem externen Scan auf Kühlsteuerungen (XWEB, StoreView, Site Supervisor, pCOWeb) und offene HMI/VNC-Ports prüfen und Funde sofort abschalten.
2. Bei allen Kühlanlagen Sollwerte, Abtauzeiten und Alarmgrenzen mit dem dokumentierten Stand vergleichen und Benutzerkonten auf unbekannte Einträge prüfen.
3. Cisco ASA/FTD und Veeam 13 auf die Fix-Versionen aktualisieren.
4. Bei allen S7-1500 und ET 200SP den Webserver abschalten, wo er nicht gebraucht wird, sonst die Ports 80/443 per Firewall auf die Engineering-Station beschränken.
5. Die Zugangsdaten von Dienstleistern für Fernwartung durch persönliche Konten mit MFA ersetzen und den Zugang nur noch über einen Remote-Access-Gateway mit Sitzungsprotokoll erlauben.
6. Mit Qualitätssicherung und Produktion einen kurzen Notfallablauf „Kühlung manipuliert“ festlegen: wer entscheidet über Sperrung von Ware, wer schaltet auf Handbetrieb um.

HINWEIS ZUR QUELLENLAGE

Nicht bestätigt und deshalb nicht als Meldung aufgenommen: Laut RetailDetail (26.10.) prüft AB InBev einen möglichen Angriff, nachdem die Gruppe Emperador 3,9 GB Daten und 10 Mio. USD Lösegeld genannt hat. Rescana gibt 1 Mio. USD an, der Betrag ist also widersprüchlich (<https://www.retaildetail.eu/news/food/hackers-demand-nearly-9-million-euros-from-ab-inbev-following-a-possible-data-breach/>). Dazu kommen ein Leak-Eintrag der Gruppe Lamashtu zu einer bayerischen Traditionsbrauerei (22.10., nur über BreachSense belegt) und ein Qilin-Eintrag zu einem US-Lebensmittellieferanten (26.10., DeXpose); Bestätigungen der Firmen gibt es keine. Den Bloomberg-Artikel vom 27.10. konnte ich nicht direkt abrufen, die Angaben stammen aus Meduza und TechTimes. Der Angriff auf Ahold Delhaize (bestätigt, Beginn 11./12.10.) und die Warnung von CERT-FR (12./13.10.) liegen vor dem Berichtszeitraum und dienen nur als Hintergrund. Für die Woche vom 28. bis 30.10. habe ich keine vollständige Liste der ICS-Advisories der CISA gefunden. Alle Quellenlinks wurden am 30.10.2026 automatisch aufgerufen und inhaltlich geprüft. 2 Meldung(en) ohne überprüfbare Originalquelle wurden nicht aufgenommen.