VORFALL-LAGEBILD

Neue Angriffswelle auf vernetzte Kühlanlagen in Supermärkten: Belgien, Schweden, Luxemburg, Irland, Estland betroffen, Angriffsversuche bei Coop Schweiz

Stand 02.11.2026 18:58 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Eine Kühlsteuerung gehört nicht direkt ins Internet, Fernwartung läuft über einen abgesicherten Zugang mit persönlicher Anmeldung und zweitem Faktor (SANS CC4 Secure Remote Access).

2. Wer weiß, welche Steuerungen in seinen Filialen hängen und welche davon keine Updates mehr bekommen, kann gezielt tauschen statt raten (CC5 Risk-Based Vulnerability Management).

3. Coop Schweiz zeigt, dass Absicherung wirkt: Versuche gab es, Schaden nicht.

Wissensstand



■ Wissen 51 % ■ Wahrscheinlich 23 % ■ Nicht bekannt 26 %

Ablauf und betroffene Ketten sind durch Betreiber, nationale Cyberbehörden und Agenturen gut belegt, Zahlen (Filialen, Temperaturen, Schaden) widersprechen sich aber zwischen Quellen, und zu Tätern, genauem Einfallsweg und Verbindung zu Frankreich gibt es nur Einschätzungen.

1. Was ist passiert, und warum?

WISSEN

• Delhaize bestätigte einen IT-Vorfall an Kühlsystemen in rund 40 belgischen Filialen in der Nacht vom 1. auf den 2. November; Carrefour Belgien sprach ausdrücklich von einem Cyberangriff (15 von 700 Filialen). (100 %)

[https://nltimes.nl/2026/11/02/cyberattack-hits-delhaize-supermarket-fridges-freezers-dozens-belgium-locations]

• Carrefour-Sprecher Mich Vergauwen: „It's a cyberattack, there is no other reason“. (100 %)

[https://www.euronews.com/2026/11/02/cyberattack-hits-belgian-supermarket-fridges-and-freezers]

• Laut Kältedienstleister Sabcobel (CEO Stephan Moelans) wurden die Verdampfer per Fernzugriff in den Abtaumodus geschaltet; Techniker arbeiteten ab 1 Uhr nachts daran, die Kontrolle zurückzugewinnen. (100 %)

[https://www.nachrichten.at/wirtschaft/erneut-cyberangriffe-auf-supermaerkte-in-europa;art15,4228135]

• Am 12. Oktober 2026 waren in Frankreich Kühlanlagen in Hunderten Supermärkten manipuliert worden; Danfoss erklärte, die meisten betroffenen Systeme seien ältere Produkte ohne Sicherheitsupdates. (100 %)

[https://www.pbs.org/newshour/world/cyberattacks-disrupt-refrigeration-systems-at-european-supermarkets]

• Niemand hat sich bekannt, Lösegeldforderungen sind nicht bekannt. (100 %)

[https://www.cnbc.com/2026/11/02/cyberattack-on-fridges-hits-supermarkets-across-europe.html]

• Delhaize selbst spricht nur von einem „IT-Vorfall“, die Einstufung als Cyberangriff kommt u. a. von der Agentur Belga. (100 %) [https://www.marketscreener.com/news/cyberattack-caused-ahold-delhaize-fridges-temperature-increases-belga-reports-ce785fd8de80f126]

NICHT BEKANNT

• Wer hinter den Angriffen steckt und mit welchem Motiv.

• Ob die Welle vom 2. November technisch und personell mit dem Angriff in Frankreich zusammenhängt (Reuters konnte das laut CNBC nicht klären; heise: nicht bestätigt).

• Welche konkrete Schwachstelle oder welcher Zugang in den einzelnen Ländern genutzt wurde.

• Ob alle betroffenen Anlagen vom selben Hersteller stammen.

WAHRSCHEINLICH (Einschätzung)

• Die Angreifer haben aus dem Internet erreichbare Kühlmanagement-Oberflächen direkt angesprochen, statt erst in die Unternehmens-IT einzudringen. (75 %) – Dienstleister nennt Fernumschaltung in Abtaumodus, Danfoss und Forescout verweisen auf exponierte Altgeräte, Muster gleicht Frankreich; Primärforensik ist aber nicht veröffentlicht.

• Es handelt sich um dieselbe Kampagne bzw. dieselbe Methode wie in Frankreich. (65 %) – Gleiche Methode (Abtaumodus), gleiche Uhrzeit nachts, gleiche Gerätegruppe; zwischen Methode und Täteridentität kann aber ein Nachahmer liegen, wovor das BSI ausdrücklich gewarnt hat.

• Ziel ist Sabotage bzw. Störung, nicht Geld. (70 %) – Keine Lösegeldforderung, kein Datendiebstahl gemeldet; SentinelOne-Forscher Tom Hegel hält Sabotage für wahrscheinlich, EU-Kommissar Hansen spricht von gezieltem Versuch, die Versorgung zu stören.

2. Was ist die Auswirkung?

WISSEN

• Belgische Läden mussten laut Euronews Ware für rund 100.000 € entsorgen. (100 %)

[https://de.euronews.com/2026/11/02/belgische-supermarkte-cyberangriff-trifft-vernetzte-kuhlanlagen]

• Musgrave nahm in 13 von 223 SuperValu-Filialen in Irland Kühl- und Tiefkühlware aus dem Verkauf. (100 %)

[https://www.aljazeera.com/news/2026/11/2/freezers-in-sweden-belgium-overheat-following-possible-cyberattacks]

• Coop Schweden meldete sechs betroffene Filialen, bei einer ICA-Filiale in Stockholm stiegen Tiefkühltemperaturen auf 50 °C. (100 %)

[https://www.cnbc.com/2026/11/02/cyberattack-on-fridges-hits-supermarkets-across-europe.html]

• Axfood meldete gehackte Tiefkühlgeräte in einem Verteilzentrum im Raum Göteborg. (100 %)

[https://www.aljazeera.com/news/2026/11/2/freezers-in-sweden-belgium-overheat-following-possible-cyberattacks]

• Ein belgischer Metzgereibetrieb verlor Fleisch für rund 15.000 €. (100 %)

[https://www.cnbc.com/2026/11/02/cyberattack-on-fridges-hits-supermarkets-across-europe.html]

• Delhaize Luxemburg setzte vorsorglich seine Bestellsysteme aus. (100 %)

[https://www.euronews.com/2026/11/02/cyberattack-hits-belgian-supermarket-fridges-and-freezers]

• Frankreich (Oktober): Finanzminister Lescure sprach von rund 700 betroffenen Supermärkten, aber keinem Risiko für die Lebensmittelversorgung. (100 %)

[https://www.pbs.org/newshour/world/cyberattacks-disrupt-refrigeration-systems-at-european-supermarkets]

NICHT BEKANNT

• Gesamtschaden der Welle vom 2. November über alle Länder.

• Die tatsächlich erreichten Temperaturen: Quellen nennen 15 °C (VRT), 17 bis 18 °C (Euronews EN, CNBC), 50 °C (Schweden, Estland) und 70 °C (Euronews DE, heise).

• Ob verdorbene Ware verkauft wurde (bisher kein Hinweis).

• Ob Geräte in den neuen Ländern beschädigt wurden oder brannten (in Frankreich berichtet).

WAHRSCHEINLICH (Einschätzung)

• Für Verbraucher bleibt es bei lokal leeren Kühlregalen; eine Versorgungslage entsteht nicht. (85 %) – Betroffen sind jeweils kleine Anteile der Filialnetze (z. B. 15 von 700, 13 von 223); in Frankreich sah die Regierung trotz 700 Märkten kein Versorgungsrisiko.

• Der Gesamtschaden der Novemberwelle liegt im einstelligen bis niedrigen zweistelligen Millionenbereich. (40 %) – Belgien ca. 100.000 €, Schweden laut 20 Minuten Ware in Millionenhöhe; belastbare Summen fehlen, daher nur grobe Größenordnung.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

• Delhaize sagte, man prüfe, wie die Läden wieder in Betrieb gehen können. (100 %)
[https://www.vrt.be/vrtnws/en/2026/11/02/possible-cyberattack-hits-several-belgian-supermarket-chains/]

• Die ICA-Kvantum-Filiale in Sjöbo blieb zunächst geschlossen und hat inzwischen wieder geöffnet. (100 %)
[https://www.heise.de/news/Kuehlschraenke-in-Lebensmittellaeden-weiterer-Laender-geknackt-11507846.html]

• Laut Sabcobel genügt ein Software-Update allein nicht, nötig seien physische Änderungen. (100 %) [https://www.euronews.com/2026/11/02/cyberattack-hits-belgian-supermarket-fridges-and-freezers]

• In den Niederlanden wurden im Oktober vorsorglich viele Geräte abgeschaltet, Online-Lieferungen verzögerten sich bis zu zehn Tage. (100 %)
[https://www.20min.ch/story/seit-mitte-oktober-mysterioese-hacking-welle-trifft-europaeische-supermaerkte-103660687]

NICHT BEKANNT

• Wann alle betroffenen Filialen wieder voll bestückt sind.

• Ob Firmen die Kühlsteuerung vorerst offline betreiben oder schon ersetzt haben.

WAHRSCHEINLICH (Einschätzung)

• Die Kühlung selbst läuft in den meisten Filialen nach Stunden bis wenigen Tagen wieder, oft im Handbetrieb ohne Fernzugriff. (70 %) – Techniker waren noch in der Nacht vor Ort, ICA Sjöbo hat wieder geöffnet; Abtaumodus ist eine Betriebsart, keine Zerstörung.

• Die saubere Lösung (Altgeräte tauschen, Fernwartung neu aufbauen) dauert Wochen bis Monate. (65 %) – Für EOL-Geräte gibt es laut Danfoss keine Updates mehr, Sabcobel spricht von nötigen physischen Änderungen; Hardwaretausch über viele Filialen braucht Planung und Techniker.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

• In Frankreich kam es im Oktober zu Bränden und Lebensmittelverlusten, die Pariser Staatsanwaltschaft ermittelt auch zu gemeldeten Bränden. (100 %)
[https://www.pbs.org/newshour/world/cyberattacks-disrupt-refrigeration-systems-at-european-supermarkets]

• Laut Wikipedia-Zusammenfassung schmolzen in Frankreich Geräte oder fingen Feuer, Sprinkler verursachten Wasserschäden. (100 %)
[https://en.wikipedia.org/wiki/2026_French_supermarket_refrigerator_hack]

• Die in Frankreich betroffenen Danfoss-Modelle AK-SC355 und AK-SM800 sind seit 2016 bzw. Mai 2021 End-of-Life. (100 %) [https://en.wikipedia.org/wiki/2026_French_supermarket_refrigerator_hack]

NICHT BEKANNT

• Ob bei der Novemberwelle Hardware beschädigt wurde; bisher werden nur verdorbene Ware und Temperaturanstiege gemeldet.

• Ob Kältemittelkreisläufe oder Verdichter durch den Dauerbetrieb Schaden genommen haben.

WAHRSCHEINLICH (Einschätzung)

• Bei der Novemberwelle sind die meisten Kälteanlagen mechanisch intakt geblieben. (65 %) – Berichte erwähnen keine Brände, Temperaturen teils nur 15 bis 18 °C, Läden wie ICA Sjöbo öffneten wieder; Einzelfälle mit Hitzeschäden bleiben möglich.

• Wo Steuerungen getauscht werden müssen, dauert es durch Lieferzeiten und Technikermangel mehrere Wochen. (55 %) – Viele Filialen gleichzeitig, Fachbetriebe ausgelastet; konkrete Lieferzeiten sind nicht belegt.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Forescout fand per Shodan 12.976 öffentlich erreichbare Kühlmanagement-Dienste auf 6.017 IP-Adressen in 99 Staaten und Gebieten (Stand 22.10.2026). (100 %)
[https://www.forescout.com/blog/cold-chain-open-control-exposed-refrigeration-systems-reveal-global-risk/]

• Davon 7.075 Copeland/Dixell XWEB, 4.697 Danfoss StoreView, 551 Copeland Site Supervisor, 513 CAREL pCOWeb. (100 %)

[https://www.forescout.com/blog/cold-chain-open-control-exposed-refrigeration-systems-reveal-global-risk/]

• Rund 80 % der Danfoss-StoreView-Beobachtungen liefen mit Firmware älter als 4.3.1, die bekannte Schwachstellen schließt; gezählt wurden erreichbare, nicht gehackte Systeme. (100 %) [https://de.euronews.com/2026/11/02/belgische-supermarkte-cyberangriff-trifft-vernetzte-kuhlanlagen]

• CISA hat zu Danfoss AK-SM 8xxA ein ICS-Advisory veröffentlicht (Schwachstellen 2025 von Claroty Team82 gefunden). (100 %) [https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03]

• Das BSI richtet seine Empfehlung BSI-CS 154 „Gefährdung durch internet-verbundene OT-Systeme“ an Betreiber kleiner Anlagen, etwa zur Kühlung von Lebensmitteln oder Stromerzeugung. (100 %) [https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261013_OT-Gefaehrdung-Kleinanlagen.html]

• Shodan (aggregiert): Danfoss AK-SM800 / AK-SC355: ca. 0 öffentlich erreichbare Systeme in Schweiz (100 %)

• Shodan (aggregiert): Danfoss-Steuerung: ca. 0 öffentlich erreichbare Systeme in Schweiz (100 %)

• Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Schweiz: 50608 gesamt (DNP3 15280, EtherNet/IP 14229, ProConOS 14097, Modbus 1950, Siemens S7 602, OPC UA 392) (100 %)

NICHT BEKANNT

• Wie viele erreichbare Systeme in Deutschland, Österreich und der Schweiz stehen (Forescout zeigt Länderverteilung nur als Grafik, Zahlen im Text fehlen).

• Wie viele der erreichbaren Systeme tatsächlich angreifbar sind.

WAHRSCHEINLICH (Einschätzung)

• Auch im DACH-Raum stehen mehrere Hundert solcher Kühlsteuerungen offen im Netz. (60 %) – Weltweit fast 13.000 Dienste in 99 Ländern, Europa als Schwerpunkt erwähnt, gleiche Hersteller im Handel verbreitet; eigene Länderzählung liegt mir nicht vor.

• Neben Supermärkten sind Lebensmittelverarbeitung, Obstlager, Weingüter und Krankenhauskühlung mit denselben Geräten exponiert. (80 %) – Forescout nennt diese Bereiche laut Euronews ausdrücklich; die genaue Zahl je Branche ist offen.

6. Kann das wieder passieren?

WISSEN

• Nach Frankreich (12.10.) folgte am 2.11. eine zweite Welle in mehreren Ländern. (100 %) [https://www.20min.ch/story/seit-mitte-oktober-mysterioese-hacking-welle-trifft-europaeische-supermaerkte-103660687]

• BSI-Präsidentin Plattner warnte am 13.10., der Angriff hätte jedes Land treffen können, Nachahmer könnten jederzeit auftreten. (100 %) [https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261013_OT-Gefaehrdung-Kleinanlagen.html]

• Das belgische Cybersicherheitszentrum hält es für möglich, dass die Urheber nie ermittelt werden. (100 %) [https://www.aljazeera.com/news/2026/11/2/freezers-in-sweden-belgium-overheat-following-possible-cyberattacks]

• Coop Schweiz registrierte Angriffsversuche, die scheiterten; Migros sah keine Anzeichen. (100 %) [https://www.20min.ch/story/seit-mitte-oktober-mysterioese-hacking-welle-trifft-europaeische-supermaerkte-103660687]

• Schwedens nationales Cybersicherheitszentrum (Leiter John Billow) verweist auf zahlreiche ungepatchte, exponierte OT-Geräte. (100 %) [https://www.aljazeera.com/news/2026/11/2/freezers-in-sweden-belgium-overheat-following-possible-cyberattacks]

NICHT BEKANNT

• Ob weitere Wellen geplant sind.

• Ob auch Deutschland oder Österreich schon Versuche gesehen haben (bisher kein bestätigter Fall in DE/AT).

WAHRSCHEINLICH (Einschätzung)

• Es kommt in den nächsten Wochen zu weiteren Vorfällen dieser Art in Europa. (70 %) – Zwei Wellen in drei Wochen, tausende erreichbare Geräte, Methode öffentlich diskutiert, Nachahmer möglich.

• Ein Vorfall dieser Art trifft auch einen Betrieb in Deutschland, Österreich oder der Schweiz. (45 %) – Gleiche Hersteller im DACH-Handel, Coop Schweiz meldet bereits Versuche; dem stehen die Warnungen von BSI und Herstellern und bereits erfolgte Abschottung gegenüber.

Lage

In der Nacht zum 2. November 2026 wurden in Supermärkten in Belgien, Luxemburg, Schweden, Irland, Estland und weiteren Ländern Kühl- und Tiefkühlanlagen aus der Ferne verstellt, viele Filialen mussten Ware entsorgen. Betreiber und Behörden sprechen von Cyberangriff bzw. IT-Vorfall; ein Kältedienstleister berichtet, die Verdampfer seien wie beim Angriff auf Frankreich am 12. Oktober in den Abtaumodus geschaltet worden. Täter und Motiv sind offen, im Fokus stehen aus dem Internet erreichbare, teils veraltete Kühlmanagement-Steuerungen (u. a. Danfoss), Coop Schweiz meldet nur abgewehrte Versuche.

Angriff	Fernmanipulation von Kühl- und Tiefkühlanlagen in Supermärkten, Verdampfer laut Dienstleister in Abtaumodus geschaltet, Temperaturanstieg und Warenverlust.
Wann / Status	Nacht vom 1. auf den 2. November 2026 (laut CNBC gegen 2 Uhr); vorherige Welle Frankreich 11./12. Oktober 2026. · unklar
Täter	unbekannt; kein Bekennerschreiben, keine Lösegeldforderung. Russland bestreitet Beteiligung an Sabotage. – unbekannt
Betreiber / Branche	u. a. Delhaize, Carrefour, Intermarché, Spar (Colruyt-Franchise), De Laet en Van Haver (BE); Delhaize (LU); ICA, Coop, Axfood-Lager (SE); SuperValu/Musgrave (IE); Selver laut Euronews (EE); Versuche bei Coop Schweiz · Lebensmitteleinzelhandel
Anlage / Alter	Kühlmanagement-Steuerungen für Kühl- und Tiefkühlanlagen (in Frankreich Danfoss AK-SM800/AK-SC355, Copeland/Dixell XWEB; für November nicht je Kette bestätigt) · teils End-of-Life (AK-SC355 seit 2016, AK-SM800 seit Mai 2021); für Novemberfälle nicht je Filiale belegt
Region	Belgien, Luxemburg, Schweden, Irland, Estland, laut Euronews auch Niederlande und Finnland; Versuche in der Schweiz
Auswirkungen	Lokal leere Kühl- und Tiefkühlregale und vernichtete Ware (Belgien rund 100.000 €), einzelne Filialen zeitweise geschlossen. Kein Hinweis auf Gesundheitsgefahr durch verkaufte Ware. In Frankreich sah die Regierung trotz rund 700 Märkten kein Risiko für die Lebensmittelversorgung (https://www.pbs.org/newshour/world/cyberattacks-disrupt-refrigeration-systems-at-european-supermarkets).
Behörden	Belgien: Centre for Cybersecurity (CCB) und Bundesstaatsanwaltschaft. Schweden: nationales Cybersicherheitszentrum. Frankreich: ANSSI/CERT-FR, Cybercrime-Einheit der Pariser Staatsanwaltschaft. Niederlande: Polizei (Meldung Ahold). UK: NCSC beobachtet mit Partnern. Deutschland: BSI-Warnung vom 13.10. Irland: keine Stellungnahme des NCSC gefunden. Schweiz: keine Behördenmeldung gefunden.

Regulatorik	Lebensmittelhandel fällt unter NIS2 (Sektor Produktion, Verarbeitung und Vertrieb von Lebensmitteln) ab den Größenschwellen; in Deutschland mit dem NIS2-Umsetzungsgesetz Meldepflicht erheblicher Vorfälle an das BSI (Erstmeldung 24 Stunden). Ob die konkret betroffenen Filialbetreiber erfasst sind, hängt von Größe und Struktur ab (nicht geprüft). CRA verlangt künftig Sicherheitsupdates für vernetzte Produkte, gilt aber nicht rückwirkend für EOL-Altgeräte. Schweiz: Meldepflicht für Cyberangriffe gilt für kritische Infrastrukturen; ob Detailhandel erfasst ist, nicht geprüft.

Eingesetzte Produkte (öffentlich belegt)

• Danfoss AK-SM800 / AK-SC355 (Kühlmanagement) (Danfoss) – Presse
[https://www.heise.de/news/Kuehlschraenke-in-Lebensmittellaeden-weiterer-Laender-geknackt-11507846.html]

• Danfoss-Steuerung (Modell bei SuperValu ungenannt: „specific model of refrigeration system“) (nicht genannt) – Presse
[https://www.aljazeera.com/news/2026/11/2/freezers-in-sweden-belgium-overheat-following-possible-cyberattacks]

Angriffsvektor

Bekannt: Teilweise: laut Sabcobel Fernumschaltung in den Abtaumodus; laut Danfoss vor allem veraltete Software ohne Updates. Konkreter Einstiegsweg für November nicht veröffentlicht.

• Direkt aus dem Internet erreichbare Weboberflächen von Kühlmanagement-Steuerungen mit veralteter Firmware und bekannten, 2025 veröffentlichten Schwachstellen in der Anmeldung (hoch): In Frankreich so beschrieben (CERT-FR-Alarm, Danfoss), Forescout zählt tausende exponierte Systeme, 80 % Danfoss-Firmware veraltet; gleiches Muster im November.

• Schwache oder geteilte Zugangsdaten von Wartungsdienstleistern (Remote Access ohne MFA) (mittel): Forescout empfiehlt ausdrücklich, geteilte Dienstleister-Passwörter abzuschaffen; Zuständigkeiten zwischen Dienstleister, Markt und IT sind oft aufgeteilt.

• Kompromittierte zentrale Fernwartungsplattform eines Dienstleisters, über die viele Filialen gleichzeitig erreichbar sind (gering): Würde die zeitgleiche Wirkung erklären; gegen die Hypothese sprechen Fälle bei vielen verschiedenen Ketten und Dienstleistern, Belege fehlen.

Zeitleiste

24.03.2025 Danfoss veröffentlicht Advisory DSA-2025-03-01 zu Schwachstellen in AK-SM 800A (gefunden von Claroty Team82). – berichtet
[https://en.wikipedia.org/wiki/2026_French_supermarket_refrigerator_hack]

Mai 2025 CISA-Advisory ICSA-25-140-03 zu Danfoss AK-SM 8xxA. – bestätigt
[https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03]

11./12.10.2026 Kühlanlagen in Hunderten französischen Supermärkten nachts manipuliert. – bestätigt [https://www.pbs.org/newshour/world/cyberattacks-disrupt-refrigeration-systems-at-european-supermarkets]

12.10.2026 Albert Heijn (Ahold Delhaize) meldet Cybersecurity-Vorfall, Systeme vorsorglich abgeschaltet. – berichtet
[https://www.pbs.org/newshour/world/cyberattacks-disrupt-refrigeration-systems-at-european-supermarkets]

13.10.2026 BSI veröffentlicht Pressemitteilung und Empfehlung BSI-CS 154; CERT-FR-Alarm CERTFR-2026-ALE-012. – bestätigt [https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261013_OT-Gefaehrdung-Kleinanlagen.html]

22.10.2026 Forescout veröffentlicht Exponierungsstudie (12.976 Dienste, 99 Länder). – bestätigt
[https://www.forescout.com/blog/cold-chain-open-control-exposed-refrigeration-systems-reveal-global-risk/]

1./2.11.2026 nachts Zweite Welle: Belgien, Luxemburg, Schweden, Irland, Estland u. a. – bestätigt [https://www.cnbc.com/2026/11/02/cyberattack-on-fridges-hits-supermarkets-across-europe.html]

2.11.2026 Belgische Bundesstaatsanwaltschaft leitet Ermittlungen ein, CCB bestätigt Kenntnis eines Vorfalls. – berichtet
[https://www.euronews.com/2026/11/02/cyberattack-hits-belgian-supermarket-fridges-and-freezers]

2.11.2026 Coop Schweiz meldet gescheiterte Angriffsversuche. – berichtet
[https://www.20min.ch/story/seit-mitte-oktober-mysterioese-hacking-welle-trifft-europaeische-supermaerkte-103660687]

Vergleichsfälle

• Kühlanlagen-Angriff Frankreich (2026): Altgeräte mit offenem Webzugang lassen sich massenhaft in einer Nacht verstellen, Alarme griffen nicht.
[https://en.wikipedia.org/wiki/2026_French_supermarket_refrigerator_hack]

• Coop Schweden: Kassen nach Kaseya-Angriff auf Dienstleister (2021): Eine Schwachstelle beim Dienstleister kann hunderte Filialen gleichzeitig lahmlegen.
[https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant]

• Claroty-Forschung zu Danfoss-Kühlsteuerungen (2025): Die Schwachstellen waren über ein Jahr vor den Angriffen öffentlich und gepatcht, nur nicht überall eingespielt bzw. Altgeräte nicht ersetzt. [https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers]

Begriffe einfach erklärt

OT: Operational Technology, also Technik, die Maschinen und Anlagen steuert, hier die Kühlung.

Abtaumodus: Normale Betriebsart, in der die Kühlung kurz heizt, um Eis zu entfernen; dauerhaft eingeschaltet wird es im Regal warm.

End-of-Life: Der Hersteller liefert für das Gerät keine Sicherheitsupdates mehr.

Fernwartung: Der Techniker greift aus der Ferne auf die Anlage zu, statt vor Ort zu kommen.

Firmware: Die fest eingebaute Software einer Steuerung.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.