V O R F A L L - L A G E B I L D

Angriff auf vernetzte Supermarkt-Kühlschränke in Frankreich: CERT-FR erweitert Warnung, BSI mahnt, DACH-Handel meldet keine Fälle

Stand 14.10.2026 18:40 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand



■ Wissen 42 % ■ Wahrscheinlich 26 % ■ Nicht bekannt 32 %

Schadensbild, Ablauf, betroffene Produktfamilien und Behördenwarnungen sind behördlich bzw. von Herstellern belegt (A und B übereinstimmend). Ungeklärt oder widersprüchlich sind die Zahl der Märkte, der genaue Zugangsweg und die Täter. Die Zahlen zu exponierten Systemen stammen aus unterschiedlichen Scans und weichen stark voneinander ab.

1. Was ist passiert, und warum?

WISSEN

• CERT-FR meldet zahlreiche Kompromittierungen von Fernsteuerungen für Kälteanlagen. Betroffen sind Danfoss AK-SC, Danfoss AK-SM, Copeland XWEB und Dixell XWEB. Die Erstversion der Warnung stammt vom 12.10.2026, die Ergänzung um weitere Geräte vom 13.10.2026. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• CERT-FR wertet eine direkt aus dem Internet erreichbare Verwaltungsoberfläche als Verstoß gegen gute Sicherheitspraxis. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Die Angreifer haben die Abtaufunktion missbraucht: Statt rund zwei Stunden täglich lief sie dauerhaft und erhitzte auf etwa 50 °C, teils schon vor Mitternacht. Laut Mousquetaires-Chef Cotillard waren es 50 °C. In Rennes war ein Gefrierschrank auf 95 °C programmiert. (100 %) [https://next.ink/261236/des-frigos-pirates-dans-des-supermarches-a-cause-dequipements-obsoletes-ou-non-mis-a-jour/ ; https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/un-piratage-pas-si-sophistique-que-ca-ce-que-l-on-sait-de-la-cyberattaque-qui-a-fait-monter-en-temperature-les-frigos-de-supermarches_8235061.html]

• Laut Danfoss (u. a. gegenüber AFP) sind die betroffenen Geräte überwiegend Altprodukte ohne Software- oder Sicherheitsupdates (AK-SM 800, AK-SC 355) oder nicht aktualisierte AK-SM 800A. Zahlen hat Danfoss nicht genannt. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/un-piratage-pas-si-sophistique-que-ca-ce-que-l-on-sait-de-la-cyberattaque-qui-a-fait-monter-en-temperature-les-frigos-de-supermarches_8235061.html ; https://www.khaleejtimes.com/world/europe/french-supermarkets-refrigerator-shutdown-cyberattack]

• Nach Angaben eines BSI-Sprechers waren die Passwörter der Steuerungen offenbar schon bei der Auslieferung unzureichend gesichert. (100 %) [https://www.heise.de/news/BSI-gemahnt-auch-Betreiber-kleiner-vernetzter-Anlagen-11487069.html]

• Die Pariser Staatsanwaltschaft ermittelt von sich aus und hat den Fall an das Office anti-cybercriminalité (OFAC) gegeben. Bis zum 13.10. gab es laut Reuters weder ein Bekennerschreiben noch eine Lösegeldforderung. ANSSI-Direktor Strubel sagt, es sei „rien de réellement établi“. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/un-piratage-pas-si-sophistique-que-ca-ce-que-l-on-sait-de-la-cyberattaque-qui-a-fait-monter-en-temperature-les-frigos-de-supermarches_8235061.html ; https://next.ink/261236/des-frigos-pirates-dans-des-supermarches-a-cause-dequipements-obsoletes-ou-non-mis-a-jour/]

• Für die Danfoss AK-SM 8xxA Serie gibt es seit Mai 2025 ein CISA-Advisory zu einer Authentifizierungsumgehung (CVE-2025-41450, behoben ab R4.2). Im August 2025 kamen

CVE-2025-41451 und CVE-2025-41452 dazu (behoben ab R4.3.1). Zum Zeitpunkt des Advisorys meldete CISA keine bekannte Ausnutzung. (100 %)
[https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03]

NICHT BEKANNT

• Wer die Angriffe ausgeführt hat und mit welchem Motiv

• Welcher Zugangsweg genau genutzt wurde: bekannte Schwachstelle, schwache oder Standard-Zugangsdaten oder ein Dienstleister-Zugang

• Ob eine der bekannten Danfoss-Schwachstellen ausgenutzt wurde. Laut Next und lebigdata ist das nicht belegt, laut einem von franceinfo zitierten Experten wurde eine dokumentierte Lücke genutzt (widersprüchlich).

• Ob alle Vorfälle bei Danfoss, Copeland und Dixell von denselben Tätern stammen

• Ob die berichteten Vorfälle in den Niederlanden und Belgien mit dem Fall zusammenhängen

WAHRSCHEINLICH (Einschätzung)

• Die Angreifer kamen über Weboberflächen der Steuerungen, die direkt aus dem Internet erreichbar waren, und nicht über die Büro-IT der Händler. (80 %) – A und B übereinstimmend. CERT-FR nennt die Exposition ausdrücklich, CERT-FR und Danfoss empfehlen als Erstes, den Internetzugang zu trennen, und heise und das BSI sprechen von ungepatchten, erreichbaren Anlagen. Eine forensische Bestätigung wurde nicht veröffentlicht.

• Schwache oder unveränderte Standard-Zugangsdaten haben den Zugriff erleichtert. (60 %) – Dafür sprechen die BSI-Aussage zu unzureichend gesicherten Passwörtern ab Werk und die Empfehlung von CERT-FR, Standardpasswörter zu ändern. Für die konkreten Fälle gibt es keinen Beleg.

• Die Angreifer haben eine öffentlich bekannte Schwachstelle in veralteter Firmware ausgenutzt (widersprüchlich: A: laut Next/lebigdata nicht belegt / B: laut einem von franceinfo zitierten Experten eine dokumentierte Lücke, ANSSI soll laut Regierungsumfeld eine Schwachstelle in dänischer Software gefunden haben). (50 %) – Es gibt CISA-Advisories zu den Danfoss-Geräten, und Danfoss nennt veraltete Firmware. Eine offizielle Bestätigung einer konkreten CVE fehlt, die Quellen widersprechen sich, deshalb ist der Wert gesenkt.

• Das Ziel war Sabotage, nicht Erpressung oder Datendiebstahl. (65 %) – Es gibt keine Lösegeldforderung und kein Bekennerschreiben. Der Schaden ist rein physisch und zielte auf Lebensmittel, viele Ketten wurden in kurzer Zeit getroffen. Der Experte Domingo spricht von Schadensabsicht. Das Motiv bleibt offen. A und B nennen 60 bzw. 70 %.

• Hinter der Kampagne steckt ein staatlicher oder staatsnaher Threat Actor (hybride Kriegsführung). (25 %) – Das vermuten bisher nur einzelne Fachleute (SRF-Redaktor Widmer, PwC Österreich). Keine Behörde hat eine Attribution vorgenommen, technische Belege fehlen, und auch Hacktivisten oder Kriminelle kommen in Frage.

2. Was ist die Auswirkung?

WISSEN

• Finanzminister Roland Lescure hat vor dem Parlament von rund 700 betroffenen Märkten von etwa 10.000 gesprochen und sieht kein Risiko für die Versorgung. Laut netzwelt (nach Tagesschau) stammt die Zahl von der Pariser Staatsanwaltschaft. (100 %)
[https://cedarnews.net/francais/1057906/quand-on-decouvert-lattaque-elle-nous-inquietes/ ; https://netzwelt.de/news/259561-verdorbene-lebensmittel-sagen-aldi-lidl-kaufland-cyberattacke-supermarkt-kuehlsysteme-frankreich.html]

• Betroffen sind mindestens 300 Intermarché- und Netto-Märkte, weniger als 100 Märkte von Coopérative U, 80 Carrefour-Märkte, rund 30 Monoprix-Filialen und mehrere E.Leclerc-Märkte. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/un-piratage-pas-si-sophistique-que-ca-ce-que-l-on-sait-de-la-cyberattaque-qui-a-fait-monter-en-temperature-les-frigos-de-supermarches_8235061.html]

• Die Zahl der Märkte ist widersprüchlich: 150 (SRF), 250–350 (BleepingComputer), über 300 (futurezone), rund 500 (Der Bund/Borncity) und rund 700 von etwa 10.000 (Lescure bzw. Pariser Staatsanwaltschaft). (100 %) [https://netzwelt.de/news/259561-verdorbene-lebensmittel-sagen-aldi-lidl-kaufland-cyberattacke-supermarkt-kuehlsysteme-frankreich.html ;

https://bleepingcomputer.com/news/security/cyberattack-shuts-down-refrigerators-at-french-supermarkets]

• Einzelschäden: ein Hypermarkt 180.000–200.000 €, zwei Intermarché in Haguenau zusammen 270.000 €, Issy-les-Moulineaux 55.000 €, Étréchy rund 60.000 €. Insgesamt geht es geschätzt um mehrere Millionen Euro. Laut Intermarché zahlen die Versicherungen oft nicht. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/un-piratage-pas-si-sophistique-que-ca-ce-que-l-on-sait-de-la-cyberattaque-qui-a-fait-monter-en-temperature-les-frigos-de-supermarches_8235061.html]

• Laut Pariser Staatsanwaltschaft (via AFP) wurden Kühlschränke über Nacht stundenlang auf 50 °C erhitzt, und es kam zu Brandausbrüchen („départs de feu"). (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/des-centaines-de-frigos-mis-hors-service-apres-une-cyberattaque-contre-les-supermarches_8234473.html ; https://next.ink/261236/des-frigos-pirates-dans-des-supermarches-a-cause-dequipements-obsoletes-ou-non-mis-a-jour/]

• Fachleute rechnen höchstens mit vorübergehenden lokalen oder regionalen Engpässen, nicht mit flächendeckenden (Thomas Kress). (100 %) [https://netzwelt.de/news/259561-verdorbene-lebensmittel-sagen-aldi-lidl-kaufland-cyberattacke-supermarkt-kuehlsysteme-frankreich.html]

NICHT BEKANNT

• Die gesicherte Gesamtzahl betroffener Märkte

• Die Gesamtschadenssumme und ob Versicherungen zahlen

• Ob verdorbene Ware verkauft wurde (dafür gibt es keine Hinweise)

• Wie groß und wie schwer die Brände waren

WAHRSCHEINLICH (Einschätzung)

• Die Versorgung der Bevölkerung war nicht ernsthaft gefährdet, es gab nur leere Kühlregale in einzelnen Märkten. (85 %) – A und B übereinstimmend. Der Minister hat das ausdrücklich gesagt, die Märkte blieben offen, und Fachleute sehen allenfalls lokale Engpässe. Ein Rest an Unsicherheit bleibt, weil die Angriffe laut CERT-FR weiterlaufen können.

• Die Gesundheit von Kunden war nicht gefährdet, weil die Ware erkannt und entsorgt wurde. (70 %) – Temperaturüberwachung und Teams haben die Ausfälle bemerkt (Beispiel Bordeaux). Bei Hunderten Märkten lässt sich eine Lücke aber nicht ganz ausschließen.

• Die Zahl 700 ist die vollständigste Zählung, weil sie alle Ketten umfasst. (55 %) – Es ist die einzige amtliche Gesamtzahl. Die niedrigeren Zahlen beziehen sich oft auf einzelne Ketten oder frühere Zeitpunkte. Eine Methodik ist nicht veröffentlicht, und die Quellen schreiben die Zahl unterschiedlich zu (Minister bzw. Staatsanwaltschaft).

• Der Gesamtschaden liegt im zweistelligen Millionenbereich (widersprüchlich: A: rechnerisch zweistellig / B: Schätzung „mehrere Millionen"). (45 %) – Hunderte Märkte mal Einzelschäden von 55.000–270.000 € ergeben rechnerisch einen zweistelligen Millionenbetrag. Öffentlich genannt sind nur „mehrere Millionen", deshalb ist der Wert gesenkt.

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

WISSEN

• Für kompromittierte Geräte empfiehlt CERT-FR: Internetzugang trennen, auf Werkseinstellungen zurücksetzen, Zugriff nur über VPN wieder einrichten, neu konfigurieren und die Firmware aktualisieren. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Bei End-of-Life-Geräten ohne Patch entfernt ein Reset zwar die Persistenz, das Gerät bleibt aber verwundbar und wird voraussichtlich erneut kompromittiert. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Danfoss empfiehlt, die AK-SC 355 durch die AK-SM-800-Reihe zu ersetzen. Die AK-SM 800A bekommt weiterhin Updates. (100 %) [https://next.ink/261236/des-frigos-pirates-dans-des-supermarches-a-cause-dequipements-obsoletes-ou-non-mis-a-jour/]

• Laut einem Bericht sollten die Anlagen am 12.10. wieder laufen. Die Fernsteuerung bleibt aber bis zum Patch abgeschaltet. (100 %) [https://borncity.com/blog/2026/10/13/cyberangriff-auf-danfoss-kuehlanlagen-details-und-hintergruende/]

• Ein Markt in Issy-les-Moulineaux hat die digitale Anbindung seiner Kühlschränke getrennt. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/un-piratage-pas-si-sophistique-que-ca-ce-que-l-on-sait-de-la-cyberattaque-qui-a-fait-monter-en-temperature-les-frigos-de-supermarches_8235061.html]

NICHT BEKANNT

• Wie viele Märkte ihre Steuerungen schon bereinigt haben und wieder normal laufen

• Wie lange EOL-Steuerungen ohne Fernwartung im Notbetrieb bleiben müssen

• Ob die Angreifer eine Persistenz hinterlassen haben (CERT-FR deutet das an, Details gibt es nicht)

• Ob CERT-FR IoCs nachliefert (bisher keine)

WAHRSCHEINLICH (Einschätzung)

• Die Kühlung selbst lief in den meisten Märkten nach Stunden bis wenigen Tagen wieder: trennen, zurücksetzen, neu einstellen. Die Anlagen lassen sich auch ohne Fernzugang vor Ort steuern. (70 %) – A und B übereinstimmend. Das entspricht dem Vorgehen nach CERT-FR, den Berichten über den Neustart am 12.10. und den geöffneten Märkten. Der Engpass ist der Kältetechniker vor Ort, nicht die IT. Eine Statistik dazu gibt es nicht.

• Die saubere digitale Wiederherstellung mit Austausch der EOL-Steuerungen und abgesicherter Fernwartung dauert Wochen bis Monate. (65 %) – Laut CERT-FR sind EOL-Geräte auch nach einem Reset verwundbar. Bei Hunderten Märkten hängen Hardware, knappe Kältefachbetriebe und Termine voneinander ab. Konkrete Angaben dazu gibt es nicht.

• Einige Märkte arbeiten vorübergehend ohne Fernwartung und kontrollieren die Kühlung manuell. (65 %) – Für Issy-les-Moulineaux ist das belegt. Borncity berichtet, dass die Fernsteuerung bis zum Patch abgeschaltet bleibt, und CERT-FR empfiehlt die Trennung vom Internet.

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

WISSEN

• Laut Staatsanwaltschaft gab es in einzelnen Märkten Brandausbrüche („départs de feu“). franceinfo berichtet, dass Geräte teils Feuer gefangen haben. (100 %) [https://orf.at/stories/3444862/ ; https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/un-piratage-pas-si-sophistique-que-ca-ce-que-l-on-sait-de-la-cyberattaque-qui-a-fait-monter-en-temperature-les-frigos-de-supermarches_8235061.html]

• Laut Intermarché wurden die Produkte aus den betroffenen Geräten entnommen, einige Frisch- und Tiefkühlregale waren außer Betrieb. (100 %)
[https://bleepingcomputer.com/news/security/cyberattack-shuts-down-refrigerators-at-french-supermarkets]

• Bei Dixell-Geräten soll in der zweiten Nacht ein Sollwert von 150 °C statt −22 °C gesetzt worden sein. Das war ein eingestellter Wert, kein gemessener, und stammt aus einem einzelnen, nicht unabhängig geprüften Fallbericht. (100 %)
[https://www.lebigdata.fr/cyberattaque-des-supermarches-une-deuxieme-vague-fait-monter-les-frigos-a-150-c]

NICHT BEKANNT

• Ob Verdichter, Verdampfer, Kältekreise oder Abtauheizungen bleibend beschädigt sind

• Ob die Brände durch die Heizstäbe beim Abtauen verursacht wurden

• Wie viele Geräte wegen der Brände ausgetauscht werden müssen

• Ob Ersatz-Steuerungen in ausreichender Zahl lieferbar sind

WAHRSCHEINLICH (Einschätzung)

• Der größte Teil des Schadens ist die Ware, nicht die Hardware. Die meisten Anlagen sind mechanisch intakt. (70 %) – A und B übereinstimmend. Das Abtauen ist eine normale Betriebsfunktion, gemeldet wurden vor allem Warenverluste, und Brände gab es nur in Einzelfällen.

• In einzelnen Märkten mit Brandschäden fallen Kühlschränke oder Teile davon für Wochen aus. (45 %) – Die Brände sind bestätigt, ihr Umfang nicht. Bei Brandschäden sind Austausch und Ersatzteile nötig, Lieferzeiten im Einzelfall sind aber nicht belegt. A und B nennen 50 bzw. 45 %.

• Der Ersatz veralteter Steuerungen im großen Stil dauert Monate. (55 %) – Danfoss empfiehlt die Migration. Ob sie kommt, ist eine Investitionsentscheidung, und Liefermengen und Fachbetriebe sind knapp.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Laut International Cyber Digest (Shodan-Screenshot, via netzwelt) und BleepingComputer sind weltweit rund 4.500 Danfoss-Systeme öffentlich erreichbar. Laut International Cyber Digest liegen davon 2.960 in Frankreich. Deutschland ist nicht unter den Top 5, hat aber ebenfalls exponierte Systeme. Die Zahl stammt aus einem Social-Media-Post und ist nicht unabhängig geprüft. (100 %) [https://netzwelt.de/news/259561-verdorbene-lebensmittel-sagen-aldi-lidl-kaufland-cyberattacke-supermarkt-kuehlsysteme-frankreich.html ; https://bleepingcomputer.com/news/security/cyberattack-shuts-down-refrigerators-at-french-supermarkets]

• Predicta Lab fand am 12.10. 2.752 erreichbare Danfoss-Systeme, davon 1.590 in Frankreich (widersprüchlich zu 2.960 in Frankreich laut International Cyber Digest). (100 %) [https://bleepingcomputer.com/news/security/cyberattack-shuts-down-refrigerators-at-french-supermarkets]

• Claroty Team82 zählte per Censys 2.765 erreichbare AK-SM 800A. Das sagt laut Claroty nichts über den Firmware-Stand aus. (100 %) [https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers]

• heise security hat in Deutschland nur wenige möglicherweise verwundbare Systeme gefunden und nicht geprüft, ob sie wirklich verwundbar sind. (100 %) [https://www.heise.de/news/BSI-gemahnt-auch-Betreiber-kleiner-vernetzter-Anlagen-11487069.html]

• Das BSI warnt ausdrücklich auch Betreiber kleiner Anlagen wie Solar-Wechselrichter, Kühlanlagen, einzelne Windräder und Trinkwasserstellen. (100 %) [https://www.heise.de/news/BSI-gemahnt-auch-Betreiber-kleiner-vernetzter-Anlagen-11487069.html]

• Für Copeland XWEB Pro sind mehrere kritische Schwachstellen veröffentlicht, u. a. eine Authentifizierungsumgehung (CVE-2026-21718). (100 %) [https://nvd.nist.gov/vuln/detail/CVE-2026-21718]

• Spar Österreich setzt die in Frankreich betroffenen Steuerungen nach eigener Aussage nicht ein. (100 %) [https://www.topagrar.com/oesterreich/nach-cyberangriffen-auf-supermarkte-wie-sicher-ist-osterreich-20030130.html]

• Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 142581 gesamt (DNP3 33176, OMRON FINS 22996, ProConOS 16412, EtherNet/IP 15788, Siemens S7 8290, OPC UA 5651) (100 %)

NICHT BEKANNT

• Belastbare Zahlen für Deutschland, Österreich und die Schweiz

• Wie viele der erreichbaren Systeme noch verwundbare Firmware haben

• Wie viele Copeland- und Dixell-XWEB-Systeme exponiert sind, auch im DACH-Raum

• Welche Ketten in DACH die betroffenen Gerätefamilien überhaupt einsetzen

WAHRSCHEINLICH (Einschätzung)

• Weltweit sind einige tausend Kälte-Steuerungen der genannten Hersteller direkt aus dem Internet erreichbar. (85 %) – Mehrere unabhängige Scans (Shodan, Censys, Predicta Lab) kommen allein für Danfoss auf 2.700 bis 4.500 Systeme.

• In Deutschland sind eher Dutzende als Hunderte Systeme dieser Hersteller direkt erreichbar. (45 %) – Heise spricht von einer geringen Zahl, und Deutschland ist nicht in den Top 5. Genaue Zählungen fehlen, und Zugänge über Mobilfunk-Router oder Cloud sind in Scans oft unsichtbar.

Lage

In der Nacht vom 11. auf den 12. Oktober 2026 haben Unbekannte in Frankreich Steuerungen von Kühlanlagen in Supermärkten aus der Ferne manipuliert. Die Steuerungen waren über das Internet erreichbar. Die Kühlschränke liefen im Dauer-Abtaumodus und heizten auf bis zu 50 °C auf. Ware verdarb, und laut Pariser Staatsanwaltschaft gab es in einigen Märkten Brandausbrüche. Laut Finanzminister Lescure sind rund 700 von etwa 10.000 Märkten betroffen,

andere Quellen nennen deutlich niedrigere Zahlen (widersprüchlich). CERT-FR hat seine Warnung am 13.10. von Danfoss AK-SM/AK-SC auf Copeland und Dixell XWEB ausgeweitet und hält die Kampagne für wahrscheinlich noch aktiv. Danfoss spricht vor allem von End-of-Life-Geräten bzw. Geräten mit veralteter Firmware. Täter, Motiv und genauer Zugangsweg sind offen. Deutschland, Österreich und die Schweiz melden bisher keine betroffenen Märkte.

Täter	unbekannt – unbekannt

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