

Cyberangriff auf Danfoss-Kühlsteuerungen: Kühlanlagen in französischen Supermärkten auf 50 °C gestellt

Stand 15.10.2026 14:20 · Sendung: – · · Belegstärke: **bestätigt** · berichtet · **vermutet** · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand

■ Wissen 50 % ■ Wahrscheinlich 19 % ■ Nicht bekannt 31 %

Hergang, Schadensbild, betroffene Produktfamilien und die grobe Größenordnung sind durch CERT-FR, die Regierung, die Staatsanwaltschaft, Hersteller und Handelsketten gut belegt (A und B übereinstimmend). Weiter offen sind Täter, Motiv, genauer Angriffsweg, die genutzte Schwachstelle und die genaue Zahl betroffener Märkte. Die Zählungen reichen von 350 bis rund 700 Märkten, A nennt auch Angaben ab 150.

1. Was ist passiert, und warum?

WISSEN

- CERT-FR-Alarm CERTFR-2026-ALE-012 (Erstversion 12.10.2026, am 13.10.2026 um Copeland/Dixell erweitert): CERT-FR meldet zahlreiche Kompromittierungen von Fernsteuerungen für Kälteanlagen. Betroffen sind Danfoss AK-SM, Danfoss AK-SC, Copeland xweb und Dixell xweb. (100 %) [<https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/>]
- CERT-FR nennt als Ursache allgemein, dass Management-Oberflächen direkt im Internet erreichbar waren, was guter Praxis widerspricht. Die Angriffskampagnen laufen wahrscheinlich weiter. End-of-Life-Geräte ohne Patch, die im Internet hängen, werden laut CERT-FR mit sehr hoher Wahrscheinlichkeit kompromittiert. (100 %) [<https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/>]
- Les Mousquetaires (Intermarché) bestätigen einen Angriff auf die Kälteanlagen mit Sollwerten bis 50 °C. Coopérative-U-Chef Dominique Schelcher bestätigt den Angriff ebenfalls. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/un-piratage-pas-si-sophistique-que-ca-ce-que-l-on-sait-de-l-a-cyberattaque-qui-a-fait-monter-en-temperature-les-frigos-de-supermarches_8235061.html]
- Die Angreifer haben die Abtaufunktion missbraucht und die Kühlschränke mit hohen Sollwerten auf Dauer-Abtauen gestellt (berichtet). (100 %) [<https://www.cnn.com/2026/10/14/europe/france-cyberattack-supermarket-fridges-intl/>]
- Danfoss spricht gegenüber Medien von 'incidents in France' mit 'a limited number of refrigeration management systems'. Die meisten betroffenen Geräte sind laut Danfoss ältere Modelle am Ende ihres Lebenszyklus: AK-SM800 ist seit 2021 End-of-Life, AK-SC355 seit 2016 ausgelaufen. Hinzu kommen AK-SM800A mit veralteter Firmware. Die Altsysteme erhalten keine Sicherheitsupdates mehr (auch berichtet von franceinfo und Reuters). (100 %) [<https://www.coolingpost.com/world-news/danfoss-moves-to-mitigate-cyberattack/> ; <https://complexdiscovery.com/refrigeration-hack-affected-about-700-french-supermarkets-government-says-as-danfoss-interfaces-stay-online/>]
- Copeland (Eigentümer von Dixell) spricht von einer Schwachstelle in einer eingestellten Controller-Generation, bestätigt aber keine Kompromittierungen in Frankreich (berichtet: Reuters/AP). (100 %) [<https://www.news4jax.com/business/2026/10/13/cyberattack-targeting-refrigeration-systems-hit-s-700-supermarkets-french-government-says/>]
- Die Staatsanwaltschaft Paris ermittelt von Amts wegen (Cybercrime-Abteilung, OFAC), und Premierminister Lecornu hat die ANSSI eingeschaltet. Bis 14.10. gab es weder ein Bekennterschreiben noch eine Lösegeldforderung, was die Ermittler laut Reuters verwundert (berichtet). (100 %)

[<https://www.nbcnews.com/world/europe/hackers-heat-french-supermarket-fridges-sparking-fires-spoiling-food-rcna603151> ; <https://www.tbsnews.net/worldbiz/europe/investigators-hunt-french-supermarket-fridge-hackers-no-claim-responsibility-1571811>]

- Berichtet: In der Nacht vom 12. auf den 13.10. gab es eine weitere Welle bei Märkten mit Dixell-Reglern (Gironde, Tarn). Dabei wurden mehrere Parameter pro Sekunde geändert, was ein Kältetechniker als automatisiert einschätzt (Le Monde via LeBigData). (100 %)

[<https://www.lebigdata.fr/cyberattaque-des-supermarches-une-deuxieme-vague-fait-monter-les-frigos-a-150-c>]

- Claroty Team82 hat Schwachstellen in Danfoss AK-SM 800A veröffentlicht: CVE-2025-41450 (Umgehung der Authentifizierung) und zwei weitere, die eine Anmeldung voraussetzen. Behoben sind sie in Firmware R4.3.1, laut CISA ist CVE-2025-41450 schon in R4.2 behoben. Laut Claroty ist nicht belegt, dass dieselben Lücken auch in den Altgeräten AK-SM800 und AK-SC355 stecken. (100 %) [<https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers>]

- CISA hat CVE-2025-41450 schon im Advisory ICSA-25-140-03 vom 20.05.2025 für AK-SM 8xxA vor R4.2 gemeldet. (100 %) [<https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03>]

NICHT BEKANNT

- Wer die Täter sind und welches Motiv sie haben.
- Über welchen Weg die Angreifer genau eingedrungen sind: CERT-FR nennt keinen Vektor, und unklar ist, welche Schwachstelle oder welche Zugangsdaten genutzt wurden.
- Ob die von Claroty/CISA beschriebenen CVEs tatsächlich ausgenutzt wurden.
- Welche Schwachstelle die ANSSI laut einer Reuters-Quelle aus dem Umfeld des Premierministers gefunden hat (nicht veröffentlicht).
- Ob Dienstleister-Plattformen der Kältetechnik-Firmen als Zwischenstation dienten.
- Ob die Angriffe auf Copeland/Dixell von denselben Tätern stammen.

WAHRSCHEINLICH (Einschätzung)

- Es war gezielte Sabotage und kein technischer Fehler. (97 %) – Mehrere Hersteller und Ketten waren gleichzeitig in der Nacht betroffen. CERT-FR spricht von Kompromittierungen, und die Staatsanwaltschaft ermittelt (B; A geht ebenfalls von einem Angriff aus).
- Die Angreifer haben vor allem direkt aus dem Internet erreichbare Steuerungen mit alter Firmware oder schwachem Schutz der Zugangsdaten massenhaft angesprochen, statt über eine zentrale Plattform oder einen Dienstleister-Zugang einzudringen. (70 %) – A und B kommen übereinstimmend auf 70 %. CERT-FR nennt die Internet-Exposition als Ursache, Danfoss verweist auf End-of-Life-Geräte und alte Firmware, und drei Hersteller sind betroffen. Scanner zählten vorher über 1.500 erreichbare Danfoss-Systeme in Frankreich, und ein Kältetechniker beschreibt automatisierte Änderungen. Offiziell bestätigt ist der Weg nicht.
- Ziel war Störung, Sabotage oder Demonstration und nicht Erpressung oder Geld. (70 %) – A schätzt 65 %, B 75 %. Es gab kein Lösegeld, kein Bekenntnis und keinen gemeldeten Datenabfluss, das Schadensbild ist rein physisch. Ein späteres Bekenntnis oder eine spätere Forderung ist möglich, laut Sekoia ist das Motiv unbekannt.
- Ein staatlicher Akteur im Rahmen hybrider Kriegsführung steckt dahinter. (20 %) – Dafür gibt es keinen Beleg. Die Einschätzung stammt aus Kommentaren (z. B. SRF), und Experten halten auch Gelegenheitstäter für möglich. B hält einen staatlichen Hintergrund nur für nicht ausschließbar.

2. Was ist die Auswirkung?

WISSEN

- Finanzminister Roland Lescure nannte im Parlament rund 700 von etwa 10.000 Supermärkten als betroffen. Die Lebensmittelversorgung sei nicht gefährdet, der Angriff treffe aber das Herz der Ernährungssicherheit (berichtet: AP). (100 %) [<https://www.news4jax.com/business/2026/10/13/cyberattack-targeting-refrigeration-systems-hits-700-supermarkets-french-government-says/> ; <https://complexdiscovery.com/refrigeration-hack-affected-about-700-french-supermarkets-government-says-as-danfoss-interfaces-stay-online/>]
- Nach Angaben der Händler sind betroffen: mindestens 300 Intermarché/Netto-Märkte, unter 100 Coopérative-U-Märkte (widersprüchlich: A 'knapp 100 bzw. 80 von 2.000' / B 'weniger als

100'), 80 Carrefour, rund 30 Monoprix (5 % von etwa 490) und mehrere E.Leclerc. (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]

- Zu den Schäden nennt Schelcher einige Zehntausend Euro für einen kleinen Markt und 180.000–200.000 € für einen Hypermarkt. Zwei Intermarché in Haguenau verloren zusammen 270.000 €, Étréchy etwa 60.000 €, Issy-les-Moulineaux etwa 55.000 €. (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 Intermarché decken Versicherungen diese Art von Vorfall oft nicht ab (berichtet). (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 Staatsanwaltschaft Paris und Reuters gab es neben Lebensmittelverlusten in mehreren Märkten auch Brände. Die Ermittlungen umfassen Geräte, die Feuer gefangen haben. Orte und Anzahl sind nicht genannt (berichtet). (100 %) [<https://www.nbcnews.com/world/europe/hackers-heat-french-supermarket-fridges-sparking-fires-spoiling-food-rcna603151> ; <https://www.tbsnews.net/worldbiz/europe/investigators-hunt-french-supermarket-fridge-hackers-no-claim-responsibility-1571811>]

- Thierry Cotillard (Les Mousquetaires/Intermarché) sprach gegenüber BFMTV von Verlusten im zweistelligen Millionenbereich ('zig Millionen') an einem einzigen Tag (berichtet: Reuters). (100 %) [<https://www.nbcnews.com/world/europe/hackers-heat-french-supermarket-fridges-sparking-fires-spoiling-food-rcna603151> ; <https://complexdiscovery.com/refrigeration-hack-affected-about-700-french-supermarkets-government-says-as-danfoss-integrates-stay-online/>]

- Kassensysteme und Kundendaten waren laut bisherigen Berichten nicht betroffen. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/des-magasins-systeme-u-et-intermarche-touche-par-une-cyberattaque-contre-leurs-installations-frigorifiques_8233720.html]

NICHT BEKANNT

- Die genaue Zahl betroffener Märkte, denn die Zählungen sind nicht einheitlich: 350 laut Reuters, etwa 400 laut BBC, rund 700 laut Regierung; A nennt Angaben ab 150.

- Der Gesamtschaden.

- Wie viele Brände es gab, wo, wie schwer und aus welcher Ursache.

- Wie groß die zweite Welle bei Dixell/Copeland war.

- Ob Märkte außerhalb Frankreichs betroffen sind, etwa in DE, ES, PT, BE oder PL: Sekoia hält das für möglich, behördlich bestätigt ist es nicht.

WAHRSCHEINLICH (Einschätzung)

- Für Verbraucher bestand keine Gesundheitsgefahr, weil betroffene Ware vorsorglich entsorgt wurde. (80 %) – A schätzt 85 %, B 80 %. Die Ketten melden Entsorgung, teils mit Protokoll eines Gerichtsvollziehers, und Erkrankungen sind nicht gemeldet. Ein Restrisiko besteht bei unbemerkt erwärmter Ware.

- Der Gesamtschaden liegt im zweistelligen Millionenbereich. (55 %) – A schätzt 60 %, B 55 %. Bei 300–700 Märkten mit Schäden von Zehntausenden bis 200.000 € pro Markt ist das rechnerisch plausibel und passt zu Cotillards 'zig Millionen'. Eine amtliche oder geprüfte Summe fehlt.

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

WISSEN

- CERT-FR empfiehlt für kompromittierte Geräte, sie vom Internet zu trennen, auf Werkseinstellungen zurückzusetzen, neu zu konfigurieren und danach nur noch per VPN zuzugreifen. Ein Reset allein reicht nicht, wenn das Gerät verwundbar bleibt. (100 %)

[<https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/>]

- Für die End-of-Life-Geräte von Danfoss (alte AK-SM/AK-SC) und für Copeland/Dixell-Altgeräte gibt es laut Berichten keinen Fix. Für AK-SM 8xxA bietet Danfoss Firmware an. (100 %)

[<https://techinformed.com/french-supermarket-cyberattack-triggers-wider-security-alert/>]

- Laut dem Handelsverband FCD waren einige Märkte bereits wieder in Betrieb (berichtet). (100 %) [<https://thehackernews.com/2026/10/attackers-heat-french-supermarket.html>]
- Les Mousquetaires haben zusätzlich 100 Märkte vorsorglich vom Internet getrennt (berichtet). (100 %) [<https://complexdiscovery.com/refrigeration-hack-affected-about-700-french-supermarkets-government-says-as-danfoss-interfaces-stay-online/>]
- Kassensysteme waren laut Berichten nicht betroffen. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/des-magasins-systeme-u-et-intermarche-touche-par-une-cyberattaque-contre-leurs-installations-frigorifiques_8233720.html]

NICHT BEKANNT

- Wie viele Märkte ihre Steuerungen schon bereinigt, abgesichert und vollständig wiederhergestellt haben.
- Wie schnell Kältetechnik-Dienstleister End-of-Life-Geräte ersetzen können.
- Ob Kassen- oder Warenwirtschaftssysteme mitbetroffen waren (bisher nein).

WAHRSCHEINLICH (Einschätzung)

- Die Kühlung läuft vielerorts schon wieder oder lässt sich lokal innerhalb von Stunden bis wenigen Tagen sicher betreiben, sobald Sollwerte korrigiert und die Geräte vom Internet getrennt sind. (75 %) – A und B schätzen beide 75 %. Die Manipulation betraf Einstellungen und keine verschlüsselten Daten. Die Sofortmaßnahme ist technisch einfach und von CERT-FR empfohlen, und Märkte meldeten früh den Wiederbetrieb.
- Eine dauerhaft sichere Wiederherstellung dauert Wochen bis Monate. Dazu gehören der Ersatz der End-of-Life-Geräte und sicherer Remote Access per VPN statt direktem Zugang. (65 %) – A und B schätzen beide 65 %. Für End-of-Life-Geräte gibt es keinen Patch, also braucht es Hardwaretausch. Hunderte Standorte sind gleichzeitig betroffen, und die Kältefachbetriebe sind der Engpass. Danfoss rät seit Langem zur Migration.

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

WISSEN

- Laut Staatsanwaltschaft und Reuters gab es in mehreren Märkten Brände, die Ermittlungen umfassen Geräte, die Feuer gefangen haben. Details fehlen. (100 %) [<https://www.thestar.com.my/tech/tech-news/2026/10/14/copeland-dixell-refrigeration-systems-also-hacked-french-cybersecurity-agency-says> ; 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]
- Gemeldet sind manipulierte Sollwerte und Abtauzyklen, also Konfiguration und nicht primär zerstörte Hardware. (100 %) [<https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/>]
- Laut Danfoss sind viele betroffene Steuerungen End-of-Life und bekommen keine Sicherheitsupdates mehr. Sicher betreiben lassen sie sich nur durch Austausch oder strikte Abschottung. (100 %) [<https://www.coolingpost.com/world-news/danfoss-moves-to-mitigate-cyberattack/>]

NICHT BEKANNT

- Ob Kompressoren, Heizstäbe, Elektrik oder Kühlschränke durch den Dauer-Abtaubetrieb dauerhaft beschädigt wurden.
- Ausmaß und Ursache der Brände.
- Ob die Angreifer Persistenz eingerichtet haben (CERT-FR erwähnt Persistenzmechanismen nur allgemein).

WAHRSCHEINLICH (Einschätzung)

- Die Kältetechnik ist in den meisten Märkten mechanisch intakt, den Hauptschaden macht die verdorbene Ware aus. (65 %) – A schätzt 70 %, B 65 %. Abtauen ist eine normale Betriebsfunktion, Abtauheizungen sind dafür ausgelegt, Schutzfunktionen greifen in der Regel, und Märkte gingen wieder in Betrieb. Die gemeldeten Brände zeigen aber Einzelfälle mit Sachschaden.
- Vereinzelt gibt es Hardwareschäden an Abtauheizungen oder Verkabelung oder durch Brand, deren Behebung Wochen dauert. (45 %) – A schätzt 50 %, B 45 %. Brände sind berichtet, und ein

Dauer-Abtaubetrieb ist nicht vorgesehen. Technische Befunde liegen aber nicht öffentlich vor.

5. Wie viele solcher Ziele gibt es?

WISSEN

- Reuters fand am 13.10. per Shodan mindestens 4.500 öffentlich sichtbare Danfoss-Weboberflächen. Laut Onyphe nutzt nur eine kleine Minderheit die aktuelle Software. (100 %) [<https://www.euronews.com/2026/10/14/thousands-of-supermarket-fridges-still-exposed-after-cyberattack> ; <https://complexdiscovery.com/refrigeration-hack-affected-about-700-french-supermarkets-government-says-as-danfoss-interface-stay-online/>]
- Predicta Lab zählte am 12.10. 2.752 exponierte Danfoss-Systeme, davon 1.590 in Frankreich. Die Zahlen der verschiedenen Scanner lassen sich nicht addieren. (100 %) [<https://complexdiscovery.com/refrigeration-hack-affected-about-700-french-supermarkets-government-says-as-danfoss-interfaces-stay-online/>]
- Claroty zählte im August per Censys 2.765 exponierte AK-SM 800A. (100 %) [<https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers>]
- Laut Claroty sind auch nach dem Angriff noch exponierte Danfoss-Geräte online. (100 %) [<https://www.tomsguide.fr/cyberattaque-des-frigos-de-supermarches-des-appareils-danfoss-exposes-sont-toujours-en-ligne/>]
- BSI: In Deutschland gibt es keinen bestätigten Fall. Das BSI warnt Betreiber kleiner Anlagen wie Kühlung und Energieerzeugung. (100 %) [https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261013_OT-Gefaehrdung-Kleinanlagen.html]
- heise fand in Deutschland nur eine kleine Zahl potenziell verwundbarer, aus dem Internet erreichbarer Systeme, ohne zu prüfen, ob sie ausnutzbar sind. (100 %) [<https://www.heise.de/news/BSI-gemahnt-auch-Betreiber-kleiner-vernetzter-Anlagen-11487069.html>]
- Schweiz: Migros, Coop und Lidl Schweiz melden keine Betroffenheit, einzelne Migros-Filialen nutzen Danfoss. (100 %) [<https://www.srf.ch/news/international/hacker-gegen-supermaerkte-kuehlregale-im-visier-hybrider-angriff-auf-frankreich>]
- 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

- Wie viele solcher Steuerungen in Deutschland, Österreich und der Schweiz genau offen im Internet erreichbar sind (widersprüchlich: A fand keine öffentliche Zahl / B: heise spricht von einer kleinen Zahl in Deutschland, ohne Zahl zu nennen).
- Wie viele weitere Hersteller und Gerätetypen ähnlich exponiert sind.

WAHRSCHEINLICH (Einschätzung)

- Auch in DACH sind Kälte-Steuerungen direkt aus dem Internet erreichbar, wobei unklar ist, ob es Dutzende oder Hunderte sind (widersprüchlich: A schätzt mindestens Hunderte / B: heise fand in Deutschland nur eine kleine Zahl). (50 %) – Die Hersteller sind in DACH stark vertreten, die Muster der Fernwartung sind gleich, und weltweit gibt es Tausende Treffer. Die heise-Stichprobe spricht für Deutschland aber nur von wenigen Systemen, eine konkrete DACH-Zählung fehlt. Die Prozentangabe wurde wegen des Widerspruchs gesenkt.
- Das Problem betrifft weit mehr Anlagentypen als Kühlung, etwa PV-Wechselrichter, Gebäudeleittechnik und Wasser. (80 %) – Das BSI nennt ausdrücklich weitere Kleinanlagen wie Solarwechselrichter und Trinkwasserstellen, und frühere Advisories zeigen das gleiche Muster.

Lage

In der Nacht vom 11. auf den 12.10.2026 haben Unbekannte über das Internet die Fernsteuerungen von Kälteanlagen in Hunderten französischen Supermärkten manipuliert. Die Kühlschränke liefen im Dauer-Abtaubetrieb mit Sollwerten bis 50 °C, die Märkte mussten Ware entsorgen, und laut Staatsanwaltschaft Paris kam es auch zu Bränden. Die französische Regierung nennt rund 700 betroffene Supermärkte. CERT-FR nennt neben Danfoss AK-SM/AK-SC auch die xweb-Steuerungen von Copeland und Dixell und hält die Kampagnen für vermutlich noch aktiv. Die Pariser Staatsanwaltschaft ermittelt. Täter, Motiv und genauer Angriffsweg sind

offiziell nicht bekannt. Hersteller und Behörden verweisen auf direkt im Internet erreichbare, teils nicht mehr unterstützte Geräte.

Täter

unbekannt – unbekannt

Früherer Stand: Erstmeldung (12.10.2026 14:20)

Wissen 43 % · wahrscheinlich 22 % · nicht bekannt 35 %

In der Nacht vom 11. auf den 12.10.2026 haben Unbekannte aus der Ferne die Kühl- und Tiefkühlschränke in Supermärkten mehrerer französischer Ketten verstellt. Nach Berichten lösten sie die Abtauung dauerhaft aus und setzten den Sollwert auf bis zu 50 °C. Les Mousquetaires (Intermarché) und Coopérative U haben den Angriff bestätigt, und Les Mousquetaires ordnen ihn dem Zulieferer Danfoss zu. Viele Märkte mussten frische und tiefgekühlte Ware entsorgen. Täter, Angriffsweg, betroffene Firmware-Versionen und die Frage, ob die von Claroty Team82 im August 2026 veröffentlichten Schwachstellen genutzt wurden, sind offen. Ein Statement von Danfoss und eine Mitteilung einer Behörde fehlen bisher (Stand 12.10.2026).

Früherer Stand: Nach 24 Stunden (13.10.2026 14:37)

Wissen 46 % · wahrscheinlich 22 % · nicht bekannt 32 %

Am Abend des 11.10. und in der Nacht zum 12.10.2026 haben Angreifer per Remote Access die Kältesteuern in Hunderten französischen Supermärkten manipuliert. Sie erzwangen eine Dauer-Abtauung mit Sollwert bis 50 °C. Die Märkte mussten gekühlte und tiefgekühlte Ware entsorgen, und laut Staatsanwaltschaft Paris kam es teils zu Bränden. CERT-FR bestätigt zahlreiche Kompromittierungen von Danfoss AK-SM/AK-SC und nennt offen aus dem Internet erreichbare Management-Oberflächen als Problem. Danfoss nennt veraltete Altgeräte (AK-SM 800, AK-SC 355) und AK-SM 800A mit nicht aktualisierter Firmware. Am 13.10. hat CERT-FR auch Copeland xweb und Dixell xweb in seinen Alert aufgenommen. Täter, Motiv und der genaue Angriffsweg sind offiziell nicht geklärt. Sekoia nennt weitere Länder, darunter Deutschland, aber keine Behörde hat das bestätigt.

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