VORFALL-LAGEBILD

Erster öffentlich bekannter Cyberangriff auf eine Kühlanlage in der Schweiz: Metzgerei in Köniz BE

Stand 08.11.2026 15:34 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Nach allem, was bekannt ist, wurde in Köniz eine Kühlsteuerung manipuliert, die in eine europaweite Welle gegen offen erreichbare Kältetechnik passt.

2. Die Abhilfe ist bekannt: Steuerung raus aus dem offenen Internet, Fernwartung nur über gesicherten Zugang mit zweitem Faktor, Firmware aktuell halten (SANS CC4 Secure Remote Access und CC5 Risk-Based Vulnerability Management).

3. Auch kleine Betriebe schaffen das, wenn sie mit ihrem Kältetechniker eine Liste machen, was am Netz hängt und wer von wo zugreift.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Die Metzgerei schreibt: «Durch einen gezielten Cyberangriff wurde die elektronische Steuerung unserer Kühl- und Tiefkühlanlagen manipuliert».	100 %	100 %	bestätigt
Im Flyer ist von «erheblichen Temperaturabweichungen» die Rede. Die Anlage wurde vom Netzwerk getrennt und die Filiale vorübergehend geschlossen.	100 %	95 %	präzisiert
Betroffen ist die Filiale in Köniz-Liebefeld. Laut Blick hat die Kette insgesamt vier Standorte.	100 %	100 %	bestätigt
CERT-FR meldet seit dem 12.10.2026 zahlreiche Kompromittierungen von Fernsteuerungen für Kälteanlagen (Danfoss AK-SC und AK-SM, Copeland xweb, Dixell xweb). Grundproblem sind Verwaltungsoberflächen, die aus dem Internet erreichbar sind.	100 %	100 %	bestätigt
Der Fall gehört zur europäischen Angriffswelle auf Kältesteuerungen.	70 %	72 %	offen
Der Zugriff lief über eine aus dem Internet erreichbare Oberfläche der Kältesteuerung.	65 %	65 %	offen
Die Filiale ist geschlossen, die Wiedereröffnung ist für den 20. November geplant, sofern die Anlagen wieder zuverlässig kühlen.	100 %	100 %	bestätigt
Laut Inhaberin bzw. Inhaber erreichte der Tiefkühler 50 bis 70 Grad. Gefrorenes Fleisch war «wie gekocht», Preisschilder geschmolzen, und der Raum war nur mit Gesichtsmaske zu betreten.	100 %	100 %	bestätigt
Die anderen Filialen sind laut Berichten nicht betroffen, gemeldet wird nur die Schließung in Köniz.	100 %	85 %	präzisiert

Frühere Aussage	vorher	jetzt	Status
Die gesamte Kühl- und Tiefkühlware der Filiale musste entsorgt werden.	75 %	78 %	offen
Für die Bevölkerung bestand kein Gesundheitsrisiko.	70 %	70 %	offen
Laut Betreiber werden sämtliche Prozesse und Anlagen geprüft, Ziel ist die Wiedereröffnung am 20.11.	100 %	90 %	präzisiert
CERT-FR: Geräte ohne Patch, die weiter aus dem Internet erreichbar sind, bleiben gefährdet. Empfohlen werden Trennung vom offenen Internet, Firmware-Update, Modus «Strict» und Wechsel der Standardpasswörter.	100 %	100 %	bestätigt
Die reine Neueinrichtung der Steuerung dauert Tage. Die Zeit bis zum 20.11. geht vor allem in Prüfung, Reinigung und sichere Neuanbindung.	55 %	55 %	offen
Ältere Steuerungen ohne Updates werden ersetzt statt nur zurückgesetzt.	40 %	40 %	offen
Der Betreiber macht die Wiedereröffnung davon abhängig, dass die Anlagen wieder zuverlässig kühlen.	100 %	100 %	bestätigt
In Belgien haben die Angreifer Kühlgeräte in den Abtaumodus geschaltet, andernorts wurden Sollwerte auf bis zu 50 Grad gestellt.	100 %	90 %	präzisiert
Die Kältetechnik selbst ist weitgehend intakt, der Aufwand liegt bei Reinigung, Desinfektion und Steuerung.	55 %	55 %	offen
Der Kühlraum muss wegen Geruch und Hygiene aufwendig gereinigt werden, eventuell auch mit Ersatz von Dichtungen oder Einbauten.	50 %	50 %	offen
Laut Claroty-Zahlen, über die OCCRP berichtet, waren trotz eines Danfoss-Updates aus dem August 2025 weiterhin 2.765 Danfoss-Controller im Internet erreichbar (weltweit).	100 %	80 %	präzisiert
Betroffen waren Ketten in Belgien, Schweden, Irland, Estland, den Niederlanden, Finnland, Portugal und Italien, keine Kette mit mehr als einigen Dutzend Märkten.	100 %	75 %	präzisiert
Coop Schweiz hat Angriffsversuche registriert, die laut Coop erfolglos blieben. Migros hatte keine Hinweise auf einen Angriff.	100 %	100 %	bestätigt
Die Zahl der in Frankreich betroffenen Märkte wird unterschiedlich angegeben: Die Polizei spricht von bis zu 700, andere Berichte von 150 oder 350.	100 %	90 %	bestätigt

Neu seit dem letzten Stand

• Kantonspolizei Bern seit Montag 02.11. informiert, keine Anzeige, Sprecher Joël Regli: «Weitere Abklärungen sind im Gang» (20min).

• Betrieb hat rund 20 Mitarbeitende, Standorte Oberdiessbach, Köniz, Gerlafingen, Biel (bluewin).

• BACS-Empfehlungen: Updates, Trennung vom Büronetz, Remote Access mit 2FA (bluewin).

• US-Joint-Advisory von CISA, FBI, HHS, USDA, DOT vom 05.11.2026 (ic3.gov).

• Bekenntnis von NoName057(16) und Z-Pentest, unbestätigt (Paris Match, 04.11.).

• CERT-FR-Alarm: letzte Version 16.10.2026 mit überarbeiteten Empfehlungen, u. a. Modus «Strict»; Reset allein reicht nicht.

• Die frühere Angabe, das BACS habe einen meldepflichtigen Vorfall bestätigt, ließ sich nicht verifizieren.

Wissensstand



■ Wissen 48 % ■ Wahrscheinlich 23 % ■ Nicht bekannt 29 %

Was in Köniz passiert ist und welche Folgen es hat, ist über die Mitteilung der Metzgerei und mehrere unabhängige Medien gut belegt; Tatzeitpunkt, Steuerungshersteller, Zugangsweg und Täter sind öffentlich nicht bekannt, und die Einordnung in die Welle ist bisher eine Schlussfolgerung.

1. Was ist passiert, und warum?

WISSEN

• Die Metzgerei schreibt auf ihrer Webseite: «Durch einen gezielten Cyberangriff wurde die elektronische Steuerung unserer Kühl- und Tiefkühlanlagen manipuliert.» (100 %)
[https://www.watson.ch/schweiz/digital/169213020-metzgerei-luethis-fleischwaren-aus-der-schweiz-meldet-cyberangriff]

• Im Flyer der Metzgerei steht, die Anlage sei «vom Netzwerk getrennt» und die Filiale vorübergehend geschlossen worden. (100 %)
[https://www.20min.ch/story/koeniz-be-filiale-musste-schliessen-hacker-greifen-berner-metzgerei-an-103662735]

• Betroffen ist die Filiale in Köniz-Liebefeld. Die Kette hat vier Standorte (Oberdiessbach, Köniz, Gerlafingen, Biel) und rund 20 Mitarbeitende. (100 %)
[https://www.bluewin.ch/en/digital/now-in-switzerland-too-cyberattack-on-a-swiss-butcher-shop-li.3662996]

• Die Kantonspolizei Bern wurde am Montag (02.11.2026) informiert und klärt ab. Bis zum Bericht lag keine Anzeige vor. Sprecher Joël Regli: «Weitere Abklärungen sind im Gang». (100 %)
[https://www.20min.ch/story/koeniz-be-filiale-musste-schliessen-hacker-greifen-berner-metzgerei-an-103662735]

• CERT-FR warnt seit dem 12.10.2026 vor Angriffen auf Kältesteuerungen: Danfoss AK-SC und AK-SM, Copeland xweb und Dixell xweb. Laut CERT-FR laufen die Kampagnen «probablement toujours en cours». (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Drei Volg-Filialen in der Schweiz meldeten verstellte Parameter in Kühlregalen (100 %)
[https://www.srf.ch/news/schweiz/kuehlanlage-manipuliert-berner-metzgerei-opfer-von-hackerangriff-auch-volg-betroffen]

• Beim BACS ist laut watson (07.11.2026) bisher eine meldepflichtige Meldung zu Angriffen auf gewerbliche Kühlanlagen eingegangen (100 %) [https://www.watson.ch/wirtschaft/schweiz/373139916-cyberangriffe-auf-kuehlanlagen-das-steckt-hinter-den-sabotage-wellen]

NICHT BEKANNT

• Wann der Angriff in Köniz stattfand (fest steht nur: Polizei am 02.11. informiert)

• Welcher Hersteller und welches Modell in Köniz eingebaut ist

• Über welchen Zugang die Angreifer kamen (Weboberfläche, Fernwartung des Dienstleisters, Zugangsdaten)

• Wer dahintersteckt und warum

• Ob die beim BACS eingegangene meldepflichtige Meldung zu Kühlanlagen den Fall Köniz betrifft

WAHRSCHEINLICH (Einschätzung)

• Der Fall gehört zur europäischen Welle in der Nacht zum 02.11.2026. (72 %) – Die Polizei wurde am Montag 02.11. informiert, also in der Woche der zweiten Welle; das Muster passt (Heizen statt Kühlen, kein Lösegeld). Die Tatzeit in Köniz ist nicht bekannt, behördlich bestätigt ist der Zusammenhang nicht.

• Der Zugriff lief über eine aus dem Internet erreichbare Oberfläche der Kältesteuerung oder ihres Fernwartungszugangs. (65 %) – CERT-FR, BSI und US-Behörden raten vor allem, die Geräte

aus dem offenen Internet zu nehmen; den konkreten Einstiegsweg haben die Behörden nicht veröffentlicht. Für Köniz gibt es keinen Beleg.

• Motiv ist Sabotage oder Aufmerksamkeit, keine Erpressung. (60 %) – Für Köniz ist weder eine Lösegeldforderung noch ein Datenabfluss gemeldet. Laut Paris Match (04.11.2026) haben sich die pro-russischen Gruppen NoName057(16) und Z-Pentest für die Welle bekannt; unabhängig bestätigt ist das nicht.

2. Was ist die Auswirkung?

WISSEN

• Laut Inhaber wurden im Tiefkühler 50 bis 70 Grad vorgefunden, das Fleisch war «wie gekocht», Preisschilder schmolzen, der Raum war nur mit Mundschutz betretbar. (100 %)
[https://www.srf.ch/news/schweiz/kuehlanlage-manipuliert-berner-metzgerei-opfer-von-hackerangriff-auch-volg-betroffen]

• Die Anlage wurde vom Netz getrennt, die Filiale geschlossen. Die Wiedereröffnung ist für den 20.11. geplant, wenn die Kühlung bis dahin zuverlässig läuft (100 %)
[https://www.bluewin.ch/en/news/first-known-cyberattack-on-a-cooling-system-in-switzerland-li.3662790]

• Die Höhe des Schadens kommentiert der Betrieb nicht. Eine Bildunterschrift kündigt zur Wiedereröffnung ein «100 Prozent frisches Sortiment» an. (100 %)
[https://www.20min.ch/story/koeniz-be-filiale-musste-schliessen-hacker-greifen-berner-metzgerei-an-103662735]

• Laut dpa sprach EU-Agrarkommissar Christophe Hansen von einem gezielten Versuch, die Lebensmittelversorgung zu stören und das Vertrauen der Verbraucher zu untergraben. Die Versorgungssicherheit sei derzeit aber nicht gefährdet (100 %) [https://lebensmittelpraxis.de/handel-aktuell/zentrale-management/50246-cyberkriminalitaet-hacker-heizen-kuehlanlagen-in-supermaerkten-auf.html]

NICHT BEKANNT

• Die Schadenshöhe

• Wie viel Ware genau entsorgt wurde

• Ob eine Kunde oder ein Kunde verdorbene Ware gekauft hat

WAHRSCHEINLICH (Einschätzung)

• Die gesamte Kühl- und Tiefkühlware der Filiale wurde entsorgt. (78 %) – Bei 50 bis 70 Grad bleibt lebensmittelrechtlich nichts verkaufsfähig, dazu passt das angekündigte «100 Prozent frische Sortiment»; ausdrücklich gesagt hat es niemand.

• Für die Bevölkerung bestand kein Gesundheitsrisiko. (70 %) – Der Schaden war offensichtlich (Geruch, geschmolzene Etiketten), der Laden wurde sofort geschlossen. Eine behördliche Aussage dazu fehlt.

• Die anderen drei Filialen sind nicht betroffen. (85 %) – Alle Berichte nennen nur Köniz; ausdrücklich ausgeschlossen hat es der Betrieb nicht.

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

WISSEN

• Geplant ist die Wiedereröffnung am 20.11.2026, unter der Bedingung, dass die Kühlung zuverlässig läuft. (100 %)
[https://www.bluewin.ch/en/news/first-known-cyberattack-on-a-cooling-system-in-switzerland-li.3662790]

• CERT-FR empfiehlt, die Geräte aus dem offenen Internet zu nehmen, die Firmware zu aktualisieren, den Modus «Strict» zu nutzen und Standardpasswörter zu ändern. Geräte ohne Patch (End of Life), die weiter erreichbar sind, bleiben laut CERT-FR stark gefährdet (100 %)
[https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Laut Danfoss sind vor allem ältere Produkte betroffen. Genannt werden laut Fachpresse AK-SM 800 (End of Life seit Mai 2021) und AK-SC 355 (2016 abgekündigt) (100 %)
[https://labs.cloudsecurityalliance.org/research/csa-research-note-danfoss-controller-french-retail-sabotage/]

• Das BACS empfiehlt regelmäßige Updates, Trennung vom Büronetz und Remote Access mit Zwei-Faktor-Authentisierung. (100 %)
[https://www.bluewin.ch/en/digital/now-in-switzerland-too-cyberattack-on-a-swiss-butcher-shop-li.3662996]

NICHT BEKANNT

• Ob in Köniz ein Altgerät ohne Patch eingebaut ist

• Ob die Steuerung ersetzt oder neu eingerichtet wird

• Ob es eine Datensicherung der Konfiguration gab

WAHRSCHEINLICH (Einschätzung)

• Die reine Neueinrichtung der Steuerung dauert wenige Tage; die Zeit bis zum 20.11. geht vor allem in Reinigung, Neubestückung und sichere Neuanbindung. (55 %) – Übliche Praxis bei Kältetechnikern; konkrete Angaben des Betriebs fehlen.

• Die Steuerung wird ersetzt statt nur zurückgesetzt. (40 %) – Bei Altgeräten ohne Patch rät CERT-FR davon ab, sie weiter erreichbar zu betreiben; welches Gerät in Köniz steht, ist unbekannt.

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

WISSEN

• Der Betreiber macht die Wiedereröffnung davon abhängig, dass die Anlagen zuverlässig kühlen. (100 %)
[https://www.bluewin.ch/en/news/first-known-cyberattack-on-a-cooling-system-in-switzerland-li.3662790]

• In Frankreich wurden Kühlregale in Supermärkten in den Abtaumodus geschaltet (100 %)
[https://www.bluewin.ch/en/digital/now-in-switzerland-too-cyberattack-on-a-swiss-butcher-shop-li.3662996]

• In der Oberpfalz veränderten die Angreifer laut Polizei die Temperatureinstellungen mehrerer Kühlhäuser einer Metzgerei auf bis zu 150 Grad. dpa schreibt, die Kühlhäuser hätten sich auf bis zu 150 Grad erhitzt; einen gemessenen Wert nennt die Polizei nicht (100 %) [https://www.infranken.de/bayern/cyberangriff-auf-metzgerei-in-der-oberpfalz-hacker-stellen-kuehlhaus-temperatur-auf-150-grad-art-6408573]

• Die US-Behörden warnen, Manipulationen könnten Warenverlust und Geräteschäden verursachen sowie die Temperaturanzeige ausfallen lassen (Denial of View) (100 %)
[https://www.ic3.gov/CSA/2026/261105.pdf]

NICHT BEKANNT

• Ob in Köniz Bauteile (Verdichter, Lüfter, Dichtungen, Sensoren) beschädigt sind

• Wie die Anlage technisch auf 50 bis 70 Grad kam (Abtauheizung, Sollwert)

WAHRSCHEINLICH (Einschätzung)

• Die Kältetechnik ist weitgehend intakt, der Aufwand liegt bei Reinigung, Desinfektion und Steuerung. (55 %) – Bekannte Fälle der Welle nennen Warenverlust, keine zerstörten Anlagen; 70 Grad über längere Zeit können Dichtungen und Kunststoffteile aber angreifen.

• Der Kühlraum wird aufwendig gereinigt, eventuell mit Ersatz von Dichtungen oder Einbauten. (50 %) – Geschmolzene Etiketten und Geruch sprechen dafür; bestätigt ist nichts.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Claroty Team82 zählte 2.765 aus dem Internet erreichbare Danfoss-AK-SM-800A-Oberflächen (Censys); wie viele davon verwundbar sind, ist offen. (100 %)
[https://refindustry.com/news/danfoss-copeland-and-trane-address-controller-security-vulnerabilities/]

• Nach dem Angriff in Frankreich fand eine Shodan-Suche mindestens 4.500 erreichbare Danfoss-Kältesteuerungen. (100 %)
[https://labs.cloudsecurityalliance.org/research/csa-research-note-danfoss-controller-french-retail-sabotage/]

• In Frankreich waren laut Berichten bis zu 700 Supermärkte betroffen. (100 %)
[https://www.bluewin.ch/en/digital/now-in-switzerland-too-cyberattack-on-a-swiss-butcher-shop-li.3662996]

• Coop Schweiz registrierte Angriffsversuche, laut Coop erfolglos. Migros, Lidl und Aldi Suisse haben keine Hinweise auf erfolgreiche Angriffe. (100 %) [https://www.netzwoche.ch/news/2026-11-02/update-angriffe-auf-kuehlanlagen-treffen-weitere-supermaerkte-auch-coop-im-visier]

• In den Niederlanden wurden Kühlanlagen bei 17 Firmen manipuliert. (100 %)
[https://www.dutchnews.nl/2026/11/albert-heijn-sister-chain-hit-as-fridge-hacks-spread-in-europe/]

NICHT BEKANNT

• Eine belastbare Zahl erreichbarer Kältesteuerungen in der Schweiz: Eine nach Ländern aufgeschlüsselte öffentliche Zählung ist nicht bekannt

• Wie viele kleine Betriebe (Metzgereien, Bäckereien, Gastro) solche Steuerungen per Fernwartung angebunden haben

WAHRSCHEINLICH (Einschätzung)

• Kleine Betriebe sind stärker gefährdet als große Ketten. (65 %) – Große Ketten melden erfolglose Versuche; Kleinbetriebe hängen meist am Fernwartungszugang ihres Kältetechnikers, ohne eigene IT-Sicherheit.

6. Kann das wieder passieren?

WISSEN

• CERT-FR: Kampagnen gegen diese Geräte laufen wahrscheinlich weiter. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• CISA, FBI, HHS, USDA und DOT warnten am 05.11.2026 vor einer laufenden Bedrohung für Kälte- und Kühlkettensysteme und raten: weg vom offenen Internet, Trennung vom Firmennetz, Updates. (100 %) [https://www.ic3.gov/CSA/2026/261105.pdf]

• Das BSI rät: Internetverbindung trennen, sonst VPN, Mehrfaktor-Anmeldung, Protokollfilter, Updates. (100 %) [https://www.heise.de/en/news/Cyberattacks-hit-refrigerators-in-Bavaria-and-North-Rhine-Westphalia-11509173.html]

NICHT BEKANNT

• Ob die Täter weitere Wellen planen

• Wie viele Schweizer Betreiber ihre Geräte inzwischen vom Netz genommen haben

WAHRSCHEINLICH (Einschätzung)

• Es kommt in den nächsten Wochen zu weiteren Fällen in DACH. (75 %) – Zwei Wellen in drei Wochen, Behörden gehen von andauernden Kampagnen aus, viele Geräte bleiben erreichbar.

• Derselbe Betrieb wird erneut getroffen, wenn das Gerät wieder offen erreichbar ist. (70 %) – Laut CERT-FR bleibt die Schwachstelle nach einem Reset bestehen; ob Köniz das Gerät vom Netz nimmt, ist unbekannt.

Lage

Bei Lüthi's Fleischwaren in Köniz-Liebefeld hat jemand die elektronische Steuerung der Kühl- und Tiefkühlanlagen manipuliert. Laut Inhaber wurden im Tiefkühler 50 bis 70 Grad vorgefunden. Die Filiale ist geschlossen und soll am 20.11.2026 wieder öffnen. Der Fall fällt zeitlich in die europäische Angriffswelle auf aus dem Internet erreichbare Kältesteuerungen, die in Frankreich am 12.10.2026 begann und in der Nacht zum 02.11.2026 mehrere Länder erreicht hat. Für Köniz selbst sind Hersteller, Zugangsweg und Täter nicht öffentlich bekannt.

Angriff	Manipulation der elektronischen Steuerung der Kühl- und Tiefkühlanlagen, im Tiefkühler laut Inhaber 50 bis 70 Grad vorgefunden.
Wann / Status	Tatzeitpunkt nicht öffentlich; Polizei am Montag 02.11.2026 informiert, öffentlich am 05.11.2026. · eingedämmt
Täter	Unbekannt. Für die europäische Welle haben sich die pro-russischen Gruppen NoName057(16) und Z-Pentest auf Telegram bekannt, unabhängig nicht überprüft. Ein Bekenntnis speziell zu Köniz ist nicht bekannt. – unbekannt
Betreiber / Branche	Lüthi's Fleischwaren, Filiale Köniz-Liebefeld · Lebensmittel, Metzgerei mit Direktverkauf
Anlage / Alter	Kühl- und Tiefkühlanlagen mit elektronischer, vernetzter Steuerung (Hersteller nicht öffentlich) · nicht bekannt
Region	Köniz, Kanton Bern, Schweiz

Auswirkungen	Lokal: eine Filiale geschlossen, Ware verdorben. Für die Bevölkerung keine Versorgungslücke; laut EU-Agrarkommissar Hansen ist die Versorgungssicherheit derzeit nicht gefährdet (dpa). In Frankreich soll auch die Kühlung beim Blutspendedienst EFS manipuliert worden sein; Schweizer Blutspendedienste kennen laut SDA keine solchen Fälle.
Behörden	Kantonspolizei Bern (Abklärungen, keine Anzeige bis 05.11.). BACS mit allgemeinen Empfehlungen; beim BACS ist laut watson eine meldepflichtige Meldung zu Kühlanlagen eingegangen, eine eigene Mitteilung zum Fall gibt es nicht. International: CERT-FR, BSI, Polizei Niederbayern und Regensburg, EU-Kommission (zwei Krisentreffen), CISA/FBI/HHS/USDA/DOT.
Regulatorik	Schweiz: Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ans BACS seit 01.04.2025 (Blick); eine einzelne Metzgerei fällt voraussichtlich kaum darunter, bei Großverteilern ist das offen (nicht geprüft). EU: CRA-Meldepflicht für aktiv ausgenutzte Schwachstellen seit 11.09.2026, strengere Herstellerpflichten ab Dezember 2027 (heise). Deutschland: NIS2-Umsetzung für Lebensmittelsektor ab Schwellenwerten; Kleinbetriebe in der Regel nicht erfasst.

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

• Aus dem Internet erreichbare Weboberfläche der Kältesteuerung (Altgerät ohne Patch oder bekannte Schwachstelle) (hoch): Für die Welle von CERT-FR, BSI und US-Behörden beschrieben; Danfoss nennt vor allem EOL-Geräte, für AK-SM 800A gibt es veröffentlichte Schwachstellen (CVE-2025-41450 bis 41452, Danfoss DSA-2025-03, CISA ICSA-25-140-03).

• Standard- oder schwache Zugangsdaten an einer erreichbaren Steuerung (hoch): CERT-FR empfiehlt ausdrücklich, Standardpasswörter zu ändern; die Bekennergruppen behaupten, Zugangsdaten veröffentlicht zu haben (unbestätigt).

• Fernwartungszugang oder Cloud-Portal des Kältedienstleisters (mittel): Kleine Betriebe werden meist vom Kältetechniker per Remote Access betreut; ein kompromittierter Dienstleisterzugang würde mehrere Kunden gleichzeitig öffnen. Für Köniz gibt es keinen Hinweis darauf.

• Zugriff über das Büro- oder Kassennetz (Phishing, Lateral Movement) (gering): Die Welle zeigt kein Ransomware- oder Datendiebstahlsmuster; Ziel war nur die Kältesteuerung.

Zeitleiste

20.05.2025 CISA-Advisory ICSA-25-140-03 zu Schwachstellen in Danfoss AK-SM 8xxA – bestätigt [https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03]

Nacht 11./12.10.2026 Frankreich: Kühlregale in Hunderten Supermärkten in den Abtaumodus geschaltet – berichtet [https://labs.cloudsecurityalliance.org/research/csa-research-note-danfoss-controller-french-retail-sabotage/]

12.10.2026 (Ergänzungen 13.10. und 16.10.) CERT-FR-Alarm CERTFR-2026-ALE-012 zu Danfoss AK-SC/AK-SM, Copeland und Dixell xweb – bestätigt [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

Nacht zum 02.11.2026 Zweite Welle: u. a. Reisbach (Niederbayern), Oberpfalz (bis 150 Grad), Belgien, Schweden, Niederlande, Luxemburg – berichtet [https://www.nordbayern.de/bayern/cyberangriff-auf-metzgerei-in-der-oberpfalz-kuhlhauser-erhitzen-sich-auf-bis-zu-150-grad-1.15340446]

02.11.2026 Coop Schweiz meldet erfolglose Angriffsversuche – berichtet [https://www.netzwoche.ch/news/2026-11-02/update-angriffe-auf-kuehlanlagen-treffen-weitere-supermaerkte-auch-coop-im-visier]

Montag, 02.11.2026 Kantonspolizei Bern wird zum Fall Köniz informiert – berichtet [https://www.20min.ch/story/koeniz-be-filiale-musste-schliessen-hacker-greifen-berner-metzgerei-an-103662735]

04.11.2026 Bekenntnis von NoName057(16) und Z-Pentest auf Telegram, nicht verifiziert – berichtet [https://www.parismatch.be/actualites/societe/2026/11/04/cyberattaques-contre-des-supermarches-des-hackers-prorusses-revendiquent-les-attaques-QSYUP7ZMKBFHDNM72SWSVNOFBM/]

05.11.2026, 12:16 Uhr SRF berichtet über Köniz und drei Volg-Filialen – berichtet [https://www.srf.ch/news/schweiz/kuehlanlage-manipuliert-berner-metzgerei-opfer-von-hackerangriff-auch-volg-betroffen]

05.11.2026 Gemeinsame Warnung von CISA, FBI, HHS, USDA und DOT zu Kälte- und Kühlkettensystemen – bestätigt [https://www.ic3.gov/CSA/2026/261105.pdf]

20.11.2026 Geplante Wiedereröffnung der Filiale Köniz – berichtet [https://www.bluewin.ch/en/news/first-known-cyberattack-on-a-cooling-system-in-switzerland-li.3662790]

Vergleichsfälle

• Frankreich, Hunderte Supermärkte im Abtaumodus (2026): Altgeräte ohne Patch, die offen im Netz hängen, lassen sich in einer Nacht massenhaft umstellen. [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Metzgerei Landkreis Neustadt a. d. Waldnaab, Kühlhäuser auf bis zu 150 Grad gestellt (2026): Früh erkannt hält der Schaden sich in Grenzen, Alarmierung zählt. [https://www.nordbayern.de/bayern/cyberangriff-auf-metzgerei-in-der-oberpfalz-kuhlhauser-erhitzen-sich-auf-bis-zu-150-grad-1.15340446]

• Edeka Reisbach, Kühlung auf 50 Grad (2026): Der Betreiber hat die Anlage vom Internet getrennt und will sie vorerst nicht wieder anschließen. [https://www.heise.de/en/news/Cyberattacks-hit-refrigerators-in-Bavaria-and-North-Rhine-Westphalia-11509173.html]

• Schwachstellen in Danfoss AK-SM 800A (Claroty Team82) (2025): Die Lücken waren seit 2025 bekannt und gepatcht; das Problem ist der Patch-Rückstand im Feld. [https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03]

Begriffe einfach erklärt

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

Kältesteuerung: Ein kleiner Computer, der Temperatur, Abtauen und Alarme der Kühlgeräte regelt.

Abtaumodus: Eine Funktion, die Eis vom Verdampfer schmilzt, indem sie kurz heizt; dauerhaft eingeschaltet wird die Kühlung zur Heizung.

Fernwartung / Remote Access: Der Zugang, über den der Techniker die Anlage aus der Ferne betreut.

Patch / Firmware-Update: Eine Software-Aktualisierung, die bekannte Sicherheitslücken schließt.

BACS: Bundesamt für Cybersicherheit der Schweiz, Meldestelle für Cybervorfälle.

Früherer Stand: Erstmeldung (05.11.2026 13:35)

Wissen 39 % · wahrscheinlich 27 % · nicht bekannt 34 %

Lüthi's Fleischwaren schreibt, ein gezielter Cyberangriff habe die elektronische Steuerung der Kühl- und Tiefkühlanlagen ihrer Filiale in Köniz-Liebefeld manipuliert. Die Anlagen wurden vom Netz(werk) getrennt, die Filiale bleibt bis voraussichtlich 20. November zu. Laut SDA und SRF ist es der erste öffentlich bekannte (laut SRF: der erste erfolgreiche) Fall dieser Art in der Schweiz. Er fällt in eine europäische Angriffswelle auf internetverbundene Kältesteuerungen, die am 11. und 12. Oktober in Frankreich begann und sich in der Nacht auf den 2. November auf weitere Länder ausgeweitet hat.

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