VORFALL-LAGEBILD

Angriff auf die Kühlanlagen eines Caterers in Holtwick (Bocholt): Die Überwachung hat größeren Schaden verhindert

Stand 15.11.2026 09:18 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. In Bocholt hat genau das funktioniert, was viele kleine Betriebe nicht haben: eine Überwachung, die Alarm schlägt, wenn die Temperatur wegläuft.

2. Die Angriffe sind opportunistisch, wer seine Steuerung offen im Netz hat oder den Fernwartungszugang nicht im Griff hat, kann getroffen werden, egal ob Supermarkt, Caterer oder Kühlhaus.

3. Die Gegenmaßnahmen kosten wenig: Steuerung raus aus dem offenen Internet, Fernwartung nur abgesichert mit zweitem Faktor, Altgeräte ersetzen und eine unabhängige Temperaturüberwachung.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Das BBV berichtet am 12.11.2026, 05:00 Uhr (Autor Fabian Wilmers), unter der Überschrift „Überwachungssystem verhindert riesigen Schaden“ über einen Cyberangriff auf die Kühlanlagen von ABH Event- und Gastroservice in Holtwick. Zwischenüberschriften: „Fernzugriff als Einfallstor“ und „Überwachung verhindert Schaden“. Geschäftsführer Jan Hellwig erklärt laut Vorspann, wie es dazu kam.	100 %	100 %	bestätigt
Holtwick ist ein Ortsteil von Bocholt (Kreis Borken, PLZ 46399) mit Gewerbegebiet. Nicht zu verwechseln mit Holtwick in Rosendahl (Kreis Coesfeld).	100 %	100 %	bestätigt
Das BSI hat Vorfälle bei einzelnen Supermärkten in Deutschland und weiteren europäischen Ländern bestätigt, bei denen aus dem Internet erreichbare Kühlsteuerungen manipuliert wurden (Pressemitteilung 13.10.2026, aktualisiert 03.11.2026).	100 %	90 %	präzisiert
Frankreichs Außenminister Barrot schrieb die Angriffe vom 11./12. Oktober am 09.11.2026 den iranischen Revolutionsgarden zu. Die Pariser Staatsanwaltschaft nennt die Einheit Shahid Kaveh, Angreifer hätten über Weboberflächen Dauer-Abtauzyklen ausgelöst und Temperaturalarme abgeschaltet.	100 %	85 %	präzisiert
Der Bocholter Fall gehört zum Muster der europäischen Welle (Manipulation von Kühlsteuerungen über Fernzugriff).	65 %	65 %	offen

Frühere Aussage	vorher	jetzt	Status
Derselbe Täter wie in Frankreich steckt dahinter.	35 %	30 %	offen
Laut BBV-Überschrift hat ein Überwachungssystem einen „riesigen Schaden“ verhindert.	100 %	100 %	bestätigt
Zum Vergleich: In Lilienthal bei Bremen musste ein Händler laut eigener Aussage Ware für über 360.000 Euro wegwerfen, in Reisbach (Niederbayern) wurden Kühlanlagen laut Markt auf bis zu 50 Grad hochgeheizt.	100 %	100 %	bestätigt
Das BSI sieht die Versorgungssicherheit in Deutschland nicht gefährdet.	100 %	95 %	bestätigt
Der Schaden in Bocholt ist deutlich kleiner als bei den Supermärkten mit Totalverlust der Kühlware.	70 %	70 %	offen
CERT-FR empfiehlt für kompromittierte Geräte: Internet-Erreichbarkeit entfernen, Gerät neu starten oder auf Werkseinstellung zurücksetzen, neu konfigurieren, Zugang nur per VPN wiederherstellen. Ein Reset allein reicht nicht, weil das Gerät verwundbar bleibt.	100 %	95 %	bestätigt
Die reine Wiederherstellung der Kühlsteuerung dauert Stunden bis wenige Tage, nicht Wochen.	60 %	55 %	präzisiert
CISA und FBI warnen, dass erzwungene Heiz- und Abtauzyklen die Lebensdauer der Anlagen verkürzen und Brandgefahr erzeugen können.	100 %	100 %	bestätigt
In Frankreich gab es laut Bericht rund 20 Brände.	100 %	85 %	präzisiert
Danfoss erklärte, die meisten betroffenen Geräte seien Altmodelle (AK-SM 800, AK-SC 355) ohne Sicherheitsupdates.	100 %	100 %	bestätigt
In Bocholt ist kein länger dauernder Hardwareschaden entstanden.	55 %	55 %	offen
Falls ein nicht mehr unterstützter Controller im Einsatz ist, muss er ersetzt werden, was je nach Lieferzeit Wochen dauern kann.	40 %	40 %	offen
Censys zählte am 11.10.2026 weltweit 2.991 aus dem Internet erreichbare Danfoss-StoreView-Steuerungen, davon 1.825 in Frankreich. Drei Tage später waren es 71 Prozent weniger.	100 %	95 %	präzisiert
Ein Forscher zählte 10.354 öffentlich erreichbare Kühlsteuerungen in Europa und 2.843 in den USA.	100 %	95 %	bestätigt
CERT-FR nennt neben Danfoss AK-SC/AK-SM auch Copeland XWEB und Dixell XWEB als betroffene Produktfamilien.	100 %	100 %	bestätigt
In Deutschland sind weiterhin mehrere Hundert Kühlsteuerungen direkt aus dem Internet erreichbar.	60 %	50 %	offen
CERT-FR warnt, die Angriffe laufen wahrscheinlich weiter.	100 %	100 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
BSI-Empfehlung 154 „Gefährdung durch internet-verbundene OT-Systeme“: kein direkter Internetzugriff auf Steuerungen, Fernzugriff nur per VPN mit Mehr-Faktor-Authentisierung, Updates, Erreichbarkeit r…	100 %	95 %	bestätigt

Neu seit dem letzten Stand

• 13.11.2026: BSI-Warnung Stufe Orange zu neuen Schwachstellen in Danfoss AK-SM 800A (bis 5.3.2, auch 5.4.0 nicht ausgeschlossen); im schlimmsten Fall Austausch der Geräte nötig

• Raesfeld (Rewe, 02.11.) liegt wie Bocholt im Kreis Borken

• BMI: keine Erkenntnisse für eine Zuordnung in Deutschland; BfV und GAZ Hybrid befassen sich mit den Fällen

• UniBw CODE: Angreifer schalteten in Fällen auch Alarme ab; Angriff offenbar über Fernwartungszugang eines Dienstleisters

• ABH-Adresse Heinrich-Hertz-Str. 24, 46399 Bocholt, gegründet 2001, beliefert laut Webseite auch Kantinen, Schulen und Kitas

Wissensstand



■ Wissen 47 % ■ Wahrscheinlich 21 % ■ Nicht bekannt 32 %

Zum Bocholter Fall selbst gibt es nur Überschrift, Vorspann und zwei Zwischenüberschriften (der Artikeltext ist hinter der Paywall). Zur europäischen Welle ist die Lage dagegen gut belegt: Behörden in Frankreich, Deutschland und den USA haben sich geäußert.

1. Was ist passiert, und warum?

WISSEN

• Laut BBV vom 12.11.2026, 05:00 Uhr (Autor Fabian Wilmers) war das Bocholter Cateringunternehmen ABH von einem Cyberangriff auf seine Kühlanlagen betroffen. Die Zwischenüberschriften lauten „Fernzugriff als Einfallstor“ und „Überwachung verhindert Schaden“. (100 %) [https://www.bbv-net.de/bocholt/hackerangriff-bocholt-abh-cateringunternehmen-kuehlanlagen-ueberwachung-verhindert-schaden-w1273057-6000661438]

• Holtwick ist ein Ortsteil von Bocholt (PLZ 46399, Kreis Borken) mit Gewerbegebiet. Nicht zu verwechseln mit Holtwick in Rosendahl. (100 %) [https://bocholt.de/en/holtwick]

• Außenminister Jean-Noël Barrot schrieb den Angriff den iranischen Revolutionsgarden zu. (100 %) [https://www.t-online.de/nachrichten/ausland/id_101520546/frankreich-sieht-iran-hinter-angriff-auf-kuehlanlagen.html]

• Die Pariser Staatsanwaltschaft hat eine gerichtliche Untersuchung gegen den Chef der IRGC-Einheit Shahid Kaveh und zwei Stellvertreter eingeleitet und internationale Haftbefehle beantragt. Für die Angriffe in anderen europäischen Ländern ist die Gruppe nicht offiziell beschuldigt. Iran weist die Vorwürfe zurück. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/qu-est-ce-que-shahid-kaveh-le-groupe-cyber-iranien-accuse-d-avoir-attaque-les-frigos-de-supermarches-en-france_8276177.html]

• In Deutschland waren Märkte in Reisbach, Wetter-Volmarstein, im münsterländischen Raesfeld, in Wuppertal und in Lilienthal betroffen. In Wetter richtete sich der Angriff laut AWO gegen die Firma, die die Kühlanlagen aus der Ferne wartet. (100 %) [https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

• Laut heise fanden die Täter offene Systeme mit automatisierten Suchprogrammen. Sie kamen über bekannte Schwachstellen oder unveränderte Standardpasswörter hinein, in mindestens einem Fall über einen externen Wartungsdienstleister. Das BMI hat keine Erkenntnisse, die eine klare Zuordnung zu einem Akteur erlauben. (100 %) [https://www.heise.de/news/Supermarkt-Kuehlsysteme-Deutsche-Geheimdienste-ermitteln-nach-Sabotageakten-11516390.html]

NICHT BEKANNT

• Wann genau der Angriff auf ABH stattfand

• Welcher Hersteller und welches Steuerungsmodell bei ABH im Einsatz sind

• Ob der Fernzugriff ein direkt erreichbares Web-Interface war oder der Zugang eines Dienstleisters

• Ob ABH Anzeige erstattet hat und ob die Polizei ermittelt

• Wer dahintersteckt

WAHRSCHEINLICH (Einschätzung)

• Der Bocholter Fall gehört zum Muster der europäischen Welle (Manipulation von Kühlsteuerungen über Fernzugriff). (65 %) – Er passt im Zeitraum, im Anlagentyp und im Vektor „Fernzugriff“, und Raesfeld liegt im selben Kreis. Technische Belege für Bocholt fehlen aber.

• Derselbe Täter wie in Frankreich steckt dahinter. (30 %) – Frankreich hat nur die eigenen Fälle zugeordnet, das BMI hat keine Zuordnung. Das BSI warnt ausdrücklich vor Nachahmern.

2. Was ist die Auswirkung?

WISSEN

• Laut BBV-Überschrift hat ein Überwachungssystem einen „riesigen Schaden“ verhindert. (100 %) [https://www.bbv-net.de/bocholt/hackerangriff-bocholt-abh-cateringunternehmen-kuehlanlagen-ueberwachung-verhindert-schaden-w1273057-6000661438]

• Zum Vergleich: In Lilienthal musste der Inhaber nach eigener Aussage Ware für über 360.000 Euro wegwerfen. In Reisbach wurden Kühlanlagen laut Markt auf bis zu 50 Grad hochgeheizt. (100 %) [https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

• Die Bundesregierung sieht keine unmittelbare Gefahr für die Lebensmittelversorgung, weil die betroffenen Betriebe unter den KRITIS-Schwellen liegen. (100 %) [https://www.heise.de/news/Supermarkt-Kuehlsysteme-Deutsche-Geheimdienste-ermitteln-nach-Sabotageakten-11516390.html]

NICHT BEKANNT

• Ob bei ABH Ware entsorgt werden musste und wie viel

• Ob Kunden oder Veranstaltungen betroffen waren

• Was genau das Überwachungssystem gemeldet hat

WAHRSCHEINLICH (Einschätzung)

• Der Schaden in Bocholt ist deutlich kleiner als bei den Supermärkten mit Totalverlust der Kühlware. (70 %) – Die Überschrift betont, dass größerer Schaden verhindert wurde. Zahlen fehlen.

• Eine unabhängige Temperaturüberwachung mit Alarm hat die Abweichung früh gemeldet. (60 %) – UniBw CODE berichtet, dass Angreifer in anderen Fällen auch die Alarme der Steuerung abschalteten. Eine getrennte Überwachung wäre die naheliegende Erklärung, ist für Bocholt aber nicht belegt.

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

WISSEN

• CERT-FR empfiehlt für kompromittierte Geräte: Internet-Erreichbarkeit entfernen, auf Werkseinstellungen zurücksetzen, neu konfigurieren und den Zugang nur über eine gesicherte Verbindung wiederherstellen. (100 %)
[https://refindustry.com/news/french-cybersecurity-agency-warns-of-attacks-on-refrigeration-controllers/]

• Am 13.11.2026 warnte das BSI (Stufe Orange) vor neuen Schwachstellen in Danfoss AK-SM 800A bis Version 5.3.2. Im schlimmsten Fall wird die Betriebssoftware ersetzt, und die Geräte müssen manuell wiederhergestellt oder ausgetauscht werden. (100 %) [https://handelsblatt.com/politik/deutschland/hackerangriffe-cyberbehoerde-warnt-vor-neuen-sicherheitsluecken-in-kuehlanlagen/100269729.html]

NICHT BEKANNT

• Ob die Steuerung bei ABH schon wieder normal läuft

• Ob ein Dienstleister die Wiederherstellung übernimmt

WAHRSCHEINLICH (Einschätzung)

• Wenn nur Sollwerte verstellt wurden, ist die Kühlsteuerung in Stunden bis wenigen Tagen wieder sicher in Betrieb. (55 %) – Zurücksetzen und neu konfigurieren geht schnell. Die neue BSI-Warnung zeigt aber, dass auch ein Firmware-Tausch möglich ist, und dann dauert es länger.

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

WISSEN

• CISA, FBI und weitere US-Behörden warnen am 05.11.2026, dass erzwungene Dauer-Heiz- und Abtauzyklen eine Brandgefahr schaffen und die Lebensdauer der Anlage beeinträchtigen können. (100 %) [https://www.cisa.gov/resources-tools/resources/us-government-partners-urge-hardening-industrial-refrigeration-and-cold-chain-monitoring-systems]

• Danfoss erklärte, die meisten betroffenen Geräte seien Altmodelle (AK-SM 800, AK-SC 355) ohne Sicherheitsupdates. (100 %) [https://thehackernews.com/2026/10/attackers-heat-french-supermarket.html]

• In Frankreich nennt die Staatsanwaltschaft laut Bericht rund 20 Brandausbrüche. (100 %) [https://actu17.fr/international/frigos-a-50-degres-dans-700-supermarches-la-justice-francaise-remonte-jusqu-aux-gardiens-de-la-revolution-iraniens.html]

NICHT BEKANNT

• Ob bei ABH Hardware beschädigt wurde

• Ob dort ein nicht mehr unterstütztes Steuerungsmodell im Einsatz ist

WAHRSCHEINLICH (Einschätzung)

• In Bocholt ist kein länger dauernder Hardwareschaden entstanden. (55 %) – Eine frühe Erkennung spricht dagegen, dass die Anlage lange im Heiz- oder Abtaumodus lief. Belegt ist das nicht.

• Falls ein nicht mehr unterstützter Controller im Einsatz ist, muss er ersetzt werden, was je nach Lieferzeit Wochen dauern kann. (40 %) – Für Altgeräte gibt es keine Patches. Ob bei ABH so eines steht, ist unbekannt.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Censys zählte am 11.10.2026 weltweit 2.991 aus dem Internet erreichbare Danfoss-StoreView-Oberflächen, davon 1.825 in Frankreich. Am 14.10. waren es in Frankreich 537 (minus 71 Prozent). (100 %) [https://www.infosecurity-magazine.com/news/france-expose-danfoss-controllers/]

• Der Forscher Anurag Sen zählte 10.354 öffentlich erreichbare Kühlsteuerungen in Europa und 2.843 in den USA. Deutschland liegt bei ihm unter den fünf Ländern mit den meisten. (100 %) [https://san.com/cc/us-supermarket-refrigerators-among-thousands-vulnerable-to-cyberattacks/]

• Forescout fand am 22.10.2026 weltweit 6.017 IP-Adressen mit Kühlsystem-Oberflächen in 99 Ländern, die meisten davon Copeland/Dixell XWEB (7.075 Dienst-Beobachtungen) und Danfoss StoreView (4.697). (100 %) [https://www.forescout.com/blog/cold-chain-open-control-exposed-refrigeration-systems-reveal-global-risk/]

• CERT-FR nennt neben Danfoss AK-SC/AK-SM auch Copeland XWEB und Dixell XWEB. (100 %) [https://www.securityweek.com/supermarket-refrigeration-attack-widens-to-copeland-dixell-controllers/]

NICHT BEKANNT

• Eine belastbare aktuelle Zahl für Deutschland

• Wie viele Caterer, Kantinen und Kühlhäuser (also keine Supermärkte) betroffen sind

WAHRSCHEINLICH (Einschätzung)

• In Deutschland sind weiterhin mehrere Hundert Kühlsteuerungen direkt aus dem Internet erreichbar. (50 %) – Deutschland liegt in der Zählung von Sen weit vorne, eine konkrete Zahl wird aber nicht veröffentlicht. Zählweisen und Honeypots verzerren das Bild (Bitsight).

6. Kann das wieder passieren?

WISSEN

• CERT-FR hält es für wahrscheinlich, dass die Angriffskampagnen weiterlaufen. (100 %) [https://refindustry.com/news/french-cybersecurity-agency-warns-of-attacks-on-refrigeration-controllers/]

• BSI-Präsidentin Plattner: Der Angriff hätte jedes Land treffen können und kann jederzeit Nachahmer finden. Das BSI veröffentlichte die Empfehlung BSI-CS 154 „Gefährdung durch internet-verbundene OT-Systeme“. (100 %) [https://www.it-daily.net/?p=190696]

• Am 13.11.2026 hat das BSI vor neuen Schwachstellen in Danfoss AK-SM 800A gewarnt und Betreiber aufgefordert, „unverzüglich“ zu handeln. (100 %) [https://handelsblatt.com/politik/deutschland/hackerangriffe-cyberbehoerde-warnt-vor-neuen-sicherheitsluecken-in-kuehlanlagen/100269729.html]

NICHT BEKANNT

• Ob ABH den Fernzugang inzwischen geändert hat

WAHRSCHEINLICH (Einschätzung)

• In den nächsten Wochen werden weitere Betriebe in Deutschland getroffen. (75 %) – Es gab schon zwei Wellen in einem Monat, die Kampagne läuft laut CERT-FR weiter, und für das neueste Danfoss-Modell gibt es neue Schwachstellen.

Lage

Das Bocholter Volksblatt (BBV) berichtet am 12.11.2026, dass Unbekannte die Kühlanlagen des Caterers ABH in Bocholt-Holtwick angegriffen haben. Laut Zwischenüberschrift kamen sie über einen Fernzugriff herein, und ein Überwachungssystem soll einen „riesigen Schaden“ verhindert haben. Der Fall fällt in die europaweite Angriffswelle auf Kühlsteuerungen seit dem 11./12.10.2026. Ob er technisch und täterseitig dazugehört, ist öffentlich nicht belegt.

Angriff	Manipulation der Kühlanlagen über einen Fernzugriff (laut BBV-Zwischenüberschrift). Die Details stehen hinter der Paywall.
Wann / Status	Gemeldet am 12.11.2026, Angriffszeitpunkt nicht öffentlich · unklar
Täter	unbekannt; für die französischen Fälle hat Frankreich die IRGC-Einheit Shahid Kaveh beschuldigt, für Deutschland gibt es keine Zuordnung – unbekannt
Betreiber / Branche	ABH OHG, Event- & Gastroservice (Bocholt) · Catering / Gemeinschaftsverpflegung (Lebensmittel)
Anlage / Alter	Kühlanlagen mit fernzugänglicher Steuerung; Hersteller nicht öffentlich · nicht bekannt
Region	Bocholt-Holtwick, Kreis Borken, NRW
Auswirkungen	Keine Auswirkung auf die Versorgung der Bevölkerung bekannt. Die Bundesregierung sieht keine unmittelbare Gefahr, weil die Betriebe unter den KRITIS-Schwellen liegen (heise). ABH beliefert laut eigener Webseite auch Kantinen, Schulen und Kindergärten. Ob diese betroffen waren, ist nicht bekannt (nicht geprüft).
Behörden	Für Bocholt nicht öffentlich. Bundesweit: BSI (Warnungen, BSI-CS 154), BfV und GAZ Hybrid (BND, MAD, Polizei) laut heise/Handelsblatt; in einzelnen deutschen Fällen ermittelt laut ZDF die Staatsanwaltschaft.
Regulatorik	Die betroffenen Betriebe liegen laut Bundesregierung unter den KRITIS-Schwellen (rund 500.000 versorgte Personen). Ob ein Caterer dieser Größe unter NIS2 fällt (Sektor Lebensmittel: Produktion, Verarbeitung, Vertrieb, ab mittlerer Unternehmensgröße), ist nicht geprüft und wahrscheinlich nicht der Fall. Der CRA nimmt künftig die Hersteller in die Pflicht (Updates, Schwachstellenmeldungen), hilft aber nicht bei Altgeräten im Feld.

Angriffsvektor

Bekannt: Laut BBV-Zwischenüberschrift ein Fernzugriff („Fernzugriff als Einfallstor“); die genaue Art ist nicht öffentlich.

• Direkt aus dem Internet erreichbares Web-Interface der Kühlsteuerung mit Standard- oder schwachem Passwort (hoch): So sind die meisten Fälle der Welle abgelaufen (heise, BSI, CERT-FR). Gefunden werden die Systeme per automatisierter Suche.

• Fernwartungszugang eines Kälte-Dienstleisters (gemeinsame Zugangsdaten oder kompromittiertes Dienstleisterkonto) (mittel): In Wetter-Volmarstein und laut UniBw CODE lief der Angriff über den Dienstleister. Ein Dienstleister betreut oft viele Kunden in einer Region.

• Ausnutzung bekannter Schwachstellen in alter Firmware (Altgeräte ohne Patches) (mittel): Danfoss nennt Altmodelle ohne Updates, und das BSI warnt seit 13.11. vor neuen Schwachstellen auch im aktuellen Modell. Für Bocholt ist kein Gerät bekannt.

• Fernwartungssoftware auf einem Büro-PC (z. B. Remote-Desktop-Tool) mit anschließendem Zugriff auf die Kühlsteuerung (gering): In kleinen Betrieben verbreitet, aber in dieser Welle nicht als Muster berichtet.

Zeitleiste

11./12.10.2026 (Nacht) Angriff auf Kühlsteuerungen in rund 700 französischen Supermärkten – bestätigt
[https://www.t-online.de/nachrichten/ausland/id_101520546/frankreich-sieht-iran-hinter-angriff-auf-kuehlanlagen.html]

12.10.2026, aktualisiert 13.10. CERT-FR-Warnung: Danfoss AK-SM/AK-SC, später auch Copeland/Dixell XWEB – bestätigt
[https://www.securityweek.com/supermarket-refrigeration-attack-widens-to-copeland-dixell-controllers/]

Oktober 2026 (nach 12.10.) BSI ruft Betreiber kleiner Anlagen zur Absicherung auf, Empfehlung BSI-CS 154 – berichtet [https://www.it-daily.net/?p=190696]

14.10.2026 Censys: erreichbare Danfoss-Oberflächen in Frankreich minus 71 Prozent – berichtet
[https://www.infosecurity-magazine.com/news/france-expose-danfoss-controllers/]

Nacht auf 02.11.2026 Zweite Welle in mehreren EU-Ländern, auch in Deutschland (Reisbach, Wetter, Raesfeld, Wuppertal, Lilienthal) – berichtet
[https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

05.11.2026 CISA, FBI, HHS, USDA und DoT veröffentlichen Härtungsempfehlungen für Kühl- und Kühlkettensysteme – bestätigt [https://www.cisa.gov/resources-tools/resources/us-government-partners-urge-hardening-industrial-refrigeration-and-cold-chain-monitoring-systems]

09.11.2026 Frankreich beschuldigt die Revolutionsgarden, die Pariser Staatsanwaltschaft ermittelt gegen die Spitze von Shahid Kaveh – bestätigt [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/qu-est-ce-que-shahid-kaveh-le-groupe-cyber-iranien-accuse-d-avoir-attaque-les-frigos-de-supermarches-en-france_8276177.html]

10.11.2026 Deutsche Nachrichtendienste (BfV, GAZ Hybrid mit BND und MAD) befassen sich mit den Angriffen – berichtet [https://www.heise.de/news/Supermarkt-Kuehlsysteme-Deutsche-Geheimdienste-ermitteln-nach-Sabotageakten-11516390.html]

12.11.2026, 05:00 Uhr BBV berichtet über den Angriff auf ABH in Bocholt-Holtwick – berichtet [https://www.bbv-net.de/bocholt/hackerangriff-bocholt-abh-cateringunternehmen-kuehlanlagen-ueberwachung-verhindert-schaden-w1273057-6000661438]

13.11.2026 BSI warnt (Stufe Orange) vor neuen Schwachstellen in Danfoss AK-SM 800A – berichtet [https://handelsblatt.com/politik/deutschland/hackerangriffe-cyberbehoerde-warnt-vor-neuen-sicherheitsluecken-in-kuehlanlagen/100269729.html]

Vergleichsfälle

• Supermarkt-Welle Frankreich (rund 700 Märkte) (2026): Offen erreichbare Kühlsteuerungen lassen sich massenhaft in einer Nacht manipulieren.
[https://www.t-online.de/nachrichten/ausland/id_101520546/frankreich-sieht-iran-hinter-angriff-auf-kuehlanlagen.html]

• Lilienthal bei Bremen, über 360.000 Euro Warenverlust (2026): Ohne frühen Alarm wird ein kleiner Markt zum Totalschaden.
[https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

• AWO-Markt Wetter-Volmarstein, Angriff über Fernwartungsdienstleister (2026): Der Fernzugang des Dienstleisters gehört in die eigene Sicherheitsplanung.
[https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

• Claroty Team82: Schwachstellen in Danfoss AK-SM 800A (2025): Die Schwachstellen waren lange vor der Welle öffentlich bekannt. [https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers]

Begriffe einfach erklärt

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

Fernwartung / Remote Access: Der Techniker schaltet sich übers Internet auf die Anlage auf, statt vorbeizukommen.

Kühlsteuerung: Ein kleiner Computer, der Temperaturen, Abtauzeiten und Alarme der Kühlmöbel regelt.

Abtauzyklus: Das Kühlgerät heizt kurz, um Eis zu entfernen; dauerhaft ausgelöst wird es warm im Kühlregal.

VPN: Ein verschlüsselter, abgesicherter Tunnel ins Firmennetz, statt die Anlage offen ins Internet zu stellen.

Früherer Stand: Erstmeldung (12.11.2026 09:06)

Wissen 43 % · wahrscheinlich 20 % · nicht bekannt 37 %

Laut Bocholter Borkener Volksblatt (BBV) vom 12.11.2026 wurden die Kühlanlagen des Cateringbetriebs ABH Event- und Gastroservice in Bocholt-Holtwick angegriffen. Eine Zwischenüberschrift nennt einen Fernzugriff als Einfallstor, ein Überwachungssystem soll größeren Schaden verhindert haben. Zeitpunkt, Schaden, Hersteller und Ermittlungen stehen hinter der Bezahlschranke und sind nicht geprüft. Ob der Fall zur europaweiten Welle gehört, die Frankreich den iranischen Revolutionsgarden zuschreibt, ist nicht belegt.

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