

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 13.10.2026, 07:27 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	13.10.2026
Herausgeber	Maximilian Gilg, OT-Cyber.de, Rosenheim
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen
Online	https://ot-cyber.de/ot-lage/

Dieses Lagebild fasst öffentlich zugängliche Meldungen zusammen – automatisch zusammengestellt, ohne Gewähr. Die Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen in Deutschland, Österreich und der Schweiz.

Management Summary

Diese Ausgabe enthält 3 Meldungen, davon 2 mit hoher Relevanz für Betreiber in DACH.

- ****Update Danfoss: Sekoia nennt weitere betroffene Länder, auch Deutschland (13.10.)****
- ****Update Danfoss: neue Zahlen, die sich teils widersprechen**

GESAMTBEWERTUNG

Hoch – vorrangig die Meldungen mit hoher Relevanz prüfen und umsetzen.

Lageübersicht

ID	Meldung	Relevanz
L-01	**Update Danfoss: Sekoia nennt weitere betroffene Länder, auch Deutschland (13.10.)**	HOCH
L-02	**Update Danfoss: neue Zahlen, die sich teils widersprechen	HOCH
L-03	**Ahold Delhaize: Cybervorfall, Systeme vom Netz genommen (12.10.)**	MITTEL

Meldungen im Detail

L-01 ****Update Danfoss: Sekoia nennt weitere betroffene Länder, auch Deutschland (13.10.)****

Relevanz: HOCH

Laut Félix Aimé, Senior Threat-Intelligence-Analyst bei Sekoia, waren neben Frankreich auch Deutschland, Spanien, Portugal, Polen und Belgien betroffen (zitiert von ABC/Reuters und Al Jazeera). Das ist bisher eine einzelne Quelle; Details zu den einzelnen Ländern nennt sie nicht. Laut einer Person aus dem Umfeld von Premierminister Lecornu hat die ANSSI eine Schwachstelle in Danfoss-Software identifiziert; Lecornu hat die ANSSI mit der Untersuchung beauftragt. Täter und Angriffsweg sind weiter offen. Danfoss spricht von einer „begrenzten Zahl“ betroffener Kälte-Managementsysteme mit veralteter Firmware. Gegenüber Cooling Post nennt Danfoss die AK-SM800 (End-of-Life 2021) und AK-SC355 (abgekündigt 2016); betroffene AK-SM800A liefen laut Cooling Post mit veralteter Firmware. Zum AK-SM 800A hatte Claroty Team82 am 9. August Schwachstellen veröffentlicht (laut ABC/Reuters). Die Pariser Staatsanwaltschaft meldet neben Warenverlusten auch Entstehungsbrände; Ort und Ausmaß nennt sie nicht. Unsere Einschätzung: Betreiber von Gebäudeautomation und Kältetechnik in DACH sollten jetzt prüfen, ob Danfoss AK-SM800, AK-SC355 oder AK-SM800A mit alter Firmware aus dem Internet erreichbar sind. Fernwartung über Hersteller-Steuerungen gehört ins Asset-Inventar und nie direkt ins Internet (SANS Critical Control 4, Secure Remote Access). Laufender Stand im Vorfall-Lagebild: <https://ot-cyber.de/bl og/vorfall-lagebild-hacker-stellen-danfoss-supermarktkuehlung-auf-50-c.html> –

Quelle: <https://www.abc.net.au/news/2026-10-13/french-supermarkets-hacked-causing-fires-and-food-loss/107258724>

Quelle: <https://www.aljazeera.com/news/2026/10/13/unprecedented-cyberattack-hits-french-supermarkets-causing-food-losses>

Quelle: <https://www.coolingpost.com/world-news/danfoss-moves-to-mitigate-cyberattack/>

L-02 ****Update Danfoss: neue Zahlen, die sich teils widersprechen**

Relevanz: **HOCH**

und Reaktionen aus Handel und EU** – Les Mousquetaires (Intermarché) spricht laut ABC/Reuters jetzt von rund 150 Märkten, deren Kühlschränke über Nacht sechs Stunden lang auf 50 °C gestellt waren; 50 °C war der Sollwert, nicht die gemessene Temperatur. Zuvor war von etwa 300 Intermarché- und Netto-Märkten die Rede (BFMTV, zitiert von The Record) – widersprüchlich. Laut Al Jazeera nennt Monoprix rund 5 % seiner etwa 490 Märkte; der Handelsverband FCD verlangt von Danfoss „volle Transparenz“, einige betroffene Märkte laufen wieder. Frankreich stimmt sich laut Lecornus Büro mit europäischen Partnern ab, weil weitere Länder betroffen sein könnten. EU-Agrarkommissar Christophe Hansen: „the weaponisation of food has become a reality“ (Cooling Post). Unsere Einschätzung: Die OT der Lebensmittel- und Kühlkette rückt damit in die Debatte um KRITIS und NIS2.

Quelle: <https://www.abc.net.au/news/2026-10-13/french-supermarkets-hacked-causing-fires-and-food-loss/107258724>

Quelle: <https://therecord.media/cyberattack-disrupts-refridgeration-in-france>

Quelle: <https://www.aljazeera.com/news/2026/10/13/unprecedented-cyberattack-hits-french-supermarkets-causing-food-losses>

Quelle: <https://www.coolingpost.com/world-news/danfoss-moves-to-mitigate-cyberattack/>

L-03 ****Ahold Delhaize: Cybervorfall, Systeme vom Netz genommen (12.10.)****

Relevanz: **MITTEL**

Der Konzern meldet: „Ahold Delhaize is experiencing a security issue within its network“ und hat einige Systeme vorsorglich vom Netz genommen. Laut BleepingComputer konnten Kunden von Albert Heijn, Etos, Gall & Gall (Niederlande) und Delhaize (Belgien) Webseiten, Apps und Kundenservice nicht nutzen; in den USA kamen Mitarbeiter von Stop & Shop nicht an Dienstpläne, Food Lion meldete Probleme bei Online-Bestellungen. Die Märkte sind geöffnet. Ob Ransomware dahintersteckt, ist nicht bestätigt; Hinweise auf OT oder einen Zusammenhang mit dem Danfoss-Angriff gibt es bisher nicht. Unsere Einschätzung: Fällt die Geschäfts-IT aus, muss die Anlage trotzdem weiterlaufen – das gehört in den Incident-Response-Plan (SANS Critical Control 1, ICS Incident Response).

Quelle: <https://www.bleepingcomputer.com/news/security/retail-giant-ahold-delhaize-takes-systems-offline-after-cyberattack/>

Einordnung und Unterstützung: OT-Cyber.de · Am Esbaum 12, 83022 Rosenheim · +49 8031 8603164 · akademie@ot-cyber.de · <https://ot-cyber.de/>