

ALERTĂ DNSC | 14 OCTOMBRIE 2026

Atac cibernetic asupra instalațiilor frigorifice din Franța

Pe 14 octombrie, DNSC a preluat o alertă a CERT-FR (ANSSI, Franța) despre compromiterea unui număr mare de controlere prin care instalațiile frigorifice sunt administrate și monitorizate de la distanță. V-o semnalăm pentru că problema nu ține nici de Franța, nici doar de supermarketuri.

350+

supermarketuri afectate în Franța

+50°C

temperatura atinsă în unele frigidere

4

familii de echipamente vizate

Ce s-a întâmplat

Interfețele de administrare ale acestor echipamente erau accesibile direct din Internet. Atacatorii au intrat în ele și au modificat de la distanță temperaturile și programele de dezghețare. Sunt afectate magazine din rețelele Carrefour, Monoprix, Intermarché și Coopérative U. În unele frigidere temperatura a urcat până la +50°C, marfa s-a deteriorat, iar în câteva cazuri s-au produs incendii.

Echipamente vizate	Copeland xweb, Danfoss seria AK-SC, Danfoss seria AK-SM, Dixell xweb
Ce nu se știe încă	CERT-FR nu a publicat versiunile afectate, coduri CVE sau indicatori de compromitere. Semnele rămân cele din funcționarea echipamentului: setări schimbate fără ca cineva din echipă să le fi modificat, conectări administrative neobișnuite, temperaturi care nu au o explicație.

Cine ar trebui să verifice

Oricine folosește echipamente care pot fi administrate de la distanță printr-o interfață web. Ne gândim în primul rând la:

- frigiderele pentru medicamente, vaccinuri sau probe din clinici, cabinete, farmacii și laboratoare;
- camerele frigorifice și depozitele din producție, logistică, HoReCa și retail;
- sistemele HVAC și de management al clădirii, UPS-urile, camerele video și controlul accesului.

Legea nr. 58/2023 (art. 5 lit. a) pune securitatea cibernetică a unui sistem în sarcina celui care îl deține, îl organizează, îl administrează sau îl utilizează. Faptul că echipamentul a fost instalat și este întreținut de un furnizor nu mută această responsabilitate.

Dacă observați ceva suspect

Deconectați echipamentul de la Internet, resetați-l la setările din fabrică și reconfigurați-l, cu firmware actualizat și acces doar prin VPN. Resetarea singură nu rezolvă problema, pentru că un echipament care rămâne expus poate fi atacat din nou. Anunțați-ne cât mai repede, ca să stabilim împreună dacă situația trebuie notificată.

Ce vă recomandăm

1 Inventarul echipamentelor conectate

Faceți o listă cu tot ce este conectat la rețea (frigorifice, HVAC, camere, control acces) și aflați ce anume se vede din Internet. Cereți furnizorului de IT să vă confirme în scris.

2 Fără acces direct din Internet

Interfețele de administrare se închid către exterior. Accesul de la distanță, acolo unde este nevoie de el, se face prin VPN.

3 Parolele implicite

Se schimbă pe fiecare echipament. Conturile comune sau pe care nu le mai folosește nimeni se șterg.

4 Firmware și setări de securitate

Actualizați la ultima versiune și urmați recomandările producătorului (la Danfoss, nivelul de securitate „Strict”). Echipamentele care nu mai primesc actualizări trebuie planificate pentru înlocuire.

5 Configurația actuală

Verificați temperaturile setate, programele de dezghețare și pragurile de alarmă și păstrați o copie a configurației corecte.

6 Furnizorul de mentenanță

Clarificați cine are acces, de unde și prin ce canal. Filtrarea IP-urilor lui pe firewall ajută pe moment, dar nu este o soluție definitivă. Înainte să opriți transmiterea datelor către furnizor, verificați polița de asigurare.

7 O alarmă separată

Un senzor de temperatură independent, cu alertă prin SMS sau e-mail, vă anunță chiar dacă sistemul principal a fost manipulat.

8 Planul de răspuns la incidente

Includeți și aceste echipamente în plan: cine observă problema, pe cine anunță și în cât timp.

TOTODATĂ

Prima amendă DNSC pentru nenotificare

Pe 29 septembrie 2026, DNSC a amendat cu 50.000 lei o instituție a administrației publice centrale, din sectorul „Administrație publică” (Anexa nr. 1 la OUG nr. 155/2024). Motivul: nu și-a respectat obligația de notificare în termenul prevăzut de art. 18 alin. (2), faptă sancționată de art. 60 alin. (1) lit. o) din același act.

Este primul caz de acest fel și arată că DNSC aplică efectiv sancțiunile prevăzute de lege. Dacă organizația dumneavoastră intră sub incidența OUG nr. 155/2024, merită verificat acum dacă notificările către DNSC au fost făcute la timp.

50.000

lei

amenda aplicată

Dacă aveți astfel de echipamente sau nu știți sigur dacă vă încadrați în OUG nr. 155/2024, scrieți-ne la dpo@gdprcomplet.ro și ne uităm împreună.

Echipa GDPR Complet

Surse: DNSC, alertă privind vulnerabilități ale unor instalații frigorifice (14.10.2026); CERT-FR, alerta CERTFR-2026-ALE-012; DNSC, comunicat de presă din 30.09.2026. Materialul are caracter informativ și nu înlocuiește o analiză adaptată organizației dumneavoastră.