CYBERCRIMEINFO
onafhankelijk kennisplatform over cybercriminaliteit



ONAFHANKELIJKE DREIGINGSANALYSE

Van scherm naar schap

Wanneer een digitale aanval fysiek wordt

Een dreigingsanalyse voor Nederland en België, **november 2026**

Auteur: **Peter Lahousse**, oprichter van Cybercrimeinfo

Gebaseerd op openbare waarschuwingen van NCSC, CCB, CERT-FR, ENISA, CISA en FBI en op het Cybersecuritybeeld Nederland 2026

Dit rapport mag vrij worden gedeeld en geciteerd met bronvermelding Cybercrimeinfo · www.ccinfo.nl

Managementsamenvatting

Jarenlang ging het bij een cyberaanval vooral over gegevens. Wat is er gestolen, wie moet worden ingelicht, hoe hoog is de schade aan de reputatie. Dit najaar zagen we in Nederland en België een ander soort schade. Bij supermarkten en koelhuizen werden koelregelaars op afstand overgenomen. Vriezers gingen 's nachts in een ontdooicyclus tot 50 graden, met vernietigde voorraad en lege schappen tot gevolg.

Het Centrum voor Cybersecurity België meldde meerdere incidenten in België en noemde Nederland, Luxemburg, Zweden, Ierland en Estland bij de landen waar de tweede golf toesloeg. ENISA, de Europese Commissie, Europol en de Europese netwerken van cyberteams riepen op 4 november gezamenlijk op tot onmiddellijke actie. Een dag later volgden de Amerikaanse diensten CISA en FBI met een eigen waarschuwing.

De les van dit kwartaal is niet dat koelkasten gevaarlijk zijn. De les is dat het zwakke punt verschuift naar apparaten die we zelden als computer herkennen. Een koelregelaar, een klimaatsysteem, een camera, een omvormer. Ze hangen aan internet omdat dat handig is voor onderhoud, ze worden vaak beheerd door een installateur of leverancier, en in de organisatie voelt zelden iemand zich eigenaar van de beveiliging ervan.

Drie feiten bepalen dit kwartaal.

- **Enkele uren.** Zo kort was in 2026 volgens het Cybersecuritybeeld Nederland van de NCTV de tijd tussen de ontdekking van een kwetsbaarheid en het misbruik ervan. In 2024 waren dat nog enkele maanden. Die reeks is een richting en geen precieze maat, zie hoofdstuk 6.
- **Zes.** Zoveel onbekende kwetsbaarheden vond het onderzoeksbureau Midnight Blue in de toen nieuwste software van een koelregelaar van Danfoss. Op het moment van publicatie was er geen update beschikbaar. Het CCB noemt het weghalen van de regelaar van het open internet daarom de enige echte oplossing.
- **2,5 miljoen.** Zoveel slimme apparaten staan er volgens hetzelfde Cybersecuritybeeld minimaal in Nederland die niet steeds de laatste updates hebben gehad. Er zijn geen aanwijzingen dat koelkasten thuis worden aangevallen, maar de vraag wie aan de knoppen kan draaien geldt ook daar.

De kern van dit rapport in één zin. Weet welke apparaten van u aan internet hangen, en wie erbij kan. Dat is geen dure maatregel en u kunt er morgen mee beginnen.

1. Wat er gebeurde, van Frankrijk naar heel Europa

Op 12 oktober 2026 publiceerde het Franse CERT-FR een waarschuwing. Het had kennis van talrijke compromitteringen van koelregelaars van Danfoss uit de reeksen AK-SM en AK-SC, en van Copeland xweb en Dixell xweb. Een dag later nam het Belgische CCB die waarschuwing over. In beide berichten staat dezelfde vaststelling. De beheerschermen van deze regelaars waren rechtstreeks via het internet bereikbaar, en dat is in strijd met goede beveiligingspraktijk.

Op 2 november volgde een tweede golf. Volgens het CCB troffen de aanvallen toen supermarkten en koelhuizen in heel Europa, met België, Luxemburg, Nederland, Zweden, Ierland en Estland bij naam genoemd. De aanvallers zetten de regelaars 's nachts in een ontdooicyclus tot 50 graden, met volledige vernietiging van de voorraad en verstoring van de bevoorrading bij meerdere Europese winkelketens tot gevolg. Het CCB meldde dat het op de hoogte was gebracht van meerdere incidenten met koelsystemen in België.

Het Nederlandse NCSC meldde op 2 november dat er in Europa en dus ook in Nederland meerdere aanvallen waren op koelinstallaties van diverse leveranciers. Het NCSC beschreef hoe aanvallers via zwakke of standaardwachtwoorden op afstand binnenkomen en daarna bijvoorbeeld de temperatuur of de ontdooicycli kunnen veranderen.

Op 4 november kwam een gezamenlijke verklaring van ENISA, de Europese Commissie, het Europese cybercrimecentrum van Europol en twee Europese netwerken van nationale cyberteams. Zij spraken van grootschalige incidenten met commerciële koelsystemen en vergelijkbare apparaten in meerdere lidstaten, en riepen organisaties op om direct maatregelen te nemen.

Op 5 november publiceerden CISA, de FBI en drie andere Amerikaanse overheidsdiensten een waarschuwing over kwaadwillende activiteit tegen industriële koelsystemen en systemen die de koude keten bewaken, wereldwijd. Zij wijzen erop dat deze systemen niet alleen in supermarkten staan, maar ook in de zorg, de chemie, de voedselketen en het gekoeld vervoer.

Op 12 november volgde het CCB met nieuw onderzoek van Midnight Blue. Dat vond zes kwetsbaarheden in de Danfoss AK-SM800A, tot en met firmwareversie 5.3.2, waarmee een aanvaller zonder in te loggen de volledige controle over het apparaat kan krijgen. Er was op dat moment nog geen update beschikbaar.

Dit rapport gaat bewust niet over de vraag wie hierachter zit. Daar lopen onderzoeken naar, en het is niet aan ons om daarop vooruit te lopen. Voor de les die dit kwartaal ons leert, maakt het ook niet uit. Het zwakke punt is hetzelfde, wie er ook misbruik van maakt.

2. Van gestolen gegevens naar fysieke schade

Wat deze golf anders maakt dan veel aanvallen van de afgelopen jaren, is het soort schade. Er is geen database gestolen en geen losgeld gevraagd voor versleutelde bestanden. De schade zat in het schap. Bederf, weggegooide voorraad, verstoorde bevoorrading.

De Amerikaanse diensten maken in hun waarschuwing duidelijk hoe breed die schade kan zijn. Een gewijzigde temperatuur kan de levensduur van een installatie verkorten, brandgevaar opleveren, voorraad laten verloren gaan en indirect consumenten schaden als producten na onveilige opslag toch worden gegeten. Ook kan een aanvaller het zicht op de werkelijke temperatuur wegnemen, zodat de eigenaar niet meer ziet wat er gebeurt.

Helemaal nieuw is het niet. Het Cybersecuritybeeld Nederland 2026 van de NCTV beschrijft dat een hacktivistische groep op 1 en 3 juni 2026 claimde bij twee Nederlandse organisaties in klimaatbeheersingssystemen te zijn binnengedrongen. Bij één organisatie zou de groep via een bedieningsscherm de temperatuur hebben kunnen aanpassen, bij de andere zou zij een warmtepomp op afstand hebben kunnen besturen. Het gaat om claims die de NCTV beschrijft, niet om vastgestelde schade. In hetzelfde rapport waarschuwt de NCTV voor de cyberfysieke dreiging bij thuisbatterijen en omvormers van zonnepanelen, waar misbruik kan leiden tot brand of instabiliteit van het stroomnet.

Onze analyse is dat wat in juni nog incidenten waren, in oktober en november op schaal gebeurde. Dat verband leggen wij zelf, het is geen uitspraak van de NCTV. En het is één golf, geen meerjarige meting. Maar de richting is duidelijk genoeg om er nu op te handelen. Een aanval op een apparaat dat iets in de fysieke wereld regelt, raakt niet alleen de administratie, maar de bedrijfsvoering zelf.

3. Het apparaat dat we niet als computer zien

Vraag een winkelier hoeveel computers er in de zaak staan, en u hoort de kassa, de laptop op kantoor en misschien een tablet. De koelregelaar in de technische ruimte wordt zelden meegeteld. Toch is het een computer, met een besturingssysteem, een webscherm, een wachtwoord en een verbinding met internet.

Uit de waarschuwingen van CERT-FR, het CCB, het NCSC en de Amerikaanse diensten komt steeds hetzelfde beeld naar voren. De aanvallers gebruikten drie zwakke punten.

- **Bereikbaar vanaf internet.** Het beheerscherm stond open, zodat het overal ter wereld te vinden en te proberen was.
- **Standaardwachtwoorden.** Wachtwoorden die de fabrikant meelevert en die niet zijn veranderd.
- **Verouderde software.** Firmware zonder de laatste updates, of apparaten die de fabrikant helemaal niet meer ondersteunt.

Geen van deze drie is geavanceerd. Het zijn dezelfde basisfouten die we al jaren zien bij routers, camera's en servers. Het verschil is dat ze hier zitten in apparaten die buiten het zicht van de IT vallen. Ze staan vaak niet in het overzicht van de systeembeheerder, ze krijgen niet vanzelf updates mee in de maandelijkse ronde, en er gaat geen alarm af als er 's nachts iemand inlogt.

Het CCB wijst nog op een detail dat veel ondernemers zal verrassen. Een 4G of 5G modem is op zichzelf geen beveiliging. Als het beheerscherm van de regelaar via die verbinding vanaf internet bereikbaar blijft, staat het gewoon open.

Het Cybersecuritybeeld laat zien dat het thuis niet anders is. Een derde van de Nederlanders installeert updates voor slimme apparaten niet of niet op tijd. Volgens de NCTV staan er daardoor in Nederland

minimaal 2,5 miljoen apparaten die niet steeds de laatste updates hebben gehad. Vaak worden ze geleverd met zwakke standaardwachtwoorden die daarna niet worden aangepast.

4. De installateur aan het stuur



Illustratief beeld, gemaakt voor dit rapport. Geen bestaande winkel of installatie.

Waarom hangt een koelregelaar eigenlijk aan internet? Meestal om een goede reden. De installateur of leverancier wil op afstand kunnen meekijken, storingen verhelpen en de temperatuur bewaken. Soms vraagt de verzekering dat de temperatuur continu wordt vastgelegd. Dat is handig en vaak noodzakelijk.

Juist daar ontstaat de blinde vlek. De winkelier denkt dat de installateur de beveiliging regelt. De installateur levert een werkende koeling en zet het beheerscherm soms open om erbij te kunnen. Vaak is niet afgesproken wie verantwoordelijk is voor het wachtwoord, de updates en de vraag of het scherm wel open moet staan.

De Franse en Belgische waarschuwingen houden daar uitdrukkelijk rekening mee. Zij adviseren om eerst de verzekeringsvoorwaarden en de afspraken met de koelleverancier na te kijken, voordat u de verbinding naar die leverancier afsluit. Het CCB adviseert in zijn laatste waarschuwing om beveiligde toegang op afstand te regelen, zodat het noodzakelijke toezicht door kan gaan. Het is dus geen kwestie van de stekker eruit trekken, maar van het samen met de leverancier veilig inrichten.

Dit is hetzelfde patroon dat we in het vorige rapport beschreven bij de toeleveringsketen. Uw beveiliging is zo sterk als de zwakste partij die bij uw systemen kan. Alleen is die partij hier geen softwareleverancier op afstand, maar de vakman die ook de compressor komt vervangen.

5. Wat niet is aangetoond

Een eerlijk rapport zegt ook wat het niet weet. Na de aanvallen op supermarkten kwam bij veel mensen de vraag op of hun eigen koelkast thuis gevaar loopt. Het CCB zegt daarover via Safeonweb dat het geen aanwijzingen heeft dat koelkasten in huishoudens ook het doelwit zijn. Wij nemen dat zo over. Er is geen reden om uw koelkast thuis van het netwerk te halen uit angst voor deze aanvallen.

Wel geeft Safeonweb een nuchter advies dat voor elk slim apparaat geldt. Vervang het standaardwachtwoord, installeer updates zodra ze beschikbaar zijn, beveilig uw wifi en zet slimme apparaten waar mogelijk op een apart netwerk.

Ook over de daders doet dit rapport geen uitspraak. In de berichtgeving circuleren verschillende claims en vermoedens. Daar is nog niets van vastgesteld, en het hoort niet in een analyse die organisaties wil helpen. Wat vaststaat is genoeg om te handelen. Volgens de diensten maakten de aanvallers gebruik van apparaten die vanaf internet bereikbaar waren, van ongewijzigde standaardwachtwoorden en van verouderde software.

Tot slot is de verschuiving van gegevens naar fysieke schade onze eigen duiding. Ze rust op één golf in dit kwartaal en op de signalen die de NCTV beschrijft, niet op een meting over meerdere jaren. Wij brengen het als richting, niet als bewezen trend.

6. Waarom updaten alleen niet genoeg is

De reflex na een waarschuwing is updaten. Dat blijft goed advies. Maar het onderzoek van Midnight Blue laat zien waarom het bij deze apparaten niet volstaat.

De zes kwetsbaarheden die het bureau vond, werken zonder dat een aanvaller hoeft in te loggen. Volgens het CCB gaven een nieuwe firmware, een veranderd standaardwachtwoord en de strengste instelling voor sessies samen nog geen veilige regelaar zolang die vanaf internet bereikbaar bleef. Het onderzoek vond zelfs een zwakte in die sessiebeveiliging zelf. Bovendien waarschuwen de onderzoekers dat een aanvaller zich mogelijk zo kan nestelen dat hij een terugzetting naar de fabrieksinstellingen of een update overleeft, of de regelaar helemaal onbruikbaar maakt.

Daarom noemt het CCB het weghalen van de regelaar van het open internet de enige echte oplossing, en zegt het uitdrukkelijk dat die stap niet mag wachten op een update. Toegang op afstand hoort via een beveiligde en bijgewerkte VPN of een afgeschermd intern netwerk te lopen. Apparaten die de fabrikant niet meer ondersteunt, horen bovenaan de lijst voor vervanging.

Dit sluit aan bij wat het Cybersecuritybeeld Nederland breder vaststelt. De tijd tussen het bekend worden van een kwetsbaarheid en het misbruik ervan is gekrompen van enkele maanden in 2024, via enkele weken in 2025, tot enkele uren in 2026. Wie zijn beheerschermen open laat staan en rekent op de volgende update, is te laat. Wat in die race het meest helpt, is zorgen dat de deur niet openstaat.

Een kanttekening hoort daarbij. De NCTV baseert die reeks op Zero Day Clock, een openbaar dashboard van Sergej Epp van het beveiligingsbedrijf Sysdig, geraadpleegd op 5 juli 2026. Dat dashboard publiceert een tijd tot misbruik inmiddels zelf niet meer, omdat recente jaren er in die meting sneller uitzien dan ze zijn. Er was simpelweg minder tijd om bewijs van misbruik te verzamelen. Lees de reeks daarom als een richting en niet als een precieze maat. De les van dit hoofdstuk verandert er niet door.

7. Handelingsperspectief per doelgroep

Dit rapport is niet bedoeld om te alarmeren, maar om te helpen kiezen waar u morgen begint. De stappen hieronder bouwen voort op de adviezen van het NCSC, het CCB, CERT-FR en de Amerikaanse diensten.

Voor de winkelier, de slager en het mkb

- Maak een lijst van alles in uw zaak dat met internet verbonden is. Niet alleen computers, ook koeling, klimaat, verlichting, camera's, het alarm en de zonnepanelen.
- Bel uw installateur of leverancier en stel drie vragen. Is mijn koel of klimaatsysteem vanaf internet bereikbaar? Is het standaardwachtwoord veranderd? Draait de laatste software, en wordt het apparaat nog ondersteund?
- Spreek af wie verantwoordelijk is voor de beveiliging van dat apparaat, en leg het vast.
- Kijk naar uw verzekeringsvoorwaarden voordat u verbindingen afsluit, en laat de leverancier veilige toegang op afstand inrichten.

Voor de installateur en de leverancier

- Zet geen beheerscherm rechtstreeks open op internet, ook niet tijdelijk en ook niet via een 4G of 5G modem.
- Verander bij elke installatie het standaardwachtwoord en gebruik waar het kan een tweede factor bij het inloggen.
- Houd per klant bij welke apparaten u op afstand beheert, welke software erop draait en wanneer ondersteuning stopt.
- Zie beveiliging als onderdeel van uw vakmanschap. Uw klant rekent erop, ook als het niet is uitgesproken.

Voor ketens, koelhuizen, zorg en overheid

- Neem apparaten in de technische ruimte op in het overzicht van uw IT en uw risicoanalyse.
- Scheid deze apparaten van het kantoornetwerk en beperk wie erbij kan tot bekende partijen.
- Stel grenzen in voor de temperatuur en laat een afwijking direct alarm geven. Leg de logboeken vast en kijk ze na.
- Oefen wat u doet als de koeling 's nachts wegvalt. Wie wordt gebeld, waar gaat de voorraad heen, en hoe herstelt u het apparaat veilig?

Thuis

- Er is geen reden om uw koelkast van het netwerk te halen. Wel geldt voor elk slim apparaat hetzelfde, een eigen sterk wachtwoord, updates aan, en waar het kan een apart netwerk.

8. Wet en keten wijzen dezelfde kant op

Sinds 15 augustus 2026 geldt in Nederland de Cyberbeveiligingswet, de Nederlandse uitwerking van de Europese NIS2 richtlijn. Volgens het NCSC gelden sindsdien nieuwe verplichtingen voor ruim 8.000 organisaties. Voor organisaties die eronder vallen, betekent dit kwartaal iets concreets. Een koelregelaar of klimaatsysteem dat de dienstverlening kan stilleggen, hoort in de risicoanalyse thuis, en een ernstig incident ermee kan onder de meldplicht vallen.

Ook voor fabrikanten verandert er iets. In de gezamenlijke verklaring van 4 november herinneren ENISA en de Europese partners eraan dat fabrikanten sinds 11 september 2026 ernstige incidenten en actief misbruikte kwetsbaarheden moeten melden onder de Europese Cyber Resilience Act. De belangrijkste eisen van die wet, zoals veilig ontwerp en het tijdig verhelpen van kwetsbaarheden, gelden vanaf 11 december 2027.

Voor veel kleine winkeliers verandert de wet niet direct iets. Maar de grotere organisaties die wel onder de wet vallen, zullen naar verwachting vragen gaan stellen aan hun leveranciers en installateurs. Wie kan laten zien welke apparaten hij beheert en hoe die zijn beveiligd, blijft een betrouwbare partner.

Cybercrimeinfo volgt het dreigingsbeeld voor Nederland en België dagelijks. Die kennis staat aan de basis van de Cyber Dreigingsradar, een instrument dat bijhoudt wat er wordt aangevallen en misbruikt en dat vertaalt naar een concreet advies. Een waarschuwing als die over de koelregelaars hoort een organisatie op de dag zelf te bereiken, en niet pas als de schappen leeg zijn. Wij noemen het hier niet om iets te verkopen, maar omdat het precies doet wat dit rapport bepleit, weten wat er nu speelt.

9. Bronnen en methodologie

Werkwijze. Dit rapport verbindt openbare waarschuwingen van overheidsdiensten tot een handelingsperspectief. Elke feitelijke bewering is gecontroleerd tegen de originele publicatie van de betreffende dienst of onderzoeker, die op 16 november 2026 opnieuw is opgehaald en gelezen. Op 24 november 2026 is de kanttekening bij de reeks van maanden, weken en uren toegevoegd. Het rapport bevat geen eigen registratiecijfers. Waar wij zelf een verband leggen, zoals tussen de claims van juni en de golf van oktober en november, staat dat er uitdrukkelijk bij. Over daders en lopende onderzoeken doet dit rapport bewust geen uitspraak.

Gebruikte bronnen.

- CERT-FR, CERTFR-2026-ALE-012, Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération, eerste versie 12 oktober 2026, laatste versie 16 oktober 2026. https://www.cert.ssi.gouv.fr/alerte/CERTFR-2026-ALE-012/
- Centrum voor Cybersecurity België, Warning, Security Incidents in France Targeting Remote Controllers of Refrigeration Installations, 13 oktober 2026. https://ccb.belgium.be/advisories/warning-security-incidents-france-targeting-remote-controllers-refrigeration
- Centrum voor Cybersecurity België, Warning, Update, Security Incidents Across Europe Targeting Remote Controllers of Refrigeration Installations, 3 november 2026. https://ccb.belgium.be/advisories/warning-update-security-incidents-across-europe-targeting-remote-controllers
- Centrum voor Cybersecurity België, Warning, Six New Danfoss Vulnerabilities, Refrigeration Controllers at Risk, 12 november 2026, op basis van onderzoek van Midnight Blue. https://ccb.belgium.be/advisories/warning-six-new-danfoss-vulnerabilities-refrigeration-controllers-risk-immediate-action
- Midnight Blue, Don't bother patching, multiple remote code execution vulnerabilities in Danfoss AK-SM800A, november 2026. https://www.midnightblue.nl/blog/multiple-rce-danfoss-aksm800a

- Nationaal Cyber Security Centrum, In het nieuws, cyberaanvallen op koelinstallaties in Europa, 2 november 2026. https://www.ncsc.nl/nieuws/in-het-nieuws-cyberaanvallen-op-koelinstallaties-in-europa
- ENISA, Joint statement on cyber incidents in refrigeration systems across the EU, 4 november 2026. https://www.enisa.europa.eu/news/joint-statement-on-cyber-incidents-in-refrigeration-systems-across-the-eu
- CISA, FBI, HHS, USDA en DoT, US Government Partners Urge Hardening Industrial Refrigeration and Cold Chain Monitoring Systems, 5 november 2026. https://www.ic3.gov/CSA/2026/261105.pdf
- Safeonweb, Following the incidents involving fridges in supermarkets, could your smart fridge become an oven overnight?, 5 november 2026. https://safeonweb.be/en/news/following-incidents-involving-fridges-supermarkets-could-your-smart-fridge-become-oven
- NCTV, Cybersecuritybeeld Nederland 2026, AI versnelt, verdiept en verbreedt de dreiging, november 2026, rapportageperiode augustus 2025 tot augustus 2026. https://www.tweedekamer.nl/downloads/document?id=2026D56215
- Zero Day Clock, About, waarom het dashboard geen tijd tot misbruik publiceert, gelezen op 24 november 2026. https://zerodayclock.com/about
- Nationaal Cyber Security Centrum, Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht, 7 juli 2026. https://www.ncsc.nl/nieuws/cbw-en-wwke-vanaf-15-augustus-2026-van-kracht

Belangenverklaring. Dit rapport is opgesteld door Cybercrimeinfo, een onafhankelijk kennisplatform over cybercriminaliteit. De genoemde Cyber Dreigingsradar is een instrument dat op basis van deze dreigingsinformatie is gebouwd. De onafhankelijkheid van de analyse staat los van dat instrument. Cybercrimeinfo heeft geen band met de genoemde fabrikanten of onderzoeksbureaus.

Cybercrimeinfo, november 2026. Vragen over dit rapport kunnen via www.ccinfo.nl. Dit rapport mag vrij worden gedeeld en geciteerd met bronvermelding Cybercrimeinfo.