Gids cyberbeveiliging voor de voedingsretail

Bescherm koelinstallaties, monitoringsystemen en de bedrijfscontinuïteit.

Deze gids is bestemd voor voedingsretailketens, winkeluitbaters, koeltechnische installateurs, GBS/GTC-integratoren en onderhoudsdienstverleners.

Nederlandse AI-vertaling | Origineel: Guide Cybersécurité Retail Alimentaire (CAREL)

Waarom deze gids?

Koelinstallaties vormen vandaag een kritieke infrastructuur in de winkel.

Ze sturen koelmeubelen, koelcellen, koelcentrales, warmtepompen, systemen voor energieterugwinning, technische alarmen en energiemonitoring aan.

De toenemende digitalisering van winkels verbetert de energieprestaties en het voorspellend onderhoud, maar stelt de installaties ook bloot aan cyberrisico's.

Een geslaagde cyberaanval kan leiden tot verlies van de bewaking van de winkel, gedeeltelijke of volledige uitval van apparatuur, verlies van gekoelde of diepgevroren producten, dure noodinterventies en aanzienlijke gevolgen voor de bedrijfsactiviteiten.

Het goede nieuws is dat de meeste risico's sterk kunnen worden beperkt met enkele eenvoudige regels voor ontwerp en exploitatie.

De meest voorkomende risico's

1/ Rechtstreekse blootstelling van een regel- en bewakingssysteem aan het internet

In het verleden werden veel installaties als volgt geconfigureerd:

- een openbaar IP-adres
- een poortdoorschakeling op de router
- open toegang op afstand via het internet.

Deze werkwijze is vandaag nog steeds een van de belangrijkste risicofactoren.

Een publiek bereikbaar apparaat kan automatisch worden opgespoord met scantools die kwaadwillenden dagelijks gebruiken.

Een koeltechnisch bewakingssysteem mag nooit rechtstreeks via het internet toegankelijk zijn.

CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

2/ Gebruik van zwakke of gedeelde wachtwoorden

Algemene accounts zoals Admin, Administrator, Service en Maintenance vormen een groot risico wanneer meerdere personen ze gebruiken.

Standaardwachtwoorden of ongewijzigde wachtwoorden behoren nog altijd tot de belangrijkste oorzaken van beveiligingsincidenten.

3/ Systemen die niet worden bijgewerkt

Net als andere IT-apparatuur moeten bewakingssystemen en communicatiegateways regelmatig worden bijgewerkt.

Een verouderde softwareversie kan publiek bekende kwetsbaarheden bevatten.

4/ Onvoldoende beheerde toegang voor leveranciers

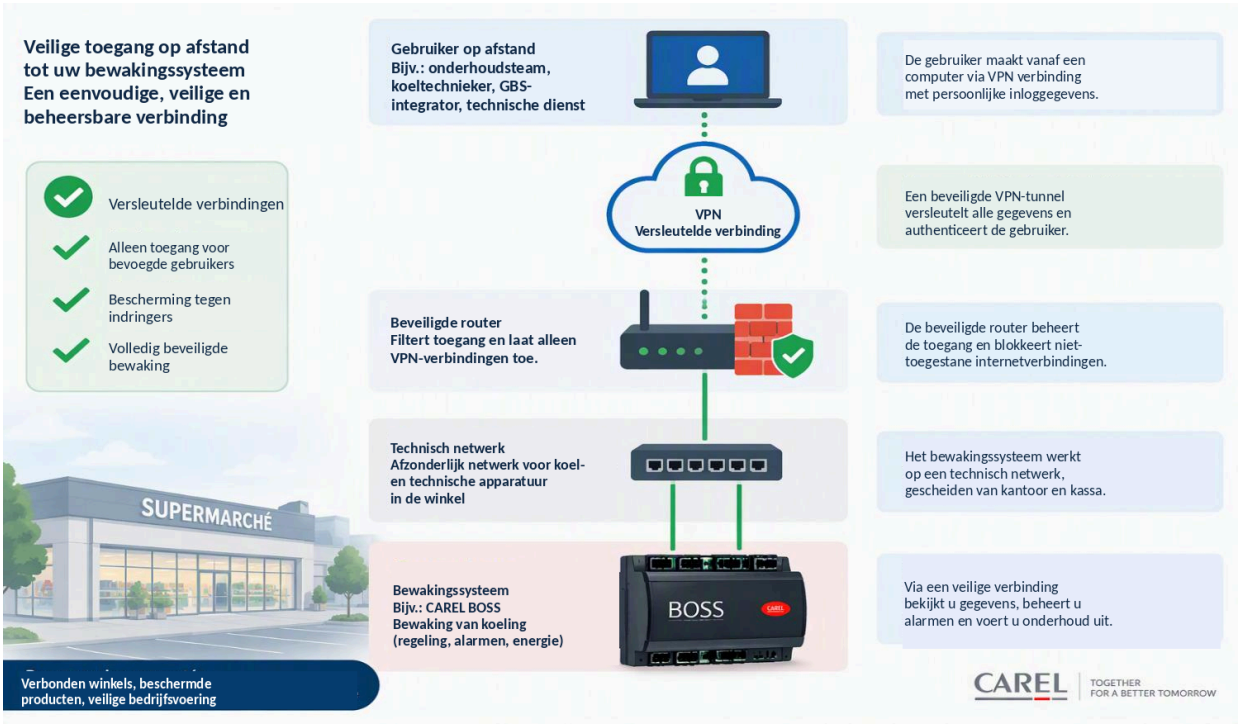
Een winkel kan tegelijk toegang verlenen aan de koeltechnieker, de GBS-integrator, de klant/gebruiker en de externe bewakingsdienst.

Zonder duidelijke afspraken is het moeilijk te weten wie verbinding maakt, wanneer dat gebeurt en met welke rechten.

De 5 gouden regels voor cyberbeveiliging van koelinstallaties

1. Stel het bewakingssysteem nooit rechtstreeks bloot aan het internet

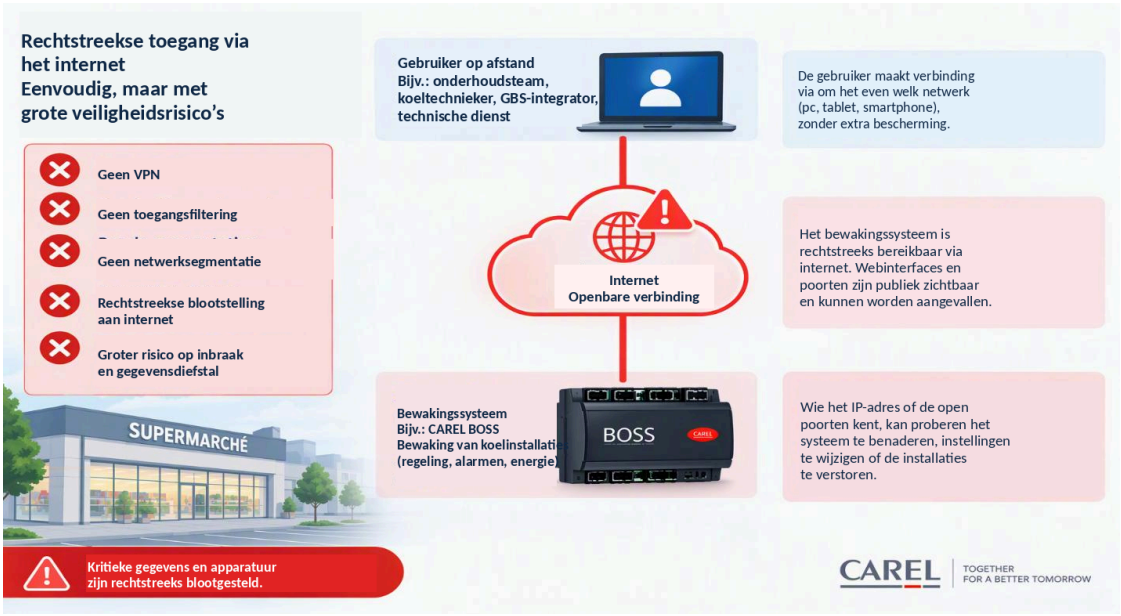
✅ Goede praktijk:



CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

❌ Slechte praktijk:



2. Gebruik een VPN voor alle verbindingen op afstand

De VPN moet de enige toegangspoort zijn.

Een VPN zorgt voor gebruikersauthenticatie, versleuteling van het gegevensverkeer, traceerbaarheid van verbindingen en toegangscontrole.

Een winkelketen met honderden vestigingen kiest best voor een gecentraliseerde VPN-architectuur, beheerd door de IT-afdeling.

3. Segmenteer de netwerken

Het koeltechnische netwerk mag niet dezelfde omgeving delen met kassasystemen, wifi voor klanten, kantoorcomputers of administratieve systemen.

4. Beheer gebruikersaccounts strikt

Elke betrokkene moet een eigen account, rechten aangepast aan zijn functie en individuele traceerbaarheid hebben.

Vermijd algemene accounts, gedeelde wachtwoorden en permanente toegang voor onderaannemers.

5. Houd de apparatuur up-to-date

Controleer minstens de bewakingssystemen, controllers, IP-gateways, VPN-apparatuur en netwerkapparatuur.

Een jaarlijkse controle van de geïnstalleerde versies hoort in het onderhoudscontract.

CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

Snelle zelfevaluatie

Laag risiconiveau ✅

- Bewakingssysteem niet toegankelijk via het internet
- VPN verplicht
- Persoonlijke gebruikersaccounts
- Gesegmenteerd netwerk
- Regelmatige updates
- Gecontroleerde back-ups

Gemiddeld risiconiveau ⚠️

- VPN slechts gedeeltelijk ingevoerd
- Gedeelde wachtwoorden
- Onvolledige documentatie
- Softwareversies niet gecontroleerd

Hoog risiconiveau 🚨

- Openbaar IP-adres
- Open poorten
- Algemene gebruikersaccounts
- Geen opvolging van softwareversies
- Geen controle op toegang op afstand

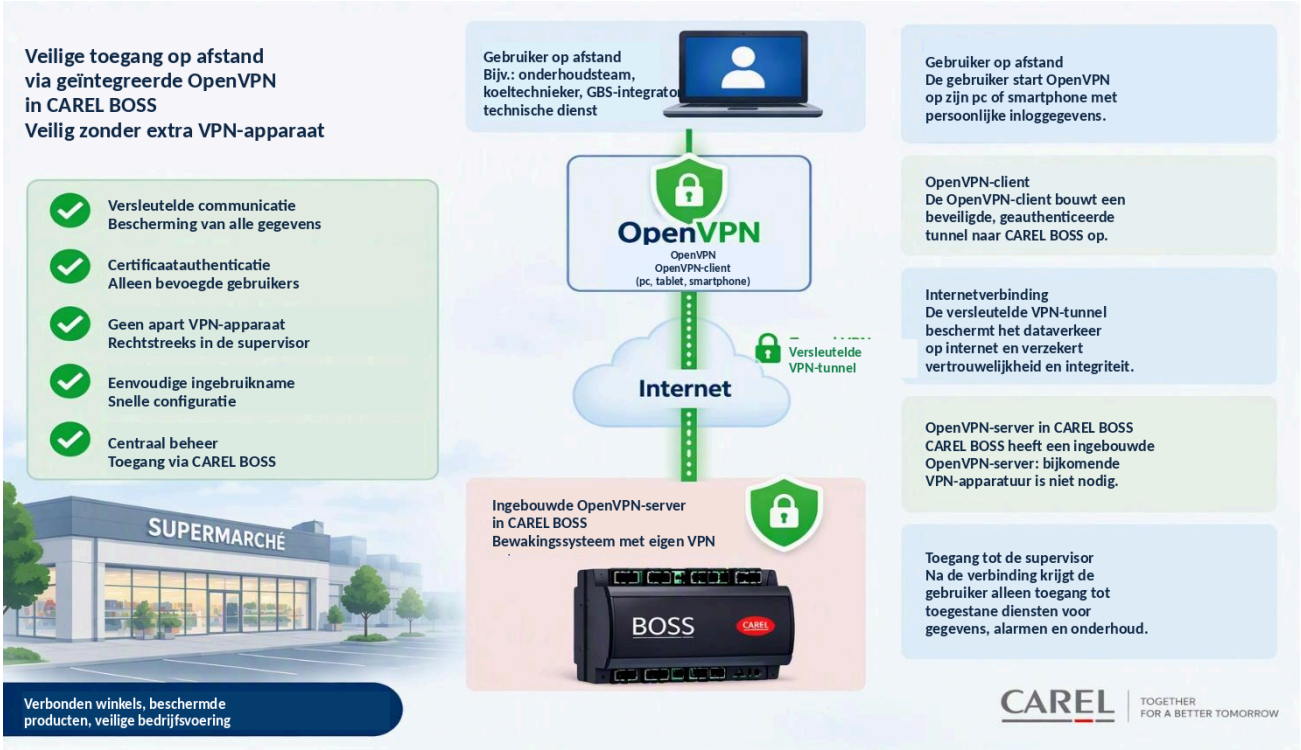
CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

Alternatieven voor een VPN beheerd door de klant (of diens onderaannemer)

1/ In CAREL BOSS geïntegreerde OpenVPN

De OpenVPN-client is standaard geïntegreerd in uw BOSS-bewakingssysteem en kan zonder extra software worden gebruikt. Alle werkzaamheden voor de configuratie, het beheer en het onderhoud van de oplossing via de OpenVPN-server moeten door de klant worden uitgevoerd. Deze optie is geschikt voor klanten die over de nodige kennis beschikken om met standaardtools een beveiligd communicatiekanaal te beheren.



Neem contact op met uw IT-verantwoordelijke en uw CAREL-integrator om deze VPN-toegang te configureren zonder bijkomende kosten voor hardware of software.

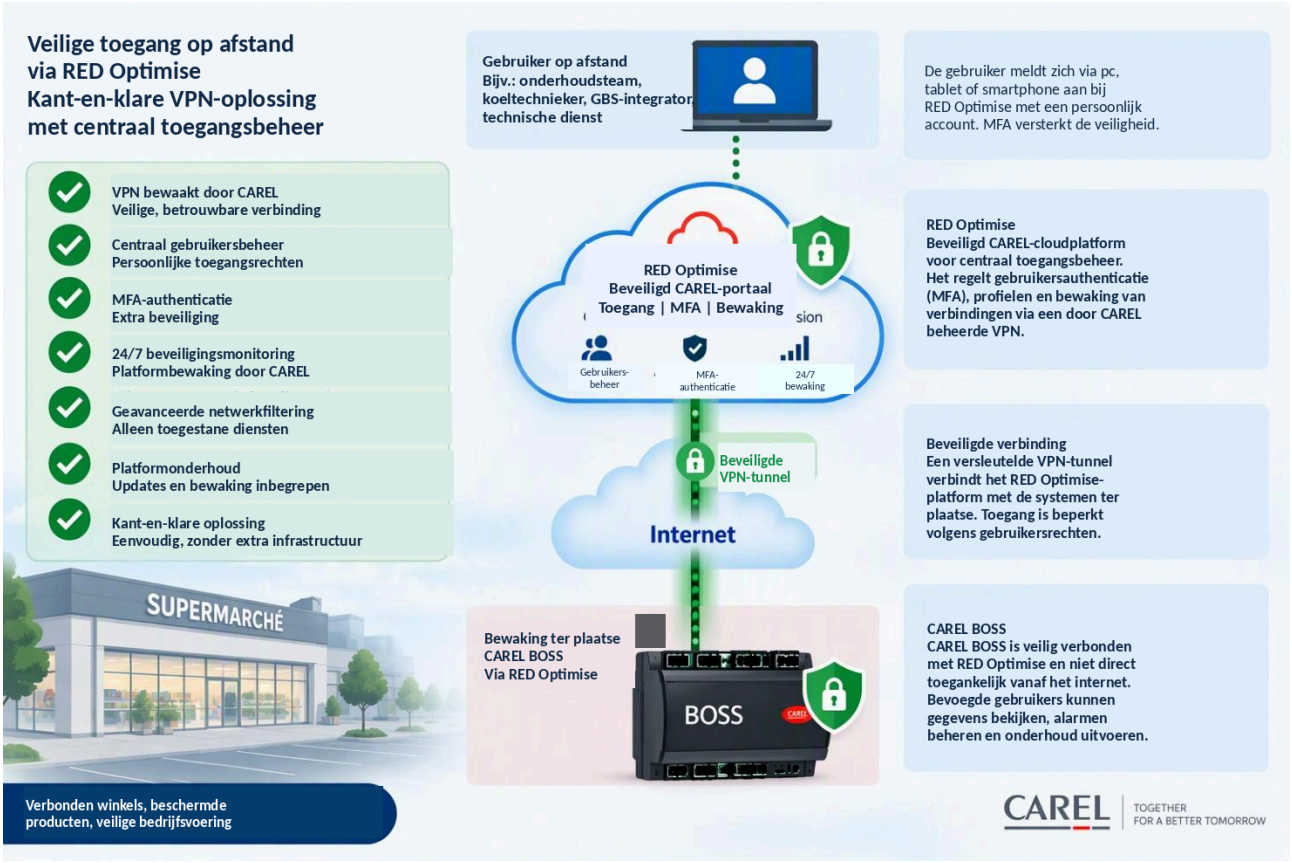
CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

2/ Beveiligde verbinding via aansluiting van bewakingssystemen op RED Optimise

RED Optimise biedt een kant-en-klare oplossing om de beveiliging van klanten te versterken.

Voor klanten die een kant-en-klare oplossing zoeken om hun BOSS-bewakingssystemen te beveiligen, is het aanbod ‘Contractor - Basic’ de instapoplossing.



Met ‘Contractor - Basic’ kunnen onderhoudsactiviteiten via een eenvoudige, intuïtieve interface efficiënter worden beheerd dankzij:

- beveiligde toegang tot locaties via een permanent bewaakte VPN-verbinding, met centraal beheer van gebruikers en profielen
- een dashboard met status en versies van alle geïnstalleerde bewakingssystemen, zodat software-updates gepland kunnen worden zodra nieuwe versies beschikbaar zijn.

RED Optimise omvat meer bepaald de volgende beveiligingsfuncties:

‘Security by design’ (beveiliging vanaf het ontwerp): fysieke en logische beveiligingsmaatregelen

- versleutelde communicatie via HTTPS/TLS en VPN
- geavanceerde filtering van netwerkverkeer
- periodieke kwetsbaarheidsanalyses en penetratietests
- naleving van erkende cyberbeveiligingsnormen en -richtlijnen, waaronder NIST-kaders en kwetsbaarheidsinformatie op basis van CVE’s
- multifactorauthenticatie (MFA)

CAREL beheert het platform en houdt permanent toezicht, waaronder:

- 24/7 bewaking van de infrastructuur
- 24/7 bewaking van de toepassingen
- 24/7 beveiligingsmonitoring
- vier afzonderlijke omgevingen voor ontwikkeling, tests, kwaliteitsborging en productie (Dev, Test, QA en Prod)
- geautomatiseerde inrichting van de infrastructuur en configuratiebeheer.

De kosten voor RED Optimise bestaan uit een jaarlijks abonnement per winkel en een eenmalige opstartvergoeding per winkel.

Hebt u belangstelling voor RED Optimise? Neem dan contact op met uw CAREL-contactpersoon. Die bezorgt u de gebruiks- en abonnementsvoorwaarden.

Afdeling Project & Dealer

CAREL France SAS

Disclaimer - AI-vertaling en aansprakelijkheid

Dit document is een met behulp van artificiële intelligentie (AI) vervaardigde Nederlandse vertaling van het oorspronkelijke Franstalige CAREL-document “Guide Cybersécurité Retail Alimentaire”.

Deze vertaling wordt door HEYTEC uitsluitend ter informatie ter beschikking gesteld. Bij eventuele verschillen, onduidelijkheden of interpretatieverschillen geldt uitsluitend de oorspronkelijke Franstalige versie als referentiedocument.

HEYTEC is niet verantwoordelijk voor de oorspronkelijke inhoud en biedt geen garantie op de juistheid, volledigheid of actualiteit van de vertaling of de verstrekte informatie. HEYTEC aanvaardt, voor zover wettelijk toegestaan, geen aansprakelijkheid voor rechtstreekse of onrechtstreekse schade voortvloeiend uit het gebruik, de interpretatie of de toepassing van de informatie en aanbevelingen in dit document.

Beschikbaarheid in België en dienstverlening door HEYTEC

Niet alle in dit document vermelde producten, oplossingen en diensten zijn noodzakelijk beschikbaar in België of worden door HEYTEC aangeboden of ondersteund. De vermelding ervan vormt geen aanbod of verbintenis van HEYTEC. De actuele beschikbaarheid en voorwaarden moeten vooraf bij HEYTEC worden bevestigd.

CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498