
Grow IT Secure
Gerben Broenink
12 November 2026
Start presentation
TNO innovation for life


TNO innovation for life
HORTIVATION
TECHNICAL GREEN INNOVATION HOLLAND
HortiQ
GREENHOUSE TECHNOLOGY CERTIFICATION
VAA
DATA WORKS
RIDDER
hoogendoorn
growth management
Grow IT Secure (GITS)

Doelstelling GITS





GITS richt zich zowel op het delen van informatie tijdens de bouwfase van de kas als de operationele fase waarbij aparatuur in de kas geautomatiseerd samenwerkt.

In deze presentatie gaan we in op het operationele deel

Waarom cybersecurity?



RTL Z

Koelkasten gehackt in supermarkten België en Zweden: 'Op 70 graden gezet'

RTL Z · 2 november 2026 · Aangepast: 2 november 2026

Vriezers en koelkasten van de Belgische supermarktketen Delhaize zijn gehackt, melden Belgische media. De zusterketen van Albert Heijn spreekt van een 'IT-incident' bij koelinstallaties. Zeker veertig supermarkten zouden zijn getroffen. Er zijn ook problemen in België bij supermarkten van Carrefour, Spar en Intermarché en bij supermarkten in Zweden, Ierland en Estland.

Maak RTL je Google-favoriet



Source: https://www.rtl.nl/nieuws/economie/artikel/5662435/koelkasten-bij-belgische-supermarktketen-delhaize-zijn-gehackt

RTL Nieuws

Grote cyberaanval: koel- en vriesinstallaties Franse supermarkten uitgezet

RTL Nieuws · 12 oktober 2026 · Aangepast: 12 oktober 2026

Honderden winkels van de Franse supermarktketens Intermarché en Coopérative U zijn getroffen door een cyberaanval. Veel winkels moeten hun gekoelde en diepvriesproducten weggooien: de aanval, afgelopen nacht, was gericht op koel- en vriesinstallaties.

Maak RTL je Google-favoriet

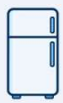


Source: https://www.rtl.nl/nieuws/buitenland/artikel/5658642/hackers-zetten-koelkasten-franse-supermarkten-op-50-graden-schade

Wat is er gebeurd?

- Hackers hebben de vriezers van supermarkten aangevallen.
- ‘s nachts zijn de defrostfuncties aangezet
- Vriezers zijn verwarmt tot 70 graden
- Voedsel vernietigd, beginnende brandjes in de installaties.

Hoe is dit ontstaan?



1 vriezer

Defrost aansturing fysiek op het apparaat zelf

Geen automatisering

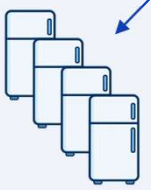
Geen netwerkverbinding

Geen beveiliging

In het verleden had een supermarkt 1 (of meerdere) vriezers, die niet verbonden waren, en geen cybersecurity nodig hadden.

Hoe is dit ontstaan?

Bij een groeiend aantal vriezers, werd dit veel werk voor het personeel om deze allemaal handmatig in te stellen. Met Risico op fouten, waarbij de inhoud van de vriezer kon smelten



- Meerdere vriezer in 1 winkel
- Defrost aansturing fysiek op het apparaat zelf
- Geen automatisering
- Geen netwerkverbinding
- Geen beveiliging

Probleem!
Medewerker moet alle vriezers handmatig aan en uitzetten

Hoe is dit ontstaan?

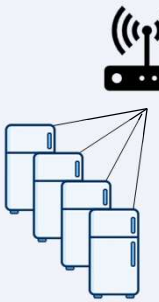
De oplossing is het onderling verbinden van deze vriezers.

Meerdere vriezers in 1 winkel

Alle koelkasten verbonden via netwerk

Netwerk niet verbonden met internet

Medewerker kan via 1 apparaat alle vriezers bedienen



Probleem!
EU vereist registratie van temperatuur (EG 37/2005)

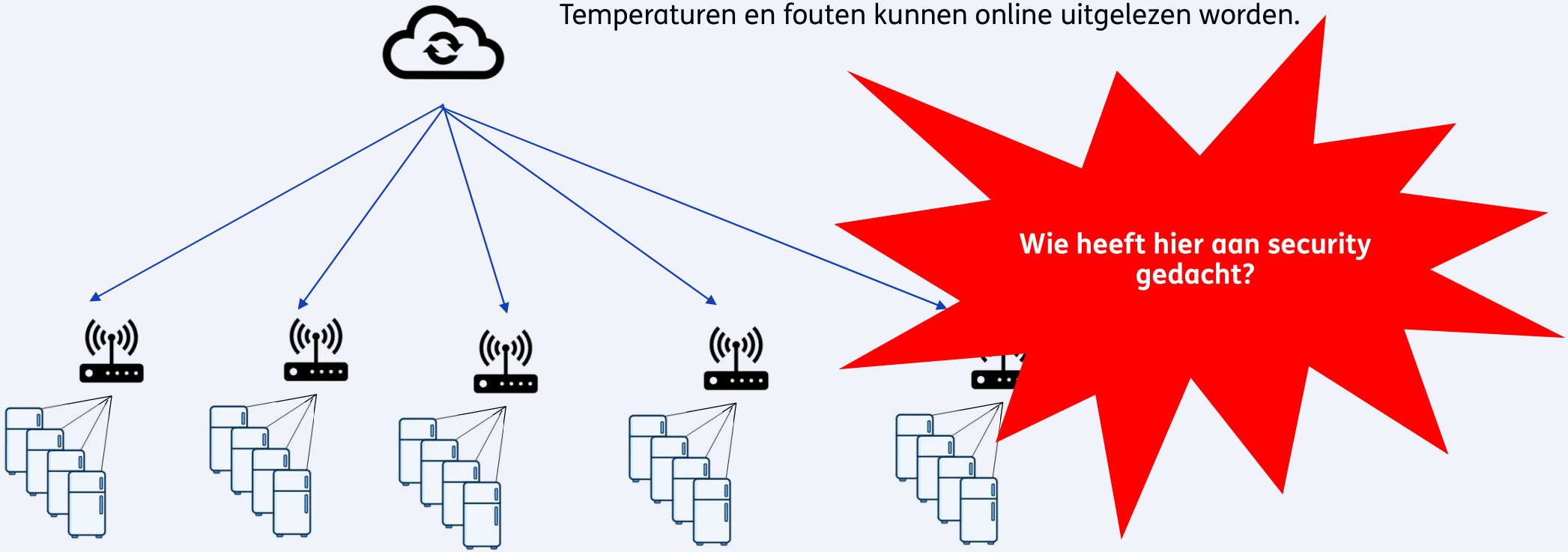
Hoe is dit ontstaan?

Door alle vriezers met het internet te verbinden, is het mogelijk om alle vriezers online uit te lezen, en de data (centraal) op te slaan

Alle netwerken verbonden met internet (niet de EU eis)

Medewerker kan vanaf computer/telefoon/locale interface bedienen

Temperaturen en fouten kunnen online uitgelezen worden.



Hoe zit het met security?

Handleiding voor snelle set-up | System Manager, AK-SM 800

Service Tool Support

Uw AK-SM ondersteunt de Danfoss Service Tool (versie 3.23 en hoger). De Service Tool (CT) moet via een IP-interface worden aangesloten. Als er verbinding is gemaakt, toont de ST de AK-SM en alle apparaten met AK2-platform. Let wel dat apparaten die niet op het AK2-platform zijn gebaseerd niet in de ST-apparaat-lijst worden getoond.



Als u een nieuwe verbinding in uw ST maakt, kies dan het TCP/IP-kanaal.
We gaan er vanuit dat de gebruikersnaam en het wachtwoord uit de fabriek gelden, voer dan in
Supervisor voor de Bestemming
12345 voor het wachtwoord



Ga na aansluiting naar de gewenste regelaar in de beschikbare lijst. U hebt via deze verbinding toegang tot alle AK2-parame-ters.

Een deel van de aangevallen systemen zijn van het merk Danfoss. Het systeem bevat een username en password, welke in de handleiding genoemd worden. (5 keer)

Source: handleiding Danfoss system manager AK-SM 800

Hoe zit het met security?

Ook is er een kwetsbaarheid, waardoor een aanvaller een wachtwoord kan raden. Deze kwetsbaarheid stamt uit 2025, maar in veel gevallen is de update die deze kwetsbaarheid oplost is vaak niet geinstalleerd.

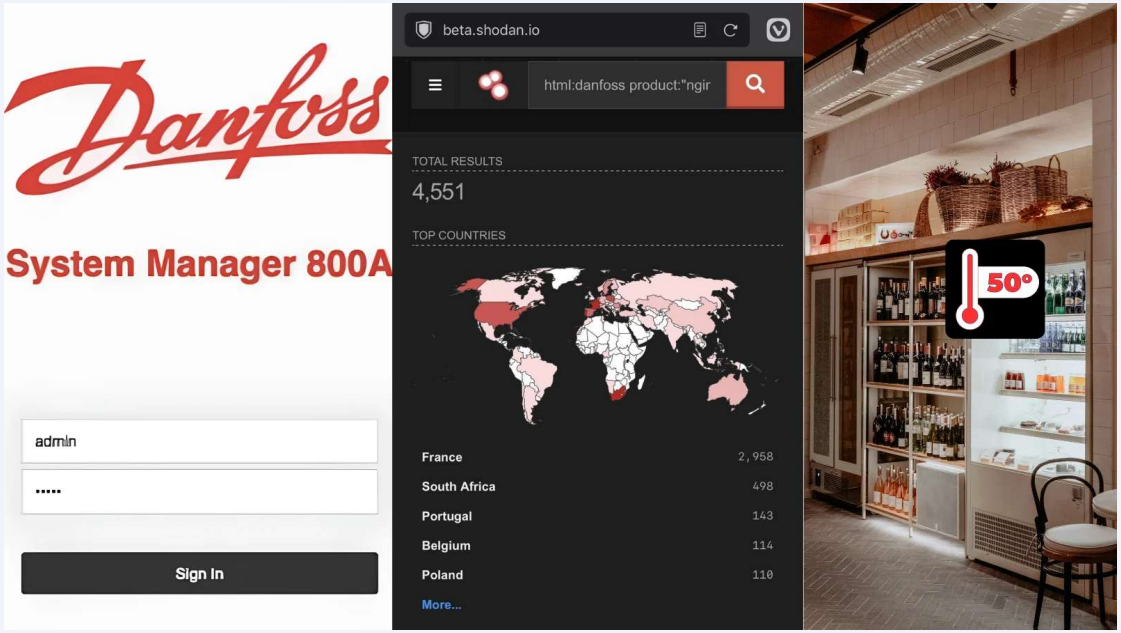
IDENTIFIERS CVE-2025-41450 CWE-287 · Improper Authentication

CVE-2025-41450 is an improper authentication vulnerability affecting Danfoss AK-SM 8xxA refrigeration controllers running software earlier than version 4.2. The embedded web application contains an undocumented code-of-the-day authentication mechanism that bypasses the configured administrator password. Specific attributes in a getauth request direct processing through xml_get_data to check_code_of_day, which validates a code derived solely from the device's current date. An unauthenticated attacker who reproduces the algorithm can generate an accepted code and obtain a fully authenticated administrative session. The vulnerability enables unauthorized management access and sensitive information disclosure.

https://mallory.ai/vulnerabilities/CVE-2025-41450

Hoe zit het met security?

Shodan is een tool waarmee eenvoudig een scan kan worden uitgevoerd om een bepaald type systeem op het internet te vinden. Een scan levert 4551 systemen op, waarvan 2958 in Frankrijk



https://cybersecuritynews.com/danfoss-refrigeration-hack-exposed-hosts

Wat is er waarschijnlijk gebeurd?

Wat we weten:

- Veel systemen van buitenaf bereikbaar
- Systemen van verschillende fabrikanten (Danfoss, maar ook Copeland/Dixell)
- Verouderde / end-of-life systemen
- Beveiliging zeer minimaal
- Patches voor bekende kwetsbaarheden vaak niet uitgevoerd

Waarschijnlijk scenario:

- Verkenning gedaan naar publiek bereikbare controllers
- Aanvallen met:
    - Default usernames en passwords
    - code-of-the-day passwords
    - bekende kwetsbaarheden
- Alle controllers in defrost mode gezet.

Onderliggende oorzaken



IT – Informatie Technologie

VS



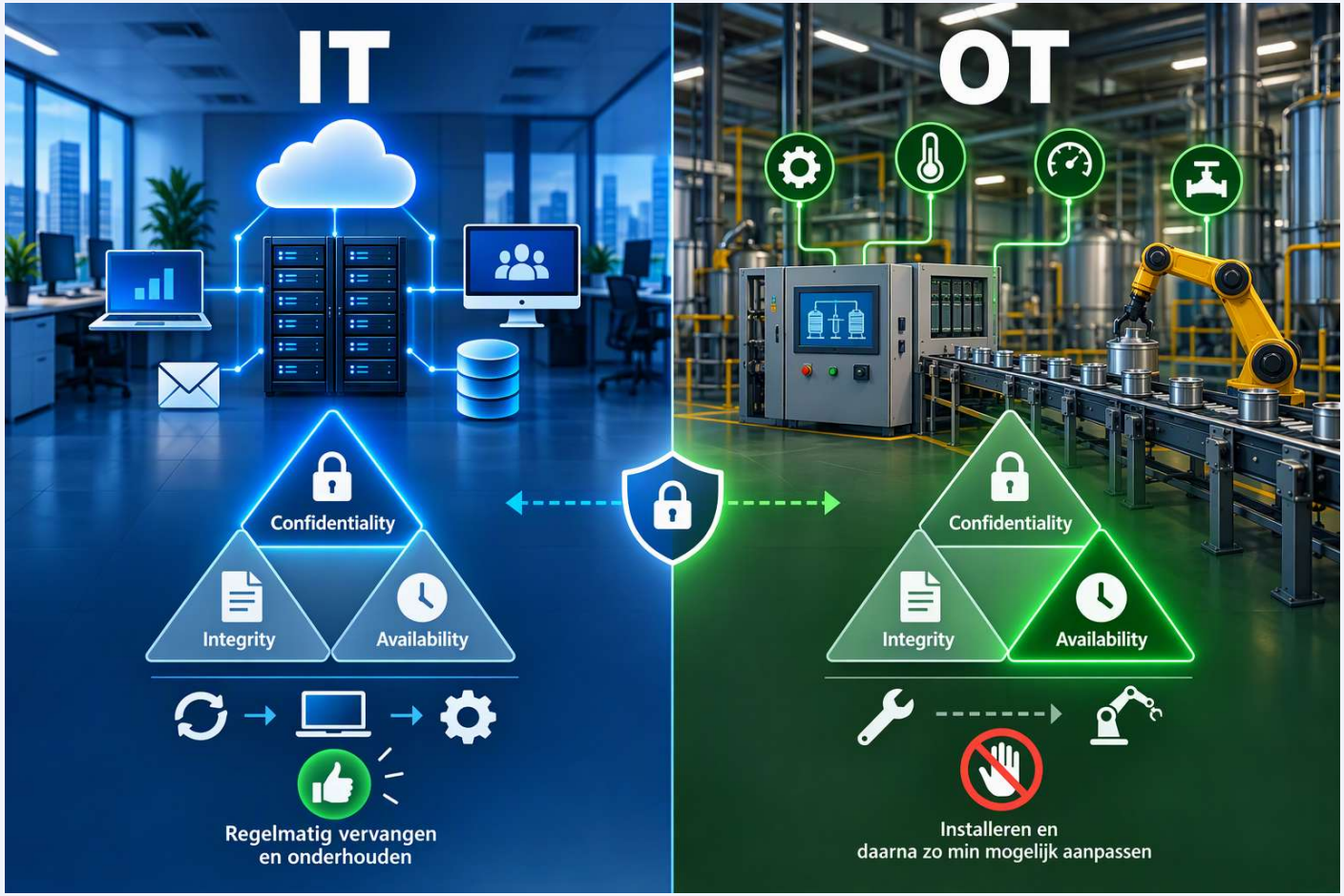
OT – Operationele Technologie

Er zijn 2 soorten computersystemen. IT systemen, zoals computers, laptops, servers en datacenters. En OT systemen, dit zijn computersystemen die gebruikt worden op industriele en operationele systemen aan te sturen. Denk aan een computer die een machine in een fabriek aanstuurt, of een computer die een verwarmingssysteem in een kas aanstuurt.

Onderliggende oorzaken

IT systemen zijn ingericht om de vertrouwelijkheid (confidentiality) van de data te beschermen. Daarom bevatten de systemen wachtwoorden en encryptie.

Ook worden updates vaak doorgevoerd, en worden die systemen na enkele jaren vervangen

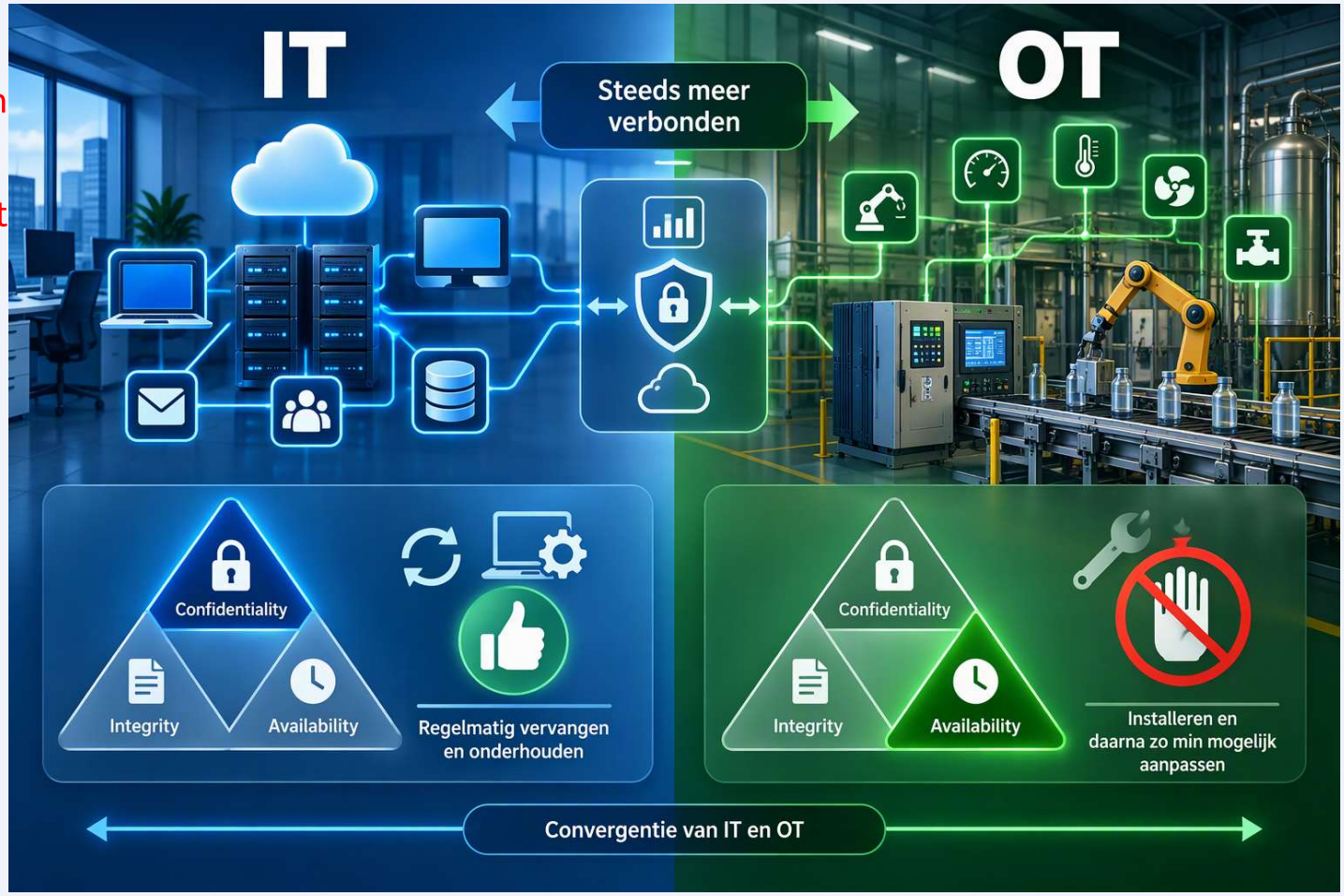


IT systemen zijn ingericht om de beschikbaarheid (availability) van de systemen te beschermen, zodat een machine nooit stil staat (dat is namelijk erg kostbaar)

Updates wordt weinig tot niet doorgevoerd, en wachtwoorden worden bij voorkeur niet gebruikt. Dit kan namelijk de beschikbaarheid Schaden.

Wat is de kern van het probleem?

Deze twee soorten systemen worden steeds vaker verbonden met elkaar. Zo kan het management op kantoor de productiecijfers uit de fabriek zien, en heeft de teler op zijn telefoon inzicht in wat er in de kas gebeurt.



MAAR, er ontstaan nieuwe Risico's. Deze OT hebben niet de bescherming die nodig is om aan het internet verbonden te zijn.

Interesante links:

https://thehackernews.com/2026/10/attackers-heat-french-supermarket.html

Deze publicatie is enkele maanden voor de aanval gepubliceerd:

https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers

En hoe zit het met kassen?

Kassen zijn ook OT systemen, welke steeds meer met het internet verbonden zijn. Zijn deze ook kwetsbaar?



Fysieke bescherming

Sterke focus op beschikbaarheid

Weinig updates

If it ain't broken, don't fix it

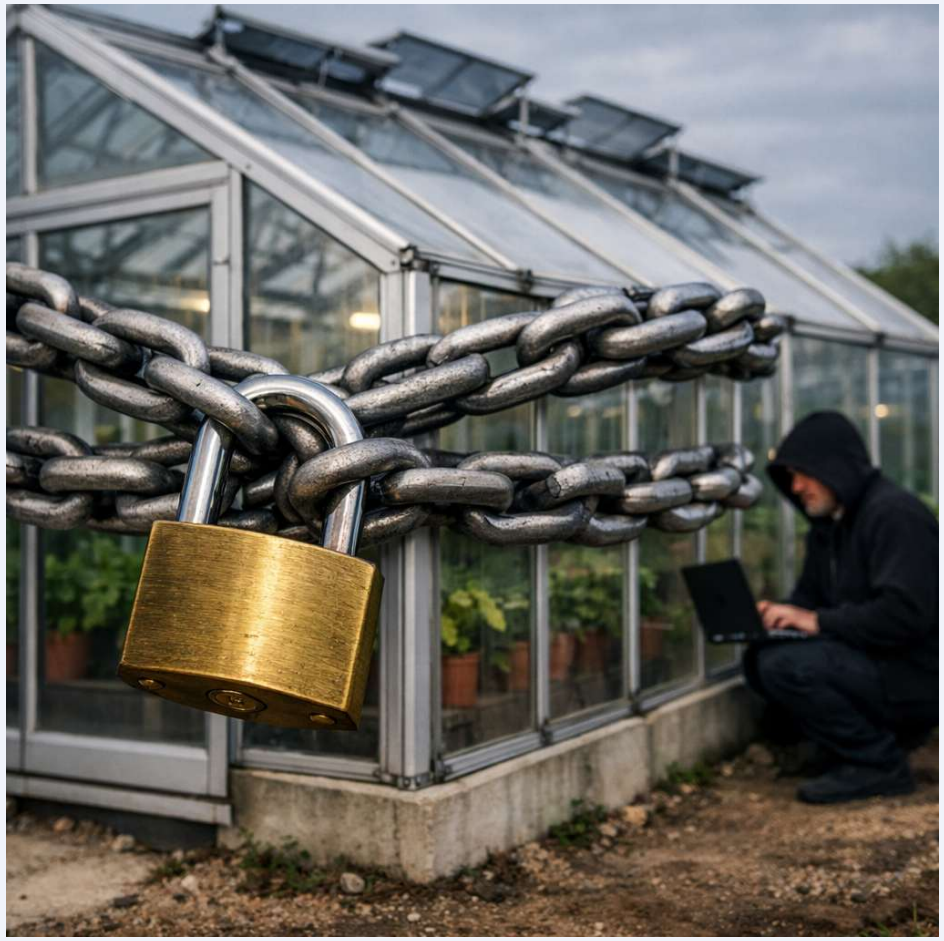
En hoe zit het met kassen?

Op de langere termijn zien we steeds meer verbindingen tussen systemen in de kas, en systemen buiten de kas.



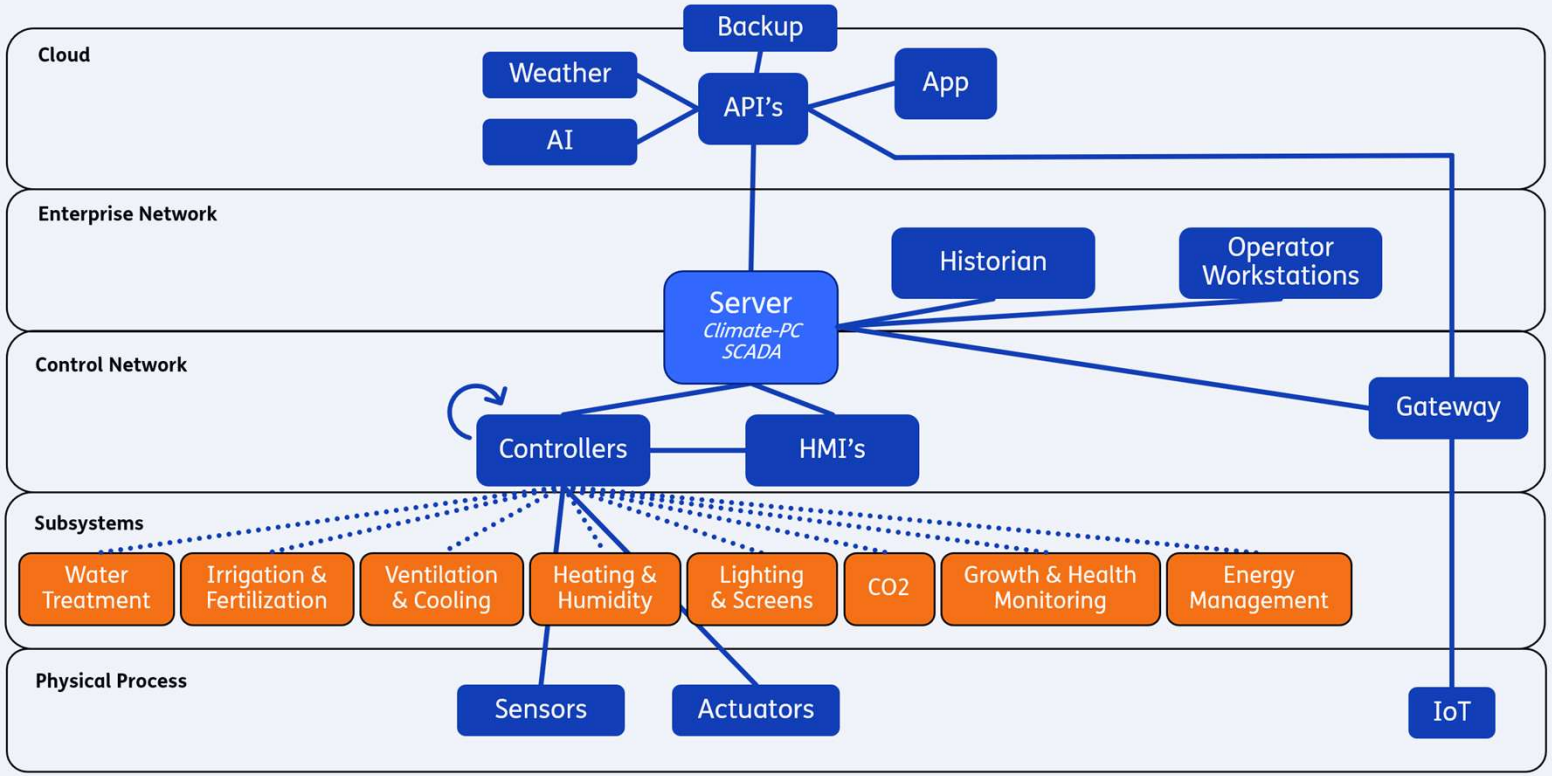
En hoe zit het met kassen?

Als we niks doen, worden
Kassen dus ook kwetsbaar



Referentiearchitectuur

TNO heeft een referentiearchitectuur gemaakt, om een analyse te doen over de kwetsbaarheden in de kas



Risicoanalyse

De risicoanalyse laat zien dat de ervaren risico's met name betrekking hebben op de planten in de kas. (mislukte oogst en verminderde opbrengst)

		Kans	Impact	Kans * impact
1	Oogst mislukt	2,3	3,0	7,0
2	Verminderde opbrengst	3,7	1,5	5,5
3	Verminderde kwaliteit	3,7	1,3	4,9
4	Fysieke schade	1,7	2,7	4,4
5	Niet nakomen jurisdische verplichtingen	3,0	1,0	3,0
6	Niet nakomen energieovereenkomst	2,7	1,7	4,4
7	Kostenverhoging	3,0	1,7	5,0
8	Ongevallen	1,7	2,5	4,2
9	Ransomware	4,0	1,3	5,3
10	Imago	2,7	1,7	4,4
11	IP	2,3	2,0	4,7

Maatregelen

Het NIST framework laat de orde van maatregelen zien.

Naast beschermende maatregelen (protect) zijn er ook andere maatregelen mogelijk.

TNO richt zich in het onderzoek op detectieve maatregelen. Er is altijd een mogelijkheid dat een aanval slaagt, en daarom wil je in staat zijn om die te detecten zodat je kunt reageren om de schade te beperken



Source: https://www.device42.com/compliance-standards/nist-csf-categories/

Proof-of-Concept

- Cyber security monitoring in Tomatoworld
- Verzamelen van sensor en netwerk data
- Anomaliedetectie op OT
- Simulatie van aanval om de detectie te demonstreren
- Dit leidt uiteindelijk tot een blauwdruk ‘Cyberweerbaarheid tuinbouw’



Was dit een oplossing geweest in Frankrijk?

- Inlogpogingen vanuit andere ip-addressen
- Alle vriezers werden tegelijk in ‘defrost mode’ gezet
- ‘s nachts
- Voor de hele nacht

Effectieve detectieve maatregelen zouden in staat zijn geweest om de aanval in Frankrijk te detecteren. Zodat maatregelen genomen konden worden voordat er grootschalige schade zou zijn ontstaan.



TNO | innovation for life

Vragen?

