# Hack FRL

*13 april 2026 - Leeuwarden*

Van Risicovolle Continuïteit naar Zorgeloos Douchen

Theun Prins

06-53 24 59 73 | t.prins@yourpartner.nl

# Aanleiding en doel vandaag

Alle deelnemers inzicht te geven in digitale kwetsbaarheden en daarmee bij te dragen aan een sterkere cyberweerbaarheid van overheden.

# 'Friesland onder water' en de Gemaalkast

Tijdens Hack.FRL wordt live door ethical hackers geprobeerd gemaalcomputer te hacken. De opstelling *'Friesland onder water'* vindt u samen met de Gemaalkast tegenover het Auditorium.

# YP Your Partner – Telemetrie specialist

Industrieel software ontwikkelaar uit Drachten. Sinds 1987 focus op water & infra. Engineering en software development in eigen huis. Het CARS IIoT platform is de rode draad in ons bestaan. Lid van het Innovatiecluster Drachten.

your partner

# CARS IoT platform openbare ruimte

Your Partner bouwt en beheert het Webbased Industrial Internet of Things (IIoT) platform. Volledig merkonafhankelijk, 100% made in Holland. Publieke ruimte van +40 gemeenten, provicie, Rijkwaterstaat maar ook in andere domeinen.

https://www.linkedin.com/in/theunprins/




# Theun Prins

Passionate about connecting IoT innovation with strategic opportunities. Let's build the future together.

Drachten, Friesland, Nederland

www.yourpartner.nl

12.950 volgers · 500+ connecties

**Directeur / Eigenaar**
YP Your Partner BV · Fulltime
sep. 2003 - heden · 22 jr 8 mnd

**Lid**
Innovatiecluster Drachten
okt. 2014 - heden · 11 jr 7 mnd

**Oprichter**
BEER EYE - Tank Monitoring · Zelfstan
jan. 2024 - heden · 2 jr 4 mnd

your partner

https://cyberborg.eu

CYBERBORG

PROBLEEM DIENSTEN MARKT OVER ONS

NULMETING AANVRAGEN

DE OT-SECURITY AUTORITEIT VOOR GEMEENTELIJKE VITALE INFRASTRUCTUUR

# NIEMAND WEET WAT ER IN UW GEMALEN RONDGAAT.

Slechts 95% van de rioolinstallaties is voldoende beveiligd. **De resterende 5% hebben we echter niet in beeld — en dat is een stevig risico.** Cyber Borg brengt het in kaart en dicht de gaten.

NULMETING AANVRAGEN →

WIE ZIJN WIJ


7.500

0

24u

NIS2

# Casus voor vandaag

your partner

# Veere – 14 februari 2012

# TV: “ Sluizen, gemalen en bruggen slecht beveiligd ”

https://eenvandaag.avrotros.nl/artikelen/sluizen-gemalen-en-bruggen-slecht-beveiligd-39770

1V EenVandaag

## Sluizen, gemalen en bruggen slecht beveiligd

14 feb 2012, 18:15 Joost Blokzijl Willem Jan Bloem

Delen

**Het blijkt kinderlijk eenvoudig om sluizen, gemalen, rioleringspompen en zelfs bruggen in Nederland via internet op afstand te bedienen. In EenVandaag een reportage die bijvoorbeeld laat zien hoe slecht de rioleringspompen en gemalen van de gemeente Veere zijn beveiligd. Met een paar simpele handelingen zijn ze vanaf een thuiscomputer te bedienen. De Nationaal Coördinator Terrorismebestrijding (NCTB) waarschuwt al enkele jaren voor de kwetsbaarheid van deze zogenoemde 'SCADA-systemen' maar dat lijkt weinig te helpen.**

Beveiligingsexperts van instituut NIKHEF en kennisorganisatie TNO zeggen dat veel meer Scada-systemen in Nederland kwetsbaar zijn, variërend van parkeergarages en verwarmingssystemen tot complete bruggen en sluizen. Een nieuwe zoekmachine laat zelfs honderden Nederlandse systemen zien die met gemak te hacken zijn. In sommige gevallen zijn die beveiligd met een standaard wachtwoord, in andere gevallen is er in het geheel geen wachtwoord nodig om in de betreffende apparatuur binnen te dringen. Beveilingsspecialist Oscar Koeroo, werkzaam bij het Nationaal instituut voor subatomaire fysica (NIKHEF) is geschokt. Over de situatie in Veere zegt hij: 'De machines staan bloot aan het internet. Er is geen beveiliging die ervoor zorgt dat alleen de beheerder toegang heeft'.**Niet slim**

Eric Luiijf, Scada-expert en onderzoeker bij TNO waarschuwt al jaren voor de gevaren van dit soort systemen. 'Vanaf 2001 ben ik hier al mee bezig en in 2005 hebben we de overheid zelfs al gewaarschuwd.' Volgens hem hoef je geen ervaren hacker te zijn om in de systemen in te kunnen breken: 'Je hoeft hier helemaal niet slim voor te zijn, dat is juist het gevaarlijke'.**Ernstige bedreiging**

De NCTB schreef in december 2011 nog over de gevaren van aanvallen op Scada-systemen: 'Dergelijke aanvallen vormen een potentieel ernstige bedreiging voor de nationale veiligheid wanneer zij de vitale infrastructuur (zoals energie, water, financiën) treffen. Bij dergelijke complexe aanvallen is het risico van maatschappelijke ontwrichting reëel*'. In een reactie laat de NCTB weten bezorgd te zijn over de door EenVandaag ontdekte situatie en de organisatie staat de gemeente Veere bij om voor de uitzending van vanavond de systemen goed te beveiligen.

Onderlopen

Peter van Rooij, expert op het gebied van de waterhuishouding, is geschrokken. 'Als je dit niet goed beveiligd, dan loopt Nederland onder, zo kwetsbaar zijn we hier. Eric Luiijf van TNO benadrukt dat het gevaar nog niet eens van hackers hoeft te komen. 'De echter hacker, die denkt nog na over welke schade hij aanbrengt. De eerste de beste 13-jarige die binnenkomt en pompen uitzet veroorzaakt behoorlijke schade'.

your partner

# Veere – 15 februari 2012

# Tweede Kamer: “ Kwetsbaarheid systemen ‘betreurenswaardig’ ”

BNR Nieuws Radio Programma's & Podcasts Video Overig

ANP • 15 feb '12 17:03

## Kwetsbaarheid systemen 'betreurenswaardig'

ANP

DEN HAAG (ANP) - Betreurenswaardig, bloedserieus. Zo noemde minister Ivo Opstelten (Veiligheid) het feit dat het zo simpel is sluizen, gemalen, pompen en bruggen via internet te beïnvloeden. VVD en D66 stelden dit woensdag aan de orde, naar aanleiding van een uitzending van EenVandaag.

Als voorbeeld had het programma gemalen en riolering in Veere gekraakt. Het password bleek eenvoudig te achterhalen.

De verantwoordelijkheid voor dergelijke installaties ligt echter bij de eigenaren ervan, aldus Opstelten, en het toezicht bij de toezichthouders. Pas als de nationale veiligheid in het geding is, komt hij aan zet, en zover is het niet gekomen. Wel zal het Nationaal Cyber Security Centrum bij het overleg over dit soort kwetsbaarheden worden betrokken.

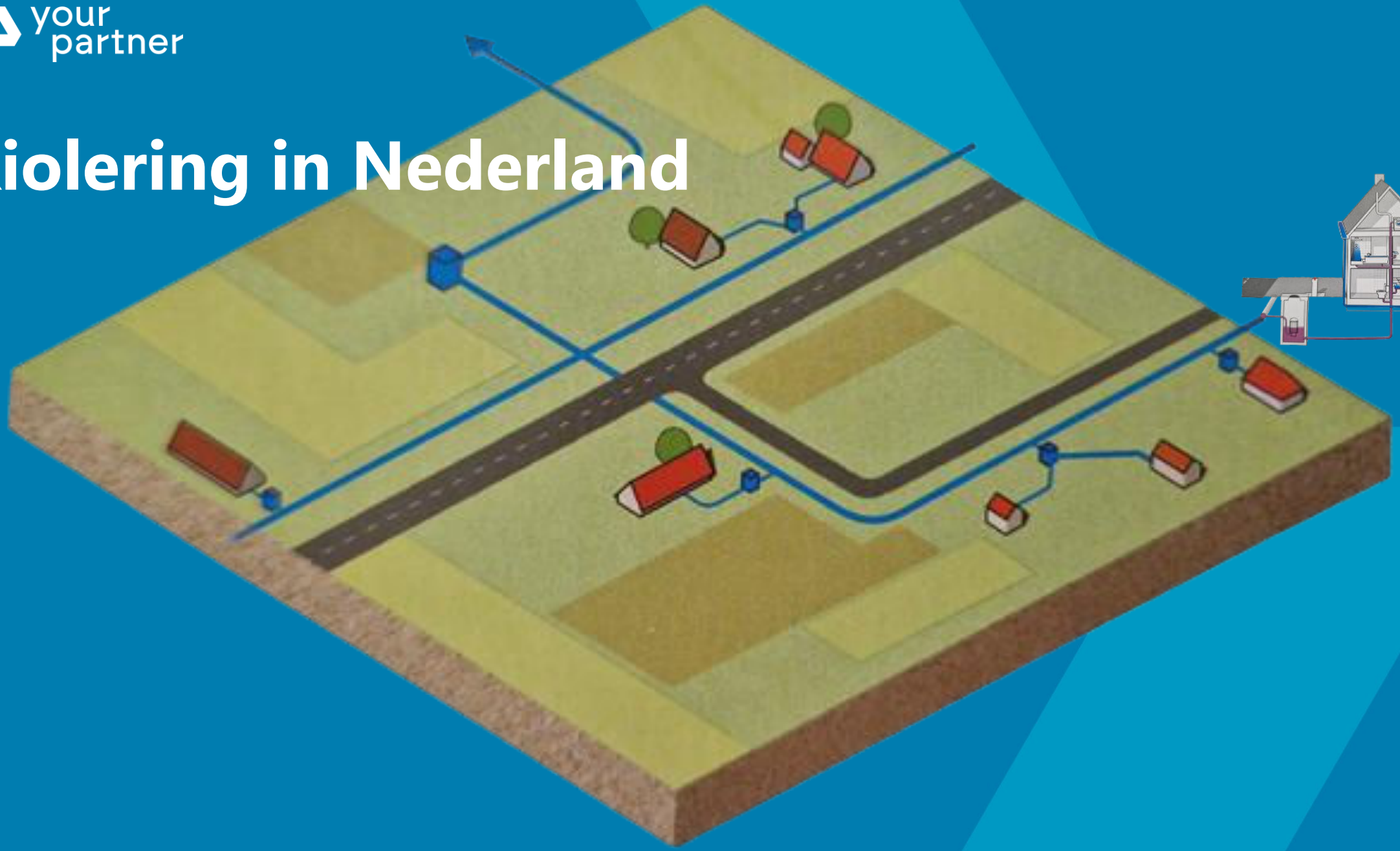
https://www.bnr.nl/nieuws/anp/10246658/kwetsbaarheid-systemen-betreurenswaardig

# Wat is er vervolgens gebeurd?

# Mini-cursus Riolering in Nederland

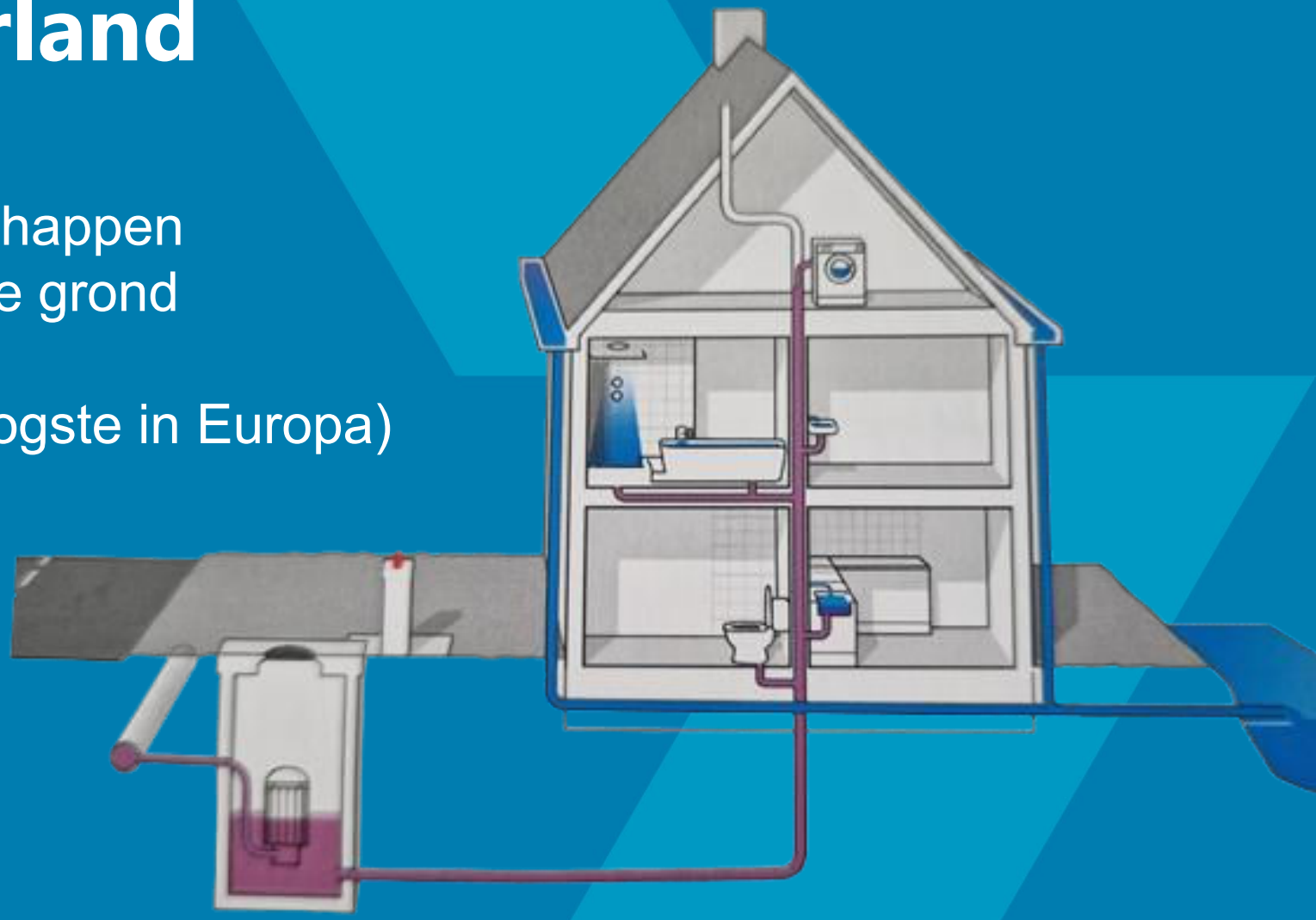
your partner

# Riolering in Nederland



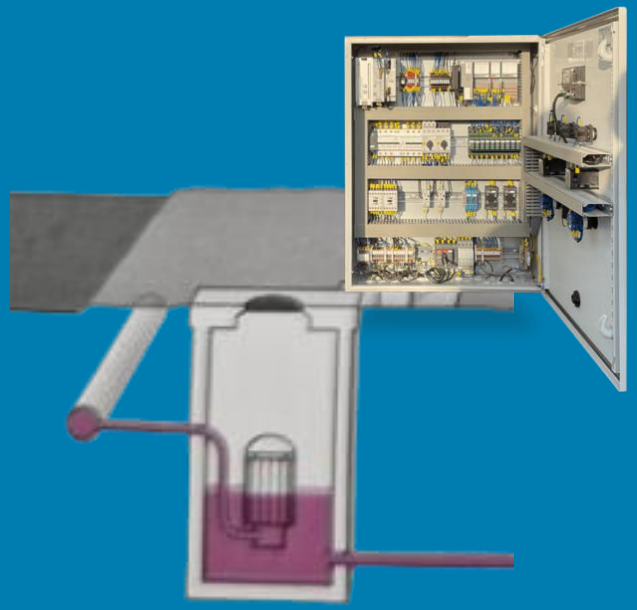
# Riolering in Nederland

- 340 Gemeenten / 21 Waterschappen
- ~130.000 km aan buizen in de grond
- >150.000 pompunits
- Aansluitingsgraad 99,7% (hoogste in Europa)



your partner

# Riolering in Nederland



your partner

# Gemaalbesturingen

Hoofd gemalen

Alles state of the Art

Super veilig MITS juist geconfigureerd

your partner

# Gemaalbesturingen

Drukriolering

Eenvoudig en straight forward

Veilig MITS juist geconfigureerd

your partner

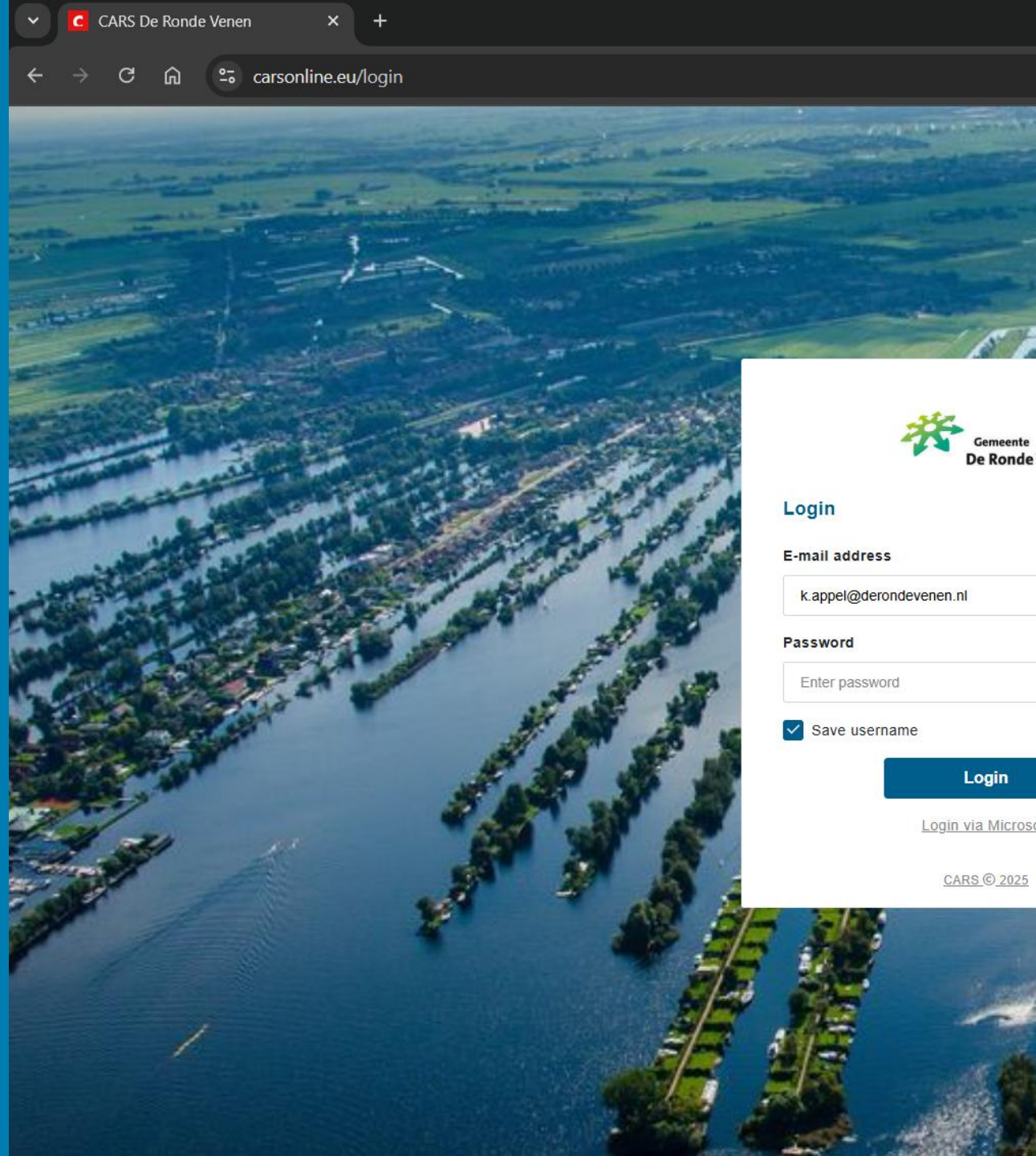
# Connectivity

- Managed SIM Kaarten
- VPN tunnels
- APN
- Pro actieve monitoring

# Gemalen achter het Saas-model

- Beveiligde web server
- Toegang via Single Sign-On (SSO)
- 2 factor authenticatie

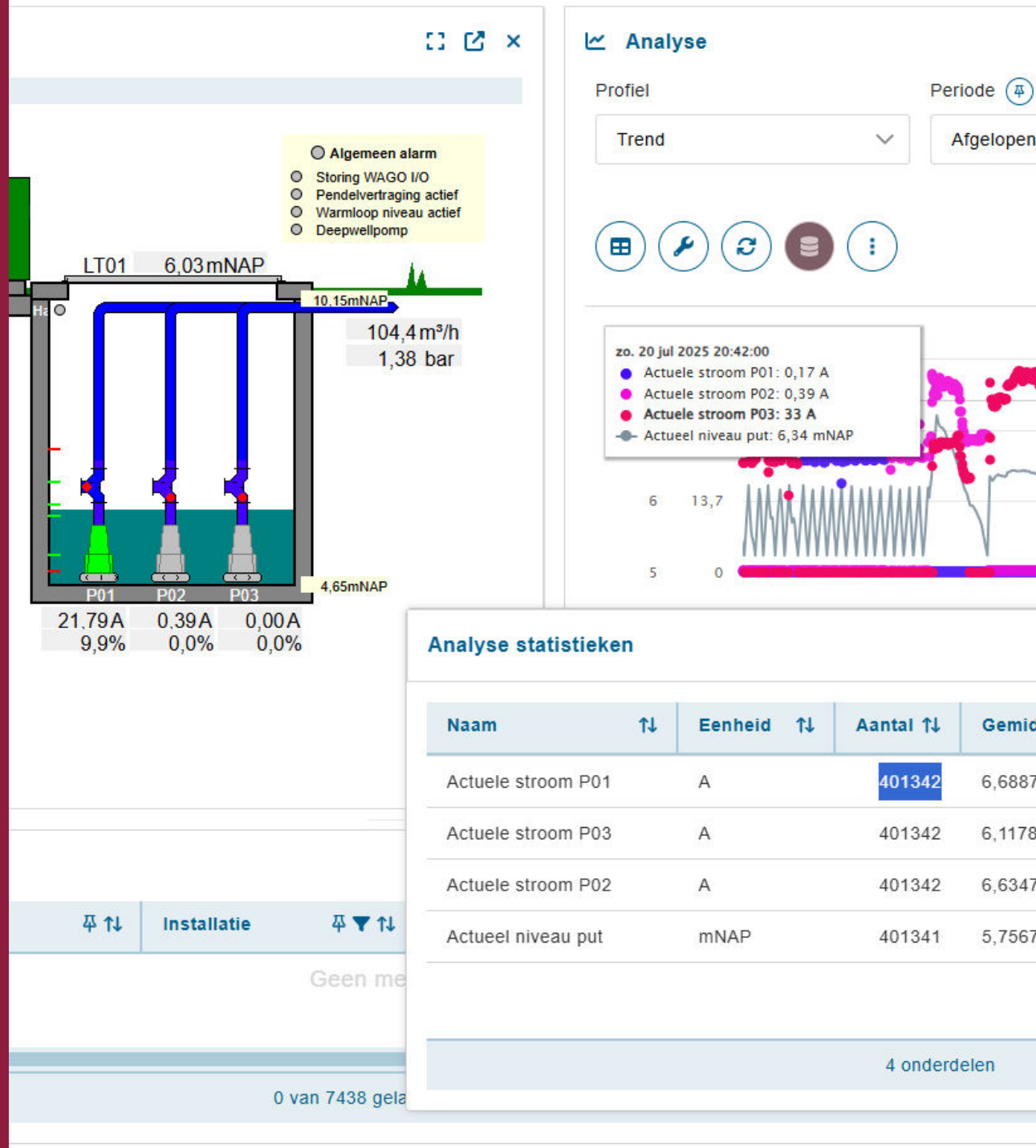
*Bron: De Ronde Venen*



# Remote Control van objecten

- Live meekijken en sturen in processen
- Historische data inzien
- Alarmen afhandel via app of web

*Bron: Gemeente Duiven (1Stroom)*

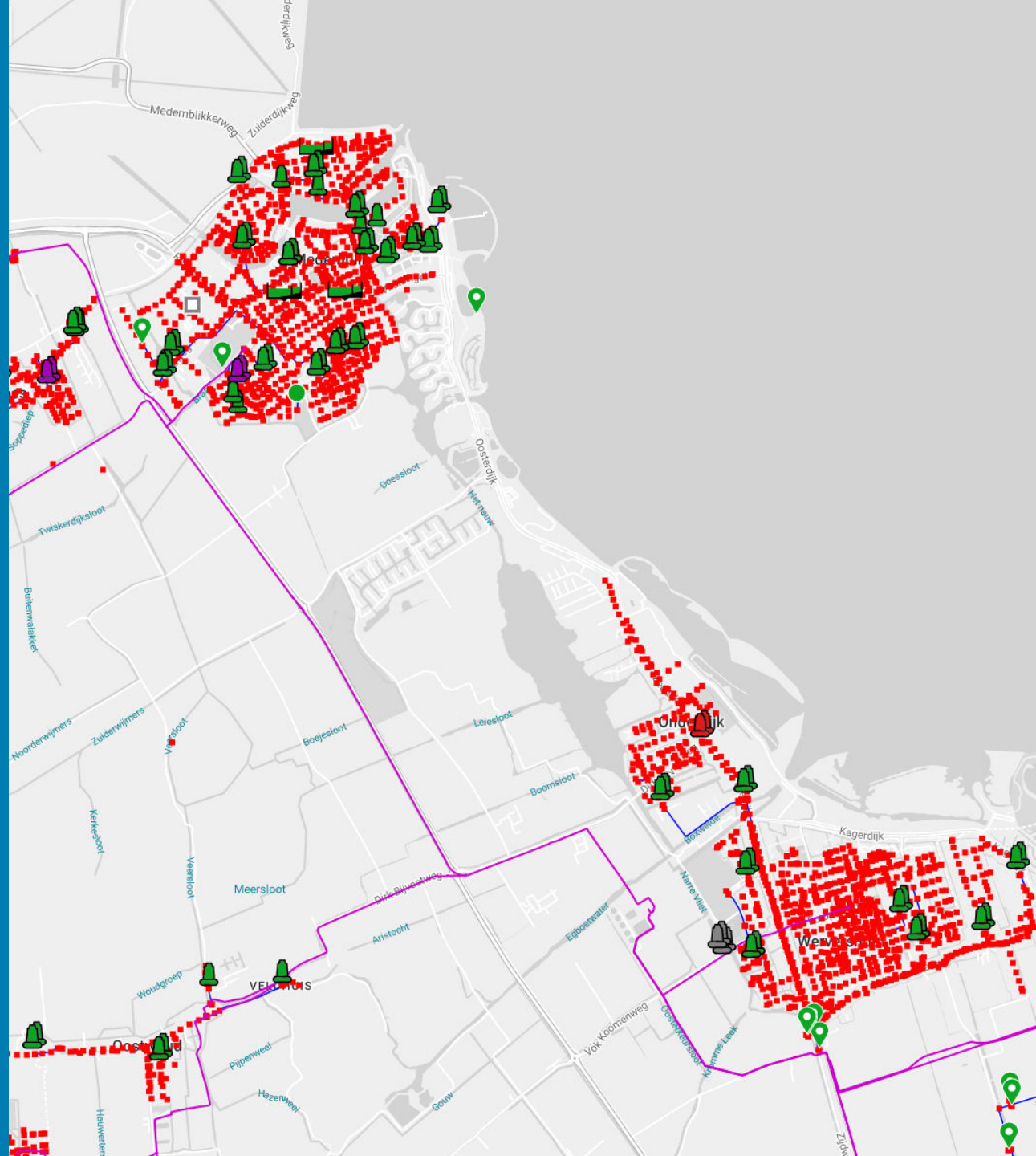


your partner

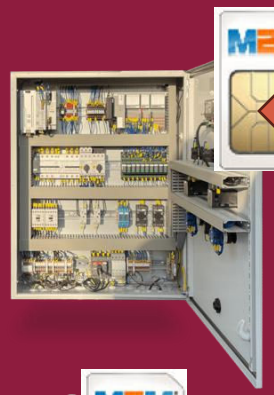
# Geografische Mogelijkheden (GIS)

- Alle objecten op een dynamische kaart
- Integratie van externe kaartlagen (o.a. PDOK, GWSW)
- Koppelingen met verschillende bronnen

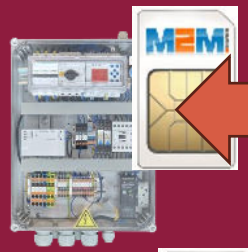
*Bron: Gemeente Medemblik*



your partner



Secure



Secure

LON

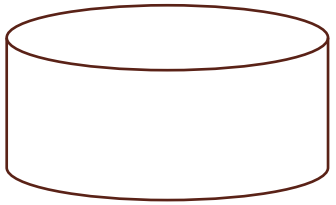
Provider

KPN/Ziggo/Vodafone

VPN

SaaS
Web Hoofdpost

Centraal Alarmering en
Registratie Systeem



Fixed IP

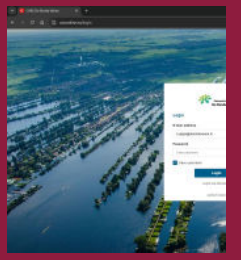
Laptop
HACKER

https://

Tablet
monteur

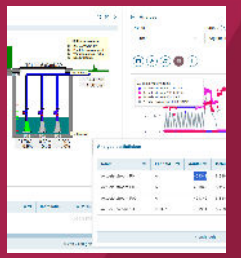
https://

Desktop
Adviseur



https://

Laptop
aannemer



# … terug naar Veere

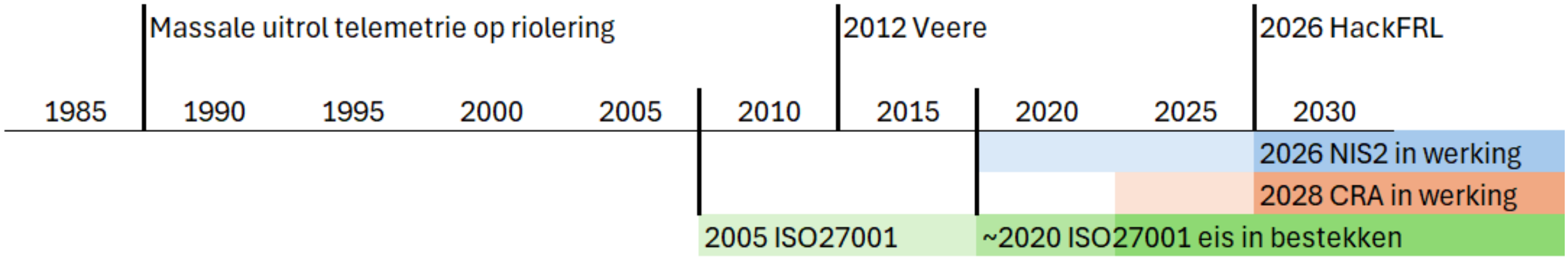
your partner

# 16 februari 2012

# Oorzaak bleek: veere / veere


https://www.visbardomburg.nl/

# Globale tijdlijn

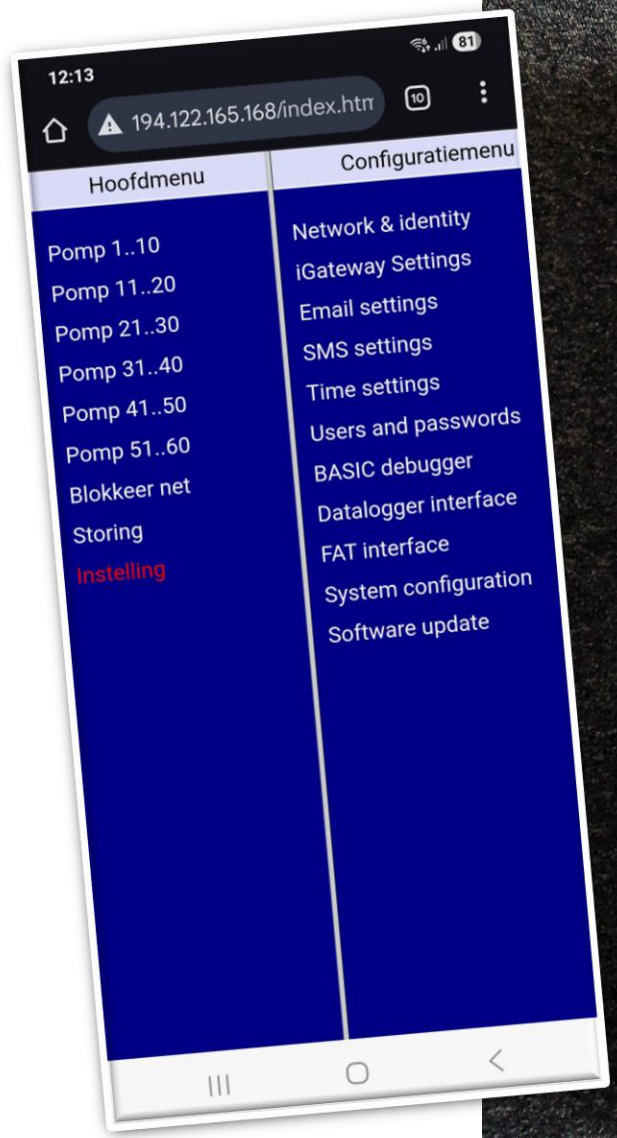


# Zijn alle lekken gedicht na 2012?

your partner

**Vrijdag 23 januari 2026**

Direct via smartphone
toegang tot een gemaal…



# Het kan dus nog steeds
# … en nu ?!

your partner

# NIS2 Inventarisatie

**Vandaag nog starten met OT/IT inventarisatie**

- Risico-inventarisatie van ALLE objecten
- Vastlegging PLC-type, firmware, wachtwoorden, e.d.
- Opslag van PLC-broncodes (waar beschikbaar)
- NIS2 en CRA-compliance op alle onderdelen
- Betrek uw leveranciers in de inventarisatie
- Pentest\audit van uw (web)hoofdpost

- Haal de stekker uit wat niet veilig is!

your partner

# NIS2 Inventarisatie

Onderdelen die u minimaal in beeld moet hebben:

- Fysieke besturingskast
  - Sleutelbeheer
- Besturingscomputer (PLC)
  - Vrije poorten
- Modem/Router
- SIM kaart of eSIM
- Provider of Providers
- VPN / APN op connectivity
- Beveiliging en beheer van de hoofdpost
- Toegang gebruikers tot systemen

# NIS2 Inventarisatie

Belangrijk om in het achterhoofd te houden:

“Geen geld” en vooral “geen tijd voor” zijn de tegenargumenten om de kwetsbaarheden aan te pakken. Maar zeker ook gebrek aan kennis om de risico’s van kwetsbaarheden afdoende te kunnen inschatten. Een rioolbeheerder heeft namelijk geen IT of OT achtergrond, zorg voor voldoende vakkundige ondersteuning op dat vlak.

# Dank voor uw aandacht

Theun Prins

06 - 53 24 59 73

t.prins@yourpartner.nl

www.yourpartner.nl | www.cyberborg.eu