



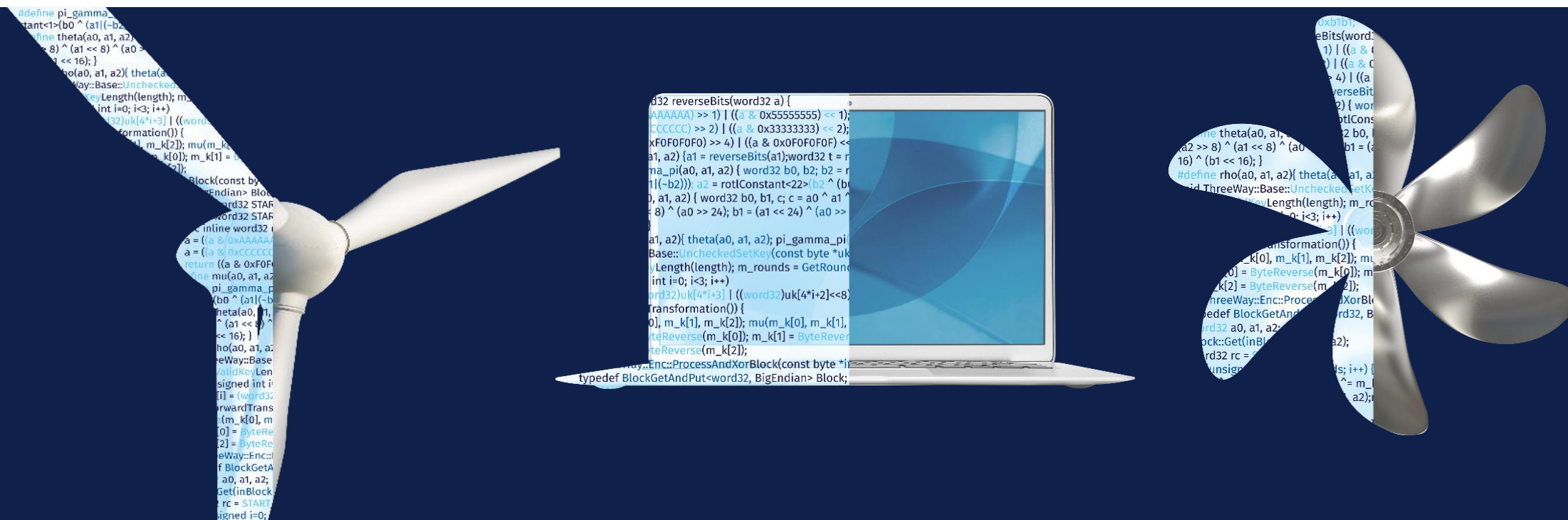
WHEN TRUST MATTERS

EU:NIS2 wat betekent dat voor jou?

DNV Cyber

Mark Bakker, Sales Director, Applied Risk

2 October 2024



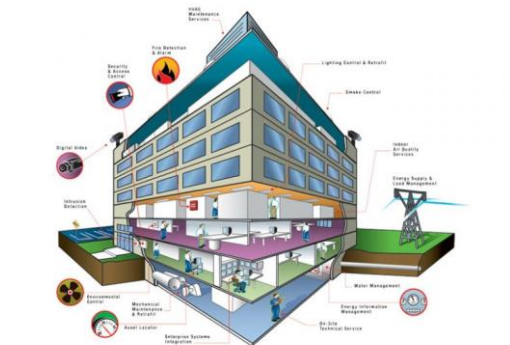
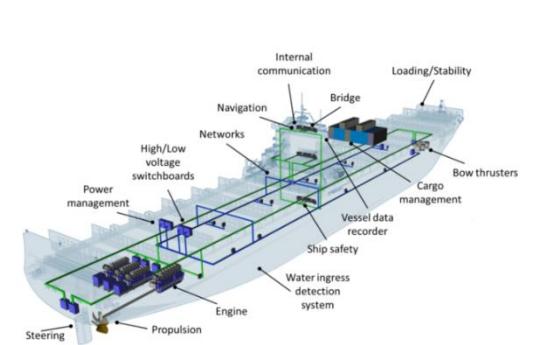
Wat is OT vs IT?

Information Technology (IT): computer systemen, software, programmeertalen en data/informatie verwerking en -opslag

Operational Technology (OT): hardware en software dat een verandering detecteert of veroorzaakt, door middel van het direct monitoren en/of besturen van industriële systemen, "assets", processen en "events"



Eigenschap	IT	OT
Vertrouwelijkheid	Hoog	Laag
Integriteit	Medium	Erg hoog
Beschikbaarheid	Laag-Medium	Erg hoog
Authenticatie	Wijdverspreid	Niet gebruikelijk
Tijd kriticaliteit	Vertragingen getolereerd	Kritisch
Systeem "Downtime"	Getolereerd	Niet acceptabel
Systeem Levensduur	3-5 jaar	15-25 jaar
Software Changes	Frequent	Zelden
Worst Case Impact	Verlies van data	Productieverlies, fysieke schade aan systemen, letsel
Standaarden	ISO-27001	IEC-62443
Wetgeving	GDPR	EU:NIS(2), CRA, IMO UR26/UR27



Waarom is OT Cyber security belangrijk?

Operational Technology (OT) wordt overal gebruikt

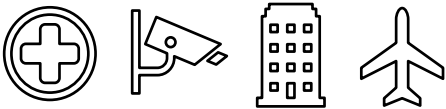


1. Introduction

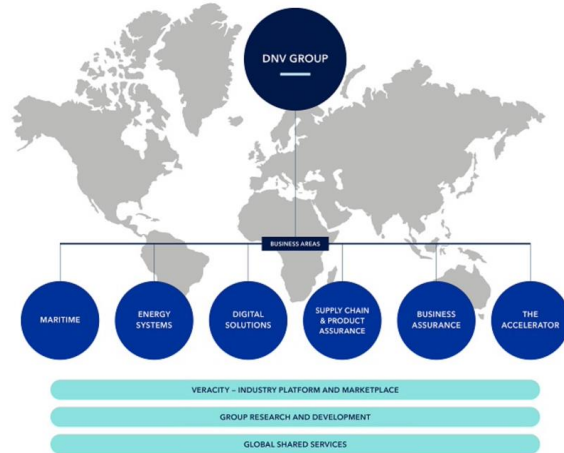
1a. DNV Cyber

Purpose

Safeguarding life, property, and the environment.

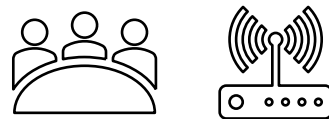
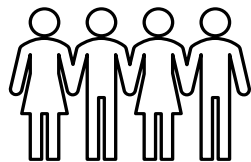


Global



Approx.

500
Cybersecurity
Specialists



100% IT & OT
cybersecurity services for
business resilience.

DNV Group (2023)

- ✓ **Customers:** > 100,000
- ✓ **Employees:** > 15,000
- ✓ **Employees with Higher Education:** 89%
- ✓ **Nationalities:** 122
- ✓ **Sustainability:** Top 1% of companies assessed by EcoVadis
- ✓ **Revenue:** NOK 31 Bio (approx. **USD 3 Bio**)
- ✓ **Remi Eriksen** - Group President and CEO DNV
- ✓ **Global:** based in more than 100 countries
- ✓ **About us:** Since 1864, our Purpose has been to safeguard life, property, and the environment. Our Vision is to be a trusted voice to tackle global transformations
- ✓ **Growth:** DNV recorded year-on-year growth of 26.2%
- ✓ **EBITDA:** NOK 5.4 Bio
- ✓ **Equity Ratio:** 57.7%

Wij beveiligen IT & OT omgevingen in vele sectoren

-  Agriculture
-  Construction services
-  Defence and national security
-  Energy
-  Manufacturing
-  Maritime
-  Media & Telecom
-  Pharmaceuticals

-  Forest, pulp and paper
-  Governmental and public sectors
-  Health
-  ICT, technology and automation
-  Process industry
-  Retail
-  Transportation
-  Finance

DNV Cyber omzet per Market & Industry Sector

Market & Industry Sector	Omzet p/jr MEUR
Energy	15-18
ICT, technology and automation	14-16
Government and Defence	10-12
Industrial products and construction	8-10
Financial	6-8
Maritime	2-3
Other	15-17

2. EU:NIS2



EU:NIS2 - Doel

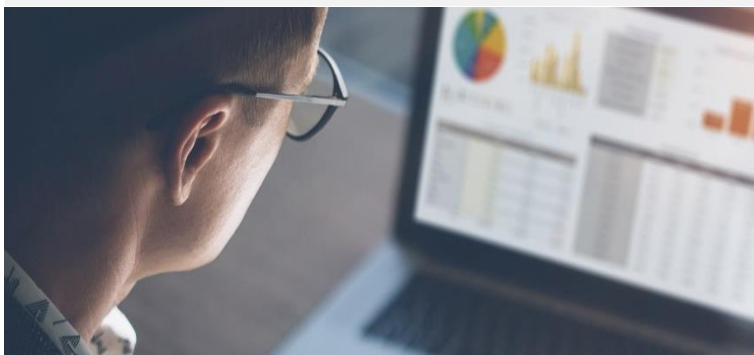
Creëer een algemeen
cyber security niveau
onder de lidstaten

Introductie - NIS 2 regelgeving



Waarom

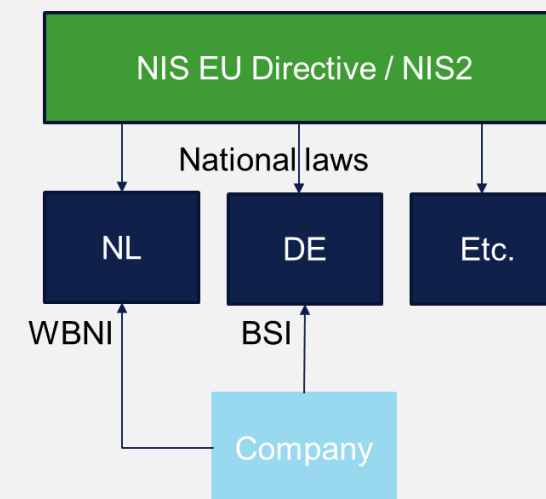
- Zorg voor cyber weerstand voor kritieke infrastructuur, essentiële diensten en hun supply chain (lever keten)
- Zorg voor faire competitie via het eisen van een algemeen cyber security niveau in de EU
- Minimaliseer de impact van incidenten
- Deel informatie aan nationale overheden om verdere escalatie te voorkomen



Wie



- Minimale drempel van 250 medewerkers of 43 mln EUR omzet



Sectors of High Criticality

- Proactief toezicht
- Hogere boetes mogelijk (> 2% van totale wereldwijde jaaromzet of €10 mln)
- Certificaties kunnen vereist worden
- Ad hoc audit rechten
- Persoonlijke aansprakelijkheid voor verantwoordelijke natuurlijke personen (MT, directie)

Other Critical Sectors

- Reactief toezicht
- Boetes zijn lager (>1,4% van totale wereldwijde jaaromzet of €7 mln)
- Certificaties mogelijk, maar niet vereist
- Verplichting om informatie te verstrekken na audit

Op weg naar NIS2

Legend

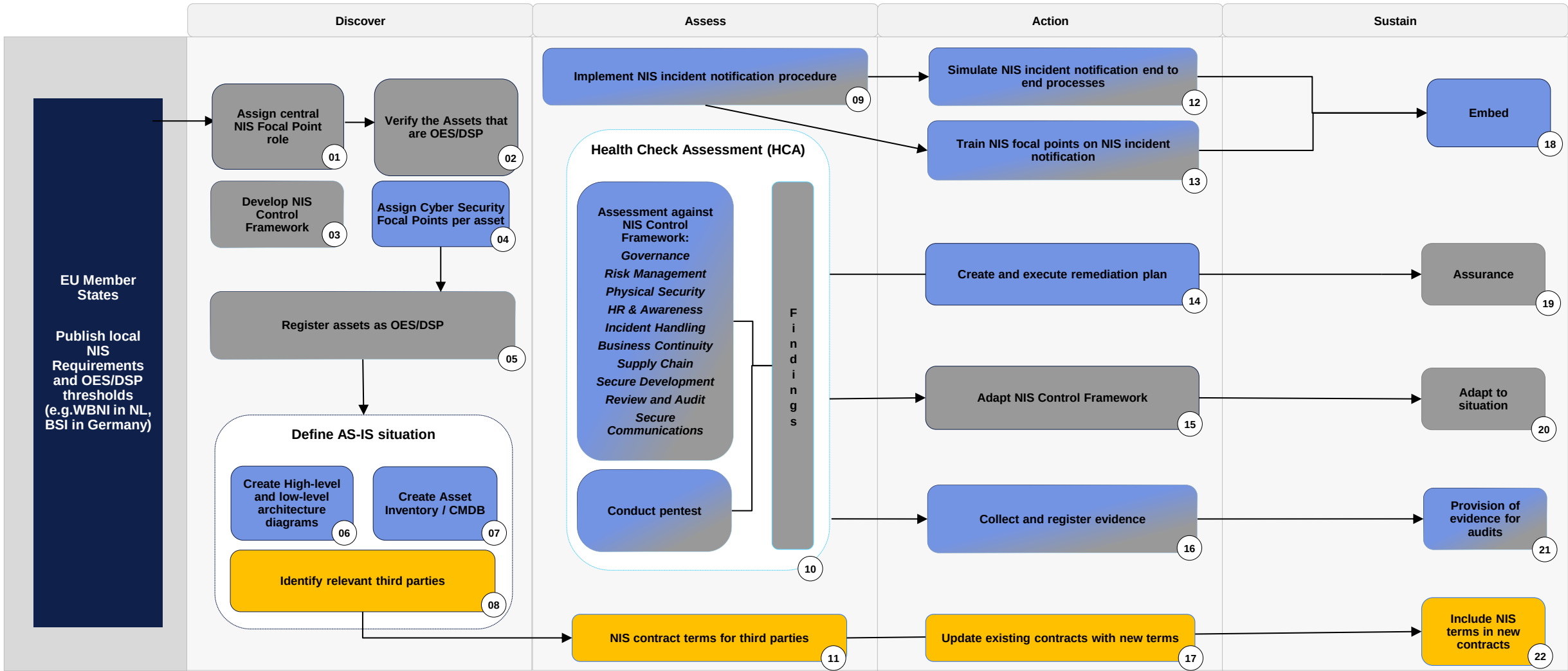
Regulator/Competent Authority

Asset NIS activity

Central Company NIS activity

Compliance & Procurement

Activity number



Wat nu?



Stop de paniek!

Begrijp de scope van NIS2

Belangrijk versus essentieel.
Identificeer uw assets.

Meet de onbekenden

Maturity assessment omtrent
het huidige framework.
Gebruik framework voor IT/OT
cybersecurity (bijv. ISO 27001,
NIST, IEC 62443).

Ontwikkel een stappenplan voor NIS2-naleving

Risicogebaseerde aanpak.
Prioritering van taken en
maatregelen mogelijk maken.
Opstellen van een business
case.
Tijdige naleving.

3. Voorbeelden



Energiebedrijf (NL)

Uitdaging: Energiebedrijf is onderdeel van de High Critical Sector (EU:NIS2)

Nodig: Cyber Security Management System (EU:NIS2 requirement)

Oplossing: Hulp bij het implementeren van een CSMS

- Ontdek
- Beoordeel
- Actie
- Onderhoud: OT Monitoring, IR Plan, IRF Expertise

Startpunt: Begin met een ISMS, zelfs met een klein budget:

- Statement of Applicability
- Als je al ISO-27001 hebt, wat kan je her-gebruiken?
- Verwijs naar internationale Cyber Security standaard bij aankopen
- Netwerk architectuur / Segmentatie: IEC-62443 (purdue)
- IRP en borg inhuren van expertise

Airport Automation System Integrator

Uitdaging: Luchthavens zijn onderdeel van High Critical Sector (EU:NIS2).

Luchthavens vereisen dus Cyber Secure by Design systemen

Nodig: Lever cyber secure baggage systemen

Oplossing: IEC-62443 ondersteuning bij:

- -3-1: Security Technologies for IACS
- -3-2: Security Risk Assessment and System Design
- -3-3: System Security Requirements and Security Levels
- -2-4: Security Program Requirements for IACS Service Providers;

Startpunt: Zorg dat je Cyber Secure by Design componenten gebruikt

- -4-2: Technical Security Requirements voor IACS componenten → in lijst met eisen opnemen
- -2-4: Zorg dat jouw systemen ook up-to-date blijven
- Zorg wel dat de updates 1e getest worden
- Remote Access – doe dat veilig en registreer wie, wanneer, welke toegang heeft (PAM)
- IRP en borg inhuren van expertise





Packaging OEM

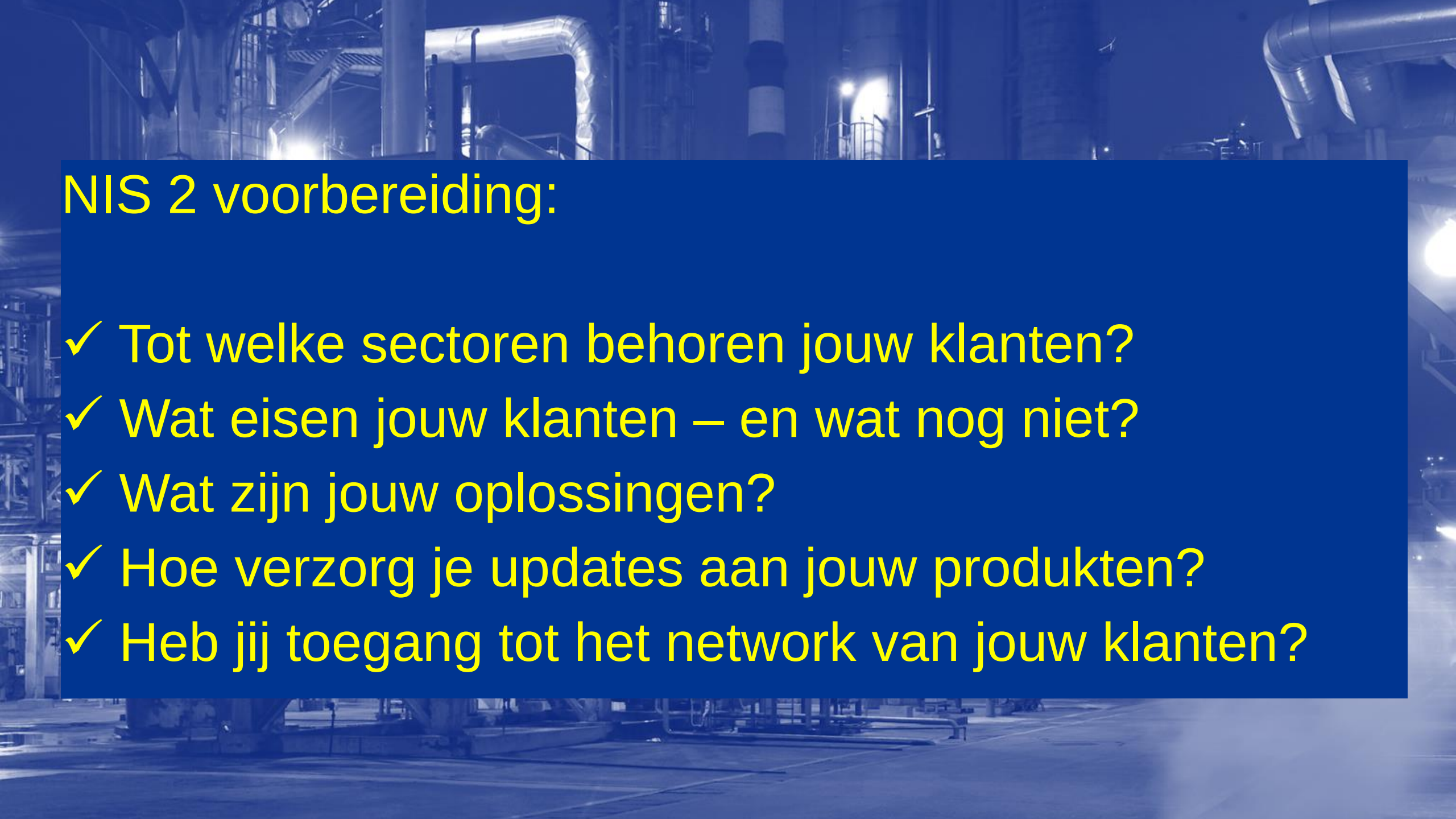
Uitdaging: Verpakkingsmachinefabriek in NL levert aan farma-klienten die onderdeel zijn van andere Kritieke Sectoren (EU:NIS2)

Nodig: Lever een cyber secure verpakkingsmachine (OEM is onderdeel van de toeleveringsketen voor de farma klant).

Oplossing: IEC-62443 certificatie ondersteuning:

- -3-3: System Security Requirements and Security Levels
- -4-2: Technical Requirements for IACS Components;

Startpunt: Onze OT Cyber Security Experts hielpen de klanten snel op weg Cyber Secure te ontwerpen en ontwikkelen op basis van IEC-62443

The background of the slide is a blue-tinted photograph of an industrial facility. It features a complex network of large, metallic pipes, some of which are insulated with reflective material. In the distance, several tall smokestacks or chimneys are visible against a dark sky. The overall scene suggests a manufacturing or processing plant.

NIS 2 voorbereiding:

- ✓ Tot welke sectoren behoren jouw klanten?
- ✓ Wat eisen jouw klanten – en wat nog niet?
- ✓ Wat zijn jouw oplossingen?
- ✓ Hoe verzorg je updates aan jouw producten?
- ✓ Heb jij toegang tot het network van jouw klanten?



Basis hygiëne:

- 1. Secure Network Architectuur (Purdue Model)**
- 2. Secure (Remote) Access**
- 3. Secure Componenten / Systemen / Installaties**
- 4. Incident Response Plan & Expertise**
- 5. Beleid & Procedures**

Relax, je kan mij contacteren!

Mark.Bakker@dnv.com