Rijksinspectie Digitale Infrastructuur
*Ministerie van Economische Zaken*

# Samenwerken aan digitale weerbaarheid

NIS2 en andere relevante wet- en regelgeving

DCC kennislunch IT-dienstverleners

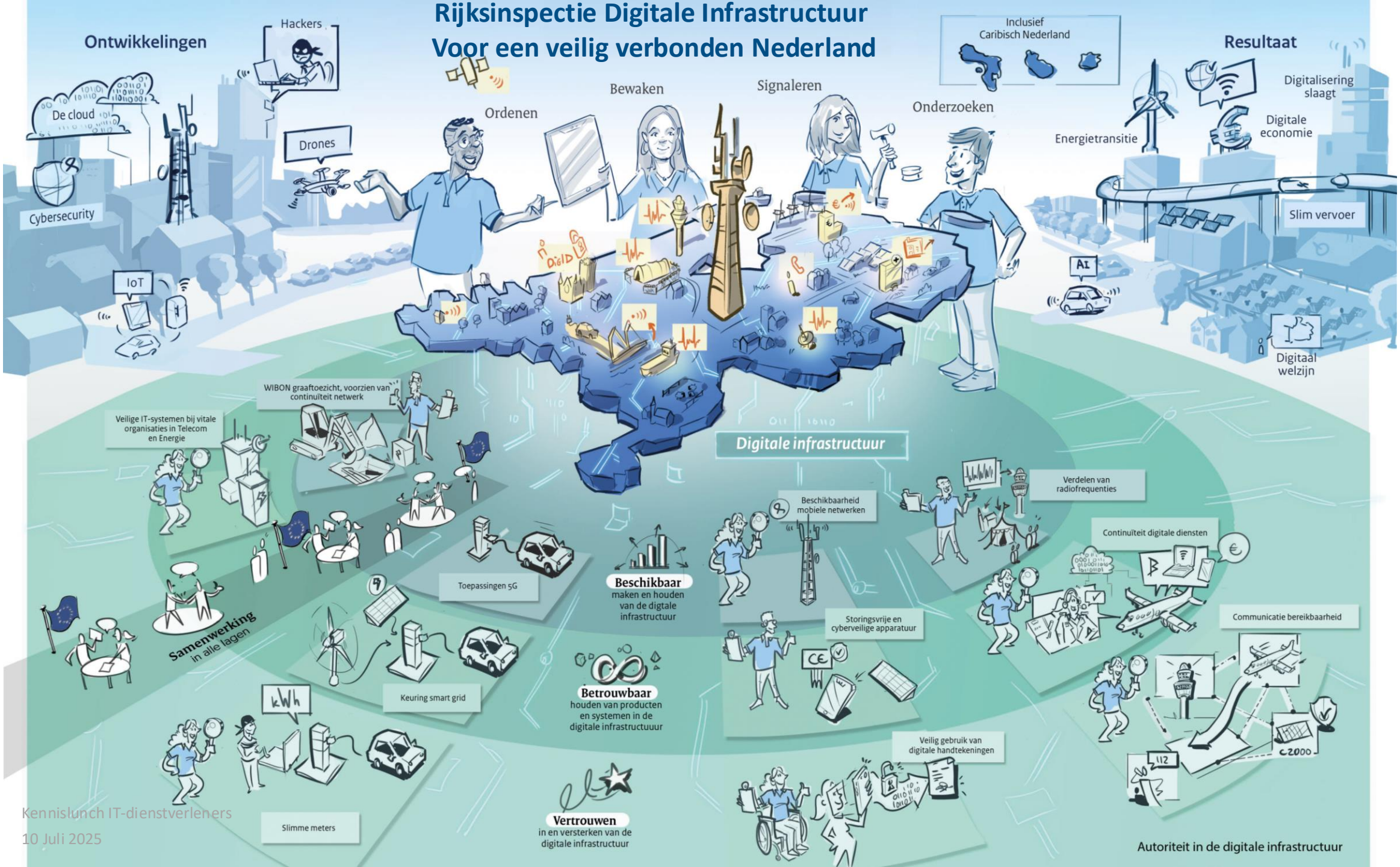
10 juli 2025


# Agenda

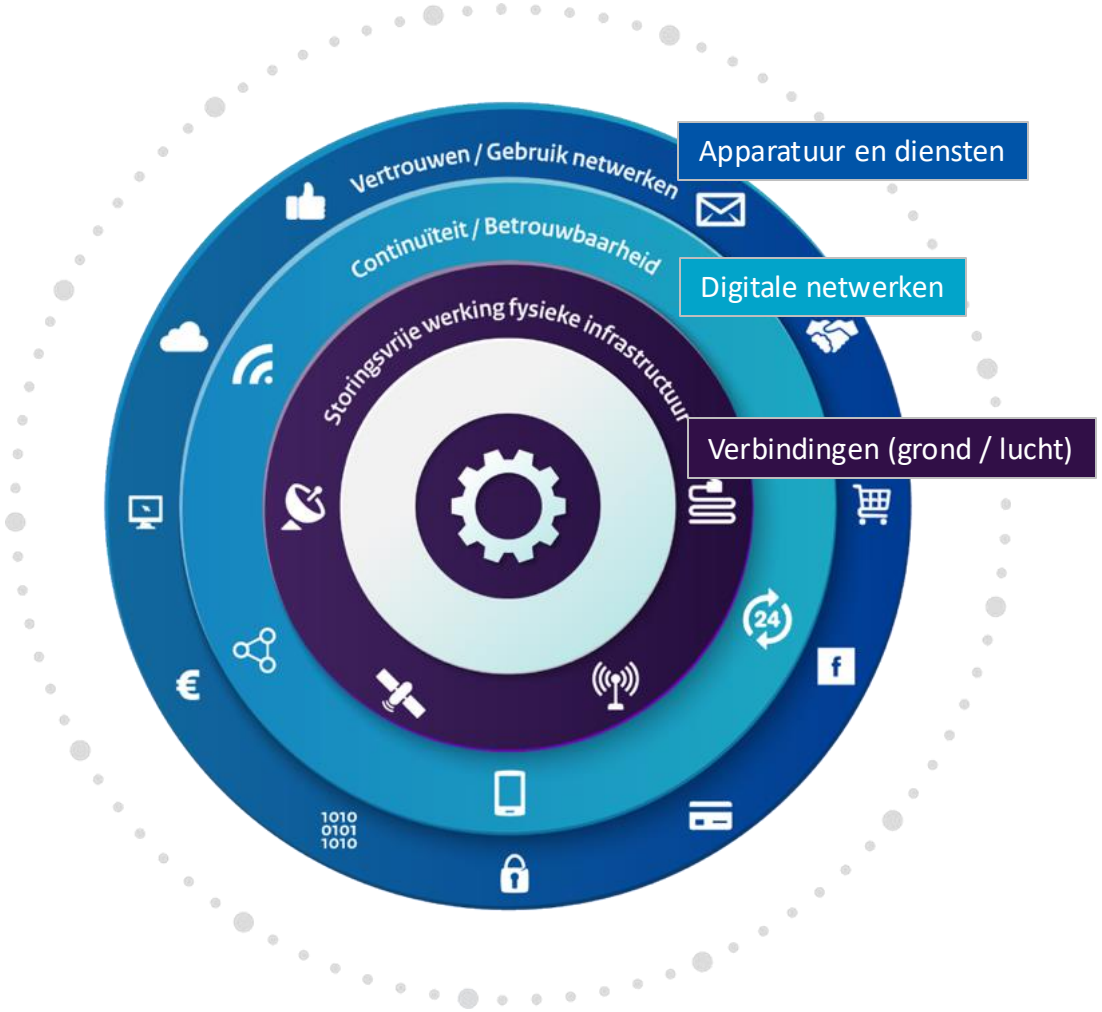
1. Wie is de RDI?
2. Wat is digitale weerbaarheid en waarom is het belangrijk?
3. Wet en regelgeving – CSA
4. Wet en regelgeving – NIS2/Cbw
5. Wat kunt u van de RDI verwachten?
6. Waar kunt u nu al mee aan de slag?

# 1. Wie is de RDI?

# Rijksinspectie Digitale Infrastructuur
## Voor een veilig verbonden Nederland



# De RDI staat voor de beschikbaarheid en betrouwbaarheid van telecommunicatie- en IT-netwerken



# 2. Wat is digitale weerbaarheid en waarom is het belangrijk?

**Digitale weerbaarheid =**

- bedreigingen kunnen weerstaan
- snel kunnen herstellen na verstoring of cyberaanval

Voorbeelden

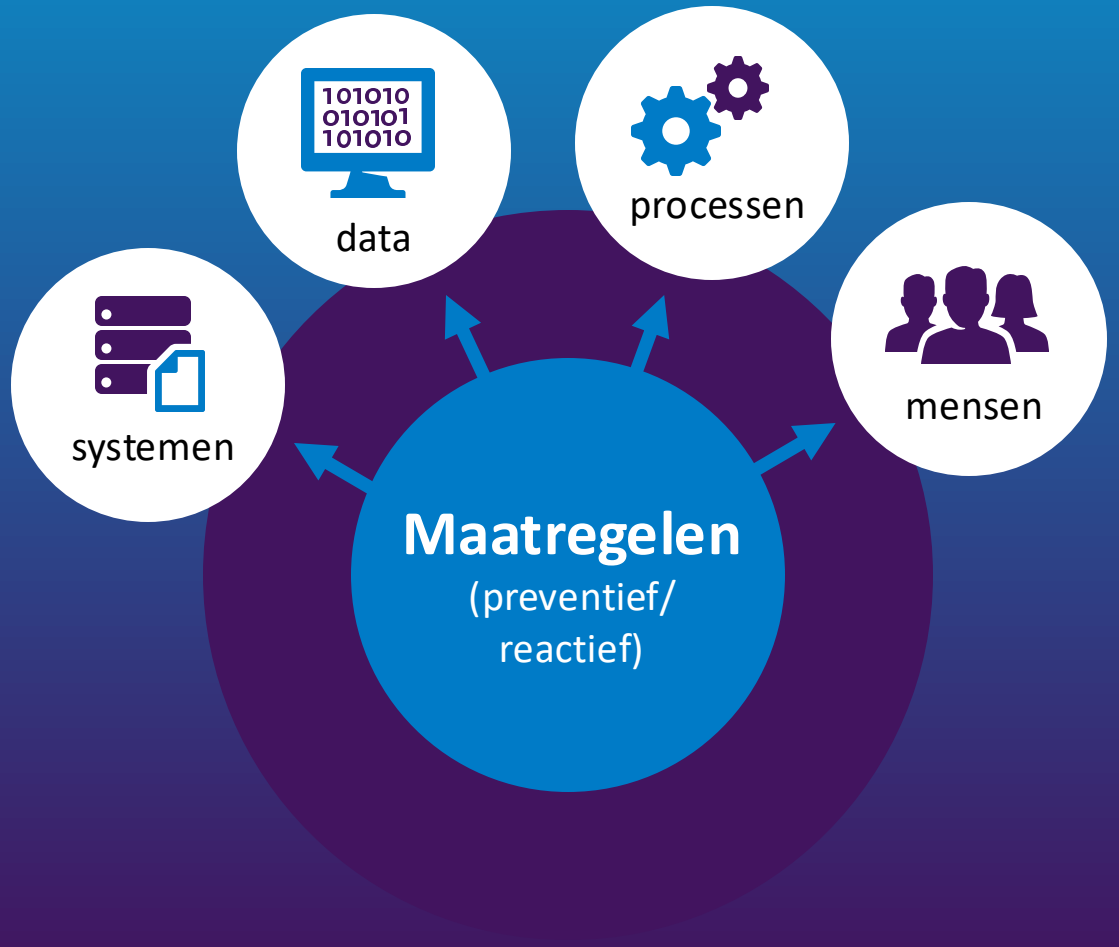
Dienstverlener die te maken krijgt met **gijzelsoftware**


**Internetstoring** bij een fabriek

Energiebedrijf dat wordt **gehackt**

**Digitale weerbaarheid:**

- vraagt om preventieve en reactieve maatregelen en voortdurend verbeteren
- verdient strategische aandacht binnen organisaties
- is cruciaal voor het vertrouwen van onze samenleving in digitalisering

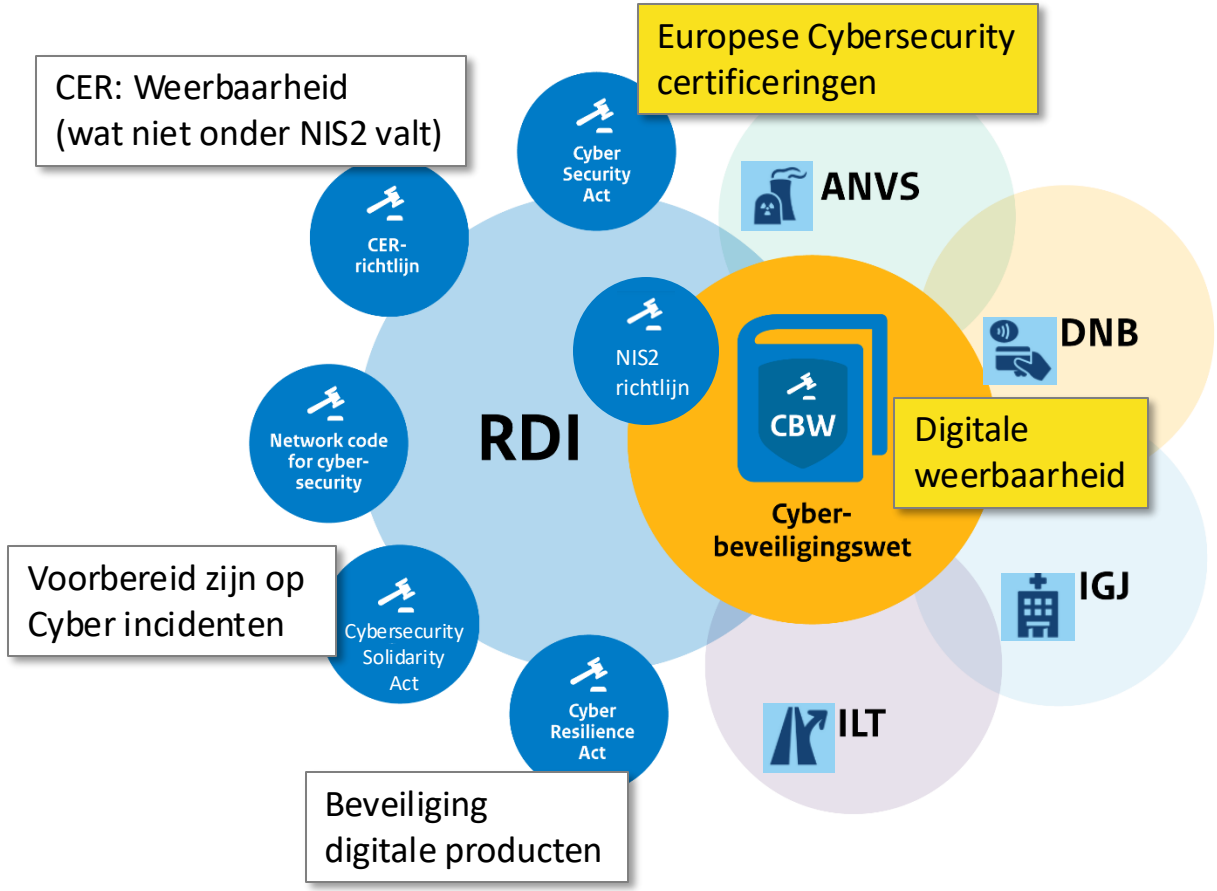


# De 5 basisprincipes van veilig digitaal ondernemen

- Breng risico’s in kaart
- Bevorder veilig gedrag
- Bescherm systemen, apparaten en applicaties
- Beheer toegang
- Bereid voor op incidenten

# Wetgeving rondom digitale weerbaarheid

- Verschillende EU wetten rond Digitale Weerbaarheid raken steeds meer vervlochten
- Meerdere toezichthouders, met verschillende opdrachten en focus op sectoren



# 3. Wet en regelgeving CSA

Kennislunch IT-dienstverleners

10 Juli 2025

# Cyber Security Act geïntroduceerd in 2019, de EU heeft hiermee twee centrale doelen:


1. Europees **certificeringstelsel** voor producten, diensten, en processen op het gebied van Cybersecurity

2. **Vereenvoudiging** door vervangen nationale Cybersecurity certificeringen door EU certificering

# Certificeringsschema’s


- ENISA ontwikkelt de verschillende certificeringsregelingen, dit zijn **certificeringsschema’s**
- Certificering kan worden **voorgeschreven** door nationale of Europese regelgeving
- Drie **CSA zekerheidsniveaus** waarop gecertificeerd kan worden; basis, substantieel en hoog

# NCCA

- Certificerende instellingen (CBI) voeren de certificeringen uit en reiken Europese certificaten uit
- RDI is de Nationale Cybersecurity Certificeringsautoriteit (NCCA) voor Nederland die toezicht houdt op de naleving van certificeringsvoorwaarden door de certificerende instellingen
- RDI geeft als NCCA voorafgaande goedkeuring aan de uitreiking van een certificaat door een certificerende instelling



## Overzicht EU certificeringsschema's

- EUCC certificering van producten
  - Gerelateerd aan CRA
  - Gereed sinds februari 2024
- EUCS certificering clouddiensten
  - Gerelateerd aan NIS2 en CRA
  - In eindfase
- EUMSS certificering managed security services
  - Gerelateerd aan Cybersecurity Solidarity Act
  - In ontwikkeling

# Certificering Managed Security Services

- ENISA start een ad-hoc werkgroep voor het opstellen van een EUMSS certificeringsregeling
- Experts met kennis en ervaring van cybersecuritycertificering worden uitgenodigd voor deelname aan deze werkgroep
- Sluitingstermijn: 20 juli 2025 !


**Rob Augustinus** • You
IT-Security Expert/Auditor at Dutch Authority for Digital Infrastructure - Co-ch...
1w •

Belangrijk voor #MSSP's in Nederland! #ENISA start een werkgroep voor een Europese certificering voor Managed Security Services. Ook NL experts op het gebied van #cybersecurity #certificering kunnen hieraan deelnemen!

https://www.enisa.europa.eu/news/eu-managed-security-services-certification-to-drive-the-cybersecurity-market

# 4. Wet en regelgeving NIS2 / Cbw

Kennislunch IT-dienstverleners

10 Juli 2025

# Met de nieuwe Europese richtlijn NIS2 heeft de EU twee centrale doelen:


1. Verbeteren van **digitale weerbaarheid** van essentiële dienstverlening

2. Versterken van de **samenwerking** tussen EU-lidstaten (sterkere EU markt en gelijk EU speelveld)

# Cyberbeveiligingswet


- **Implementatiewet** van Europese NIS2-richtlijn in Nederland
- Opvolger **Wbni** (Wet beveiliging netwerk- en informatiesystemen)
- Inwerkingtreding verwacht in tweede kwartaal van **2026**

# Cbw geldt voor alle sectoren

- Maar… voor entiteiten met een grensoverschrijdende karakter is ook een NIS2 Europese uitvoeringsverordening van toepassing:

- Voor die entiteiten geldt:
  - Dezelfde maatregelen en meldcriteria in alle EU lidstaten
  - One-jurisdictie principe (dezelfde toezichthouder in alle EU lidstaten)

## NIS2 uitvoeringsverordening 2024/2690

Wordt in Nederland van kracht samen met het in werking treden van de Cbw

## “Cross-border” entiteiten in scope:

- ✓ DNS service providers
- ✓ TLD name registries
- ✓ Cloud computing service providers
- ✓ Data center service providers
- ✓ Content delivery network (CDN) providers
- ✓ Managed service providers (MSP’s)
- ✓ Managed security service providers (MSSP’s)
- ✓ Online marketplaces
- ✓ Online search engines
- ✓ Social networking services platforms
- ✓ Trust service providers (TSP’s)

# 3. Wat betekent de cyberbeveiligingswet voor IT-dienstverleners?

# Wat zijn de belangrijkste verplichtingen?

**Zorgplicht**: uitvoering van passende technische en organisatorische maatregelen

**Meldplicht**: melding van significante ICT-incidenten bij CSIRT en toezichthouder

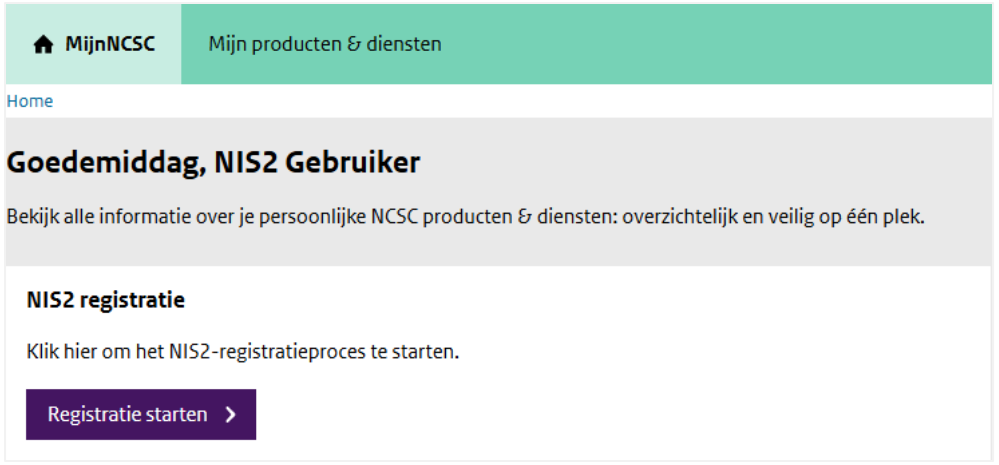
**Registratieplicht**: registratie in een entiteitenregister

**Bestuur:** Moet de maatregelen goedkeuren en toezicht houden op de uitvoering, zij dienen daarvoor over de nodige kennis te beschikken

# Registratieplicht

Voor organisaties die onder de NIS2/Cbw vallen geldt een wettelijke verplichting om zich te registreren* in het NCSC entiteitenregister.

https://mijn.ncsc.nl/




* eHerkenning EH2+

# Hoe weet ik als M(S)SP of ik onder de NIS2/Cbw val?

**Doe de check op:**

https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

Welk soort entiteit voor de sector Beheer van ICT-diensten (business-to-business) is van toepassing?

**Voldoe ik aan de definitie van een M(S)SP?**

- [x] Aanbieders van beheerde diensten
- [x] Aanbieders van beheerde beveiligingsdiensten

Bepaling hoofdvestiging: Is de Hoofdvestiging binnen de Unie en worden beslissingen met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's hoofdzakelijk in de Unie genomen?

**Val ik onder de jurisdictie van Nederland?**

- (•) ja
- ( ) nee

Hoeveel medewerkers zijn werkzaam in de gehele organisatie?

- ( ) 1 - 49
- (•) 50 - 249
- ( ) ≥ 250

**Grootte van je organisatie bepaalt of:**

- ➢ Je er wel of niet onder valt
- ➢ Je belangrijk of essentieel bent

Hoe hoog was de jaaromzet van het laatst gesloten boekjaar van de onderneming?

- ( ) < 10 miljoen euro
- (•) 10 - < 50 miljoen euro
- ( ) ≥ 50 miljoen euro

Wat was de balans van laatst afgesloten boekjaar van de onderneming?

- ( ) < 10 miljoen euro
- (•) 10 - < 43 miljoen euro
- ( ) ≥ 43 miljoen euro

Is er in Nederland een bekende uitsluiting (bv nationale veiligheid) voor de organisatie?

- ( ) ja
- (•) nee

**Is er een uitsluiting voor mij van toepassing?**

Is er sectorspecifieke cyberwetgeving (een Lex Specialis) van toepassing voor de organisatie?

- ( ) ja
- (•) nee

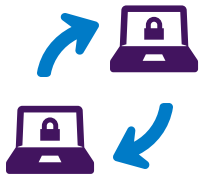
Is de organisatie gemarkeerd/aangewezen als essentiële entiteit (bv onder NIS1/Wbni/Bbni)?

- (•) ja
- ( ) nee

**Sta ik al onder toezicht voor de NIS2/Wbni?**

# Zorgplicht

## Voorbeeld van maatregelen



Beveiliging van de **toeleveranciers-keten**

## Maatregelen in Annex Uitvoeringsverordening 2024/2690

https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

**5. Supply chain security (Article 21(2), point (d), of Directive (EU) 2022/2555)**

5.1. Supply chain security policy

5.1.1. For the purpose of Article 21(2), point (d) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.

5.1.2. As part of the supply chain security policy referred to in point 5.1.1, the relevant entities shall ….

# Zorgplicht

ENISA guidance voor entiteiten hoe maatregelen te implementeren



## NIS2 Technical Implementation Guidance

Guidance voor het implementeren van de maatregelen in verordening 2024/2690:


https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

# Meldplicht

Voorbeeld van meldplicht voor IT-dienstverleners (MSP’s en MSSP’s)



## Meldcriteria in Uitvoeringsverordening 2024/2690

https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

**Article 10 - Significant incidents with regard to managed service providers and managed security service providers**

With regard to managed service providers and managed security service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a managed service or managed security service is completely unavailable for more than 30 minutes;

(b) the availability of a managed service or managed security service is limited for more than 5 % of the service’s users in the Union, or for more than 1 million of the service’s users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a managed service or managed security service is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a managed service or a managed security service, is compromised with an impact on more than 5 % of that managed service’s or that managed security service’s users in the Union, or on more than 1 million of the service users in the Union, whichever number is smaller.

# Bestuur

## Voorbeelden besturende maatregelen

Bestuurders moeten de **Cybersecurityrisico's** van hun organisatie weten

**Kennis en vaardigheden** zodat bestuurder en CISO dezelfde taal spreken

**CISO uitnodigen** in het bestuurs-overleg

# 5. Wat kunt u van de RDI verwachten?

# De organisatie is zelf verantwoordelijk voor de invulling van maatregelen

Toezichthouders bepalen:

- **op welke manier** ze toezicht bij organisaties houden;
- **of passend invulling is gegeven** aan de verplichtingen uit de wet;
- **welke interventies** ze inzetten.

# Bij ons toezicht op digitale weerbaarheid werken we vanuit duidelijke uitgangspunten

- We zetten het publieke belang centraal
- We hebben een brede, onafhankelijke blik op het digitale stelsel
- We zijn reflectief en risicogericht en zien sancties als ultieme middel.
- We werken samen met markt- en andere overheidspartijen

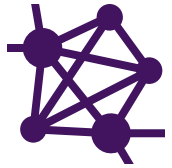
# Hoe doen we dat?

We gebruiken **openbare bronnen** en **data-analyses**

Toezichthouders voeren **gezamenlijke inspecties uit**

Overheidspartijen ontwikkelen samen **tools**

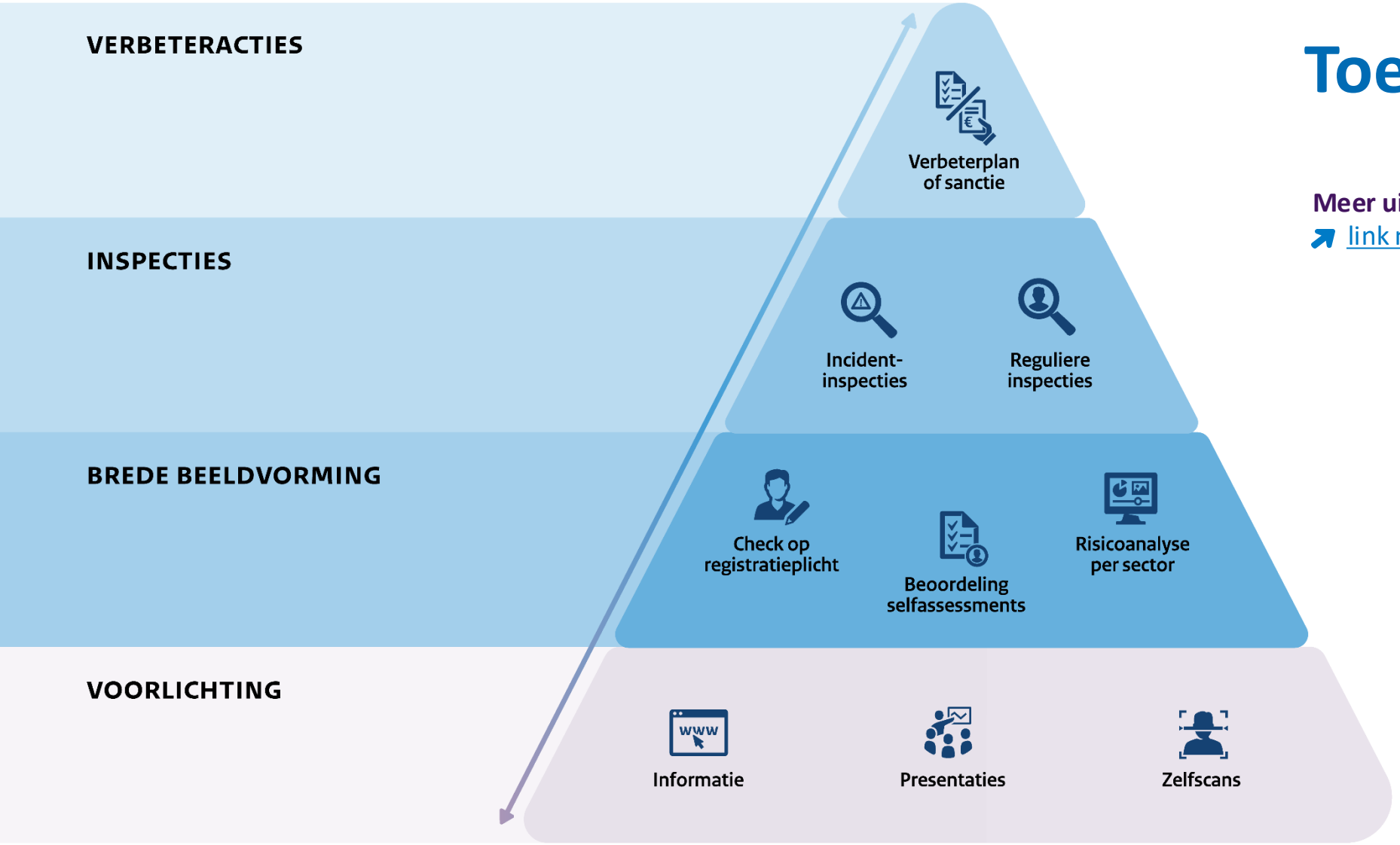
We geven **uitleg over toezicht** en delen **goede voorbeelden**



We halen **informatiebehoeften** op bij branche-organisaties

We **delen onze bevindingen** met beleidmakers

# Toezichtsmodel




**Meer uitleg op de website van de RDI**

link naar gehele infographic

# Hoe kunnen IT-dienstverleners bijdragen aan de digitale weerbaarheid?

**Unieke positie IT-dienstverleners**: Spilfunctie voor het verhogen van digitale weerbaarheid door klanten te helpen met voldoen aan de NIS2/Cbw

**Val je onder de NIS2/Cbw**: Met jouw kennis kan je klanten helpen om aan de NIS2/Cbw te voldoen

**Val je niet onder de NIS2/Cbw:** Je kan niet onder de NIS2/Cbw komen te vallen door jouw klanten die eronder vallen, maar deze verwachten misschien wel dat je kennis ervan hebt

# 6. Waar kan je nu al mee aan de slag?

# Wacht niet af, maar ga nu alvast aan de slag met digitale weerbaarheid

1. Inschatten of je onder de richtlijn valt met de **NIS2-Zelfvaluatie**
   regelhulpenvoorbedrijven.nl/NIS-2-NL

2. Ontdekken waar je organisatie staat met de **NIS2-Quickscan**
   regelhulpenvoorbedrijven.nl/NIS2-Quickscan

3. (Vrijwillig) **Registreren**
   https://mijn.ncsc.nl/

4. Kijk wat je moet doen als je valt onder de **uitvoeringsverordening**
   www.enisa.europa.eu/news/supporting-nis2-implementation-through-actionable-guidance

# Vragen?