# EEN IMPULS VOOR...

Impuls Zeeland

**Cyber veiligheid**

# Webinar NIS2 / Cyberbeveiligingswet

## Doel webinar:

- Inzicht geven in NIS2
- Waarom, wat, voor wie...
- Praktische handvatten
- Praktische ondersteuning

Impuls Zeeland

KIC MPi
Kennis- en innovatiecentrum
Maintenance Procesindustrie

ZEELAND CONNECT
VERSTERKT LOGISTIEK IN ZEELAND

FOODDELTA ZEELAND

KLIKOPMORGEN.nl
EDIH Zuid-Nederland

Provincie Zeeland

Rijksinspectie Digitale Infrastructuur
*Ministerie van Economische Zaken en Klimaat*

PVO

avans hogeschool

***Rutger van der Male**, 0639398464, rutgervandermale@impulszeeland.nl*

# Agenda

1. *Introductie over de noodzaak en urgentie van cyberveiligheid in bedrijven en ketens.*
   - *Roel de Beer (Avans Hogeschool)*

2. *Waarom is cyberbeveiligingswet ingevoerd, welke organisaties vallen eronder, welke verplichtingen zijn er, hoe ziet toezicht er uit, …*
   - *Stan van Bommel (Rijksdienst voor Digitale Infrastructuur, RDI)*

3. Praktische invulling van de wetgeving, concrete handvatten.
   - *Ben Stofbergen en Jorrit de Boer (Platform Verantwoord Ondernemen, PVO)*

4. Q&A, praktische ondersteuning vanuit Avans, RDI, PVO, Impuls.

# Wat doen we nog meer?

18 september: **Fabriek van de Toekomst Tour**: Alternate en MDE Automation.
https://www.impulszeeland.nl/agenda/fabriek-van-de-toekomst-editie-1

24 september: **Bijeenkomst Talentontwikkeling & AI op de werkvloer.**
https://www.impulszeeland.nl/agenda/ai-op-de-werkvloer-wat-vraagt-een-leven-lang-ontwikkelen

4 november: **The State of Humanoids conferentie.**
https://www.impulszeeland.nl/agenda/the-rise-of-the-humanoids-conferentie

1 december: **AI-Conferentie rond veilig en verantwoord AI-gebruik.**
https://www.impulszeeland.nl/agenda/ai-conferentie

10 december: **Business Bootcamp rond cyberveiligheid en AI.**

# Praktische zaken

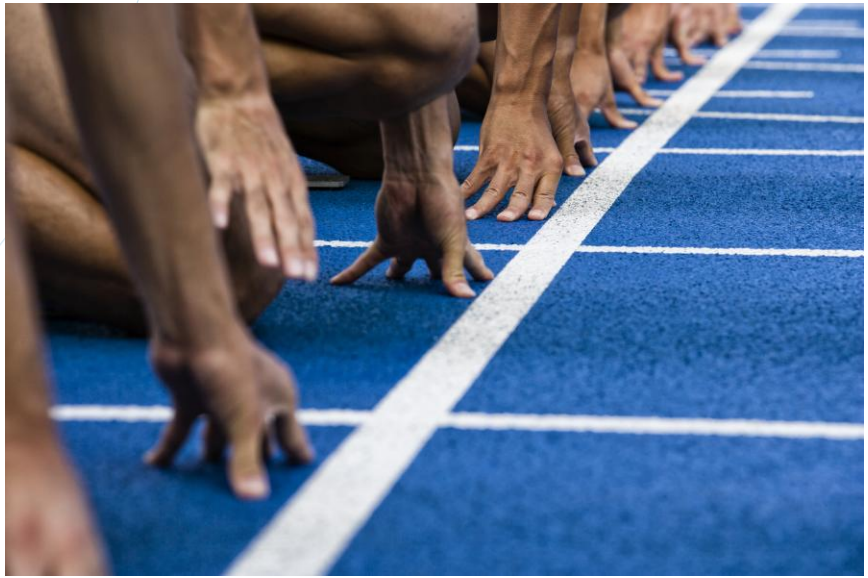
1. *Tijdens presentaties graag microfoons uit.*
2. *Presentatie wordt opgenomen. Heeft iemand hier bezwaar tegen?*
3. *Na elke presentatie is er gelegenheid om vragen te stellen.*
4. *Vragen kunnen ook via de chat gesteld worden.*
5. *We sluiten af met een Q&A.*
6. *Presentaties en contactgegevens worden na afloop naar u gemaild.*
7. *We zijn benieuwd naar uw mening! Enquête in zelfde email.*

Introductie over de noodzaak en urgentie van cyberveiligheid in bedrijven en ketens.

***Roel de Beer (Avans)***

Webinar NIS2
10 september 2026

# NIS2 als startpunt voor cyberweerbaarheid



Roel de Beer
*Docent-onderzoeker Lectoraat Cyberweerbare Organisaties*
*Centre of Expertise Veiligheid & Veerkracht, Avans Hogeschool*

avans hogeschool

Centre of Expertise
Veiligheid & Veerkracht
Een initiatief van avans

# MKB is geen eiland

In een keten verspreidt verstoring zich vaak sneller dan verantwoordelijkheid.

‘Ben ik interessant

van wie ben ik afhankelijk? En wie is van mij afhankelijk?

Klanten | Leveranciers | ICT-dienstverleners | Data & systemen

Jouw continuïteit

2026




# De keten voelt het meteen…

Cyberincidenten zijn geen abstract IT-risico: ze raken klanten, leveringen, data, planning en vertrouwen

Wat leren deze cases?

1. De ingang is vaak de mens, leverancier of basisbeheer
2. Schade ontstaat in je bedrijfsproces, niet alleen in je IT
3. In de keten wordt ‘jouw incident’ snel het probleem van je klant
4. Herstelvermogen bepaalt of de impact uren, dagen of weken duurt

# Kwetsbaarheid zit vaak in de basis

Maatregelen nemen toe, maar zicht op risico's, herstel en ketenafhankelijkheden blijft vaak beperkt

**29%**
**Phishing of spoofing**
kreeg hiermee te maken
*bijna 1 op 3 **

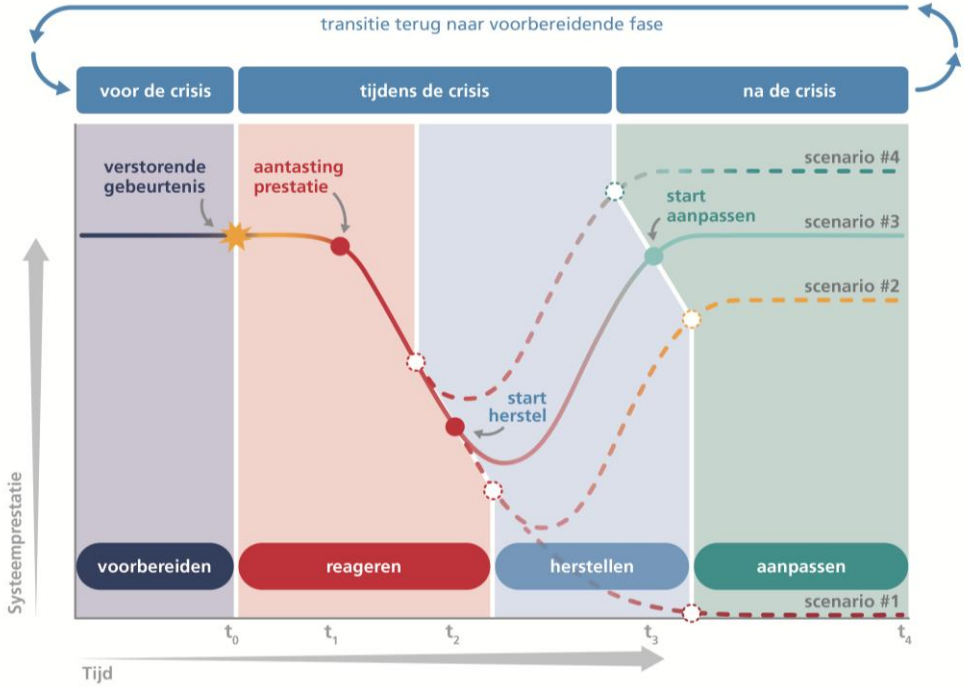
**6%**
**Cyberincident met gevolgen**
door aanval van buitenaf
*ongeveer 1 op 17 **

**7%**
**Cyberincident geoefend**
in het afgelopen jaar
*ongeveer 1 op 14 **



*Bron: CBS Cybersecuritymonitor 2025,*
** bedrijven met 10-50 werknemers*

# Cyberweerbaarheid is breder dan preventie



# Waarom nu?
# Drie ontwikkelingen die samenvallen…

**1. Cyberdreiging raakt bedrijfscontinuïteit**

Ransomware komt nog vaak binnen via bekende kwetsbaarheden en accountmisbruik

**2. Afhankelijkheid neemt toe**

Cloud, SaaS en uitbesteding maken ketens efficiënter én kwetsbaarder

**3. NIS2 is nu praktijk**

De Cyberbeveiligingswet geldt sinds 15 augustus ‘26 voor ruim 8.000 organisaties

**Urgentie = dreiging x afhankelijkheid x wettelijke norm**

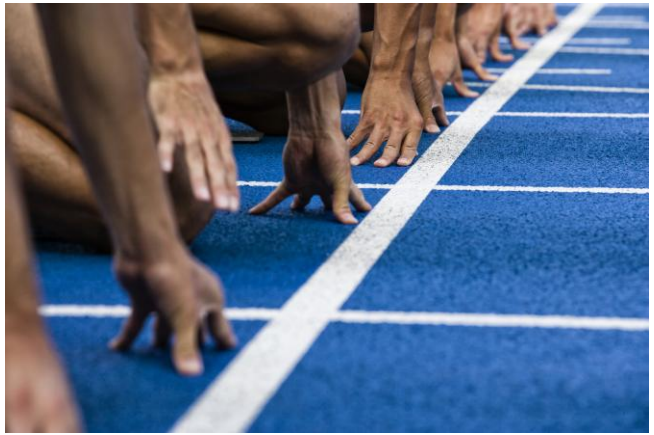
# NIS2 is geen eindpunt, maar een startpunt

**Cyberweerbaarheid begint niet bij voldoen aan regels, maar bij weten wat je moet beschermen, met wie je afhankelijk bent en hoe je blijft draaien als het misgaat.**

**1. Ken je afhankelijkheden**
Wie raakt jou — en wie raak jij?

**2. Maak het aantoonbaar**
Niet alleen vertrouwen, maar bewijsbare afspraken.

**3. Begin praktisch**
Gebruik NIS2 als kapstok om vandaag gerichte stappen te zetten.



# Meer weten over het Lectoraat Cyberweerbare organisaties en de onderzoeken die we doen?

Roel de Beer: RMG.deBeer@avans.nl

Bezoek onze website en LinkedIn pagina

Waarom is cyberbeveiligingswet ingevoerd, welke organisaties vallen eronder, welke verplichtingen zijn er, hoe ziet toezicht er uit, ...

***Stan van Bommel (RDI)***

Rijksinspectie Digitale Infrastructuur
*Ministerie van Economische Zaken*

# Samenwerken aan digitale weerbaarheid

Toezicht van RDI op de Cyberbeveiligingswet (NIS2)

Marnix Enthoven
Jorg van Putten
Stan van Bommel

# Inhoudsopgave

1. Wie is de RDI?
2. Wat betekent de Cbw voor jouw organisatie?

# Rijksinspectie Digitale Infrastructuur


- Voorheen Agentschap Telecom
- Een kantoor in Groningen en Amersfoort
- Bij de RDI zorgen ongeveer 450 professionals ervoor dat Nederland veilig verbonden is.

## Toezichthouder op basis van o.a.

- Telecommunicatiewet
- Zorgplicht Telecom Security
- Wbni
- eIDAS
- CRA
- Cybersecurity Act (CSA)
- Radio Equipment Directive
- EMC-richtlijn
- LVD-richtlijn
- Wet informatie-uitwisseling bovengrondse en ondergrondse netten en netwerken (WIBON)
- Metrologiewet
- Cyberbeveiligingswet (NIS2)
- Waarborgwet
- Wet Ruimtevaartactiviteiten
- Wet Digitale Overheid (na inwerkingtreding)

# 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

TERUG

# Wat betekent de Cyberbeveiligingswet voor jouw organisatie?

**Registratieplicht**
• Organisaties die onder de wet vallen moeten zich registreren in het nationale register.
• In Nederland gebeurt dit via het NCSC (mijn.ncsc.nl).

**Zorgplicht**
• Organisaties moeten passende technische, organisatorische en operationele beveiligingsmaatregelen nemen.

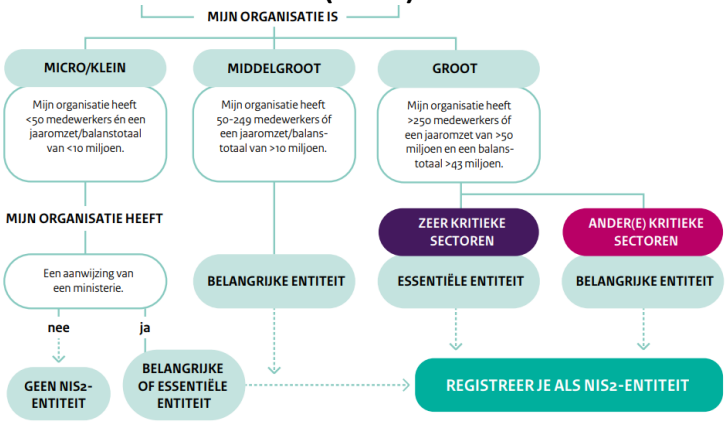
**Meldplicht**
• Essentiële en belangrijke entiteiten moeten significante cyberincidenten melden aan hun CSIRT en toezichthouder.

**Bestuurlijke verantwoordelijkheid en training**
• Het bestuur is verantwoordelijk voor het cyberbeveiligingsbeleid en de naleving van de wet.
• Bestuurders moeten beveiligingsmaatregelen goedkeuren en hiervoor passende training volgen.

**Toezicht**
• Toezichthouders controleren of organisaties voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

# Registratieplicht

- Registratie via mijn.ncsc.nl
- Bijlage 1 (essentieel) en 2 (belangrijk) van de Cbw bevatten overzichten met (sub)sectoren




- Bepalend is:
  - Aantal medewerkers
  - Jaaromzet
  - Balans
- Registreer alle subsectoren. Essentieel gaat voor belangrijk gaat

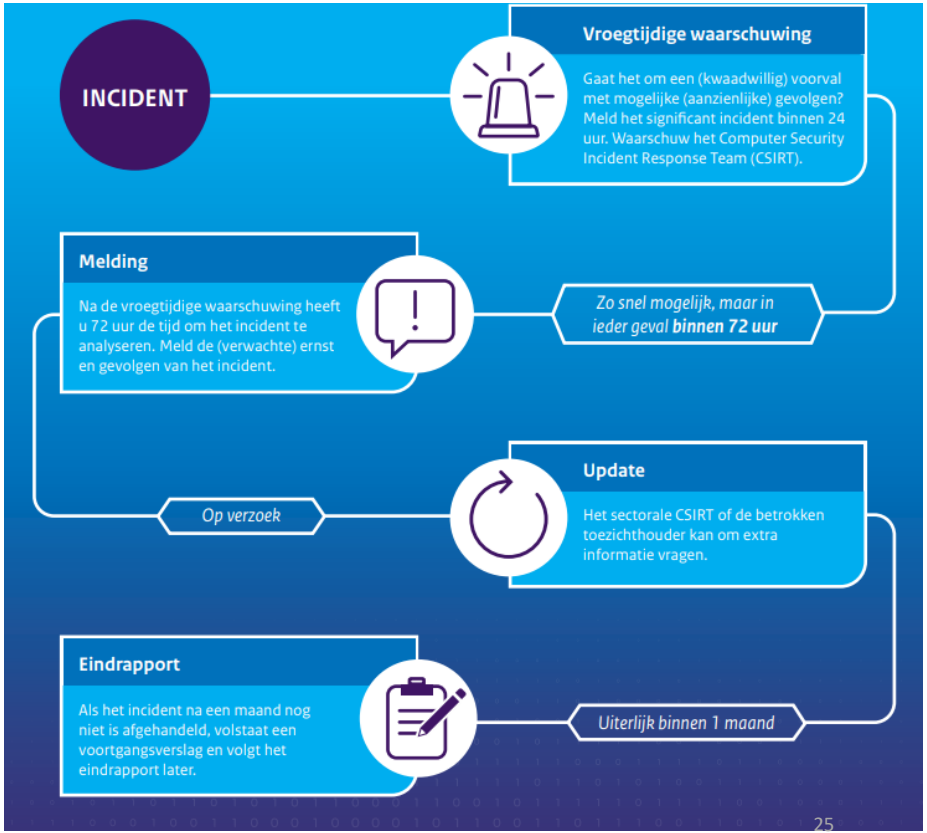
# Hoe verbeter je de digitale weerbaarheid?

**Zorgplicht:**

- Artikel 21 Cbw: neem passende maatregelen op basis van een risico analyse
- NCSC – Zorgplicht
- Ministerie van EZK heeft een ministeriële regeling uitgewerkt voor nadere invulling van de zorgplicht
- Gebruik de NIS2-Quickscan van de RDI om te toetsen of jouw bestaande maatregelen van jouw organisatie voldoen aan de eisen van de NIS2-richtlijn
- RDI publiceert inzichten uit inspecties op haar website

# Meldplicht

- Meldplicht Cyberbeveiligingswet | Rijksinspectie Digitale Infrastructuur (RDI)
- Meld significante cyberincidenten
- Ministerie van EZK heeft een ministeriële regeling uitgewerkt voor nadere invulling van de meldplicht (artikel 12)



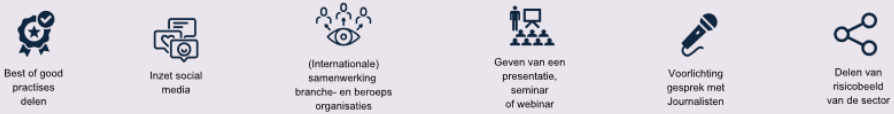
# Toezicht: De organisatie is zelf verantwoordelijk voor de invulling van maatregelen

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.

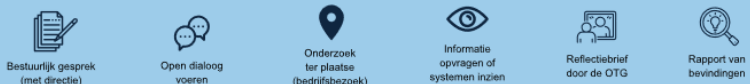
Mogelijkheid tot **aanwijzen** essentiële entiteiten→ pro-actief toezicht.

## VOORLICHTING, KENNISDELING EN HANDVATTEN




## BEELDVORMING


## INSPECTEREN & TERUGKOPPELEN




## VERBETERACTIES

# Zijn er nog vragen?

Praktische invulling van de wetgeving, concrete handvatten.

***Ben Stofbergen en Jorrit de Boer (PVO)***

# NIS2/CBW

Ben Stofbergen & Jorrit de Boer | Impuls Zeeland

10 september 2026

PVO Zeeland West-Brabant

# PVO Zeeland West-Brabant

Weerbaarder maken van ondernemers tegen:

- Cybercriminaliteit
- Georganiseerde ondermijnende criminaliteit
- Veelvoorkomende Vermogenscriminaliteit (VVC)


# Bowtie Model

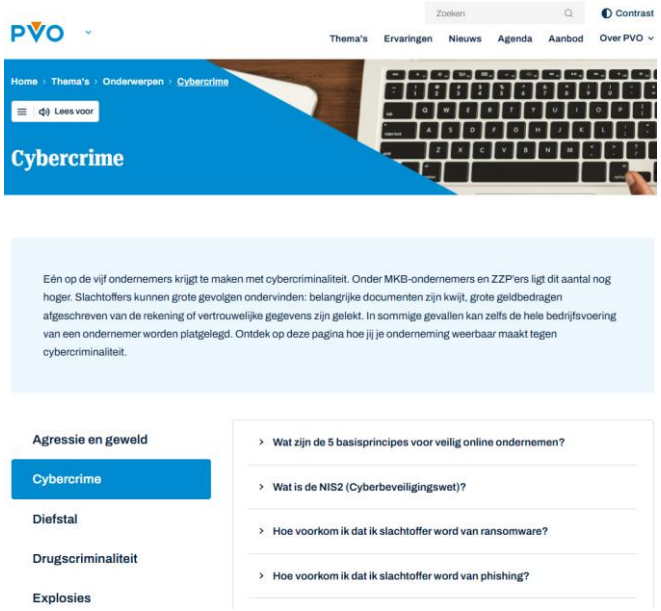
## Maatregelen ‘vooraf’

- Voer een risico analyse uit
- Gebruik veilige inlogmethoden, zoals MFA
- Bewustwordingstrainingen onder het personeel

## Maatregelen ‘achteraf’

- Richt incident respons in
- Beveilig uw toeleveringsketen
- Maak regelmatig back-ups (ook fysieke kopieën)
- Maak een Bedrijfscontinuïteitsplan (BCP)

# Kijk op




**pvo-zeelandwestbrabant.nl**

Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

Beginnen met cybersecurity

Processen verbeteren en borgen

Verdiepen in ontwikkeling en kennis

Veilig inkopen en uitbesteden

Voldoen aan wetgeving en beleid


## Bekijk de 5 basisprincipes

Er zijn heel wat maatregelen die je (vandaag nog) kunt nemen om je bedrijf of organisatie beter te beschermen tegen cyberaanvallen. Als je de maatregelen treft die voortkomen uit de 5 basisprincipes, zet je een mooie basis neer. Lees wat je minimaal moet doen en hoe je dit aanpakt.


## Doe de CyberVeilig Check

Speciaal voor kleinere bedrijven en organisaties is er de CyberVeilig Check. Besteed 5 minuten aan deze zelfscan en weet hoe je ervoor staat qua basisveiligheid. Download je eigen actielijst en ga vandaag nog aan de slag met de eerste kleine maatregelen waarmee je grote stappen zet in je digitale weerbaarheid. Bouw het daarna gefaseerd uit.

**ncsc.nl**


PVO
Veilig ondernemen.
Daar maken we ons sterk voor.

# Q&A, ondersteuning

Impuls Zeeland

Rijksinspectie Digitale Infrastructuur
*Ministerie van Economische Zaken en Klimaat*

PVO

avans hogeschool