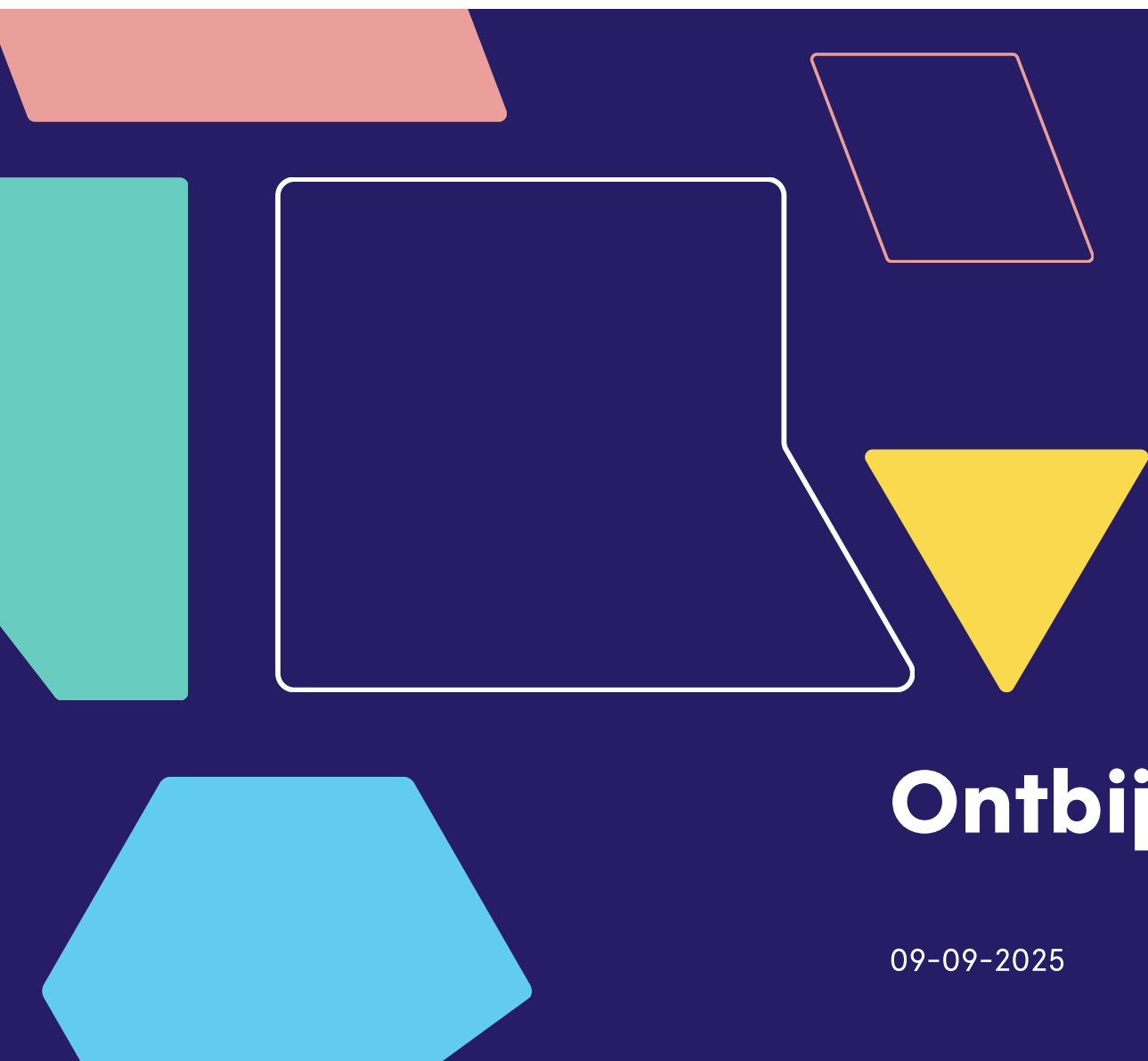




vrieling



datect



nicecloud



Ontbijtsessie

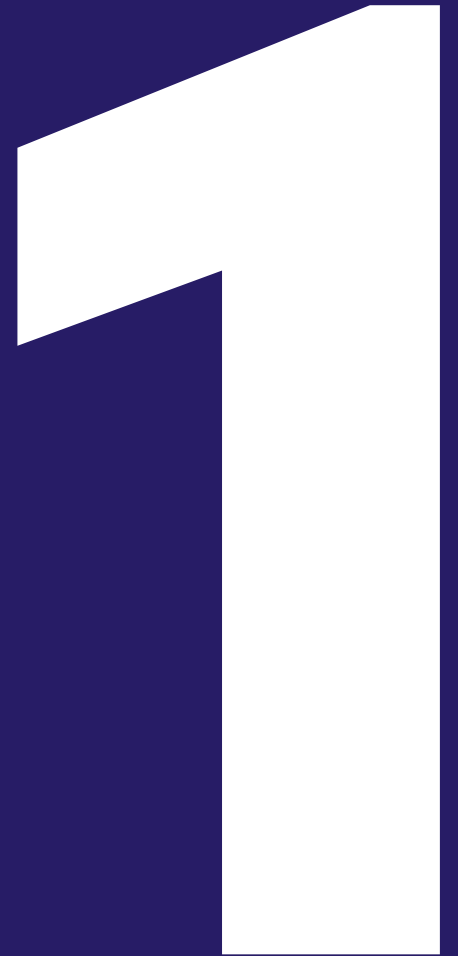
09-09-2025



vrieling

Welkom ontbijtsessie

- Serge Evers -



Welkom

- Digitale weerbaarheid wordt steeds belangrijker.
- Doel ontbijt sessie:
 - Wat betekent NIS2?
 - Wat verandert er voor organisaties?
 - Welke stappen kun je zelf zetten?
- Experts
 - Paul Verhoef – Datect
 - Ron Lourens – Nicecloud
 - Martijn Schakelaar – Vrieling

vrieling

Cyber security van Datect

- Paul Verhoef -



2

Datect B.V.

Risk Assessment
& Audits

Certificeringen

Business
Continuity

Pentesting

Awareness &
Training

ISMS

- Gevestigd in Naarden.
- Team van 35 professionals.
- Vest.nl.
- Meer dan 20 jaar ervaring.
- Eigen pentest team.
- Samenwerking in de IT-keten.
- Altijd vaste prijs afspraken.

NIS2 Directive



Cyberbeveiligingswet





Wat zijn de belangrijkste onderdelen van de cyberbeveiligingswet?



Onderscheid tussen essentiële en belangrijke entiteiten.



Zorgplicht, registratieplicht en meldplicht.



Bestuurlijke aansprakelijkheid en opleidingsplicht voor bestuurders.



Meer sectoren en organisaties.



Toezicht en handhaving.



Inrichting van stelsel van Computer Security Incident Response Teams (CSIRTs) voor bijstand aan NIS2 entiteiten.

Handhavingsinstrumenten.

→ **Essentiële entiteiten**

- Controlefunctionaris.
- Beveiligingsscan.
- Beveiligingsaudit.
- Openbaarmaking overtreding.
- Bindende aanwijzing.
- Last onder bestuursdwang.
- Verzoek tot schorsing certificering of vergunning.
- Verzoek tot schorsing leden van het bestuur.
- Bestuurlijke boete.

→ **Belangrijke entiteiten**

- Beveiligingsscan.
- Beveiligingsaudit.
- Openbaarmaking overtreding.
- Bindende aanwijzing.
- Last onder bestuursdwang.
- Bestuurlijke boete.

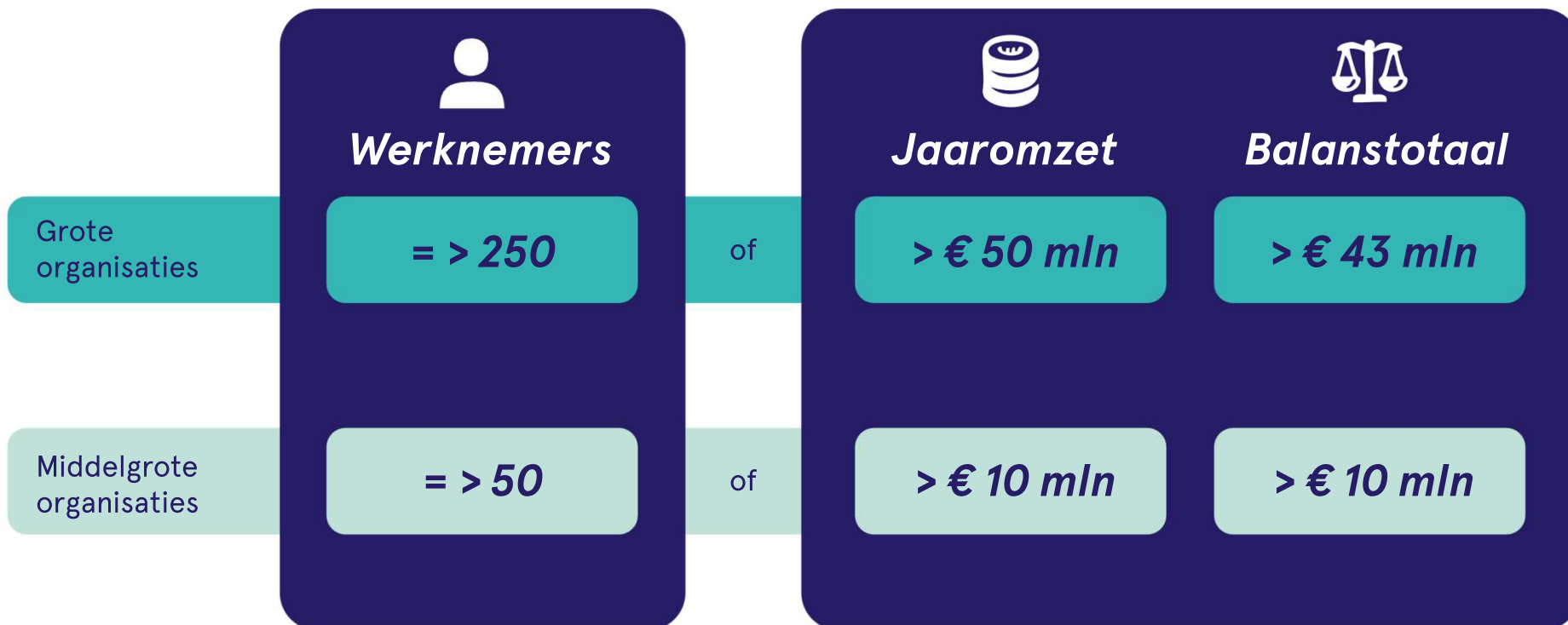
Bijlage 1: Zeer kritieke sectoren



Bijlage 2: Andere kritieke sectoren



Entiteiten die domeinregistratiediensten aanbieden vallen ook onder NIS2, ongeacht hun omvang, maar behoren niet tot bijlage 1 of 2, aangezien op deze categorie andersoortige verplichtingen van toepassing zijn.



Bevoegde autoriteit	Sector	Subsector	Grote organisaties	Middelgrote organisaties	Kleine- en micro-organisaties
Minister van Economische Zaken	 Digitale aanbieders	Online marktplaatsen, zoekmachines, social media platforms	Belangrijk	Belangrijk	Niet van toepassing
Minister van Economische Zaken	 Post- en koeriersdiensten		Belangrijk	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	 Afvalstoffen-beheer	Alleen als afvalstoffenbeheer de voornaamste economische activiteit is	Belangrijk	Belangrijk	Niet van toepassing
Minister van Landbouw, Visserij, Voedselzekerheid en Natuur	 Levensmiddelen	Groothandelsproductie, industriële productie, verwerking	Belangrijk	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	 Chemische stoffen	Vervaardiging, productie, distributie	Belangrijk	Belangrijk	Niet van toepassing
Nader te bepalen	 Onderzoek	Onderzoekinstellingen (met uitzondering van onderwijsinstellingen)	Belangrijk	Belangrijk	Niet van toepassing
Minister van Economische Zaken	 Vervaardiging	(in-vitro diagnostische) medische apparaten; computer-, elektronische optische producten; elektrische apparatuur; machines; motorvoertuigen, aanhangwagens, opleggers	Belangrijk	Belangrijk	Niet van toepassing

Bevoegde autoriteit	Sector	Subsector	Grote organisaties	Middelgrote organisaties	Kleine- en micro-organisaties
Minister van Economische Zaken	 Digitale infrastructuur	Niet-gequalificeerde vertrouwensdienstverleners	Essentieel	Belangrijk	Belangrijk
		Aanbieders van internet exchange points	Essentieel	Belangrijk	Niet van toepassing
		Cloudserviceprovider	Essentieel	Belangrijk	Niet van toepassing
		Datacenter serviceprovider	Essentieel	Belangrijk	Niet van toepassing
		Content delivery network providers	Essentieel	Belangrijk	Niet van toepassing
Minister van Economische Zaken	 Beheerders van ICT-diensten	Managed service providers, managed security service providers	Essentieel	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	 Afvalwater	Alleen als het een essentieel onderdeel is van de algemene activiteit	Essentieel	Belangrijk	Niet van toepassing

Bevoegde autoriteit	Sector	Subsector	Grote organisaties	Middelgrote organisaties	Kleine- en micro-organisaties
Minister van Volksgezondheid, Welzijn en Sport	 Gezondheidszorg	Zorgverleners; laboratoria; onderzoek & ontwikkeling van geneesmiddelen; vervaardiging van farmaceutische basisproducten en -preparaten; vervaardiging van medische hulpmiddelen die van cruciaal belang zijn bij noodsituaties op het gebied van de volksgezondheid	Essentieel	Belangrijk	Niet van toepassing
		Entiteiten met een distributievergunning voor geneesmiddelen: alleen indien geïdentificeerd als kritieke aanbieder in de Critical Entities Resilience Directive (CER-richtlijn)	Essentieel	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	 Drinkwater		Essentieel	Belangrijk	Niet van toepassing
Minister van Economische Zaken	 Digitale infrastructuur	Gekwalificeerde vertrouwensdienstverleners (QTSP)	Essentieel	Essentieel	Essentieel
		Registers voor topleveldomeinnamen	Essentieel	Essentieel	Essentieel
		Verleners van domeinnaamregistratiediensten	Essentieel	Essentieel	Essentieel
		Aanbieders van openbare elektronische communicatienetwerken en -diensten	Essentieel	Belangrijk	Niet van toepassing

Conformiteit met artikel 21.2d

- Zorgt voor naleving van de wettelijke eisen zoals gesteld in artikel 21.2d van de NIS2-richtlijn.
- Helpt bedrijven te voldoen aan hun verplichtingen om passende beveiligingsmaatregelen in de toeleveringsketen te garanderen.

NIS2 wetgeving: de beveiliging van de toeleveringsketen is verplicht.

Verplicht aan de slag met je leveranciers.

Logistieke partners
Transporteurs en opslagbedrijven zorgen dat je producten op tijd bij klanten komen. Een cyberaanval op hen kan dit proces verstoren.

Financiële dienstverleners
Je accountant, boekhouder of payroll-provider beheert gevoelige financiële gegevens. Een hack bij hen kan eventueel leiden tot financieel misbruik.

Productiesystemen en machines

Van lopende banden tot verpakkingsmachines: als deze systemen worden gehackt, kunnen productieprocessen stilvallen.

Facilitaire leveranciers

Schoonmaakdiensten of beveiligingsbedrijven met fysieke toegang spelen rol in de veiligheid van je bedrijf.

ICT-dienstverleners en software

Leveranciers die je netwerk, firewalls en back-ups beheren, zijn een stevig risico voor je cyberveiligheid. En ook je software is natuurlijk een risico.

Leveranciers zoals ontwerpers of marketing- en communicatiebureaus

Door met één standaard te werken, verminder je de complexiteit, verlaag je kosten en biedt je jouw leveranciers heldere richtlijnen. Dit zorgt voor een veerkrachtige en stabiele keten, zelfs in crisissituaties.

Alle leveranciers zijn een potentieel risico

Voor je bedrijfsprocessen, je plannen, je financiële gegevens, de contracten met grote klanten. Jij bent daar zelf voor verantwoordelijk. Vraag certificering aan je leveranciers. Kijk op www.samendigitaalveilig.nl/inkoop

Gelaagde veiligheid die past bij het risiconiveau

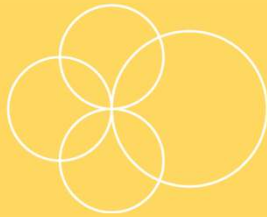
- Risico gebaseerde benadering: leveranciers worden beoordeeld en waar nodig gecertificeerd op een niveau dat past bij hun specifieke risico.
- Vermijd overbelasting van leveranciers door onnodig zware eisen. Het voorkomt dat je leveranciers teveel tijd kwijt zijn of te hoge kosten maken.

vrieling

**Betrouwbaar, betrokken,
deskundig en nice!**

- Ron Lourens -

nicecloud

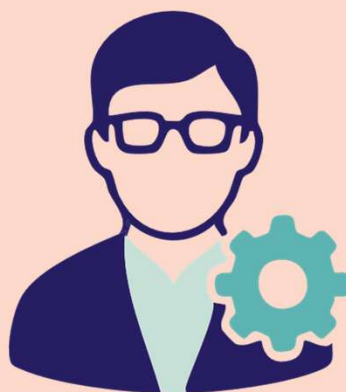


- Tijden van verandering.
- Cybersecurity is geen IT-onderwerp meer.
- Het is een strategisch fundament voor vertrouwen, continuïteit én groei





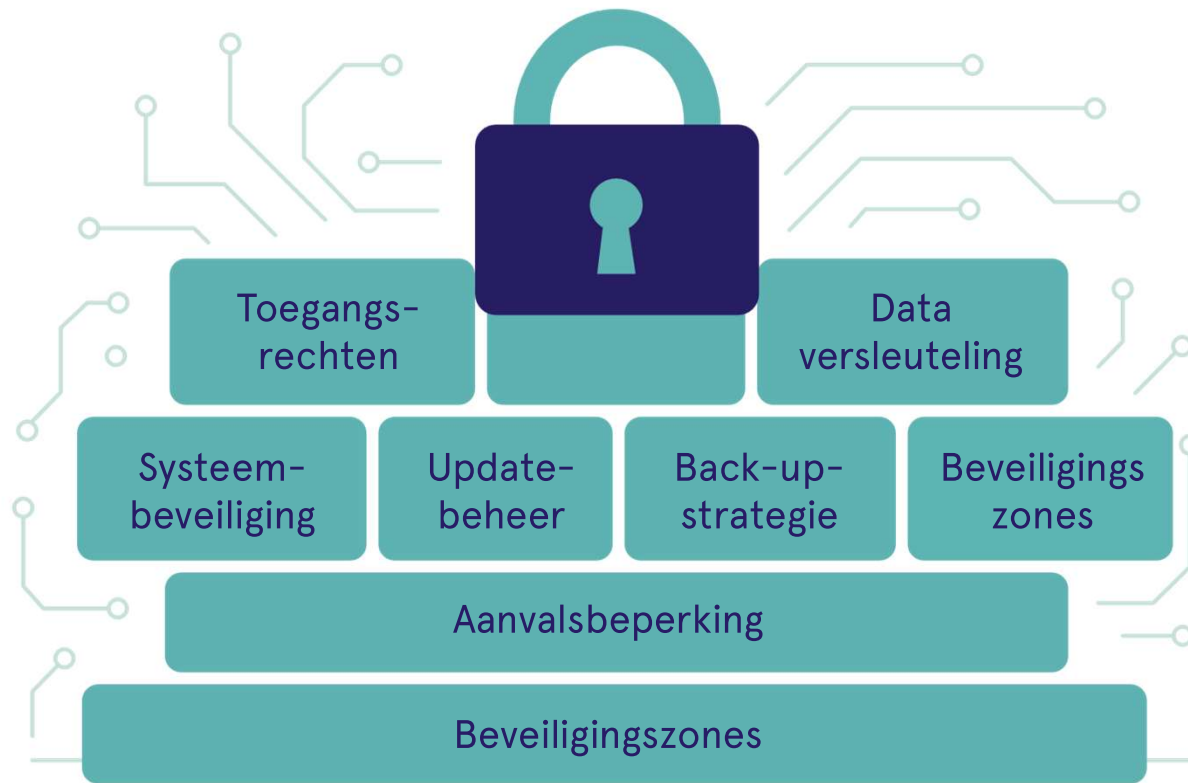
Gebruiker



Beheerder



Controleur



Cyberbewustzijn

Internet en Netwerk

- Nicecloud is internetprovider voor alle glasvezelnetwerken.
- Netwerkbeheer zorgt voor een betrouwbaar en volgens ontwerp veilig netwerk.



Excellence
Partner



Microsoft 365 Azure Cloud

- De werkplek van NU.
- Het beste van Microsoft 365 met persoonlijke ondersteuning, slimme beveiliging en voorspelbare IT-kosten, zodat jouw organisatie veilig, flexibel en productief kan werken, altijd en overal.

Vast en Mobiel bellen

- Communicatie op het meest betrouwbare netwerk van Nederland.
- Bereikbaarheid is essentieel voor klantcontact, samenwerking en flexibiliteit.





Datect
- Paul Verhoef -

vrieling



NIS2-Quality Mark

→ Prima oplossing voor de toeleveringsketen.

**Voor
toeleveranciers**

Jouw klant eist naleving
van NIS2-wetgeving.



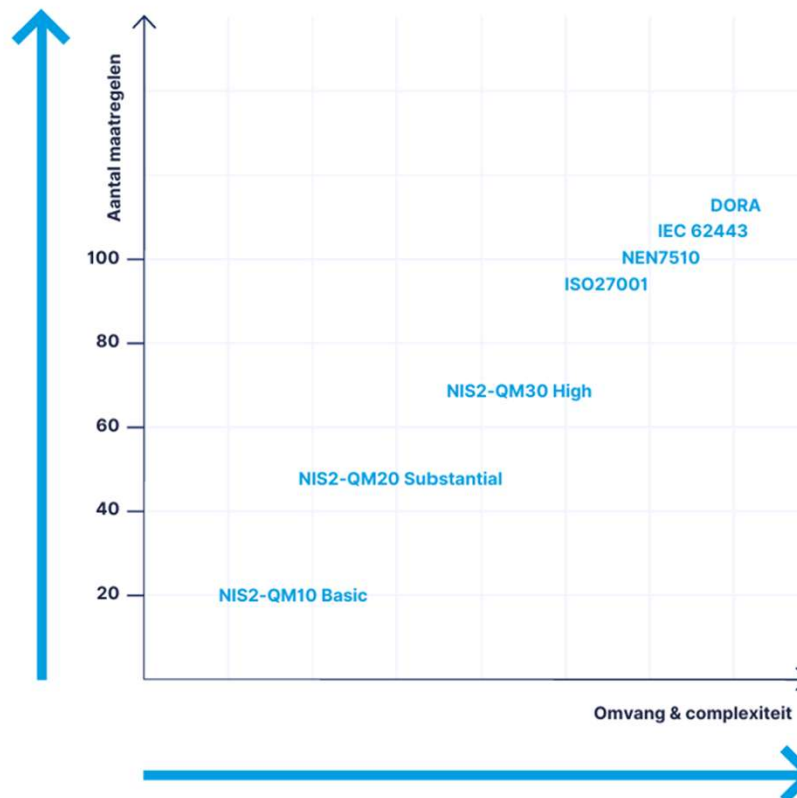
De makkelijkste manier
om samen te werken.

**Voor essentiële en
belangrijke organisaties**

Maak de NIS2-wet haalbaar
voor jouw toeleveranciers.

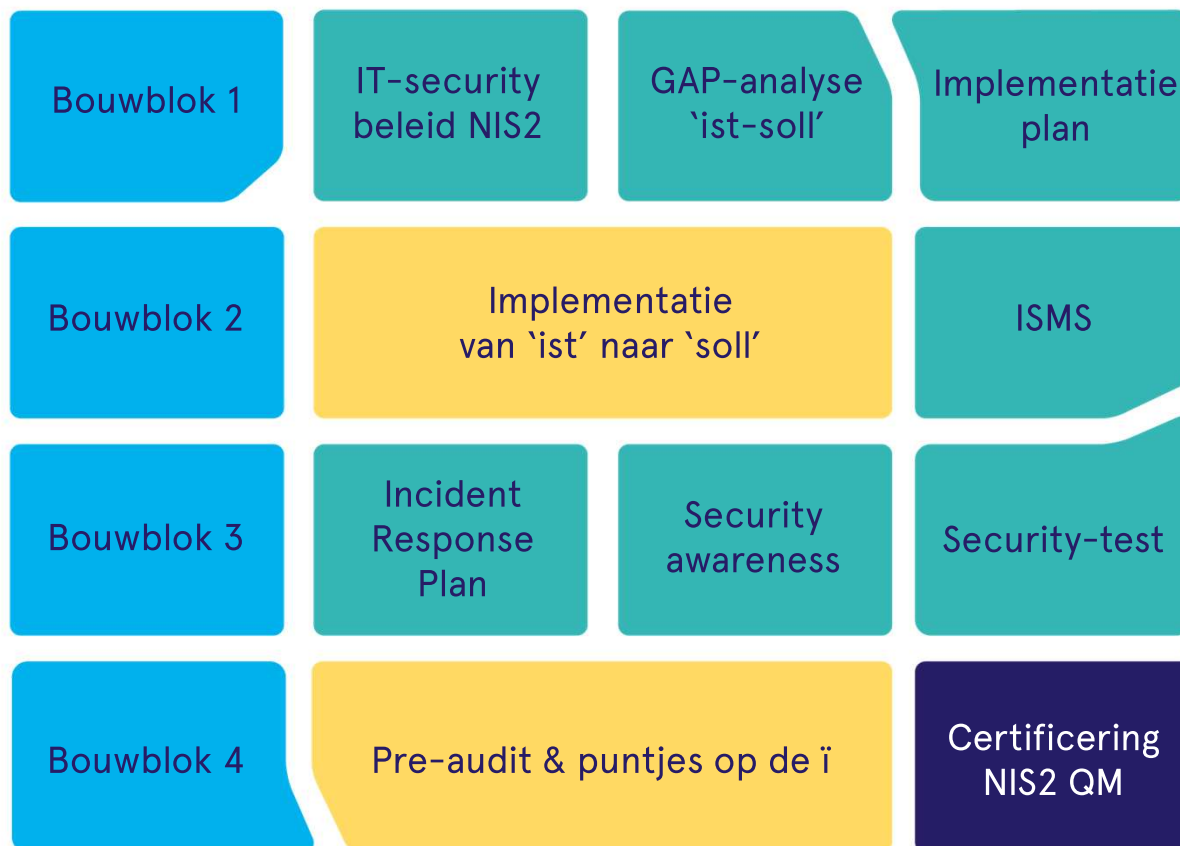
NIS2- Quality Mark

Optimale normen voor alle bedrijven



Voor risicoafdekking bij mkb-bedrijven past het NIS2 Quality Mark heel goed.

NIS2-QM Cyber Programma





vrieling

Vrieling
- Martijn Schakelaar -

5

→ Vraag:

→ En dan? Verzekeren? Kan je eigenlijk nog wel zonder?

→ Vraag:

→ Wat is er dan verzekerd?

→ Want:

- Wij hebben toch een bedrijfsschadeverzekering.
- Wij hebben toch een aansprakelijkheidsverzekering.
- Wij hebben toch een electronicaverzekering.

Waarom dan toch ook nog (of als alternatief) een cyber(risico)verzekering?

Wat kan een cyberverzekering afdekken

- Incidentresponseteam:
 - Juridische en IT-diensten, reconstructie van data en communicatie/kennisgeving betrokkenen (bhv).
- Bedrijfsschade (ten gevolge van netwerkonderbreking en/of systeemfalen).
- Aansprakelijkheid (verlies van data of financiële schade van een derde).
- Cyberafpersing (ransomware).
- Boetes vanuit AVG.
- Telefoonhacking.
- Elektronisch afgebogen betalingen.

Aandachtspunten – veelal beperkt gedekt

- Ransomware tot een beperkte (sub)limiet.
- Wijdverspreide incidenten tot een beperkte (sub)limiet.
- Bedrijfsschade na wachtturen en aftopping periode.
- Social engineering: wordt als fraude beschouwd en niet als een cyberincident.

Randvoorwaarden voor dekking – 'basishygiëne' (?)

- Antivirusprogramma's.
- Structuur in back-up procedure.
- Actief wachtwoordbeleid.
- Updates direct uitvoeren.
- Besturingssystemen moeten worden ondersteund door fabrikant gebruik van 2F/MF authenticatie.
- Incidentresponseplan.
- Awareness trainingen personeel.

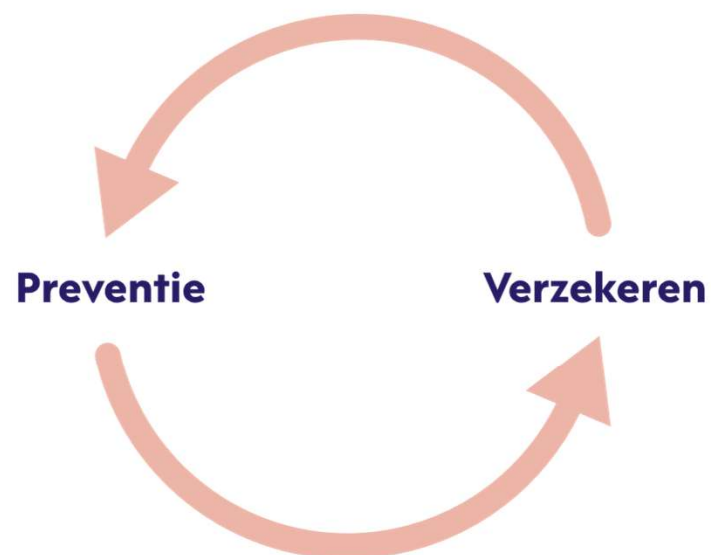
Unieke verzekeringsoplossing in combinatie met NIS2 certificering!

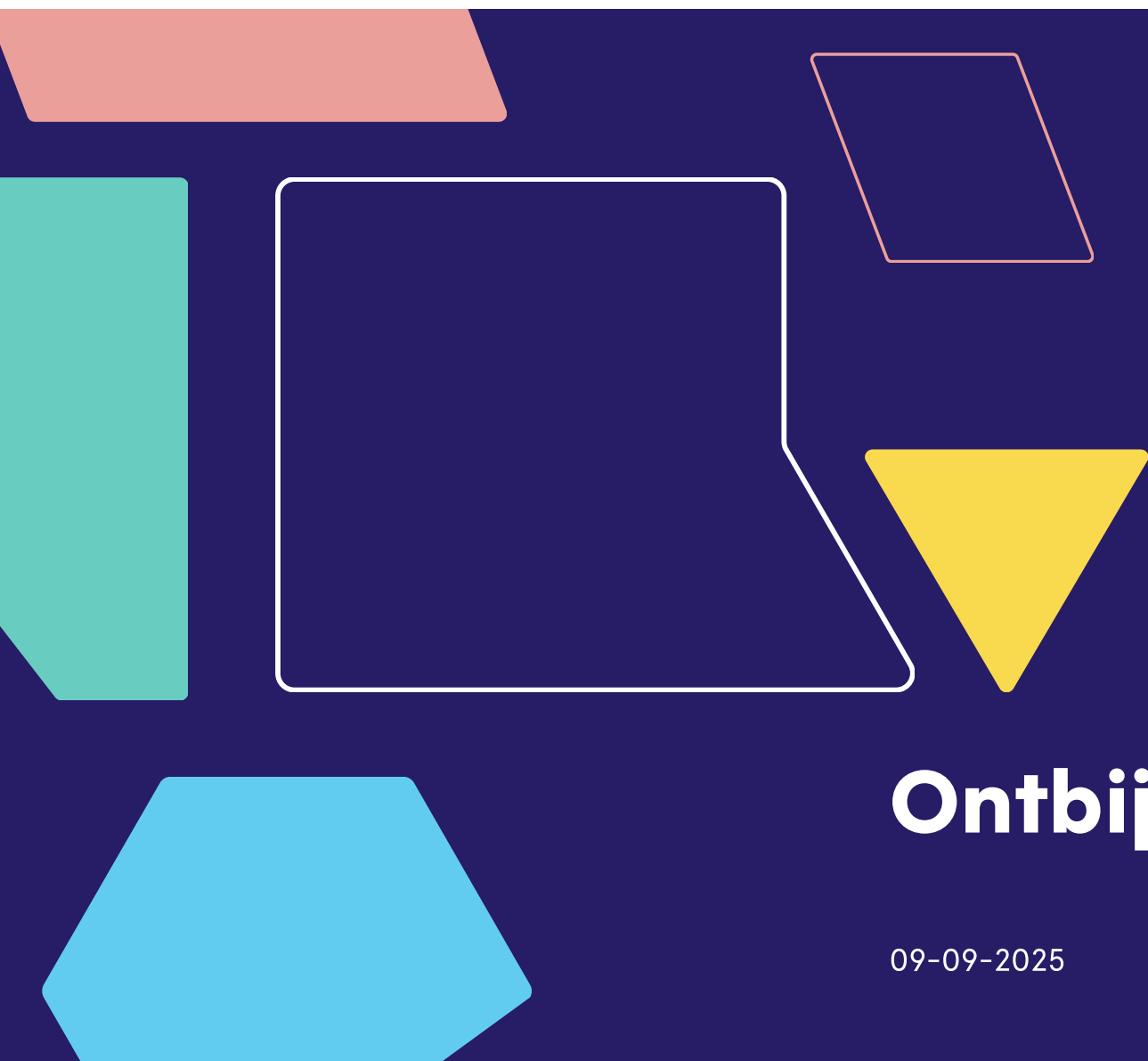
- Verkorte aanvraag met beperkt aantal (technische) vragen.
- Korting op de reguliere premie.
- Nederlandstalige incidentresponse.
- Geen beroep op uitsluitingen in voorwaarden ten aanzien van niet genomen maatregelen.
- Volledige dekking ransomware mogelijk.
- Volledige dekking wijdverspreide incidenten mogelijk.

Conclusie

(Cyber)risico's managen is een samenspel tussen

Geeft daarmee rust, continuïteit en zekerheid.





vrieling



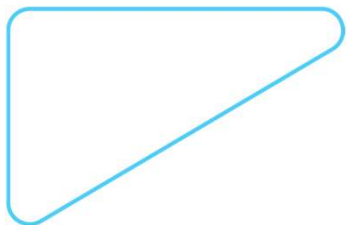
 **datect**



nicecloud 

Ontbijtsessie

09-09-2025



AXXOR