vrieling

Whitepaper

# NIS2 en cyberverzekeringen

## Digitaal veilig ondernemen in een nieuw tijdperk

Goed geregeld met Vrieling

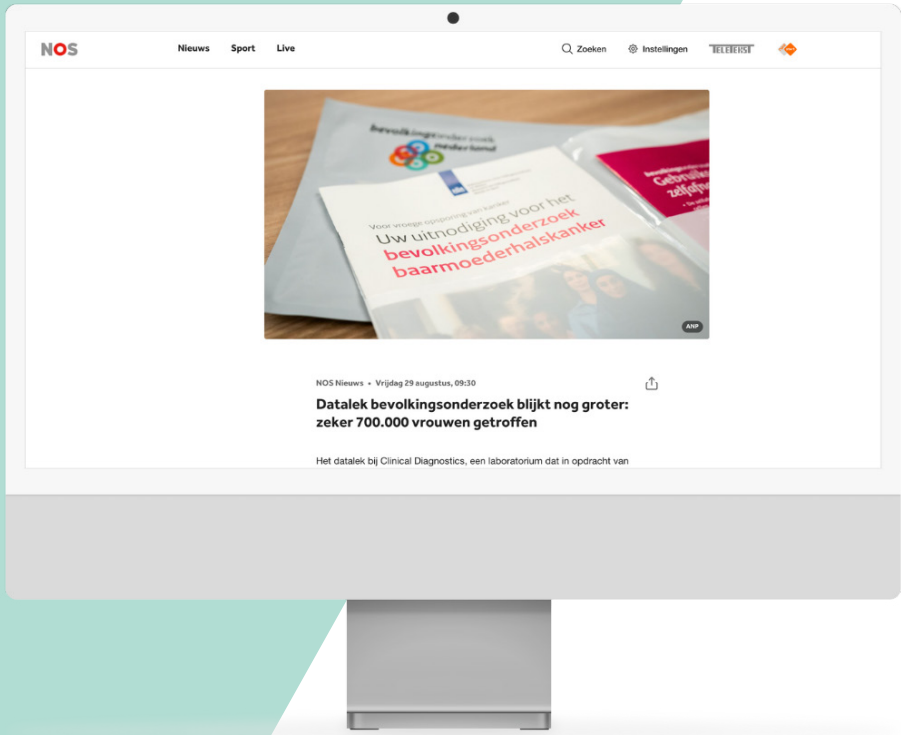
# NIS2 en cyberverzekeringen

## Digitaal veilig ondernemen in een nieuw tijdperk

De recente hacks bij bevolkingsonderzoeken en medische laboratoria maakten veel los. Gegevens van honderdduizenden vrouwen liggen inmiddels op het dark web. Hackers eisen losgeld en dreigen meer informatie te publiceren.

Vanaf 2026 geldt bovendien de Europese NIS2-richtlijn in Nederland. Deze wet verplicht bedrijven om hun digitale veiligheid aantoonbaar op orde te hebben. In deze whitepaper lees je wat dat betekent, welke risico's er spelen en hoe jij jouw bedrijf kunt beschermen met een combinatie van preventie, kennis en verzekering.

De gevolgen zijn enorm. Niet alleen voor de getroffen organisaties, maar ook voor patiënten, medewerkers en het vertrouwen in de hele sector. Het laat zien: cybercriminaliteit is geen ver-van-je-bedshow. Iedere organisatie kan getroffen worden.




vrieling

# Cyberaanvallen dichtbij huis

Cyberaanvallen klinken vaak groot en ingewikkeld, maar de praktijk laat zien dat ze vaak klein beginnen.

- Een medewerker die een phishingmail opent.
- Een vergeten update.
- Een zwak wachtwoord.

**Meer dan**

**60%**

**van de incidenten ontstaat door menselijke fouten.[1]**

Voorbeelden dichtbij:

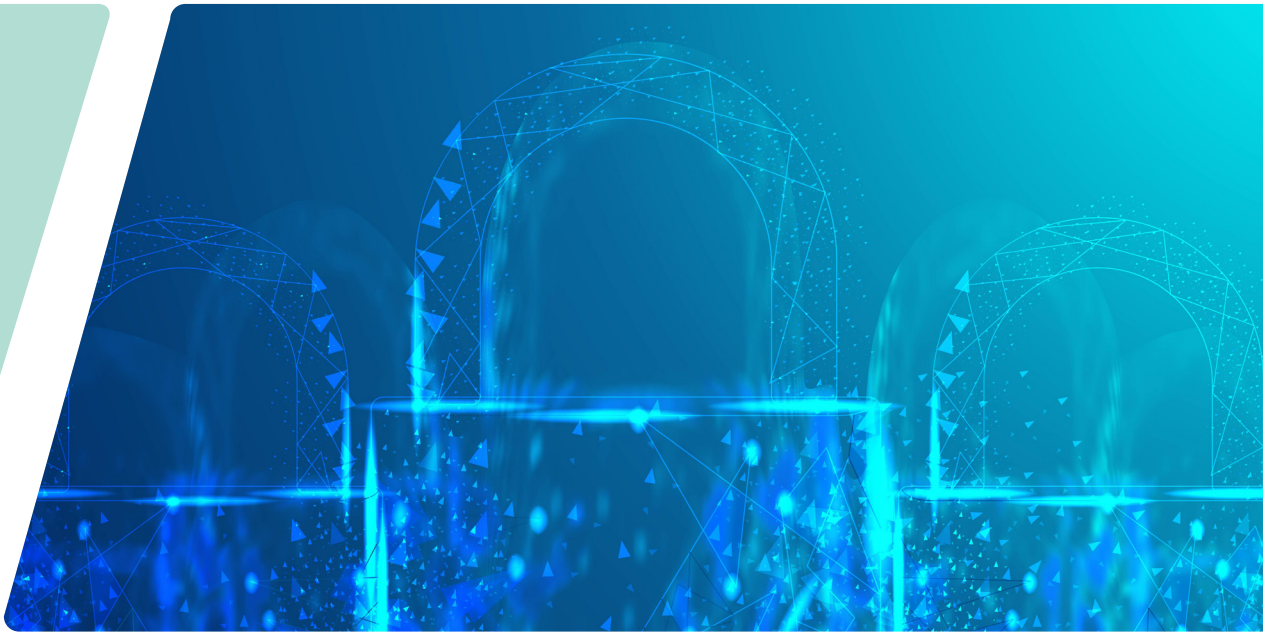
- Een tandartspraktijk kon dagenlang geen dossiers openen na een phishingaanval.
- Een transportbedrijf legde de logistiek plat toen hun chauffeurs-app gehackt werd.
- Een mkb-webshop kreeg na een datalek zelfs een AVG-boete opgelegd.
- Zelfs een gemeente als Hof van Twente werd volledig gegijzeld en leed meer dan 4 miljoen euro schade.[2]

# De urgentie in cijfers

De financiële schade van een cyberaanval is vaak groter dan verwacht. De gemiddelde kosten van een ransomware-aanval lopen op tot tonnen.[3] Het losgeld zelf is zelden het grootste probleem; de echte schade zit in omzetverlies en herstelkosten.

Slechts **60%** past multi-factor (2F) authenticatie toe voor kritieke systemen, terwijl dit straks verplicht wordt onder NIS2.

Uit cijfers blijkt dat **70%** van de organisaties nog verouderde systemen gebruikt die niet meer geüpdatet worden.



# Wat is NIS2?

De NIS2-richtlijn is Europese wetgeving die vanaf 2025 ook in Nederland gaat gelden. Het doel: een hoger en uniform niveau van digitale veiligheid.

De regels gelden voor organisaties in vitale sectoren én hun leveranciers en ketenpartners. Daarmee raakt NIS2 veel meer bedrijven dan vaak gedacht.

- Concreet vraagt NIS2 dat organisaties risicoanalyses uitvoeren en passende maatregelen nemen.
- Incidenten binnen 24–72 uur melden.
- Bestuurders en directies persoonlijk verantwoordelijkheid nemen en rekening houden met forse boetes bij niet-naleving: tot 10 miljoen euro of 2% van de wereldwijde omzet.

# Cyberrisico's in de praktijk

Cybercriminelen gebruiken steeds meer middelen om bedrijven te raken. Denk aan ransomware, phishing en datadiefstal. Steeds vaker gebeurt dit via de keten: één leverancier wordt gehackt en brengt de hele sector in gevaar.

Een ondernemer uit de maakindustrie verwoordde het zo:

**"We dachten dat cybercrime alleen grote bedrijven trof. Tot ons eigen netwerk gegijzeld werd. Dankzij de verzekering konden we dezelfde dag weer doorwerken."**

vrieling

# Digitale weerbaarheid opbouwen

Digitale veiligheid draait om drie pijlers: **Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV)**. **Beschikbaarheid** betekent dat systemen toegankelijk moeten blijven, **integriteit** staat voor betrouwbare gegevens en **vertrouwelijkheid** voorkomt dat gevoelige informatie op straat belandt.

Weerbaarheid vraagt om techniek, processen én mensen. Multi-factor authenticatie, veilige back-ups, monitoring en tijdig patchmanagement zijn essentieel. Maar techniek alleen is niet genoeg. Medewerkers zijn vaak de zwakste schakel. Training en bewustwording maken het verschil.

# De rol van een cyberverzekering

Zelfs met goede maatregelen blijft er altijd een risico. Cybersecurity verkleint de kans, maar sluit het nooit uit. Daarom is een cyberverzekering het sluitstuk van digitale veiligheid.

Een goede verzekering biedt niet alleen financiële dekking, maar ook directe hulp:

- Altijd dekking bij schade.
- 24/7 ondersteuning door een Nederlands responsteam.
- Aantoonbaar veilig ondernemen richting klanten en toezichthouders.
- Preventie en training inbegrepen.
- Juridische en communicatie-ondersteuning bij incidenten.

# Onze aanpak en oplossing.

Een losse cyberverzekering is niet alles. Cyberveiligheid begint bij de preventie. Afhankelijk van jouw bedrijf en situatie kijken wij naar de best passende oplossing voor jou. Dit kan zijn het begeleiden van een NIS2 certificeringstraject via onze partner Datect. Of de zekerheid hebben van jouw digitale veiligheid via onze partner Eye. De cyberverzekering is het sluitstuk. Goede hulp op het moment dat het toch mis gaat. En de zekerheid dat jouw cyberverzekering ook dekking biedt.

Datect helpt bij het verbeteren van processen en systemen. Tegelijkertijd regelen wij een passende verzekering bij Markel. Zo weet je dat je niet alleen veilig onderneemt, maar ook beschermd bent als het misgaat.

Een logistiek ondernemer zei:

**“De check gaf ons direct inzicht. Binnen een week hadden we maatregelen doorgevoerd en de verzekering afgesloten. Dat gaf rust.”**

# Wie vallen onder NIS2?

De NIS2-richtlijn maakt onderscheid tussen essentiële entiteiten en belangrijke entiteiten. Daarnaast gelden er criteria op basis van omvang.

## Essentiële sectoren

- Energie (elektriciteit, olie, gas).
- Vervoer (luchtvaart, spoor, water, weg).
- Bankwezen.
- Gezondheidszorg.
- Drinkwater.
- Digitale infrastructuur.

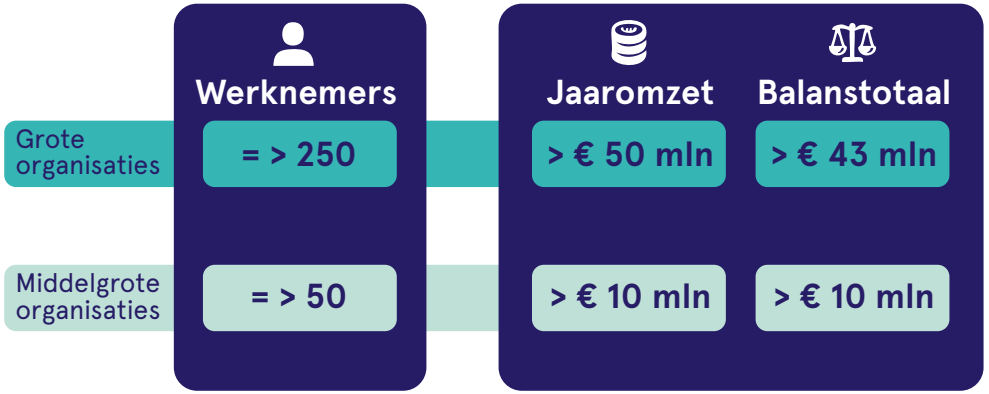
## Andere kritieke sectoren

- Post- en koeriersdiensten.
- Afvalstoffenbeheer.
- Chemie, voeding, productie.
- Digitale aanbieders (cloud, datacenters, online marktplaatsen).

## Domeinregistratiediensten

Vallen óók onder NIS2, ongeacht omvang.

## Omvangscriteria:




Met andere woorden: veel meer organisaties dan vaak gedacht vallen straks onder NIS2. Niet alleen vitale sectoren zelf, maar ook leveranciers en ketenpartners moeten aantoonbaar digitaal veilig werken.

# Conclusie – Wachten is geen optie

Recente datalekken laten zien hoe groot de gevolgen van cybercrime zijn. Met NIS2 wordt digitaal veilig ondernemen bovendien verplicht.

**De vraag is dus niet óf je iets moet regelen, maar wanneer.**

Doe de gratis cybercheck en ontvang binnen 24 uur inzicht.
Neem contact op voor een adviesgesprek.
0523 – 28 27 26 | mail@vrieling.nl

Bronnen / Voetnoten:
1. Avans+ – Cyber risk management Basis.
2. Autoriteit Persoonsgegevens; NOS, 2020.
3. Avans+ – Cyber risk management Basis; IBM – Cost of a Data Breach Report 2024.
4. Avans+ – Cyber risk management Regulations.
5. ENISA – Cybersecurity Requirements 2023.
6. Europese Commissie – NIS2 Directive (2022).
7. Avans+ – Cyber risk management Basis.
8. Avans+ – De cyberverzekeringsmarkt; Markel productinformatie.