HUIJBREGTS
ict & cybersafety

WHITEPAPER

NIS2 & de Cyberbeveiligingswet

Wat betekent het voor jouw organisatie en hoe word je compliant?

Whitepaper | oktober 2026

Dronten & Emmeloord

INHOUD

01. Voorwoord 3

02. NIS2 in het kort 4

03. Valt jouw organisatie eronder? 5

04. De pijlers van de wet 8

05. Toezicht en sancties 11

06. In 8 stappen klaar voor NIS2 12

07. Veelgestelde vragen 13

08. Quick-scan checklist 14

09. Zo helpen wij je 15

10. Nuttige bronnen 16

Over deze whitepaper

Deze whitepaper is geschreven voor directies, ondernemers, IT-verantwoordelijken en security-officers die willen weten wat NIS2 en de Cyberbeveiligingswet concreet betekenen. We leggen uit wie onder de wet valt, welke plichten er gelden en hoe je stap voor stap aan de slag gaat. Achterin vind je een checklist waarmee je snel ziet waar je staat.

Stand van zaken: oktober 2026. De Cyberbeveiligingswet en het Cyberbeveiligingsbesluit zijn op 15 augustus 2026 in werking getreden.

HOOFDSTUK 01

VOORWOORD

Digitale veiligheid is geen IT-onderwerp meer. Het is een kwestie van continuïteit, van vertrouwen van klanten en van verantwoordelijkheid richting de samenleving.

Cyberaanvallen zijn de afgelopen jaren professioneler, gerichter en vaker ontwrichtend geworden. Ransomware legt productielijnen stil, phishing opent de deur naar klantdata en een storing bij één leverancier kan in één keer tientallen organisaties raken. Geopolitieke spanningen, verregaande digitalisering en de afhankelijkheid van cloud- en ketenpartners maken het risico alleen maar groter.

Daarom heeft de Europese Unie de NIS2-richtlijn opgesteld. In Nederland is die richtlijn omgezet in de **Cyberbeveiligingswet (Cbw)**, die sinds **15 augustus 2026** van kracht is. Ruim 8.000 organisaties in Nederland vallen direct onder de wet. Daarnaast krijgen veel mkb-bedrijven er indirect mee te maken, omdat hun klanten als ketenpartner eisen gaan stellen aan hun digitale veiligheid.

Bij Huijbregts ict & cybersafety merken we dat veel ondernemers en IT-verantwoordelijken met dezelfde vragen zitten: *Vallen wij eronder? Wat moeten we precies doen? En waar beginnen we?* Met deze whitepaper willen we die vragen helder en praktisch beantwoorden, zonder onnodig juridisch jargon.

Ons advies is eenvoudig: zie NIS2 niet als papieren verplichting, maar als een kans om je organisatie aantoonbaar weerbaarder te maken. De maatregelen die de wet vraagt, zoals risicoanalyse, multifactorauthenticatie, goede back-ups, patchmanagement en een geoefend incidentplan, zijn precies de maatregelen die je in de praktijk beschermen. Ook als je formeel niet onder de wet valt.

We wensen je veel leesplezier en denken graag met je mee.

Team Huijbregts ict & cybersafety
Dronten & Emmeloord

In het kort

- De **Cyberbeveiligingswet** is de Nederlandse uitwerking van NIS2 en vervangt de Wbni. Hij geldt sinds 15 augustus 2026.
- De wet geldt voor middelgrote en grote organisaties in **18 sectoren**, plus een aantal aanbieders ongeacht omvang.
- Je moet **zelf** vaststellen of je eronder valt. Een brief van de overheid hoef je niet af te wachten.
- Vier kernplichten: **registratie**, **zorgplicht**, **meldplicht** en **bestuurlijke verantwoordelijkheid**.
- Significante incidenten meld je in stappen: **24 uur, 72 uur en 1 maand**.
- Het bestuur is eindverantwoordelijk en kan persoonlijk worden aangesproken.

HOOFDSTUK 02

NIS2 IN HET KORT

NIS staat voor *Network and Information Security*. NIS2 is de tweede, flink uitgebreide versie van de Europese richtlijn die de digitale weerbaarheid van organisaties versterkt die belangrijk zijn voor de samenleving en de economie.

Het doel van NIS2 is één gemeenschappelijk, hoog niveau van cyberbeveiliging in de hele EU. Daarvoor legt de richtlijn de lat voor alle lidstaten gelijk: welke organisaties eronder vallen, welke maatregelen ze minimaal nemen, hoe ze incidenten melden en hoe toezichthouders mogen handhaven. Waar de AVG de bescherming van persoonsgegevens regelt, gaat NIS2 over de continuïteit en veiligheid van de diensten zelf.

Van NIS1 naar NIS2

De eerste NIS-richtlijn stamt uit 2016 en werd in Nederland uitgevoerd via de Wet beveiliging netwerk- en informatiesystemen (Wbni). Die richtlijn gold maar voor een beperkte groep aanbieders, en lidstaten gaven er elk een eigen invulling aan. NIS2 trekt dat recht en gaat een stuk verder:

Onderwerp	NIS1 / Wbni	NIS2 / Cyberbeveiligingswet
Reikwijdte	Beperkt aantal aangewezen vitale aanbieders en digitale dienstverleners	18 sectoren; alle middelgrote en grote organisaties in die sectoren, plus een aantal aanbieders ongeacht omvang
Wie bepaalt?	De overheid wees aanbieders aan	Organisaties stellen zelf vast of ze eronder vallen (zelfidentificatie)
Maatregelen	Algemene zorgplicht	Zorgplicht met tien minimale maatregelen, uitgewerkt in het Cyberbeveiligingsbesluit
Melden	Melding van incidenten met aanzienlijke gevolgen	Gefaseerde meldplicht: 24 uur, 72 uur en 1 maand
Bestuur	Geen expliciete rol	Bestuur keurt maatregelen goed, houdt toezicht, volgt training en is aanspreekbaar
Keten	Nauwelijks geregeld	Beveiliging van de toeleveringsketen is een verplicht onderdeel
Handhaving	Beperkt	Proactief en reactief toezicht, hoge boetes en persoonlijke maatregelen

De Cyberbeveiligingswet in Nederland

Een Europese richtlijn werkt pas als lidstaten hem omzetten in nationale wetgeving. In Nederland is dat de **Cyberbeveiligingswet (Cbw)**. Die vervangt de Wbni en is op **15 augustus 2026** in werking getreden (Staatsblad 2026, 187), nadat de Eerste Kamer op 7 juli 2026 had ingestemd. De wet wordt uitgewerkt in:

- het **Cyberbeveiligingsbesluit (Cbb)**, dat de zorgplicht concreet maakt: van beleid en risicomanagement tot toegangsbeleid, cryptografie en training;

- **ministeriële regelingen** met onder meer sectorale drempelwaarden die bepalen wanneer een incident significant is;
- voor een aantal digitale dienstverleners (zoals cloud, datacenters en managed service providers) daarnaast gedetailleerde **Europese uitvoeringsregels**.

Tegelijk met de Cbw is ook de **Wet weerbaarheid kritieke entiteiten** (Wwke) in werking getreden. Die implementeert de Europese CER-richtlijn en richt zich op de fysieke en organisatorische weerbaarheid van ongeveer 500 aangewezen kritieke organisaties. Voor de meeste lezers van deze whitepaper is de Cbw de belangrijkste wet.

Tijdlijn: van richtlijn naar wet

2016	Eerste Europese NIS-richtlijn aangenomen.
2018	De Wbni treedt in werking als Nederlandse uitvoering van NIS1.
2022 / 2023	NIS2 wordt vastgesteld en gepubliceerd en treedt op 16 januari 2023 in werking op EU-niveau.
17 okt 2024	Uiterste datum waarop lidstaten NIS2 hadden moeten omzetten. Nederland had meer tijd nodig.
7 juli 2026	De Eerste Kamer stemt in met de Cyberbeveiligingswet.
15 aug 2026	**Cyberbeveiligingswet en Cyberbeveiligingsbesluit in werking** (Stb. 2026, 187). De Wbni vervalt. Ook de Wwke (CER) treedt in werking.

HOOFDSTUK 03

VALT JOUW ORGANISATIE ERONDER?

De belangrijkste verandering ten opzichte van de oude regels: je wordt niet meer aangewezen, je moet **zelf vaststellen** of je organisatie onder de Cyberbeveiligingswet valt. Dat hangt af van drie vragen.

1 **In welke sector ben je actief?**

De wet onderscheidt sectoren met een zeer hoge kritikaliteit en overige kritieke sectoren (zie de tabel hieronder). Kijk niet alleen naar je hoofdactiviteit: ook een nevenactiviteit kan onder een sector vallen.

2 **Hoe groot is je organisatie?**

In principe valt een organisatie eronder als zij minimaal **middelgroot** is: 50 of meer medewerkers (fte), of een jaaromzet én balanstotaal van meer dan 10 miljoen euro. Let op: bij partner- en verbonden ondernemingen tellen de cijfers van de groep mee.

3 **Geldt er een uitzondering of juist een aanwijzing?**

Sommige aanbieders vallen eronder ongeacht hun omvang. Andersom kan een organisatie ook door de overheid worden aangewezen vanwege haar unieke rol in de samenleving.

De 18 sectoren

Sectoren met zeer hoge kritikaliteit (11)	Overige kritieke sectoren (7)
Energie (elektriciteit, gas, olie, warmte, waterstof, laadpalen)	Post- en koeriersdiensten
Vervoer (lucht, spoor, water, weg)	Afvalstoffenbeheer
Bankwezen	Vervaardiging, productie en distributie van chemische stoffen
Infrastructuur voor de financiële markt	Productie, verwerking en distributie van levensmiddelen
Gezondheidszorg (zorgaanbieders, laboratoria, farmacie, medische hulpmiddelen)	Vervaardiging (o.a. medische hulpmiddelen, computers, elektronica en optica, elektrische apparatuur, machines, voertuigen)
Drinkwater	Digitale aanbieders (online marktplaatsen, zoekmachines, sociale netwerken)
Afvalwater	Onderzoek
Digitale infrastructuur (o.a. DNS, cloud, datacenters, CDN, vertrouwensdiensten, communicatienetwerken)	
Beheer van ICT-diensten business-to-business (managed services en managed security services)	
Overheid	
Ruimtevaart	

Essentieel of belangrijk?

Organisaties die onder de wet vallen, zijn een **essentiële** of een **belangrijke** entiteit. De plichten zijn voor beide grotendeels gelijk; het verschil zit vooral in de manier van toezicht en de hoogte van de boetes.

Omvang	Sector met zeer hoge kritikaliteit	Overige kritieke sector
Groot 250 fte of meer, of omzet > EUR 50 mln en balanstotaal > EUR 43 mln	**Essentiële** entiteit	**Belangrijke** entiteit
Middelgroot 50 fte of meer, of omzet en balanstotaal > EUR 10 mln	**Belangrijke** entiteit	**Belangrijke** entiteit
Klein en micro minder dan 50 fte en omzet of balanstotaal tot EUR 10 mln	Valt in principe niet onder de wet, tenzij een uitzondering of aanwijzing geldt	Valt in principe niet onder de wet, tenzij aangewezen

Uitzonderingen op de omvangsregel

- Een aantal aanbieders valt **ongeacht omvang** onder de wet, zoals DNS-dienstverleners, registers voor topleveldomeinen, (gekwalificeerde) verleners van vertrouwensdiensten en aanbieders van openbare elektronische communicatienetwerken of -diensten.

- Overheidsorganisaties kunnen ook onder de wet vallen als ze kleiner zijn.
- De overheid kan een organisatie **aanwijzen** als zij de enige aanbieder is van een kritieke dienst, of als een verstoring grote gevolgen kan hebben voor de veiligheid of de economie.
- Voor financiële instellingen gaan de specifieke Europese regels voor digitale weerbaarheid in de financiële sector (DORA) voor op een groot deel van de plichten uit de Cbw.

Twijfel je? Gebruik de zelftest van de overheid

De Rijksoverheid en het NCSC bieden een online vragenlijst waarmee je nagaat of je organisatie onder de Cyberbeveiligingswet valt en in welke categorie. Leg de uitkomst en je redenering vast: dat laat later zien dat je bewust en zorgvuldig hebt beoordeeld.

Geen NIS2-plicht? Dan ben je er waarschijnlijk toch mee bezig

Ook als je organisatie te klein is of niet in een van de 18 sectoren actief is, kun je met NIS2 te maken krijgen. Organisaties die wél onder de wet vallen, moeten namelijk de risico's in hun **toeleveringsketen** beheersen. Ben jij leverancier, IT-partner, onderaannemer of logistiek dienstverlener van zo'n organisatie, dan kun je verwachten dat zij:

- beveiligingseisen opnemen in contracten en inkoopvoorwaarden;
- vragenlijsten sturen over onder meer MFA, back-ups, patchbeleid en incidentafhandeling;
- vragen om aantoonbaar bewijs, zoals beleidsdocumenten, een certificaat of auditrapport;
- afspraken maken over hoe snel je hen informeert als er bij jou een incident is.

Onze kijk

Voor veel mkb-bedrijven in Flevoland en de Noordoostpolder komt NIS2 niet via de toezichthouder, maar via de klant. Wie zijn basisbeveiliging aantoonbaar op orde heeft, wint vertrouwen en houdt opdrachten vast.

HOOFDSTUK 04

DE PIJLERS VAN DE WET

De Cyberbeveiligingswet rust op vier pijlers. Samen zorgen ze ervoor dat organisaties hun risico's kennen, passende maatregelen nemen, snel melden als het misgaat en dat de leiding er bovenop zit.

1	2	3	4
Registratieplicht	**Zorgplicht**	**Meldplicht**	**Bestuur**
Meld je organisatie aan bij het NCSC	Neem passende en evenredige maatregelen	Meld significante incidenten op tijd	Leiding keurt goed, ziet toe en wordt getraind

1. Registratieplicht

Iedere essentiële en belangrijke entiteit moet zich registreren in het nationale **entiteitenregister**, dat wordt beheerd door het **Nationaal Cyber Security Centrum (NCSC)**. Zo weet de overheid wie er onder de wet valt, kan zij organisaties gericht waarschuwen bij dreigingen en weet de toezichthouder wie hij moet controleren.

Bij registratie geef je onder meer je organisatienaam, sector en type dienst, adres- en contactgegevens (inclusief e-mailadres en telefoonnummer), je IP-adresreeksen en de EU-landen waarin je diensten levert door. Wijzigingen moet je tijdig doorgeven. Bereid je voor met de checklist van het NCSC en houd de gegevens centraal en actueel.

2. Zorgplicht

De zorgplicht verplicht je om **passende en evenredige** technische, operationele en organisatorische maatregelen te nemen om risico's voor je netwerk- en informatiesystemen te beheersen en de gevolgen van incidenten te beperken. 'Passend' betekent: afgestemd op jouw risico's, je omvang, de stand van de techniek en de kosten. De wet hanteert een *all-hazards*-benadering: niet alleen hackers, maar ook brand, stroomuitval, menselijke fouten en fysieke inbraak horen in je risicoanalyse.

NIS2 (artikel 21) noemt tien maatregelen die je minimaal moet afdekken. Het Cyberbeveiligingsbesluit werkt deze verder uit.

De tien minimale maatregelen

1. **Risicoanalyse en beveiligingsbeleid**
   Beleid voor risicoanalyse en de beveiliging van informatiesystemen, vastgesteld door de leiding.
2. **Incidentbehandeling**
   Procedures om incidenten te detecteren, te analyseren, in te dammen en op te lossen.
3. **Bedrijfscontinuïteit en crisisbeheer**
   Back-upbeheer, herstel na een calamiteit (disaster recovery) en een crisisorganisatie.
4. **Beveiliging van de toeleveringsketen**
   Risico's van leveranciers en dienstverleners beoordelen en afspraken vastleggen.
5. **Veilige aanschaf, ontwikkeling en onderhoud**
   Beveiliging bij inkoop, ontwikkeling en beheer van systemen, inclusief het omgaan met en bekendmaken van kwetsbaarheden.
6. **Effectiviteit beoordelen**
   Beleid en procedures om te toetsen of je maatregelen echt werken, bijvoorbeeld via audits en tests.
7. **Cyberhygiëne en training**
   Basismaatregelen zoals updates en sterke wachtwoorden, en regelmatige bewustwordingstraining voor iedereen.
8. **Cryptografie en encryptie**
   Beleid voor het gebruik van versleuteling van gegevens, opgeslagen en onderweg.
9. **Personeel, toegang en assets**
   Personeelsbeveiliging, toegangsbeleid (wie mag wat) en een actueel overzicht van bedrijfsmiddelen.
10. **MFA en beveiligde communicatie**
    Multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatie waar passend.

Zorgplicht is ook bewijsplicht

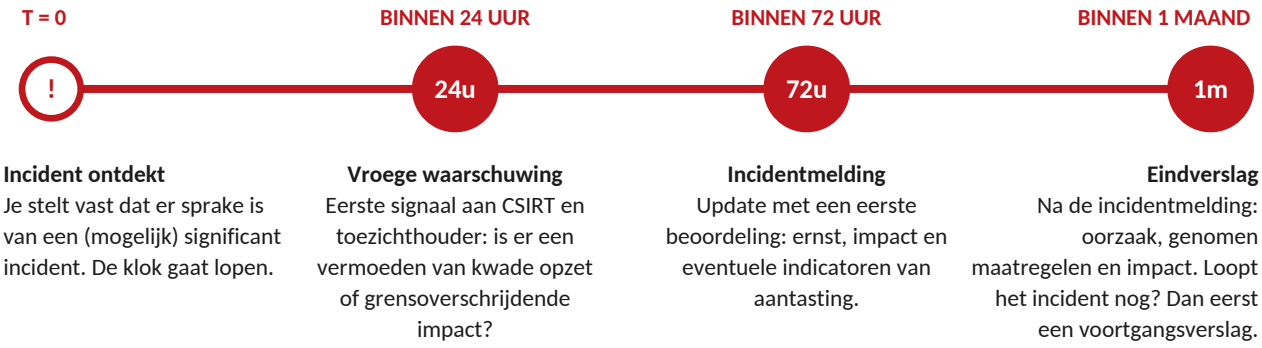
Maatregelen nemen is niet genoeg: je moet ook kunnen **aantonen** dat je ze hebt genomen en dat ze blijvend werken. Een eenmalige scan van vorig jaar overtuigt geen toezichthouder. Leg vast wat je doet, wie verantwoordelijk is, hoe vaak je test en wat de uitkomsten waren. Denk in een doorlopende cyclus van plannen, uitvoeren, controleren en verbeteren.

Het Cyberbeveiligingsbesluit in vogelvlucht

Het Cbb werkt de zorgplicht uit in thema's die je in je beleid terug moet laten komen: informatiebeveiligingsbeleid, risicomanagement, incidentbehandeling, bedrijfscontinuïteit en crisisbeheer, beveiliging van de toeleveringsketen, veilige aanschaf, ontwikkeling en onderhoud, beoordeling van de effectiviteit, cyberhygiëne en training, cryptografie, personeelsbeveiliging, toegangsbeleid en beheer van bedrijfsmiddelen.

3. Meldplicht

Gaat het mis, dan moet je een **significant incident** melden bij het **CSIRT** én bij de **bevoegde toezichthouder**. Dat doe je via het meldportaal van het NCSC. Een incident is significant als het je dienstverlening ernstig verstoort of tot aanzienlijke financiële schade leidt, of als het anderen aanzienlijke materiële of immateriële schade kan berokkenen. In ministeriële regelingen staan per sector drempelwaarden die bepalen wanneer dat het geval is.



- Op verzoek van het CSIRT of de toezichthouder lever je tussentijds een **voortgangsverslag**.
- Waar nodig informeer je ook de **afnemers** van je dienst over het incident en over maatregelen die zij zelf kunnen nemen.
- Zijn er persoonsgegevens betrokken? Dan geldt daarnaast de meldplicht datalekken uit de AVG: binnen 72 uur bij de **Autoriteit Persoonsgegevens**. Dat zijn twee aparte meldingen.
- Ook incidenten die niet significant zijn, of bijna-incidenten, kun je vrijwillig melden. Je krijgt dan hulp en draagt bij aan een beter dreigingsbeeld.

Tip: bereid je melding nu al voor

- Leg in je incidentresponsplan vast wie beslist dat een incident significant is en wie meldt.
- Zet contactgegevens en inloggegevens voor het meldportaal klaar, ook offline.
- Werk conceptteksten uit voor de vroege waarschuwing en de incidentmelding.
- Ga ervan uit dat je e-mail en netwerk tijdens een incident niet werken: regel een alternatief.

4. Bestuurlijke verantwoordelijkheid

Cyberbeveiliging hoort onder NIS2 nadrukkelijk op de agenda van de directie of het bestuur. De leiding moet de maatregelen voor risicobeheer **goedkeuren**, toezien op de **uitvoering** en zelf een passende **training** volgen om risico's te kunnen beoordelen. Het is gebruikelijk en verstandig om medewerkers ook regelmatig te trainen.

Schiet het bestuur tekort, dan kunnen bestuurders daar **persoonlijk op worden aangesproken**. Bij essentiële entiteiten kan de toezichthouder in het uiterste geval zelfs een bestuurder tijdelijk verbieden een leidinggevende functie uit te oefenen. Uitvoerende taken kun je beleggen bij IT of een externe partner, maar de eindverantwoordelijkheid blijft bij de top.

HOOFDSTUK 05

TOEZICHT EN SANCTIES

Met de Cyberbeveiligingswet krijgt toezicht echt tanden. Per sector is een toezichthouder aangewezen, zoals de Rijksinspectie Digitale Infrastructuur (RDI) voor onder meer digitale infrastructuur en ICT-dienstverlening. Het CSIRT ondersteunt bij incidenten; de toezichthouder controleert en handhaaft.

	Essentiële entiteit	Belangrijke entiteit
Soort toezicht	**Proactief** (vooraf): de toezichthouder kan op eigen initiatief controleren	**Reactief** (achteraf): toezicht naar aanleiding van signalen, incidenten of aanwijzingen
Instrumenten	Inspecties ter plaatse en op afstand, audits, beveiligingsscans, opvragen van informatie en bewijs	Vergelijkbare instrumenten, ingezet als er aanleiding voor is
Maximale boete*	**EUR 10 miljoen** of **2%** van de wereldwijde jaaromzet (het hoogste bedrag)	**EUR 7 miljoen** of **1,4%** van de wereldwijde jaaromzet (het hoogste bedrag)
Persoonlijke maatregelen	Mogelijk tijdelijk verbod op leidinggevende functie voor een bestuurder	Aanspreken van het bestuur op zijn verantwoordelijkheid

* Maxima zoals vastgelegd in de NIS2-richtlijn.

Wat kan de toezichthouder doen?

Boetes zijn het sluitstuk. Meestal begint handhaving met minder zware middelen, die wel degelijk impact hebben:

- een **waarschuwing** of een verzoek om informatie en bewijsstukken;
- een **bindende aanwijzing** om binnen een bepaalde termijn maatregelen te nemen;
- een **last onder dwangsom**: betalen zolang je de overtreding niet herstelt;
- de verplichting om afnemers te informeren over een dreiging of tekortkoming;
- een **bestuurlijke boete**, met de maxima hierboven.

Meer dan een boete

De grootste schade van een cyberincident zit zelden in de boete. Stilstand, herstelkosten, verloren klantvertrouwen en reputatieschade wegen vaak zwaarder. Bovendien kan een incident met persoonsgegevens ook tot een AVG-onderzoek leiden.

Goed nieuws: wie aantoonbaar werkt aan zijn maatregelen, staat sterk richting toezichthouder, klanten en verzekeraar.

HOOFDSTUK 06

IN 8 STAPPEN KLAAR VOOR NIS2

NIS2 voer je niet in met een rondmail met do's en don'ts. Het is een samenhangend programma dat je organisatie blijvend weerbaarder maakt. Met deze acht stappen breng je structuur aan.

1

Stel vast of en hoe je eronder valt

Bepaal sector, omvang en of een uitzondering geldt. Ben je essentieel of belangrijk? Of krijg je vooral via klanten met eisen te maken? Leg je onderbouwing vast en **registreer je** bij het NCSC als je onder de wet valt.

2

Maak het een bestuursonderwerp

Wijs een eigenaar aan, reserveer budget en capaciteit en zorg dat directie of bestuur de benodigde training volgt. Spreek af hoe vaak het bestuur over de voortgang wordt geïnformeerd.

3

Breng je organisatie en IT in kaart

Welke processen en diensten zijn kritiek? Inventariseer hardware, software, cloudomgevingen, datastromen, toegangspunten (thuiswerken, mobiele apparaten, externe koppelingen) en de leveranciers waarvan je afhankelijk bent.

4

Voer een risicoanalyse en nulmeting uit

Breng dreigingen, kwetsbaarheden en de impact op je dienstverlening in kaart. Vergelijk je huidige situatie met de tien maatregelen en het Cyberbeveiligingsbesluit en prioriteer de gaten op risico.

5

Leg beleid en procedures vast

Stel een informatiebeveiligingsbeleid op, met onder meer toegangsbeleid, back-up- en continuïteitsbeleid, cryptografiebeleid, leveranciersbeleid en een incidentresponsplan. Houd het praktisch en laat het bestuur het goedkeuren.

6

Neem de technische basismaatregelen

Voer MFA in voor alle accounts, regel patchmanagement, maak back-ups volgens de 3-2-1-regel (waarvan één kopie offline of onveranderbaar), segmenteer je netwerk, versleutel gevoelige data en zorg voor monitoring en logging. Vervang systemen die geen beveiligingsupdates meer krijgen.

7

Organiseer incidentrespons en meldplicht

Leg vast wie wat doet bij een incident, wie beslist en wie meldt. Bereid meldteksten voor, regel een communicatiematrix voor klanten en ketenpartners en **oefen**: simuleer een incident en test of je back-ups echt terug te zetten zijn.

8

Borg, test en verbeter continu

Train medewerkers regelmatig, laat periodiek kwetsbaarheidsscans of penetratietests uitvoeren, beoordeel leveranciers en rapporteer aan het bestuur. Evalueer, verbeter en plan de volgende ronde in. Compliance is geen eindpunt.

HOOFDSTUK 07

VEELGESTELDE VRAGEN

V We zijn al ISO 27001-gecertificeerd. Zijn we dan klaar?

Je hebt een flinke voorsprong: een informatiebeveiligingsmanagementsysteem (ISMS) met risicoanalyses, beleid en audits dekt een groot deel van de zorgplicht af. Hetzelfde geldt voor NEN 7510 in de zorg en de BIO bij de overheid. Een certificaat betekent echter niet automatisch dat je voldoet. Controleer vooral de meldplicht met de korte termijnen, de registratie, de rol en training van het bestuur, de eisen aan je toeleveringsketen en of de scope van je certificaat alle relevante diensten omvat.

V We vallen niet onder NIS2. Moeten we dan niets doen?

Wettelijk niet, maar het is wel verstandig. Klanten die onder de wet vallen, gaan eisen stellen aan hun leveranciers. En de maatregelen beschermen je gewoon tegen de dreigingen van vandaag. Gebruik NIS2 als kompas voor je eigen basisbeveiliging.

V We zijn een klein bedrijf, maar leveren aan een zorginstelling of gemeente. Wat betekent dat?

Je valt zelf waarschijnlijk niet onder de wet, maar je klant moet zijn toeleveringsketen wel beveiligen. Verwacht vragenlijsten, contractuele afspraken en verzoeken om bewijs. Wie die vragen snel en overtuigend kan beantwoorden, heeft een voorsprong.

V Is NIS2 een taak voor de IT-afdeling of voor de directie?

Beide. IT voert veel maatregelen uit, maar de wet legt de eindverantwoordelijkheid nadrukkelijk bij het bestuur. Bovendien raakt NIS2 ook HR (personeelsbeveiliging, training), inkoop (leveranciers) en communicatie (incidenten).

V Moeten we elk incident melden?

Nee, alleen **significante** incidenten zijn meldplichtig. Of een incident significant is, hangt af van de impact en van de drempelwaarden voor jouw sector. Leg vooraf vast hoe je dat beoordeelt, zodat je bij een incident niet kostbare uren kwijt bent.

V Wat als er bij een incident ook persoonsgegevens zijn gelekt?

Dan meld je het incident onder de Cyberbeveiligingswet bij het CSIRT en de toezichthouder, en daarnaast het datalek binnen 72 uur bij de Autoriteit Persoonsgegevens. Neem beide routes op in je incidentresponsplan.

V Kunnen we NIS2 uitbesteden aan onze IT-partner?

Uitvoerende taken zoals beheer, monitoring, back-up en patchmanagement kun je prima uitbesteden. De verantwoordelijkheid voor de keuzes en het toezicht daarop blijft bij jouw organisatie. Maak dus heldere afspraken en laat je partner rapporteren.

V De wet geldt sinds 15 augustus 2026. Zijn we te laat?

Als je onder de wet valt, gelden de plichten nu. Wacht dus niet langer: registreer je, zorg dat je incidenten kunt melden en werk aantoonbaar aan je maatregelen. Een concreet plan met prioriteiten is al een belangrijke stap.

HOOFDSTUK 08

QUICK-SCAN CHECKLIST

Hoe staat jouw organisatie ervoor? Loop de vragen hieronder door. Elke vraag die je niet met een overtuigd **ja** kunt beantwoorden, is een actiepunt.

TOEPASSELIJKHEID & BESTUUR

- ☐ We hebben vastgesteld of we onder de Cyberbeveiligingswet vallen, en deze beoordeling is vastgelegd.
- ☐ We weten of we een essentiële of belangrijke entiteit zijn, of welke klanten ons als ketenpartner eisen opleggen.
- ☐ We zijn geregistreerd bij het NCSC en onze gegevens zijn actueel (indien van toepassing).
- ☐ Directie of bestuur heeft het beveiligingsbeleid goedgekeurd en heeft een cybersecuritytraining gevolgd.

RISICO'S & BELEID

- ☐ We hebben een actueel overzicht van kritieke processen, systemen, data en leveranciers.
- ☐ We voeren minimaal jaarlijks een risicoanalyse uit en hebben een plan van aanpak met prioriteiten.
- ☐ We hebben vastgelegd beleid voor informatiebeveiliging, toegang, back-up en cryptografie.

TECHNIEK

- ☐ Multifactorauthenticatie staat aan voor alle gebruikers en zeker voor beheerders en externe toegang.
- ☐ Updates en patches worden centraal en tijdig uitgerold; verouderde systemen zijn vervangen of afgeschermd.
- ☐ We maken back-ups volgens de 3-2-1-regel, met een offline of onveranderbare kopie, en testen het terugzetten.
- ☐ Systemen worden gemonitord en logs worden bewaard, zodat we afwijkingen snel zien.

INCIDENTEN & CONTINUÏTEIT

- ☐ Er is een incidentresponsplan met rollen, beslisbevoegdheden en contactgegevens (ook offline beschikbaar).
- ☐ We kunnen een vroege waarschuwing binnen 24 uur en een incidentmelding binnen 72 uur doen.
- ☐ We hebben het afgelopen jaar een incident of uitwijk geoefend.

MENSEN & KETEN

- ☐ Alle medewerkers volgen regelmatig een awareness-training, inclusief herkennen van phishing.
- ☐ We beoordelen de beveiliging van onze belangrijkste leveranciers en hebben afspraken in contracten vastgelegd.

Twijfel bij een of meer vragen? Dan is een NIS2 quick-scan een logische volgende stap. Samen zetten we de antwoorden om in een concreet en geprioriteerd actieplan.

HOOFDSTUK 09

ZO HELPEN WIJ JE

Huijbregts ict & cybersafety is jouw ICT- en securitypartner uit de regio, met vestigingen in Dronten en Emmeloord. We combineren dagelijks IT-beheer met cybersecurity. Zo vertalen we de eisen uit de wet naar maatregelen die passen bij jouw organisatie: praktisch, betaalbaar en aantoonbaar.

NIS2 quick-scan en risicoanalyse

We stellen samen vast of en hoe NIS2 op jou van toepassing is, brengen je huidige situatie in kaart en leveren een helder overzicht van de gaten en prioriteiten.

Beleid en documentatie

We helpen bij het opstellen van informatiebeveiligingsbeleid, toegangsbeleid, back-upbeleid en een incidentresponsplan dat in de praktijk werkt, zodat je kunt aantonen wat je doet.

Technische maatregelen

Van multifactorauthenticatie en veilige back-ups tot patchmanagement, endpointbeveiliging, netwerksegmentatie en versleuteling: we richten het in en houden het bij.

Monitoring en 24/7 bereikbaar

We houden je omgeving in de gaten en zijn 24/7 bereikbaar. Zo worden afwijkingen snel opgemerkt en opgepakt.

Moderne en veilige werkplek

Als Microsoft gecertificeerd partner richten we een moderne werkplek in waarbij de beschikbare beveiligingsmogelijkheden goed zijn geconfigureerd en beheerd.

Cybersecurity awareness training

Medewerkers zijn je eerste verdedigingslinie. Met praktische trainingen leren ze phishing en andere risico's herkennen. Ook voor directie en bestuur.

Ondersteuning bij incidenten

Gaat het mis, dan staan we naast je: van indammen en herstellen tot het vastleggen van de informatie die je nodig hebt voor je meldingen.

Leveranciers- en ketenbeoordeling

We helpen je leveranciers te beoordelen en beveiligingsafspraken vast te leggen. En sta je zelf als leverancier voor vragen van klanten? Dan helpen we je die goed te beantwoorden.

Plan een vrijblijvend gesprek of NIS2 quick-scan

Bel **088 100 5100** of mail naar **info@huijbregtsgroep.nl**. We komen graag bij je langs in Dronten, Emmeloord en omgeving.

HOOFDSTUK 10

NUTTIGE BRONNEN

Wil je verder lezen of zelf aan de slag? Deze onafhankelijke overheidsbronnen zijn betrouwbaar en actueel.

Bron	Waarvoor?
Nationaal Cyber Security Centrum (NCSC)	Informatie over de Cyberbeveiligingswet, registratie in het entiteitenregister, het meldportaal en adviezen en dreigingsinformatie.
Rijksoverheid	Achtergrond bij de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit, en de online zelftest of je organisatie onder de wet valt.
Digital Trust Center	Praktische informatie, tools en zelftests voor ondernemers, waaronder handvatten voor een incidentresponsplan en het testen van back-ups.
Autoriteit Persoonsgegevens	Informatie over de AVG en het melden van datalekken.
Sectorale toezichthouders, zoals de RDI	Informatie over toezicht en handhaving in jouw sector.
ENISA	Het Europese agentschap voor cyberbeveiliging, met Europese richtsnoeren bij NIS2.

Begrippenlijst

- **Cbw** - Cyberbeveiligingswet, de Nederlandse uitwerking van NIS2.
- **Cbb** - Cyberbeveiligingsbesluit, waarin de zorgplicht en andere plichten worden uitgewerkt.
- **CSIRT** - Computer Security Incident Response Team; ontvangt meldingen en helpt bij incidenten.
- **Essentiële / belangrijke entiteit** - de twee categorieën organisaties onder de wet.
- **Significant incident** - een incident met ernstige gevolgen dat binnen de wettelijke termijnen gemeld moet worden.
- **Wwke** - Wet weerbaarheid kritieke entiteiten, de Nederlandse uitwerking van de CER-richtlijn.
- **MFA** - multifactorauthenticatie: inloggen met een extra factor naast een wachtwoord.

HUIJBREGTS
ict & cybersafety

Klaar voor de volgende stap?

Neem contact met ons op voor een vrijblijvend gesprek of een NIS2 quick-scan.
We denken graag met je mee, dichtbij en in begrijpelijke taal.

ALGEMEEN

088 100 5100

info@huijbregtsgroep.nl

www.huijbregtsgroep.nl

VESTIGING DRONTEN

Haringweg 25
8251 RR Dronten
T 0321-382939

VESTIGING EMMELOORD

Dukaat 17
8305 BC Emmeloord
T 0527-610123

Disclaimer - Deze whitepaper is bedoeld als algemene, informatieve uitleg en is geen juridisch advies. De inhoud geeft de stand van zaken weer in oktober 2026 (Cyberbeveiligingswet en Cyberbeveiligingsbesluit, in werking sinds 15 augustus 2026). Wet- en regelgeving, sectorale drempelwaarden en uitleg door toezichthouders kunnen wijzigen. Raadpleeg voor jouw specifieke situatie altijd de actuele informatie van de bevoegde instanties of een juridisch adviseur. © 2026 Huijbregts ict & cybersafety.