GIDS

De complete gids voor NIS2 compliance begeleiding

Cyberbeveiligingswet, zorgplicht, kosten, implementatie, boetes en bestuurdersaansprakelijkheid. Met actuele Nederlandse marktdata.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De Cyberbeveiligingswet komt eraan. Dit zijn de feiten die je moet kennen.

~10.000

Nederlandse bedrijven vallen direct onder de Cyberbeveiligingswet (NIS2)

Digitale Overheid [1]

EUR 10M

Maximale boete voor essentieel bedrijf, of 2% van de wereldwijde jaaromzet

NIS2-richtlijn [2]

12–22%

Verhoging ICT-beveiligingsuitgaven nodig om aan NIS2 te voldoen

PwC [3]

Q2 2026

Verwachte inwerkingtreding Cyberbeveiligingswet in Nederland

Digitale Overheid [1]

121+

Unieke ransomware-incidenten in Nederland in 2024

NCSC / Project Melissa [4]

77%

van het MKB heeft in de afgelopen 2 jaar te maken gehad met cybercrime

Vodafone Business [5]

EUR 270K

Gemiddelde schade per cyberincident voor het MKB in Nederland

Verzekercyber.nl [6]

24 uur

Meldplicht: eerste melding binnen 24 uur na significant incident

NIS2 art. 23 [2]

1. Wat is NIS2?

NIS2 is de Europese richtlijn die cybersecurity verplicht maakt voor bedrijven in kritieke sectoren. In Nederland wordt dit de Cyberbeveiligingswet.

De Network and Information Security Directive 2 (NIS2) is de opvolger van de eerste NIS-richtlijn uit 2016. Waar NIS1 alleen de allergrootste vitale sectoren raakte, trekt NIS2 het bereik veel breder: 18 sectoren, kleinere bedrijven en de hele toeleveringsketen [1].

In Nederland wordt NIS2 omgezet in de Cyberbeveiligingswet (Cbw), die de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangt. De verwachte inwerkingtreding is Q2 2026 [1].

WAT VERANDERT ER CONCREET?

- **Breder bereik** -- Van alleen vitale infrastructuur naar 18 sectoren, inclusief MKB-leveranciers
- **Zorgplicht** -- 10 verplichte beveiligingsmaatregelen, aantoonbaar geimplementeerd
- **Meldplicht** -- Significante incidenten melden binnen 24 uur (eerste melding), 72 uur (beoordeling) en 1 maand (eindrapport)
- **Bestuurlijke verantwoordelijkheid** -- Bestuurders zijn persoonlijk aansprakelijk en kunnen geschorst worden
- **Ketenverantwoordelijkheid** -- Je bent verantwoordelijk voor de cybersecurity van je leveranciers

> **NIS2 is geen IT-project**
>
> NIS2 raakt de hele organisatie: governance, risicomanagement, HR (training), juridisch (meldplicht), inkoop (leveranciersbeoordeling) en uiteraard IT. Behandel het als een organisatiebreed compliance-traject, niet als een technisch project [7].

2. Val je onder de Cyberbeveiligingswet?

NIS2 maakt onderscheid tussen essentieel en belangrijk. De verplichtingen zijn vergelijkbaar, het toezicht verschilt.

ESSENTIEEL VS BELANGRIJK

KENMERK	ESSENTIEEL	BELANGRIJK
Sectoren	Energie, transport, bankwezen, gezondheid, drinkwater, digitale infrastructuur, overheid, ruimtevaart	Post, afval, chemie, voeding, productie, digitale aanbieders, onderzoek
Bedrijfsgrootte	Groot (250+ medewerkers of >EUR 50M omzet)	Middelgroot (50+ medewerkers of >EUR 10M omzet)
Toezicht	Proactief: toezichthouder controleert actief	Reactief: controle na incidenten of meldingen
Maximale boete	EUR 10.000.000 of 2% wereldwijde omzet	EUR 7.000.000 of 1,4% wereldwijde omzet

LET OP: KETENEFFECT

Ook als je bedrijf niet direct onder NIS2 valt, kun je indirect geraakt worden. Grote opdrachtgevers in scope moeten hun leveranciers beoordelen op cybersecurity. Als ketenpartner kun je de facto verplicht worden om NIS2-niveau te halen om contracten te behouden [8].

De overheid biedt een gratis NIS2 Quickscan aan op regelhulpenvoorbedrijven.nl waarmee je in 10 minuten kunt checken of jouw organisatie in scope valt [9].

3. De 10 verplichte maatregelen

NIS2 schrijft 10 beveiligingsmaatregelen voor. Dit is geen keuzemenu -- alle 10 zijn verplicht.

#	MAATREGEL	WAT HET INHOUDT
1	**Risicoanalyse en beveiligingsbeleid**	Structureel risicobeheer voor je informatiesystemen
2	**Incidentenbehandeling**	Detectie, respons, herstel en rapportage van incidenten
3	**Bedrijfscontinuiteit**	Backup-strategie, disaster recovery, crisisbeheer
4	**Beveiliging toeleveringsketen**	Leveranciers en dienstverleners beoordelen op cybersecurity
5	**Beveiliging bij verwerving en ontwikkeling**	Secure development, vulnerability handling bij inkoop en ontwikkeling
6	**Effectiviteit beoordelen**	Testen en auditen van je maatregelen: werkt wat je doet?
7	**Cyberhygiene en training**	Awareness-programma, basispraktijken voor alle medewerkers
8	**Cryptografiebeleid**	Versleuteling van data in rust en in transit, sleutelbeheer
9	**Toegangsbeleid**	Identity & access management, MFA, privileged access management
10	**Asset management**	Inventarisatie en classificatie van je systemen en data

TIP

Begin met maatregel 1 (risicoanalyse) en maatregel 10 (asset management). Als je niet weet wat je hebt en waar je risico's liggen, kun je de overige 8 maatregelen niet goed invullen.

MELDPLICHT BIJ INCIDENTEN

MELDING	TERMIJN	INHOUD
Eerste melding	Binnen 24 uur	Indicatie van een significant incident
Tussentijdse update	Binnen 72 uur	Eerste beoordeling: ernst, impact, indicatoren

MELDING	TERMIJN	INHOUD
Eindrapport	Binnen 1 maand	Volledige beschrijving, oorzaak, genomen maatregelen

4. Wat kost NIS2 compliance?

De kosten hangen af van je huidige volwassenheidsniveau, je bedrijfsgrootte en de sector waarin je opereert.

EENMALIGE IMPLEMENTATIEKOSTEN

BEDRIJFSGROOTTE	EENMALIG	STRUCTUREEL PER JAAR	TOELICHTING
Klein MKB (10–50 pers.)	EUR 5.000--15.000	EUR 2.000--5.000	Quickscan, basisbeleid, awareness
Middelgroot MKB (50–250 pers.)	EUR 15.000--50.000	EUR 5.000--20.000	Gap-analyse, beleid, technische maatregelen
Groot bedrijf (250+ pers.)	EUR 44.400 gemiddeld	EUR 15.000--50.000+	Volledige implementatie, governance, audits

Organisaties moeten hun ICT-beveiligingsuitgaven met 12--22% verhogen om aan NIS2 te voldoen. Bij 95% van de organisaties moet budget worden herverdeeld uit andere bedrijfsonderdelen [3].

KOSTENCOMPONENTEN

COMPONENT	KOSTEN
NIS2 Quickscan	EUR 1.250--2.500
Gap-analyse (uitgebreid)	EUR 2.000--10.000
Beleidsvorming	EUR 3.000--15.000
Technische maatregelen	EUR 5.000--50.000+
Training en awareness	EUR 1.000--5.000/jaar
Externe begeleiding	EUR 150--250/uur
Certificering / audit	EUR 3.000--15.000

De werkelijke kost van niets doen

Een gemiddeld cyberincident kost het MKB EUR 270.000 [6]. De maximale NIS2-boete is EUR 10.000.000 [2]. 60% van kleine bedrijven gaat failliet binnen 6 maanden na een ernstige aanval [10]. De investering in compliance is een fractie van het alternatief.

5. Het implementatietraject

NIS2 compliance is geen eenmalig project. Het is een doorlopend proces van verbeteren, meten en bijsturen.

1 Quickscan en scope-bepaling

WEEK 1--2

Bepaal of je direct of indirect onder NIS2 valt. Gebruik de gratis overheids-quickscan of laat een NIS2-scan uitvoeren door een specialist.

2 Gap-analyse

WEEK 3--6

Breng je huidige situatie in kaart tegen de 10 NIS2-maatregelen. Identificeer tekortkomingen en prioriteer op risico.

3 Risicoanalyse

WEEK 4--8

Voer een formele risicoanalyse uit op je informatiesystemen. Dit is maatregel 1 van NIS2 en de basis voor alle vervolgstappen.

4 Beleid en governance

WEEK 6--12

Ontwikkel het benodigde beleid: informatiebeveiligingsbeleid, incident response plan, backup-beleid, toegangsbeleid, leveranciersbeleid.

5 Technische implementatie

WEEK 8--20

Implementeer de technische maatregelen: MFA, encryptie, monitoring, backup, netwerksegmentatie. Prioriteer op basis van de risicoanalyse.

6 Training en awareness

DOORLOPEND

Train bestuurders op hun verantwoordelijkheden. Rol awareness-programma uit voor alle medewerkers. NIS2 vereist aantoonbare cyberhygiene.

7 Testen en valideren

WEEK 16--24

Test je maatregelen: penetratietest, incident response oefening, backup-restore test. NIS2 eist dat je aantoont dat je maatregelen werken.

8

Continue verbetering

DOORLOPEND

Richt een PDCA-cyclus in. Beoordeel periodiek, stel bij, documenteer. NIS2 is geen eenmalig project maar een doorlopend proces.

6. Boetes en bestuurdersaansprakelijkheid

NIS2 legt de verantwoordelijkheid voor cybersecurity expliciet in de bestuurskamer. Met persoonlijke consequenties.

SANCTIES BIJ NON-COMPLIANCE

SANCTIE	ESSENTIEEL	BELANGRIJK
Maximale boete	EUR 10.000.000 of 2% wereldwijde omzet	EUR 7.000.000 of 1,4% wereldwijde omzet
Last onder dwangsom	Ja	Ja
Waarschuwing	Ja	Ja
Bestuurder schorsen	Ja	Nee

PERSOONLIJKE AANSPRAKELIJKHEID

Onder NIS2 moet iedere bestuurder de beveiligingsmaatregelen goedkeuren en toezicht houden op de uitvoering. Bij nalatigheid kan de bestuurder persoonlijk aansprakelijk worden gesteld. Toezichthouders kunnen bestuurders van essentiele entiteiten zelfs schorsen [11].

Dit is niet theoretisch. De Europese Commissie heeft de richtlijn bewust zo ontworpen dat cybersecurity geen IT-kwestie meer is, maar een bestuurskwestie. Het argument "dat is iets van IT" is onder NIS2 juridisch onhoudbaar [12].

7. NIS2 en DORA: hoe ze samenhangen

NIS2 en DORA zijn twee Europese wetten die allebei over cybersecurity gaan, maar met een ander bereik. Ze vullen elkaar aan.

KENMERK	NIS2	DORA
Type wetgeving	Richtlijn (omzetting in nationale wet)	Verordening (direct toepasbaar)
Scope	18 sectoren, breed	Financiele sector specifiek
Van kracht	Q2 2026 (NL)	17 januari 2025
Bij overlap	NIS2 wijkt	DORA gaat voor (lex specialis)
Focus	Risicomanagement, meldplicht, governance	Digitale operationele weerbaarheid

Als je in de financiele sector opereert, voldoe je primair aan DORA. NIS2 kan aanvullende verplichtingen opleggen waar DORA niet in voorziet. Buiten de financiele sector geldt alleen NIS2 [13].

> **Synergie met AVG**
>
> Veel technische en organisatorische maatregelen voor NIS2 dragen direct bij aan betere AVG-compliance. Door beide trajecten te integreren, voorkom je dubbel werk en bespaar je kosten [14].

8. Veelgemaakte fouten

De meeste organisaties maken dezelfde fouten bij NIS2-implementatie. Hier zijn de tien valkuilen die je kunt vermijden.

#	FOUT	WAAROM HET FOUT GAAT
1	**Compliance theater**	Beleid op papier, maar geen uitvoering in de dagelijkse praktijk. NIS2 vereist aantoonbare implementatie [7]
2	**Te laat beginnen**	NIS2-implementatie kost 6--12 maanden. Wie nu nog niet begonnen is, loopt achter de feiten aan
3	**Alleen techniek**	NIS2 vraagt ook governance, processen en cultuurverandering. Een firewall is geen compliance
4	**CISO zonder mandaat**	De CISO als "eigenaar van alles" zonder budget of besluitrecht. Dat is afschuiven, geen governance
5	**Documentatie onderschatten**	Geen bewijs = geen compliance. Achteraf evidence verzinnen leidt tot gaten in je systeem
6	**Keten negeren**	Leveranciers niet beoordelen op cybersecurity, terwijl NIS2 ketenverantwoordelijkheid expliciet vereist
7	**Eenmalig project**	NIS2 is een doorlopend proces. Zonder PDCA-cyclus verval je binnen een jaar
8	**Te breed beginnen**	Alles tegelijk willen aanpakken leidt tot verlamming. Focus op hoogste risico's eerst
9	**Meldplicht onderschatten**	Binnen 24 uur melden vereist een geoefend incident response team. Niet iets dat je improviseert
10	**Geen bestuurderscommitment**	Zonder budget en draagvlak van boven strandt elk NIS2-traject

TIP

De grootste valkuil voor MKB: "Wij zijn te klein voor NIS2." Ook als je niet direct in scope valt, kunnen je opdrachtgevers NIS2-niveau eisen als ketenpartner. Bereid je voor, ook als je twijfelt.

9. Subsidies en financiering

De overheid biedt financiele ondersteuning voor MKB-bedrijven die hun cybersecurity willen verbeteren.

REGELING	BEDRAG	VOORWAARDEN
Mijn Cyberweerbare Zaak (RVO)	50% subsidie, max EUR 1.250	MKB, eenmalig per bedrijf
SECURE-project (EU)	Tot EUR 30.000	MKB in de EU, gericht op cybersecurity
NIS2 Quality Mark	Vanaf EUR 1.200/jaar (met partnerkorting)	Toeleveranciers, aantoonbare compliance
Branchespecifieke fondsen	Variabel	Via brancheverenigingen

Het Digital Trust Center (DTC) van het Ministerie van Economische Zaken biedt gratis tools, checklists en informatie specifiek voor het MKB. Dit is een goed startpunt als je nog moet beginnen met NIS2-voorbereiding [15].

> **Tip: combineer subsidies**
>
> Je kunt de RVO-subsidie gebruiken voor een NIS2 Quickscan (EUR 1.250), zodat je effectief maar EUR 625 betaalt voor een eerste compliance-check. Begin daar en gebruik de resultaten om een gerichte business case op te bouwen voor verdere investering.

10. Trends 2025--2026

Het NIS2-landschap ontwikkelt zich snel. Dit zijn de ontwikkelingen die je moet kennen.

WETGEVING EN REGULERING

- **Cyberbeveiligingswet (NL):** Verwachte inwerkingtreding Q2 2026. Na inwerkingtreding volgt handhaving [1]
- **Europese Commissie amendementen:** Op 20 januari 2026 zijn wijzigingen voorgesteld voor meer juridische duidelijkheid en vereenvoudiging [16]
- **ICT Supply Chain Security Toolbox:** EU-brede aanpak voor cybersecurity in toeleveringsketens [16]
- **Convergentie NIS2-DORA-CRA-AI Act:** Integraal Europees kader voor digitale veiligheid

MARKT EN TECHNOLOGIE

- **Van reactief naar preventief:** Nieuwe wetgeving focust op preventie, transparantie en samenwerking
- **Tekort cybersecurity-professionals:** Groeiende vraag, gelijkblijvend aanbod -- managed services als alternatief
- **Automatisering compliance:** Tools voor continue monitoring en rapportage winnen terrein
- **Ketenverantwoordelijkheid groeit:** Steeds meer grote bedrijven eisen NIS2-compliance van leveranciers
- **Bestuurlijke aansprakelijkheid als driver:** Boardroom awareness groeit door persoonlijke consequenties

WAT BETEKENT DIT VOOR JOU?

- Begin nu met voorbereiding als je dat nog niet hebt gedaan -- de wet komt eraan
- Informeer je bestuurders over hun persoonlijke aansprakelijkheid
- Beoordeel je leveranciers -- ketenverantwoordelijkheid is een van de 10 maatregelen
- Overweeg managed compliance services als je geen interne expertise hebt
- Gebruik subsidies -- de overheid helpt MKB-bedrijven financieel

Bronnenlijst

[1] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2-richtlijn). https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[2] **NIS2-richtlijn** -- Boetes en sancties. https://kynexis.nl/nis2-boetes-cyberbeveiligingswet-uitgelegd/

[3] **PwC** -- Nieuwe Europese richtlijn NIS2: strengere eisen cybersecurity. https://www.pwc.nl/nl/actueel-en-publicaties/themas/risk-regulation/nieuwe-europese-richtlijn-nis2-strengere-eisen-cybersecurity.html

[4] **NCSC** -- Cybersecuritybeeld 2025. https://www.ncsc.nl/nieuws/cybersecuritybeeld-2025-dreigingen-divers-en-onvoorspelbaar-digitale-basishygiene-op-orde-blijft-cruciaal

[5] **Vodafone Business** -- CBS Cybersecuritymonitor: security voor het mkb. https://www.vodafone.nl/zakelijk/inspiratie/cbs-cybersecuritymonitor-security-mkb

[6] **Verzekercyber.nl** -- Wat kost een cyberverzekering? https://verzekercyber.nl/wat-kost-een-cyberverzekering/

[7] **Consultancy.nl** -- NIS2 implementeren: Governance, keten en bewijsvoering. https://www.consultancy.nl/nieuws/65908/nis2-implementeren-governance-keten-en-bewijsvoering-in-vijf-bouwblokken

[8] **Emerce** -- Duizenden bedrijven dreigen klanten kwijt te raken door NIS2. https://www.emerce.nl/wire/duizenden-bedrijven-dreigen-klanten-kwijt-raken-door-onvoldoende-compliance-nis2

[9] **Regelhulpenvoorbedrijven.nl** -- NIS2 Quickscan. https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/

[10] **Laurus Verzekeringen** -- 60% van kleine bedrijven failliet na cyberaanval.

[11] **ICTRecht** -- Verplichtingen voor bestuurders onder NIS2. https://www.ictrecht.nl/blog/de-nis2-is-van-kracht-hoe-zit-het-met-de-verplichtingen-voor-bestuurders

[12] **CertificeringsAdvies Nederland** -- NIS2 bestuursaansprakelijkheid. https://certificeringsadvies.nl/nis2-bestuursaansprakelijkheid-en-persoonlijke-aansprakelijkheid/

[13] **Pragmaat** -- NIS2 vs. DORA: welke richtlijn is van toepassing? https://pragmaat.nl/nis2-vs-dora-welke-richtlijn-is-van-toepassing-op-mijn-organisatie/

[14] **Orange Cyberdefense** -- NIS2, DORA & meer. https://www.orangecyberdefense.com/nl/jouw-uitdagingen/security-themas/voldoen-aan-cybersecurity-wet-en-regelgeving

[15] **Digital Trust Center** -- NIS2 informatie en tools. https://www.digitaltrustcenter.nl/nis2/toegangsbeleid

[16] **Kennedy Van der Laan** -- Cyber in 2026: NIS2 in aantocht. https://kvdl.com/en/articles/cyber-in-2026-nis2-in-aantocht

[17] **CBS** -- Cybersecuritymonitor 2024. https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[18] **ITRiskCarriere** -- Dit gaat NIS2 aan tijd en geld kosten. https://www.itriskcarriere.nl/artikel/dit-gaat-nis2-aan-tijd-en-geld-kosten

[19] **SDE Consultancy** -- Kosten van NIS2 compliance voor het MKB. https://www.sdeconsultancy.nl/blog/nis2-compliance-kosten-mkb

[20] **ABN AMRO Verzekeringen** -- Gevolgen NIS2 voor mkb. https://www.abnamroverzekeringen.nl/artikelen/nis2-wat-het-mkb-moet-weten