Cybersecurity in Europa

De herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS 2)

Nynke Brouwer & Jurriaan van Mil[1]

In juli 2016 heeft de Europese wetgever de Netwerk- en Informatiebeveiligingsrichtlijn (NIS 1) aangenomen. Deze beoogt overkoepelende doelen en waarden te creëren, die bedrijven en organisaties naar eigen inzicht, maar bezien vanuit de betreffende cyberrisico's, dienen na te streven en te bewerkstelligen. Een nieuw voorstel (NIS 2) beoogt het gemeenschappelijk niveau van cybersecurity in de Europese Unie verder te verhogen, mede wegens aanzienlijke implementatieverschillen tussen de lidstaten. In deze bijdrage worden de verschillen in kaart gebracht tussen het huidige regelgevende kader (NIS 1 en de nationale implementatie daarvan) en het toekomstige kader gericht op vier onderwerpen: toepassingsbereik, beveiligingsplicht, meldplicht en toezicht en handhaving. NIS 2 draait op al deze fronten de duimschroeven aan en vormt een belangrijke stap in de digitale strategie van de EU. Daarbij verschuift NIS 2 de verantwoordelijkheid voor cybersecurity duidelijk omhoog richting de *boardroom*.

1. Inleiding

'*Digitale risico's onverminderd groot*', zo kopt een van de hoofdstukken van het Cybersecuritybeeld Nederland 2022.[2] Terecht wijst de Nederlandse Coördinator Terrorismebestrijding en Veiligheid erop dat digitale veiligheid onlosmakelijk is verbonden met nationale veiligheid. Vitale en kritieke processen in onze samenleving zijn dermate gedigitaliseerd, dat een succesvolle aanval daarop kan leiden tot maatschappelijke ontwrichting.[3] Cyberaanvallen en cyberincidenten kunnen om die reden niet alleen grote schade toebrengen aan bedrijven en organisaties zelf. Ook kunnen zij leiden tot een belemmering van economische bedrijvigheid, ondermijning van het gebruikersvertrouwen en als gevolg daarvan tot ernstige schade aan de economie van de Unie.[4] Om die reden noemt de Europese Unie de beveiliging van netwerk- en informatiesystemen, die wij in deze bijdrage zullen aanduiden als 'cybersecurity', essentieel voor een goede werking van de interne markt.[5]

Tegen deze achtergrond van de toenemende digitalisering en cyberincidenten hebben de EU-wetgevers in juli 2016 de Netwerk- en Informatiebeveiligingsrichtlijn (hierna: NIS 1) aangenomen.[6] NIS 1 beoogt een hoog gemeenschappelijk niveau van cybersecurity tot stand te brengen om zo de werking van de interne markt te verbeteren.[7] Daartoe richt NIS 1 zich onder andere op het verbeteren van cybersecurity (preventief) en weerbaarheid (reactief).[8] NIS 1 is *principle-based* en *risk-based*: de richtlijn beoogt in wezen overkoepelende doelen en waarden te creëren, die bedrijven en organisaties naar eigen inzicht, maar bezien vanuit de betreffende cyberrisico's, dienen na te streven en te bewerkstelligen.[9]

Vanaf het moment van inwerkingtreding is de Europese Commissie al gestart met de evaluatie en herziening van NIS 1. Uit de evaluatie blijkt onder andere dat NIS 1 de manier waarop over cybersecurity wordt gedacht heeft veranderd, maar ook dat er aanzienlijke implementatieverschillen tussen de lidstaten bestaan.[10] Dit heeft geleid tot het aannemen van de NIS 2-richtlijn (hierna: NIS 2) op 14 december 2022.[11] NIS 2 breidt de bepalingen uit NIS 1 verder uit. NIS 2 maakt deel uit van de op 1 maart 2021 door de Europese Commissie gepresenteerde *Digital Decade*, waaruit reeds meerdere wetsvoorstellen zijn voortgevloeid.[12] NIS 2 is halverwege januari 2023 in werking getreden.[13] De lidstaten moeten de richtlijn uiterlijk op 17 oktober 2024 hebben geïmplementeerd.[14]

In deze bijdrage brengen wij de verschillen tussen het huidige regelgevend kader (NIS 1) en het toekomstig kader (NIS 2) in kaart. Wij beperken ons tot vier onderwerpen: toepassingsbereik, beveiligingsplicht, meldplicht en toezicht en handhaving. Wij starten met een uiteenzetting van het huidige kader, dus NIS 1, en de nationale implementatie daarvan in Nederland (par. 2). Vervolgens bespreken wij de herziene NIS 2, waarbij wij ingaan op de genoemde onderwerpen (par. 3).[15] In par. 4 geven wij onze eerste beschouwingen over de betekenis van de herziene

NIS 1 heeft de manier waarop over cybersecurity wordt gedacht veranderd, maar er bestaan ook aanzienlijke implementatieverschillen tussen de lidstaten

richtlijn, waarbij wij ook de vraag opwerpen in hoeverre de wijzigingen in NIS 2 zullen bijdragen aan een veiligere en weerbaardere EU. Par. 5 concludeert.

2. NIS 1 en de nationale implementatie in Nederland

2.1 Toepassingsbereik

2.1.1 NIS 1

NIS 1 is van toepassing op aanbieders van essentiële diensten en digitaledienstverleners.[16] NIS 1 wijst 33 entiteiten aan als aanbieders van essentiële diensten, verspreid over zeven sectoren: energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater, en digitale infrastructuur.[17] Het is aan de lidstaten om de aanbieders van essentiële diensten op hun grondgebied aan te wijzen.[18] NIS 1 laat de lidstaten veel vrijheid om te bepalen welke entiteiten als aanbieder van essentiële diensten worden aangemerkt.[19] Digitaledienstverleners zijn onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten.[20]

2.1.2 Toepassingsbereik Nederlandse implementatie (Wbni en Bbni)

NIS 1 is in 2018 geïmplementeerd in de Nederlandse Wet beveiliging netwerk- en informatiesystemen (Wbni) en het bijbehorende Besluit beveiliging netwerk- en informatiesystemen (Bbni). De Wbni wijst – via de weg van het Bbni – zogenoemde vitale aanbieders aan. Onder vitale aanbieders vallen twee categorieën entiteiten: de in NIS 1 genoemde aanbieders van essentiële diensten, en de 'andere' vitale aanbieders.[21] Door ook een categorie 'andere' vitale aanbieders op te nemen, hanteert Nederland een ruimer toepassingsbereik van de Wbni dan NIS 1 voorschrijft.[22] De 'andere' vitale aanbieders die in Nederland zijn aangewezen, zijn entiteiten in de volgende sectoren: nucleair, keren en beheren (bijvoorbeeld sluizen en waterkeringen), financieel en elektronische communicatienetwerken en -diensten/ICT.[23]

Concreet heeft de Nederlandse wetgever onder andere de volgende entiteiten als aanbieders van essentiële diensten aangemerkt: zie tabel 1.[24]

Auteurs

1. Mr. dr. N.M. Brouwer en mr. J.J.H. van Mil zijn beiden advocaat bij Stibbe te Amsterdam. Brouwer is tevens als *fellow* verbonden aan het Onderzoekcentrum Onderneming & Recht (OO&R) van de Radboud Universiteit Nijmegen. De auteurs bedanken Claire ten Heuvelhof en Anne van Boekel voor hun ondersteunende onderzoeken. Dit artikel is op persoonlijke titel geschreven.

Noten

2. NCTV, *Cybersecuritybeeld Nederland 2022*, 4 juli 2022, p. 15, nctv.nl.

3. NCTV, *Cybersecuritybeeld Nederland 2022*, 4 juli 2022, p. 15, nctv.nl. Een voorbeeld van de gevolgen van een aanval op de kritieke infrastructuur is de aanval op de Colonial Pipeline in de Verenigde Staten: na de aanval werden (uit voorzorg) alle leidingen afgesloten, zie bijvoorbeeld 'Oliepijpleidingen VS stilgelegd vanwege cyberaanval', *NOS* 8 mei 2021.

4. Overweging 2 NIS 1.

5. Overweging 3 NIS 1; overweging 3 NIS 2.

6. Voluit: Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

7. Art. 4 lid 1 NIS 1.

8. S.S.D. Nizamoeddin, 'Cybersecurity en gegevensbescherming bij energienetwerken', *Energierecht* 2019, afl. 1.

9. Vgl. J.D. Michels & I. Walden, 'Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?', *European Law Review* 2020/45, p. 25-47. Deze auteurs merken NIS 1 aan als '*principle-based meta-regulation*': "*It is principle based, in that the Directive sets out high-level objectives and values, while OES* [operators of essential services; auteurs] *are left free to devise their own systems to implement the principles in practice. It is meta-regulation, in that it requires OES to develop their own internal, self-regulatory responses to a public problem. The aim is to stimulate self-critical evaluation and self-organisation within companies, who then report to regulators on the strategy they have put in place.*" Zie uitgebreid over 'meta-regulation': C. Coglianese & E. Mendelson, 'Meta-regulation and Self-regulation', in: M. Cave e.a., *The Oxford Handbook on Regulation*, 2010, U of Penn Law School, Public Law Research Paper No. 12-11, U of Penn, Inst for Law & Econ Research Paper No. 12-06.

10. Overweging 2 en 4 NIS 2. Dit is naar onze mening niet geheel onverwachts, omdat NIS 1 slechts voorziet in minimumharmonisatie (art. 3 NIS 1) en de lidstaten veel ruimte laat om eigen implementatiekeuzes te maken.

11. Voluit: Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).

12. Zie ook M. de Koning & T. van Canneyt, 'Regulering van de digitale economie: de EU neemt veel hooi op haar vork', *Computerrecht* 2022/217.

13. Art. 45 NIS 2.

14. Art. 41 NIS 2.

15. Zowel NIS 1 als NIS 2 bevatten een gedeelte over het delen van (dreigings)informatie. Hoewel dit een belangrijk onderdeel is van de Richtlijn, behandelen wij dit in deze bijdrage niet. Wij richten ons bewust op de materiële vereisten uit de NIB-Richtlijn(en) en de betekenis daarvan voor de betreffende bedrijven en organisaties.

16. Overweging 7 NIS 1.

17. Bijlage II NIS 1.

18. Art. 5 lid 1 NIS 1.

19. Vgl. overweging 19, 20 en 25 bij NIS 1.

20. Bijlage III NIS 1.

21. Art. 5 Wbni.

22. Deze verruiming kent haar oorsprong in de eerdere Wet gegevensbescherming en meldplicht cybersecurity. Zie *Kamerstukken II* 2017/18, 34883, nr. 3 (MvT), p. 7. Zie uitgebreid over de Wgmc en de totstandkoming van de Wbni: J.P. Kalis & G.P. van Duijvenvoorde, 'Een nieuw kader voor netwerk- en informatiebeveiliging: een cultuuromslag?', *NtER* 2018, nr. 3-4, p. 114-124.

23. Art. 3 Bbni. Deze laatste categorie betreft netwerken die telefoon-, sms- of internettoegangsdienst aan minimaal 1 miljoen eindgebruikers aanbieden.

24. Art. 2 Bbni. Deze weergave is een vereenvoudigde weergave van het Bbni. Ten behoeve van de leesbaarheid zijn de verwijzingen naar de diverse verordeningen en richtlijnen weggelaten. De volledige lijst is terug te vinden in de Bbni. Zie ook uitgebreid: A.W. Hagdorn, 'De Wet beveiliging netwerk- en informatiesystemen. Betekenis voor de vervoersector in het licht van cybersecurity', *Tijdschrift Vervoer & Recht* 2021/5, p. 110-122.

© Andriy Onufriyenko / Getty Images

Tabel 1: Voorbeelden van aanbieders van essentiële diensten

Sector	*Aanbieder*	*Essentiële dienst*
Energie	De Nederlandse Aardolie Maatschappij B.V.	Het opsporen, winnen en opslaan van gas
	Stichting Centraal Orgaan Voorraadvorming Aardolieproducten	Het beheren van strategische olievoorraden
Vervoer (lucht, spoor, water, weg)	Royal Schiphol Group N.V.	Een veilige en vlotte vlucht- en vliegtuigafhandeling voor wat betreft de luchthaven Schiphol
	De Divisie Havenmeester van het Havenbedrijf Rotterdam N.V.	Het afwikkelen van scheepvaartverkeer
Bankwezen	Kredietinstellingen	Het aanbieden en afwikkelen van betalings-en effectenverkeer
Infrastructuur voor de financiële markt	Exploitanten van handelsplatformen	Het aanbieden en afwikkelen van effectenverkeer
	Centrale tegenpartijen	
Drinkwater	Drinkwaterbedrijven in de zin van de Drinkwaterwet	Het leveren van deugdelijk drinkwater door middel van een openbare drinkwatervoorziening
Digitale infrastructuur	Aanbieders van internetknooppunten	Het voorzien van het internet- en dataverkeer
	Registers voor topleveldomeinnamen	Het beheren en registreren van domeinnamen onder een topleveldomein

Het is opvallend dat de sector gezondheidszorg in de Nederlandse implementatie ontbreekt.[25]
De Nederlandse wetgever heeft ervoor gekozen om die sector niet onder de Wbni en het Bbni te scharen, omdat er voor de zorg reeds een meldplicht voor incidenten bestaat.[26]

Digitaledienstverleners zijn imperatief en limitatief voorgeschreven in NIS 1 en zijn dus richtlijnconform overgenomen in de nationale wetgeving.

2.2 Beveiligingsplicht en meldplicht

2.2.1 NIS 1

NIS 1 bevat zowel een beveiligingsplicht als een meldplicht voor het melden van incidenten. De beveiligingsplicht is een open norm: aanbieders van essentiële diensten dienen passende en evenredige maatregelen te treffen met betrekking tot risicobeheersing en het voorkomen en minimaliseren van gevolgen van incidenten.[27]

‘Incidenten’ omvatten onder NIS 1 iedere gebeurtenis met een daadwerkelijk schadelijk effect op de cybersecurity

Deze maatregelen dienen, gezien de stand van de techniek, te zijn afgestemd op de cyberrisico’s die zich voordoen.[28] Dit is dus een *risk-based approach*. De beveiligingsplicht voor digitaledienstverleners is op een vergelijkbare manier vormgegeven.[29] Wel geeft NIS 1 digitaledienstverleners iets meer (algemene) handvatten waarmee zij rekening dienen te houden bij het nemen van cybersecuritymaatregelen.[30] Het gaat dan bijvoorbeeld om het beheer van de bedrijfscontinuïteit, toezicht, controle en testen.

Doet zich een incident voor, dan moeten de aanbieders van essentiële diensten en digitaledienstverleners dit in bepaalde gevallen onverwijld mededelen aan onder andere de bevoegde autoriteit.[31] ‘Incidenten’ omvatten iedere gebeurtenis met een daadwerkelijk schadelijk effect op de cybersecurity.[32] Aanbieders van essentiële diensten hoeven uitsluitend incidenten met *aanzienlijke* gevolgen te melden, en digitaledienstverleners hoeven uitsluitend incidenten met *substantiële* gevolgen te melden. Of een incident *aanzienlijke* gevolgen heeft, moet worden bepaald aan de hand van de volgende factoren: (1) het aantal gebruikers dat door de verstoring van de essentiële dienst wordt getroffen; (2) de duur van het incident; en (3) de omvang van het geografische gebied dat door het incident is getroffen.[33] Of een incident *substantiële* gevolgen heeft, moet worden bepaald aan de hand van deze drie factoren en de volgende twee factoren: (4) de omvang van de verstoring van de werking van dienst; en (5) de omvang van de impact op de economische en maatschappelijke activiteiten.[34] De meldplicht geldt voor digitaledienstverleners enkel als zij toegang hebben tot de informatie die nodig is om deze beoordeling uit te voeren.[35] Voor digitaledienstverleners is de meldplicht dus wat minder stringent dan voor aanbieders van essentiële diensten.[36] Voor aanbieders van essentiële diensten en digitaledienstverleners geldt dat een melding niet leidt tot verhoogde aansprakelijkheid.[37]

2.2.2 Beveiligingsplicht en meldplicht in Nederlandse wetgeving

De wettekst van de beveiligingsplicht in de Wbni is exact hetzelfde als die in NIS 1.[38] De beveiligingsplicht in de Wbni is dus ook een open norm. Het Bbni vult deze open norm iets verder in door te verwijzen naar een bijlage waarin vijf maatregelen zijn opgenomen die aanbieders van essentiële diensten ten minste moeten treffen.[39] Dit zijn:

1. risicogebaseerde aanpak: een overzicht van de betreffende netwerk- en informatiesystemen en een risicoanalyse;
2. organisatie van netwerk- en informatiebeveiligingsbeheer: een organisatorisch cybersecuritybeleid en -strategie;
3. incidenten voorkomen: een gelaagde, technische cybersecuritystrategie;
4. detectie en respons: systemen en cybersecuritymaatregelen die het mogelijk maken om (potentiële) incidenten te detecteren, analyseren, monitoren en loggen en daartegen op te treden; en
5. gevolgen van incidenten beperken: bedrijfscontinuïteitsbeleid en crisismanagementbeleid.

Aanbieders van essentiële diensten en andere vitale aanbieders moeten incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende dienst onverwijld melden bij onder andere de bevoegde autoriteiten.[40] Dit geldt ook voor inbreuken op de cybersecurity die aanzienlijke gevolgen *kunnen* hebben voor de continuiteit van hun dienstverlening.[41] Ook op dit punt bevat de Nederlandse implementatie dus een uitbreiding van NIS 1, dat enkel gebeurtenissen met een *daadwerkelijk* schadelijk effect als ‘incident’ aanmerkt.[42] De bevoegde autoriteiten verschillen per sector. Wij gaan hier in par. 2.3 verder op in.

Digitaledienstverleners dienen de melding onverwijld te doen bij de bevoegde autoriteit en bij het CSIRT voor digitale diensten. Dat is de Minister van Economische Zaken en Klimaat.[43]

25. Zie bijlage II onder 5 bij NIS 1.
26. *Kamerstukken II* 2017/18, 34883, nr. 3 (MvT), p. 12-13. Zie ook de nota van toelichting bij Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wbni, *Stb.* 2018, 338.
27. Art. 14 lid 1 NIS 1. Zie over deze beveiligingsnorm, zowel in het kader van de NIS-richtlijn als (uitgebreid) in het kader van de AVG: J.A. Hofman, *De beveiliging van persoonsgegevens* (diss. Nijmegen), Deventer: Wolters Kluwer 2022, met name par. 7.3.5.
28. Art. 14 lid 1 NIS 1.
29. Art. 16 lid 1 NIS 1.
30. Art. 16 lid 1 NIS 1.
31. Art. 14 lid 3 en 16 lid 3 NIS 1.
32. Art. 4 sub 7 NIS 1.
33. Art. 14 lid 4 NIS 1.
34. Art. 16 lid 4 NIS 1.
35. Art. 16 lid 4 NIS 1.
36. Zie ook J.P. Kalis, ‘De Netwerk en informatiebeveiligingsrichtlijn’, *Computerrecht* 2017/48, p. 63 en J.C. Hulsebosch, ‘De Europese Cybersecurity Act’, *Computerrecht* 2019/215.
37. Art. 14 lid 3 en 16 lid 3 NIS 1. Dat een melding niet leidt tot een verhoogd aansprakelijkheidsrisico, betekent volgens ons niet zonder meer dat een melding leidt tot een *lager* aansprakelijkheidsrisico.
38. Art. 7 Wbni en 14 lid 1 NIS 1.
39. Art. 9 Wbni jo. art. 3a Bbni en bijbehorende bijlage. Voor de sectoren drinkwater en vervoer zijn deze maatregelen nader uitgewerkt in de Regeling beveiliging netwerk- en informatiesystemen IenW, zie *Stcrt.* 2021, 25471.
40. Art. 10 lid 1 en 2 Wbni. Zie uitgebreid Hagdorn 2021, p. 118 e.v.
41. Art. 10 lid 1 en 2 Wbni. Zie uitgebreid Hagdorn 2021, p. 118 e.v.
42. Het effect van de meldplicht is bekritiseerd door de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in haar rapport *Voorbereiden op digitale ontwrichting* uit 2019 (p. 57) en door de Cyber Security Raad (CSR); zie ‘Cyber Security Raad dringt aan op het versneld delen van incidentinformatie’, 23 februari 2021 op www.csr.nl. De CSR onderzoekt bovendien de mogelijkheid om data afkomstig uit meldplichten (zowel uit de AVG als uit NIS 1) beter te benutten (WRR 2019, p. 93). De vraag is immers wat de zin van melden is als er vervolgens niets gebeurt. Zie in dit kader ook B. Nieuwesteeg, M. van Eeten & M. Faure, *Scientific research data breach notification obligation*, 29 november 2018.
43. Art. 13 lid 1 jo. 4 lid 2 Wbni. Zie ook *Stb.* 2018, 389.

NIS 2 moet de verschillen tussen de lidstaten wegwerken om zo een hoger gemeenschappelijk niveau van cybersecurity te bereiken en daarmee de werking van de interne markt te verbeteren

2.3 Handhaving en toezicht

2.3.1 NIS 1

De lidstaten moeten zorgen dat de bevoegde autoriteiten de naleving van de beveiligings- en meldplicht en de effecten daarvan op cybersecurity kunnen beoordelen.[44] Daartoe moeten de bevoegde autoriteiten bijvoorbeeld informatie kunnen vorderen van aanbieders van essentiële diensten en digitaledienstverleners.[45] Als de bevoegde autoriteiten een nalevingsprobleem hebben geconstateerd, moeten zij maatregelen kunnen nemen,[46] zoals het geven van een bindende aanwijzing en het informeren van het publiek over een incident.[47] Het openbaar maken van zulke informatie is precies hetgeen bedrijven en organisaties in de regel liever niet doen, bijvoorbeeld uit angst voor reputatieschade. De lidstaten hebben de vrijheid om zelf de sancties vast te stellen die van toepassing zijn op overtredingen op nationale bepalingen.[48] Wel schrijft NIS 1 voor dat deze sancties doeltreffend, evenredig en afschrikkend moeten zijn.[49]

2.3.2 Handhaving in de Wbni

De Nederlandse wetgever heeft ervoor gekozen om toezicht en handhaving en advisering van elkaar te scheiden en bij verschillende autoriteiten te beleggen.[50] Wij gaan in op toezicht en handhaving.

De Nederlandse wetgever heeft gekozen voor sectoraal toezicht, waardoor hij diverse bevoegde autoriteiten heeft aangewezen. De Minister van Economische Zaken en Klimaat houdt toezicht op digitaledienstverleners. De uitvoerende taken zijn neergelegd bij de Rijksinspectie Digitale Infrastructuur.[51] Voor aanbieders van essentiële diensten zijn de volgende bevoegde autoriteiten en toezichthoudende diensten aangewezen: zie tabel 2.

De bevoegde autoriteiten zijn belast met de bestuursrechtelijke handhaving van de Wbni.[58] Daartoe kunnen de bevoegde autoriteiten sowieso gebruikmaken van het handhavingsinstrumentarium uit de Algemene wet bestuursrecht.[59] Deze handhavingsbevoegdheden gelden ten aanzien van aanbieders van essentiële diensten en digitaledienstverleners en dus niet ten aanzien van de andere vitale aanbieders.[60]

De bevoegde autoriteiten hebben verder een auditbevoegdheid: zij kunnen onderzoek naar de naleving van de beveiligingsplicht door een onafhankelijk deskundige gelasten.[61] Als de beveiligingsplicht wordt geschonden, kunnen de bevoegde autoriteiten een bindende aanwijzing geven om maatregelen te treffen.[62] Ook kunnen de bevoegde autoriteiten het publiek informeren over incidenten.[63] Tot slot kunnen de bevoegde autoriteiten een last onder bestuursdwang en in het uiterste geval een bestuurlijke boete van maximaal € 5 miljoen opleggen.[64]

Er is ons tot op heden slechts één Nederlands handhavingsgeval bekend, namelijk het verscherpte toezicht op Waternet door de Inspectie Leefomgeving en Transport.[65]

3. De herziene Richtlijn: NIS 2

De relatief grote mate van vrijheid die NIS 1 aan de lidstaten geeft, heeft tot grote verschillen tussen de lidstaten geleid, bijvoorbeeld in toepassingsbereik, in verplichtingen rondom de meldplicht en in cybersecurityniveau. Er bestaan daarom nog steeds grote verschillen in cyberweerbaarheid tussen de lidstaten.[66] Een lager niveau van cybersecurity en cyberweerbaarheid in de ene lidstaat, tast ook het niveau in andere lidstaten aan.[67] Om die redenen, maar ook vanwege het inmiddels sterk veranderde dreigingslandschap, was herziening van NIS 1 noodzakelijk.[68] NIS 2 moet de verschillen tussen de lidstaten wegwerken om zo een hoger gemeenschappelijk niveau van cybersecurity te bereiken en daarmee de werking van de interne markt te verbeteren.[69]

3.1 Toepassingsbereik

Onder NIS 2 vervalt het verschil tussen aanbieders van essentiële diensten en digitaledienstverleners. Dit verschil bleek achterhaald.[70] In plaats daarvan maakt NIS 2 onderscheid tussen 'essentiële' en 'belangrijke' entiteiten.[71] Het verschil tussen deze twee categorieën zit vooral in de wijze van toezicht en handhaving: voor essentiële entiteiten

Tabel 2: bevoegde autoriteiten en toezichthoudende diensten

AED-sectoren	Bevoegde autoriteit[52]	Toezichthoudende dienst
• Energie	Minister van Economische Zaken en Klimaat	Rijksinspectie Digitale Infrastructuur[53]
• Digitale infrastructuur	Minister van Economische Zaken en Klimaat	Rijksinspectie Digitale Infrastructuur[54]
• Bankwezen	De Nederlandsche Bank[55]	
• Infrastructuur voor de financiële markt	De Nederlandsche Bank	
• Vervoer	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving & Transport[56]
• Levering en distributie van drinkwater	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving & Transport[57]

is het toezicht (pro)actief; voor belangrijke entiteiten juist reactief.[72]

Het aantal sectoren – en daarmee het aantal bedrijven en organisaties – waarop NIS 2 betrekking heeft, wordt fors uitgebreid. NIS 2 wijst tientallen soorten entiteiten aan, verspreid over elf zeer kritieke sectoren en zeven andere kritieke sectoren (zie tabel 3 voor een overzicht). Om de verschillen tussen de lidstaten weg te werken en de rechtszekerheid te vergroten, laat NIS 2 de lidstaten veel minder vrijheid met betrekking tot het toepassingsbereik.[73] NIS 2 formuleert een uniform criterium aan de hand waarvan wordt bepaald welke entiteiten binnen het toepassingsbereik vallen: een *size-cap*. Alle middelgrote ondernemingen, die actief zijn in de in NIS 2 genoemde sectoren, vallen binnen het toepassingsbereik van de richtlijn.[74] Groter dan middelgrote ondernemingen kunnen essentiële entiteiten zijn.[75] En middelgrote ondernemingen kunnen slechts belangrijke entiteiten zijn.[76] De *size-cap* geldt niet voor bepaalde entiteiten, bijvoorbeeld de enig aanbieder van een dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten.[77]

NIS 2 zich met een apart artikel over *governance* rechtstreeks tot het bestuur van de entiteiten

Tabel 3. De dikgedrukte sectoren zijn nieuw ten opzichte van NIS 1. Dit is een verkorte weergave van de bijlagen bij NIS 2.

Zeer kritieke sectoren	Andere kritieke sectoren
• Energie (elektriciteit incl. **producten**, **laaddiensten**, **opslagdiensten**), **stadsverwarming en -koeling**, aardolie, aardgas, **waterstof** • Vervoer (lucht, spoor, water, weg) • Bankwezen • Infrastructuur voor de financiële markt • Gezondheidszorg (zorgaanbieders, **EU-referentielaboratoria, onderzoek en ontwikkeling m.b.t. geneesmiddelen, farmaceutische basisproducten en bereidingen, medische hulpmiddelen voor noodsituaties**) • Drinkwater • **Afvalwater** • Digitale infrastructuur • **Beheer van ICT-diensten (aanbieders internetknooppunten, DNS dienstverleners, register voor toplevel-domeinnamen, aanbieders datacenterdiensten, aanbieders netwerken voor levering van inhoud, verleners van vertrouwensdiensten, aanbieders elektronische-communicatienetwerken en -diensten** • **Overheid** • **Ruimtevaart**	• **Post- en koeriersdiensten** • **Afvalstoffenbeheer** • **Vervaardiging, productie en distributie van chemische stoffen** • **Productie, verwerking en distributie van levensmiddelen** • **Vervaardiging (medische hulpmiddelen; informatica-, elektronische en optische producten; elektrische apparatuur; machines, apparaten, en werktuigen; motorvoertuigen, aanhangers en opleggers; andere transportmiddelen)** • Digitale aanbieders (onlinemarktplaatsen, onlinezoekmachines, platforms voor **sociale-netwerkdiensten**) • **Onderzoek**

44. Art. 15 lid 1 NIS 1. Daartoe moeten de lidstaten zorgen dat de bevoegde autoriteiten over de nodige middelen beschikken om hun taken doeltreffend en efficiënt uit te kunnen voeren (art. 8 lid 5 NIS 1). Voor digitaledienstverleners geldt trouwens een licht en reactief toezichtregime. De bevoegde autoriteiten hebben geen algemene verplichting om toezicht op hen te houden en hoeven pas maatregelen te nemen als er bewijs is dat zij met een nalevingsprobleem kampen (overweging 60 NIS 1).

45. Art. 15 lid 2 en 17 lid 2 NIS 1.

46. Art. 15 lid 3 en 17 lid 1 NIS 1.

47. Art. 15 lid 3 respectievelijk art. 14 lid 6 en 16 lid 7 NIS 1.

48. Art. 21 NIS 1.

49. Art. 21 NIS 1.

50. Het CSIRT is belast met advies en bijstand. Voor de aanbieders van essentiële diensten is het Nationaal Cyber Security Centrum (NCSC) aangewezen als CSIRT. Voor digitaledienstverleners is dat de Minister van EZK.

51. Tot 1 januari 2023 was de Rijksinspectie Digitale Infrastructuur het Agentschap Telecom, zie rdi.nl/actueel/nieuws/2022/11/07/nieuwe-naam-vooragentschap-telecom-vanaf-1-januari-2023.

52. Art. 4 lid 1 Wbni.

53. Besluit van de Minister van Economische Zaken en Klimaat van 5 november 2018, nr. WJZ/18213911, tot aanwijzing toezichthouders Wet beveiliging netwerk- en informatiesystemen voor de sectoren energie, digitale infrastructuur en voor digitale diensten.

54. *Ibid*.

55. Wij zijn niet bekend met een besluit op basis waarvan DNB een toezichthoudende dienst heeft aangewezen. Daarom nemen wij aan dat DNB zelf als toezichthouder optreedt.

56. Besluit van de Minister van Infrastructuur en Waterstaat, van 30 oktober 2018, nr. IENW/BSK-2018/224867, houdende aanwijzing van ambtenaren belast met het toezicht op de naleving van de Wet beveiliging netwerk- en informatiesystemen.

57. *Ibid*.

58. Art. 4 lid 3 Wbni.

59. Art. 5:11 tot en met 5:20 Awb.

60. Art. 24 Wbni.

61. Art. 26 Wbni.

62. Art. 27 Wbni.

63. Art. 23 Wbni.

64. Art. 28 en 29 Wbni.

65. Kamerbrief d.d. 2 april 2021, ILT-2021/19822, *Kamerstukken II* 2020/21, 27625, nr. 529.

66. Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148, COM(2020) 823 final, 2020/0359(COD), p. 1-2. Zie ook overweging 5 NIS 2.

67. *Ibid*, p. 4.

68. Overweging 5 NIS 2.

69. Overweging 5 en art. 1 lid 1 NIS 2.

70. Overweging 7 NIS 2.

71. Overweging 15 NIS 2.

72. Zie ook par. 3.4.

73. Overweging 7 NIS 2.

74. Voor de beoordeling of een onderneming middelgroot is, moet naar Aanbeveling 2003/361/EG worden gekeken (art. 2 lid 1 NIS 2). Voluit: Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en microondernemingen.

75. Art. 3 lid 1 aanhef en onder a NIS 2.

76. Art. 3 lid 2 NIS 2.

77. Art. 2 lid 2 sub b en overweging 7 NIS 2. Zie ook art. 2 lid 2 en 3 en art. 3 lid 1 sub b tot en met g NIS 2.

3.2 Beveiligingsplicht

NIS 2 bevat een uitgebreidere en explicietere beveiligingsverplichting dan NIS 1. Daarbij richt NIS 2 zich met een apart artikel over *governance* bovendien rechtstreeks tot het bestuur van de entiteiten: bestuursorganen dienen de cybersecuritymaatregelen goed te keuren, toe te zien op de uitvoering ervan en moeten bovendien aansprakelijk kunnen worden gehouden indien de entiteit zich niet aan de beveiligingsplicht houdt.[78] Daarnaast schrijft NIS 2 voor dat bestuurders zich scholen: zij moeten dus een cybersecurityopleiding volgen.[79]

De open norm van 'passende technische en organisatorische maatregelen' komt in NIS 2 weer terug.[80] NIS 2 geeft daaraan echter meer duiding. Bij het nemen van maatregelen moeten entiteiten rekening houden met de stand van de techniek, Europese en internationale normen, maar ook met de uitvoeringskosten.[81] De maatregelen moeten zijn afgestemd op het risico. Welke maatregelen moeten worden getroffen, hangt dus af van een risicobeoordeling en een evenredigheidstoets. Het maakt daarbij niet uit of entiteiten het beheer of onderhoud van de netwerk- en informatiesystemen hebben uitbesteed aan een derde.[82]

De te treffen maatregelen moeten betrekking hebben op 'alle' gevaren, wat inhoudt dat zowel de informatiesystemen als fysieke omgeving moeten worden beschermd.[83] Anders dan NIS 1 schrijft NIS 2 concrete basismaatregelen voor, waaronder: risicobeleid, incidentenbehandeling, back-upbeheer en noodvoorzieningsplannen, cyberhygiëne en opleidingen, beleid voor encryptie, multifactor-authenticatie en beveiligde noodcommunicatiesystemen.[84] Andere basismaatregelen die entiteiten moeten toepassen zijn *zero trust*-beginselen, softwareupdates, configuratie van apparaten, netwerksegmentatie, het vergroten van bewustzijn van cyberdreigingen, phishing en social engineering.[85] Verder schenkt NIS 2 aandacht aan de toeleveringsketen: entiteiten worden aangespoord om cybersecuritymaatregelen overeen te komen in de contracten met hun leveranciers en dienstverleners.[86] De nadruk op de toeleveringsketen is belangrijk, omdat beveiligingsproblemen zich vaak niet bij de entiteit zelf afspelen, maar bij de leverancier of een onderaannemer.

De voornoemde maatregelen zijn dus minimummaatregelen. De Europese Commissie kan de maatregelen door middel van uitvoeringshandelingen nader concretiseren en uitbreiden. Om aan te tonen dat aan de beveiligingsverplichting is voldaan, kunnen lidstaten eisen dat de entiteiten gebruik maken van gecertificeerde producten of diensten in de zin van de Cybersecurity Act.[87]

Een incident is significant als het een ernstige operationele verstoring van de diensten van of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken

3.3 Meldplicht

Ook de meldplicht is onder NIS 2 uitgebreid. Entiteiten moeten ieder *significant* incident melden aan het CSIRT of aan de bevoegde autoriteit.[88] Een 'incident' is een gebeurtenis die – kort gezegd – de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of van de diensten die worden aangeboden in gevaar brengt. Deze definitie is ruimer dan de definitie onder NIS 1, die een 'daadwerkelijk schade-effect' vereist. Een incident is significant als het een ernstige operationele verstoring van de diensten van of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken.[89] Daarnaast is een incident significant als het andere natuurlijke personen of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.[90]

Het tijdspad waarbinnen de melding moet worden gedaan, is getrapt:

1. Onverwijld en in elk geval binnen 24 uur na kennisname van het incident moet een vroegtijdige waarschuwing worden gegeven. Daarin moet worden aangegeven of sprake is van een onrechtmatige of kwaadwillende oorzaak en van mogelijke grensoverschrijdende gevolgen.[91]
2. Onverwijld en in ieder geval binnen 72 uur na kennisname van het incident moet een (grondige) incidentmelding worden gedaan. Daarin moet een initiële beoordeling van het incident, met inbegrip van de ernst en de gevolgen ervan, worden opgenomen.[92]
3. Uiterlijk binnen één maand na de incidentmelding moet een eindverslag worden ingediend. Daarin moeten onder andere een gedetailleerde omschrijving van het incident en de genomen cybersecuritymaatregelen worden genoemd.[93]
4. Indien het incident nog gaande is als het eindverslag moet worden ingediend, kan in plaats daarvan een voortgangsverslag worden ingediend. Zodra het incident is afgehandeld, moet binnen één maand alsnog het eindverslag worden ingediend.[94]

De reden voor deze gefaseerde melding is om een evenwicht te vinden tussen enerzijds een snelle melding die verdere gevolgen kan beperken en anderzijds een grondige melding die het mogelijk maakt dat er van incidenten kan worden geleerd.[95]

Indien ontvangers van de verleende dienst mogelijk door het incident worden geraakt, dan moeten de entiteiten hen ook onverwijld informeren over de maatregelen die zij kunnen treffen.[96] Net als onder NIS 1 vermeldt NIS 2 expliciet dat het doen van een melding niet leidt tot een verhoogde aansprakelijkheid.[97]

3.4 Toezicht en handhaving

Onder NIS 2 zijn de bepalingen met betrekking tot toezicht en handhaving uitgebreider en strikter geformuleerd dan onder NIS 1. Waar NIS 1 voorschrijft dat de bevoegde autoriteiten de nodige bevoegdheden en middelen moeten hebben om de naleving van de beveiligingsplicht te kunnen beoordelen, bepaalt NIS 2 dat de lidstaten ervoor moeten zorgen dat de bevoegde autoriteiten *effectief toezicht* houden op en de *noodzakelijke maatregelen nemen* om te zorgen voor naleving van de richtlijn.[98]

NIS 2 somt op welke onderzoeksbevoegdheden bevoegde autoriteiten ten minste moeten hebben. Het gaat dan bijvoorbeeld om het uitvoeren van inspecties, audits en beveiligingsscans en het opvragen van informatie, gegevens en andere documenten.[99] Opgeleide beroepsbeoefenaars dienen de toezichtstaak uit te voeren.[100]

Als de bevoegde autoriteiten een nalevingsprobleem hebben geconstateerd, moeten zij doeltreffende, evenredige en afschrikkende sancties kunnen opleggen.[101] Zo moeten zij entiteiten kunnen gelasten om hun afnemers in kennis te stellen van de aard van een dreiging en de mogelijke maatregelen die zij kunnen nemen.[102] Daarbij moeten de bevoegde autoriteiten maatwerk kunnen bieden.[103] In het uiterste geval moeten de bevoegde autoriteiten een boete kunnen opleggen.[104] Daarbij geldt voor essentiële entiteiten een boetemaximum van € 10 miljoen of 2% van de wereldwijde jaarlijkse omzet in het voorgaande financiële jaar bedragen en voor belangrijke entiteiten een boetemaximum van € 7 miljoen of 1,4% van de wereldwijde omzet in het voorgaande financiële jaar.[105] Het reeds in Nederland bestaande boetemaximum van € 5 miljoen zal dus moeten worden opgehoogd.[106]

Wat verder nieuw is, is dat NIS 2 voorziet in 'vervolgsancties' die aan essentiële entiteiten kunnen worden opgelegd. Als een waarschuwing, bindende aanwijzing of bepaald gebod niet doeltreffend blijkt te zijn, dan moeten bevoegde autoriteiten de essentiële entiteit in kwestie een termijn kunnen opleggen.[107] Binnen die termijn moet de essentiële entiteit dan alsnog het geconstateerde nalevingsprobleem oplossen of aan de eisen van de bevoegde autoriteit voldoen.[108]

Als dat niet wordt gedaan, dan moet de bevoegde autoriteit een certificering of vergunning van de essentiele entiteit tijdelijk kunnen opschorten of daarom kunnen verzoeken bij bijvoorbeeld de rechter.[109] Ook moeten de bevoegde autoriteiten de rechter kunnen verzoeken om de algemeen directeur of wettelijk vertegenwoordiger van de essentiële entiteit tijdelijk te verbieden om diens functie uit te oefenen.[110] De achterliggende gedachte is dat deze vervolgsancties dit laatste handhavingsinstrument en het gehele handhavingsinstrumentarium nog doeltreffender en afschrikwekkender maakt.[111] Gezien de impact van deze vervolgsancties moet hier proportioneel mee worden omgegaan, en mogen zij slechts als ultimum remedium worden toegepast.[112]

Zoals wij eerder hebben besproken, worden bestuursorganen ook verantwoordelijk voor compliance.[113] In het verlengde daarvan bepaalt NIS 2 dat de bestuurders van een essentiële entiteit aansprakelijk moeten kunnen worden gehouden als zij die verplichting niet nakomen.[114] De lidstaten zijn echter niet verplicht om te voorzien in strafrechtelijke of civielrechtelijke aansprakelijkheid van de bestuurder voor schade die derden dientengevolge lijden.[115] De tijd zal moeten leren door wie en waarvoor bestuurders op grond van NIS 2 aansprakelijk kunnen zijn en om wat voor soort aansprakelijkheid het dan gaat.[116]

Wat verder nieuw is, is dat NIS 2 voorziet in 'vervolgsancties' die aan essentiële entiteiten kunnen worden opgelegd

4. Betekenis van de herziene Richtlijn: eerste beschouwingen

NIS 2 draait op alle fronten de duimschroeven aan: het toepassingsbereik, de beveiligingsplicht, de meldplicht en de handhaving. Wij lichten een aantal aspecten uit voor een eerste beschouwing.

78. Art. 20 lid 1 NIS 2. Zie ook art. 32 lid 6 NIS 2. Het begrip 'bestuursorgaan' wordt niet gedefinieerd.
79. Art. 20 lid 2 NIS 2.
80. Art. 21 lid 1 NIS 2.
81. Art. 21 lid 1 NIS 2.
82. Overweging 83 NIS 2.
83. Art. 21 lid 2 en overweging 79 NIS 2.
84. Art. 21 lid 2 sub a tot en met j NIS 2.
85. Overweging 89 NIS 2.
86. Overweging 85 en art. 21 lid 2 sub d NIS 2.
87. Art. 24 lid 1 NIS 2. Voluit: Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening).
88. Art. 23 lid 1 NIS 2.
89. Art. 23 lid 3 aanhef en onder a NIS 2.
90. Art. 23 lid 3 aanhef en onder b NIS 2.
91. Art. 23 lid 4 aanhef en onder a NIS 2.
92. Art. 23 lid 4 aanhef en onder b NIS 2.
93. Art. 23 lid 4 aanhef en onder c NIS 2.
94. Art. 23 lid 4 aanhef en onder e NIS 2.
95. Overweging 101 NIS 2.
96. Art. 23 lid 2 en overweging 103 NIS 2.
97. Art. 23 lid 1 NIS 2.
98. Art. 31 lid 1 NIS 2.
99. Art. 32 lid 2 en 33 lid 2 NIS 2. Specifiek met betrekking tot Nederland is het de vraag of dit veel verandert; de Wbni en de Algemene wet bestuursrecht voorzien reeds in deze onderzoeksbevoegdheden.
100. Overweging 125 NIS 2.
101. Art. 32 lid 1 en 33 lid 1 NIS 2.
102. Art. 32 lid 4 aanhef en onder e en 33 lid 4 aanhef en onder e NIS 2.
103. Zie art. 32 lid 7 NIS 2, waarin een lijst van factoren wordt genoemd die de bevoegde autoriteiten in acht moeten nemen bij het opleggen van sancties aan essentiële entiteiten. Via art. 33 lid 5 NIS 2 geldt dit ook als bevoegde autoriteiten sancties opleggen aan belangrijke entiteiten.
104. Art. 32 lid 4 aanhef en onder i en 33 lid 4 aanhef en onder h NIS 2. Zie ook art. 34 NIS 2.
105. Art. 34 lid 4 en 5 NIS 2.
106. Zie par. 2.3.2.
107. Art. 32 lid 5 NIS 2.
108. Art. 32 lid 5 NIS 2.
109. Art. 32 lid 5 aanhef en onder a NIS 2.
110. Art. 32 lid 5 aanhef en onder b NIS 2.
111. Overweging 133 NIS 2.
112. Overweging 133 NIS 2.
113. Zie par. 3.2.
114. Art. 32 lid 6 NIS 2. De wettekst spreekt van *'elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiële entiteit op basis van de bevoegdheid om deze te vertegenwoordigen'*.
115. Overweging 128 NIS 2.
116. Naar onze mening bieden het Nederlands ondernemingsrecht (art. 2:9 BW) en de Nederlandse onrechtmatige daad (art. 6:162 BW) al de mogelijkheid om bestuurders, zowel intern als extern, aansprakelijk te houden voor ontoereikende cybersecurity. Beslissend is dan telkens of de bestuurder ernstig verwijtbaar respectievelijk persoonlijk ernstig verwijtbaar heeft gehandeld door niet te voorzien in passende cybersecurity. Zie voor de relevante criteria HR 10 januari 1997, *NJ* 1997/360 (*Staleman/Van de Ven*) respectievelijk HR 8 december 2006, *NJ* 2006/659 (*Ontvanger/Roelofsen*). Het is ons nog niet duidelijk hoe 'bestuurdersaansprakelijkheid' onder NIS 2 zich verhoudt tot interne en externe bestuurdersaansprakelijkheid onder Nederlands recht.

Het risico is dat er verschil van inzicht kan ontstaan tussen bijvoorbeeld de toezichthouder en de normadressaat, maar ook dat slechts sprake is van *paper compliance*

4.1 Meer bedrijven gehouden tot cyberbeveiligingsmaatregelen

In par. 3.1 bespraken wij dat het toepassingsbereik van NIS 2 sterk wordt uitgebreid.[117] Voor bedrijven en organisaties betekent dit op de eerste plaats dat zij zullen moeten onderzoeken of zij onder het toepassingsbereik vallen. NIS 2 verwijst veelvuldig naar andere verordeningen en richtlijnen, waardoor de exacte reikwijdte mogelijk niet altijd direct helder is. Daarnaast zullen aangewezen entiteiten hun volledige cybersecuritybeleid moeten toetsen aan de beveiligingsvereisten in NIS 2 en de nationale implementatie daarvan. De relatief concrete lijst met basismaatregelen die in NIS 2 is opgenomen, biedt bedrijven daarbij wel meer houvast. De verwachting is dat het voor veel entiteiten een aanzienlijke investering zal vergen om aan de vereisten te voldoen, bijvoorbeeld waar het gaat om permanente monitoring, het optuigen van incident response-procedures en het herbeoordelen van contracten met derden, zoals leveranciers.[118]

4.2 Cybersecurity in de boardroom

Net als andere EU-wetgeving kent NIS 2 met expliciete bepalingen over *governance* een grote(re) verantwoordelijkheid aan het bestuur toe.[119] In NIS 2 komt deze bestuurdersverantwoordelijkheid bovendien nog sterker naar voren, nu expliciet is opgenomen dat bestuurders aansprakelijk kunnen worden gehouden bij non-compliance en dat tegen de bestuurders handhavingsmaatregelen kunnen worden getroffen zoals een tijdelijk bestuursverbod. NIS 2 brengt hiermee tot uiting wat in de juridische literatuur al meermaals is betoogd: cybersecurity hoort in de *boardroom*.[120]

4.3 Meer incidenten sneller melden

Een ander element dat aandacht verdient is de meldplicht. Wij benoemden al dat de nieuwe definitie van het begrip 'incident' maakt dat sneller sprake zal zijn van een incident. Waar onder NIS 1 sprake moet zijn van een daadwerkelijk schadelijk effect voor de cybersecurity, is onder NIS 2 voldoende indien een gebeurtenis de beschikbaarheid van de dienst of van de verwerkte gegevens in gevaar brengt.

Daarnaast lijkt de meldingsdrempel onder NIS 2 te zijn verlaagd. Onder NIS 1 gaat het om een incident met 'aanzienlijke gevolgen voor de continuïteit van de dienst'. Dat moet worden vastgesteld aan de hand van het aantal gebruikers dat door de verstoring wordt getroffen, de duur van het incident en de omvang van het geografische gebied. Onder NIS 2 gaat het om een 'significant incident'. Daarvan is sprake bij een ernstige operationele verstoring van de diensten van de betrokken entiteit of financiële verliezen voor de betrokken entiteit. Ook is daarvan sprake als het incident andere natuurlijke personen of rechtspersonen treft of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.[121]

Een ransomware-aanval waarbij de getroffen entiteit het losgeld direct betaalt, zou onder NIS 1 mogelijk niet hoeven te worden gemeld, omdat de duur van het incident dan zeer beperkt is. Een ransomware-aanval op de kritieke infrastructuur is echter wel degelijk ernstig, en informatie daarover kan uitermate relevant zijn voor bijvoorbeeld de bevoegde autoriteiten. Onder de criteria van NIS 2 lijkt een ransomware-aanval wel te moeten worden gemeld, ook indien direct zou worden betaald. In ieder geval lijdt de getroffen entiteit een financieel verlies in de vorm van het losgeld. En de operationele verstoring die de ransomware-aanval teweeg heeft gebracht, kan ondanks de korte duur toch ernstig zijn geweest.

Onder NIS 2 is in ieder geval sneller sprake van een incident en lijkt een incident ook eerder meldingswaardig.

4.4 Hoger niveau van cybersecurity?

De hiervoor besproken aspecten – toepassingsbereik, beveiligingsplicht, *governance* en meldplicht – betreffen relatief concrete veranderingen, die op het eerste oog bij kunnen dragen aan het realiseren van het doel van NIS 2: een hoog gemeenschappelijk niveau van cybersecurity bereiken om zo de werking van de interne markt te verbeteren. Een overkoepelende vraag is of NIS 2 zo is ontworpen dat dit doel kan worden gerealiseerd.

De *principle-based* en *risk-based* benadering van NIS 1 en NIS 2 geeft gereguleerde bedrijven en organisaties de nodige vrijheid om naar eigen inschatting invulling te geven aan de toepassing van de wetgeving in de eigen bedrijfsvoering. Gelet op de snelheid waarmee het dreigingslandschap zich ontwikkelt, is dat vreemd noch onwenselijk, maar de risico's van dergelijke wetgeving zijn bijvoorbeeld dat het voor normadressaten onduidelijk is wat zij concreet moeten doen en dat de markt niet voorziet in standaard passende cybersecurityoplossingen. De Algemene verordening gegevensbescherming is daarvan een voorbeeld: de AVG kent talloze open normen, die weliswaar technologieneutraal en *future proof* zijn, maar (dus) ook op uiteenlopende wijze kunnen worden geïnterpreteerd. De beveiligingsnorm in de AVG is in grote mate vergelijkbaar met de beveiligingsnorm in NIS (1 en 2), en is moeilijk in zijn algemeenheid te concretiseren.[122] Het risico is dan ook dat er verschil van inzicht kan ontstaan tussen bijvoorbeeld de toezichthouder en de normadressaat, maar ook dat slechts sprake is van *paper compliance*.[123]

Het risico van *paper compliance* is in de literatuur ook ten aanzien van NIS 1 gesignaleerd.[124] Omdat NIS 2 eenzelfde systematiek en benaderingswijze hanteert, bestaat ook onder NIS 2 het risico dat deze regelgeving een onvoldoende drijfveer vormt voor entiteiten om daadwerkelijk te voldoen. Toezicht en handhaving spelen daarbij een belangrijke rol. Hoewel NIS 2 ook dit punt aanscherpt, voorzien wij dat de aard van de richtlijn mogelijk uitdagingen opwerpt voor effectieve handhaving. Als gevolg daarvan voorziet

NIS 2 mogelijk in onvoldoende stimulans voor bedrijven en organisaties om cybersecurity zodanig hoog op de agenda te plaatsen dat dit uiteindelijk leidt tot een gemeenschappelijk hoger cybersecurityniveau.

Het belang dat NIS 2 beoogt te beschermen, is vooral een maatschappelijk belang. Zeker indien het (cyber)risicobewustzijn van bedrijven en organisaties laag is, loopt het maatschappelijk belang niet altijd gelijk met hun (gepercipieerde) eigen belang. Risicogebaseerde regelgeving gaat ervan uit dat normadressaten de maatschappelijke belangen internaliseren en laten meewegen in hun risicomanagement.[125] Ten aanzien van NIS 1 is in de literatuur gesignaleerd dat dit in de praktijk niet altijd gebeurt en dat bedrijven mogelijk dus slechts minimale maatregelen zullen treffen.[126]

De aangescherpte handhavingsbevoegdheden van NIS 2 kunnen bijdragen aan het vergroten van de externe prikkel voor bedrijven en organisaties om meer of verdergaande maatregelen te treffen dan zij mogelijk op grond van een eigen risicoafweging hadden gedaan. In dat opzicht kan NIS 2 inderdaad bijdragen aan een hoger niveau van cybersecurity binnen de kritieke infrastructuur. Praktisch gezien is het de vraag of de bevoegde autoriteiten voldoende capaciteit hebben om effectief te kunnen handhaven. Met betrekking tot de AVG is de klacht al jarenlang dat de Autoriteit Persoonsgegevens onvoldoende budget heeft om effectief te handhaven.[127] Handhaving van de implementatie van NIS 2 betekent een extra taak voor de verschillende sectorale toezichthouders. Die taak wijkt bovendien mogelijk inhoudelijk af van waar deze toezichthouders zich normaliter mee bezighouden. Ook ten aanzien van andere regelgeving, bijvoorbeeld het voorstel voor de Cyber Resilience Act die ziet op de veiligheid van producten met digitale elementen, heeft men de vraag gesteld waar voldoende gekwalificeerd personeel vandaan moet komen, bijvoorbeeld voor het uitvoeren van conformiteitsbeoordelingen.[128] Die vraag geldt onzes inziens ook voor het uitvoeren van audits onder NIS 2.

Daarbij komt dat het voor de externe bevoegde autoriteiten een behoorlijke opgave zou kunnen zijn om effectief te controleren of essentiële en belangrijke entiteiten op adequate wijze een cybersecuritybeleid in de organisatie hebben geïmplementeerd. In de eerste plaats kunnen ook de bevoegde autoriteiten moeite hebben met het maken van de vertaalslag tussen de juridische open normen en de feitelijke implementatie daarvan. Daarnaast kan niet alleen worden gekeken naar de implementatie van technische maatregelen, nu uit NIS 2 volgt dat een passend cybersecuritybeleid ook ziet op het inregelen van processen, trainen van mensen en algehele *governance*. Bij het onderzoek naar Waternet heeft de Inspectie Leefomgeving & Transport bijvoorbeeld terecht ook gekeken naar de algemene werkcultuur om het cybersecurityniveau goed te kunnen begrijpen.[129] Voor een externe toezichthouder kan het controleren van de implementatie van dergelijke maatregelen in een organisatie een intensieve en daarmee tijdrovende taak zijn. Opvallend detail is daarom dat, anders dan bijvoorbeeld de AVG, NIS 2 niet nadrukkelijk verplicht tot het aanstellen van een onafhankelijke, interne toezichthouder, zoals de Functionaris Gegevensbescherming onder de AVG. Een *Chief Information Security Officer* die regelmatig daadwerkelijk op de werkvloer aanwezig is, zou veel eerder kunnen bijsturen dan de bevoegde autoriteiten achteraf. Dit zou kunnen leiden tot een verlichting van de last van de sectorale toezichthouder en daarmee tot effectievere handhaving.[130]

5. Tot besluit

NIS 2 vormt een belangrijke stap in de digitale strategie van de EU. Door de uitbreiding van het toepassingsbereik en de aanscherping van de beveiligingseisen en handhavingsbevoegdheden laat de EU zien dat zij grote prioriteit toekent aan betere cybersecurity. Een gezamenlijke aanpak is noodzakelijk om het gemeenschappelijk niveau van cybersecurity in de EU te verhogen. Daarbij verschuift NIS 2 de verantwoordelijkheid voor cybersecurity duidelijk omhoog richting de *boardroom*.

NIS 2 tracht de beveiliging, veiligheid en weerbaarheid van (kritieke) dienstverlening te waarborgen. Daarmee vormt NIS 2 een belangrijk onderdeel van de Europese digitale strategie, met als nadere uitwerking de Digital Operational Resilience Act voor de financiële sector en als tegenhanger de voorgestelde Verordening voor de veiligheid van producten met digitale elementen, de Cyber Resilience Act.[131] Met dit pakket maakt Europa een grote slag in het reguleren van de digitale wereld. Van bedrijven en organisaties vergt dit een verdere omslag in de wijze waarop zij omgaan met digitale risico's, waardoor beveiliging, veiligheid en weerbaarheid ook in onze digitale samenleving heel normaal wordt. •

117. Zie par. 3.1.

118. T. Sievers, 'Proposal for a NIS Directive 2.0: companies covered by the extended scope of application and their obligations', *International Cybersecurity Law Review* 2021/2, p. 223-231.

119. Zie bijvoorbeeld de Digital Operational Resilience Act, die van toepassing is op de financiële sector en bij overlappende bepalingen als specialis van NIS 2 heeft te gelden.

120. Zie bijvoorbeeld M.J.C. van Falier & A.J.F. Lafarre, 'Risicomanagement in een data-gedreven wereld: de rol en expertise van bestuurders en commissarissen nader beschouwd', *TvOB* 2020/4, p. 118-129; C.D.J. Bulten, B.P.F. Jacobs & C.J.H. Jansen, 'Cybersecurity: Chefsache!', *Ondernemingsrecht* 2021/79, p. 475 e.v.

121. Art. 24 lid 3 sub a en b NIS 2.

122. Hofman 2022, p. 325-327.

123. Vgl. J.D. Michels & I. Walden, 'Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?', *European Law Review* 2020/45, p. 25-47.

124. Vgl. Michels & Walden 2020.

125. *Ibid*, p. 39.

126. *Ibid*, p. 39-40.

127. Zie bijvoorbeeld de Position Paper uit 2021 (autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_position_paper_mei_2021.pdf) en het Onderzoek taken en financiële middelen bij de AP uit 2020 (autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/kpmg-onderzoek_taken_en_middelen_ap.pdf).

128. Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020, COM(2022) 454 final, 2022/0272(COD), 15 september 2022. Zie ook de uitspraken van Europarlementariër Groothuis in 'Waarom er grote zorgen zijn over nieuwe Europese security-wetgeving', *AG Connect* 15 november 2022.

129. Inspectie Leefomgeving en Transport, *Onderzoeksrapport Stichting Waternet*, 31 maart 2021, online te raadplegen via ilent.nl/documenten/rapporten/2021/4/2/onderzoeksrapport-stichting-waternet.

130. Mogelijk biedt de *governance*-bepaling in NIS 2 aanknopingspunten voor bestuurders om een CISO aan te stellen.

131. (Het voorstel voor) de Cyber Resilience Act kent op zichzelf weer de nodige raakvlakken met de AI Act, de AI Liability Directive en de herziene Productaansprakelijkheidsrichtlijn. Zie over de Cyber Resilience Act en aanpalende regelgeving: N.M. Brouwer & M.D. Reijneveld, 'De ontwikkeling van cyberveiligheid in Europa: wetsvoorstel voor de Cyber Resilience Act', *NJB* 2023/675, afl. 10, p. 758-769.