Consultatie Cyberbeveiligingswet

1 juli 2024

HVG Law, EY Accountants & EY Adviseurs

1. INLEIDING

1.1 Door advocaten van HVG Law (Digital, Cyber & Privacy) is, gezamenlijk met EY Adviseurs (Technology Consulting) en EY Accountants (Technology Risk), de volgende reactie geschreven ten aanzien van de consultatieversie van de Cyberbeveiligingswet.

1.2 EY Accountants, EY Adviseurs en HVG Law (**wij, ons**) verwelkomen de implementatie van de NIS2-Richtlijn middels de Cyberbeveiligingswet. Het is immers van groot belang om te bewerkstelligen dat er een duidelijk raamwerk ontstaat ter harmonisatie van weerbaarheid in de gehele IT-waardeketen. Wij hebben met aandacht het voorstel voor de Cyberbeveiligingswet bestudeerd en wij zien daarin enkele onderwerpen waarbij wij graag een aantal opmerkingen plaatsen. De opmerkingen zien toe op de volgende vier onderwerpen: (i) governance en aansprakelijkheid (opgesteld door EY Adviseurs); (ii) maatregelen (opgesteld door EY Adviseurs en EY Accountants gezamenlijk); (iii) handhaving en toezichthouders (opgesteld door HVG Law); en (iv) reikwijdte en definities (opgesteld door HVG Law).

2. EY: GOVERNANCE EN AANSPRAKELIJKHEID

Introductie

2.1 De voorgestelde Cyberbeveiligingswet (Cbw) is een belangrijke stap om verantwoordelijkheid omtrent cybersecurity voor essentiële en belangrijke entiteiten te waarborgen op bestuursniveau. Voor de onderdelen governance en aansprakelijkheid vermelden wij graag onze zienswijze omtrent de volgende punten:

(i) Kennis en vaardigheden inzake het identificeren en beoordelen van risicobeheersingsmaatregelen

(ii) Training en certificering

Kennis en vaardigheden inzake het identificeren en beoordelen van risico-beheersingsmaatregelen

2.2 Wij erkennen dat de formalisatie van bestuursverantwoordelijkheid voor informatiebeveiliging, middels artikel 26 Cbw, een positieve impact kan hebben om dit onderwerp te agenderen op het niveau van het bestuur van essentiële en belangrijke entiteiten. Dit bevordert de daadwerkelijke implementatie van maatregelen en versterkt daarmee de veiligheid van de IT-waardeketen.

2.3 Voorts begrijpen wij daarbij dat de huidige formulering van artikel 26 lid 2 sub a en b Cbw direct is overgenomen uit artikel 20 lid 2 van de NIS2-Richtlijn.

2.4 Echter, de bepaling lijkt te breed te zijn overgenomen, breder dan de Europese wetgever bedoeld lijkt te hebben. In de huidige opzet heeft de bepaling namelijk mogelijk als ongewenst effect dat bestuurders worden geacht om in algemene zin risico's te kunnen identificeren, en beheersmaatregelen te beoordelen, in plaats van alleen de risico's en beheersmaatregelen ten aanzien van de diensten die door de entiteit worden verleend.

2.5 Echter, de identificatie van cybersecurityrisico's en de beoordeling van de gevolgen van deze risico's vergt, in de meeste gevallen, diepgaande kennis van informatiesystemen, -processen, en de bijbehorende reeds getroffen maatregelen, in de specifieke context van de desbetreffende entiteit. Het

zou dus te ver gaan om de identificatie en beoordeling van risico's en beheersmaatregelen los te koppelen van de diensten van de desbetreffende entiteit.

2.6 Wij zouden aanbevelen om deze formulering aan te passen in die zin dat eenzelfde specificering wordt aangebracht in sub a en sub b als reeds is aangebracht in sub c, om aan te duiden dat deze verplichtingen specifiek gelden binnen de context van de desbetreffende entiteit.

Training en certificering

2.7 Wij verwelkomen de plicht voor bestuurders ex artikel 26 leden 3, 4 en 5 Cbw om deel te nemen aan trainingen om hun kennis en vaardigheden op het gebied van de beveiliging van netwerk- en informatiesystemen te verhogen. Zonder een dergelijk ondersteunend stelsel zal het lastig zijn om bestuurders volledig de verantwoordelijkheid te laten nemen voor de cybersecurityrisico's binnen de essentiële of belangrijke entiteit.

2.8 Artikel 26 lid 6 Cbw vermeldt ten aanzien van voornoemde trainingen dat nadere details omtrent trainingen gespecificeerd zullen worden middels Algemene Maatregelen van Bestuur (**AMvB**), waaronder regels over de duur en het niveau van de training.

2.9 Het probleem met de huidige opzet van de bepaling is echter dat op voorhand niet voldoende duidelijk is welke instellingen toegestaan zullen zijn om dergelijke trainingen te geven. Daarnaast mist het voorstel details over de frequentie van de trainingen, de wijze waarop certificaten van deelname overlegd dienen te worden alsmede de instantie waaraan deze overleg dienen te worden.

2.10 Hoewel wij ervan uitgaan dat dergelijke onderwerpen reeds geagendeerd waren voor de AMvB, achten wij deze van dermate groot belang dat reeds in het wetsvoorstel dan wel bij Memorie van Toelichting verduidelijkt dient te worden hoe het stelsel van trainingen zal functioneren. Wij bevelen dus aan om nader te verduidelijken hoe deze norm ingevuld zal worden in de AMvB. Daarbij vernemen wij specifiek graag de eisen die gesteld zullen worden aan entiteiten die gemachtigd zijn desbetreffende trainingen en certificaten uit te geven, en op welke wijze entiteiten certificaten dienen te overleggen, de frequentie hiervan, en aan welke autoriteit of instantie.

3. EY: MAATREGELEN

Introductie

3.1 Wij verwelkomen de invoering van maatregelen om operationele weerbaarheid te waarborgen en inbreuken op deze weerbaarheid te melden. Zo erkennen wij de noodzaak van bijvoorbeeld de zorgplicht conform artikel 23 lid 1, waarbij iedere essentiële en belangrijke entiteit passende en evenredige technische, operationele en organisatorische maatregelen neemt om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt. Deze zorgplicht dient als belangrijke bouwsteen voor de harmonisatie van sectorale cybersecuritymaatregelen. Daarbij wensen wij wel specifiek voor de opgenomen maatregelen nadere opmerkingen te delen omtrent de volgende punten:

(i) Specificatie van maatregelen in AMvB

(ii) Specificatie van meldplicht voor ontvangers van diensten

Specificatie van maatregelen in AMvB

3.2 De Cbw legt de globale verwachtingen omtrent cybersecurity risicomanagement vast voor essentiële en belangrijke entiteiten. De Cbw voorziet middels artikel 23 verdere invulling van verplichtingen door middel van AMvB door de bevoegde autoriteiten.

3.3 De gekozen aanpak biedt ruimte om passende maatregelen te definiëren per sector. Wij willen hierbij opmerken dat deze aanpak mogelijk zou kunnen leiden tot een gefragmenteerd raamwerk van verplichtingen voor entiteiten die actief zijn in meerdere sectoren.

3.4 Wij adviseren om, waar mogelijk, een eenduidige aanpak te hanteren in de specificatie van maatregelen per sector en om minimumharmonisatie als uitgangspunt te kiezen, vergelijkbaar met de BBN-methodiek in de Baseline Informatiebeveiliging Overheid.

3.5 Daarnaast merken wij graag op dat er geen tijdslijnen zijn gedefinieerd omtrent de sectorale AMvB. Onze sector-overstijgende ervaring is dat essentiële en belangrijke entiteiten gebaat zijn bij een zekere mate van voorspelbaarheid om adequate maatregelen te kunnen nemen. Daarom adviseren wij om een duidelijke tijdslijn te definiëren omtrent de publicatie van AMvB door de bevoegde autoriteiten.

3.6 Tot slot wordt, in tegenstelling tot artikel 21 lid 2 van de NIS2-richtlijn, in de Cbw geen minimale set van onderwerpen beschreven waarvoor maatregelen dienen te worden getroffen. Hierdoor bestaat onduidelijkheid voor entiteiten welke onderwerpen minimaal onderdeel dienen te zijn van de technische, operationele en organisatorische maatregelen.

3.7 Wij adviseren om in de wet te verduidelijken welke onderwerpen minimaal onderdeel dienen te zijn van de technische, operationele en organisatorische maatregelen.

Specificatie van meldplicht voor ontvangers van diensten

3.8 Wij verwelkomen artikel 32 Cbw, dat regelt dat een essentiële of belangrijke entiteit de ontvangers van haar diensten in kennis stelt van significante incidenten die een nadelige invloed kunnen hebben op de verlening van haar diensten of van significante cyberdreigingen. Een dergelijke meldplicht garandeert een effectievere aanpak van cyberdreigingen die mogelijk effect kunnen hebben in de gehele IT-waardeketen.

3.9 Wij bespreken eerst graag in het bijzonder lid 2, dat specifiek vermeldt dat het bij de meldplicht van cyberdreigingen gaat om de ontvangers van diensten, die “mogelijkerwijs door een significante cyberdreiging in relatie tot het ontvangen van die diensten worden getroffen”.

3.10 De oorspronkelijke tekst van de artikel 23 lid 2 van de NIS2-Richtlijn stelt dat essentiële en belangrijke entiteiten verplicht moeten zijn om “de ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen” onverwijld mee te delen welke maatregelen zij kunnen nemen in reactie op die dreiging.

3.11 Het stuk “in relatie tot het ontvangen van die diensten” is dus toegevoegd ten opzichte van de NIS2-Richtlijn. Wij begrijpen de keuze om het artikel zo te formuleren. Immers, het is niet de bedoeling (noch wenselijk) dat essentiële en belangrijke entiteiten hun klanten over *alle* cyberdreigingen moeten informeren, bijvoorbeeld als die dreigingen geen relatie hebben met hun bedrijfsactiviteiten of de door hen geleverde diensten.

3.12 Echter, door de wijze waarop de bepaling nu is geformuleerd, kan de bepaling mogelijk te restrictief geïnterpreteerd worden (i.e. restrictiever dan oorspronkelijk bedoeld door de Europese wetgever). Immers, conform NIS2 dient melding gemaakt te worden van alle cyberdreigingen die ernstige gevolgen kunnen hebben door het veroorzaken van aanzienlijke materiële of immateriële schade, die de ontvangers van diensten mogelijkerwijs kunnen treffen. Dergelijke dreigingen kunnen echter ook

bestaan zonder directe relatie tot het ontvangen van de diensten, bijvoorbeeld bij een risico op diefstal van data.

3.13 Wij raden derhalve aan om te specificeren dat de melding dient plaats te vinden bij alle significante cyberdreigingen die kunnen bestaan als gevolg van het ontvangen van de diensten, niet alleen bij de cyberdreigingen met relatie tot de diensten.

3.14 Voorts raden wij aan om de melding van significante incidenten (i.e. reeds verwezenlijkte dreigingen) ook los te koppelen van de diensten, in tegenstelling tot hetgeen is opgenomen in artikel 23 lid 1 van de NIS2-Richtlijn alsmede artikel 32 lid 1 Cbw.

3.15 Het kan namelijk voorkomen dat een incident zich reeds verwezenlijkt voordat de essentiële of belangrijke entiteit in staat is geweest om de dreiging te identificeren. In een dergelijk geval bestaat geen meldplicht, indien er geen sprake is van een nadelige invloed op de diensten.

3.16 Echter, zoals hiervoor besproken, zijn er incidenten die significante nadelige gevolgen kunnen hebben zonder directe relatie tot het ontvangen van de diensten, zoals diefstal van data (specifiek relevant is hier uiteraard data niet zijnde persoonsgegevens, waar nog geen meldplicht op rust). Hierbij kan de dienst vrijelijk doorlopen, maar de ontvanger van de dienst zal alsnog nadelige effecten (kunnen) ondervinden.

3.17 In dit kader adviseren wij de rapportageplicht ex artikel 32 lid 1 Cbw te verruimen in die zin dat zij niet enkel zal gelden voor zover een incident nadelige invloed kan hebben op de verlening van de diensten, maar ook wanneer de ontvangers nadelige invloed ervaren van het incident (bijvoorbeeld in het geval van het stelen van data).

3.18 Hierbij zou kunnen worden aangesloten bij de volgende elementen uit het begrip ‘beveiliging van netwerk- en informatiesystemen’ uit de NIS2-Richtlijn: “elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen”.

4. HVG LAW: HANDHAVING EN TOEZICHTHOUDERS

Introductie

4.1 Wij erkennen de waarde van toezicht onder de Cbw. Effectief toezicht waarborgt de implementatie van maatregelen, hetgeen de operationele weerbaarheid van de gehele IT-waardeketen versterkt. Evenwel hebben wij zorgen over bepaalde aspecten van het voorgestelde toezichtstelsel onder de Cbw. Wij wensen specifiek de volgende punten in dit onderwerp te bespreken:

(i) Sectoraal toezicht versus gecentraliseerd toezicht

(ii) Handhavingsinstrumentarium

Sectoraal toezicht versus gecentraliseerd toezicht

4.2 Artikel 16 Cbw bouwt voort op het reeds onder de Wbni gevestigde toezichtstelsel, waarbij de toezichthoudende taak toegewezen is aan de vakministers en door hen gedelegeerd is aan een inspectiedienst, dan wel toezichthoudende autoriteit, onder de bevoegdheid van die respectievelijke ministers.

4.3 Wij begrijpen dat gekozen is voor een systeem dat voortbouwt op de Wbni, mede omdat het nu eenmaal eenvoudiger is om bestaand beleid voort te zetten dan om over te gaan tot het opzetten van een nieuw toezichtstelsel. Voorts begrijpen wij dat het opzetten van een nieuwe toezichthoudende autoriteit meer investeringen zouden kosten en wij begrijpen eveneens dat sommige bedrijven juist de voorkeur hebben om te melden aan de toezichthouder onder de vakminister en willen vermijden dat ze bij verschillende toezichthouders moeten melden.

4.4 Echter, in de praktijk is gebleken dat het bestaande toezichtstelsel onder de Wbni niet geheel effectief is. Op basis van het rapport 'Samenhangend inspectiebeeld cybersecurity vitale processen 2021-2022', afkomstig van de toezichthouders zelf, kan geconcludeerd worden dat er verschillende niveaus van kennis over cybersecurity zijn tussen toezichthouders en dat dit leidt tot een verschillende aanpak voor bedrijven.

4.5 Wij vrezen dat de keuze om wederom sectoraal toezicht te implementeren voor de Cbw zou kunnen leiden tot onbedoelde negatieve effecten, doordat er een gefragmenteerd en inefficiënt systeem ontstaat dat afdoet aan de rechtszekerheid van onder toezicht staande entiteiten. Immers, wat een entiteit in de praktijk kan verwachten van de toezichthouder zal in grote mate per sector verschillen. Daarnaast zou het verschil in kennis bij de toezichthouder kunnen leiden tot ongelijkheid in niveaus van cybersecurity per sector, wat afdoet aan de veiligheid van de gehele IT-waardeketen en contrair zou zijn aan de doelen van de Europese wetgever bij het opstellen van de NIS2-Richtlijn. Het uitgangspunt van deze richtlijn is immers juist beveiliging van de gehele IT-waardeketen door middel van minimumharmonisatie.

4.6 Zeker nu de wet het aanwijzen van specifieke maatregelen overlaat aan (nog op te stellen) AMvB, zoals hiervoor besproken, is het van belang om een uniform, geharmoniseerd kader te creëren voor (toezicht op) cybersecurity in Nederland. Daarvoor is een meer gecentraliseerd toezichtstelsel nodig, met een toezichthouder die de juiste kennis en voldoende capaciteit heeft om aandacht te besteden aan dit onderwerp. Daar komt bij dat een centrale toezichthouder effectief toezicht kan houden op de uniforme, juiste aanpak van kwetsbaarheden en dreigingen. IT-dreigingen hebben immers ook geen sectorale aanpak – één bepaalde dreiging kan zich in iedere sector voordoen. Indien een dergelijke dreiging in de ene sector effectief gemitigeerd wordt en in een andere sector niet, dan kan het keteneffect er alsnog toe leiden dat beide sectoren geraakt worden door het verwezenlijken van die dreiging. Het opzetten van een centrale toezichthouder zorgt dus voor meer geharmoniseerde risicomitigatie.

4.7 Omdat wij begrijpen dat dergelijke ingrijpende wijzigingen in reeds voorgestelde wetgeving lastig kunnen zijn, zeker met het oog op de naderende deadline voor implementatie, stellen wij de volgende drie opties voor die er met minimale wijzigingen aan de wettekst alsnog voor zouden kunnen zorgen dat toezicht onder de Cbw meer gecentraliseerd is en daarmee effectiever is. Wij hebben deze opties gerangschikt van meer naar minder gecentraliseerd.

(i) Optie 1: het afschaffen van sectoraal toezicht en het volledig centraliseren van toezicht onder de Cbw, middels delegatie vanuit de vakministers. Hoewel de vakministers in theorie de toezichthoudende bevoegdheid zouden hebben, delegeren zij dit aan een centrale (nog op te zetten dan wel reeds bestaande) toezichthouder, verantwoordelijk voor het toezicht op alle sectoren in de praktijk. De voordelen hiervan zijn dat dit de standaard van cybersecurity zal verhogen en dat er meer duidelijkheid en rechtszekerheid bewerkstelligd wordt voor de onder toezicht staande entiteiten. Evenwel begrijpen wij dat nadelen hiervan kunnen zijn dat slechts beperkte sectorkennis aanwezig zou zijn bij de toezichthouder, waarbij het uitbreiden van deze sectorkennis kosten zou meebrengen, en dat onder toezicht staande entiteiten mogelijk een dubbele rapportageverplichting hebben als gevolg van sectorale wetgeving.

(ii) Optie 2: een hybride model, in lijn met hetgeen in Italië geïmplementeerd is voor toezicht onder de NIS-Richtlijn. Hierbij zou een centrale toezichthouder opgezet dan wel aangesteld worden die gericht is op cybersecurity in het algemeen. Deze toezichthouder zou fungeren als centraal rapportagepunt voor sectorale toezichthouders en als single point of contact onder de Cbw. Hierdoor kunnen de sectorale toezichthouders ondersteund worden met voldoende technische kennis, maar wordt voorkomen dat sectorale kennis verloren gaat en dat er een dubbele rapportageverplichting ontstaat voor onder toezicht staande entiteiten.

(iii) Optie 3: toezichthouden op basis van centrale standaarden. Wij hebben kennisgenomen van de initiatieven in België omtrent implementatie van de NIS2-Richtlijn, specifiek het opzetten van het CyberFundamentals Framework. Door het definiëren van algemene, risico-gebaseerde standaarden is daar een geharmoniseerd stelsel opgezet dat effectiever toezicht mogelijk maakt in de praktijk. Indien er wordt gekozen voor volledig sectoraal toezicht, dan heeft het de voorkeur om een dergelijk stelsel eveneens in Nederland te implementeren. Daarbij is het onvoldoende om aan te sluiten bij een internationale (ISO-)standaard – dat zou immers de risico-gebaseerde aanpak van de NIS2-Richtlijn tenietdoen. Het Nederlandse stelsel zou, evenals het Belgische raamwerk, diverse niveaus van beveiligingsmaatregelen dienen te hanteren die zijn afgestemd op het risiconiveau van de entiteit. Op die manier hebben sectorale toezichthouders duidelijkere handvatten om de implementatie van beveiligingsmaatregelen te toetsen. Dit zou eveneens gecombineerd kunnen worden met (vrijwillige dan wel verplichte) certificering, zoals voorgesteld in België.

Handhavingsinstrumentarium

4.8 Het handhavingsinstrumentarium van de toezichthouder onder de Cbw is uitgebreid ten opzichte van de Wbni, met onder andere het toevoegen van de controlefunctionaris (artikel 68 Cbw) en de beveiligingsscan (artikel 69 Cbw).

4.9 Hoewel wij het uitbreiden van het handhavingsinstrumentarium verwelkomen om een risico-gebaseerde benadering in het toezicht te ondersteunen, achten wij de voorwaarden voor gebruik van deze bevoegdheden (alsook andere controlebevoegdheden) nogal ruim geformuleerd. Specifiek gaan wij graag nader in op het aanstellen van een controlefunctionaris.

4.10 Wij begrijpen dat de aanstelling van een controlefunctionaris gebonden is aan diverse bestaande geschreven en ongeschreven rechtsbeginselen, waaronder de algemene beginselen van behoorlijk bestuur. Een toezichthouder zal dus niet zomaar in staat zijn om een controlefunctionaris aan te wijzen.

4.11 Evenwel gaat het hier om een bijzonder ingrijpende maatregel, waarbij een onder toezicht staande entiteit verplicht is om op haar kosten een onafhankelijk deskundige in te schakelen. Naast de kosten brengt dit eveneens risico’s met zich voor de bedrijfsgeheimen en waardevolle knowhow van entiteiten, informatie die zij niet graag prijsgeven aan derden.

4.12 Wij begrijpen dat, conform lid 4 van artikel 68 Cbw, bij AMvB aanvullende regels gesteld kunnen worden, waaronder de vereisten die gelden voor de aanwijzing van de controlefunctionaris. Gelet op de grote impact die het gebruik van een dergelijke bevoegdheid zou hebben, achten wij deze formulering onvoldoende. Wij stellen voor dat in het artikel zelf nadere voorwaarden opgenomen worden die garanderen dat de aanstelling van een controlefunctionaris proportioneel is, waaronder een geheimhoudingsplicht voor de controlefunctionaris.

4.13 Overigens verdient het vermelding dat naar ons inzicht het gedeelte “zijnde een natuurlijk persoon” uit artikel 68 lid 4 Cbw verwijderd dient te worden. Immers, dit is geen vereiste van de NIS2-Richtlijn en in bepaalde gevallen kan het juist voordelen bieden om een samenwerkingsverband van deskundigen aan te stellen als controlefunctionaris, bijvoorbeeld bij complexe entiteiten of entiteiten met een brede scope van bedrijfsactiviteiten.

5. HVG LAW: REIKWIJDTE EN DEFINITIES

Introductie

5.1 Vanwege het tempo van zowel grensoverschrijdende ontwikkelingen als dreigingen binnen cybersecurity, is het een welkome toevoeging dat meer entiteiten binnen de ICT-sector onder de reikwijdte van de NIS2-Richtlijn en de Cbw kunnen vallen en harmonisatie op Europese Unie-niveau wordt bewerkstelligd. Gezien de mate van impact bij een incident binnen deze sector, is het begrijpelijk dat een brede definitie wordt toegekend aan de aanbieders van beheerde diensten en beheerde beveiligingsdiensten.

5.2 Een belangrijk aandachtspunt bij brede definities is het opbouwen van een duidelijke afbakening door de wetgever om entiteiten handvatten te bieden om zélf te beoordelen of zij binnen of buiten de brede definitie vallen. Aangezien de NIS2-Richtlijn en daarmee de Cbw gestoeld zijn op de principes van zelfevaluatie door entiteiten wat betreft het al dan niet gereguleerd worden door deze voorgaande wetgeving, levert het ontbreken van deze duidelijke afbakening een hoge mate van rechtsonzekerheid op voor entiteiten. Daarbij gaat deze reactie nader in op de definities die (niet) worden gegeven aan aanbieders van beheerde diensten en aanbieders van beheerde beveiligingsdiensten, alsmede de consequenties van voornoemde (gebrek aan) definities en mogelijke oplossingen.

Definities

5.3 Binnen de Cbw en de NIS2-Richtlijn zijn momenteel (slechts) enkele handvatten aanwezig voor entiteiten om de beoordeling te maken of en in hoeverre zij als aanbieder van beheerdiensten en beheerde beveiligingsdiensten worden geclassificeerd.

5.4 Artikel 1, tweede streep, Cbw verwijst voor wat betreft de begripsbepalingen van aanbieders van beheerde diensten en aanbieders van beheerde beveiligingsdiensten terug naar artikel 6 van de NIS2-Richtlijn. Deze twee categorieën van entiteiten worden in de Bijlage 1 van de Cbw als subsectoren geschaard onder de sector beheer van ICT-diensten, zijnde business-to-business aanbieders. Ook in Bijlage 1 bij de NIS2-Richtlijn wordt deze sector genoemd. Dat suggereert dat het in ieder geval moet gaan om een business-to-business dienstverlening en ICT-diensten.

5.5 Artikel 6, onder 39 en 40, NIS2-Richtlijn bieden de definities van de aanbieder van beheerde diensten en beheerde beveiligingsdiensten:

(a) “aanbieder van beheerde diensten”: een entiteit die diensten verleent die verband houden met de installatie, het beheer, de exploitatie of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesystemen, via bijstand of actieve administratie bij de consument ter plaatse of op afstand;

(b) “aanbieder van beheerde beveiligingsdiensten”: een aanbieder van beheerde diensten die bijstand biedt of verleent voor activiteiten die verband houden met risicobeheer op het gebied van cyberbeveiliging.

5.6 In de NIS2-Richtlijn vindt men nog de definities van digitale dienst, cloudcomputingdienst (een categorie digitale dienst) en datacentrumdienst:

(a) “digitale dienst”: een dienst zoals gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (zijnde: elke dienst van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht);

(b) “cloudcomputingdienst”: een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn;

(c) “datacentrumdienst”: een dienst die structuren of groepen van structuren omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van IT en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole.

5.7 Zowel de Cbw, inclusief de Memorie van Toelichting, als de NIS2-Richtlijn bieden entiteiten geen verdere richtlijnen om de zelfbeoordeling uit te voeren waar het gaat om aanbieders van beheerde diensten en beheerde beveiligingsdiensten.

5.8 In paragraaf 5.2.1. van de Memorie van Toelichting op de Cbw staat vermeld dat “in de overheidscommunicatie over dit wetsvoorstel worden digitale hulpmiddelen ter beschikking gesteld om entiteiten te helpen bij het bepalen van hun omvang.” Het is daarbij voor de lezer niet helder naar welke overheidscommunicatie wordt verwezen en waar een entiteit terecht zou kunnen voor deze digitale hulpmiddelen, mocht zij worstelen met het beoordelen van de toepasselijkheid van de NIS2-Richtlijn en Cbw.

Consequenties

5.9 Bovenstaand kader biedt een uitgebreid doch verwarrend overzicht voor entiteiten in hun beoordeling van de toepasselijkheid van de definities uit de NIS2-Richtlijn en Cbw. Het is mogelijk dat een entiteit niet in staat is om deze vertaalslag te maken, waarbij de verschillende bovenstaande definities ogenschijnlijk overlap zullen hebben. Een aanbieder van beheerdiensten zou bijvoorbeeld ook cloudcomputingdiensten, datacentrumdiensten of digitale diensten kunnen aanbieden.

5.10 De eerste vraag die een entiteit zichzelf stelt bij nieuwe wet- of regelgeving is: “Is dit op mij van toepassing?”. We zien in de markt een grote hoeveelheid entiteiten die momenteel over onvoldoende informatie kunnen beschikken om deze vraag te beantwoorden. De huidige set aan definities en de afwezigheid van duidelijke uitleg daarbij draagt bij aan het bestaan van rechtsonzekerheid bij entiteiten in de digitale sector.

5.11 De Europese wetgever heeft met de NIS2-Richtlijn getracht om een duidelijk overzicht in te stellen van onder meer aanbieders van beheerde diensten en beveiligingsdiensten via een door ENISA op te richten en te beheren register van gerelateerde entiteiten. Dit moet worden gestoeld op door de lidstaten te verstrekken informatie en waar nodig, nationale mechanismen voor zelfregistratie van de betrokken entiteiten, zoals nader uiteengezet in artikel 27 van de NIS2-Richtlijn.

5.12 Het registratiemechanisme komt ook terug in artikelen 45 en 47 Cbw, mede van toepassing voor de aanbieders van beheerde diensten en beheerde beveiligingsdiensten. Dit mechanisme is afhankelijk van de informatievoorziening die vanuit entiteiten zelf wordt geleverd op basis van de verplichtingen

uit de Cbw. Als een entiteit niet in staat is om de eerste vraag over toepasselijkheid goed of volledig te beantwoorden, zal dit ook de informatievoorziening ernstig beïnvloeden. Daarmee worden ook de doelstellingen van het ENISA-register belemmerd aangezien de grensoverschrijdende informatievoorziening ontoereikend en onvolledig kan raken.

5.13 Op basis van artikel 21(5) en artikel 23(11) NIS2-Richtlijn komt de Europese Commissie nog met nadere uitvoeringshandelingen over de technische en methodologische vereisten en rapportageverplichtingen uit artikel 21(2) en artikel 23(3) voor onder meer de aanbieders van beheerde (beveiligingsdiensten). Wederom zal het gecreëerde onvermogen voor de beoordeling van de toepasselijkheid uiteindelijk ook mogelijk een gebrekkige implementatie van de geharmoniseerde horizontale beveiligings- en rapportageverplichtingen tot gevolg hebben.

Oplossingen

5.14 De Digital Operational Resilience Act (DORA) is de lex specialis van de NIS2-Richtlijn, waarbij in de DORA ook ruim aandacht wordt gegeven aan de reikwijdte van ICT-diensten. De Europese wetgever heeft met de DORA ook het belang benadrukt van het verhogen van de weerbaarheid rondom ICT-diensten, specifiek voor de financiële sector. Dit lijkt hetzelfde digitale component als waar in de NIS2-Richtlijn zorg en aandacht aan wordt besteed met het formuleren van de aanbieders van gerelateerde diensten.

5.15 De bijlage 1 bij zowel de Cbw als NIS2-Richtlijn bevat de sector Beheer van ICT-Diensten. De definitie van ICT-diensten in DORA is als volgt:

(a) “ICT-diensten”: digitale en gegevensdiensten die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers worden verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten;

5.16 Een verplichting op basis van de DORA is het bijhouden van een register van informatie. Op 10 januari 2024 is een conceptversie gepubliceerd van de *Regulatory Technical Standards (RTS) on the standard templates of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers*. Als onderdeel van dit informatieregister moet ook de categorie van ICT-diensten worden opgegeven. In bijlage 3 bij deze RTS wordt een lijst gegeven van ICT-diensten waaruit gekozen kan worden.

5.17 Deze lijst is een goed voorbeeld van concrete aanvullende middelen die de Nederlandse wetgever kan bieden aan aanbieders van beheerde (beveiligings)diensten om te beoordelen of zij aanbieder zijn van het beheer van ICT-diensten, zoals de sector uit bijlagen 1 van de NIS2-Richtlijn en Cbw.

5.18 Daarbij kan ook de Nederlandse wetgever dergelijke kaders gebruiken om een uniforme informatievoorziening te realiseren op basis van de verplichtingen uit artikelen 45 en 47 Cbw in het kader van het registratiemechanisme, door onder meer de ICT-diensten te integreren.

5.19 Gezien het belang van het reguleren en implementeren van horizontale cybersecurityvereisten in de digitale sector, is het aanvullen van rechtszekerheid door duidelijke en uniform te interpreteren definities cruciaal. Voor de Nederlandse wetgever liggen openingen door te kijken naar vergelijkbare wetgeving zoals de DORA en daaraan verbonden publicaties inclusief RTS.