Post- en bezoekadres
Dr. Kuyperstraat 5
2514 BA Den Haag
T 070-3053333
E info@nlconnect.org
I www.nlconnect.org

Reactie vereniging NLconnect op consultatie Cyberbeveiligingswet (Cbw)

Vereniging NLconnect behartigt de belangen van zo'n 90 partijen uit de telecom- breedband- en glasvezelindustrie. Als branche is het onze ambitie om de voorsprong die ons land heeft op het gebied van digitale connectiviteit te behouden en uit te bouwen door ervoor te zorgen dat elke Nederlander en elk Nederlands bedrijf de beschikking heeft over uitmuntende en veilige breedbandverbindingen. Wij zijn van mening dat een toekomstvaste digitale infrastructuur en hoogwaardige digitale toepassingen van levensbelang zijn voor ons vestigingsklimaat, onze maatschappij en de zich snel ontwikkelende digitale economie. Een veilig en vrij internet is daarbij instrumenteel.

Uiteraard steunt NLconnect het doel om de digitale weerbaarheid te vergroten en de gevolgen van cyberincidenten te verkleinen. In de MvT valt te lezen dat het aantal entiteiten dat onder de Cyberbeveiligingswet (verder: Cbw) komt te vallen wordt geschat op ongeveer 8.100. Deze schatting wordt niet verder onderbouwd, maar roept wel de vraag op hoe deze implementatie beheersbaar kan blijven voor de toezichthouders. Met de Cbw vallen ook steeds meer leden van onze vereniging en van het bredere internet-ecosysteem onder het toepassingsbereik van de regels voor cyberbeveiliging. We stellen het daarom bijzonder op prijs in de gelegenheid te worden gesteld te reageren op deze consultatie van de Cbw. We maken graag de volgende opmerkingen bij de consultatieversie.

Scope van de Cbw in relatie tot de Wwke

Het toepassingsbereik van de Cbw is vastgelegd in hoofdstuk 3 van de Cbw. In de MvT, paragraaf 2.4, wordt daarbij een toelichting gegeven op de verhouding van de Cbw tot de CER-richtlijn, die in de Wet weerbaarheid kritieke entiteiten (verder: Wwke) wordt geïmplementeerd. Entiteiten moeten op basis van de Cbw maatregelen treffen om de risico's voor netwerk- en informatiesystemen te beheersen voor zowel 1) de digitale beveiliging van die systemen als 2) voor de bescherming van de fysieke omgeving en componenten van die systemen, zoals gebouwen en ruimtes waar die systemen zich bevinden. In de MvT wordt daarbij toegelicht dat, indien een incident of bijna-incident gevolgen heeft die zowel de netwerk- en informatiesystemen betreffen als een verstoring van *andere fysieke aspecten die de essentiële dienstverlening raken*, ook de verplichtingen van de Wwke gelden.

Getuige de MvT lijkt het verschil te zitten in 'andere fysieke aspecten die de essentiële dienstverlening raken', niet zijnde de fysieke omgeving of componenten van die systemen. Het zou behulpzaam zijn als dat wordt gespecificeerd en/of hiervan door de wetgever voorbeelden worden gegeven. Daarnaast wordt in de Wwke de toepassing van bepaalde verplichtingen expliciet uitgesloten voor de sectoren bankwezen, financiële infrastructuur en digitale infrastructuur, in elk geval in de artikelen 15 lid 1 (toepassingsbereik en vrijstelling verplichting risicobeoordeling), 17 lid 1 (toepassingsbereik en vrijstelling zorgplicht), artikel 19 lid 1 (toepassingsbereik en vrijstelling meldplicht), artikel 24 lid 1 (vrijstelling aanwijzing verbindingsfunctionaris en meldplicht verlening essentiële diensten aan of in zes of meer lidstaten), en artikel 27 lid 1 (toepassingsbereik en vrijstelling verplichtingen kritieke entiteit van bijzonder Europees belang).

Naar aanleiding hiervan lijkt de conclusie getrokken te kunnen worden dat de Wwke in het geheel niet voor de digitale infrastructuur geldt. Om elke onduidelijkheid daarover weg te nemen verdient het de aanbeveling dit duidelijk in de MvT van zowel de Wwke als de Cbw op te nemen. Voor zover er toch nog verplichtingen zouden gelden verdient het aanbeveling deze nader te specificeren. NLconnect zal dit punt ook inbrengen in de parallel lopende consultatie van de Wwke.

- ***NLconnect verzoekt om de MvT van de Cbw en Wwke aan te passen om de onduidelijkheden over geldende verplichtingen weg te nemen.***

Zorgplicht: geen nationale koppen

De zorgplicht wordt omschreven in artikel 23 lid 1 en 2. NLconnect onderschrijft deze invulling, maar maakt wel enkele kanttekeningen bij de toelichting bij dit artikel in de MvT. Allereerst blijkt uit de MvT, onder paragraaf 5.3.5, dat wordt aangenomen dat, op grond van artikel 23 lid 4 Cwb, in een AMvB maatregelen zullen worden opgenomen die een *hoger beveiligingsniveau* voorschrijven aan bedrijven in Nederland dan het beveiligingsniveau dat voor Europa is vastgelegd in NIS2. NLconnect acht dat onwenselijk: het druist in tegen harmonisatie - een van de belangrijkste doelen van de NIS2 - en is nadrukkelijk niet wenselijk gezien de ervaring met de NIS1. In overweging 4 en 5 van de NIS2 staat beschreven dat een belangrijk gebrek van de NIS1 richtlijn juist was dat er geen uniforme implementatie was in de diverse Europese landen, met als gevolg hogere kosten, negatieve effecten voor de interne markt en een hogere kwetsbaarheid voor cyberdreigingen.[1] Aanvullende vereisten sluiten ook niet aan bij het Hoofdlijnenakkoord van PVV, VVD, NSC en BBB, waarin is opgenomen dat er geen nieuwe nationale koppen op Europees beleid komen.

Ook is de Europese Commissie momenteel bezig een uitvoeringshandeling op te stellen op basis van art 21 lid 5 van NIS2.[2] De verwachting is dat deze uitvoeringshandeling ook richtsnoeren met betrekking tot de invulling van de zorgplicht zal bevatten die in algemene zin zullen gaan gelden. Het verdient ook hierom de aanbeveling om geen aanvullende eisen op te leggen maar aan te sluiten bij de richtsnoeren die uniform in de hele Unie gaan gelden.

- ***NLconnect verzoekt om geen aanvullende vereisten op te leggen aan Nederlandse bedrijven, maar aan te sluiten bij eisen die zijn opgelegd in de NIS2.***

In de MvT, paragraaf 5.3.4, ontbreken in het kader van verplichtingen rondom de toeleveringsketen van partijen in de digitale infrastructuur verder verwijzingen naar de Cyber

[1] Zie onder andere de volgende passages uit overwegingen 4 en 5: "De cyberbeveiligingseisen die worden gesteld aan entiteiten die diensten of economisch belangrijke activiteiten verrichten, verschillen aanzienlijk van lidstaat tot lidstaat wat betreft het soort eisen, de mate van gedetailleerdheid en de wijze van toezicht. Die verschillen brengen extra kosten met zich mee en leveren problemen op voor entiteiten die goederen of diensten aanbieden over de grenzen heen. De eisen die door de ene lidstaat worden gesteld en die verschillen van of zelfs in strijd zijn met de door een andere lidstaat gestelde eisen kunnen een aanzienlijke invloed hebben op deze grensoverschrijdende activiteiten. (...) Al deze verschillen leiden tot een versnippering van de interne markt en kunnen een nadelig effect hebben op de werking ervan, wat met name gevolgen heeft voor de grensoverschrijdende dienstverlening en het niveau van de digitale weerbaarheid als gevolg van de toepassing van diverse maatregelen. Uiteindelijk kunnen die verschillen sommige lidstaten uiteindelijk meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele Unie."

[2] Uiterlijk op 17 oktober 2024 stelt de Commissie uitvoeringshandelingen vast met de technische en methodologische vereisten van de in lid 2 bedoelde maatregelen met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten en aanbieders van vertrouwensdiensten.

Resilience Act (CRA) en Radio Equipment Directive (RED). Deze regelgeving is aanstaande in respectievelijk 2027 en 2025.

- ***NLconnect verzoekt om in MvT paragraaf 5.3.4 verwijzing naar de CRA en RED op te nemen.***

Ten slotte wordt in paragraaf 5.3.5 van de MvT ook ingegaan op de mogelijkheid om verplichte certificering op te leggen met betrekking tot bepaalde ICT-producten, - diensten en -processen. Hier wordt de afweging gemaakt of dit op Europees niveau geregeld moet worden (onder meer in verband met gelijk speelveld) of beperkt kan blijven tot nationaal niveau, bijvoorbeeld omdat een sector niet grensoverschrijdend actief is. In dit laatste geval moet rekening gehouden worden met het feit dat bijvoorbeeld aanbieders van openbare elektronische communicatienetwerken – of diensten weliswaar nationaal of zelfs lokaal kunnen opereren, maar dat hun toeleveranciers in vrijwel alle gevallen grensoverschrijdend actief zijn en dus het risico lopen op deze manier in verschillende lidstaten met verschillende, nationale certificeringsregels te maken te krijgen. Voor onze industrie zou dat onnodig kostbaar zijn. Een internationale oriëntatie van certificering heeft daarmee de sterke voorkeur van NLconnect, uiteraard gebaseerd op objectieve technische eisen.

- ***NLconnect verzoekt om in te zetten op een internationale oriëntatie van certificering.***

<u>Meldplicht: aansluiten bij drempelwaarden van de Wbni</u>
In de MvT, paragraaf 5.5.1, wordt aangegeven dat op basis van artikel 37 Cbw in een Amvb nader regels zullen worden gesteld aan de invulling van de term ‘significant incident’ van artikel 27. De drempelwaarden die zullen worden bepaald zijn bepalend voor de last, de uitvoerbaarheid en de efficiëntie. De last ziet vooral op de administratieve last voor de bedrijven die de meldingen moeten doen, inclusief updates, tussentijdse verslagen, voortgangsverslag en eindverslag. Gelijk daarmee loopt natuurlijk de administratieve last voor het meldpunt en de achterliggende partijen met wie de informatie wordt gedeeld. De uitvoerbaarheid ziet onder meer op de bepaling van artikel 27 lid 2 die ook een ‘kan’ bepaling omvat, waardoor, indien de drempelwaarde niet zorgvuldig wordt gekozen, het meldpunt overspoeld kan worden door meldingen. Dit kan in dat geval leiden tot verlaging van de efficiëntie omdat de daadwerkelijk significante meldingen dan lastiger te identificeren zijn.

NLconnect pleit daarom voor een proportionele en op risico gebaseerde drempelwaarde voor de meldplicht. Focus moet liggen op continuïteit van de essentiële of belangrijke dienstverlening. Het wettelijk melden moet gericht blijven op de (mogelijke) continuïteitssituaties. Voor een algemeen beeld en inzicht in mogelijke aanvallen en kwetsbaarheden et cetera waar entiteiten mee geconfronteerd kan gebruik worden gemaakt van informatie die gedeeld wordt in onder meer de sectorale ISAC’s waar het NCSC aan deelneemt. Onder de Wbni zijn ook drempelwaarden bepaald voor de meldingen op grond van die wet. Deze drempelwaarden worden door NLconnect gesteund.

- ***NLconnect verzoekt om bij de invulling van die term ‘significant incident’ in artikel 27 Cbw aan te sluiten bij de huidige invulling van deze term onder de Wbni.***

<u>Meldplicht: concentratie van meldloketten</u>
Naast de Cbw zijn en worden op onze sector meer wetten van toepassing die een meldplicht bij incidenten met zich meebrengen, zoals de AVG en de CRA. Het is aannemelijk dat bij één incident meldingen moeten worden gedaan bij meerdere toezichthouders, én bij de CSIRTs én bij Enisa. Dergelijke versnippering komt de cyberbeveiliging niet ten goede. Zeker gedurende een incident moet zoveel mogelijk energie worden gestoken in het oplossen

daarvan en niet in het voldoen aan een veelvoud aan meldplichten. Dit moet worden gestroomlijnd.

- ***NLconnect roept op om het aantal meldplichten te beperken, de meldplichten zoveel mogelijk met elkaar in lijn te brengen en het aantal meldloketten te concentreren.***

Meldplicht: zorgvuldig proces rondom ontvangers

Hoewel de meldplicht al een instrument is voor de overheid om geïnformeerd te worden over verstoringen in de dienstverlening van essentiële dienstverleners, wordt deze verplichting vanaf artikel 27 Cbw verder aangescherpt. Hoewel dit in beginsel in lijn is met NIS2, had het onze voorkeur gehad dat op dit punt verdergaande harmonisatie had plaatsgevonden binnen de Unie. Immers, naast een oplossende functie op nationale schaal, hebben meldingen ook tot doel bijvoorbeeld Enisa te voeden met informatie. We maken ons zorgen dat de grote hoeveelheid informatie die ten gevolge van de Cbw gaat stromen al snel onbeheersbaar wordt en daarmee zinledig.

- ***NLconnect adviseert om behoefte en wens aan informatie op elkaar af te stemmen en een duidelijke invulling te geven aan meldplichten bij verstoringen van de dienstverlening.***

Tegelijkertijd levert het veelvuldig melden van verstoringen ook een stroom aan bedrijfsvertrouwelijke informatie op die naar zijn aard niet zomaar verspreid kan worden. De voorgestelde Cbw geeft veel mogelijkheden aan ontvangers van die informatie om deze, zonder de eigenaar ervan te raadplegen, te delen. Deze bevoegdheid is vergaand, hetgeen betekent dat potentieel bedrijfsgevoelige of vertrouwelijke informatie in handen komt van autoriteiten die deze als “nice to know” kunnen opvragen, terwijl de wet gericht is op het “need to know” verkrijgen van informatie. Wanneer het onderscheid niet goed wordt gemaakt en er geen delingscriteria bestaan, zal de cyberveiligheid afnemen in plaats van toenemen. Er is immers op basis van de Cbw geen reden om erop te vertrouwen dat de ontvanger van de informatie er op een zorgvuldige manier mee omgaat. Aldus verwordt een goedbedoelde regulering tot het grootste cyberbeveiligingsrisico dat de essentiële bedrijven kennen. Dat kan niet de bedoeling zijn.

- **NLconnect verzoekt om zorgvuldigheidseisen ten aanzien van gedeelde informatie naar aanleiding van incidenten vast te leggen, teneinde te voorkomen dat de overheid zelf als ontvanger van informatie het grootste cyberbeveiligingsrisico van de essentiële bedrijven wordt.**

In de MvT, paragraaf 5.5.1 bij kopje ‘significante incidenten’ staat het volgende omschreven: *“De meldplicht ziet alleen op significante incidenten. De meldplicht ziet niet op bijna-incidenten of dreigingen. Een incident is significant als het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken of als het andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken (zie artikel 23, derde lid, NIS2-richtlijn). Het gaat derhalve ook om incidenten waarbij de hiervoor genoemde mogelijke aanzienlijke gevolgen zich nog niet hebben voorgedaan, maar mogelijk wel gaan plaatsvinden. Ook ten aanzien van zulke incidenten is het van belang dat deze worden gemeld bij het CSIRT en de toezichthoudende instantie.”*

De tweede zin van deze alinea suggereert dat er niet altijd sprake is van een meldplicht terwijl dat in het vervolg van de alinea vervolgens weerlegd lijkt te worden. Als hier bedoeld wordt dat er geen meldplicht geldt als een bijna-incident of dreiging niet significant is (en dus niet valt onder de nog te bepalen drempelwaarden) dan verdient het de aanbeveling dit ook expliciet zo te stellen.

- ***NLconnect verzoekt om in de MvT expliciet op te nemen dat geen meldplicht geldt als een bijna-incident of dreiging niet significant is (en dus niet valt onder de nog te bepalen drempelwaarden).***

Geen uitbreiding openbaarmaking meldingsinformatie buiten algemeen belang

Artikel 90 van de Cbw wijzigt de bijlage bij artikel 8.8 van de Wet open overheid (verder: Woo). In deze bijlage staan de uitzonderingen voor openbaarmaking opgesomd, waaronder ook de Telecommunicatiewet (verder: Tw), artikel 11a.2 lid 3.[3] Uit deze huidige bepaling volgt dat beveiligingsincidenten en informatie die wordt verstrekt om de beveiliging van de netwerken of diensten van telecompartijen te beoordelen niet op elk moment door eenieder op te vragen is, maar slechts indien dat in het algemeen belang is. De grondslag hiervoor is het tweede lid van artikel 40 EECC. Met de Cbw verdwijnt dit artikel uit de Tw en wordt het materieel getransponeerd naar artikel 39 Cbw. Door de invoering van artikel 90 Cbw zou genoemde uitzondering op de openbaarmaking op grond van de Woo komen te vervallen. Deze uitzondering wordt slechts vervangen door een uitzondering voor de communicatie tussen het CSIRT en de overheid (artikel 65). NLconnect maakt daar bezwaar tegen: het openbaar maken van alle meldingen op elk moment, zoals nu omschreven in artikel 90 Cbw, komt niet ten goede aan de nationale veiligheid in het algemeen. Het verdient aanbeveling om artikel 90 zodanig te wijzigen dat in de bijlage bij artikel 8.8 van de Woo ook artikel 39 van de Cbw wordt genoemd.

- ***NLconnect pleit voor een aanpassing van artikel 90 waarbij de lijn van het huidige artikel 11a.2 Tw wordt gevolgd: slechts verstrekking van informatie over meldingen die zijn gedaan indien dit in het algemeen belang is.***

Governance: realiteitszin in de eisen aan bestuurders

NLconnect maakt zich zorgen over de interpretatie die in de Cbw wordt gegeven aan de invulling van artikel 20 NIS2. In het tweede lid van artikel 26 Cbw staat dat *ieder* lid van het bestuur geacht wordt om over de benodigde kennis en vaardigheden te beschikken om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren en beoordelen, alsmede de gevolgen daarvan voor de diensten. In onze ogen is dit een verkeerde lezing van artikel 20 lid 2 van de NIS2-richtlijn, dat een opleiding voor leden van bestuursorganen eist, zodat ze met voldoende kennis en vaardigheden en kennelijk met de bedoeling om *met de eveneens opgeleide werknemers* risico's te kunnen identificeren en de uitvoering van de maatregelen te kunnen beoordelen.

De NIS2 ziet dus op het via een opleiding kennis verwerven door de specialistische werknemers in de entiteit en niet zozeer door *alle* bestuursleden zelf. Dat ligt ook voor de hand: het identificeren van risico's en in eerste instantie beoordelen van risicobeheersmaatregelen en de gevolgen daarvan, zijn taken die binnen een entiteit door speciaal daarvoor (hoog) opgeleide en ervaren medewerkers worden uitgevoerd. Bestuurders van bedrijven zijn ook verantwoordelijk voor onder andere de financiën, de human resources, de operaties en de strategievorming en uitvoering van het bedrijf en er is ook geen wetgeving die alle bestuurders dwingt diepgaand verstand te hebben van de inhoud van al die onderwerpen. Een goede cyberbeveiliging stelt met andere woorden verschillende eisen aan de opleidingsniveaus van bestuurders onderling en van werknemers.

[3] Artikel 11a.2 lid 1-3 van de Telecommunicatie luiden als volgt: *"1. Aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten stellen Onze Minister onverwijld in kennis van beveiligingsincidenten met aanzienlijke gevolgen voor het functioneren van hun netwerken of diensten. 2. Aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten verstrekken onze Minister op zijn verzoek alle informatie die nodig is om de beveiliging van hun netwerken of diensten te beoordelen. 3. Op grond van het eerste en tweede lid verstrekte gegevens zijn niet openbaar. Indien openbaarmaking in het algemeen belang is, kan Onze Minister een inbreuk op de veiligheid en een verlies van integriteit, bedoeld in het eerste lid, openbaar maken of de aanbieder verplichten tot openbaarmaking."*

Dit past ook in de bevindingen van het ‘Samenhangend Inspectiebeeld cybersecurity vitale processen 2024’, waarin de RDI op basis van meerjarige ervaring met handhaving van de Wbni stelt dat cybersecurity meer prioriteit op de agenda van het bestuur verdient. Dit wordt in 2.2.2 van genoemd rapport uitgewerkt: het is aan het bestuur om kaders te stellen en te zorgen voor de besturing van het risicomanagement. Artikel 26 lid 2 van het wetsvoorstel dient daarmee in lijn te worden aangepast.

Daartoe hoeft (en mag) niet afgedaan worden aan de bepalingen uit de NIS2. Een nadere beschrijving van scope en doel van de opleiding die dient te worden gevolgd is wenselijk, bij voorkeur gelieerd aan de mate van verantwoordelijkheid die een individu als bedrijfsbestuurder draagt.

- ***NLconnect vraagt om enige realiteitszin aan te brengen in de eisen die aan bestuurders van ondernemingen worden gesteld, door lid 2, sub a van artikel 26 uit het wetsvoorstel Cbw te verwijderen.***

<u>Toezicht en handhaving: rechtvaardig, proportioneel en subsidiair</u>
Enkele bepalingen in hoofdstuk 16 geven NLconnect nog niet het vertrouwen dat het toezicht en de handhaving altijd in verhouding zullen staan tot de overtreding en in een goede subsidiaire inzet van het instrumentarium. Zo bevatten de artikelen 68, 69, 70, 79 en 80 zeer vergaande maatregelen waarvan het niet duidelijk is wanneer of waarom deze maatregelen ingezet kunnen worden. Dat roept vragen op over proportionaliteit. En bij de artikelen 73, 74 en 77 is de subsidiariteit van de inzet van het instrumentarium onvoldoende geborgd.

Artikel 68 stelt ten aanzien van de controlefunctionaris dat de bevoegde autoriteit (toezichthouder) bij essentiële entiteiten voor een bepaalde periode een controlefunctionaris kan aanwijzen. Het is niet duidelijk wat de criteria hiervoor zijn. Wanneer wordt dit instrument ingezet? Het lijkt NLconnect niet rechtvaardig om dit instrument in te zetten bij een entiteit die reeds audits heeft laten uitvoeren en certificering in bezit heeft. In lid 4 van dit artikel wordt aangegeven dat in een AMvB nadere regels zullen worden gesteld over onder meer de professionele kwalificaties van de controlefunctionaris maar niet over de omstandigheden waarin een dergelijke functionaris wordt aangesteld. We bevelen aan de criteria hiervoor in overleg met de sector vast te stellen.

- ***NLconnect stelt voor om de bepalingen over de inzet van de controlefunctionaris in de wet nader uit te werken.***

Ook ten aanzien van de beveiligingsscan van artikel 69 zal er een aanleiding moeten zijn deze in te zetten. Daar blijkt nu noch in de MvT noch in het artikel zelf iets van. NLconnect beveelt aan hier in de MvT aandacht aan te besteden zodat de voorspelbaarheid van de inzet van dit middel wordt verduidelijkt en vergroot. Het ligt ook hier voor de hand dat een scan niet wordt opgelegd aan een entiteit die bestaande audits of geldige certificeringen aan kan voeren.

In lid 2 van artikel 69 is opgenomen dat de bevoegde autoriteit de kosten van de beveiligingsscan draagt, tenzij een bij AMvB omschreven geval zich voordoet waarin deze kosten moeten worden gedragen door de betrokken entiteit. NLconnect maakt op voorhand bezwaar tegen een dergelijke AMvB: wij zien geen reden waarom de kosten van de scan niet altijd door de bevoegde autoriteit worden gedragen. Hetzelfde geldt voor artikel 79.

- ***NLconnect stelt voor om in de MvT aandacht te besteden aan de voorspelbaarheid van de inzet van de beveiligingsscan en geen AMvB op te stellen die de kosten bij de entiteit legt.***

Ten aanzien van de artikelen 70 en 70a, de beveiligingsaudit, is bepaald dat de kosten daarvoor bij de essentiële entiteit komen te liggen; dit terwijl deze maatregel volgens de tekst van de Cbw op ieder moment aan iedere essentiële entiteit kan worden opgelegd. Dit is niet proportioneel. Een audit is een vergaande maatregel die veel kosten met zich meebrengt en vaak arbeidsintensief is. NLconnect is van mening dat een audit nooit eerder kan worden opgelegd dan nadat een scan heeft plaatsgevonden. De scan, op kosten van de toezichthouder, leidt dan tot een conclusie waarin besloten wordt al dan niet de audit uit te laten voeren. Hetzelfde geldt voor artikel 80.

- ***NLconnect stelt voor om in de wet op te nemen dat een beveiligingsaudit nooit eerder kan worden opgelegd dan nadat een scan heeft plaatsgevonden.[4]***

In artikel 73 wordt het middel 'last onder bestuursdwang' beschreven. In de MvT staat in paragraaf 5.7.10 dat de toezichthoudende instantie bevoegd is om in plaats van een last onder bestuursdwang een last onder dwangsom op te leggen (op grond van artikel 5:32, eerste lid, Awb). NLconnect vraagt zich af waarom niet in de eerste plaats het minder ingrijpende middel 'last onder dwangsom' in de wet is opgenomen, met als tweede mogelijkheid de 'last onder bestuursdwang' en dit alternatief (dwangsom) nu alleen in de MvT wordt aangekaart. De argumentatie dat een last onder dwangsom soms niet voldoende is om de overtreding door de overtreder ongedaan te laten maken gaat voorbij aan het feit dat dit middel vaak wel volstaat en effectief genoeg is om het gewenste resultaat te bereiken.

- ***NLconnect stelt voor de last onder dwangsom ook op te nemen in artikel 73.***

Artikel 74 stelt dat, en hoe de bevoegde autoriteit kan overgaan tot het bepalen van een einddatum waarop een essentiële entiteit de overtreding moet hebben beëindigd. Hoewel in de MvT, paragraaf 5.7.11.2, valt te lezen dat de toezichthoudende instantie in de meeste gevallen eerst zal overgaan tot het opleggen van andere maatregelen, staat artikel 74 lid 2 na het afgeven van de lichtste maatregel - het afgeven van een waarschuwing - een vrijwel directe escalatie toe van een bindende aanwijzing en een last onder dwangsom. NLconnect is van mening dat een getrapte aanpak meer voor de hand ligt, bijvoorbeeld door na de waarschuwing eerst te escaleren naar bijvoorbeeld artikel 72.

- ***NLconnect stelt voor om artikel 74 lid 2 aan te passen naar "nadat zij <u>twee</u> of meer van de in het derde lid genoemde maatregelen".***

Overigens vraagt NLconnect zich af of de verwijzing in de inleiding van paragraaf 5.7.11.2 van de MvT naar diezelfde paragraaf 5.7.11.2 klopt en of het niet de bedoeling is naar een andere paragraaf te verwijzen?

Net als hierboven gesteld bij art 74 over de combinatie van een waarschuwing en een einddatum lijkt de in artikel 77 lid 1a beschreven bevoegdheid om in combinatie met een waarschuwing ook een bestuurlijke boete op te leggen disproportioneel. Na het geven van een waarschuwing, het lichtste handhavingsmiddel, beschikt de toezichthouder daarna

[4] Indien deze suggestie onverhoopt niet wordt overgenomen is het noodzakelijk dat in de Cbw duidelijk wordt gemaakt dat bezwaar en beroep open moet staan tegen een opgelegde beveiligingsaudit.

immers nog over andere zwaardere handhavingsmiddelen die tot het beoogde resultaat zouden kunnen leiden, zonder dat dan ook al een boete is opgelegd, om datzelfde resultaat te bereiken. Aan het eind van paragraaf 4.7.12 staat in dit kader dat dit, gelet op de voor de toezichthoudende instantie geldende juridische kaders slechts denkbaar is in uitzonderlijke gevallen. NLconnect is benieuwd waar in dit kader aan gedacht moet worden.

Artikelsgewijs

- Artikel 23. De in lid 3 van dit artikel opgenomen passage dat maatregelen gebaseerd moeten zijn op een benadering die *alle* gevaren omvat is te breed om uitvoerbaar of handhaafbaar te kunnen zijn. Alle gevaren zijn niet te managen, het minimaliseren van relevante risico's is beter in te richten. De Engelse NIS2 tekst spreekt immers van "all hazards", hetgeen ook vertaald kan worden in "alle risico's".

- Artikel 26. NLconnect leest dit artikel zo dat onder bestuur het bestuur wordt verstaan in de zin van Boek 2 van het Burgerlijk Wetboek; het bestuur bestaat uit de personen die zijn belast met het besturen van de vennootschap, oftewel de algemeen directeur en de overige wettelijke vertegenwoordigers. De Raad van Commissarissen heeft tot taak toezicht te houden op het beleid van het bestuur en op de algemene gang van zaken in de vennootschap en de met haar verbonden onderneming (ook Boek 2 BW). De leden van de Raad van Commissarissen vallen daarmee niet onder het bestuur van de vennootschap. Om misverstanden te voorkomen verzoekt NLconnect om dit te verduidelijken in de wet of de toelichting daarop.

Vanzelfsprekend altijd bereid tot nadere toelichting,

met vriendelijke groet,

Mathieu Andriessen
Directeur NLconnect