Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Briefnummer
24-122488

Onderwerp
Reactie internetconsultatie Cbw

Den Haag
26 juni 2024

Telefoonnummer
+31620319264

E-Mail
gielens@vnoncw-mkb.nl

Geachte heer, mevrouw,

Met veel belangstelling hebben VNO-NCW en MKB-Nederland kennisgenomen van de concept Cyberbeveiligingswet (Cbw) ter implementatie van de Europese NIS2-richtlijn. Wij maken graag gebruik van de mogelijkheid hierop te reageren.

VNO-NCW en MKB-Nederland staan in beginsel positief tegenover de doelen uit de NIS2-richtlijn en het daarmee voorliggende concept Cbw. Verhoging van de digitale veiligheid en weerbaarheid is van groot belang voor de continuïteit van bedrijven en organisaties, en daarmee voor het functioneren van de economie en maatschappij. Dit geldt vooral in een tijd waarin de digitale dreiging onverminderd groot is. In dat kader hebben wij recent onze koers uitgebreid met een nieuwe pijler, te weten, weerbaarheid.

Wij ondersteunen dan ook dat in de voorliggende Cbw (t.o.v. de huidige Wet beveiliging netwerk- en informatiesystemen) méér bedrijven en organisaties verplicht worden hun cyberveiligheid aan te scherpen en hun weerbaarheid te vergroten, en dat er concrete doelvoorschriften komen, o.a. gericht op de toeleveringsketen. Dat is niet alleen van belang voor de continuïteit van bedrijven zelf, maar ook ter versterking van de (waarde)ketens. Hiermee zal de door de Cyber Security Raad geconstateerde weerbaarheidskloof afnemen c.q. de cyberweerbaarheid van het MKB doen toenemen. Hierbij is het wel van belang dat de eisen die door bedrijven en organisaties aan toeleveranciers (veelal MKB) worden gesteld proportioneel en risicogericht zijn, en de administratieve lasten beperkt worden.

Voorts hebben wij nog een aantal andere zorgpunten rondom voorliggende Cbw en de verdere uitwerking en implementatie. De belangrijkste zijn:

1. Door het ontbreken van eenduidige uitleg van begrippen en criteria in de Cbw, is het voor een aantal bedrijven nog onduidelijk in hoeverre zij onder de reikwijdte van de NIS2 vallen en zo ja, of zij als essentieel en/of belangrijk moeten worden beschouwd. Wij pleiten ervoor dat hier op korte termijn duidelijkheid over komt zodat bedrijven weten waar ze aan toe zijn en zich waar nodig kunnen voorbereiden.
2. Doordat de uitwerking van de zorgplicht wordt doorgeschoven naar de nog op te stellen AMvB, wordt de tijdspanne voor bedrijven om de eisen uit de Cbw te implementeren zeer

krap. Wij pleiten ervoor dat toezichthouders hiermee rekening houden en niet per medio 2025 direct overgaan tot het opleggen van sancties maar inzetten op lerend vermogen.
3. Met de scope-uitbreiding van de NIS2-richtlijn ontstaat het risico van verlies aan focus op beveiliging en bescherming van díe netwerk- en informatiesystemen die randvoorwaardelijk zijn voor de continuïteit van de essentiële of belangrijke dienst(verlening) of proces. Wij pleiten ervoor dat de risico gebaseerde aanpak zoals nu opgenomen in de Cbw, expliciet als leidend principe in de AMvB én bij het vormgeven van het toezicht wordt doorgevoerd.
4. De overheid maakt een strikt onderscheid tussen de Cbw (cyber) en de Wet weerbaarheid kritieke entiteiten (fysiek). Bedrijven werken echter veelal op een all hazards benadering. Wij pleiten dan ook voor een goede samenloop tussen beide wetten om dubbele (toezichts)lasten aan de zijde van bedrijven te voorkomen.
5. Het nationale register (en onderliggende online registratievoorziening) met daarin de namen van entiteiten en ook hun IP-bereiken, vormt een groot cyberrisico. Wij pleiten voor goede waarborgen rondom de veiligheid van het register / registratievoorziening. Daarnaast pleiten wij ervoor dat aanlevering van IP-bereiken optioneel is en geen wettelijke verplichting.
6. De opgenomen verwachting om in de AMvB een hoger cyberbeveiligingsniveau te borgen dan de NIS2-richtlijn vereist, zou een nationale kop impliceren. Omwille van een gelijk speelveld pleiten wij ervoor om conform het Hoofdlijnenakkoord 2024-2028 geen nationale koppen op Europese regelgeving te zetten.
7. Wanneer het Computer Security Incident Respons Team (CSIRT) vrijwillige meldingen gaat doorzetten naar de toezichthouder onder de Wet weerbaarheid kritieke entiteiten, zal de bereidheid bij bedrijven om vrijwillig te melden aanzienlijk afnemen. Wij pleiten ervoor dit terug te draaien en het aan bedrijven zelf over te laten of zij haar toezichthouder willen informeren. Het systeem van vrijwillig melden moet gericht blijven op leren en verbeteren in een vertrouwelijke setting.

In de bijlage bij deze brief is een artikelsgewijze reactie (incl. aandachtspunten voor de komende AMvB) en een aantal procesvragen.

Tot slot willen wij de oproep aan het Rijk doen om op een aantal in de Cbw opgenomen activiteiten, expliciet de samenwerking te zoeken met (branches van de) betrokken entiteiten en met VNO-NCW en MKB-Nederland. Hierbij gaat het o.a. om:
- Uitwerking van de risico gebaseerde benadering van het CSIRT met de onderliggende vraag hoe prioriteit wordt gegeven aan het verlenen van hulp en bijstand aan entiteiten;
- Het opstellen van de drempelwaarden voor de meldplicht;
- Het opstellen c.q. actualiseren van de nationale cyberbeveiligingsstrategie en van het nationaal plan voor grootschalige cyberbeveiligingsincidenten.

Bij deze zaken is publiek-private samenwerking onontbeerlijk.

Uiteraard zijn wij bereid een nadere toelichting te geven op onze reactie. Hiervoor kunt u contact opnemen met Sabine Gielens (zie boven voor de contactgegevens).

Wij wensen u veel succes met de verwerking van de reactie op de internetconsultatie, en zien in het najaar graag de consultatie van de AMvB tegemoet.

Met vriendelijke groet,

Mw. I.C. Linthorst
Directeur Beleid

Bijlage met artikelsgewijze reactie op de concept Cyberbeveiligingswet (Cbw)

1. Begripsbepaling (H1)

- Verzoek is om in artikel 1 een omschrijving op te nemen van leden van het bestuur.
- Voor de leesbaarheid van de wet, raden wij aan om in artikel 1 de definitie van Netwerk- en informatiesystemen uit de NIS2-richtlijn op te nemen. Conform de tekst in de MvT, aangeven dat hier óók Operationele Technologie (OT) onder valt.

2. Essentiële entiteiten en belangrijke entiteiten (H4)

- Een belangrijk verschil met de eerste NIS-richtlijn is dat organisaties automatisch onder de NIS2-richtlijn vallen als zij actief zijn in bepaalde sectoren en volgens de bepaalde criteria gekenmerkt kunnen worden als ‘essentiële’ of ‘belangrijke’ entiteit. Om na te gaan of je als bedrijf/organisatie onder de Cbw valt en vervolgens als essentieel of belangrijk wordt beschouwd, is er met name voor bedrijven met complexe bedrijfsstructuren meer duidelijkheid (criteria) nodig. Wanneer gelden bv. verwante ondernemingen als één entiteit en wanneer gelden zij afzonderlijk als entiteit? Dit is ook van belang voor de reikwijdte van de zorg- meld- en registratieplicht.
  Ook is er nadere duiding nodig voor samengestelde entiteiten over hoe zij de criteria moeten toepassen. Geldt dit altijd voor de gehele entiteit, of kan ook volstaan worden met risico-inschattingen per deelentiteit waarbij verschillende afwegingen kunnen worden gemaakt per onderdeel.
  Wij pleiten ervoor dat de online vragenlijst van de RDI op korte termijn wordt doorontwikkeld om bedrijven/organisaties z.s.m. duidelijkheid te geven, als ook voor een nadere toelichting in de MvT bij de Cbw.

- Op basis van voorliggende Cbw zijn bij bedrijven vragen ontstaan of zij als essentieel en/of belangrijk moeten worden beschouwd. Diverse industriële sectoren, die opgenomen zijn in bijlage 1 en 2 van de Cbw, zoals farmacie, chemie en levensmiddelen, hebben vaak ook processen zoals afvalwaterzuiveringsinstallaties (AWZI’s) en/of afvalbeheer die het primaire proces ondersteunen. Zowel afvalwaterzuivering als afvalbeheer vallen onder de Cbw, behalve wanneer het een ‘niet- essentieel onderdeel’ is van de algemene activiteit, dan wel niet de ‘voornaamste activiteit’ is. Vraag is: Wat is de afbakening van met name ‘een niet-essentieel onderdeel’ (bij Afvalwater), als ook ‘niet-voornaamste activiteit’ (bij Afvalstoffenbeheer)? Graag een éénduidige uitleg / definitie hiervan.
  Hierbij pleiten wij ervoor om processen die (enkel) ondersteunend zijn aan het primaire proces, volledig uit te sluiten van de reikwijdte van Afvalbeheer en Afvalstoffenbeheer. Dit is in lijn met de risicogerichte benadering. Indien dat niet gebeurt, zijn de gevolgen in termen van administratieve lasten voor entiteiten groot. Ter illustratie: indien een entiteit uit bijlage 2, bv. uit een levensmiddelenbedrijf (bijlage 1, onder LNV) met een eigen AWZI (bijlage 2, onder IenW) op basis van de uitleg/definitie van ‘niet-essentieel onderdeel’ óók onder Afvalwater uit bijlage 1 valt, dan krijgt deze entiteit met twee regimes te maken, namelijk essentieel én belangrijk, met als gevolg: twee verschillende vakdepartementen en toezichthouders, verschillende type toezichtsregimes, en verschillende eisen (bv. sectorale drempelwaarden voor levensmiddelen én afvalwater). Het moge duidelijk zijn dat dit zeer onwenselijk is en moet worden voorkomen.

- In het verlengde van bovenstaand punt het volgende. Zoals hierboven aangegeven, is in bijlage 1 en 2 bij een groot aantal entiteiten (zoals bij Afvalbeheer en Afvalstoffenbeheer) een afbakening aangegeven. Wanneer het een ‘niet-essentieel onderdeel’ / ‘niet-voornaamste activiteit’ is, dan is het uitgezonderd van de Cbw. Bij een aantal andere entiteiten is er echter geen afbakening opgenomen, zoals bij “Digitale Infrastructuur” en “Beheer van ICT diensten (business-to-business)”. Hiermee wordt een situatie gecreëerd waarin bedrijven /organisaties onder twee of meer van de sectoren in bijlage en 1 en 2

vallen waarvan er i.i.g. één niet de kerntaak of -activiteit betreft. Dit is niet in lijn met de beoogde risicogerichte benadering. Wij pleiten er dan ook voor om ook bij “Digitale Infrastructuur” en “Beheer van ICT diensten (business-to-business)” de toevoeging te doen dat dit niet van toepassing is wanneer het niet tot de voornaamste activiteit behoort.

3. Aanwijzing en taken van instanties (H5)

- Artikel 17 lid 2 stelt dat het CSIRT o.a. als taak heeft om, indien van toepassing, te reageren op incidenten en het verlenen van bijstand aan de betrokken essentiële entiteit of belangrijke entiteit. Vraag is wat entiteiten mogen verstaan onder bijstand? Wat mogen/ kunnen zij verwachten van de overheid?

- Artikel 17 lid 3 stelt dat het CSIRT een openbaar toegankelijk netwerk- en informatiesysteem van een essentiële entiteit en belangrijke entiteit proactief en niet-intrusief kan scannen met het oog op het opsporen van een kwetsbaar of onveilig geconfigureerd netwerk- en informatiesysteem. Vragen hierbij zijn: wordt de betrokken entiteit op voorhand geïnformeerd over het scannen, hoe wordt de veiligheid van de dienstverlening van de betrokken entiteit geborgd, en wie is aansprakelijk indien er onverhoopt schade optreedt door het scannen? Wij zien op deze punten graag verduidelijking in de MvT.

- Artikel 38 schrijft voor dat het CSIRT onverwijld en zo mogelijk binnen 24 uur na ontvangst van een vroegtijdige waarschuwing over een significant incident op verzoek van een entiteit operationeel advies geeft. Het idee achter melden en het zo vroegtijdig ervan, is het voorkomen van erger (zowel binnen de entiteit als met oog op cascade-effecten). Hulp en bijstand kunnen in die fase zijn dus van groot belang zijn. In het verlengde daarvan, vragen wij ons af of de ambitie om zo mogelijk binnen 24 uur te voorzien in advies, de juiste is. Moet niet gesteld dat er binnen 24 uur op verzoek van de entiteit hulp en bijstand wordt geboden door het CSIRT?

- In de rolbeschrijving van het CSIRT dat lidstaten moeten aanwijzen, wordt o.a. de AIVD als betrokken partij genoemd. In de beschrijving is te lezen dat informatie waarover het CSIRT vanwege haar taakuitoefening beschikt, gedeeld kan/mag worden met de AIVD. Er staat echter niet dat de AIVD informatie mag/kan delen met het CSIRT terwijl dát juist van groot belang is, met name als het gaat om statelijke actoren. We pleiten ervoor dat expliciet wordt gemaakt dat de informatie-uitwisseling tussen de twee partijen tweezijdig is.

- Tot slot willen we op het punt van het CSIRT aandacht vragen voor de benodigde capaciteit voor het NCSC als nationaal CSIRT. Met de vergrote doelgroep die het NCSC moet gaan bedienen (van ong. 350 naar meer dan 10.000 organisaties) is het noodzaak dat er tijdig wordt geïnvesteerd in de benodigde capaciteit, kennis en automatisering.
  Daarnaast moet bij de dienstverlening goed rekening gehouden worden met de verschillende volwassenheidsniveaus van organisaties, en daarmee gepaard gaande behoeftes. De meer volwassen organisaties hebben vooral behoefte aan een snelle aanlevering van ruwe data. De minder volwassen organisaties en het MKB hebben juist behoefte aan concrete handelingsperspectieven (wat, hoe en wanneer).

4. Zorgplicht (H7)

- Algemeen zorgpunt rondom de zorgplicht is dat de uitwerking ervan wordt doorgeschoven naar lagere regelgeving die nu nog niet voor handen is. Verwachting is dat de AMvB eind dit jaar ter consultatie wordt gebracht en de wetgeving medio 2025 van kracht gaat. Hiermee hebben bedrijven slechts een half jaar de tijd om op basis van de nadere regels hun zorgplicht in te vullen en te implementeren. Wij roepen het Rijk, en met name de toezichthouders, op om met deze korte tijdspanne rekening te houden en niet per medio

2025 direct over te gaan tot het opleggen van sancties wanneer entiteiten nog niet aan alle vereisten voldoen, maar in eerst instantie in te zetten op lerend vermogen.

- Waar de eerste NIS-richtlijn zich nog richtte op beveiliging van die netwerk- en informatiesystemen die van belang zijn voor de essentiële dienst, gaat NIS2 over álle netwerk- en informatiesystemen van entiteiten. Dit betekent een forse scope-uitbreiding van de zorgplicht van bedrijven. Hierachter gaat het risico schuil dat er bij bedrijven verlies optreedt in focus (qua mensen en middelen) op beveiliging en bescherming van díe netwerk- en informatiesystemen die randvoorwaardelijk zijn voor de continuïteit van de essentiële of belangrijke dienst(verlening) of proces. Gezien het groeiende tekort aan cybersecurityexperts is het aanbrengen van focus – voor zowel bedrijven als de overheid – van groot belang.
  Daar tegenover staat dat de NIS2 een risicogerichte benadering hanteert. Wij zijn blij dat die risicogerichte benadering expliciet is opgenomen in voorliggend concept wetsvoorstel. Wij lezen dat risicomanagement of een risicobeoordelingscyclus ten grondslag ligt aan de zorgplicht van entiteiten.
  Wij verzoeken het Rijk met klem ervoor zorg te dragen dat deze risicogerichte benadering bij het verder vormgeven en invullen van de zorg- en meldplicht in de AMvB, als ook bij het vormgeven en invullen van het toezicht op bedrijven, expliciet leidend is en blijft.

- Ook onderschrijven wij het uitgangspunt dat het aan entiteiten zelf is om - op basis van een risicobeoordeling - vast te stellen welke maatregelen passend en evenredig zijn om invulling/uitwerking te geven aan de voorgeschreven doelvoorschriften, waarbij ze hun eigen normenkader(s) kunnen (blijven) hanteren. Entiteiten hebben immers de meeste kennis van hun systemen incl. de kwetsbaarheden.
  Uiteraard dient hierbij gekeken te worden naar Europese- en internationale normen die relevant zijn voor de beveiliging van netwerk- en informatiesystemen.

- Het is vervolgens aan de betrokken toezichthouder om te beoordelen of de genomen maatregelen voldoende zijn om de risico's te mitigeren dan wel zoveel als mogelijk beheersen en/of wat evt. aanvullend benodigd is. Zoals ook in de MvT staat aangegeven, is het volledig uitsluiten van risico's en 100% veiligheid niet mogelijk of reëel. Wij zijn positief gestemd dat dit wordt erkend. Restrisico's zullen er altijd zijn, en over de afwegingen die daaraan ten grondslag liggen zal het gesprek tussen entiteiten en toezichthouders moeten gaan.

- Een verschil met de eerste NIS-richtlijn zijn de nieuwe eisen rondom de toeleveringsketen. Entiteiten moeten rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener, en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners.
  Gezien de afhankelijkheden van de keten, is aandacht voor ketenveiligheid meer dan terecht en ook noodzakelijk. Voor een goede uitvoerbaarheid van de eisen en beheersbaarheid ervan, staan wij volledig achter de afbakening, te weten, rechtstreekse of directe leveranciers. In aanvulling hierop, pleiten wij ervoor dat de focus ligt op leveranciers en dienstverleners van netwerk- en informatiesystemen die kritisch / randvoorwaardelijk zijn voor het borgen van de continuïteit van de essentiële of belangrijke dienst(verlening) of proces.

- Hetgeen in de MvT bij de paragraaf over leveranciersmanagement ontbreekt, is de notie dat er Europese wet- en regelgeving op het gebied van digitale producten aan komt, te weten, de Delegated Act van de Radioapparatenrichtlijn (RED) in 2025 en de Europese Cyber Resilience Act (CRA) in 2027. De RED en CRA stellen cybersecurityeisen aan producten met digitale elementen (hardware, software en losse componenten). Deze hogere veiligheid

van geleverde producten zal het leveranciersmanagement van NIS2-entiteiten verlichten en daarmee de bewijslast en toezichtsdruk. Het is van belang om dit gegeven op te nemen in de MvT.

- Voor de uit te voeren risicoanalyse door entiteiten is inzicht in actuele dreigingen en gevaren noodzakelijk / randvoorwaardelijk. Voor de eerste categorie (dreigingen) is informatie benodigd vanuit de inlichtingendiensten. Wij roepen het Rijk op om de betrokken entiteiten (meer) te voorzien van sectorspecifieke (dreigings)informatie over o.a. actoren, de kans van optreden, modus operandi etc. De huidige Wet op de inlichtingen- en veiligheidsdiensten maakt dit mogelijk.

- We zijn verbaasd over de tekst bij 5.3.5. van de MvT waarin staat aangegeven dat Nederland naar verwachting gebruik gaat maken van de mogelijkheid om in AMvB bepalingen vast te stellen die een hoger cyberbeveiligingsniveau waarborgen.
  Uit gesprekken met uw ministerie is begrepen dat deze alinea is opgenomen om, wanneer de nationale veiligheid daarom vraagt, de overheid aanvullende cybersecurity-eisen kan stellen. Met name gezien de huidige geopolitieke situatie, is hier in beginsel begrip voor. Echter, eerst moet worden bezien of deze bevoegdheid niet reeds op bestaande wetgeving kan worden toegepast. Zo niet, dan moet dan moet de bevoegdheid heel scherp afgebakend worden in het wetsvoorstel zelf, met een duidelijke toelichting in de MvT.
  Op basis van de huidige tekst kan de alinea geïnterpreteerd worden als een nationale kop. Dit zou haaks staan op de door uw ministerie gecommuniceerde uitgangspunten (namelijk zo dicht mogelijk bij de tekst van de NIS2-richtlijn blijven), als ook op het Hoofdlijnenakkoord 2024 – 2028. Het opleggen van aanvullende eisen vanuit Nederland creëert een ongelijk speelveld, en is voor entiteiten die in meerdere lidstaten opereren onwerkbaar.

- Er wordt in de Cbw een strikt onderscheid gemaakt tussen de Cbw en de Wet weerbaarheid kritieke entiteiten (Wwke). De Cbw beperkt zich tot netwerk- en informatiesystemen incl. hun fysieke omgeving, en de Wwke tot alle overige fysieke aspecten. In de wettelijke zorgplicht van bedrijven wordt dit onderscheid doorgevoerd. Waar de zorgplicht uit de Cbw zich beperkt tot netwerk- en informatiesystemen en hun fysieke componenten, beslaat de zorgplicht uit de Wwke weerbaarheid in brede zin. Bedrijven maken in hun bedrijfsvoering, risicobeoordeling etc. die splitsing veelal niet. Zij werken op basis van een all hazards benadering. Wij pleiten er dan ook voor om in lagere regelgeving ervoor te zorgen dat bedrijven die onder beide wetten vallen, de mogelijkheid moeten krijgen om via één integrale risicoanalyse en één pakket aan (aanvullende) maatregelen de naleving van hun zorgplicht uit de Cbw en Wwke aan de toezichthouder te kunnen aantonen.

- Er moet vanuit alle betrokken toezichthouders een gemeenschappelijk beeld/interpretatie van de zorgplicht komen: wanneer is goed goed genoeg? Dit is m.n. van belang voor entiteiten die actief zijn in meerdere sectoren en daarmee te maken hebben met meerdere toezichthouders.

- De bewijslast waarmee entiteiten aantonen dat zij voldoen aan hun zorgplicht dient zoveel als mogelijk bij de entiteiten zelf te (blijven) liggen. Een groot aantal entiteiten heeft (op basis van bestaande sectorale wet- en regelgeving) reeds te maken met wettelijke verplichtingen rondom cybersecurity en daarmee gepaard gaande planvorming / documentatie die bij de toezichthouder wordt ingediend. In het kader van de lastendruk, moet zoveel mogelijk aansluiting worden gezocht bij bestaande werkwijzen en planvorming.

5. Governance (H8)

- Het is niet helder wat wordt verstaan onder ‘leden van het bestuur’. Hoe verhoudt dit zich dit tot (leden van) een Raad van Commissarissen en/of Dagelijks Bestuur? Voorstel is om het begrip ‘leden van het bestuur’ te voorzien van een definitie en op te nemen in artikel 1 van de wet (begripsbepaling).

- Wij pleiten ervoor om bij artikel 26 lid 2 de tekst uit de NIS2-richtlijn aan te houden. Op die manier wordt duidelijker het onderscheid gemaakt tussen enerzijds hun taken/verantwoordelijkheden genoemd bij artikel 26 lid 1 - zijnde goedkeuring maatregelen voor de beheersing van cyberbeveiligingsrisico’s incl. toezicht op uitvoering ervan - en de doelstellingen achter de training. Tekstvoorstel bij artikel 26 lid 2: *De leden van de bestuursorganen van essentiële en belangrijke entiteiten volgen een opleiding zodat ze over voldoende kennis en vaardigheden beschikken om risico’s te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.*

- In artikel 26 lid 6 staat dat bij AMvB nadere regels kunnen worden gesteld over de training waaronder de duur en het niveau. Dit gaat o.i. verder dan de NIS2-richtlijn voorschrijft en gaat daarmee voorbij aan de beleidsarme omzetting.
  Afgezien daarvan, is het voor entiteiten die in meerdere lidstaten opereren onwerkbaar wanneer op lidstaat-niveau nadere eisen worden gesteld over de duur en het niveau. Deze entiteiten willen voor het gehele bedrijf een uniforme training opzetten en uitrollen zonder gehinderd te worden door aanvullende / verschillende eisen vanuit individuele lidstaten. Wij pleiten er dan ook voor om op dit punt geen nadere regels te stellen.

- Uit artikel 26 wordt niet helder of de training een externe training moet zijn of dat het bv. ook een interne training mag zijn. Voor entiteiten die in meerdere lidstaten opereren, is de uitrol van een interne training efficiënter. Wij zijn graag (in de MvT) verduidelijking op dit punt waarbij het aan entiteiten wordt gelaten of zij de training extern willen beleggen en/of intern willen doen.

6. Significante incidenten, incidenten, bijna-incidenten, significante cyberdreigingen, cyberdreigingen en kwetsbaarheden (H9)

Meldplicht (§ 9.1)

- Wij pleiten voor een proportionele en risico gebaseerde drempelwaarde voor de meldplicht die ziet op zgn. significante incidenten. Focus moet liggen op continuïteit van de essentiële of belangrijke dienstverlening / borging van de leveringszekerheid (ofwel op die dienstverlening op basis waarvan de entiteiten als essentieel of belangrijk zijn aangemerkt). Temeer gezien de administratieve lastendruk die de meldplicht met zich meebrengt voor entiteiten. De meldplicht beperkt zich immers niet alleen tot de officiële melding (met daaraan voorafgaande nog wellicht een vroegtijdige waarschuwing), maar vereist ook updates, tussentijdse verslagen, een voortgangsverslag en een eindverslag.

  NB Het feit dat er in het verleden te weinig gemeld zou zijn onder de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) mag geen reden zijn tot het verlagen van de drempelwaarden. Wettelijk melden moet gericht zijn en blijven op (mogelijke) continuïteitssituaties waarbij waar nodig, z.s.m. hulp en bijstand wordt geboden om de situatie dan wel de gevolgen ervan te beheersen.
  Voor een algemeen beeld/inzicht in trends, ofwel in het hetgeen waar entiteiten zoal mee geconfronteerd worden op het gebied van mogelijke aanvallen, kwetsbaarheden etc., kan gebruik worden gemaakt van informatie afkomstig vanuit vrijwillige meldingen, en informatie die gedeeld wordt in o.a. de sectorale ISAC’s waar het NCSC aan deelneemt. Kortom,

oproep is om het doel achter de wettelijke meldplicht voorop te stellen - hulp en bijstand om erger te voorkomen - en de drempelwaarden daarop af te stemmen. Inzicht in trends is een ander doel waar andere methoden voor zijn. Hiertoe dient het vrijwillig melden gepromoot te worden. In de zin van laagdrempeligheid en borging van de vertrouwelijkheid (dat de verstrekte informatie niet één op één wordt doorgezet naar de toezichthouder). Daarnaast dient te worden ingezet op een goede informatie-uitwisseling binnen de ISAC's.

- Het per AMvB uitwerken van de in de NIS2-richtlijn voorgeschreven generieke parameters en het opstellen van eventuele aanvullende parameters (die tezamen de drempelwaarde voor de meldplicht gaan vormen) dient in nauwe samenwerking tussen de entiteiten en vakdepartementen plaats te vinden. Het is immers aan de entiteiten om aan te geven wanneer de continuïteit van hun essentiële/belangrijke dienstverlening / leveringszekerheid in gevaar komt of kan komen.
  Hierbij moeten ook de (drempelwaarden van de) meldplicht op basis van reeds bestaande sectorale wetgeving in ogenschouw worden genomen, als ook – voor internationaal opererende bedrijven – de vigerende drempelwaarden in andere landen. Dit alles moet zo goed mogelijk op elkaar aansluiten.

- De uitgewerkte drempelwaarden moeten SMART geformuleerd worden zodat er in de praktijk géén discussie kan ontstaan tussen entiteiten, toezichthouders en het nationale CSIRT (ofwel het NCSC) of significante incidenten al dan niet gemeld hadden moeten worden.

- Voor organisaties die onder de Wbni vallen, zijn reeds drempelwaarden voor de wettelijke meldplicht opgesteld. Vraag is of er voor hen nieuwe / aangepaste drempelwaardes (moeten) komen. Wij pleiten ervoor om de bestaande drempelwaarden onder de Wbni in ieder geval als uitgangspunt te hanteren (in de nadere gesprekken tussen entiteiten en vakdepartementen).

- Wij krijgen graag inzicht in het gehele proces rondom het overeenkomen en vaststellen van de drempelwaardes (ook in tijd), en de betrokkenheid van entiteiten hierbij.

- Voor entiteiten die in meerdere sectoren actief zijn en daarmee met meerdere toezichthouders te maken hebben/krijgen, moet op voorhand duidelijkheid komen bij welke toezichthouder wat gemeld moet worden.

- Mede met het oog op bovenstaand punt, roepen wij het Rijk op om toe te werken naar één centraal meldloket van de overheid voor alle meldingen op basis van de Cyberbeveiligingswet, Wet weerbaarheid kritieke entiteiten én sectorale wetgeving. Hierbij is het van belang dat de meldingen goed gekanaliseerd worden (dus alleen naar de toezichthouder gaan indien dat ook als zodanig staat aangegeven of bv. alleen naar het NCSC in geval van vrijwillig melden). In het buitenland zijn diverse voorbeelden en good practices van deze één-loket werkwijze.

- In artikel 27 lid 2 sub a wordt gesproken over materiële- en immateriële schade. Vraag is: wat wordt verstaan onder immateriële schade in relatie tot een entiteit (rechtspersoon)? Het Nederlandse recht kent niet het gehanteerde onderscheid tussen materiële- en immateriële schade; wel schade als in vermogensschade en ander nadeel (zie artikel 6:95 BW). Voorstel is om daar in zijn algemeenheid naar te verwijzen zodat het schadebegrip in voorliggend wetsvoorstel aansluit op het Nederlandse rechtssysteem.

- In artikel 29 lid 1 sub d 'indien van toepassing' toevoegen.

- In artikel 30 staat aangegeven dat een CSIRT of de bevoegde autoriteit om een tussentijds verslag over relevante updates kan vragen. Uit de MvT wordt niet of nauwelijks duidelijk in welke geval dit van entiteiten gevraagd wordt. Graag verduidelijking op dit punt met daarbij in achtneming de algemene lastendruk en de capaciteit die bij entiteiten op het moment van een (dreigend) incident benodigd is voor de operatie in plaats voor het opstellen van tussentijdse verslagen.

Informeren van ontvangers van diensten (§ 9.2)

- Artikel 32 stelt dat een essentiële of belangrijke entiteit ontvangers van haar diensten in kennis stelt over significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten. Wat wordt verstaan onder 'ontvangers'? Graag een verdere verduidelijking hiervan in de MvT. En geldt voor dit artikel de nader op te stellen drempelwaarde onder artikel 27?

- Hoe verhouden de artikelen 32 (informeren van ontvangers van diensten) en 40 (in kennis stelling natuurlijke personen of rechtspersonen door entiteit) zich tot elkaar? Graag verduidelijking hiervan (in de MvT).

Vrijwillige meldingen (§ 9.4)

- In artikel 35 lid 3 toevoegen dat de melder op de hoogte wordt gesteld van de doorsturing (zie 5.5.3 MvT).

Informatieverstrekking i.v.m. meldingen (§ 9.7)

- Artikel 41 lid 2 beveiligingsbelangen vervangen door veiligheidsbelangen (conform art. 65 lid d).

- Artikel 42 lid 2 stelt dat het CSIRT informatie over vrijwillige meldingen van (bijna-)incidenten van een essentiële entiteit die tevens een kritieke entiteit is onder de Wwke, doorzet naar de bevoegde autoriteit onder de Wwke. Waarom is hiervoor gekozen; wat is de achtergrond hiervan? Vrijwillig melden moet omwille van het van elkaar leren en verbeteren te allen tijde gestimuleerd worden, en dus zo laagdrempelig mogelijk gemaakt worden. Indien informatie rondom vrijwillige meldingen van (bijna-)incidenten één op één wordt doorgezet naar de toezichthouder onder de Wwke zal de bereidheid om vrijwillig te melden afnemen en zijn doel verliezen. Wij verzoeken het Rijk met klem om vrijwillige meldingen aan het CSIRT niet door te zetten aan de toezichthouder maar dit aan de bereidheid van het betrokken bedrijf over te laten.

7. Nationaal register van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinregistratiediensten verlenen (H11)

- Artikel 45 schrijft voor dat essentiële en belangrijke entiteiten zich t.b.v. het in artikel 22 genoemde nationale register moeten registreren. Welke termijn geldt voor de informatieverstrekking? Dezelfde vraag geldt voor artikel 48 lid 2.

- Entiteiten moeten op basis van artikel45 onder meer hun contactgegevens, e-mailadressen, telefoonnummers en IP-bereiken aanleveren (via een nog op te zetten online registratievoorziening). Vanuit onze leden worden vragen gesteld over het doel en de noodzaak van aanlevering van (al) hun IP-bereiken:
  - Lang niet alle IP-bereiken zijn namelijk in de context van voorliggende concept wet relevant en/of noodzakelijk om als overheid te hebben. Dit is namelijk afhankelijk van de technische inrichting van de netwerken van entiteiten.
  - Daarnaast is er niet altijd een directe koppeling tussen een IP-adres en bedrijf of gebruiker waardoor je met alleen het beschikken over IP-bereiken als NCSC niet goed uit de voeten kunt.

- Tot slot zijn er bedrijven die zélf (wereldwijd) cybermonitoring op hun IP-bereiken uitvoeren.

Wij pleiten ervoor dat het aanleveren van IP-bereiken als optioneel wordt opgenomen en niet als een (wettelijke) verplichting wordt gesteld.

- Afgezien van bovenstaande, wordt de aanlevering- en onderhoud van IP-bereiken in een online registratievoorziening door onze leden als een groot en reëel cyberrisico gezien. Het moge duidelijk zijn dat een dergelijk online registratiesysteem met IP-bereiken van meer dan 10.000 organisaties zeer aantrekkelijk kan zijn voor kwaadwillende. Onze leden hebben hierover zorgen en willen graag duidelijke waarborgen vanuit het Rijk hebben rondom de (digitale en fysieke) beveiliging van de online registratievoorziening en het nationale register. Dit beperkt zich overigens niet alleen tot IP-bereiken maar álle aan te leveren data (incl. persoonsgegevens). Daarnaast willen we graag helderheid over de vraag wie toegang heeft/krijgt tot de IP-bereiken. Dit zou volgens ons beperkt moeten worden tot enkel en alleen het CSIRT.

- Het continue actueel houden van gegevens in de online registratievoorziening vergt de nodige tijd en capaciteit van entiteiten. Vanuit het Rijk zal op dit punt gerichte communicatie moeten plaatsvinden richting entiteiten. Vraag hierbij is ook hoe dit voor internationaal opererende bedrijven werkt.
  Wij pleiten voor een gerichte Rijksbrede voorlichtingscampagne over de registratieplicht (incl. het actueel houden van de eigen gegevens), als óók over de zorg- en meldplicht uit de Cbw. Waar wenselijk, kunnen VNO-NCW en MKB Nederland hierin een rol vervullen richting de branches van entiteiten.

- In de voorbereiding van bovengenoemde campagne – als ook overige communicatieve uitingen – moet aandacht uitgaan naar een juist gebruik van terminologie. In de wetsvoorstellen ter implementatie van de CER- en NIS2- richtlijn, bijbehorende beleidsstukken en communicatie wordt een groot aantal verschillende termen gebruikt voor entiteiten/organisaties/(sub)sectoren in het kader van het borgen van de weerbaarheid op het gebied van fysieke, digitale en economische veiligheid. Dit leidt tot onduidelijkheid bij de betrokken individuele bedrijven/organisaties, (sub)sectoren en branches. Daarom pleiten we voor een consistent gebruik van termen. Ook moet meer helderheid komen wat de relatie is met de Nederlandse vitale infrastructuur en de daarbij aangewezen vitale processen.

8. Samenwerking en informatie-uitwisseling (H14)

- Wat wordt in artikel 54 bedoeld met ‘gemeenschappen van entiteiten’? De NIS2-richtlijn geeft hier geen duidelijkheid over.

9. Verwerking van gegevens (H15)

- In artikel 65 lid 1 staat opgenomen dat onder een aantal voorwaarden vertrouwelijke gegevens kunnen worden uitgewisseld tussen de bevoegde autoriteit, het centrale contactpunt, de Minister van JenV en de Europese Commissie. In de MvT staat uiteengezet wat in beginsel onder vertrouwelijke gegevens wordt verstaan. Er staat echter niet uiteengezet hoe de vertrouwelijkheid van informatie-uitwisseling tussen betrokken partijen geborgd wordt. Graag op voorhand verduidelijking en/of nadere uitwerking hiervan (in de MvT).

- In de MvT wordt bij artikel 65 lid 1 aangegeven dat ook met de Autoriteit Persoonsgegevens vertrouwelijke gegevens mag worden uitgewisseld. Vraag is: waarom is hiervoor gekozen; wat is de achterliggende gedachte? Dit zou toch in principe enkel op aangeven van de

meldende partij moeten gebeuren en indien die een meldingsplichtig incident betreft onder de AVG?

- Wij zijn blij dat in artikel 65 lid 3 de bijzondere openbaarheidsregeling voor vertrouwelijke gegevens (zijnde gegevens die in beginsel vertrouwelijk door entiteiten aan het nationaal CSIRT zijn verstrekt) uit de huidige Wbni is overgenomen. Hiermee worden gegevens rondom de incidenten maar ook informatie die t.b.v. het toezicht is verkregen, uitgesloten van de Wet open overheid (Woo). Openbaarmaking van dit soort gegevens kan immers een (direct) risico vormen voor de entiteit in kwestie.

10. Toezicht en handhaving (H16)

- Wij zijn blij dat – conform eerder pleidooi – gekozen is voor (behoud van integraal) sectoraal toezicht, belegd bij de vakdepartementen.

- Gezien de samenloop / samenhang tussen de Cbw en Wwke, pleiten we voor een samenhangende aanpak in het toezicht op uitvoering van de eisen uit de twee wetten. In het verlengde daarvan, zijn wij blij dat de bevoegde autoriteit onder de Wwke overeenkomt met de bevoegde autoriteit onder de Cbw. Vraag: Kunnen we hieruit opmaken dat de toezichthouder voor entiteiten die zowel onder de Cbw als de Wwke vallen, hetzelfde is? Graag verduidelijking op dit punt.

- Toezicht op entiteiten moet plaatsvinden op basis van een risico gebaseerde benadering. Ofwel, focus moet liggen op die systemen waarmee het essentiële of belangrijke proces/dienst wordt bestuurd / van belang zijn voor leveringszekerheid.

- Voor entiteiten die in meerdere sectoren actief zijn en daarmee met meerdere toezichthouders te maken hebben/krijgen, wordt gepleit voor een transparante- en op elkaar afgestemde aanpak in het toezicht en handhaving ten einde toezichtslasten voor álle partijen te beperken. Wij zijn dan ook positief gestemd over het in de MvT genoemde samenwerkingsprotocol waarin toezichthouders onderling afspraken maken over gemeenschappelijk aangelegenheden. Wij pleiten ervoor dat dit in de praktijk ook daadwerkelijk wordt opgepakt.

- Artikel 68 stelt dat de bevoegde autoriteit (toezichthouder) bij essentiële entiteiten voor een bepaalde periode een controlefunctionaris kan aanwijzen. Vervolgens wordt ingegaan op de taken van de controlefunctionaris en wie de kosten voor inzet draagt. De meest elementaire vraag - wanneer dit instrument ingezet kan worden - wordt doorgeschoven naar de AMvB. Op basis van voorliggende wettekst wordt de indruk gewekt dat inzet van een controlefunctionaris op elk gewenst moment door de toezichthouder kan worden ingezet. Dat is zeer onwenselijk en wij pleiten er dan ook voor om in voorliggend wetsvoorstel de inzet van de controlefunctionaris te voorzien van een duidelijke inkadering met nadere uitwerking in de AmvB.

- Artikel 74 lid 2 sub b stelt dat de bevoegde autoriteit na één of meerdere maatregelen te hebben opgelegd aan een essentiële entiteit die er vervolgens niet toe heeft of hebben geleid dat de overtreding is beëindigd, kan overgaan tot het bepalen van een einddatum waarop de entiteit de overtreding moet hebben beëindigd. Eén van de maatregelen betreft de lichtste maatregel, te weten, het afgeven van een waarschuwing aan de entiteit voor een overtreding. VNO-NCW en MKB Nederland pleiten ervoor dat na het afgeven van de lichtste maatregel niet direct wordt overgegaan tot het bepalen van een einddatum maar eerst nog andere beschikbare maatregelen worden ingezet, zoals het geven van een bindende aanwijzing en/of een last onder bestuursdwang. In de MvT staat dit ook als zodanig: “In de meeste gevallen zal de toezichthoudende instantie eerst overgaan tot het

opleggen van andere maatregelen.” Voor een duidelijke inkadering van het instrument ‘einddatum’, pleiten wij voor de volgende aanpassing van lid 2b: “nadat zij twee of meer van de in het derde lid genoemde maatregelen heeft opgelegd aan de betrokken entiteit, …”

- De artikel 77 en 84 stellen dat ‘tezamen met of na het afgeven van een waarschuwing aan een essentiële of belangrijke entiteit’ een bestuurlijke boete kan worden opgelegd. Dit staat weliswaar als zodanig in de Europese NIS2-richtlijn maar in het kader van proportionaliteit pleiten we ervoor dat in de praktijk eerst wordt overgegaan tot enkel een waarschuwing en dat dit niet meteen tezamen gaat met een bestuurlijke boete. In de MvT staat terecht dat dit “gelet op de voor de toezichthoudende instantie geldende juridische kaders slechts denkbaar is in uitzonderlijke gevallen.” Wij pleiten ervoor dat dit zich inderdaad beperkt tot zeer uitzonderlijke gevallen.

- Artikel 75 gaat over het verzoek tot schorsing van certificering of vergunning. Dit heeft als doel om te voorkomen dat zolang de essentiële entiteit niet voldoet aan de eisen van de toezichthoudende instantie, activiteiten van deze entiteit leiden tot onacceptabele schade en/of risico’s voor derden. Vraag hierbij is: wat is onacceptabele schade en/of risico’s voor derden? Wij pleiten ervoor om dit in lagere regelgeving goed uit te werken zodat helder is wanneer dit (verregaande) handhavingsinstrument ingezet kan/mag worden.

11. Procesvragen

- We krijgen graag inzicht in de nadere tijdslijn van 1) de consultatie van de AMvB, 2) het opstellen van de drempelwaarden, en 3) eventuele ministeriële regelingen.

- Vanaf wanneer kunnen entiteiten zich registreren? En wat is de deadline voor registratie?

- Het is de verwachting dat de Cbw medio 2025 van kracht gaat. Is dit op het moment dat de wet, AMvB en drempelwaardes gereed zijn of wanneer het gehele pakket aan wet- en regelgeving (dus incl. de eventuele ministeriële regelingen met daarin nadere regels rondom de zorgplicht die voor een aantal sectoren wordt opgesteld) gereed is?

- Vanaf wanneer gaat het toezicht op de eisen uit de Cbw van kracht? Is dat het moment dat de wet, AMvB en drempelwaardes gereed zijn of wanneer het gehele pakket aan wet- en regelgeving (dus incl. de eventuele ministeriële regelingen met daarin nadere regels rondom de zorgplicht die voor een aantal sectoren wordt opgesteld) gereed is?

- Naar verluidt kunnen nieuwe NIS2-entiteiten (dus entiteiten die niet onder de huidige Wbni vallen) op basis van de door de Europese Commissie vastgestelde implementatiedatum van 17 oktober 2024 hulp en bijstand krijgen vanuit het NCSC. De plichten en het toezicht zouden echt pas in gaan wanneer de Cbw van kracht is. Wij zien dit graag bevestigd.

- Vervolgvraag is of entiteiten voor het verkrijgen van hulp en bijstand vanuit het NCSC zich eerst geregistreerd moeten hebben. En zo ja, hoe wordt in de periode totdat de Cbw van kracht is, de vertrouwelijkheid van gegevens geborgd? De Cbw met daarin de waarborgen is immers nog niet van kracht.