Den Haag, 28 juni 2024

Kenmerk B-24-056

Onderwerp Reactie VNCI consultatie Cyberveiligingswet (Cbw) / implementatie NIS2-richtlijn

Inleiding

De Koninklijke Vereniging van de Nederlandse Chemische Industrie (VNCI) heeft kennisgenomen van het wetsvoorstel Cyberbeveiligingswet (afgekort als Cbw). Dit voorstel implementeert de Europese NIS2-richtlijn en beoogd de digitale weerbaarheid te versterken. We maken graag gebruik van de internetconsultatie om op het wetsvoorstel te reageren.

Dit wetsvoorstel is gelijktijdig in consultatie gebracht met het wetsvoorstel Wet weerbaarheid kritieke entiteiten (Wwke), die zich richt op het versterken van de fysieke weerbaarheid van zogenaamde 'kritieke' entiteiten'. De VNCI dient ook een reactie op dit wetsvoorstel in, mede vanwege de beoogde samenhang tussen deze twee wetsvoorstellen.

Reactie consultatie Cyberbeveiligingswet (Cbw)

De VNCI merkt op dat meerdere onderdelen van het wetsvoorstel Cbw, waaronder de verdere invulling van de verplichtingen, nog nader moeten worden uitgewerkt in Algemene Maatregelen van Bestuur (AMvB's), (eventuele) ministeriële regelingen en onder meer een nationaal plan voor grootschalige cyberbeveiligingsincidenten. Het gevolg is dat de exacte uitwerking en impact van het wetsvoorstel op dit moment nog niet op alle onderdelen goed kan worden beoordeeld.

Daarom verzoeken wij of we betrokken kunnen worden bij de nadere uitwerking hiervan. Ook stellen we voor de concept AMvB's voor te leggen ter consultatie en hierbij de voorhang-procedure toe te passen.

Naast een algemene reactie heeft onze inbreng betrekking op de volgende onderdelen van het wetsvoorstel Cbw en de bijbehorende Memorie van Toelichting (MvT):

1. Algemene reactie
2. Reikwijdte wetsvoorstel
3. Verhouding tot nationale wetgeving
4. Normadressaat
5. Essentieel en/of belangrijke entiteit
6. Registratieplicht
7. Zorgplicht
8. Meldplicht
9. Governance
10. Toezicht

Koninklijke Vereniging van de Nederlandse Chemische Industrie
Loire 150 \ 2491 AK Den Haag \ Postbus 443 \ 2260 AK Leidschendam
www.vnci.nl \ T (070) 337 87 87 \ KvK-nr: 40408889 \ BTW-nr.: NL 0027 114 12 B01

1. Algemene reactie

De VNCI staat in beginsel positief tegenover de doelen van de NIS2-richtlijn en het bijbehorende wetsvoorstel van de Cyberbeveiligingswet (Cbw). Het verhogen van digitale veiligheid en weerbaarheid is cruciaal voor een veilige bedrijfscontinuiteit van de chemiebedrijven en daarmee de vitale rol van de chemiesector voor de economie en maatschappij. Dit geldt in het bijzonder in een tijd waarin (internationale) digitale en fysieke dreigingen onverminderd groot zijn.

In de NIS2- richtlijn is gekozen voor een risico gebaseerde aanpak. We ondersteunen deze benadering. Daarom vragen we dit leidend principe van 'risico gerichte aanpak' ook door te voeren in de nog op te stellen AMvB's en eventuele ministeriële regelingen én bij het vormgeven van het toezicht.

Daarnaast waarderen wij de voorgestelde invoering van doelvoorschriften in het wetsvoorstel, omdat daarmee maatwerk kan worden geleverd op individueel bedrijfsniveau. Hiermee wordt recht gedaan aan de eigen verantwoordelijkheid van bedrijven voor het waarborgen van hun digitale weerbaarheid. Het is wel van belang dat de eisen die aan de bedrijven worden gesteld proportioneel en risicogericht zijn. Ook de administratieve lasten moeten daarbij zo beperkt mogelijk blijven. In het wetsvoorstel zijn echter een aantal bepalingen opgenomen, die kunnen leiden tot hoge administratieve lasten voor bedrijven en tot een versnippering en in sommige gevallen dubbel toezicht.

Omdat cyberrisico's een internationaal karakter hebben is het van belang dat er minimaal een gelijk Europees speelveld is op het gebied cyberbeveiliging. De NIS2-richtlijn creëert de kaders voor gelijkluidende Europese spelregels.
Daarom verzoeken wij dringend bij de nadere uitwerking in AMvB's en eventuele ministeriële regelingen geen nationale koppen te introduceren, zoals ook opgenomen in het Hoofdlijnenakkoord 2024-2028. In de MvT van het wetsvoorstel (zie paragraaf 5.3.5 MvT) is echter aangegeven dat Nederland naar verwachting in een AMvB maatregelen wil vaststellen die een hoger cyberbeveiligingsniveau eisen, waarmee een nationale kop zal worden geïntroduceerd. Het stellen van aanvullende eisen door individuele lidstaten druist in tegen het doel van de NIS2-richtlijn, namelijk een gelijkspeelveld in Europa. Daarnaast hebben de (chemie)bedrijven, die onder de NIS2-richtlijn vallen, veelal entiteiten die in meerdere lidstaten opereren. Aanvullende nationale regels zullen daarom onwerkbaar zijn voor dergelijke bedrijven.

In het kader van onder meer de registratie- en meldplicht, moeten bedrijven bepaalde gegevens en informatie aanleveren. Ook kunnen op basis van de NIS2-richtlijn door de entiteiten verstrekte gegevens gedeeld worden tussen onder meer bevoegde autoriteiten en de Europese Commissie. Dit zijn cyber kritische processen, waar de hoogste beveiligings- en beschermings-eisen voor moeten gelden met in achtneming van de privacyregelgeving. Daarom dringen we erop aan de vertrouwelijkheid en beveiliging van deze informatie-uitwisseling tussen bedrijven en autoriteiten op grond van deze wet te waarborgen. Daarnaast benadrukken we dat geborgd moet worden dat bedrijfsvertrouwelijke informatie niet openbaar wordt gemaakt.

Gezien de onderlinge verbanden tussen de cyberbeveiligingswet (Cbw) en de Wet Weerbaarheid kritieke entiteiten (Wwke) doen we een dringend beroep op de wetgever om de gehanteerde begrippen in deze wetgeving uniform en eenduidig toe te passen. Zowel in de voorliggende wetsvoorstellen als in de uitgebrachte communicatiemiddelen worden verschillende termen gebruikt voor vergelijkbare begrippen. Het betreft onder meer belangrijke en essentiële entiteiten (Cbw), essentiële diensten en kritieke entiteiten (Wwke), maar ook andere begrippen zoals zeer kritieke en kritieke sectoren (zie Informatiebrochure NIS2).
Het gebruik van deze wirwar aan begrippen leidt tot onduidelijkheid voor bedrijven of zij onder de reikwijdte van deze wetten vallen en zo ja welke kwalificatie op hen van toepassing is (kritiek en/of essentieel of belangrijk). We verzoeken dan ook om deze begrippen in de MvT van de beide wetsvoorstellen (Wwke en Cbw) en in de externe communicatie te verhelderen, zodat bedrijven weten waar zij aan toe zijn en zij zich waar nodig kunnen voorbereiden.

2. Reikwijdte wetsvoorstel

In de NIS2-richtlijn en de Cbw is een brede definitie opgenomen van een netwerk- en informatiesysteem. Gelet op de risico gebaseerde aanpak in de NIS2-richtlijn en de Cbw zijn wij van oordeel dat de focus moet komen te liggen op de beveiliging en bescherming van die netwerk- en informatiesystemen die randvoorwaardelijk zijn voor de veilige continuïteit van de kernactiviteiten van een bedrijf en verzoeken u dit te verduidelijken in de MvT.

3. Verhouding tot nationale wetgeving

Met de Cbw wordt beoogd om de NIS2-richtlijn in één centrale wet te implementeren en niet in sectorale wetgeving (zie paragraaf 2.4 MvT). Dit uitgangspunt wordt door de VNCI ondersteund.

Een deel van de bedrijven in de chemiesector valt onder de zogenaamde Europese Seveso wetgeving, die in Nederland is opgenomen in sectorale wetgeving. In de MvT (zie paragraaf 7.4 MvT) is aangegeven dat er voor de sector chemie geen sprake is van botsing van bestaande wetgeving met de uit de NIS2-richtlijn voortvloeiende verplichtingen.

In de huidige praktijk blijkt echter dat door toezichthouders van de Seveso wetgeving ook het aspect cyberweerbaarheid in het kader van Seveso wetgeving wordt meegenomen bij inspecties of hebben aangekondigd dit te zullen doen, in het bijzonder door te verlangen van bedrijven dat cyberrisico's ook worden meegenomen in hun veiligheidsbeheerssystemen (VBS) [1].
Wij pleiten daarom ook voor een goede scheiding en afbakening tussen de verplichtingen op grond van Cybersecuritywetgeving en de Seveso-verplichtingen om onduidelijkheden, mogelijke tegenstrijdigheden en onnodige overlap in de uitvoering tegen te gaan en stapeling van administratieve en (toezichts)lasten voor bedrijven te voorkomen.
Wij stellen dan ook voor om deze duidelijke afbakening op te nemen en nader toe te lichten in de MvT voor de sector chemie en eventuele andere sectoren waarvoor de Seveso wet- en regelgeving van toepassing is (bijvoorbeeld raffinaderijen). De verplichtingen vanuit de Cbw moeten leidend zijn als het gaat om digitale weerbaarheid.

4. Normadressaat

De verplichtingen in de Cbw gelden voor zogenaamde essentiële en belangrijke entiteiten (de normadressaat). In artikel 1 van de Cbw is het begrip nader gedefinieerd.

Bij de uitvoering en het toezicht dient er echter rekening mee gehouden te worden dat bij grotere bedrijven in het algemeen cybersecurity en de netwerk- en informatiebeveiliging niet op het niveau van de individuele "entiteiten", maar centraal op corporate niveau heeft georganiseerd. Het betreft veelal internationaal opererende bedrijven.
Bij de implementatie van de registratie-, zorg- en meldplicht is het van belang dat de ontwikkelde corporate aanpak hierin wordt meegenomen. Denk bijvoorbeeld aan het melden van cyberincidenten, dat (veelal) op corporate niveau plaatsvindt.

Voor bedrijven, die op een internationale markt actief zijn, zoals de chemische industrie, is het in het kader van (Europese) rechtszekerheid en – gelijkheid van belang dat de door de corporate organisatie ontwikkelde aanpak voor het beheersen van de beveiliging van de netwerk- en informatiesystemen conform de NIS2-richtlijn resp. de Cbw op dezelfde wijze wordt beoordeeld op zowel (decentraal) 'bedrijfsniveau' als (centraal) 'corporate niveau'. Ook is het van belang dat bepaalde verplichtingen op corporate niveau kunnen worden belegd, bijvoorbeeld het melden van cyberincidenten.
We verzoeken deze 'corporate aanpak' nader toe te lichten in de MvT.

[1] Zie artikel 4.11 Besluit activiteiten leefomgeving.

5. Essentieel en/of belangrijke entiteit

In artikel 8 tot en met 11 van de Cbw is bepaald welke entiteiten zgn. essentiële entiteiten zijn en in de artikelen 12, 13 en 14 is de aanwijzing van zgn. belangrijke entiteiten geregeld. In deze artikelen wordt verwezen naar de in bijlage 1 en 2 opgenomen lijst van entiteiten en sectoren. Voor een aantal bedrijven/organisaties is het op basis van de voorliggende tekst echter niet duidelijk onder welke sector zij vallen en daarmee of zij als essentieel of belangrijk moeten worden beschouwd. Gevolg hiervan is dat het niet duidelijk is 'welk toezichtregime' van toepassing is; voor essentiële entiteiten geldt namelijk een zwaardere toezichtregime dan voor belangrijke entiteiten.
We lichten dit hieronder nader toe aan de hand van een aantal verschillende situaties.

<u>Primaire bedrijfsprocessen versus ondersteunende processen</u>

Bedrijven binnen verschillende industriële sectoren die vallen onder het bereik van de Cbw, waaronder de chemische sector, de farmaceutische sector en de levensmiddelenindustrie, hebben vaak 'ondersteunende' processen zoals een afvalwaterzuiveringsinstallatie en/of afvalbeheer. In bijlage 1 en 2 van de Cbw is bepaald dat afvalwaterzuivering en afvalbeheer vallen onder de sectoren afvalwater resp. afvalstoffenbeheer, tenzij de afvalwateractiviteit of het afvalstoffenbeheer een 'niet essentieel onderdeel' is van de algemene activiteit, resp. 'niet de voornaamste economische activiteit' is van de onderneming[2].
Daarbij is echter niet aangegeven wat precies bedoeld wordt met een 'niet essentieel onderdeel' resp. 'niet de voornaamste economische activiteit'. Daardoor zal het voor bedrijven niet altijd duidelijk zijn tot welke sector zij behoren en of sprake is van een essentiële of belangrijke entiteit en welke eisen en welk toezichtregime van toepassing zal zijn.

Daarom stellen we het voor om de kernactiviteit van een bedrijf leidend te laten zijn bij het bepalen tot welke sector het bedrijf behoort. Voor de sector chemie is het voorstel om in de MvT te verduidelijken dat de processen 'afvalwaterzuivering resp. afvalbeheer', ondersteunende activiteiten zijn van de kernactiviteiten van de bedrijven in de chemische industrie. Een vergelijkbare benadering kan waarschijnlijk ook worden toegepast op andere industriële sectoren.
Daarbij merken we op dat deze ondersteunende processen in het kader van de risicogerichte aanpak wel onderdeel kunnen zijn van de risicoanalyse en eventuele beheersmaatregelen in het kader van de cyberbeveiliging om een veilige bedrijfscontinuiteit te waarborgen.

[2] Zie onder sector afvalwater resp. afvalstoffenbeheer, bijlagen 1 en 2 van Cbw.

Primaire processen, die onder verschillende Cbw sectoren vallen

Daarnaast zijn er bedrijven met verschillende bedrijfsprocessen, die vallen onder verschillende sectoren, waardoor zij zowel als essentieel als belangrijk kunnen worden aangeduid.
Diverse bedrijven in de chemische sector hebben bijvoorbeeld naast de productie en/of distributie van chemische stoffen (zoals genoemd in bijlage 2 van Cbw) ook processen die gericht zijn op de productie/opslag en distributie van aardolie en waterstof (zoals genoemd in bijlage 1 van Cbw). Dit zou tot gevolg kunnen hebben dat een dergelijk bedrijf onder verschillende sectoren valt en gekwalificeerd kan worden zowel als een essentiële als een belangrijke entiteit.
In de tekst en toelichting van de NIS2-richtlijn en het wetsvoorstel Cbw wordt nadrukkelijk onderscheid gemaakt tussen essentiële en belangrijke entiteiten. Het kan dan ook niet de bedoeling zijn dat een bedrijf of organisatie een dubbele kwalificatie krijgt, dat wil zeggen zowel als 'essentieel' als 'belangrijk' wordt bestempeld.

Indien bedrijven onder verschillende sectoren vallen en een dubbele kwalificatie hebben, kunnen deze bedrijven bovendien te maken krijgen met verschillende autoriteiten, vakdepartementen en toezichthouders (zie artikel 16 Cbw). Gevolg hiervan is dat diverse sectorale eisen van toepassing zijn met verschillende toezicht regimes en daarmee ontstaat een enorme toename in administratieve en toezichtslasten voor deze bedrijven.

Overigens kan deze situatie zich ook voordoen bij overheidsorganisaties, zoals een waterschap die zowel valt onder de sector 'overheid' als 'afvalwater'.

Daarom pleiten wij ervoor dat één toezichthouder wordt aangewezen voor de bedrijven c.q. organisaties die op basis van hun kernactiviteiten/primaire processen onder verschillende sectoren vallen, die namens alle betrokken vakdepartementen toezicht houdt op de naleving van de Cbw verplichtingen.

6. Registratieplicht

In het kader van de registratieverplichting moeten bedrijven zich zelf registreren via een online registratievoorziening, inclusief de benodigde contactgegevens en IP-adressen (zie onder andere artikel 45, lid 1.b Cbw). Deze gegevens worden opgenomen in een nationale registratie. Dergelijke digitale gegevensprocessen kunnen worden beschouwd als een 'high risk' cyberrisico. We pleiten daarom voor goede waarborgen rondom de beveiliging van het register en de digitale informatie-uitwisseling (zowel nationaal als internationaal). Daarnaast pleiten we ervoor dat de aanlevering van IP-adressen geen wettelijke verplichting wordt.

7. Zorgplicht

We onderschrijven het in de CbW opgenomen uitgangspunt dat het aan entiteiten zelf is om - op basis van een risicobeoordeling - vast te stellen welke maatregelen passend, kosteneffectief en evenredig zijn om invulling/uitwerking te geven aan de zorgplicht. Hierbij kunnen zij hun eigen 'normenkader(s)' hanteren volgens de MvT. Entiteiten hebben immers de meeste kennis van hun systemen inclusief de kwetsbaarheden. Daarom pleiten we er voor dat naast het gebruik van internationale, nationale of sectorale standaarden en richtsnoeren ook mogelijk is een kader te gebruiken dat op corporate niveau is opgesteld conform de uitgangspunten van de NIS2-richtlijn resp. de Cbw.
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. In de MvT is terecht aangegeven, dat het volledig uitsluiten van risico's en 100% veiligheid niet mogelijk of reëel is. Restrisico's zullen er helaas altijd zijn en over de afwegingen die daaraan ten grondslag liggen zal het gesprek tussen entiteiten en toezichthouders moeten gaan.

Entiteiten moeten niet alleen naar de cybersecurity van hun eigen organisatie kijken, maar ook rekening houden met de specifieke kwetsbaarheden van hun rechtstreekse leveranciers en dienstverleners. Volgens de MvT moeten ook de algemene kwaliteit van de cyberveiligheid kritische producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners hierbij worden meegenomen.
Gezien de afhankelijkheden van de partners in de keten op het gebied van cybersecurity, is aandacht voor ketenveiligheid terecht en ook noodzakelijk. Voor een goede uitvoerbaarheid van de eisen en beheersbaarheid ervan, staan wij volledig achter de voorgestelde afbakening van de ketenverantwoordelijkheid conform artikel 21 lid 2 onder d en derde lid van de NIS2-richtlijn, namelijk de rechtstreekse of directe leveranciers en dienstverleners. In aanvulling hierop, pleiten wij ervoor dat de focus komt te liggen bij de (directe/rechtstreekse) leveranciers en dienstverleners van netwerk- en informatiesystemen die kritisch zijn voor het borgen van de continuïteit van de kernactiviteiten. Niet alle leveranciers en dienstverleners zijn van belang voor de continuïteit van de kritische IT/OT systemen van het bedrijf. Graag zouden we zien dat deze aanvullende toelichting wordt opgenomen in de MvT.

Voor de uit te voeren risicoanalyse door entiteiten is inzicht in actuele dreigingen en gevaren een vereiste. Voor de eerste categorie (dreigingen) is informatie benodigd vanuit de inlichtingen- en/of overheidsdiensten. We roepen de verantwoordelijke overheidsautoriteiten 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 onder meer mogelijk.

Tot slot wijzen we nog op de mogelijke overlap tussen de zorgplicht in de Cbw en de zorgplicht in de Wet weerbaarheid kritieke entiteiten (Wwke). Voor sommige entiteiten zijn beide zorgplichten van toepassing. Bedrijven maken in hun bedrijfsvoering en risicomanagement geen onderscheid tussen beide zorgplichten, maar passen een zogenaamde all risk benadering toe. Wij pleiten er dan ook voor dat bedrijven die onder beide wettelijke regimes vallen, de mogelijkheid krijgen om via één integrale risicoanalyse en één pakket van maatregelen de naleving van hun zorgplichten uit de Cbw en Wwke aan de toezichthouder aan te tonen.

8. Meldplicht

Wij pleiten voor een proportionele en risico gebaseerde drempelwaarde voor de meldplicht voor zogenaamde significante incidenten. De focus moet daarbij liggen op de beveiliging van de continuïteit van de kernactiviteiten van bedrijven en organisaties.

Oproep is om bij het vaststellen van de drempelwaarden het doel van de wettelijke meldplicht voorop te stellen, namelijk het verlenen van hulp en bijstand om de nadelige gevolgen van incidenten zoveel mogelijk te beperken c.q. beheersen.
Hoewel het melden van incidenten ook beoogd hiervan te leren en kan leiden tot beter inzicht in bepaalde trends, stellen wij hier een andere aanpak voor. Je kan hierbij denken aan het stimuleren van het vrijwillig melden, gebaseerd op laagdrempeligheid, inclusief de borging van de vertrouwelijkheid (d.w.z. verstrekte informatie niet wordt doorgezet naar de toezichthouder). Daarnaast dient te worden ingezet op een goede informatie-uitwisseling binnen de ISAC's, die ook bijdraagt aan het versterken van het leervermogen.

Volgens artikel 27 lid 2 sub b Cbw moet een incident als significant incident worden aangemerkt als het andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële- en immateriële schade te veroorzaken. Van immateriële schade kan geen sprake zijn bij rechtspersonen, maar alleen bij natuurlijke personen.
Het Nederlandse recht kent niet het gehanteerde onderscheid tussen materiële- en immateriële schade, maar spreekt in artikel 6:95 BW over schade die bestaat uit vermogensschade en ander nadeel. Voorstel is om daar in zijn algemeenheid naar te verwijzen zodat het schadebegrip in voorliggend wetsvoorstel aansluit op het Nederlandse rechtssysteem.

Daarnaast pleiten we ervoor de administratieve lastendruk die de meldplicht op basis van de Cbw met zich meebrengt voor de entiteiten zoveel mogelijk te beperken. De meldplicht beperkt zich immers niet alleen tot het doen van de officiële melding (met daaraan voorafgaande nog wellicht een vroegtijdige waarschuwing), maar vereist ook updates, tussentijdse verslagen, een voortgangsverslag en een eindverslag (zie onder meer artikel 27 t/m artikel 31 Cbw). Het is niet altijd helder wat de verschillen zijn van deze verplichtingen.

Zo is bijvoorbeeld in artikel 29 en 30 Cbw opgenomen dat een Computer Security Incident Response Team (CSIRT) of de bevoegde autoriteit om een tussentijds verslag over relevante updates kan vragen. Uit de wetstekst en de MvT wordt niet of nauwelijks duidelijk in welke gevallen dergelijke tussentijdse verslagen en updates van entiteiten gevraagd kunnen worden. Daarom rijst de vraag wat de meerwaarde is van de verschillende rapportageverplichtingen in het kader van een incidentmelding.
Het dringend verzoek is het 'meldingsproces' efficiënt (lean and mean) in te richten en te overwegen de rapportageverplichtingen tot het geven van updates en indienen van tussentijdse verslagen zoveel mogelijk te beperken. We verzoeken daarom de wet en/of de MvT daarop aan te passen met daarbij in achtneming de algemene lastendruk en de capaciteit die bij entiteiten op het moment van een (dreigend) incident benodigd is voor de beperking/ beheersing van de nadelige gevolgen van het incident en het veiligstellen van de continuïteit van de operatie in plaats van het opstellen van tussentijdse verslagen.

Verder onderstrepen we nogmaals het belang dat het uitwerken van de nadere regels over meldingen van significante incidenten (zie paragraaf 9.5 Cbw) plaats zal vinden in nauwe samenwerking met de betrokken sectoren en vakdepartementen. Het zijn immers de entiteiten zelf die kunnen bepalen wanneer de bedrijfscontinuiteit in gevaar komt of kan komen. De uitgewerkte drempelwaarden moeten SMART geformuleerd worden zodat er in de praktijk géén discussie kan ontstaan tussen entiteiten, toezichthouders en het CSIRT (ofwel het NCSC) of significante incidenten al dan niet gemeld hadden moeten worden.
Hierbij moet ook op Europees niveau afstemming plaatsvinden bij het uitwerken van de eisen aan de meldplicht (inclusief de drempelwaarden), waardoor wordt bijgedragen aan een gelijk speelveld voor de sectoren, waaronder de internationaal opererende bedrijven.

Daarnaast roepen wij de wetgever op om toe te werken naar één centraal meldloket voor alle meldingen. Diverse sectoren, zoals de chemische industrie, hebben naast de meldplicht op basis van de Cbw en de Wwke te maken met diverse sectorale wetgeving, waarvoor een meldplicht geldt. Bovendien kan er sprake zijn van 'overlap' dan wel 'samenhang' tussen deze meld-verplichtingen. Denk hierbij aan bedrijfsstoringen, die van belang zijn op basis van de Wwke, Cbw en sectorale wetgeving, zoals het melden van ongewone voorvallen in kader van de Omgevingswet.
Afhankelijk van de type / aard van de melding is het van belang dat de meldingen via zo'n centraal meldpunt goed gekanaliseerd worden, zodat alleen de melding naar de betrokken toezichthouder(s) en/of het CSIRT en/of NCSC gaat.

Tenslotte willen we ook hier benadrukken dat door entiteiten verstrekte (digitale) informatie op de juiste en adequate wijze wordt beveiligd, waarbij bedrijfsvertrouwelijke informatie wordt beschermd en niet openbaar wordt gemaakt.

9. Governance

Ingevolge artikel 26 Cbw is het bestuur van de betrokken entiteit eindverantwoordelijk voor de zorgplicht. Het bestuur moet de maatregelen ter uitvoering van de zorgplicht goedkeuren en toezicht houden op de uitvoering hiervan. In artikel 26 lid 2 e.v. zijn voorts opleidings-verplichtingen opgenomen voor de leden van het bestuur. Het is echter niet helder wat precies moet worden verstaan onder (de leden van) het bestuur van een entiteit. Voorgesteld wordt om voor het begrip 'bestuur' resp. 'leden van het bestuur' een definitie op te nemen in artikel 1 Cbw (begripsbepaling).

Daarnaast gaat artikel 26 lid 4 t/m lid 6 Cbw volgens ons verder dan de NIS2-richtlijn voorschrijft. In de NIS2-richtlijn wordt namelijk gesproken van het volgen van een training, terwijl in de Cbw een certificaat van deelname wordt geëist, inclusief dat via een AMvB nadere regels kunnen worden gesteld aan de te volgen training. Hiermee gaat de Cbw voorbij aan de beleidsarme omzetting.
Het is voor entiteiten die in meerdere lidstaten opereren namelijk onwerkbaar wanneer op lidstaat niveau nadere eisen worden gesteld over de duur en het niveau van een training. Deze entiteiten willen voor het gehele bedrijf een uniforme training opzetten zonder gehinderd te worden door aanvullende / verschillende eisen vanuit individuele lidstaten.
Verder stellen we voor om in de MvT aan te geven dat dit zowel een interne als externe training mag zijn. Dat juichen wij toe, aangezien voor entiteiten, die in meerdere lidstaten opereren, de uitrol van een interne training efficiënter is.
Gelet op het voorafgaande verzoeken wij om op dit punt geen nadere regels te stellen en vragen om dit onderdeel van de Cbw in lijn te brengen met de NIS2-richtlijn. Volgens ons volstaat het met een toelichting in de MvT, waarbij de uitwerking van de benodigde kennis en vaardigheden maatwerk is op bedrijfsniveau.

10. Toezicht

Toezicht op entiteiten moet plaatsvinden op basis van vertrouwen en een risico gebaseerde benadering, waarbij de focus moet liggen op die systemen, die van belang zijn voor een veilige bedrijfscontinuiteit. Hierbij dringen we aan op transparante toetsingskaders voor de toezichthouders.

Zoals eerder opgemerkt worden sommige chemiebedrijven zowel als een essentiële als belangrijke entiteit gekwalificeerd ('dubbele kwalificatie'), omdat zij actief zijn in verschillende sectoren. Bij deze bedrijven pleiten wij voor één toezichthouder voor de Cbw (zie 5. Essentiële en/of belangrijke entiteit).

Daarnaast heeft de chemische industrie te maken met meerdere toezichthouders vanwege sectorale wetgeving. Om versnippering en stapeling van toezicht te voorkomen pleiten we voor een transparante- en op elkaar afgestemde aanpak in het toezicht en handhaving ten einde toezichtslasten voor álle betrokken partijen zoveel mogelijk 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, waarbij niet alleen het afgestemde toezicht op de verplichtingen in het kader van Cbw worden opgenomen, maar ook de afstemming met het toezicht op andere relevante (sectorale) wetgeving, zoals de Wwke en de Seveso wetgeving. Belangrijk daarbij is een duidelijk afbakening in taken en verantwoordelijkheden, zoals eerder in deze reactie is opgemerkt (zie 3. Verhouding tot nationale wetgeving).

Artikel 68 Cbw 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.
Op basis van voorliggende wettekst wordt de indruk gewekt dat inzet van een controle-functionaris 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 in te kaderen door het opnemen van algemene criteria, die vervolgens nader kunnen worden uitgewerkt in een AMvB.

Artikel 77 en 84 Cbw 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. In het kader van proportionaliteit pleiten we ervoor dat in de praktijk eerst wordt overgegaan tot een waarschuwing en dat dit niet meteen gepaard zal gaan 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.

Graag verzoeken wij om de hiervoor ingebrachte punten mee te nemen in de verdere uitwerking het voorliggende wetsvoorstel.
Desgewenst zijn wij graag bereid bovengenoemde punten nader toe te lichten.

Tenslotte brengen we graag onze kennis en ervaringen in bij de (eventuele) uitwerking van de wettelijke regels en het opstellen van het nationaal plan voor grootschalige cyberincidenten en respons.

Met vriendelijke groet,

Peter Bareman
Senior Beleidsadviseur
bareman@vnci.nl
T: 06 - 349 248 72

Deze brief is verzonden aan:
- Ministerie van Justitie en Veiligheid
- Ministerie van Infrastructuur en Waterstaat
- VNO-NCW en MKB Nederland