Den Haag, 27 maart 2025

Kenmerk	B-25-014
Onderwerp	VNCI reactie internetconsultatie Cyberbeveiligingsbesluit en bijbehorende Ministeriele Regeling

Inleiding

De Koninklijke Vereniging van de Nederlandse Chemische Industrie (VNCI) heeft kennisgenomen van de concept Algemene Maatregel van Bestuur (AMvB) Cyberbeveiligingsbesluit (afgekort als Cbb) en de bijbehorende concept Ministeriële regeling (MR).
In de concept AMvB zijn de regels uit het wetsvoorstel Cyberbeveiligingswet (Cbw) uitgewerkt.
In de concept MR zijn aanvullende eisen over de zorgplicht uitgewerkt onder meer voor de chemische industrie.
Via de Cyberbeveiligingswet en onderliggende uitvoeringsregels wordt de Europese Network and Information Security Directive (NIS2-richtlijn) geïmplementeerd.

Reactie consultatie

We maken graag gebruik van de internetconsultatie om op de concept AMvB Cyberbeveiligings-besluit en de bijbehorende concept MR te reageren[1].

In de algemene reactie heeft onze inbreng betrekking op de volgende onderwerpen:

1. Minimumharmonisatie – geen aanvullende nationale eisen
2. Invulling van de zorgplicht door middel van doelbepalingen
3. Ondersteuning bedrijven bij uitvoering
4. Verduidelijking complexe bedrijfsmodellen
5. Geef voldoende tijd voor implementatie en voorkom dubbele toezichtslasten

Verder hebben we een artikelsgewijze reactie opgenomen op het Cbb en sluiten we af met een reactie op de MR.

[1] Deze concept AMvB en MR zijn gelijktijdig in consultatie gebracht met het concept Besluit weerbaarheid kritieke entiteiten (Bwke). In de concept Bwke zijn de regels uit het wetsvoorstel Wet weerbaarheid kritieke entiteiten (Wwke) uitgewerkt. De VNCI dient ook een reactie op dit concept besluit.

Algemene reactie

1. Minimumharmonisatie – geen aanvullende nationale eisen

Cyberrisico's hebben veelal een internationaal karakter, denk aan buitenlandse hackers. Internationale bedrijven, die onder de NIS2-richtlijn vallen, zoals bedrijven in de chemische sector, opereren vaak met meerdere entiteiten in verschillende lidstaten. Bij deze bedrijven is de cyberbeveiliging veelal op corporate niveau belegd.
Mede gelet op deze internationale context is het van belang dat er een gelijk Europees speelveld is op het gebied van cyberbeveiliging. De NIS2-richtlijn creëert de kaders voor gelijkluidende Europese spelregels. Het stellen van aanvullende eisen door individuele lidstaten druist in tegen het doel van de NIS2-richtlijn, namelijk een gelijk speelveld in Europa.

Hoewel in de Memorie van Toelichting (MvT) van de Cbw[2] is aangegeven dat momenteel **niet** wordt gekozen voor zwaardere eisen dan de minimumeisen van de NIS2-richtlijn, bevatten het concept Cbb en de MR toch een aantal aanvullende eisen, zoals extra eisen met betrekking tot noodcommunicatiesystemen (artikel 9 Cbb), het omgaan met informatie (artikel 16 Cbb), de training (artikel 20- 22 Cbb) en aanvullende regels voor de zorgplicht (MR).
VNCI is van mening dat er - conform het Hoofdlijnenakkoord 2024-2028 waarin is afgesproken geen nationale koppen op Europese regelgeving te zetten – géén aanvullende / zwaardere eisen ter uitvoering van de NIS2-richtlijn moeten worden gesteld. VNCI dringt er op aan dat het voorliggend concept Cbb en MR daarop worden herzien.

2. Invulling van de zorgplicht door middel van doelbepalingen

De huidig voorgestelde (detail)uitwerking van de zorgplicht[3] in het concept Cbb leidt tot een papieren werkelijkheid en daarmee tot extra regeldruk in plaats van de beoogde versterking van de cyberbeveiliging- en weerbaarheid van bedrijven. Volgens de VNCI is de voorliggende uitwerking van de zorgplicht praktisch onwerkbaar en onnodig belastend. Bovendien is dit in strijd met de NIS2-richtlijn en de Cbw. In de MvT van de Cbw[4] is namelijk opgenomen dat in het kader van de zorgplicht de entiteiten zelf verantwoordelijk zijn voor het vaststellen van maatregelen die passend en evenredig zijn om de risico's waarmee zij geconfronteerd kunnen worden, beheersbaar te houden. Entiteiten hebben immers zelf inzicht – op basis van een risicobeoordeling – in de risico's die hun dienstverlening kunnen raken en hebben de meeste kennis van hun eigen systemen en processen.

[2] Zie pagina 58 MvT van de Cbw.
[3] Zie ook onze artikelsgewijze reactie op de zorgplichtbepalingen.
[4] Zie onder meer pagina 18 MvT van de Cbw.

Zoals in eerdere overleggen met de overheid is aangegeven, zou de overheid zich wat de zorgplicht betreft moeten beperken tot het stellen van duidelijk omschreven *doelvoorschriften,* waarbij de invulling aan bedrijven zélf wordt overgelaten. Dit dwingt bedrijven om zélf op een risicogebaseerde wijze na te denken over wat nodig is en wat daadwerkelijk bijdraagt aan de beveiliging en continuïteit van hun netwerk- en informatiesystemen. Het is daarbij van belang de cyberweerbaarheid te richten op de netwerk- en informatiesystemen, die randvoorwaardelijk en/of kritisch zijn voor hun essentiële- c.q. belangrijke dienstverlening. Dit sluit ook aan bij de risicogebaseerde benadering die centraal staat in de NIS2-richtlijn.
In nagenoeg elk artikel én sub-artikel van hoofdstuk 4 (zorgplicht) van het concept Cbb wordt van bedrijven geëist dat zij over vastgesteld beleid, procedures en/of planvorming beschikken, gevolgd door een uiteenzetting van wat dit beleid, deze procedures en planvorming moeten omvatten.
Deze huidige opzet van de zorgplicht leidt vooral tot het veelvuldig opstellen en invullen van documenten wat zeer veel capaciteit vergt – zowel qua mensen als qua middelen – en leidt tot administratieve rompslomp. We zijn van mening dat dit de cyberveiligheid niet ten goede komt. Deze aanpak vergroot de regeldruk en leidt tot een enorme toename in administratieve lasten. Daarom dragen de voorgestelde middelvoorschriften onvoldoende bij aan een risicogebaseerde zorgplicht voor een proportionele en uitvoerbare cyberbeveiliging bij de individuele bedrijven.

VNCI doet daarom een dringende oproep aan de wetgever om de opzet van de zorgplicht-bepalingen in het voorliggend Cbb te herzien door deze middelvoorschriften te vervangen door duidelijk omschreven doelvoorschriften. Mogelijk kan de wetgever daarbij gebruik maken van voorbeelden in andere regelgeving, die gericht is op het voorkomen en mitigeren van andere type veiligheidsrisico's. Hierbij kan bijvoorbeeld worden gedacht aan de doelvoorschriften die in artikel 4.9 en volgende van het Besluit Activiteiten Leefomgeving zijn gesteld in het kader van de Europese Seveso richtlijn.

Naast deze doelvoorschriften pleiten wij ervoor om, in samenwerking met de betrokken sectoren, een handreiking voor bedrijven op te stellen. Deze handreiking kan handvatten bieden voor onder meer het opstellen van risicoanalyses en de te nemen maatregelen.
Wij raden aan daarbij ook gebruik te maken van de kennis die aanwezig is bij het Nederlandse Platform Samen Digitaal Veilig, branches en (vitale) sectoren, zoals de chemische industrie. Mogelijk biedt de, door het Centrum voor Cybersecurity België ontwikkelde, handreiking 'framework CyberFundamentals (CyFun®) Framework' handvatten die ook bruikbaar zijn voor een Nederlandse handreiking.

3. Ondersteuning bedrijven bij uitvoering

De NIS2-richtlijn bevat ten opzichte van de NIS1-richtlijn een forse uitbreiding van de doelgroep, waardoor er meer bedrijven onder de Cbw en het Cbb komen te vallen. Dit zal ertoe leiden dat de eerder door de Cyber Security Raad geconstateerde weerbaarheidskloof zal worden verkleind en de (waarde)ketens worden versterkt.
VNCI onderschrijft deze belangen. Tegelijkertijd pleiten wij ervoor dat bij de implementatie van de NIS2-richtlijn via de Cbw, het Cbb en bij het toezicht, rekening wordt gehouden met de beschikbare middelen en menskracht van de betrokken bedrijven (in het bijzonder het MKB). Daarom pleiten wij voor gerichte overheidsondersteuning in de vorm van tools, sjablonen en handreikingen voor o.a. risicoanalyses en de te nemen cybersecurity maatregelen.

4. Verduidelijking complexe bedrijfsmodellen

VNCI pleit samen met VNO-NCW/MKB Nederland al langere tijd voor duidelijkheid over de reikwijdte van de Cbw relatie tot bedrijven met complexe bedrijfsmodellen. Denk bijvoorbeeld aan (internationale) holdings met verschillende juridische entiteiten. Aangegeven is dat er vanuit het ministerie van Justitie en Veiligheid wordt gewerkt aan een schriftelijke uitwerking van complexe bedrijfsmodellen in relatie tot de Cbw; deze is nog altijd niet beschikbaar. Hierdoor is het voor een behoorlijk aantal bedrijven nog altijd niet helder in hoeverre zij onder de Cbw vallen en of zij zich moeten voorbereiden op de wettelijke eisen uit de Cbw. Via deze weg doen wij nogmaals de oproep om zo spoedig mogelijk met de schriftelijke uitwerking te komen.

5. Geef voldoende tijd voor implementatie en voorkom dubbele toezichtslasten

Door de overheid is aangegeven dat de Cbw en bijbehorende Cbb waarschijnlijk in het najaar 2025 van kracht zullen worden. Aangezien de Cbw niet voorziet in een overgangsregeling, zal dit betekenen dat bedrijven vanaf dat moment ook ‘compliant’ zullen moeten zijn. Echter, na vaststelling van de Cbw en de bijbehorende Cbb krijgen de bedrijven pas echt inzicht in de exacte eisen die aan hen gesteld worden. Daardoor hebben bedrijven zeer weinig tijd voor de uitvoering van de wettelijke verplichtingen. Met name voor bedrijven binnen de nieuwe sectoren van de NIS2-richtlijn, zoals de chemische industrie, zal dit behoorlijk veel capaciteit, tijd en inspanning vergen. Daarom stellen we voor om op basis van artikel 93 Cbw en artikel 36 Cbb, tot een gefaseerde inwerkingtreding te komen met name voor de zorgplicht.
Zo’n gefaseerde inwerkingtreding sluit ook aan op de wettelijk implementatietermijnen van de risicoanalyse (binnen 9 maanden) en zorgplicht (binnen 10 maanden) op basis van de Wet weerbaarheid kritieke entiteiten (Wwke)[5].
Bij de invulling van het toezicht op de Cbw en het Cbb pleiten wij daarom ook voor een overgangsperiode van 10 maanden voor met name de uit te voeren zorgplicht (inclusief de uit te voeren risicoanalyse).

[5] Zie artikel 14 lid 3 en artikel 15 lid 5 Wwke.

Daarnaast zou het toezicht voor alle bedrijven onder de Cbw in eerste instantie vooral gericht moeten zijn op het versterken van het lerend vermogen van het bedrijf en niet op repressief toezicht. Deze lerende vorm van toezicht kan ook wel worden omschreven als 'compliance assistance', waarbij het toezicht plaatsvindt op basis van vertrouwen. Verder moet het toezicht gericht zijn op een risicogebaseerde benadering met focus op systemen die van belang zijn voor een veilige bedrijfscontinuiteit. Hierbij dringen we aan op transparante toetsingskaders voor de toezichthouders.

Zoals eerder opgemerkt in onze consultatiereactie met betrekking tot de Cbw[6] worden sommige chemiebedrijven zowel als een essentiële als een belangrijke entiteit gekwalificeerd (een zogenaamde 'meervoudige kwalificatie'), omdat zij actief zijn in verschillende sectoren. Naar aanleiding van deze consultatiereactie is in de aangepaste MvT van de Cbw opgenomen dat een entiteit, die valt onder verschillende NIS2-sectoren in dat geval 'enkelvoudig' gekwalificeerd wordt, waarbij het 'zwaarste regiem' geldt (uitsluitend 'essentieel').
We pleiten ervoor dat bij dergelijke entiteiten, die onder verschillende sectoren vallen, ook één toezichthouder voor de Cbw wordt aangewezen en zal optreden.

Verder heeft de chemische industrie (net als andere bedrijfssectoren) te maken met meerdere toezichthouders vanwege toezicht op andere (sectorale) wetgeving. Om versnippering en stapeling van toezicht te voorkomen, pleiten we voor een transparante en op elkaar afgestemde aanpak in het toezicht om de toezichtslasten voor álle betrokken partijen zoveel mogelijk te beperken.
Daarom zijn we in beginsel positief over het feit dat een samenwerkingsprotocol[7] zal worden opgesteld, waarin toezichthouders onderling afspraken zullen neerleggen over gemeenschappelijke aangelegenheden over toezicht op de Cbw.
We dringen er nogmaals op aan dat in dit protocol ook de afstemming met het toezicht op andere relevante (sectorale) wetgeving wordt opgenomen, zoals de Wet weerbaarheid kritieke entiteiten (Wkke) en de Seveso-regelgeving.

Bedrijven binnen de chemische industrie werken veelal op basis van een "all hazards-benadering" waarbij fysieke en digitale beveiliging en weerbaarheid integraal worden bezien en beoordeeld. Om dubbele lasten aan de zijde van zowel bedrijven als de overheid te voorkomen, is het van belang de samenloop tussen de Cbw en andere wetgeving met een risicomanagement-benadering zoals de Wwke en Seveso wetgeving goed te regelen.

[6] Zie VNCI reactie met kenmerk B-24-056 d.d. 28 juni 2024.
[7] Zie toelichting samenwerkingsprotocol in de MvT van de Cbw (pagina 34)

Belangrijk daarbij is een duidelijk afbakening in taken en verantwoordelijkheden van de toezichthouders. De VNCI pleit ervoor dit uit te werken in het hiervoor genoemde samenwerkingsprotocol.

Artikelsgewijze opmerkingen

Hoofdstuk 4, artikel 6 t/m artikel 18 (zorgplicht)
Conform de zorgplicht genoemd in artikel 21 van de Cbw pleit de VNCI ervoor dat de uitvoering van de zorgplicht is gebaseerd op een coherente risicogebaseerde management aanpak, zoals toegelicht in de MvT van de Cbw[8].
De huidige uitwerking van de zorgplicht in de artikelen 6 t/m 18 van het concept besluit heeft via middelvoorschriften plaatsgevonden, waarbij volgens de mening van de VNCI er **geen** sprake is van een samenhangende risicomanagementaanpak.
Op grond van deze artikelen wordt van de entiteiten gevraagd allerlei soorten beleidsplannen te ontwikkelen op het gebied van 'risicomanagement, crisisbeheersingsplan, bedrijfscontinuiteit- en noodvoorzieningenplan, incidentbehandeling, toegangsbeleid' etc. De samenhang tussen deze (beleids)plannen is niet helder, er is weinig ruimte voor maatwerk en beleid en uitvoering lopen door elkaar (bijvoorbeeld risicomanagementbeleid leidt niet tot maatregelen, maar een risicoanalyse leidt wel tot maatregelen, zie huidige formulering artikel 7 Cbb).
We dringen er op aan om de huidige opzet van de zorgplicht te herzien en doelvoorschriften voor deze zorgplicht op te nemen, die gebaseerd zijn op een integrale risicomanagement-aanpak conform de zogenaamde Plan-Do-Check-Act cyclus, zoals genoemd in de Nota van Toelichting van de Cbb (pagina 8).
Dit leidt er toe dat de entiteit haar verantwoordelijkheid (discretionaire ruimte) kan nemen om maatregelen te treffen die passen bij de risico's, aard en omvang van het bedrijf. Deze risicogebaseerde aanpak leidt tot een aantoonbaar en samenhangend pakket van bijpassende, evenredige en proportionele (fysieke, organisatorisch en technische) maatregelen, gebaseerd op de tien maatregelen genoemd in artikel 21, derde lid van de Cbw. Zoals eerder opgemerkt, kan de wetgever gebruik maken van voorbeelden van een bestaande risicogebaseerde aanpak bij de beheersing van veiligheidsrisico's, zoals opgenomen in de Seveso-wetgeving.

Artikel 6 (beleid over beveiliging van netwerk- en informatiesystemen)
In artikel 6 ontbreekt de belangrijke notie dat het beveiligingsniveau van de netwerk- en informatiesystemen dient te zijn afgestemd op de risico's die zich voordoen. Verzoek is om deze risicogerichte benadering toe te voegen, zodat duidelijk is dat het cyberbeveiligingsbeleid 'risicogebaseerd' moet zijn.

[8] Zie toelichting MvT van de Cbw (pagina 18), waarin risicomanagement of een risicobeoordelingscyclus door de entiteit de basis vormt voor de zorgplicht.

In artikel 6 lid 2 is bepaald dat door de betrokken entiteit moet zorgen voor een scheiding van conflicterende bevoegdheden, verantwoordelijkheden en rollen in relatie tot de beveiliging van de netwerk en informatiesystemen. Deze functiescheiding voor conflicterende belangen etc. is veelal niet haalbaar binnen MKB-bedrijven. Daarom verzoeken we dat een eventuele functiescheiding afhankelijk moet zijn van aanwezige cyberrisico's, aard en omvang van de entiteit. We stellen voor artikel 6 lid 2 aan te passen en nader toe te lichten in de Nota van Toelichting van de Cbb.

Artikel 7 (beleid over risicomanagement)
In artikel 7 lid 1 is opgenomen dat de entiteit een vastgesteld beleid heeft over risicomanagement voor de beveiliging van haar netwerk- en informatiesystemen. Daarnaast is in artikel 6 lid 4 opgenomen dat de entiteit een managementsystematiek voor de beveiliging van haar netwerk- en informatiesystemen moet hanteren.
Onze vraag is wat exact het verschil is tussen een 'managementsystematiek' (artikel 6 lid 4) en 'risico-managementbeleid' (artikel 7 lid 1). Mocht er sprake zijn van overlap, dan moet dit worden voorkomen en moeten de betrokken voorschriften daarop worden aangepast.

Artikel 8 (incidentbehandeling)
In artikel 8 lid 2 wordt de entiteit opgedragen om activiteiten in haar netwerk- en informatiesystemen te monitoren.

Volgens artikel 8 lid 2 gelden deze monitorings- en registratieverplichtingen niet alleen voor incidenten, maar ook voor 'bijna-incidenten', 'cyberdreigingen' en 'kwetsbaarheden'.
Ook hier pleiten we ervoor dat de monitoring en registratie passend moeten zijn bij de risico's, aard en omvang van de desbetreffende entiteit en dat onnodige administratieve lasten voorkomen moeten worden. Los daarvan is onduidelijk wanneer precies sprake is van bijna-incidenten. Dit begrip is niet nader gedefinieerd. Verzoek is om dit nader toe te lichten.

In artikel 8 lid 4 is voorts bepaald dat de entiteit de, voor de beveiliging van haar netwerk- en informatiesystemen relevante activiteiten, handelingen en gebeurtenissen moet loggen.
Volgens de VNCI is er mogelijk sprake van overlap tussen de verplichtingen uit artikel 8 lid 2 (monitoren) en artikel 8 lid 4 (loggen). Om stapeling van eisen te voorkomen, vragen we het verschil tussen monitoren en loggen te verhelderen en de betrokken bepalingen op dit punt aan te passen.

Artikel 9 (bedrijfscontinuiteit en crisisbeheer)
In dit artikel ontbreekt de risicogerichte benadering. Verzoek is om toe te voegen dat deze bepaling gericht moet zijn op die netwerk- en informatiesystemen van de entiteit die randvoorwaardelijk respectievelijk kritisch zijn voor hun bedrijfscontinuiteit.

Verder wordt in dit artikel gesproken over een bedrijfscontinuiteit - en noodvoorzieningenplan en een crisisbeheersingsplan. Ook hier is opnieuw sprake van mogelijke overlap respectievelijk onduidelijkheid over de exacte scope van de verschillende plannen. Zo worden bijvoorbeeld in het kader van de bedrijfscontinuiteit in voorkomende gevallen noodvoorzieningen getroffen en een crisismanagementteam geactiveerd. De vraag is of hiervoor drie aparte plannen opgesteld moeten worden. Door het opnemen van een doelbepaling kan het bedrijf zelf de verschillende aspecten over het borgen van bedrijfscontinuiteit nader (vormvrij) uitwerken en aangeven welke processen (waaronder noodvoorzieningen en crisisbeheersing) eventueel geactiveerd worden wanneer zich een ernstige verstoring, calamiteit of incident voordoet. Hiermee wordt tevens stapeling van eisen voorkomen.

Artikel 9 lid 2 vereist om procedures vast te stellen voor o.a. het terugzetten van back-ups. De VNCI merkt op dat in sommige gevallen het niet mogelijk is om back-ups terug te zetten zonder dataverlies. Bijvoorbeeld bij realtime OT (operational IT) systemen. Bij deze systemen wordt een dataverlies geaccepteerd als een back-up moet worden teruggezet, waarbij worden getest of back-ups betrouwbaar en bruikbaar zijn. Daarom stellen we voor om het woord "terugzetten" te vervangen door ‘bruikbaar zijn’. Alternatief kan zijn om dit aspect toe te lichten in de Nota van Toelichting van de Cbb.

In artikel 9 lid 3 is niet duidelijk beschreven hoe er gecommuniceerd dient te worden tussen de entiteit, het CSIRT en de bevoegde autoriteit, in welke vorm en op welke momenten. We vragen om dit bijvoorbeeld in de Nota van Toelichting van de Cbb te verhelderen.
Voorts wordt in artikel 9 lid 3 de term ‘crisis’ geïntroduceerd. In de NIS2-richtlijn wordt niet over crisis gesproken. Om nationale koppen te voorkomen dringt de VNCI er op aan deze term weg te laten.

Artikel 10 (beveiliging van de toeleveringsketen)
VNCI stelt voor om in artikel 10 lid 2 expliciet de risicogebaseerde benadering op te nemen daar waar het gaat om het stellen van cyberbeveiligingseisen aan rechtstreekse leveranciers en dienstverleners.
Vele MKB bedrijven en grote bedrijven hebben namelijk te maken met een omvangrijke groep van rechtstreekse toeleveranciers. Indien bedrijven met alle rechtstreekse toeleveranciers (schriftelijke) afspraken dienen te maken, zal dit tot enorme administratieve lasten leiden. Daarom is het voorstel om deze verplichting te beperken tot de meest kritische toeleveranciers, die op basis van een risicoanalyse door het bedrijf worden geïdentificeerd. Hoewel deze

‘risicobenadering’ min of meer in de Nota van Toelichting op artikel 10 is beschreven, is deze niet *expliciet* opgenomen in artikel 10. Daarom dringen we er op aan deze risicogebaseerde aanpak expliciet toe te voegen aan artikel 10, zodat de beveiliging van de toeleveringsketen zich richt op die rechtstreekse leveranciers die bepalend zijn voor het cyberbeveiligingsniveau dat passend is gezien de geïnventariseerde risico’s.

Artikel 12 (basispraktijken cyberhygiëne en opleiding cyberbeveiliging)
Wij pleiten ervoor om in artikel 12 lid 2 de term ‘opleiding’ te vervangen door ‘cursus’ of ‘training’. Een opleiding is van lange duur en impliceert dat een erkend diploma behaald dient te worden, terwijl – kijkende naar de Nota van Toelichting – het hier eerder lijkt te gaan om het actueel houden van kennis of kunde en/of het bijleren ervan. De termen ‘cursus’ of ‘training’ die kortdurend maar wel frequent zijn, sluiten hier beter bij aan. Ook is dit in lijn met de inhoud van de NIS2-richtlijn.

Artikel 13 (beleid over het gebruik van cryptografie)
In Artikel 13 lid 2 wordt voorgeschreven dat in het genoemde beleid over het gebruik van cryptografie o.a. moet worden uitgewerkt welke typen encryptie worden gebruikt. Hiermee wordt onterecht de indruk gewekt dat het gebruik van encryptie een plicht is. Dit strookt niet met de tekst in de NIS2-richtlijn en het wetsvoorstel Cbw waar encryptie wordt genoemd als ‘in voorkomend geval’. Voorstel is om in artikel 13 lid 2, sub b een vergelijkbare bijzin toe te voegen.

Artikel 17 (attenderingen, adviezen en informatie)
Naar het oordeel van de VNCI is de reikwijdte van artikel 17 te breed en leidt dit artikel bovendien tot onnodige administratieve lasten. We stellen daarom voor dit artikel op twee punten in te perken:

- Criteria toevoegen aan 'relevante kwetsbaarheden en cyberdreigingen', bijvoorbeeld door deze te beperken tot zogenaamde ‘high-high alerts’ van het Nationaal Cyber Security Centrum (NCSC).
- Relevante partijen beperken tot overheidspartijen zoals CSIRT's, bevoegde autoriteiten en andere betrokken overheidsinstanties.

Verder benadrukken we dat gerubriceerde informatie van inlichtingen- en veiligheidsdiensten vaak niet mag worden vastgelegd en dat het ondoenlijk is om voor alle meldingen een schriftelijke beoordeling vast te leggen. Daarom stellen we voor om ‘het schriftelijk vastleggen’ te beperken tot meldingen vanuit overheidspartijen.

Hoofdstuk 5. Training (artikelen 20 -23)

In artikel 20 van de NIS2-richtlijn is opgenomen dat leden van bestuursorganen een opleiding moeten volgen. Daardoor verwerven zij voldoende kennis en vaardigheden 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. Dit artikel uit de NIS2-richtlijn is in de Cbw én het Cbb niet correct overgenomen. In de Cbw en Cbb wordt namelijk ten onrechte gesproken over risicobeheersmaatregelen in plaats van *risicobeheerspraktijken*. Dit zijn twee verschillende zaken. Waar het bij *risicobeheerspraktijken* gaat over de algemene strategie en aanpak, gaat het bij *risicobeheersmaatregelen* om concrete acties die worden getroffen om geïdentificeerde risico's te beperken.
Het niveau waarop de trainingseisen nu in de Cbw en het Cbb zijn geformuleerd, is derhalve niet correct en sluit niet aan bij wat van een bestuurder mag worden verwacht.
Op basis van de huidige formulering is er sprake van een aanvullende eis ten opzichte van de NIS2-richtlijn.
VNCI vraagt daarom de Cbw (artikel 24, lid 2 sub b) en het voorliggend Cbb (artikel 20 én artikel 21 lid 2) hierop aan te passen.

De VNCI is voorts verbaasd over de aanvullende eisen die betrekking hebben op de opleiding van bestuursleden ten opzichte van de NIS2-richtlijn.
Hoewel de VNCI het belang van goede scholing voor bestuurders op het gebied van cyber-security erkent, maakt zij bezwaar tegen de aanvullende eis dat deze scholing door een onafhankelijke trainer moet worden gegeven met bijbehorende eisen aan deze trainer (artikel 22) en het certificaat van de training (artikel 23). Deze eisen zijn niet opgenomen in de NIS2-richtlijn. Bovendien leiden deze eisen tot hoge kosten en mogelijke wildgroei aan opleidingsprogramma's. Met deze aanvullende eisen wijkt Nederland af van andere EU-landen, wat leidt tot een ongelijk speelveld en onnodige administratieve lasten voor bedrijven.

De VNCI stelt voor om de aanvullende eisen te schrappen en bedrijven zelf de invulling van de scholing te laten bepalen, eventueel met een vrijblijvende handreiking vanuit de overheid.
Zo is het gebruik van interne trainers op dit moment een beproefde aanpak. Deze interne medewerkers hebben veel kennis van de eigen systemen. Inzet van externe trainers leidt tot onnodige extra financiële lasten. Bovendien is de uitwerking van de benodigde kennis en vaardigheden maatwerk op bedrijfsniveau.

Reactie Nota van Toelichting Cbb

Drempelwaarden meldplicht
De drempelwaarden voor de meldplicht voor significante incidenten worden op sectoraal niveau door de vakministers bij MR vastgesteld. VNCI ondersteunt de in de Nota van toelichting van de Cbb (pagina 16) opgenomen toezegging dat de sectoren worden betrokken bij het opstellen van deze drempelwaarden. Sectoren hebben immers de kennis en expertise die nodig zijn om te komen tot proportionele en bovenal zinvolle drempelwaarden.
Hierop vooruitlopend pleiten wij ervoor om bij het opstellen van drempelwaarden de focus te leggen op bewaking van de veilige bedrijfscontinuiteit van de entiteiten.
Voor bedrijven die onder meerdere sectoren vallen, zoals het geval is voor verschillende bedrijven binnen de chemiesector, is het van belang dat de drempelwaarden door de betrokken vakdepartementen op elkaar worden afgestemd. Uiteraard weer in samenspraak met de betrokken bedrijven en sectoren. Een 'simpele stapeling' van drempelwaarden leidt tot onduidelijkheid, misverstanden en verhoging van de toezichtslasten.

Gevolgen
In tabel 1 (eenmalige regeldrukkosten) van de Nota van Toelichting wordt een uurtarief gebruikt van € 54,00. Dit is niet in lijn met de uurtarieven die bedrijven op dit moment betalen voor specialisten op het gebied van cybersecurity. Dit tarief moet worden gevalideerd (inclusief een bronvermelding) waar dit bedrag vandaan komt.

Reactie Ministeriele Regeling (MR)
In de MR worden aanvullende eisen over de zorgplicht voorgesteld.
Dit is niet in lijn met de NIS2-richtlijn en de Cbw. In de MvT van de Cbw[9] is namelijk opgenomen dat de NIS2-richtlijn verschillen over de uitvoering van de verplichtingen op nationaal niveau wil voorkomen. Dergelijke verschillen zijn ten tijde van de NIS1-richtlijn geconstateerd en zijn onwenselijk, omdat zij nadelige effecten kunnen hebben op de werking van de interne markt. Ook kan dit leiden tot verschil in kwetsbaarheden tussen sectoren en lidstaten. Gelet daarop is het opvallend dat de voorgestelde eisen in de MR volgens artikel 2 van de MR niet zullen gaan gelden voor overheidspartijen.

Bovendien is in de MvT van de Cbw[10] opgenomen dat er op dit moment geen aanleiding is om te kiezen voor zwaardere eisen dan de minimumeisen van de NIS-2 richtlijn.
Op basis van het voorgaande pleiten we ervoor geen ministeriële regeling van kracht te laten gaan met aanvullende en gedetailleerde eisen over de zorgplicht.

[9] Zie paragraaf 2.1 MvT van de Cbw.
[10] zie paragraaf 9.3 MvT van de Cbw.

Overig

Graag verzoeken wij om de hiervoor ingebrachte punten mee te nemen in de verdere uitwerking en het definitief maken van het voorliggende concept Cbb. Ook stellen we voor de voorhangprocedure toe te passen voor deze concept AMvB.
Daarnaast vragen we de uitwerking van de zorgplicht in de MR te heroverwegen.

Desgewenst zijn wij graag bereid bovengenoemde punten nader toe te lichten.

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