Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Briefnummer
25-123275

Onderwerp
Reactie ministeriële regeling onder Cyberbeveiligingswet

Den Haag
21 maart 2025

Telefoonnummer
+31620319264

E-Mail
gielens@vnoncw-mkb.nl

Geachte heer, mevrouw,

Met veel belangstelling hebben VNO-NCW en MKB-Nederland kennisgenomen van de concept ministeriele regeling (MR) ter uitwerking van de zorgplicht uit het concept Cyberbeveiligingsbesluit (Cbb) voor de sectoren energie, digitale infrastructuur, ruimtevaart, post, vervaardiging, vervoer, drinkwater, afvalwater, afvalstoffenbeheer, chemie en levensmiddelen. In het concept Cbb worden regels uit het voorstel voor de Cyberbeveiligingswet uitgewerkt. De Cyberbeveiligingswet strekt op haar beurt tot implementatie van de Europese *Network and Information Security Directive* (NIS2-richtlijn). Wij maken graag gebruik van de mogelijkheid op de consultatie van de MR te reageren.

VNO-NCW en MKB-Nederland staan in beginsel positief tegenover de doelen uit de NIS2-richtlijn, namelijk versterking van de digitale en economische weerbaarheid van Europese lidstaten. Vooral in een tijd waarin de digitale dreiging onverminderd groot is, is dit van groot belang.

In voorliggende MR lezen wij nadere en gedetailleerde eisen aan het beleid, procedures en planvorming zoals worden voorgeschreven in het concept Cbb. Ook bevat de MR herhalingen ten opzichte van de Cbb, en wordt uitgegaan van onjuiste veronderstellingen over de manier waarop bedrijven zijn/mogen worden ingericht. Deze stapeling van regels op regels, maar ook herhalingen en onjuiste veronderstellingen vergroot de reeds geconstateerde disbalans tussen compliancy en praktische werkbaarheid en uitvoerbaarheid (zie onze reactie op de consultatie van het concept Cbb).

VNO-NCW en MKB-Nederland doen via deze weg de dringende oproep aan de betrokken vakdepartementen om de uitwerking van de zorgplicht in voorliggende concept MR te heroverwegen. De Cbb bevat reeds vele nadere regels en uitwerkingen. Voorliggende vraag is of er in dat opzicht überhaupt een MR noodzakelijk is.

Daarnaast zou in de MR ook de drempelwaarden voor significante incidenten voor de meldplicht worden opgenomen. Echter, wij vragen ons af of de sectorale drempelwaarden in een openbare MR thuis horen. De drempelwaarden houden - als het goed is - verband met de continuïteit van het essentiële / belangrijke proces en kunnen daarmee gevoelige informatie bevatten. Wij willen graag ter overweging meegeven om de uitgewerkte sectorale drempelwaarden als vertrouwelijk te behandelen en niet in een MR op te nemen.

In de bijlage worden bovenstaande zorgpunten nader belicht, gevolgd door een artikelsgewijze reactie.

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.

Met vriendelijke groet,

Erik te Brake
Manager Fysieke omgeving en markten

Bijlage met reactie van VNO-NCW en MKB-Nederland op de concept ministeriële regeling (MR) onder het Cyberbeveiligingsbesluit (Cbb)

Algemene opmerkingen / aandachtspunten

1. **Heroverweeg het opstellen van ministeriële regelingen voor uitwerking van de zorgplicht, en wanneer dit toch als noodzakelijk wordt gezien, beperk de inhoud tot enkel en alleen verduidelijking van eisen uit de Cyberbeveiligingswet (Cbw) zonder nadere en/of zwaardere eisen te stellen**
   Het concept Cbb schrijft een veelvoud van beleid, procedures en planvorming voor, gevolgd door een uiteenzetting van wat die moet omvatten. In voorliggend concept MR worden vervolgens (nog eens) nadere en gedetailleerde eisen gesteld aan wat het beleid, procedures en planvorming moet omvatten. Deze stapeling van regels op regels vergroot de reeds geconstateerde disbalans tussen compliancy en praktische werkbaarheid en uitvoerbaarheid.
   Deze werkwijze is ook om meerdere redenen niet in lijn met de *Network and Information Security Directive* (NIS2-richtlijn). In de NIS2-richtlijn staat de risico gebaseerde benadering centraal, waarbij het aan bedrijven/organisaties zélf is om passende en evenredige maatregelen te treffen om de geïdentificeerde risico's voor de beveiliging van de netwerk- en informatiesystemen te beheren.
   Daarnaast is één van de doelen achter de NIS2-richtlijn om de bij de NIS1-richtlijn geconstateerde verschillen t.a.v. de uitvoering van de verplichtingen op nationaal niveau - zoals het soort cyberbeveiligingseisen en de mate van gedetailleerdheid - weg te nemen. Deze verschillen kunnen nl. nadelige effecten hebben op de werking van de interne markt en kunnen sommige lidstaten meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele EU. Daarom is de NIS1-richtlijn ingetrokken en vervangen door de NIS2-richtlijn die voorziet in doeltreffende voorzieningen t.a.v. de cyberbeveiligingseisen waar bedrijven/organisaties aan moeten voldoen. Wanneer individuele lidstaten via lagere regelgeving alsnog op nationaal niveau nadere en gedetailleerde eisen gaan stellen, wordt volledig voorbij gegaan aan het beoogde doel van de NIS2-richtlijn.
   Tot slot is de werkwijze ook niet in lijn met de inhoud van de memorie van toelichting bij het voorstel voor de Cyberbeveiligingswet (Cbw). Hierin staat - in reactie op vragen vanuit het Adviescollege toetsing regeldruk - aangegeven dat de overheid op dit moment géén aanleiding ziet om te kiezen voor zwaardere eisen dan de minimumeisen van de NIS2-richtlijn. Kijkend naar de opzet en inhoud van voorliggend concept MR (als ook concept Cbb), constateren VNO-NCW en MKB-Nederland dat er via lagere regelgeving wél degelijk nadere en zwaardere eisen worden gesteld.
   VNO-NCW en MKB-Nederland doen via deze weg de dringende oproep om de uitwerking van de zorgplicht in voorliggende concept MR te heroverwegen. De Cbb bevat reeds vele nadere regels en uitwerkingen. Voorliggende vraag is of er in dat opzicht überhaupt een MR noodzakelijk is. Indien dit tóch als noodzakelijk wordt geacht, moet het gaan om verduidelijking van de eisen uit de Cbw en Cbb, en niet om aanvullende dan wel zwaardere regels of eisen.

2. **Behandel de sectorale drempelwaarden voor de meldplicht als vertrouwelijk (en neem ze niet op in een openbare MR)**
   In de inleiding op de MR staat aangegeven dat ieder van de betrokken ministers op basis van voorliggend concept MR, een eigen MR zal vaststellen. Hierin zal naast de zorgplicht,

ook andere aspecten opgenomen worden, zoals de drempelwaarden voor significante incidenten waarvoor de meldplicht geldt.
VNO-NCW en MKB-Nederland vragen zich af of dergelijke uitgewerkte sectorale drempelwaarden in een openbare MR moeten worden opgenomen. De drempelwaarden houden - als het goed is - verband met de continuïteit van het essentiële / belangrijke proces en kunnen daarmee gevoelige informatie bevatten. Wij willen graag ter overweging meegeven om de uitgewerkte sectorale drempelwaarden als vertrouwelijk te behandelen en niet in een openbare MR op te nemen.

Artikelsgewijze opmerkingen

3. **Artikel 3 (Beleid over beveiliging van netwerk- en informatiesystemen - artikel 6 Cbb)**
- Lid 2 sub b vraagt om een beschrijving van de passende en evenredige financiële middelen die noodzakelijk zijn voor de uitvoering van de doelstellingen t.a.v. beveiliging van netwerk- en informatiesystemen.
  VNO-NCW en MKB-Nederland vragen zich af met welk doel entiteiten dit moeten doen. Dient de beschrijving van financiële middelen te worden goedgekeurd door de sectorale toezichthouder, of is het enkel en alleen ter informatie? Graag verduidelijking op dit punt waarbij scherp wordt bekeken naar de rolverdeling tussen toezichthouders en bv. aandeelhouders (die in de regel over de begroting en investeringen gaan). Voorkomen moet worden dat via voorliggend Cbb de verantwoordelijkheidsverdeling van toezichthouders en aandeelhouders wordt gewijzigd en/of daarover onduidelijkheid gaat ontstaan.
- Lid 3 sub d is onduidelijk geformuleerd. Wat wordt bedoeld met de eis dat het beleid ‘de voorwaarden voor het analyseren en evalueren van de resultaten van de monitoring en meting’. Wat wordt in deze bedoeld met ‘de voorwaarden’. Graag verduidelijking op dit punt.

4. **Artikel 4 (Beleid over risicomanagement - artikel 7 Cbb)**
   De doelstelling van de gedetailleerde eisen in artikel 4 zijn niet duidelijk. Daarnaast maken veel bedrijven gebruik van standaard Governance, Risk en Compliance (GRC) systemen die het risicomanagement proces ondersteunen. De eisen die de MR stelt aan risicomanagement zijn zo gedetailleerd, dat het gebruik van dergelijke systemen in detail niet zou voldoen aan de regeling. Artikel 7 van het Cbb stelt al algemene eisen aan risicomanagement. VNO-NCW en MKB-Nederland pleiten ervoor om het daarbij te laten, dan wel de doelstellingen duidelijker te formuleren zonder de gedetailleerde eisen.

5. **Artikel 7 (Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen - artikel 11 Cbb)**
   In lid 1 sub c ontbreekt de risico gebaseerde benadering. Verzoek is om dit expliciet toe te voegen:
   1.c de vereisten voor het bewijs door leveranciers van ICT-diensten of ICT-producten dat deze voldoen aan de vermelde beveiligingseisen, bedoeld in artikel 10, tweede lid, van het Cyberbeveiligingsbesluit, alsmede documentatie van de resultaten van de ***risicogebaseerde*** *validering.*

6. **Artikel 8 ((Beveiligingsaspecten ten aanzien van personeel - artikel 14 Cbb)**
   Lid 2 vraagt om een procedure die waarborgt dat personeelsleden handelen in overeenstemming met taken, verantwoordelijkheden, etc. Een procedure kan dit niet waarborgen. Gedrag wordt gestuurd door interne gedragscodes, programma’s die gewenst gedrag communiceren en toezicht op de naleving van de gedragscode. Verzoek is om lid 2 hierop aan te passen.

7. **Artikel 9 (Beveiligingsaspecten ten aanzien van toegangsbeleid - artikel 15 Cbb)**
   In de Cyberbeveiligingswet (Cbw) is opgenomen dat entiteiten in het kader van de zorgplicht passende technische en organisatorische maatregelen moeten nemen. Bij de invulling van ‘passende maatregelen’ dient rekening te worden gehouden met de stand van de techniek.
   Gezien de huidige stand van de techniek kan in de MR niet worden opgenomen dat de speciale toegangsrechten per gebeurtenis aan gebruikers worden toegekend. Het is nl. (nog niet) gebruikelijk dat dat het toewijzen en het gebruik van speciale toegangsrechten voor de logische en fysieke toegang tot netwerk- en informatiesystemen per gebeurtenis aan gebruikers worden toegekend. Dat zou namelijk betekenen dat er steeds apart toegang wordt verleend per upgrade, installatie of bij (analyse van) incidenten. Deze werkwijze zorgt voor een onacceptabele vertraging in de noodzakelijke speciale toegang tot systemen bij diens verstorende incidenten. VNO-NCW en MKB-Nederland pleiten ervoor om in lid 1 de woorden ‘per gebeurtenis’ achterwege te laten.

8. **Artikel 10 (Beveiligingsaspecten ten aanzien van beheer van assets - artikel 16 Cbb)**

- In artikel 10 wordt gesproken over assets. In de Nota van toelichting wordt ingegaan op het begrip assets. Een duidelijke begripsbepaling ontbreekt echter. Er wordt aangegeven wat er niet onder wordt verstaan (personeel en financiële middelen) en ter illustratie wordt één voorbeeld van wat er wel onder valt (een licentie). VNO-NCW en MKB-Nederland vragen om een heldere omschrijving van het begrip asset met een expliciete inkadering naar netwerk- en informatiesystemen om te voorkomen dat het begrip te breed wordt geïnterpreteerd.
- De voorschriften in lid c en d zijn te verregaand. Bedrijven moeten de vrijheid hebben om te bepalen of en wat doelmatig is om vast te leggen. Voorstel is om deze nadere voorschriften achterwege te laten.

Tot slot, in de leeswijzer bij de MR staat de term ‘kritieke entiteiten’ genoemd. Dit begrip komt niet voor in de Cbw of het Cbb, wel in de Wwke. Graag verduidelijking óf de MR verband houdt met de Wwke, en zo ja, hoe.