Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Datum : 19 maart 2025
Onze ref. : 2025/WW/MS/005
Onderwerp : FME-reactie op de internetconsultatie van het Cyberbeveiligingsbesluit (houdende regels voor uitvoering van de Cyberbeveilingswet)

Geachte heer, mevrouw,

FME verwelkomt het initiatief van het Ministerie van Justitie en Veiligheid om het Cyberbeveiligingsbesluit via een internetconsultatie te publiceren, ondanks dat dit formeel niet verplicht is. Dit benadrukt de inzet van de overheid voor een transparante aanpak voor de implementatie van de Cyberbeveiligingswet en toont de bereidheid tot samenwerking met partijen, zoals FME. Deze openheid komt ook naar voren uit de organisatie van de mkb-toetsing (beschreven in de Nota van Toelichting, pagina 4), waarbij FME en een aantal van haar leden aanwezig waren.

De consultatie en het panel dragen hopelijk bij aan wetgeving die niet alleen aansluit bij de behoeften van grote bedrijven, maar ook rekening houdt met de realiteit van het midden- en kleinbedrijf (mkb). Het is positief dat er aandacht is voor een goede balans tussen veiligheid en werkbaarheid, zodat cybersecurity-verplichtingen niet leiden tot onevenredige lasten.

Belangrijke aandachtspunten

FME benadrukt het belang van een werkbaar, toekomstbestendig en proportioneel beleid dat alle ondernemingen, ongeacht grootte, in staat stelt om hun digitale weerbaarheid te versterken. Om dit te realiseren, zijn er enkele punten waar verdere verduidelijking en mogelijk aanpassing nodig zijn:

1. Praktische toepassing boven administratieve last

De nadruk in AMvB moet generiek meer liggen op de toepassing van het beleid in de praktijk en niet op de schriftelijke vastlegging. De administratieve druk stijgt door de Cbw significant, daarom moet er waar kan, worden vastgehouden aan de risico gebaseerde benadering. Voldoende vertrouwen vanuit de overheid dat deze aanpak, in combinatie met de bestuurdersaansprakelijkheid, zorgt voor de juiste resultaten, helpt voor een soepelere implementatie van de Cbw en CBB.

2. Duidelijkheid over criteria voor significante incidenten en maatregelen

De nadere invulling van de criteria voor significante incidenten (artikel 24 CBB) en maatregelen (artikel 19 CBB) om verschillen tussen sectoren te kunnen ondervangen is een goed uitgangspunt. Echter deze uitwerking moet niet te lang op zich laten wachten omdat het zorgt voor onzekerheid binnen de verschillende sectoren.

3. **Ondersteuning voor het mkb**

   Zoals in de Nota van Toelichting aangegeven, liggen de implementatiekosten voor het mkb erg hoog. FME vraagt daarom om heldere communicatie en, waar nodig, ontwikkeling van praktische handreikingen en sjablonen, zoals voor risicomanagementmethodieken, incidentresponsplannen, noodvoorzieningenplannen en procedures voor de veilige ontwikkeling van netwerk- en informatiesystemen. Het is essentieel dat benaderbaarheid van het DTC gehandhaafd blijft bij het samengaan met het NCSC.

4. **Erkenning en stimulering van keurmerken**

   Het actief omarmen van CCV-keurmerken voor pentesting en cyber awareness trainingen is essentieel om de ondernemers te helpen bij het vinden van een juiste aanbieder in het oerwoud van aanbieders die pretenderen een organisatie NIS2 compliant te kunnen maken. Daarnaast moet doorontwikkeling voor andere keurmerken gestimuleerd worden.

5. **Effectieve training voor bestuurders zonder overbodige details en onafhankelijkheidseis voor de trainer**

   Zoals aangegeven in het mkb-panel moet er 'gewaakt worden dat het middel het doel voorbijschiet'. Trainingstrajecten moeten bestuurders in staat stellen om goed onderbouwde beslissingen te nemen over de beveiliging van hun netwerk- en informatiesystemen. De onafhankelijkheidseis is geen garantie voor de kwaliteit van een training en de bestuurdersaansprakelijkheid zorgt er al voldoende voor dat bestuurders niet alleen een vinkje willen zetten maar goed geïnformeerd wil worden door een kwalitatieve trainer.

6. **Harmonisatie binnen EU voor effectieve uitvoering**

   FME benadrukt nogmaals dat harmonisatie en goede afstemming tussen de EU-lidstaten voor een succesvolle en haalbare uitvoering van de Cyberbeveiligingswet essentieel is.

7. **Specifieke uitdagingen en vereisten Operationele Technologie (OT)**

   FME adviseert om de specifieke risico's van OT explicieter te adresseren. OT-systemen, zoals industriële besturingen en SCADA-netwerken, in bijvoorbeeld de maakindustrie of energie en waterbeheer, kennen unieke beveiligingsuitdagingen, waaronder lange levenscycli, beperkte patchmogelijkheden en de risico's binnen de toeleveringsketen. Expliciete verwijzingen naar OT-beveiligingsstandaarden, zoals IEC 62443, en een sectorspecifieke invulling van de zorgplicht om te waarborgen dat de maatregelen werkbaar en effectief zijn binnen industriële en kritieke sectoren, kunnen hierbij helpen.

Met deze aandachtspunten kan de Cyberbeveiligingswet, in balans met de behoefte van het bedrijfsleven zorgen voor een toekomstbestendig weerbaar digitaal Nederland.

Zilverstraat 69
Postbus 190, 2700 AD Zoetermeer
www.fme.nl
T 079 353 11 00
E info@fme.nl
FME Serviceteam 088 400 8 400
BTW NL804575903B01
KvK 40413607
IBAN NL50ABNA0513627464
SWIFT ABNANL2A

Over FME

FME is de ondernemersorganisatie voor de technologische industrie. Onze 2.200 leden zijn technostarters, handelsbedrijven, middelgrote en kleine industrie (MKI) en grote industrie /multinationals die actief zijn in de sectoren metaal, elektronica, elektrotechniek en kunststof. Er werken bij onze leden 220.000 medewerkers. De gezamenlijke omzet van de FME leden bedraagt € 108 miljard en zij exporteren voor € 51 miljard. Daarmee realiseren de FME-leden een zesde van wat Nederland in totaal met export verdient.

Wij hopen u hiermee voldoende te hebben geïnformeerd en wensen u veel succes met de verwerking van de reacties. FME kijkt uit naar de verdere dialoog met het ministerie en andere stakeholders over de concrete invulling van het sectorale gedeelte en ondersteunt de overheid graag bij de communicatie van ondersteuningsmaterialen richting haar achterban.

Uiteraard staan wij open voor een gesprek om onze reactie toe te lichten. Hiervoor kunt u contact opnemen met Marlou Snelders via marlou.snelders@fme.nl of 06-57510737).

Met vriendelijke groet,
Vereniging FME

Willem Wensing
Directeur Externe Betrekkingen en Branches

Bijlage 1. Relevante artikelen en bepalingen bij FME-consultatiereactie Cbb

Artikel 6, lid 1. Is duidelijk wat er wordt bedoeld met 'beveiliging' in de beveiliging van haar netwerk-en informatiesystemen?

Artikel 6, lid 4. Wat wordt er bedoeld met managementsystematiek. En is dit direct relevant voor de beveiliging van de netwerk-en informatiesystemen van organisaties? En in hoeverre draagt de schriftelijke vaststelling hiervan bij aan de beveiliging.

Artikel 6, 15, 17, 19, 24, 27, 33 (verwijzingen naar entiteiten die een relatie hebben met defensieactiviteiten). In de artikelen worden verwijzingen gemaakt naar entiteiten die activiteiten uitvoeren voor onder andere defensie. Gezien de aard van de werkzaamheden is het raadzaam en in nationaal belang om deze entiteiten volledig uit te sluiten van de meldplicht.

Artikel 6 tot en met 9 FME ziet vanuit het oogpunt van het mkb veel overeenkomsten tussen de eisen van het Cyberbeveiligingsbesluit en de bestaande Arbowetgeving en de bijbehorende preventieve maatregelen die bedrijven moeten nemen. Veel van de structuren en procedures rondom risicobeoordeling kunnen op een vergelijkbare manier worden ingericht, zoals een RI&E. FME zou het waarderen als het RDI en DTC hiernaar zouden kijken.

Artikel 7 lid 1. Structureel (oftewel cyclisch), wat voor termijn? Wie bepaalt dat?

Artikel 8 lid 4. Het is onvoldoende duidelijk wie bepaalt wat de 'vooraf bepaalde periode' moet zijn en of er bepaalde vereiste aan de duur van deze periode zitten.

Artikel 8. Dit artikel stelt eisen aan incidentmanagement, maar OT-systemen kunnen niet zomaar 'gepatcht' worden zonder operationele onderbrekingen. Zijn er richtlijnen beschikbaar over hoe OT-incidenten en updates beheerst moeten worden zonder verstoringen in kritieke processen?

Artikel 9. Dit artikel zou administratief meer haalbaar kunnen worden door hier de focus te leggen op de risico gebaseerde aanpak van de te beschermen belangen.

Artikel 9, lid 2. Wordt 'Periodiek' bepaalt door de organisatie zelf? Dit is namelijk enorm veel werk voor een gemiddelde mkb'er en het is zelfs de vraag of dit haalbaar is.

Artikel 9, lid 3a&c. 'Wanneer passend' in c is verwarrend als a bepaalt dat het plan ten minste deze zaken moet bevatten.

Artikel 10, lid 1 'Aspecten van de toeleveringsketen die relevant zijn voor de beveiliging van de netwerk en informatiesystemen die de entiteit gebruikt voor haar werkzaamheden of die zij voor het verlenen van diensten gebruikt' is te breed te interpreteren en dient nader uitgewerkt te worden.

Artikel 10, lid 3 'Houdt de entiteit bij ... welke afspraken ... zij met die leveranciers en dienstverleners heeft gemaakt'. Het bijhouden van afspraken boven op de afspraken zelf lijkt ons wat dubbelop. Bovendien is het opleggen van maatwerk afspraken aan leveranciers vaak niet haalbaar omdat veel bedrijven zijn overgeleverd aan de voorwaarden van de hyperscalers.

Artikel 12, lid 2 FME verwacht dat de toezichthouder bij de invulling van 'regelmatig' rekening houdt met haalbaarheid en proportionaliteit voor de organisatie in kwestie.

Artikel 12, 14 en 15 Het is te overwegen om deze artikelen samen te voegen én mogelijk nuttig om de verdeling van rollen, verantwoordelijkheden en bevoegdheden (art 14) en het toegangsbeleid (art 15) op hoofdlijnen op te nemen onder de zaken waarvan personeel en andere binnen de entiteit werkzame personen, kennis van moeten nemen, voor zover relevant voor hun functie (art. 12).

Artikel 13 'Vastgesteld beleid' dubbelop met 'schriftelijk vast'.

Artikel 16 De uitleg in de nota van toelichting gaat verder dan wat gebruikelijk geregistreerd is in assetmanagement beheer. Het genereren en bijhouden van deze informatie levert dus veel extra werkzaamheden op.

Artikel 18 FME twijfelt of dit artikel een toevoeging is op de evaluatie vermeld onder de verschillende artikelen of dat dit artikel weggelaten, dan wel weggehaald kan worden in de artikelen.

Artikel 20 De definitie van 'lid van bestuur' dient verder uitgewerkt te worden. Valt hier bijvoorbeeld ook de Raad van Toezicht onder?

Artikel 22 De onafhankelijkheidseis zorgt voor een nieuwe markt voor trainers, maar is absoluut geen garantie voor de kwaliteit van een training. Sterker nog, iemand vanuit de organisatie zelf of die de organisatie goed kent, kan het bestuur naar alle waarschijnlijkheid beter meenemen in de bedrijfsspecifieke risico's dan een externe consultant of trainingsinstituut. Bovendien zien we dat de bestuurdersaansprakelijkheid uit artikel 24 Cbw ervoor zorgt dat men daadwerkelijk goed geïnformeerd wil zijn. Ook kan de onafhankelijkheidseis gezien worden als nationale kop. Dit is problematisch wanneer trainingen binnen sommige organisaties niet binnen de EU als geheel gegeven kunnen worden, doordat er in Nederland apart een externe trainer ingehuurd moet worden.

Artikel 24 Het is van belang dat de nadere invulling van de criteria voor significante incidenten zo snel mogelijk wordt uitgewerkt en helder worden geformuleerd. Op dit moment zorgt het voor nog veel onzekerheid binnen onze achterban. FME hoopt dan ook op flexibiliteit bij de toezichthouders, wanneer deze pas dicht tegen de implementatiedatum bekend gemaakt worden.

Zilverstraat 69
Postbus 190, 2700 AD Zoetermeer
www.fme.nl

T 079 353 11 00
E info@fme.nl
FME Serviceteam 088 400 8 400

BTW NL804575903B01
KvK 40413607

IBAN NL50ABNA0513627464
SWIFT ABNANL2A