Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

DATUM	27 JUNI 2024
ONZE REF.	2024/WW/ms/017
CONTACTPERSOON	Marlou Snelders (marlou.snelders@fme.nl, +31(0)6 57 51 07 37)
ONDERWERP	Internetconsultatie wetsvoorstel Cyberbeveiligingswet

Geachte heer, mevrouw,

Met veel belangstelling heeft FME kennisgenomen van het voorliggende wetsvoorstel voor de Cyberbeveiligingswet (Cbw) als Nederlandse implementatie van de Network and Information Security Directive (NIS) 2. FME steunt de beoogde doelen van de Europese Commissie en het Ministerie van Justitie en Veiligheid. Wij zijn dan ook positief over deze stap richting een toekomstbestendige en cyberweerbare digitale economie.

Cyberweerbaarheid is een absolute randvoorwaarde voor een sterke technologische industrie. Daarom staat FME haar leden bij in de strijd tegen cybercriminaliteit. Om de kwetsbaarheden binnen onze sectoren te verminderen, werken we aan cyberbewustzijn, preventie en het trainen van een adequate incidentrespons.

De Rijksoverheid is stelselverantwoordelijk en daarmee normsteller voor het opstellen van (wettelijke) kaders en voor de digitale veiligheid van Nederland. FME is ervan overtuigd dat de industrie daarin gebaat is bij een duidelijk en uniform proces, een integrale aanpak, wetgeving als hulpmiddel met concreet handelingsperspectief en niet als extra belastende regeldruk voor een sector met een groeiend tekort aan professionals (zie ook de onderzoeks rapportage onderwijs en arbeidsmarkt ter attentie van de kwantitatieve en kwalitatieve tekorten op de Nederlandse cybersecurity arbeidsmarkt).

Na consultatie met de FME achterban zijn het wetsvoorstel en de onderhavige verplichtingen, zoals bijvoorbeeld het treffen van adequate beveiligingsmaatregelen en het melden van incidenten door ons beoordeeld op *duiding, uitvoerbaarheid en handelingsperspectief, en beperken regeldruk*. In de bijlage 'Relevante artikelen en bepalingen' vindt u een analyse en opvallende zaken per relevant wetsartikel uit de Cbw of bepaling uit de bijbehorende Memorie van Toelichting (MoT).

Duiding

Uniforme en duidelijke bepalingen en scope van de Cbw zijn essentieel voor de achterban van FME, omdat zij zorgen voor een consistente en betrouwbare standaard. Dit vermindert de complexiteit en onzekerheid rondom naleving en helpt bedrijven om hun cyberbeveiligingsmaatregelen effectief en efficiënt te implementeren. Tegelijkertijd is een zekere mate van ruimte nodig om de technologische ontwikkelingen bij te kunnen blijven. De wetgever heeft dit getracht te doen door op meerdere plekken te verwijzen naar aanvullende algemene maatregelen van bestuur (AMvB's), die de flexibiliteit bieden om de wetgeving snel aan te passen aan nieuwe dreigingen en innovaties zonder de basisstructuur van de wet te hoeven wijzigen. FME is blij om te zien dat de wetgever hierbij rekening wil houden met de wensen van de verschillende sectoren en kijkt er naar uit om gezamenlijk met haar achterban mee te denken over de concrete invulling van deze AMvB's.

Uitvoerbaarheid en handelingsperspectief

Uitvoerbaarheid en concreet handelingsperspectief zijn voor FME vereisten om te zorgen dat niet alleen grote bedrijven, maar ook het midden- en kleinbedrijf (mkb) hun weerbaarheid tegen cyberdreigingen kunnen vergroten. Met name in de maakindustrie, die sterk afhankelijk is van toeleveranciers, is de beveiliging zo sterk als de zwakste schakel; een enkel bedrijf kan met een domino-effect de hele keten laten instorten. Door de wet, in het bijzonder de **registratieplicht, meldplicht** en **zorgplicht**, praktisch en toepasbaar te maken, wordt ook het mkb in staat gesteld om beveiligingsmaatregelen te implementeren zonder disproportionele lasten te dragen.

Het aanbieden van concrete hulpmiddelen en richtlijnen in de Cbw helpt deze bedrijven te voldoen aan de wet- en regelgeving. Het aanbieden van uniforme communicatie vanuit de rijksoverheid en één meldloket zijn hier rand voorwaardelijk aan. Dit voorkomt dat de cyberweerbaarheidskloof tussen grote en kleine bedrijven steeds groter wordt, waardoor het gehele technologische industriële ecosysteem beter beschermd wordt tegen cyberaanvallen. (Zie ook CSR-advies 'Verkleinen van de Cyberweerbaarheidskloof').

Beperken regeldruk

Het beperken van de regeldruk is van groot belang voor FME-leden, omdat te veel diversiteit in internationale standaarden en toezicht een onevenredig hoge administratieve en financiële last opleveren. Deze lasten maken het voor bedrijven, met name de kleinere ondernemingen, moeilijk om aan de eisen te voldoen zonder hun kernactiviteiten te verstoren. FME wil voorkomen dat certificering slechts als checkbox gebruikt wordt zonder dat het gesprek aan wordt gegaan in de keten.

FME is er voorstander van om het wetsvoorstel zo aan te passen dat (inter)nationale standaarden erin betrokken worden. Op deze wijze worden bedrijven op weg geholpen hun cyberbeveiliging op orde te krijgen op een manier die zowel effectief als betaalbaar is, zonder bovenmatige regeldruk. Zo heeft FME het CyRa-certificeringsmodel omarmt, dat specifiek is ontworpen om een praktische en haalbare aanpak te bieden voor cyberbeveiliging. Maar ziet ook meerwaarde in het CyberFundamentals Framework, naar Belgisch ontwerp. Met name voor partijen voor wie een internationale certificering zoals ISO 27001, genoemd in het wetsvoorstel, te vroeg komt.

Tot slot adviseert FME zo snel mogelijk over te gaan tot inwerkingtreding van de Cbw en mogelijkheden tot registratie aan te bieden om zo een gelijk speelveld en duidelijkheid te kunnen garanderen voor entiteiten actief in meerdere lidstaten.

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 € 139 miljard en zij exporteren voor € 59 miljard. Daarmee realiseren de FME-leden een zesde van wat Nederland in totaal met export verdient.

Wij hopen u hiermee voldoende te hebben geinformeerd en wensen u veel succes met de verwerking van de reacties. Uiteraard staan wij open voor een gesprek om onze reactie nader toe te lichten. Hiervoor kunt u contact opnemen met Marlou Snelders (zie boven voor contactgegevens).

Met vriendelijke groet,

Willem Wensing
Directeur Belangenbehartiging. a.i.

Bijlage 1. Relevante artikelen en bepalingen bij FME consultatiereactie Cbw

Relevante artikelen en bepalingen t.a.v. duiding

Artikel 2.a. OT-systemen vallen niet direct onder 'netwerk en informatiesystemen'. Wel staat in de Memorie van Toelichting vermeld dat ook OT (IACS) onder netwerken en informatiesystemen valt. FME wil voorstellen om dit ter verduidelijking te vermelden onder **Cbw Artikel 1. Begripsbepalingen,** waar ook artikel 6.1 daar naar toe verwijst. Het belang van duidelijke terminologie en onderscheid tussen IT en OT vanwege hun verschillende aard en beveiligingseisen wordt specifiek benadrukt in het CSR-advies 2020 inzake digitale veiligheid van IACS in de vitale infrastructuur. Het is van belang dat de wetgever zich bewust is van het gegeven dat ondernemers actief in de technologische industrie en werken met machines en installaties (OT) meer moeite zullen hebben om te voldoen aan de stand van de techniek gezien de levensduur en kosten van machines aanzienlijk verschilt van bedrijven die werken met IT in een kantooromgeving. Met name omdat uit het 2024 State of Operational Technology and Cybersecurity Report van Fortinet blijkt dat 25% van de cyberaanvallen gericht is op deze systemen.

Artikel 17.2 FME is benieuwd wat er onder de omschreven 'bijstand' valt en wat entiteiten kunnen verwachten en wanneer deze van toepassing is. Op dit moment oogt de bijstand als een algemene incident response-dienst. In het kader van verwachtingsmanagement is het van belang hier extra uitleg over te geven, ook om te voorkomen dat het CSIRT onnodig veel hulpverzoeken krijgt. Daarnaast is het onduidelijk wat er verstaan wordt onder 'op verzoek proactief scannen'.

Artikel 17.3 Wordt een entiteit op de hoogte worden gebracht wanneer er een ongevraagde scan plaats vindt?

Artikel 17.4 Kan er aan de voorkant inzicht worden gegeven in de kosten voor een dergelijke scan? FME pleit ervoor dat deze kosten bij de toezichthouder komen als blijkt dat een entiteit haar zaken op orde heeft.

Artikel 18.1 Wie is de coördinator bekendmakingen kwetsbaarheden?

Artikel 23.3 benoemt dat "de fysieke omgeving van die systemen" moet worden beschermt. Dit lijkt echter alleen te duiden op de ruimte waar deze systemen staan. In **MvT Art 3.** wordt een andere definitie gehanteerd, "een wettelijk kader voor het versterken van de digitale en fysieke weerbaarheid van onder meer de vitale infrastructuur". Hier lijkt fysieke weerbaarheid een bredere context te kennen. FME stelt voor een eenduidige definitie op te stellen in **Art. 1** in lijn met Operationele Technologie (zoals ook hierboven omschreven).

Artikel 30. Bij welke instantie moet tussentijds verslag worden uitgebracht. 'Op verzoek'- in welke situaties vindt dit plaats?

Artikel 32. Er ontbreekt een tijdsindicatie bij het informeren aan ontvangers.

Artikel 38.2 Wat kan een entiteit verstaan onder 'aanvullende technische ondersteuning'? Op dit punt is FME voorstander van doelwit- en slachtoffernotificatie en ziet hier een belangrijke rol weggelegd voor de Rijksoverheid als stelselverantwoordelijke.

Artikel 65. Kan explicieter worden gemaakt dat veiligheids-en commerciële belangen worden beschermd en de entiteit ten allen tijden op de hoogte gehouden wordt over met wie diens gegevens worden gedeeld.

Artikel 68. In welke situaties is het aanwijzen van een controlefunctionaris gerechtvaardigd?

MoT 5.3.1 *'Het is aan de toezichthouder om te beoordelen of de maatregelen die entiteiten hebben genomen om hun weerbaarheid te waarborgen voldoende zijn om de risico's te mitigeren'*.

FME is van mening dat dit te ruim omschreven is en daarmee de interpretatie volledig bij de toezichthouder laat en niet veel zekerheid geeft aan bedrijven dat ze voldoen aan de wet. Hetzelfde geldt voor **5.3.3.**; Hoe gaat de toezichthouder dit controleren? Kunnen we bedrijven meer handelingsperspectief geven? Bijvoorbeeld doordat een entiteit gebruik kan maken van relevante '(inter)nationale standaarden'.

MoT 5.5.1 Wat verstaan wordt onder de '*drempelwaarde*' van een significant incident zal d.m.v. art. 37 of de algemene maatregel van bestuur (AMvB) een andere invullingen gaan krijgen per sector. Het is wenselijk om dit waar mogelijk te blijven harmoniseren en dat dit in overleg zal gaan met de verschillende sectoren. In het conceptwetsvoorstel zijn enkele delegatiebepalingen opgenomen. Er is nog niet bekend hoe de nadere regelgeving zal worden ingevuld. Deze invulling is bepalend om vast te kunnen stellen hoe de betreffende wettelijke bepaling precies zal uitwerken. Dit maakt dat we op dit moment nog geen complete beoordeling kunnen geven. Het is dan ook zeer gewenst om voorafgaand aan het vaststellen van de lagere regelgeving (AMvB) een nieuwe consulatie uit te zetten, dan wel een voorhangprocedure uit te voeren ten aanzien van de lagere regelgeving.

Het is niet altijd duidelijk of de discretionaire ruimte die in de wetgeving wordt gegeven nader kan worden ingevuld door de toezichthouders. Het verdient aanbeveling om daar waar bedoeld is beleidsruimte te geven aan de ondernemers, dit nadrukkelijk in de toelichting te benoemen en waar mogelijk de (inter)nationale standaarden te volgen. Dit om te borgen dat de beleidsruimte niet middels het toezicht aanzienlijk wordt verkleind. Dit is van belang omdat er sprake is van een grote diversiteit onder ondernemers en hun toeleveranciers.

MoT 5.5.2…"*Het CSIRT en de toezichthoudende instantie kunnen naar aanleiding van de melding een essentiële entiteit of een belangrijke entiteit verzoeken om een tussentijds verslag over relevante updates van de situatie."*… Uit de Memorie van Toelichting blijkt niet of nauwelijks welk type incident een tussentijdse melding aan de toezichthouder legitimeert. Ook hier geldt dat de beperkte capaciteit van een ondernemer ingezet moeten worden voor het verhelpen van het incident in plaats van het maken van een tussentijdse rapportage aan de toezichthouder(s). FME wil hierbij ook het belang van goed vertrouwen, een goede verstandhouding en procedure met de toezichthouder benadrukken. Ook omdat dit het aantal vrijwillige meldingen kan bevorderen.

MoT 5.3.3 …*"beperkte financiële capaciteit of beperkte omvang kan een entiteit niet geheel ontslaan van de verplichting om de weerbaarheid op orde te hebben"*…Deze formulering roept vragen op waarbij de populatie kleinste ondernemers met een zeer beperkte financiële capaciteit die onder de werkingssfeer van de Cbw vallen onvoldoende handelingsperspectief heeft. Deze

groep zou gebaat zijn bij de formulering van een absoluut minimum zoals bijvoorbeeld de set basismaatregelen van het DTC.

…"*Wanneer essentiële entiteiten en belangrijke entiteiten overwegen welke maatregelen in dit verband passend zijn, moeten zij 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, met inbegrip van hun veilige ontwikkelingsprocedures."*…

Op dit moment is het voor relatief kleine ondernemers in de technologische industrie onmogelijk inzicht te krijgen in de specifieke kwetsbaarheden van één leverancier, laat staan meerdere (tientallen, honderden of duizenden). Een afdoende onderbouwing van de wetgever op het punt van de relatie tussen specifieke kwetsbaarheden enerzijds en algemene kwaliteit van de producten en cyberbeveiligingspraktijken anderzijds, ontbreekt. Bovendien biedt de wetgever geen ruimte om onderscheid te maken tussen leveranciers.

In de technologische industrie is het aanbrengen van onderscheid tussen leveranciers staande praktijk. Dit helpt ondernemers om beter in te spelen op marktdynamiek en risico's te beheersen. Een grondige beoordeling van de toeleverketenrisico's en het implementeren van strategieën om deze risico's te mitigeren is cruciaal.

Op dit moment ontbreekt een duidelijke stimulans of richtsnoer om transparantie te creëren ten aanzien van cyberbeveiliging. Hierdoor worden samenwerkende ondernemers belemmerd om inzicht te krijgen in de cyberweerbaarheid van upstream waardeketens in het algemeen en directe toeleveranciers in het bijzonder, laat staan bedrijfscontinuïteitsplannen te maken. Zonder bovengenoemde stimulans en/of richtsnoer is het bijzonder moeilijk om rekening te houden met specifieke kwetsbaarheden van één of meerdere leveranciers.

Relevante artikelen en bepalingen t.a.v. uitvoerbaarheid en handelingsperspectief

Artikel 17.5 Er kan prioriteit worden gegeven op basis van een risico gebaseerde benadering. Kan het CSIRT voldoende capaciteit garanderen om de daadwerkelijke vraag naar bijstand enigszins aan te kunnen gezien de veelzijdigheid aan taken en de lopende fusie tussen het DTC en NCSC.

Artikel 20.3 '*Regelmatige beoordeling, ten minste om de vijf jaar*.' FME wil er op wijzen dat vijf jaar, erg lang is voor een digitale economie die continue onderworpen is aan verandering. Tegelijkertijd ziet FME ook de meerwaarde van het bieden van een bepaalde mate van voorspelbaarheid.

Artikel 22. Nationaal register entiteiten komen uiterlijk 17 januari 2025 tot stand. FME zou graag meer informatie krijgen over hoe deze registratie verloopt en of deze uit eigen initiatief plaats moet vinden.

Artikel 23. 'Passende en evenredige maatregelen'. Laat erg veel ruimte over voor interpretatie en onduidelijkheid. FME is van mening dat o.a Incident Respons nu onvoldoende wordt toegelicht. FME raadt aan in de Cbw of een AMvB duidelijk uiteen te zetten wat er verwacht wordt van incident respons. Bijvoorbeeld, is het voldoende om een procedure in place te hebben? Is er een minimaal aantal oefeningen gewenst en moeten deze vervolgens gelogd worden?

Artikel 26.2 Ieder lid van bestuur moet over kennis en vaardigheden voldoen. Dus niet alleen training krijgen maar wordt volledig geacht hierover te beschikken. FME twijfelt of het proportioneel en doeltreffend is om van elke bestuurder te verwachten dat deze in staat is om risicobeheersmaatregelen en de gevolgen ervan te beoordelen. En dat deze kennis daarnaast ook actueel wordt gehouden(art. 26 lid 4). Betekent dit dat er periodiek een nieuwe training gevolgd moet worden? En met welke frequentie?

Het is van belang dat de training doeltreffend is en in lijn moet zijn met het type risico's waar de organisatie mee te maken krijgt. FME denkt niet dat dit daadwerkelijk af te vangen is met een certificaat van deelname van training. De praktijk laat namelijk vaak zien dat dergelijke trainingen gemaakt worden door directie ondersteunend personeel in plaats van bestuurders zelf. De ervaring vanuit de FME achterban is dat een fysieke training middag voor het bestuur nog het meest doeltreffend is.

Al met al is FME van mening dat dit artikel moeilijk uitvoerbaar is. Het is daarom af te vragen of de bestuursaansprakelijkheid op zichzelf niet al een voldoende maatregel is.

Artikel 27.2 Wanneer een incident significant is blijft zo ter beoordeling van de getroffen entiteit. Lastig te beoordelen door hen, helemaal in onze sector waar de kennis van cybersecurity vaak nog achterblijft. In hoeverre zijn entiteiten in staat dit goed te beoordelen? Wat zijn de consequenties als er geen melding gedaan wordt terwijl dit wel had gemoeten? FME adviseert de drempelwaarden daarom meer eenduidig vast te stellen, het liefst op Europees niveau. Zodat ondernemers niet aan verschillen standaarden hoeven te voldoen en er een gelijk speelveld blijft.

Artikel 45. Wanneer moet de entiteit zich registreren. Is dat zoals gemeld in **48.3?** Hoe zit dit dan met de implementatiedatum van de wet (verwachting halverwege 2025)?

Artikel 79. FME zou graag expliciet vermeld zien dat een beveiligingsscan altijd gecommuniceerd wordt met de belangrijke entiteit.

Artikel 93. FME vraagt zich af wat het uitzicht is op de inwerkingtreding. Hoe verhoudt zich de tussen periode tussen de Europese implementatie van NIS2 en het komen te vervallen van de NIS1 en de werking van de Wbni tot aan de inwerkingtreding van de Cyberbeveiligingswet? Het is wenselijk om de Cbw zo snel mogelijk inwerking te laten te treden, en waar dat kan de mogelijkheid voor vrijwillige registratie vast te openen om een gelijk speelveld te behouden voor entiteiten actief in meerdere Europese lidstaten.

MoT 5.3.1 ..."*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*."... Dit is voor veel maakbedrijven uit de technologische sector op dit moment niet het geval. Om die reden is FME blij met de introductie van de zorgplicht. De rijksoverheid (NCTV, NCSC, DTC) heeft een begin gemaakt met het verstrekken van voorlichting over het uitvoeren van een risicobeoordeling. FME constateert echter dat het maakbedrijven uit het MKB op dit moment onvoldoende handelingsperspectief oplevert. Daarnaast vraagt FME zich af of de risico beoordeling zowel IT als OT omvat, en daarmee risico's met betrekking tot persoonsveiligheid, milieu en operationele beschikbaarheid worden meegenomen in de afweging.

MoT 5.5_…". De meldplicht ziet niet op bijna-incidenten of dreigingen. Vs. *Het gaat derhalve ook om incidenten waarbij de hiervoor genoemde mogelijke aanzienlijke gevolgen zich nog niet hebben voorgedaan, maar mogelijk wel gaan plaatsvinden*."… Desbetreffende bepalingen zijn strijdig met elkaar en verdienen het om herformuleerd te worden. Incidenten waarvan de aanzienlijke gevolgen zich mogelijk voordoen zijn bijna-incidenten. Bovendien zou de beperkte capaciteit van een ondernemer ingezet moeten worden voor het verhelpen van het incident in plaats van het maken van een voorspellende beoordeling en rapportage aan de toezichthouder(s). Het kan niet de bedoeling zijn van de wetgever om het paard achter de wagen te spannen.

Relevante artikelen en bepalingen t.a.v. beperken regeldruk

Artikel 17.7. Hoe bevordert het CSIRT de invoering en het gebruik van deze gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's of taxonomieën? FME vraagt zich af hoe concreet wordt voorkomen dat er een wirwar van standaarden voor elke individuele autoriteit en sector ontstaat. FME is daarom voorstander van het concreet aanbevelen van specifieke classificatieschema's of standaarden zoals CyRa of Cyfun.

Artikel 28.1 Entiteiten moeten melden bij CSIRT én de bevoegde autoriteit. FME is ervan overtuigd dat dit móet met zo min mogelijk handelingen, het liefst bij één meldloket. Het 'streven' genoemd in **MoT 4.8/5.5.1 Dubbele meldplicht; "***Er wordt naar gestreefd deze dubbele meldplicht technisch zo in te richten dat het verspreiden van de benodigde informatie maar één handeling voor de entiteit vergt."* moet een garantie zijn.

Artikel 68.3, 70.4 en 80.4 Kosten van aanstellen van controlefunctionaris en gerichte beveiligingssaudits zouden bij toezichthouder moeten liggen, niet bij de essentiële entiteit. In elk geval vraagt dit om meer uitleg waarom de kosten bij de entiteit en niet bij de autoriteit moeten liggen.

MoT 2.1 Over NIS 1*"Zo zijn er aanzienlijke verschillen op gebied van de afbakening van het toepassingingsgebied van de richtlijn."* Met NIS2 blijven er verschillen aangezien deze uitgaat van minimum harmonisatie. FME is voorstander van het aanwijzen van(internationale standaarden of normenkaders. Zodat ondernemers die ook actief zijn in andere Europese landen, daar niet in een wirwar van extra administratieve lasten terecht komen.

MoT 5.3.6 Entiteiten zouden hun eigen normenkader kunnen hanteren. '*Hiermee wordt regeldruk beperkt*'. Voor de FME-achterban, die te maken heeft met veel verschillende soorten toeleveranciers wordt de regeldruk op deze manier eerder vergroot. Zoals hierboven reeds beschreven is FME dan ook voorstander van uniforme standaarden.