FERM
Samen staan we FERM

Reactie Stichting FERM Internconsultatie Cyberbeveiligingsbesluit

27 maart 2025

Een reactie namens de volgende zeehavens:

- Groningen Seaports
- North Sea Port
- Port of Moerdijk
- Port of Amsterdam
- Port of Rotterdam

FERM heeft tijdens de internetconsultatie van de Cyberbeveiligingswet (Cbw) reeds formele feedback ingediend. Sinds de indiening van deze feedback op 27 juni 2024, hebben zich bij Stichting FERM significante structurele veranderingen voorgedaan die een bondige toelichting vereisen:

FERM, opgericht in 2021, is een stichting die zich richt op het stimuleren van samenwerking tussen bedrijven in de Rotterdamse haven om het bewustzijn over cyberrisico's te vergroten en de digitale weerbaarheid te verhogen. Momenteel is FERM in transitie naar een nationaal opererend platform dat zich uitstrekt over de Nederlandse zeehavens die zijn aangesloten bij de Branche Organisatie Zeehavens. Dit betekent een andere aanpak van de activiteiten en een nieuwe missie en visie, waarbij de nadruk ligt op ketenweerbaarheid en veerkracht tegen cyberdreigingen. FERM faciliteert nu de cyberweerbaarheid van de Nederlandse zeehavens die vallen onder de Branche Organisatie Zeehavens (BOZ) door het uitwisselen van dreigingsinformatie, het delen van kennis en het versterken van de cruciale keten. De nieuwe organisatie wordt aangestuurd door de zeehavenbeheerders en werkt nauw samen met zeehavenbeheerders, nautische dienstverleners, publieke partners zoals het DTC en NCSC, en de overheid. Deze reactie komt in naam van zowel stichting FERM als de benoemde zeehavenbeheerders.

Aanleiding en doel

Op 20 februari 2025 is de consultatieronde het Cyberbeveiligingsbesluit (Cbb) van start gegaan, waarbij de regels van uit de Cbw verder worden uitgewerkt. De Cbw is de Nederlandse uitwerking van de Europese NIS2 richtlijn die op 22 november werd vastgesteld door het Europees Parlement en de Raad van de Europese Unie. Hierbij dient de Cbw als opvolger van de huidige NIS1 richtlijn. Vanuit FERM zien wij de uitwerking van de NIS2 als een belangrijke stap in de verbetering van de cyberveiligheid in de EU. Vanuit FERM verwelkomen we deze wet en zien bij zowel het Cbw, als het Cbb een hoge doeltreffendheid en doelmatigheid. Tegelijkertijd zijn er ook vragen over de implementatie. Deze zijn onderverdeeld in drie categorieën:

a. Suggesties en vragen om verduidelijking van de wetgeving om verschil in interpretatie te voorkomen.

b. Voorstellen van alternatieven om hetzelfde doel te bereiken maar met een verminderde regeldruk voor bedrijven.
c. Aanvullingen op de huidige versie van het Cbb om de doelstelling van de wet met een hogere doelmatigheid te kunnen bereiken

Context en uitdagingen in de Nederlandse Zeehavens

De digitale weerbaarheid en veerkracht van de Nederlandse Zeehavens heeft sinds begin dit jaar een nieuwe impuls gekregen. De uitbreiding van FERM naar een nationaal platform is illustratief voor het groeiende belang van weerbaarheid en veerkracht in de vitale sectors van heel Nederland. Tegelijkertijd zijn er voor de zeehavens in Nederland uitdagingen die zorgen voor een unieke complexiteit:

- Gebrek aan havenbrede governance
  Door gebrek aan havenbrede governance kunnen maatregelen om havenspecifieke scenario's te voorkomen of ter preventie van impact niet dwingend worden belegd. Populair gezegd: niemand is de baas in de haven. En dat terwijl de dreigingsscenario's duidelijk entiteit-overstijgend zijn.

  Vanuit FERM wordt er op dit soort scenario's getraind en geoefend om entiteiten voor te bereiden op dergelijke scenario's. Echter heeft deelname aan FERM en haar activiteiten een vrijwillig karakter voor bedrijven in de haven. Hierdoor wordt de continuïteit van dienstverlening in de havens onzeker, mede doordat financiële ondersteuning vanuit nationaal perspectief sectoraal is georganiseerd. Daarnaast heeft FERM geen mandaat om eisen op te leggen of sancties op te leggen als blijkt dat entiteiten zich niet voldoende inspannen om bepaalde maatregelen te nemen.

- Weerbaarheid tegen *spillover effects*
  De havengebieden zijn sterk digitaal en fysieke verbonden, waardoor cyberdreigingen kritieke gevolgen kunnen hebben. Deze dreigingen kunnen niet allen logistieke processen ontwrichten, maar ook de energievoorziening en industriële activiteiten verstoren, zoals het manipuleren van veiligheidssystemen voor chemische stoffen en het ontregelen van geautomatiseerde productieprocessen.

  De groeiende (geopolitieke) onrust in de wereld leidt tot een verhoogde dreiging. De cyberaanval op ATM Terminals/Maersk uit juni 2017 maakte de kwetsbaarheid van digitale oorzaken en fysieke gevolgen zichtbaar. De externe dreiging zorgt voor een mogelijk *spillover effect (*ofwel *collateral damage)* op de havens. Deze externe dreiging is voor de haven niet een 'nieuw normaal', maar classificeert FERM als een 'creeping crisis'. Met elk sanctiepakket of promotie voor de samenwerking binnen de NAVO context wordt

de dreiging groter.

- Regeldruk neemt toe voor bedrijven in de haven
  De regeldruk in de Nederlandse zeehavens is de afgelopen jaren aanzienlijk toegenomen. Enkele voorbeelden hiervan zijn de uitgebreide rapportageverplichtingen, zoals gedetailleerde emissieregistraties en veiligheidsbeoordelingen, die steeds meer tijd en middelen vereisen. Het is daarbij niet onwaarschijnlijk dat de betrokkenheid van het MKB bij deze toenemende regeldruk wederom achterblijft, mede door de beperkte capaciteit en middelen. Hierdoor bestaat het risico dat de beoogde beleidsdoelstellingen, zoals verbeterde duurzaamheid en veiligheid, hun doel missen en niet effectief worden geïmplementeerd. Gezien het aanhoudende personeelstekort is het daarom essentieel dat nieuwe regelgeving praktisch en uitvoerbaar blijft.

Feedback internetconsultatieronde

T.a.v. onze feedback op de internetconsultatie ronde van de Cbw zijn wij blij om te zien dat de volgende punten van onze feedback duidelijker zijn geworden in de Cbb:

- Het nader definiëren van de zorgplicht
- Verduidelijking van de regeldruk die onder de reikwijdte van de Cbw valt
- Erkenning dat bedrijven buiten de reikwijdte ook regeldruk zullen ondervinden

1. Suggesties om de regeldruk voor bedrijven te verminderen

1. Afhandeling verplichte meldpunten met één handeling en confidentialiteit van meldingen

In de internetconsultatie van de Cbw werd er naar gestreefd om de dubbele meldplicht technisch zodanig in te richten dat het verspreiden van de benodigde informatie maar één handeling voor de entiteit vergt (Memorie van Toelichting, paragraaf 5.5.1). Ook In de Cbb wordt hier helaas geen duidelijkheid over gegeven of dit ook daadwerkelijk word gerealiseerd. In Artikel 24 van de Nota van Toelichting, wordt gesteld dat hier rekening mee **kan** worden gehouden. Onze suggestie is dat hier **zal** van wordt gemaakt.

Tijdens de acute fase van een incident staat een getroffen organisatie onder grote druk. Daarom adviseren wij om de rollen van verschillende toezichthouders in deze fase zoveel mogelijk te stroomlijnen. Aangezien toezichthouders geen directe bijstand verlenen, kan een gecoördineerde aanpak de belasting voor een getroffen organisatie verminderen.

In de praktijk hebben bedrijven te maken met diverse meldplichten voor digitale incidenten. Zo moeten zij onder de AVG (GDPR) incidenten melden bij de Autoriteit Persoonsgegevens terwijl digitale incidenten in havens ook gemeld moeten worden bij de Rijkshavenmeester onder de ISPS-code of bij de omgevingsdienst volgens de Seveso-wetgeving wanneer er fysiek gevolgen zijn. Daarnaast vraagt de Nationale Politie om meldingen van cybercriminaliteit, en biedt de Douane een vrijwillige meldmogelijkheid in het kader van AEO-status, die ook cyberaspecten omvat. Deze uiteenlopende meldplichten gecombineerd met de complexiteit van rapportagevereisten, zorgen voor aanzienlijke regeldruk voor bedrijven. Om de regeldruk te beperken verzoeken we om voor allerlei mogelijke verplichte meldingen te combineren in één handeling voor bedrijven

2. <u>Registratieplicht: aanschrijven bedrijven die onder wetgeving vallen.</u>

De huidige voorgestelde uitvoer van de wet, voorziet in het registreren van bedrijven in een nationaal register (registratieplicht). In de Nota van Toelichting wordt een aantal genoemd van 8.100 bedrijven die onder de NIS2 reikwijdte gaat vallen. Dit suggereert dat het NCSC een goed beeld heeft van welke bedrijven wel of niet onder de wetgeving vallen. Tegelijkertijd wordt in het *panel MKB* aangegeven door de bedrijven dat veel van hen nog niet weten of ze onder de reikwijdte vallen.

Er zijn hierbij drie suggesties die kunnen helpen voor een bedrijf om uitsluitsel te krijgen of zij wel of niet onder de Cbw gaan vallen:

(1) Zorg dat de huidige tool van de nationale overheid (https://regelhulpenvoorbedrijven.nl/NIS-2-NL/) een definitief uitsluitsel kan geven voor een bedrijf. Hiermee bestaat er geen twijfel voor bedrijven om wel of niet NIS2 plichtig te zijn.

(2) Wijs bedrijven formeel aan door ze in het register te plaatsen en informeer ze dat ze onder de reikwijdte van de wet vallen. Indien voor deze methode wordt gekozen, waarbij centraal bedrijven kunnen worden geïnformeerd of ze onder deze wet gaan vallen – net als bij de NIS1 het geval was - zal dat de regeldruk in z'n totaliteit verlichten. Waarna ze – vanzelfsprekend – wel als wettelijke plicht hebben om zelf de registratie van de genodigde gegevens en de administratieve last voor het ingeven van contactgegevens en IP bereiken moeten dragen.

(3) Werk samen met de bedrijven om gezamenlijk de invulling van verplichtingen en registratieprocessen te bepalen. In België wordt bijvoorbeeld in samenspraak vastgesteld welk niveau vereist is (zoals CyFun Basis, Belangrijk of Essentieel). Een dergelijke gezamenlijke aanpak draagt bij aan zowel duidelijkheid als draagvlak binnen het bedrijfsleven.

Vanuit FERM hebben wij in eerder overleg vernomen dat het juridisch onmogelijk is vanuit het NCSC om entiteiten aan te wijzen die onder de NIS2 gaan vallen. Echter zien we de juridische onmogelijkheid noch in het Cbw noch in het Cbb.

3. Scheiding van rollen, verantwoordelijkheden en bevoegdheden klein bedrijf

Beleid fungeert als cruciale basis voor bedrijven om een hogere mate van cybervolwassenheid te bereiken. Artikel 6 van het Cbb is daarmee een belangrijke maatregel die bedrijven moeten treffen om te voldoen aan de zorgplicht. Echter zien wij in Artikel 6 lid 2 een uitdaging voor het kleine bedrijf “De entiteit zorg ervoor dat conflicterende rollen, verantwoordelijkheden en bevoegdheden gescheiden worden”. Voor een organisatie die qua medewerkers net binnen de reikwijdte van de Cbw valt, zal dit een enorme uitdaging met zich meebrengen. Daarom stellen we voor dat de formulering wordt aangepast zodat de scheiding van rollen, verantwoordelijkheden en bevoegdheden proportioneel is aan de grootte van de organisatie.

2. Vragen om verduidelijking

4. Parameters van verplichtingen nader bepalen

Bij onze feedback op de internetconsultatieronde van de Cbw hadden wij geattendeerd op verduidelijking van drempelwaardes in Cbb voor het melden van incidenten. In Artikel 24 lid 2 van de Cbb wordt er vermeld dat de doeltreffendheid van criteria voor melden van incidenten om de vier jaar wordt getoetst. Echter wordt er geen duidelijkheid geschept over hoe en waar deze criteria worden gedeeld. Graag zouden wij verduidelijking zien waar het gaat om deze criteria voor het melden van significante incidenten. In 2024 kregen wij vragen van participanten over de Cbw die nog steeds relevant zijn voor dit onderwerp:

- *Aanvullend op de gegeven definitie, aan welke parameters moet een incident voldoen om als significant incident te worden beschouwd?*
- *Hoe dient een multinational om te gaan met het verstrekken van IP adressen?*
- *Voor wat betreft de IP range; hoe dient er worden omgegaan met IT infrastructuur in de Cloud die niet noodzakelijkerwijs het IP adres van het bedrijf volgt.*

5. Overzicht geven koppeling met toekomstige (relevante) wet en regelgeving

Naast de relatie tussen de CBW met de WWKE (Wet Weerbaarheid Kritieke Entiteiten), komen er meer relevante wet- en regelgeving op het gebied van digitale weerbaarheid. Per 2027 zal de

Cyber Resilience Act (CRA) van kracht gaan, waarbij leveranciers van producten met een digitale component een verplichting krijgen om een Software Bill of Material (SBOM) te moeten leveren. Vanuit de participanten van FERM bestond deze vraag al langer, aangezien dit positief zal uitpakken voor de weerbaarheid van de toeleveringsketen. Incidenten zoals bij de Log4J kwetsbaarheid hebben duidelijk gemaakt dat veel entiteiten geen goed overzicht hebben van hun software supply chain.

Wat is onder deze wet verplicht en met welke maatregelen mag gewacht worden tot de invoering van de CRA verordening?

Wij zouden graag zien dat de overheid hier een actieve rol in speelt om de koppeling tussen deze wetgevingen met elkaar in kaart te brengen.

6. Verduidelijking eisen van de training

In artikel 20 tot en met artikel 23 van de AMvB wordt meer duidelijkheid gegeven over de eisen voor de training van het bestuur. Ook lezen we dat in het *panel MKB* in de NvT wordt bevestigd dat een bestuurder niet in staat hoeft te zijn om de technische aspecten van een DDoS-aanval uit te leggen. Dit draagt bij aan het verlagen van de regeldruk voor bedrijven.

Echter, er blijven enkele onduidelijkheden die verdere toelichting vereisen. Zo is het niet helder binnen welke termijn na aanstelling een bestuurslid de vereiste training moet hebben afgerond en een certificaat moet hebben behaald. Wij adviseren een harde eis op te nemen waarin expliciet wordt vermeld binnen hoeveel tijd deze verplichting moet zijn nagekomen.

Daarnaast wordt in artikel 22 van de NvT gesteld dat de trainer onafhankelijk en gekwalificeerd moet zijn. Het is echter onduidelijk hoe dit aangetoond kan worden en welke criteria worden gehanteerd om de kwalificaties van trainers te bepalen. Wij raden aan om heldere richtlijnen te formuleren die beschrijven hoe de onafhankelijkheid en de kwalificaties van trainers vastgesteld kunnen worden. Denk hierbij aan specifieke diploma's, werkervaring of certificeringen. Tegelijkertijd is het belangrijk om te waarborgen dat de commerciële marktwerking rondom trainingstrajecten niet leidt tot kwaliteitsvermindering of ongewenste effecten.

3. Aanvullende suggesties voor een hogere doelmatigheid

7. Inrichting supportstelsel voor entiteiten door samenwerkingsverbanden

Bedrijven in heel Nederland – met uitzondering van de meest mature en vitale die al onder de NIS1 vielen - werden geholpen in hun kennis en handelingsperspectief door OKTT's. Voor de meest mature bedrijven – vitaal - was support via ISACs voldoende.

Voor de bedrijven die worden geholpen door OKTT's is eenduidige support dichtbij belangrijk, net als een specifieke doorvertaalfunctie. Met het intrekken van de Wbni komen die aanwijzingen te vervallen. Momenteel is het nog onduidelijk op welke wijze de OKTT status een vervolg krijgt als gevolg van de implementatie van de Cbw. FERM ziet op grond van artikel 17 van de Cbb de mogelijkheid bedrijven te blijven ondersteunen in het havengebied. Hier wordt aangegeven dat 'relevante partijen' onder het regime van de CBW -kunnen worden gekwalificeerd als een partij om informatie mee te delen én om samenwerkingsrelaties tot stand te brengen met CSIRT's. Eerder is mondeling toegezegd dat de OKTT's zonder verdere administratieve plicht als dusdanig zouden worden aangemerkt. Graag zouden we dit ook in het Cbb genoemd zien.

8. Aanwijzingen en taken van havenCSIRT

Daarnaast zien we graag dat om Artikel 17 van de Cbb goed uit te kunnen voeren, dat er een CSIRT ingericht, wordt specifiek voor de subsector Havens. Dit vanwege de verplichte risicogebaseerde benadering voor de CSIRTs en de bijzondere situatie waarin havens en de daarin opererende ketens zich bevinden.

Onder NIS2/CBW moet er een nationaal plan komen om grote crises het hoofd te bieden. Wanneer een crisis entiteit overstijgend is zal het verantwoordelijk CSIRT helpen met de coördinatie. Echter is in het havengebied een entiteit overstijgende crisis al snel fysiek. Een havenCSIRT zal dit structureel kunnen coördineren met de veiligheidsregio.

Het havengebied kent een aantal dreigingen die uniek zijn, zoals bijvoorbeeld digitale oorzaak – fysieke gevolgen als gevolg van dreiging van statelijke actoren en de grote hoeveelheid aan chemische ketens en goederen die door het gebied lopen. Nauwe regionale samenwerking met bijvoorbeeld FERM en/of de regionale veiligheidsregio voor (cyber)gevolgbestrijding kan op die manier geborgd worden.

9. Incrementele wijziging van AMvB beperken

Vanuit FERM ondersteunen en begrijpen we de keuze om de AMvB niet volledig af te kaderen, waardoor de overheid in een wendbare positie blijft. Dit is van groot belang in het dynamische cybersecuritylandschap, waar dreigingen en oplossingen in een constant kat-en-muisspel verwikkeld zijn. Het behouden van flexibiliteit in de wetgeving is essentieel om tijdig en effectief te kunnen reageren op nieuwe uitdagingen.

Wij willen echter benadrukken dat deze flexibiliteit zorgvuldig moet worden beheerd. Incrementele wijzigingen dienen tot een minimum beperkt te worden om consistentie en duidelijkheid in de regelgeving te waarborgen. Wij adviseren daarom ervoor te waken dat wijzigingen in ministeriële regelingen enkel worden doorgevoerd wanneer deze significant van

aard zijn. Kleine wijzigingen zouden alleen goedgekeurd moeten worden als er een unanieme en duidelijke aanleiding voor is. Om dit te voorkomen, raden wij aan duidelijke en transparante criteria op te stellen voor wijzigingen. Deze criteria zouden helder moeten maken onder welke omstandigheden aanpassingen noodzakelijk en gerechtvaardigd zijn, waardoor willekeurige wijzigingen voorkomen worden.

Conclusie

FERM verwelkomt de Cyberbeveiligingswet en ziet de implementatie als een stap in de groei naar digitale weerbaarheid. We verwelkomen deze wet en verwachten een hoge mate van doeltreffendheid en doelmatigheid. Tegelijkertijd vragen we om onnodige regeldruk te voorkomen en doen we enkele suggesties als alternatief om hetzelfde doel te bereiken, maar met minder regeldruk. Ook vragen we om verduidelijkingen om verschil in interpretatie te voorkomen, welke kunnen leiden tot onjuiste of ongewenste implementatie bij entiteiten en de roep om jurisprudentie, wat vertragend gaat werken. Als laatste geven we enkele aanvullende suggesties die de doelmatigheid zal vergrootten.

(1) Suggesties om de druk voor bedrijven te verminderen

1. Zorg ervoor dat alle mogelijke verplichte meldingen gecombineerd worden in één handeling voor bedrijven, om de regeldruk te beperken en efficiënter te voldoen aan de uiteenlopende meldplichten
2. Schrijf bedrijven formeel aan door ze in het register te plaatsen en informeer ze dat ze onder de reikwijdte van de wet vallen, zodat er geen twijfel bestaat en de regeldruk in z'n totaliteit wordt verlicht.
3. Pas de formulering van Artikel 6 lid 2 aan zodat de scheiding van rollen, verantwoordelijkheden en bevoegdheden proportioneel is aan de grootte van de organisatie.

(2) Vragen om verduidelijking

4. Verduidelijk de criteria voor het melden van significante incidenten en geef aan hoe en waar deze criteria gedeeld worden, om onzekerheid bij bedrijven te voorkomen.
5. Breng de koppeling tussen de CBW, WWKE en toekomstige wet- en regelgeving zoals de Cyber Resilience Act (CRA) in kaart en zorg voor duidelijke richtlijnen over de verplichtingen en maatregelen die gelden vóór en na de invoering van de CRA.
6. Leg vast binnen welke termijn na aanstelling een bestuurslid de vereiste training moet afronden en een certificaat moet behalen, en stel duidelijke richtlijnen op voor de onafhankelijkheid en kwalificaties van trainers, waarbij kwaliteitsborging prioriteit krijgt.

(3) Aanvullende suggesties om de doelstelling te bereiken met een hoge doelmatigheid

7. Neem in het Cbb expliciet op dat OKTT's zonder verdere administratieve plicht worden aangemerkt als relevante partijen om informatie mee te delen en samenwerkingsrelaties tot stand te brengen met CSIRT's, zoals eerder mondeling is toegezegd.
8. Richt een specifiek CSIRT in voor de subsector Havens om Artikel 17 van de Cbb effectief uit te voeren, en zorg voor nauwe regionale samenwerking met de veiligheidsregio om unieke dreigingen en entiteit overstijgende crises in het havengebied structureel te coördineren.
9. Beperk incrementele wijzigingen in de AMvB tot een minimum en stel duidelijke en transparante criteria op die vastleggen onder welke omstandigheden aanpassingen noodzakelijk en gerechtvaardigd zijn, om consistentie en duidelijkheid in de regelgeving te waarborgen

FERM is vanzelfsprekend bereid zijn standpunten nader toe te lichten.