Reactie op consultatie cyberbeveiligingswet

Met betrekking tot de internetconsultatie voor de Cyberbeveiligingswet, geschreven vanuit de belanghebbenden rondom het Haven Industrieel Complex van Rotterdam en Moerdijk, door FERM Rotterdam.

FERM is een non-profit stichting, een samenwerkingsverband, die zich inzet voor het verbinden van bedrijven en organisaties om bij te dragen aan de digitale weerbaarheid van het Haven Industrieel Complex. FERM is als organisatie direct belanghebbende en vertegenwoordigd een aantal organisaties, zowel publiek als privaat, die ook belanghebbenden zijn. Tevens hebben allen relevante kennis over en ervaring met het werkveld waar de Cyberbeveiligngswet van toepassing op is.

Doel

Het beoogde doel van de NIS-2 richtlijn is een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie teneinde de werking van de interne markt te verbeteren. De Cyberbeveiligingswet (Hierna 'CBW') is de doorvertaling hiervan voor de Nederlandse lidstaat. Vanuit FERM verwelkomen wij deze wet en zien een hoge mate van doeltreffendheid en doelmatigheid. Tegelijkertijd zijn er vragen. Deze zijn in drie categorieën onderverdeeld. We vragen om:

a. het overwegen van alternatieven om hetzelfde doel te bereiken, maar met minder regeldruk;
b. 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;
c. aanvullingen – bijvoorbeeld in aanvullende maatregelen van bestuur - om de doelstelling te bereiken met een hoge(re) doelmatigheid.

Aanleiding

Op 21 mei 2024 is de consultatieronde van de CBW van start gegaan, waarbij de NIS2-richtlijn vastgesteld door het Europees Parlement en de Raad van de Europese Unie die op 22 november 2022 is aangenomen is door vertaald naar Nederlandse wetgeving. De NIS2 richtlijn dient als de opvolger van de huidige NIS-1 richtlijn. NIS2 is een belangrijke stap in de verbetering van de cyberveiligheid in de EU.

Context en uitdagingen Haven Industrieel Complex

Er gebeurt gelukkig al veel ten goede. Op projectbasis en structureel zijn er in de afgelopen jaren grote stappen gezet in het vergroten van de weerbaarheid tegen digitale verstoringen. De resultaten van de scans die worden uitgevoerd in het havengebied zijn illustratief, deze tonen namelijk een groeiend maturity niveau aan.

Daarentegen worden er ook uitdagingen zichtbaar:

- In het havengebied is de digitale en fysieke verbondenheid enorm. De digitale dreigingen zijn vrijwel allen kritiek door de enorme fysieke impact. Dan wel op logistiek vlak, dan wel op de grote hoeveelheid bedrijven die chemische stoffen bewerken of vervoeren. Ook op het gebied van ondermijning – in ons gebied synoniem voor drugsgerelateerde crimininaliteit – zien we scenario's die de oorsprong in cyber hebben. Daarnaast zien we ook een specifieke vorm van digitale fraude rondom spoofing van storage en containers.
  De maatregelen die hiertegen kunnen worden genomen, worden benoemd in de originele NIS-2 richtlijn. Maar hoe krijgen we deze scenario's, deze risico's, die zo kenmerkend zijn voor het gebied terugvertaald naar maatregelen die bedrijven kunnen nemen? De kennis is er deels en wordt deels ook nog ontwikkeld.

- 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 van de haven.
  En dat terwijl de dreigingsscenario's duidelijk entiteit-overstijgend zijn. Soms qua impact of gebiedsgericht zoals hierboven al beschreven of gebiedsdreiging zoals door statelijke actoren.
  Ondersteuning vanuit FERM wordt wel voor deze doorsnede in scenario's gegeven. FERM is beoogd onderdeel van het CWN – Cyber Weerbaarheids Netwerk, de opvolger van het Landelijk Dekkend Stelsel. Deelname aan FERM en haar activiteiten heeft echter een te vrijwillig karakter om het gat tussen dreiging en weerbaarheid te dichten. Bovendien moet FERM als onafhankelijke stichting kostendekkend zijn. Daarmee is continuïteit van dienstverlening onzeker omdat vanuit een landelijk perspectief financiële ondersteuning voor support - vanuit de verschillende ministeries - sector-gericht is.

- De regeldruk is in de afgelopen jaren is sterk toegenomen. In combinatie met personeelstekort is het belangrijk om de richtlijnen makkelijk uitvoerbaar te houden; zeker ook omdat de betrokkenheid vanuit het midden- en kleinbedrijf nog achter blijft.

1) Suggesties om de druk voor bedrijven te verminderen

1. Registratieplicht: aanschrijven bedrijven die onder wetgeving vallen.

De huidige voorgestelde uitvoer van de wet, voorziet in het registreren van bedrijven in een nationaal register (registratieplicht).
In de berekening van de regeldruk in de Memorie van Toelichting (MvT) zijn de kosten die entiteiten moeten maken om te bepalen of ze onder de reikwijdte van dit wetsvoorstel vallen niet meegenomen. Hier zien we nog onduidelijkheid bij bedrijven die zich daarop zelfs tot consultants en juristen moeten wenden. Zelfs met de tool van de nationale overheid (https://regelhulpenvoorbedrijven.nl/NIS-2-NL/) blijven er onduidelijkheden, bovendien geeft deze tool ook geen definitief uitsluitsel

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

- Ik vind het nog steeds lastig te bepalen of we er onder vallen. We zijn wel groot genoeg en hebben activiteiten die je er onder zou kunnen zien (ICT dienstverlening) maar het zou een stuk duidelijker zijn als bijvoorbeeld de SBI-codes waar het om gaat er bij worden vermeldt.

- Als de overheid de benodigde informatie heeft om dit te bepalen zou dat prettig zijn, en druk verminderen.

*- ons bedrijf valt onder een holding die wereldwijd meer dan 6.000 werknemers telt. In Nederland hebben wij een BV die als 'essentiële entiteit' wordt gedefinieerd en een andere BV die als 'belangrijke entiteit' wordt gedefinieerd. Vallen wij als gehele holding onder de NIS2 of zullen de BV's als apar*te entiteiten onder de NIS2 gaan vallen.

- multinationals: hoe verhoudt zich artikel 4, lid 4 tot doorvertalingen bij andere lidstaten?

- randen van sectordefinities

- welk balanstotaal moet ik naar kijken ten aanzien van de bedrijfsomvang?

Indien er wordt gekozen voor een methode waarbij centraal bedrijven kunnen worden geïnformeerd of ze onder deze wet gaan vallen – net als bij de NIS-1 het geval was - zal dat de regeldruk in z'n totaliteit verlichten. Dit zouden we graag als suggestie meegeven: Wijs bedrijven formeel aan door ze in het register te plaatsen en informeer ze dat ze onder de reikwijdte van de wet vallen. 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.

Vanuit FERM hebben wij in eerder overleg vernomen dat het juridisch onmogelijk is om entiteiten aan te wijzen die onder de NIS2 gaan vallen. Echter zien we de juridische onmogelijkheid niet in de NIS-2 richtlijn.

2. <u>Afhandeling verplichte meldpunten met één handeling en confidentialiteit van meldingen</u>

De MvT meldt (paragraaf 5.5.1) dat dubbele meldplicht nodig is vanuit verschillende taken. Er wordt gestreefd deze dubbele meldplicht technisch zodanig in te richten dat het verspreiden van de benodigde informatie maar één handeling voor de entiteit vergt.

In de praktijk hebben bedrijven al meerdere meldplichten digitale incidenten, zo bijvoorbeeld ook in het kader van de AVG (GDPR) bij de Autoriteit Persoonsgegevens en moeten digitale incidenten in havens ook gemeld worden onder ISPS (International Ship & Port Facility Security) bij de Rijkshavenmeester vanuit diens wettelijke taak of onder de Seveso wetgeving (voorheen: Besluit Risico Zware Ongevallen) bij de DCMR Milieudienst Rotterdam Rijnmond, daar waar het fysieke gevolgen betreft. Ook vraagt de Nationale Politie om meldingen van cybercrime en de Zeehavenpolitie om meldingen van Storage Spoofing en heeft de Douane, vrijwillig, de mogelijkheid voor het verkrijgen van de AEO-status, welke ook een haakje cyber bevat. Al met al, brengen deze verschillende meldplichten veel regeldruk met zich mee.

Om de regeldruk te beperken verzoeken we om voor allerlei mogelijke verplichte meldingen te combineren in één handeling voor bedrijven.

We snappen dat het organiseren uitdagingen met zich meebrengt, zo is ons in eerdere overleggen al duidelijk gemaakt. We snappen dat eisen van meldingen voor toezichthouders onder de CBW en de AP niet volledige overlap hebben. Echter zouden na de initiële melding van het incident belanghebbende organisaties altijd nog een uitvraag kunnen doen naar extra informatie over het incident. Doel is hier het significante verminderen van regeldruk bij bedrijven.

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

- Hoe zit het met gezamenlijk toezicht met andere toezichthouders die ook een deels fysieke verantwoordelijkheid hebben (douane, DCMR, HBR) - zijn daar mogelijkheden bespreekbaar die het makkelijk voor bedrijven gaat maken?

- Als ik een melding doe bij bv 112, komt die dan ook automatisch terecht bij de havenmeester?

- Als ik een incident meld, kan dat nooit anoniem. Mijn install-base is uniek voor mijn bedrijf. Hoe kan ik voorkomen dat een melding bij concurrenten in andere landen terecht komt?

- Als een bedrijf te maken krijgt een cyber incident moet men naar 6 tot 8 instanties een melding doen, terwijl herstel van de bedrijfscontinuïteit begrijpelijk hun hoogste prioriteit heeft. Het zou helpen als in de wetgeving de mogelijkheid/ verplichting wordt gecreëerd dat een melding binnen de overheid vertrouwelijk gedeeld wordt met belanghebbende.

- Veiligheidsregio's zouden een nog pro-actievere (signalerende) rol in kunnen gaan spelen en bijvoorbeeld afspraken maken met bedrijven in regio om eerder meldingen te krijgen als er iets speelt, zodat ze op basis daarvan potentiële impact beter kunnen monitoren. Daarmee is

niet bedoeld dat veiligheidsregio's een rol hebben in het bestrijden van het cyberincident. Zij kunnen zich op deze manier nog beter voorbereiden op de cybergevolgbestrijding.

3. <u>Regeldruk beperken voor bedrijven die niet rechtstreeks onder de reikwijdte van de wetgeving vallen.</u>

   In de MvT onder hoofdstuk 8 wordt gesteld dat dit wetsvoorstel geen gevolgen heeft voor de regeldruk voor (burgers en) bedrijven die niet binnen de genoemde sectoren of categorieën vallen, ofwel de drempelwaardes niet overschrijden ofwel niet anderszins bij besluit of regeling aangewezen zijn.
   Het is onze inschatting dat dit niet juist is. Vanwege de verplichting voor de keten van entiteiten die wel direct onder de wetgeving vallen er regeldrukeffecten gaan zijn voor bedrijven die hier niet rechtstreeks onder vallen.

   Om hier de regeldruk zo klein mogelijk te houden, zouden we graag voorstellen om met een uniform normenkader – een ‘bare minimum’ - te werken.

   Ter verduidelijking: Het treffen van maatregelen t.a.v. de cyberweerbaarheid voor deze groep zien wij zeker niet als nadeel. Sterker nog, wij zijn ervan overtuigd dat de maatregelen voorgeschreven vanuit de NIS2 een positief effect zullen hebben op de algemene cyberweerbaarheid van Nederland. Echter willen we voorkomen dat diverse maatregelen van verschillende NIS2 toezichthouders en verspreidt door verschillende entiteiten die wel onder de reikwijdte van de wet gaan vallen gaat leiden tot een grote diversiteit van eisen en dus meer regeldruk voor bedrijven die daar in de keten zitten.

Vragen en opmerkingen die we krijgen van participanten en overige organisaties: *- Zoals aangegeven in de MvT zullen voor bedrijven die voor het eerst onder de wetgeving gaan vallen 22% meer kosten met zich meebrengen voor het treffen van passende maatregelen. Voor bedrijven die al onder de Wbni vallen zal dit naar verwachting 12% zijn.* *Onze inschatting is dat die vele malen hoger ligt. Zeker voor bedrijven die hier indirect mee te maken gaan krijgen. Hoe zouden we zou dit verschil kunnen minimaliseren en de verwachte impact / effort kunnen beperken voor deze bedrijven?*

2) Vragen om verduidelijking

4. Zorgplicht nader definiëren in de Aanvullende Maatregelen van Bestuur
   Het valt op dat de zorgplicht in de CBW niet specifiek is gemaakt. We verzoeken om dit in de Aanvullende Maatregelen van Bestuur (AMvB) wel specifiek te maken om meetbaarheid en toetsbaarheid te kunnen realiseren.

   Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

   - waar moet ik precies aan voldoen?

   - hoe verhoudt zich deze implementatie in Nederland zich tot de implementatie in andere lidstaten?

   - wat moet ik doen om maatregelen voor afnemers te beperken, gaat dit alleen over voorlichting of ook over fysieke gevolgen daarvan?

   - Afgezien van de risicoanalyse en bijbehorende maatregelen (Mvt 5.3.4 / NIS2 overweging 89) is de Cyberbeveiligingswet inderdaad weinig specifiek. Voor zover wij hebben begrepen zullen er bij AMvB nog nadere eisen worden gesteld die waar mogelijk aansluiten op geldende normen in de diverse sectoren. In het geval van de zorg zal bijvoorbeeld de NEN7510 een rol gaan spelen in de toetsing van de zorgplicht.

5. Parameters van verplichtingen
   Graag zouden we verduidelijking zien waar het gaat om de parameters die de verplichtingen voorschrijven, bij voorbeeld in AMvB. Voor verdere definitie zie de vragen die we ontvangen van participanten over dit onderwerp.

   Wij snappen dat het ontbreken van duidelijk parameters de wetgeving wendbaarder en sneller implementeerbaar maakt. Anderzijds schept dit ook onduidelijkheid voor bedrijven voor het treffen van maatregelen op de lange termijn.

   Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

   - aanvullend op de gegeven definitie, welke parameters moet een incident aan voldoen om als significant incident te worden beschouwd?

   - artikel 26: wat wordt er bedoeld met ‘aantoonbaar actueel’? Wij vinden dat in de AMvB de toetsing van de bestuurders, los van de duur, ook de inhoud specifiek moet zijn aan de dreigingen die relevant zijn voor de sector.

   - 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.

6. Toeleverketens (1): verduidelijking gevraagd

De weerbaarheid van kritieke entiteiten levert vraagstukken voor de (toelever)ketens die actief zijn in de Rotterdamse haven. Artikel 23 lid 1 noemt de zorgplicht om de gevolgen van incidenten van afnemers te beperken. Gaat het hier ook om de zorgplicht om fysieke gevolgen te beperken?
In artikel 5.3.4 van de MvT wordt verwezen naar de NIS2 richtlijn, artikel 21, tweede lid, onderdeel d waar het gaat om de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners. Dit zien we als twee richtingen in de keten waarvoor zorgplicht geldt. Is dat juist?

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

- Ik hoor veel verschillende verhalen over veiligheidsmaatregelen betreffende de toeleveranciers. In Artikel 22 van de NIS2 richtlijn staat dat 'beveiligingsrisicobeoordelingen van specifieke kritieke ICT-diensten, ICT-systemen of ICT-producttoeleveringsketens' moeten worden uitgevoerd. Betekent dit dat ik dan enkel voor die toeleveranciers beveiligingsmaatregelen moet treffen, of ook voor andere directe toeleveranciers?

- moet ik audits gaan uitvoeren bij onze keten?

- Hoe ver gaat de zorgplicht voor de keten? Moet ik ze scannen op kwetsbaarheden? Ik heb gehoord dat er zelfs een organisatie is die CERTachtige hulp verleent. Wordt dit een ver-eiste?

- Is de zorgplicht in inkoopcontracten af te handelen?

7. Toeleverketens (2): risico's die entiteit overstijgend zijn en een fysiek en/of ook een fysiek element bevatten

Er is een verband tussen de wet op de weerbaarheid van de kritieke entiteiten (Wwke) en de CBW. In de praktijk van het havengebied kunnen deze niet los gezien worden van elkaar.

Risicoscenario's, zoals bijvoorbeeld bedoeld in artikel 9 van de CER lid 1.e - kunnen entiteit en sector overstijgend zijn en in geval van de haven van Rotterdam meerdere entiteiten bevatten die niet allen direct vallen onder de WWKE of de CBW.

Suggestie is om de MvT (Artikel 5.3.4) genoemde 'de beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekste leveranciers of dienstverleners.' ook de scenario's te toetsen in het risicoprofiel die verder gaan dan die voor de entiteit zelf maar een heel gebied betreffen.

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

- Waar zitten de grootste zorgen in de haven omtrent toeleveranciers? Welke instantie zoekt dit uit?

- In het havengebied zijn we naast digitaal ook fysiek verbonden. Als je kijkt naar het grote incident in 2017, zijn er bedrijven failliet gegaan vanwege leverproblemen doordat de snelwegen vol stonden. Wie maakt de vertaling van digitale oorzaak naar fysieke gevolgen en hoe past dat in deze wet?

8. <u>Cybergevolgbestrijding (response): Vergroten veerkracht en responsecapaciteit</u>

Er is een verband tussen de Wwke en de CBW, waarbij we een geïntegreerde aanpak voor digitaal en fysiek essentieel vinden.

De Minister van Buitenlandse Zaken geeft in zijn brief aan de Tweede kamer d.d. 13 oktober 2023 aan in artikel 3a dat voor de twee Europese richtlijnen -de herziening van de richtlijn netwerk- en informatiebeveiliging (de NIS2-richtlijn) en de CER-richtlijn- de samenwerking tussen Rijk, veiligheidsregio's en betrokken vitale aanbieders vergroot moet worden. Dit als onderdeel van het verhogen van weerbaarheid door de veerkracht en responscapaciteit verder te ontwikkelen. Het Ministerie van Justitie en Veiligheid wordt als eerstverantwoordelijke ministerie vermeld. Voor het vergroten van de responscapaciteit van Veiligheidsregio's is een goede informatiepositie en tijdige melding essentieel, zie ook hierboven vermeld.
De Landelijke Agenda Crisisbeheersing 2024-2029 vermeld op blz. 12 dat er gezorgd moet worden voor een robuuste informatiedeling en -verwerking. Als actiepunt wordt hierbij vermeld het maken van nadere afspraken over het verwerken van (vertrouwelijke) informatie binnen het netwerk van crisispartners, inclusief private/vitale partners.

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

- "Zorgpunt is op de informatiepositie voor de Veiligheidsregio's. Zonder een goede informatiepositie kan een veiligheidsregio de haar toebedachte rol in de (cyber) gevolgbestrijding niet goed vormgeven. Dit omvat toegang tot dreigingsinformatie en meldingen van lopende verstoringen."

- In de CBW wordt een gesproken van een zorgplicht (incl. je toeleveranciers/ onderaannemers, de zogenaamde 'keten'), een meldplicht en toezicht. In de CER wordt daarnaast ook gesproken over de ondersteuning aan kritieke entiteiten, maar weer niet vanuit een ketengedachten. Artikel 10 van de CER vermeldt mogelijke ondersteuning voor het verlenen van bijstand in het geval van crisis- of noodsituaties. Hiervoor staan in de regel veiligheidsregio's voor opgesteld. Is dat ook hier zo voor de fysieke gevolgbestrijding van digitale incidenten?

9. 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, bijvoorbeeld in de MVT.

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

- Voor organisaties die zowel onder NIS2 als de CER vallen, geld daarvoor dat er twee losse toezichthouders langskomen?

- Hoe kan ik aan de slag gaan met de beveiliging van mijn toeleveringsketen?

- Hoe verhouden de verschillende wetten zich tot elkaar?

- Stel dat een toezichthouder voor de cyberbeveiligingswet een verwijtbare tekortkoming constateert dat de procesveiligheid van een Seveso-inrichting raakt. Dan zou er náást een sanctie vanuit de cyberveiligheidswet wellicht ook een sanctie vanuit Seveso moeten volgen. Is dat logisch en wenselijk? Dit overschrijdt wellicht zowel de cyberbeveiligingswet als Seveso.

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

10. Inrichting supportstelsel voor entiteiten door samenwerkingsverbanden

Bedrijven in heel Nederland – met uitzondering van de meest mature en vitale die al onder de NIS-1 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. De MvT noemt in paragraaf 5.6.5 organisaties die op grond van de Wbni zijn aangewezen als OKTT. Dit betreffen - naast stichting FERM Rotterdam - ook Stichting Cyber Weerbaarheidscentrum Brainport (CWB), de Stichting Connect2Trust, de Vereniging Abuse Information Exchange, Stichting Nationale Beheersorganisatie Internetproviders (NBIP), Cyberveilig Nederland en de NL CISO Circle of Trust.

Met het intrekken van de Wbni komen die aanwijzingen te vervallen. Hierbij wordt aangegeven dat deze organisaties onder het regime van de CBW - onder omstandigheden - kunnen worden gekwalificeerd als een relevante 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 de MvT genoemd zien.

Ook zouden we richting CSIRT's de verplichting zien om deze samenwerkingsverbanden te ondersteunen met onder andere relevante en tijdige kennis om de preventieve en ondersteunende taak richting bedrijven te kunnen invullen. Daarmee stellen ze in staat, de rol die deze samenwerkingsverbanden richting haar achterban hebben te kunnen invullen. En daarnaast om - in bredere zin van het woord - ervoor te zorgen dat er voldoende maatregelen genomen worden om deze samenwerkingsverbanden te ondersteunen en in staat te stellen hun rol uit te voeren.

11. Aanwijzing en taken CSIRTs (1) informatiedeling

Graag zouden we wettelijk verankerd willen zien dat CSIRTs samenwerkingsverbanden zoals hierboven bedoeld – dus formeel vastgesteld - als taak krijgen om relevante en tijdige kennis te delen met samenwerkingsverbanden. De huidige formulering – dat er afspraken gemaakt kunnen worden – is te vrijblijvend.
Daarnaast zouden we graag zien dat in het kader van informatiedeling samenwerkingsverbanden namens een groep van entiteiten (essentieel en/of belangrijk) proactief deze entiteiten kunnen vertegenwoordigen. Kortom dat de taken en verdere specificering zoals bedoeld in Artikel 17 niet alleen de relatie tussen CSIRT en entiteiten rechtstreeks beschrijft, maar dat ook de relatie tussen CSIRT en samenwerkingsverbanden. En dat samenwerkingsverbanden hierin (groepen van) entiteiten mogen vertegenwoordigen.

Dit zal zowel de doelmatigheid vergrootten als de regeldruk bij bedrijven verlichten.

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

- Welke CSIRT's gaan relevant zijn voor het havengebied? (net als de ISACs zie ik meerdere die

relevant zijn vanwege de sectorale vs gebiedsorientatie)

12. Aanwijzing en taken CSIRTs (2) havenCSIRT

Daarnaast zien we graag dat om Artikel 17, lid 5 goed uit te kunnen voeren 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 de regionale veiligheidsregio voor (cyber)gevolgbestrijding kan op die manier geborgd worden.

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

- Aangezien het een gebied betreft in plaats van een sector zal het karakter hiervan wel anders zijn dan sectorale CSIRT's. CSIRT's kunnen onder de NIS2/Cbw worden aangewezen, hebben jullie vanuit FERM al eens verkend of jullie dit zelf zouden kunnen initiëren?

13. Rol NCSC als coördinator: partner voor havenspecifieke sectoroverstijgende risico's

In de CBW stelt Artikel 15 dat de Minister van J&V zorgt voor sectoroverstijgende samenwerking tussen de bevoegde autoriteiten binnen Nederland. Gezien de aard van havenactiviteiten – per definitie sector overstijgend – zouden we graag zien dat het NCSC vanuit deze rol als partner van FERM gaat optreden om de risico-scenario's uit het havengebied door te vertalen naar relevante departementen en sectoren die vanuit de verschillende andere ministeries worden bediend.
Een voorbeeld is ondermijning, dit beperkt zich niet tot één sector. Of dreiging van een statelijke actor op het gebied. Dat beperkt zich niet tot één sector maar specifiek op het gebied.

Vragen en opmerkingen die we krijgen van participanten en overige organisaties:

Net als de Rijkshavenmeester - verantwoordelijk voor de scheepsafhandeling vanuit ISPS wetgeving – zien we meerdere gevolgen in de haven (fysiek) van digitale verstoringen. Wie is verantwoordelijk voor welk scenario? Ik zou graag FERM als eerste aanspreekpunt blijven houden voor alles wat er in de haven relevant is.

Conclusies

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 noemen we enkele aanvullende suggesties die de doelmatigheid zal vergrootten.

1) Suggesties om de druk voor bedrijven te verminderen

- Registratieplicht: aanschrijven bedrijven die onder wetgeving vallen.
- Afhandeling verplichte meldpunten met één handeling en confidentialiteit van meldingen
- Regeldruk beperken voor bedrijven die niet rechtstreeks onder de reikwijdte van de wetgeving vallen.

2) Vragen om verduidelijking

- Zorgplicht nader definiëren in de Aanvullende Maatregelen van Bestuur
- Parameters van verplichtingen
- Toeleverketens (1): verduidelijking gevraagd
- Toeleverketens (2): risico's die entiteit overstijgend zijn en een fysiek en/of ook een fysiek element bevatten
- Cybergevolgbestrijding (response): Vergroten veerkracht en responsecapaciteit
- Overzicht geven koppeling met toekomstige (relevante) wet en regelgeving

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

- Inrichting supportstelsel voor entiteiten door samenwerkingsverbanden
- Aanwijzing en taken CSIRTs (1) informatiedeling
- Aanwijzing en taken CSIRTs (2) havenCSIRT
- Rol NCSC als coördinator