Reactie op consultatie Wet weerbare kritieke entiteiten

Met betrekking tot de internetconsultatie voor de Wet weerbare kritieke entiteiten, 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.

Doel

Het beoogde doel van de CER richtlijn is het verhogen van de weerbaarheid van kritieke entiteiten die een essentiële dienst verlenen in de Europese Unie. De Wet weerbare kritieke entiteiten 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. Hierbij kijken we vooral naar verduidelijkingen om verschil in interpretatie te voorkomen. Dit zou kunnen leiden tot onjuiste of ongewenste implementatie bij entiteiten en de roep om jurisprudentie wat vertragend gaat werken.

Aanleiding

Het havengebied kent een aantal dreigingen die uniek zijn, waarbij digitale oorzaken leiden tot fysieke gevolgen. Denk hierbij aan de dreiging van statelijke actoren en de grote hoeveelheid aan chemische ketens en goederen die door het havengebied lopen. Daardoor hebben we vanuit het ‘netten ophalen’ bij onze participanten voor de internetconsultatieronde van de Cyberbeveiligingswet, veel relevante overlap gezien met de Wwke. Daarnaast zullen ook meerdere van de organisaties gaan vallen onder beide wetgevingen.

<u>De punten die hieronder zijn genoemd zijn relevant voor beide wetten en in de combinatie daarvan. Vandaar dat ze volledigheidshalve als feedback op beide wetten worden gegeven.</u>

1. <u>Toeleverketens: risico's die entiteit overstijgend zijn en een fysiek en/of ook een fysiek element bevatten</u>

   Er is een verband tussen de wet op de weerbaarheid van de kritieke entiteiten (WWKE) en de cyberbeveiligingswet (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?

2. Cybergevolgbestrijding (response): Vergroten veerkracht en responsecapaciteit

Er is een verband tussen de wet op de weerbaarheid van de kritieke entiteiten (WWKE) en de cyberbeveiligingswet (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?

3. 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.

Conclusies

FERM verwelkomt de Wet weerbare kritieke entiteiten 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. Hierbij een overzicht van de suggesties vanuit deze consultatie:

- Toeleverketens: 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