Aan
Werkgroep IOV

Kopie verstuurd aan | **Documentnummer**

Vergaderdag

Project | **Auteur**
Voorstel IOV 6 | M.D. Wolthuis - Tjin Liep Shie

Onderwerp
Digitale kwetsbaarheid en cybersecurity

Gevraagde beslissing

De werkgroep wordt verzocht om voor het project Digitale kwetsbaarheid en cybersecurity € 115.000,- ter beschikking te stellen.

Toelichting

Vanaf maart 2019 loopt binnen de afdeling Inspectie en Handhaving van de DCMR de opdracht om te bekijken of en hoe het toezicht op cybersecurity kan worden vormgegeven.
Halverwege 2019 is dit project opgenomen in het IOV-programma voor 2019. Met de Brzo-OD's en kernteam BRZO+ is afgesproken dat de DCMR initiatief neemt en de voortgang rapporteert.
Er is een landelijke werkgroep cybersecurity waarin samen met de beleidsdirecties van IENW en SZW, SODM en de provincie ZH (namens IPO) geprobeerd is om duidelijkheid te krijgen in:

- de mate waarin bedrijven maatregelen hebben getroffen om de risico's op zware ongevallen door een digitale aanval te voorkomen/verkleinen;
- wat het wettelijk kader is en de daarbij behorende taken en bevoegdheden voor Brzo-omgevingsdiensten en de betrokken BRZO+-partners.

In 2019 heeft de werkgroep geen resultaten opgeleverd.

Stand van zaken 2019

- Het landelijke traject stagneert. Wel is er een duidelijk beeld welke stappen er in 2020 gezamenlijk gezet moeten worden om op het dossier cybersecurity voortgang te boeken.
- Cybersecurity stond op 21 november 2019 op de agenda van het overleg van de directeur DCMR met de CEO's van de Brzo-bedrijven in ZH en Zeeland. Tijdens dit overleg hebben de bedrijven aangegeven het logisch te vinden dat de DCMR ze schriftelijk vraagt om inzicht te geven in de scenario's die men onderkend heeft mbt cyberaanvallen en in de maatregelen die de bedriiven hiertegen hebben getroffen. Afgesproken is dat de DCMR in overleg met Deltalinqs en de ondernemersvereniging voor de Zeeuwse bedrijven, een brief opstelt. In een eerste gesprek geeft Deltalinqs aan liever over digitale kwetsbaarheid te spreken dan over cybersecurity.
- Vanuit internationale regelgeving stellen het Havenbedrijf Rotterdam (ISPS) en de douane (AEO) regels aan de cybersecurity bij bedrijven. Daarnaast voert de digitale rechercheur van de zeehavenpolitie preventieve en repressieve controles uit bij bedrijven in het havengebied. Zowel het havenbedrijf als de douane hebben nog geen invulling gegeven aan hun toezichtstaak op het gebied van cybersecurity omdat er onvoldoende inzicht is in wat

deze toezichtstaak inhoudt. Voor de DCMR is nog niet duidelijk of zij een taak heeft. Afgesproken is om gezamenlijk (inclusief de zeehavenpolitie) bij een aantal bedrijven (minimaal 4) en op vrijwillige basis te onderzoeken:

- wat de gevolgen voor de VTH-uitvoering zijn (wie is ervan, welke kennis en kunde en capaciteit);
- of er een gezamenlijk normenkader kan worden ontwikkeld;
- of door een gezamenlijke uitvoering efficiëntie kan worden bereikt.

Uitvoering 2020

Uitgangspunt is dat het Rijnmondgebied een proeftuin is om inzicht te krijgen in de:

a. stand van zaken bij de bedrijven;
b. gevolgen voor de VTH uitvoering (duidelijkheid wet- en regelgeving en gevolgen VTH-uitvoering van de betrokken BRZO+-diensten).

Ook het ministerie van IENW wil inzicht in de stand van zaken bij de (chemische) Brzo-bedrijven en meer duidelijkheid in wet- en regelgeving m.b.t. cybersecurity bij deze bedrijven. Het ministerie overwoog een voorstel voor het IOV-6 budget aan het schrijven. Dit voorstel bleek aanvullend op het plan van de Brzo-OD's voor het IOV-1 budget.

Door beide plannen samen te voegen ontstaat er enerzijds synergie en anderzijds een professionelere aanpak door het inhuren van IT-specialisten en daarmee verbetering van de kwaliteit van de uitvoering en van de resultaten.

<u>Projectvoorstel (3 sporen)</u>

Het project bewandelt de volgende drie sporen.

Spoor 1: Bedrijven
Inzicht in de mate waarin bedrijven de scenario's van risicovolle situaties in beeld hebben en de mate waarin hiervoor adequate maatregelen (waaronder cybersecurity) zijn getroffen om de risico's te beheersen. Dit traject wordt afgestemd met de Brzo-OD's en de BRZO+-partners en het bedrijfsleven.

Spoor 2: Overheid

- Verkrijgen van duidelijkheid over de wet-en regelgeving mbt digitale kwetsbaarheid en in het bijzonder cybersecurity bij Brzo-bedrijven. Inzicht in mogelijke lacunes, onduidelijkheden of onvolkomenheden in de regelgeving die adequate borging van vooral cybersecurity in de weg staan.
- In beeld brengen hoe de VTH-uitvoering mbt cybersecurity eruitziet en wat hiervoor aan kennis, kunde en capaciteit nodig is.
- Het waar mogelijk verminderen van regeldruk bij de bedrijven in het Rotterdamse havengebied en een efficiëntere uitvoering door de toezichthoudende diensten.

Het onderzoeksdeel wordt afgestemd met de Rotterdamse havenpartners (havenbedrijf, douane en zeehavenpolitie). Ook hier vindt afstemming plaats met de Brzo-OD's en BRZO+-partners. Het ministerie van IENW trekt het onderdeel wet- en regelgeving.

Spoor 3: Kennisdeling
Best practices zijn in beeld en kunnen worden uitgewisseld tussen overheden, tussen overheden en bedrijven en bedrijven onderling.
Bedrijven krijgen een handreiking om systematisch risico's te identificeren en bijbehorende maatregelen te benoemen. Voor de overheid wordt een tool ontwikkeld om de gegevens te kunnen beoordelen.

Er wordt een klankbordgroep geformeerd (bestaande landelijke werkgroep + JENV) die geconsulteerd wordt tijdens de uitvoering van de 3 sporen. Ook wordt gezorgd voor afstemming met andere al lopende projecten en voor afstemming met de branches en VNO/NCW.

Financiën

Brzo-OD	IOV-1	IOV-6	Eigen budget
Spoor 1: Bedrijven	€ 11.000,--	€ 65.000,-	€ 83.000,-
Spoor 2: Overheid	€ 10.283,-	€25.000,-	€ 25.000,-
Spoor 3: Kennisdelen	€ 4.000	€25.000	€ 5.000
Totaal	**€25.283,--**	**€ 115.000**	**€ 113.000,-**

Gevraagd budget IOV-6
De werkgroep wordt verzocht om voor het project Digitale kwetsbaarheid en cybersecurity € 115.000,- ter beschikking te stellen.
Het conceptprojectplan is toegevoegd.