FERM Rotterdam Port Cyber Resilience

Van bewustwording naar weerbaarheid

Introductie FERM

Abstract uit het Adviesrapport

Auteurs: Sandra Konings, Robert Jan Marringa, Ward Veltman en Sarah Olierook met bijdragen van de FERM werkgroep

Versie: 1.1 d.d. 4 februari 2021

Inhoudsopgave

1. Context - Vergroten digitale weerbaarheid Haven Industrieel Complex!

1.1 Het Haven Industrieel Complex als internationale gateway

Nederland dankt € 45,6 miljard ofwel 6,2% van zijn toegevoegde waarde aan de Rotterdamse haven. Deze haven biedt (direct en indirect) plaats aan meer dan 355.000 werknemers[1]. De haven is direct verbonden met de aanvoer van producten die inwoners van Nederland dagelijks nodig hebben. Dit zijn producten die door Nederlandse bedrijven worden geïmporteerd en geëxporteerd. De continuïteit en efficiëntie van de processen die plaatsvinden in de haven zijn dan ook van vitaal belang voor Nederland als handelsland.

Europees gezien heeft het haven industrieel complex ook een belangrijke functie. De haven van Rotterdam is de grootste haven van Europa en veel goederen die hier aankomen worden vervoerd richting het Europees achterland. Binnen de haven van Rotterdam zijn er meer dan 700 organisaties actief in veel verschillende sectoren. Een verstoring van een goede werking van de Rotterdamse haven kan dan ook Europees gezien economische impact genereren.

Alle organisaties in het Haven Industrieel Complex hebben te maken met de kans op digitale verstoringen waardoor mogelijk systemen uit komen te vallen of de juiste werking van systemen niet meer gegarandeerd kan worden. Dit heeft zowel betrekking op kantoorautomatisering (IT) als op procesautomatisering (OT), immers zowel de kantooromgeving als de industriële omgeving zijn de laatste jaren steeds verder gedigitaliseerd. Voor individuele organisaties is het dan ook van groot belang om een digitale verstoring te voorkomen of in ieder geval de impact van een verstoring, ook op andere partijen in het Haven Industrieel Complex, zoveel mogelijk te beperken.

1.2 Het risico, de urgentie en de noodzaak te versnellen

De cyberaanval op APM Terminals/Maersk uit juni 2017 maakt de kwetsbaarheid en afhankelijkheid van het Haven Industrieel Complex zichtbaar. Het besef is groot dat alle organisaties slachtoffer kunnen worden van een cyberaanval. Dit heeft een effect heeft op de logistieke keten, de bedrijfsprocessen van de individuele organisaties en uiteindelijk op de Nederlandse economie. Daarnaast is er een sterk bewustzijn dat digitalisering van de processen van bijvoorbeeld bedrijven in de chemie ook een impact kan hebben op de fysieke veiligheid.

Tegelijkertijd blijkt uit o.a. het Cyber Security Beeld Nederland (CSBN) van het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid dat de dreiging toeneemt en maatregelen die tegen die dreiging geïmplementeerd zijn hier geen gelijke tred mee houden. Ontwrichting van de Nederlandse maatschappij ligt op de loer volgens het NCSC.[2]

De tijd van alleen maar bewustwording creëren is dan ook voorbij. De organisaties in de Rotterdamse haven en hun nautische en veiligheidspartners moeten én willen de volgende stap zetten: het Haven Industrieel Complex meer weerbaar maken tegen digitale verstoringen.

1.3 Wat is het vertrekpunt?

Binnen het Rotterdams havengebied wordt op verschillende manieren samengewerkt om de cyberweerbaarheid te verhogen. Zo organiseert FERM sinds 2016 meerdere keren per jaar een Port Cyber Café. In de periodieke FERM Port Cyber Cafés duiken we samen met experts uit het vak in een informele setting dieper in een actueel onderwerp rond cybersecurity in het Rotterdamse Havengebied. Daarnaast informeert FERM de ondernemers in de haven via haar nieuwsbrief en

[1] https://www.portofrotterdam.com/sites/default/files/downloads/het-rotterdam-effect-pdf.pdf

[2] https://www.ncsc.nl/actueel/nieuws/2019/juni/12/csbn-2019-ontwrichting-ligt-op-de-loer

website over ontwikkelingen in cybersecurity, houdt het jaarlijks een grote cybercrisisoefening en heeft het een cybercrisisstructuur ingericht.

Naast FERM wordt er ook intensief samengewerkt en informatie gedeeld in de Haven-ISAC, de Chemie-ISAC en andere sectorspecifieke ISACs (Information Sharing and Analysis Center). In de ISACs delen veiligheidspartners en private organisaties hun kennis en ervaringen op het gebied van cyberweerbaarheid. Het deelnemerschap is vaak beperkt tot een selecte groep bedrijven en vitale organisaties.

FERM en de ISACs bestaan nadrukkelijk naast elkaar, waarbij FERM een belangrijk rol inneemt waar het het weerbaar maken van het Haven Industrieel Complex betreft. Verschil tussen FERM en de ISACs zit onder andere in het feit dat het aantal organisaties in de ISACs beperkt is en informatiedeling niet wordt geautomatiseerd. FERM heeft een groter bereik, biedt diensten aan die de weerbaarheid versterken en gaat actief op zoek naar en geeft duiding aan relevante en specifieke dreigingsinformatie.

2. Why – waar staan we voor?

2.1 Impact van digitale verstoringen

Digitalisering brengt economische en maatschappelijke kansen. Maar ook bedreigingen, onder meer door sabotage. Verregaande digitalisering maakt het Haven Industrieel Complex dan ook meer kwetsbaar; alles is immers digitaal verbonden en een verstoring bij één organisatie kan leiden tot een verstoring in de gehele keten.

Om bedreigingen het hoofd te kunnen bieden en de impact van verstoringen te verkleinen is het essentieel om binnen het Haven Industrieel Complex samen te werken. Bijvoorbeeld door onderling informatie uit te wisselen over cyber kwetsbaarheden, cyber aanvallen, verstoringen, oplossingen en best-practices. Ook is het wenselijk om samen voorbereid te zijn op een verstoring. Dit door middel van jaarlijkse gezamenlijke oefeningen die inzicht geven in welke acties ondernomen moeten worden door iedere partij in de keten mocht een incident zich voordoen.

Informatie-uitwisseling en samenwerking vormen dan ook de sleutel naar vergroting van de weerbaarheid tegen digitale verstoringen en het ondersteunen van de bedrijfscontinuïteit binnen het Haven Industrieel Complex. Voor met name kleinere organisaties is het niet of nauwelijks mogelijk dit zelfstandig te organiseren, maar wel noodzakelijk om hun bedrijfsprocessen te beveiligen, hun bestaansrecht te behouden en de impact op de rest van de keten beperkt te houden.

2.2 Ambitie en doel

Onze ambitie: “Rotterdam bevindt zich in 2023 in de top van de wereld ten aanzien van het weerbaar zijn tegen digitale verstoringen.” Dat wil zeggen dat het Haven Industrieel Complex in Rotterdam digitale dreigingen - zoveel als mogelijk is - ziet aankomen en zo georganiseerd is dat het de impact van digitale verstoringen weet te beheersen. *Hierdoor wordt de bedrijfscontinuïteit ondersteund, en het veiligheidsrisico voor omwonenden verkleind en wordt eventuele economische schade beperkt gehouden.*

Wij ambiëren dat in 2023 relevante partijen samenwerken om de impact van digitale verstoringen bij bedrijven en in de ketens op het Haven Industrieel Complex in Rotterdam te beheersen. De naam van het samenwerkingsverband is ‘FERM’. Relevante betrokken partijen zijn diverse publieke

organisaties en alle ondernemingen binnen het Haven Industrieel Complex. Met name de ondernemingen die een kritieke schakel zijn in de functie van de Rotterdamse haven zijn hierbij aangesloten. FERM wordt door deze partijen als dé onmisbare schakel tussen alle partijen gezien. De meerwaarde van FERM wordt gezien en gewaardeerd en dat vertaalt zich door in operationele en financiële participatie van alle bij FERM aangesloten organisaties.

3. How – hoe pakken we dat aan?

3.1 Een coöperatieve filosofie en aanpak

Het vergroten van de weerbaarheid tegen digitale verstoring in het Haven Industrieel Complex kunnen we alleen samen oplossen. Dit vergt een coöperatieve aanpak:

met elkaar:	samen staan we sterk
voor elkaar:	ik help jou, jij helpt mij
door elkaar:	samen lossen we het op

Een verstoring of bewuste aanval is niet uit te sluiten. Door binnen het Haven Industrieel Complex samen te werken maken de bij FERM aangesloten organisaties zichzelf en elkaar wel meer weerbaar tegen deze verstoringen en aanvallen. De impact op het Haven Industrieel Complex en de maatschappij in het algemeen wordt daardoor beperkt gehouden.

3.2 Deelnemersprofiel - Partners en Participanten van FERM

Partners

FERM is een organisatie van, voor en door publieke en private partijen in het Haven Industrieel Complex. De deelnemende publieke organisaties nemen deel vanuit hun maatschappelijk taak en opdracht. De urgentie tot samenwerken is gebaseerd op hun verantwoordelijkheid naar de samenleving om de consequenties van digitale verstoringen (zoals veiligheidsrisico's, milieurisico's en verlies van economische waarde) te verkleinen. Deze maatschappelijke taak kan samen beter, sneller en goedkoper worden uitgevoerd dan wanneer iedere partij dit individueel op zou pakken. Dit komt doordat beschikbare kennis over dreigingen, kwetsbaarheden, aanvallen en oplossingen binnen het FERM-samenwerkingsverband worden gedeeld.

Vier partijen hebben het financieel mogelijk gemaakt dat FERM tot stand is gekomen. Daarnaast is sinds 2020 de Veiligheidsregio Rotterdam – Rijnmond (VR-RR) tot de groep financierende partners toegetreden. De vijf financierende ***'Partners van FERM***' zijn:

1. Havenbedrijf Rotterdam - Divisie Havenmeester
2. Politie
3. Gemeente Rotterdam
4. Deltalinqs
5. Veiligheidsregio Rotterdam - Rijnmond

Samen met het Openbaar Ministerie en DCMR vormen zij de startkern van FERM.

Met DCMR en de Douane lopen nog gesprekken over het toetreden als financierende partner.

Participanten

Het Haven Industrieel Complex bestaat uit circa zevenhonderd private organisaties en diverse publieke partijen. Alle organisaties die aangesloten zijn bij FERM en die niet behoren tot de financierende partners noemen we de '***Participanten van FERM***''. Van participanten van FERM wordt verwacht dat ze een actieve deelname hebben, zoals het delen van dreigingen, incidenten en best-practices.

Alle organisaties uit het Haven Industrieel Complex kunnen deelnemen; het maakt niet uit hoe een organisatie de kantoorautomatisering (IT) of industriële automatisering (OT) heeft georganiseerd. Ook organisaties die de automatisering volledig hebben uitbesteed hebben baat bij deelname. Wel hanteert FERM een basale ondergrens van informatiebeveiliging en industriële beveiliging. Bij toetreding neemt iedere participant een cyberweerbaarheidsscan af waarmee de huidige stand van IT en OT security op hoofdlijnen wordt getoetst. Soms zal het advies zijn om een aantal (vaak organisatorische) maatregelen te treffen om beter aan te sluiten op het niveau van IT en OT Security van de andere participanten. Participanten kunnen elkaar onderling helpen met best-practices. Ook kan de nieuwe participant elders hulp inroepen om de adviezen uit de cyberweerbaarheidsscan op te volgen.

Ter verduidelijking: deze cyberweerbaarheidsscan is een eerste hygiëne slag, het biedt **geen** certificering. Wel toont een organisatie door participant te zijn van FERM aan dat het minimaal eraan werkt om de basis op orde te krijgen *en* dat de organisatie werk maakt van cyberweerbaarheid. Tot slot zal de deelname van nieuwe participanten vooraf worden voorgesteld en getoetst worden aan de huidige deelnemers.

De belangrijkste redenen voor een organisatie om te participeren in FERM zijn:

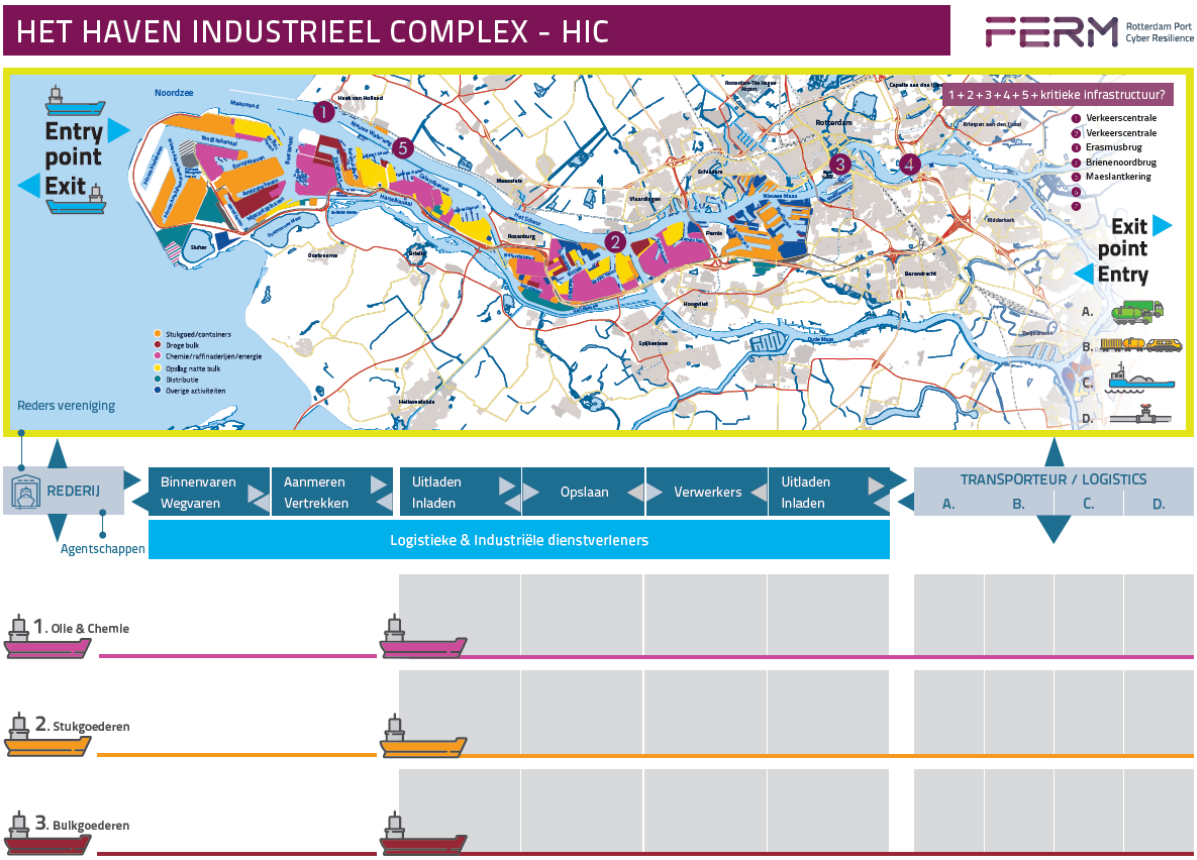
- uitval van IT-systemen (kantoorautomatisering) of OT systemen (procesautomatisering) kan flinke gevolgen hebben voor de omzet en/of bedrijfsvoering van de organisatie;
- haar klanten eisen een (aantoonbare) mate van informatiebeveiliging;
- de organisatie is een kritieke schakel binnen het Haven Industrieel Complex en het is haar economische en maatschappelijke verantwoordelijkheid om de impact van digitale verstoringen beperkt te houden.

Ketens en sleutelsectoren

De slagaders van de bloedsomloop van het Haven Industrieel Complex zijn de volgende vijf ketens en sleutelsectoren:

1. de keten Olie en Chemie (olieraffinage en procesindustrie);
2. de keten Stukgoederen (containerlogistiek en breakbulk);
3. de keten Bulkgoederen (droge massagoed en tankopslag);
4. de sleutelsector Logistieke dienstverleners (loodsen, sjorders, roeiers etc);
5. de sleutelsector Industriële dienstverleners (energie, water, onderhoud etc.).

In afbeelding 3.1 zijn deze ketens en sleutelsectoren in beeld gebracht samen met de partijen die een dominante (marktmacht) of kritieke (risico's voor keten en HIC) rol innemen. Het is belangrijk zo niet noodzakelijk deze dominante en kritieke partijen in een vroege fase van de ontwikkeling van FERM te laten participeren. Het marketingplan is dan ook gericht op deze spelers.

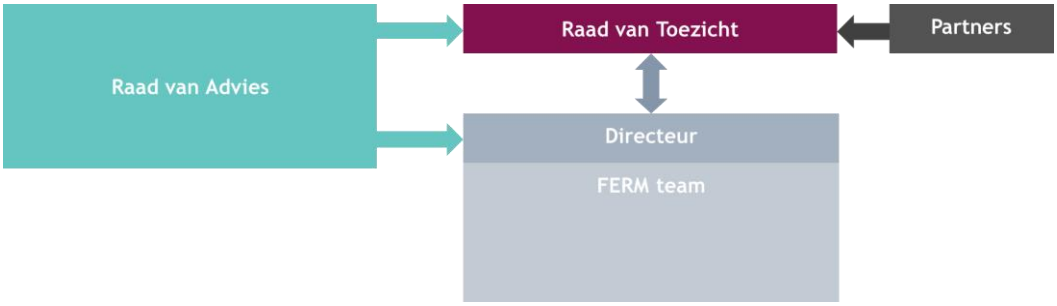


Afbeelding 3.1: Partijen met een dominante of kritieke rol in het Haven Industrieel Complex

3.3 Rechtsvorm

FERM is een stichting met één directeur-bestuurder. Deze directeur-bestuurder legt verantwoording af aan een Raad van Toezicht. De Raad van Toezicht (RvT) bestaat uit drie zeer ervaren bestuurders met expertise in de domeinen bedrijfsvoering, financiën en cybersecurity. De Raad van Toezicht houdt toezicht op de algehele besturing en richting van FERM en krijgt het jaarplan van FERM ter accordering voorgelegd.

Naast de RvT wordt een Raad van Advies (RvA) geïnstalleerd. Deze RvA vervangt de huidige werkgroep FERM. De Raad van Advies heeft het karakter van een cliëntenraad en bestaat uit vertegenwoordigers van de financierende partners en een vertegenwoordiging van de participanten. De RvA geeft collectief gevraagd en ongevraagd advies aan de directeur en de RvT over de koers en groeirichting van FERM en geeft input voor het jaarplan, geeft advies over de te ontwikkelen diensten en is een ambassadeur van FERM. In afbeelding 3.2 is het organogram van de stichting FERM weergegeven.



Afbeelding 3.2 – Organogram FERM (project)organisatie

3.4 Team en expertise

FERM start in Q4 2020 met een compacte organisatie onder leiding van een directeur (in eerste instantie een ingehuurde projectmanager). Deze directeur is de spin in het FERM web en zal leiding geven aan de andere medewerkers en externe inhuur. Bij de start bestaat er een kernteam van drie personen bestaande uit een directeur, threat intel moderator en een officemanager. Dit team heeft een voorziene capaciteit van 1,2 voltijdsbanen (fte). Naar gelang de behoefte kan de bezetting worden aangepast. Wanneer de stichting FERM is opgericht komen deze personen in dienst van (of worden ingehuurd door) de stichting FERM, voor die tijd worden ze ingehuurd door de projectorganisatie.

In afbeelding 3.3 zijn de vijf voorziene functieprofielen weergegeven. De werkgroep (Raad van Advies) wordt gevraagd te assisteren bij de selectie van de medewerkers.

3.5 Fysieke locatie

FERM zal bij de start in 2020 fysiek gevestigd zijn bij Havenbedrijf Rotterdam. In de vervolgfase wordt onderzocht welke opties er zijn voor permanente vestiging. FERM zal naar verwachting drie fysieke werkplekken innemen en zorgt zelf voor benodigde hardware en software.[3]

4. What – wat gaan we doen en leveren?

4.1 Onze belofte

Digitale weerbaarheid is niet in één dag georganiseerd. Het naar een hoger niveau tillen van de digitale weerbaarheid van het Haven Industrieel Complex vraagt constante inspanningen. Partners en participanten van FERM spelen hierin de voornaamste rol. FERM zelf faciliteert, adviseert en spant zich in om de deelnemende organisaties te helpen bij het voorkomen en tijdig herkennen van verstoringen, om zo de impact van mogelijke verstoring zo klein mogelijk te houden.

Primair ligt en blijft de verantwoordelijkheid voor cyberweerbaarheid bij de bedrijven zelf. FERM en deelnemende organisaties zijn nadrukkelijk niet verantwoordelijk voor de cyberweerbaarheid van de deelnemende organisaties en zijn niet aansprakelijk voor eventuele schade door cybercriminaliteit. Wél is FERM - door de aanwezigheid van expertise, diensten, kennis en informatie - het centrale knooppunt ten aanzien van digitale weerbaarheid in het Haven Industrieel Complex. FERM is een knooppunt waar mensen en organisaties samenkomen, samenwerken en samen streven naar digitale weerbaarheid. FERM is geen nieuwe aanbieder maar dé plek waar bedrijven elkaar onderling helpen. FERM biedt tevens een platform voor bestaande leveranciers die hun diensten aan FERM participanten kunnen leveren via een formeel aanbestedingstraject.

[3] Over gebruik van het wifinetwerk, printers, e.d. zullen aanvullende afspraken met het Havenbedrijf Rotterdam worden gemaakt.

4.2 Onze diensten

FERM biedt diverse diensten die zijn onder te verdelen in vijf categorieën: Identificatie, Bescherming, Detectie, Reactie, Herstel. [4] In afbeelding 4.1 staat een beknopt overzicht. Een aantal diensten worden door FERM-medewerkers geleverd, andere diensten worden ingekocht. Hiervoor maakt FERM de eerste jaren gebruik van de inkoopafdeling en inkoop- en leveringsvoorwaarden van het Havenbedrijf Rotterdam.

Directeur
(Evelien Bras)

Taken en verantwoordelijkheden:

- Besturing van de juridische entiteit FERM
- Aansturing van medewerkers van FERM
- Eindverantwoordelijk voor intake van nieuwe participanten
- Aanspreekpunt voor publieke partijen
- Contact voor (toekomstige) participanten op C-level
- Vertaling trends en ontwikkelingen naar dienstverlening
- Eindverantwoordelijke voor externe publicaties van FERM

Vereiste ervaring en kennis:

- Ervaring binnen het Haven Industrieel Complex
- Affiniteit met cybersecurity
- Bestuurlijke ervaring
- Afgeronde HBO of Bacheloropleiding
- Minimaal 10 jaar werkervaring, waarvan 3 jaar bestuurlijk
- Uitstekende beheersing van Nederlandse en Engelse taal
- Bezit een actief netwerk binnen landelijke en regionale samenwerkingsverbanden

Threat Intelligence Moderator
(Marrison Toussaint e/o Yu Mei Liebregt)

Taken en verantwoordelijkheden:

- Beheer van informatie die binnenkomt (Informatie beoordelen op urgentie, onderwerp, betrouwbaarheid, echtheid en relevantie voor bepaalde ontvangers en deze informatie groeperen. Informatie waar nodig verrijken met een handelingskader/ -perspectief voor de ontvangers)
- Coördinatie technische intake nieuwe participanten
- Vertaling trends en ontwikkelingen naar externe (markt)communicatie.

Vereiste ervaring en kennis:

- Thuis in cybersecurity terminologie en ervaring met het werken met cybersecurity gerelateerde informatie (zowel op strategisch, tactisch als operationeel niveau).
- In staat bij te dragen aan positionering van FERM en vergroten betrokkenheid participanten
- In staat nieuwe participanten technisch te 'onboarden'.
- Afgeronde HBO of Bacheloropleiding
- Minimaal 8 jaar werkervaring, waarvan 5 jaar op het gebied van cybersecurity
- Bij voorkeur ervaring binnen het HIC
- Een CISSP, CISA, CISM, RE, CEH of vergelijkbare certificering
- Uitstekende beheersing van Nederlands en Engels

Commercieel medewerker
(vacature)

Taken en verantwoordelijkheden:

- Werven van nieuwe participanten
- Onderhouden van netwerk met diverse private en publieke partijen

Vereiste ervaring en kennis:

- Gedegen cybersecurity kennis; weet wat er speelt binnen dit vakgebied
- Actief netwerkwerk binnen het Haven Industrieel Complex
- Afgeronde HBO of Bacheloropleiding.
- Minimaal 8 jaar werkervaring waarvan minimaal 4 in het vakgebied cybersecurity en minimaal 4 in de commercie.

Officemanager/ Managementassistent
(Vivianne Sanderse)

Taken en verantwoordelijkheden:

- Centrale contactpunt voor bestaande participanten
- Uitvoeren administratieve werkzaamheden, zoals bijhouden participanten administratie en uitvoeren van facturatie
- Ondersteunen bij fysieke bijeenkomsten en evenementen
- De marketing- en communicatieadviseur helpen met het schrijven over ontwikkelingen omtrent FERM
- Helpen onderhouden van externe website

Vereiste kennis en ervaring

Communicatieadviseur
(Rob Nijman)

Taken en verantwoordelijkheden:

- Ontwerp en executie van marketingactiviteiten om de producten en diensten van FERM aan te prijzen om participanten en leveranciers te werven.
- Vertaling van trends en ontwikkelingen naar externe (markt) communicatie
- Realisatie externe publicaties zoals trendrapportages
- Eindverantwoordelijk voor externe publieke website

Vereiste ervaring en kennis:

- Frisse ideeën over positionering van FERM en vergroten betrokkenheid participanten

[4] Afkomstig uit de internationale NIST cybersecurity richtlijn.

	• Affiniteit met cybersecurity • Administratief sterk • In staat zelfstandig te werken • Houdt van afwisselende en veelzijdige werkzaamheden • In staat nieuwe participanten te 'onboarden' • Afgeronde mbo-opleiding administratieve ondersteuning • Minimaal 8 jaar ervaring in soortgelijke functies waarvan minimaal 2 jaar als directie assistent • Uitstekende beheersing van de Nederlandse en Engelse taal	• In staat voortouw te nemen voor externe communicatie en inzet van benodigde materialen en kanalen • Afgeronde HBO of Bacheloropleiding • Minimaal 5 jaar werkervaring als marketeer • Bij voorkeur ervaring binnen het HIC • Affiniteit met cybersecurity • Uitstekende beheersing van de Nederlandse en Engelse taal • Goede persrelaties

Afbeelding 3.3: Functieprofielen medewerkers FERM

Diensten die vrij toegankelijk zijn
FERM vervult een maatschappelijke rol in het Haven Industrieel Complex en biedt niet alleen diensten aan de partners en participanten die zich hebben aangesloten bij FERM, maar biedt ook diensten aan partijen die zich niet hebben aangesloten. FERM heeft een publiek toegankelijke **website** (https://ferm-rotterdam.nl/) met allerlei praktische tips en tricks, handige documenten en relevante nieuwsberichten. Op deze website kunnen geïnteresseerden zich ook inschrijven voor de **nieuwsbrief** die elke twee maanden uitkomt. Tevens organiseert Deltalinqs onder de noemer van FERM vier tot vijf keer per jaar het **Port Cyber Café**. Hierin komen actuele cybersecurity onderwerpen aan bod, worden relevante kennis en ontwikkelingen gedeeld en worden er interactieve oefeningen gehouden. Het Port Cyber Café is publiek toegankelijk. Wel zal er bij aanmelding voorrang worden gegeven aan partners en participanten van FERM.

In enkele gevallen is een ontdekte kwetsbaarheid dusdanig ernstig dat FERM haar volledige mailinglist (alle partners, participanten en allen die zich voor de nieuwsbrief hebben ingeschreven) voorziet van **een email met informatie vanuit het Digital Trust Center over een acute dreiging.** Het Digital Trust Center, onderdeel van het Ministerie van Economische Zaken en Klimaat, stuurt dit soort e-mails uit om organisaties in Nederland te beschermen.

Doelgroep NIST Categorie	Publieke dienst voor iedereen in het Haven Industrieel Complex	Standaard dienst als onderdeel van het lidmaatschap (Basispakket)	Optioneel verdere samenwerking door gezamenlijke inkoop via FERM
Identificatie		• *Cyberweerbaarheidsscan* • *Onderlinge anonieme benchmark*	• *Aanvullend implementatieadvies n.a.v. cyberweerbaarheidsscan*
Bescherming	• Website • Nieuwsbrief • Port Cyber Café	• Vast tarief bij geselecteerde IT en OT security bedrijven voor advies en implementatie.	• *Awareness campagnes*
Detectie	• Acute dreigingen informatie vanuit DTC	• Actuele en relevante algemene dreigingsinformatie	• *Bedrijfs- en systeem specifieke dreigings-informatie en duiding* • *SOC/SIEM*
Reactie		• *Jaarlijkse gezamenlijke cyberoefening*	• *Incident response* • *Digital forensics*
Herstel		• Jaarlijks algemeen Cyber Security Beeld Rotterdamse Haven	
Alle categorieën		• *Collaboratie portal Standaardtraining en -opleiding van praktische kennis* • Werkgroepen om samen onderwerpen op te pakken	• *Aanvullende training en opleiding (maatwerk en meerdaagse training)*

Afbeelding 4.1: Dienstverlening FERM - *schuingedrukte diensten* worden extern ingekocht

Diensten voor betalende partners en participanten (basispakket)
Aan partners en participanten van FERM worden aanvullende diensten geboden. In dit zogenaamde basispakket zit een initiële ***cyberweerbaarheidsscan*** gebaseerd op de Cybersecurity Health Check

voor MKB gepubliceerd door de Cyber Security Raad. De cyberweerbaarheidsscan geeft inzage in het actuele cybersecurity-volwassenheidsniveau van de organisatie en geeft een overzicht van maatregelen die genomen kunnen worden om de weerbaarheid te vergroten. De weerbaarheidsscan kan worden ingezet op (een deel van) de IT of OT-infrastructuur afhankelijk van waar het zwaartepunt van de organisatie zich bevindt. De uitkomsten van de scan worden niet gedeeld met FERM, maar alleen met de organisatie waar de scan is uitgevoerd. Als uit de cyberweerbaarheidsscan blijkt dat een participant nog bepaalde acties kan ondernemen om het securityniveau te verhogen, kan deze participant ervoor kiezen om andere participanten en/of leveranciers te vragen te helpen met advies en best-practices, maar dat hoeft natuurlijk niet.

De cyberweerbaarheidsscan wordt periodiek (eens per 1 of 2 jaar) herhaald in de vorm van een ***onderlinge anonieme benchmark***. Participanten die laag scoren op de benchmark kunnen bij andere participanten terecht voor tips ter verbetering. Op deze manier draagt FERM bij aan het continu verbeteren van de digitale weerbaarheid van alle participerende organisaties. Omdat de benchmark anoniem is, kan via FERM hulp bij collega participanten ingeroepen worden.

Participanten van FERM kunnen gebruik maken van een **vast tarief bij geselecteerde IT- en OT security leveranciers voor advies en implementatie.** Door inzet van deze dienstverleners kunnen participanten hun weerbaarheid verhogen o.a. door het afnemen van diverse consultancy diensten, waaronder penetratietesten, compliance checks en code reviews. De participanten organiseren en betalen de opdracht zelf maar behalen inkoopvoordeel door de dienstverlening via FERM af te nemen.

FERM biedt partners en participanten **actuele en relevante dreigingsinformatie** door meldingen vanuit het NCSC, DTC en andere partners te duiden en delen. Partners en participanten worden gestimuleerd ook onderling relevante informatie te delen. FERM zal alle informatie voorzien van een duiding: waar doet de dreiging of kwetsbaarheid zich voor, wat is het potentiele risico en hoe kan de dreiging afgewend worden. Deze informatie wordt op allerlei manieren gedeeld waaronder via een digitaal ***collaboratie portal***. Dit portal zullen partner en participanten tevens gebruiken om allerlei andere informatie en best-practices met elkaar te delen. Zodra de behoefte bestaat om een bepaald actueel onderwerp verder uit te diepen, zal FERM **werkgroepen** creëren waarin participanten samen met dit onderwerp aan de slag gaan. Een bijvoorbeeld is het samen opstellen van een korte instructie over OT-security in de haven voor toezichthouders.

Verder organiseert FERM minimaal eens per jaar een ***gezamenlijke cyberoefening***. Partners en participanten kunnen hieraan deelnemen op vrijwillige basis. De oefening is erop gericht om bewustzijn te creëren over crisismanagement. Ook bevat de oefening een trainingselement om vertegenwoordigers van de organisatie de basis van cybercrisismanagement bij te brengen.

FERM stelt ieder jaar op basis van de haar beschikbare informatie een '**Cyber Security Beeld Rotterdamse Haven**' op. Dit is een rapport over de ontwikkelingen op het gebied van cybersecurity en cyberdreigingen in de Rotterdamse haven. Het is bedoeld om publieke partijen, zoals de gemeente, provincie en ministeries, en bestuursleden van organisaties in het Haven Industrieel Complex bewust te maken over wat er speelt.

FERM organiseert ***standaard trainingen en opleidingen*** voor werknemers van partners en participanten. Deze trainingen en opleidingen zijn gericht op het bijbrengen van praktische en technische kennis. Met deze kennis kunnen organisaties zelf aan de slag het weerbaarheidsniveau in

hun eigen organisatie te verhogen. De onderwerpen worden gezamenlijk door de partners en participanten van FERM vastgesteld waarna een externe partij de training of opleiding zal leveren.

Optioneel verdere samenwerking door gezamenlijke inkoop via FERM
Naast het standaardpakket van dienstverlening kunnen partners en participanten besluiten om samen additionele diensten in te kopen. Het staat de individuele partner/participant vrij om hieraan mee te doen. Voor drie van de zeven voorzien optionele diensten zijn reeds dienstverleners gecontracteerd. Deze worden hieronder toegelicht.

Zo kunnen participanten naar aanleiding van de cyberweerbaarheidsscan een ***aanvullend implementatieadvies*** bij de dienstverlener afnemen. Dit tegen een vooraf vastgesteld tarief, hiermee behalen participanten een inkoopvoordeel.

Verder biedt FERM partners en participanten de mogelijkheid om optioneel ***bedrijfs- en systeemspecifieke dreigingsinformatie*** af te nemen. Deze informatie wordt vergaard door continu het Internet, social media en het dark-web te monitoren op steekwoorden die relevant zijn voor het havengebied, de partners en de participanten. Zo krijgen partners en participanten die deze dienst afnemen specifiek op de organisatie gerichte relevante dreigingsinformatie. Ook krijgen deelnemende organisaties proactief informatie over significante kwetsbaarheden in vooraf bepaalde relevante IT en OT-platformen. Hierop kunnen partners en participanten snel maatregelen nemen om hun IT en OT-omgeving veilig te houden.

Ook zal FERM de mogelijkheid bieden om optioneel ***aanvullende training en opleiding (maatwerk en meerdaagse training)*** af te nemen. Te denken valt aan het tegen een vast tarief afnemen van in-company training of het laten ontwikkelen van specifieke training die participanten samen met elkaar afnemen.

Tot slot, andere dienstverlening die additioneel via FERM kan worden geleverd is bijvoorbeeld het gezamenlijk laten ontwikkelen van ***awareness campagnes*** of het gezamenlijk inkopen van ***SOC/SIEM***, ***Incident response*** of ***digital forensics*** diensten.

4.3 Prijsstrategie

In de prijsstrategie onderscheiden we partners en participanten. **Partners** zijn de zeven partijen (Havenbedrijf Rotterdam – Divisie Havenmeester, Politie, Gemeente Rotterdam, Veiligheidsregio Rotterdam – Rijnmond, Deltalinqs, DCMR en de Douane).

Partners
Partners verbinden zich voor een periode van drie jaar aan FERM. 5 van de 7 partners hebben in 2020 reeds € 25.000 bijgedragen en worden ook in de toekomst gevraagd om een bijdrage

Participanten
Alle participanten betalen éénmalig een entree bijdrage van € 1.500 en krijgen daarvoor een onboarding die bestaat uit registratie bij FERM, aansluiting op het digitale platform en een cyberweerbaarheidsscan. Daarna verbindt de organisatie zich voor een periode van drie jaar. In uitzonderlijke gevallen kan de samenwerking tussentijds worden ontbonden.

De bijdrage is niet afhankelijk van de omvang van de organisatie. Hiervoor is bewust gekozen, omdat doorgaans grotere organisaties naast de financiële bijdrage vaak ook meer zullen bijdragen in kennis en best-practices. De directeur kan op basis van op te stellen jaarplannen aan de Raad van Toezicht en Raad van Advies voorstellen om de participantenbijdrage te verhogen of verlagen.

De participantenbijdrage voor het basispakket is vastgesteld op € 3.500 per jaar. De additionele dienstverlening wordt (deels) voor een vast tarief vastgelegd. De prijsopgave is op aanvraag beschikbaar.

4.4 Samenwerkingspartners

Met name de additionele dienstverlening, maar ook de cyberweerbaarheidsscans zullen zoveel mogelijk door externe, door FERM geselecteerde, leveranciers geleverd worden. Door het bundelen van de vraag door FERM kunnen inkoopvoordelen worden gerealiseerd. De directeur stelt de lijst van leveranciers op. De Raad van Toezicht ziet erop toe dat de leveranciersselectie op een correcte wijze verloopt.

Een van de belangrijkste samenwerkingspartners is het Havenbedrijf Rotterdam. Deze partner levert de huisvesting en kennis voor de nieuwe organisatie. Ook Deltalinqs is een belangrijke samenwerkingspartner. Zij verzorgt de Port Cyber Cafés en levert samen met het Havenbedrijf Rotterdam belangrijke kennis over mogelijke participanten.

FERM zal ook intensief gaan samenwerken met de Haven-ISAC. Deze samenwerking bestaat uit het wederzijds uitwisselen van informatie over dreigingen, data en best-practices onder TLP:green en TLP:white. Daarnaast zal de Haven-ISAC de door haar uitgewerkte kennis, aanpak en ideeën delen met FERM. Ieder jaar kan een delegatie van de FERM participanten kennis opdoen bij bedrijven uit de Haven-ISAC door middel van een bedrijfsbezoek.

Tenslotte heeft FERM nauw contact met het Digital Trust Center (DTC) van het Ministerie van Economische Zaken en Klimaat en met het Nationaal Cyber Security Center (NCSC) van het Ministerie van Justitie en Veiligheid. Het NCSC en FERM zijn voornemens om wederzijds informatie uit te wisselen indien dit binnen vigerende regelgeving is toegestaan. Het gaat om het delen van het jaarlijkse Dreigingsbeeld FERM met het NCSC, het delen van TLP:white informatie vanuit FERM met het NCSC en het delen van dreigingsinformatie vanuit NCSC met FERM binnen de Objectief Kenbare Taak tot informatiedeling (OKTT).