FERM Rotterdam Port Cyber Resilience

“Met de veilige haven in zicht”

Cyberbeeld Haven Industrieel Complex 2022

Versie: 1.0 d.d. 18 oktober 2022

Inhoudsopgave

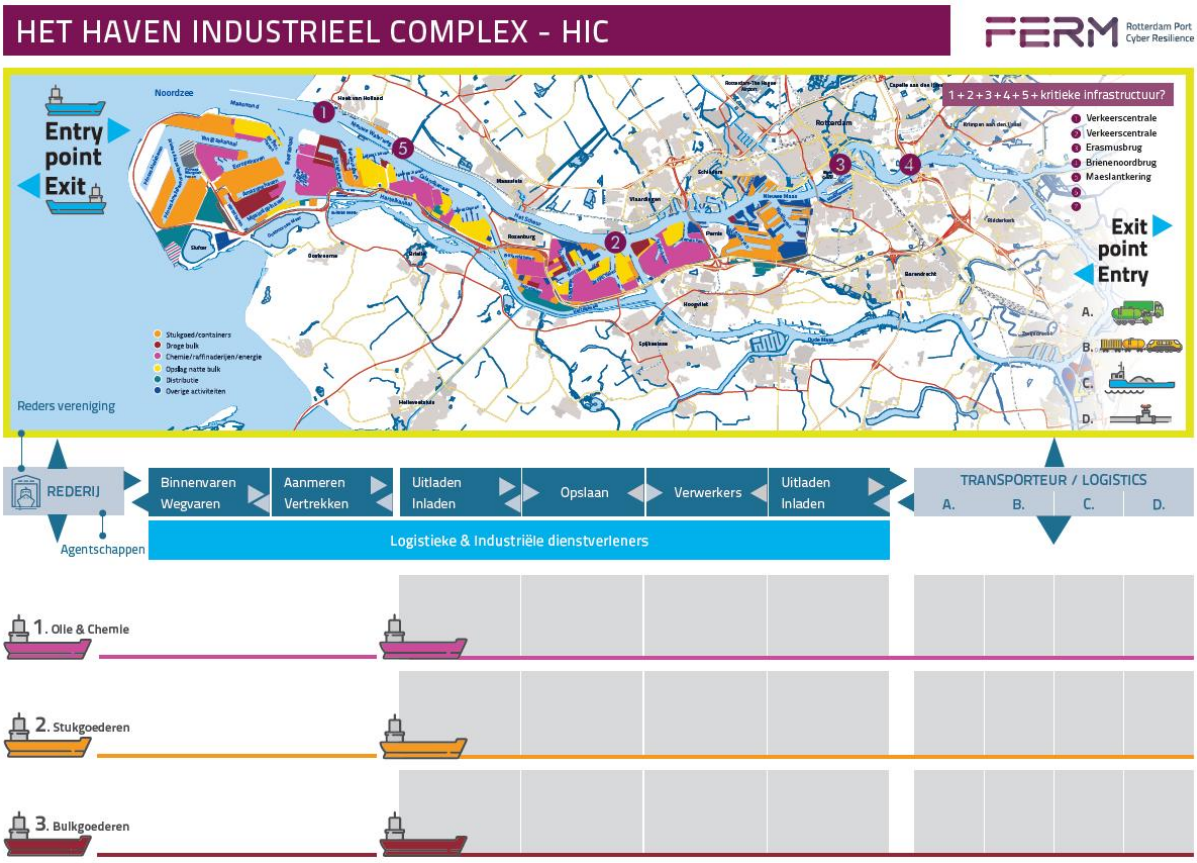
1. Doel: een digitale weerbaar Haven Industrieel Complex

1.1 Het Haven Industrieel Complex als internationale gateway

Nederland dankt € 15,9 miljard van zijn toegevoegde waarde direct aan de Rotterdamse haven[1]. De indirecte toegevoegde waarde wordt geschat op € 45,6 miljard. De haven biedt - direct en indirect - plaats aan meer dan 355.000 werknemers[2] en is direct verbonden met de aanvoer van producten die inwoners van Nederland dagelijks nodig hebben.
De continuïteit en efficiëntie van de processen die plaatsvinden in de haven zijn daarmee essentieel en van vitaal belang voor Nederland.

Maar niet alleen voor Nederland is de Rotterdamse Haven essentieel, ook Europees gezien heeft zij een belangrijke functie: De haven van Rotterdam is de grootste haven van Europa en veel goederen die hier aankomen worden vervoerd richting het Europese achterland. Denk daarbij aan olie-opslag en verwerking, container overslag maar ook militaire mobiliteit. Daarmee is de Rotterdamse haven ook op Europees niveau van essentieel belang.

Maar wat is nu precies dé haven? Wie is ervoor verantwoordelijk?
De haven is een geraffineerd samenspel van zo'n 700 organisaties actief in verschillende sectoren met verschillende toezichthouders.



[1] https://havenmonitor.nl/onewebmedia/Havenmonitor%202021%20-%20Eindrapport%20Erasmus%20UPT.pdf
[2] https://www.portofrotterdam.com/sites/default/files/downloads/het-rotterdam-effect-pdf.pdf

1.2 Risico met impact door onderlinge verbondenheid

Zoals beschreven, is de haven een geraffineerd samenspel van zo'n 700 organisaties actief in verschillende sectoren. Organisaties die digitaal met elkaar verbonden zijn, deels dezelfde infrastructuur of applicaties gebruiken of gebruik maken van de zelfde fysieke ruimte. Een digitaal incident in elk van deze organisaties kan potentieel de goede werking van de Rotterdamse haven in zijn geheel verstoren.
Alle organisaties in het Haven Industrieel Complex hebben daarmee een gezamenlijke rol - en verantwoordelijkheid - voor de digitale veiligheid van het havencomplex als geheel.

De cyberaanval op APM Terminals/Maersk in juni 2017 maakt de kwetsbaarheid en afhankelijkheid zichtbaar. NotPetya was ontworpen in de destijds digitale, nu hybride, oorlog tussen Rusland en Oekraïne. Dit incident veroorzaakte naar schatting rond $300 miljoen dollar schade bij Maersk zelf en daarnaast had het dagenlang impact op de logistieke afhandeling van het Haven Industrieel Complex.

Er is overigens wel veel veranderd sinds 2017. De cyberweerbaarheid van individuele bedrijven is gegroeid, maar ook de mate van digitalisering. Daarnaast is ook de onderlinge verbondenheid toegenomen en dankzij deze sterkere verbondenheid in verschillende ketens is ook de impact van organisaties op elkaar, in geval van een incident, groter geworden.

Afgelopen jaar, in juli 2021, zagen we bijvoorbeeld als gevolg van het incident van de EverGiven, die onderweg was naar Rotterdam, een verstoring in de wereldwijde logistieke processen. Eén schip overdwars in het Suez kanaal veroorzaakte verstoringen die na maanden nog steeds merkbaar waren.
De oorzaak van het incident was weliswaar niet digitaal, het geeft wel aan dat de ketens gevoelig(er) zijn voor een enkele verstoring.

1.3 Wat is het doel van het FERM cyberbeeld?

In dit document ligt de focus op cybersecurity van het Haven Industrieel Complex.

Cybersecurity heeft in haar aard zowel geografische als sectorale aspecten en een cyberbeeld staat nooit op zich. Met dit als uitgangspunt is het “FERM cyberbeeld” opgebouwd uit cyberbeelden vanuit andere invalshoeken.
Daarnaast beschrijft dit document de beelden die komen uit eigen bevindingen, daar waar complementair op voorgaande, en vertaalt het totaal door naar suggesties voor de individuele organisaties, ecosysteem- en ketenpartners en uiteindelijk ook naar FERM zelf.

1.4 Structuur van de inhoud

Aan de ene kant is in dit document zoveel mogelijk gekeken naar ingrediënten voor scenario’s; gebaseerd op een risico-matrix ontstaan uit externe dreigingen, interne dreigingen, assets en de toegevoegde waarde daarvan, alsook de juridische aspecten.
Aan de andere kant is gekeken naar de mogelijkheden voor ‘identify’, ‘detect’, ‘protect’, ‘response’, ‘recover’ conform het NIST-cybersecurity framework[3].

[3] https://www.nist.gov/cyberframework

2.Samenvatting cyberbeelden andere partijen

2.1 Cybersecuritybeeld Nederland 2022

De NCTV - Nationaal Coördinator Terrorismebestrijding & Veiligheid - brengt jaarlijks het “Cybersecuritybeeld Nederland” uit. Deze is bijgevoegd als bijlage 1 aan dit document. Samengevat:

Om ongestoord te kunnen functioneren, moeten we onze samenleving zo goed als mogelijk beschermen tegen digitale dreiging. Ondanks de inspanningen om de weerbaarheid te verhogen, is er sprake van scheefgroei met de toenemende dreiging. Die scheefgroei vergroot het risico op ontwrichting van onze samenleving. Denk hierbij aan de bankensector, het openbaar vervoer, energievoorziening of drinkwater.

Het is niet zozeer de vraag óf bedrijven worden aangevallen, maar wanneer. Dit geldt voor de overheid, kennisinstellingen en andere organisaties. De basismaatregelen[4] op orde hebben helpt, maar deze zijn nog lang niet overal goed doorgevoerd. Er wordt nog te weinig gewerkt met onder meer multifactor authenticatie en het maken en testen van back-ups.

[4] https://www.ferm-rotterdam.nl/nl/basismaatregelen

Cyberaanvallen door andere landen: het nieuwe normaal

Cyberaanvallen door buitenlandse inlichtingen- en veiligheidsdiensten zijn niet meer zeldzaam te noemen. Landen gebruiken de digitale ruimte om geopolitieke voordelen te behalen. Vanuit Rusland zijn meerdere EU-lidstaten succesvol geraakt door cyberaanvallen en China heeft op grote schaal en langdurig politieke doelwitten in Europa en Noord-Amerika aangevallen. Maar ook cybercriminelen zijn onverminderd in staat grote digitale schade aan te richten. Criminelen hebben primair een financiële drijfveer, maar een aanval kan zoveel impact hebben dat de nationale veiligheid geraakt wordt.

Ook kunnen staten cybercriminelen inhuren, gedogen of onder druk zetten om cyberaanvallen uit te voeren. Dat er banden zijn tussen staten en cybercriminelen bleek onlangs nog in de oorlog in Oekraïne, toen cybercriminelen gelieerd aan Rusland, waarschuwden tegenstanders van Rusland aan te willen vallen.

Ransomware, zero-days en de cloud

Aanvallen met gijzelsoftware (ransomware) worden steeds vaker ingezet met dubbele of zelfs drievoudige afpersing. Hierdoor wordt niet alleen de primair getroffen organisatie afgeperst maar ook de klanten, partners of leveranciers daarvan. Het NCSC ziet verder een toename van het aantal zero-day kwetsbaarheden. Misbruik daarvan kan grootschalige impact hebben als de kwetsbaarheid in veelgebruikte software of hardware zit. Ook misbruik van de cloud komt in toenemende mate voor. Clouddiensten zijn de afgelopen jaren cruciaal onderdeel geworden van bedrijfsprocessen. Uitval of verstoring kan grootschalige gevolgen hebben voor Nederlandse organisaties en sectoren.

Polarisatie en internationale conflicten: voedingsbodem voor hacktivisten

De directe dreiging die richting Nederland uitgaat van hackerscollectieven is klein. Er kan echter wel een afgeleide dreiging bestaan als acties van hacktivisten verkeerd worden geïnterpreteerd en landen die zij aanvallen overgaan tot een tegenreactie.

2.2 Havenbedrijf Rotterdam

Het Havenbedrijf Rotterdam beheert, exploiteert en ontwikkelt de grootste haven van Europa. Hun cyberbeeld is opgenomen als bijlage 2 aan dit document. Samengevat:

> Het Havenbedrijf Rotterdam (HbR) staat middenin de maatschappij en vervult daar een vitale rol. Ontwikkelingen in de maatschappij raken HbR en andersom. Digitalisatie met de bijbehorende kansen en dreigingen is daar een belangrijk onderdeel van. Om zich te wapenen tegen de alsmaar toenemende informatiebeveiligingsrisico's ontvangt HbR jaarlijks een dreigingsbeeld welke aan FERM beschikbaar wordt gesteld om te delen met het HIC.
>
> De voornaamste dreigingen voor HbR zijn van generieke aard; ransomware, business e-mail compromise (BEC) en de kwaadwillende insider blijven de belangrijkste dreigingen.
>
> De impact van ransomware aanvallen is gestegen. De criminelen achter deze aanvallen blijven met nieuwe manieren komen om organisaties te dwingen tot betalen over te gaan. Door het plegen van ketenaanvallen worden in één aanval meerdere organisaties getroffen. De NCTV spreekt van een bedreiging voor de nationale veiligheid.
> In het dreigingsbeeld van dit jaar zien we dat de coronapandemie veelvuldig als thema in phishing- en andere e-mail gerelateerde aanvallen gebruikt wordt.
> De insider blijft ook in onze top 3 van belangrijkste dreigingen voor HbR staan. Niet omdat de gemiddelde medewerker onbetrouwbaar is, maar mocht er toch een keer een medewerker kwaad willen, dan bevindt deze zich in een goede startpositie om snel veel schade aan te richten.
>
> In dit dreigingsbeeld wordt extra aandacht besteed aan ketenaanvallen. Ze komen steeds meer voor en HbR is als regie-organisatie bij uitstek kwetsbaar voor dit soort aanvallen. Het verdient aanbeveling zich specifiek te wapenen tegen deze incidentsoort.

2.3 bijlage 3: Gemeente Rotterdam (paragraaf Haven)

Ook de gemeente Rotterdam heeft in 2022 een cyberbeeld uitgebracht. Deze is bijgevoegd als bijlage 3. Van dit document voegen we geen samenvatting toe maar de paragraaf die gaat over de Haven:

> Het belang van de haven van Rotterdam voor de regio is groot. Door de toenemende digitalisatie van de processen en voorzieningen binnen de haven is een passend niveau van cyberweerbaarheid essentieel.
>
> De haven van Rotterdam kent meerdere ontwikkelingen op het gebied van cyberweerbaarheid. Deze ontwikkelingen worden ondersteund door FERM. FERM is een stichting gericht op het stimuleren van samenwerking tussen bedrijven in de Rotterdamse haven en het verhogen van het bewustzijn van cyberrisico's om zo de best digitaal beveiligde haven van de wereld te worden.
>
> Het is van belang om te investeren in de cyberweerbaarheid van bedrijven in de Rotterdamse haven. De volwassenheid van deze bedrijven verschilt sterkt. Het zou goed zijn als beter zicht komt op het niveau van cyberweerbaarheid (de mate van cybervolwassenheid) van deze bedrijven. Vervolgens kan dit worden gekoppeld aan bijbehorende certificering.
>
> Ondanks de lopende initiatieven, is de aandacht voor cyberweerbaarheid nog niet genoeg. In het haven industrieel complex bevinden zich veel verschillende bedrijven en niet ieder bedrijf heeft de kennis of capaciteit om hun cyberweerbaarheid te vergroten. Ook zijn de middelen te veel gefragmenteerd binnen individuele organisaties beschikbaar. Het belang van de haven is stad overstijgend, maar middelen worden niet op dit niveau toegekend.
>
> Ondertussen worden de risico's steeds groter, doordat de manieren om aan te vallen ook innoveren. Voorbeelden van innovatie zijn de ontwikkeling van ransomware als een businessmodel en storage spoofing. Bij storage spoofing worden niet-bestaande opslagcapaciteiten en voorraden van grondstoffen verkocht. Voor bedrijven kan dit leiden tot reputatieschade, omdat hun naam en reputatie door cybercriminelen beschadigd worden.
> De cyberrisico's worden versterkt door ketenafhankelijkheden. Een incident kan leiden tot een domino-effect, waardoor een incident bij één organisatie effect kan hebben op andere organisaties. De ketenafhankelijkheden beperken zich niet tot de haven, maar werken door tot in de stad, de regio en daarbuiten. Verbinding tussen de haven en de stad en regio kan helpen om samen sterker te worden.
> De haven van Rotterdam is de grootste haven van Europa. De Nederlandse overheid heeft de haven van Rotterdam aangewezen als één van de twee mainports van Nederland. De status mainport duidt op het grote belang voor de Nederlandse economie. De omvang van de Rotterdamse haven zorgt enerzijds voor economische kansen voor het gebied, maar vormt anderzijds tevens een bedreiging als een interessant target voor kwaadwillende actoren.

Haven

Sterkten

- Meerdere initiatieven in de haven om cyberweerbaarheid te versterken, ondersteund door stichting FERM.
- De maritieme sector maakt middelen beschikbaar voor het verhogen van hun cyberweerbaarheid.

Zwakten

- Grote diversiteit aan organisaties in de haven waardoor ketensamenwerking complex en niet altijd voor de hand liggend is.
- Basis ICT beveiliging bij veel organisaties niet op orde.
- Digivaardigheden van personeel zijn te laag.

Kansen

- Bedrijven in de haven meer sturen op volwassenheidsniveaus in plaats van individuele maatregelen.
- Bevoegdheden van de toezichthouder (ILT) op cybergebied onvoldoende om organisaties tot veranderen te dwingen.
- Verbinding zoeken met de stad en regio op het gebied van cyberweerbaarheid.

Bedreigingen

- Interessant doelwit voor cyberaanvallen vanwege ketenafhankelijkheden en de grote maatschappelijke impact.
- Onvoldoende aandacht voor cyberweerbaarheid en daarmee een bewapening tegen dreigingen als statelijke actoren.
- Groeiende risico's door innovatie in aanvallen zoals ransomware als businessmodel en storage spoofing.

3.Additionele bevindingen vanuit het HIC

In dit hoofdstuk zijn de bevindingen opgesomd die uit onze eigen activiteiten, achterban en projecten komen.

3.1 Scenario's

Hieronder enkele scenario's die relevant zijn voor het Haven Industrieel Complex. We hebben het over scenario's die qua aard of omvang anders zijn dan de hierboven beschreven scenario's.

- Externe dreiging ransomware in combinatie met assets onderliggend aan 'zware ongevallen'.

  Ransomware is in het Haven Industrieel Complex een groeiende dreiging - net als voor Nederland en daarbuiten.
  Daarbij maken wij ons zorgen om de assets die geraakt worden. We maken ons niet alleen zorgen om mogelijke financiële schade of verstoring van essentiële logistieke ketens.
  In het Rotterdamse Havengebied zijn er bedrijven die vallen onder BRZO wetgeving (Bedrijven Risico Zware Ongevallen). Daarvan is niet onomstotelijk bewezen dat deze allen voldoende beveiligd zijn.
  Uit de rapportage van DCMR (Milieudienst Rotterdam Rijnmond):
  > "In alle self-assessments is de volwassenheid op het gebied van OT lager ten opzichte van de overige categorieen. Organisaties geven daarmee aan dat OT-maatregelen minder volwassen zijn geïmplementeerd dan overige maatregelen"[5]

- Externe dreiging: Rusland
  Het uitbreken van de oorlog tussen Rusland en Oekraïne leidde tot verhoogde dreiging voor de Rotterdamse Haven. De ervaringen met de ransomware aanval in 2017 waar MAERSK slachtoffer van werd, heeft aangetoond dat het ook mogelijk is om geraakt te worden als collateral damage.
  Afgelopen maanden - en zo blijkt ook uit het cyberbeeld van NCTV - lijkt de dreiging vanuit Rusland een 'nieuw normaal' te worden.

  Deze externe dreiging is voor ons niet een 'nieuw normaal', maar classificeren we als een 'creeping crisis'. Met elk sanctiepakket tegen Rusland wordt de dreiging groter. Signalen blijven komen, zoals een recent item op de Russische staats TV waar aan de Rotterdamse Haven wordt gerefereerd[6].

- Interne: dreigingen: kwaadwillenden
  Hier sluiten we ons primair aan bij het beeld van het havenbedrijf Rotterdam. Daar waar zij spreken over individuele kwaadwillenden bij hen intern in de organisatie, zien we ook dreigingen waarbij kwaadwillenden in het Haven Industrieel Complex via interne mogelijkheden infrastructuur misbruiken voor criminele doeleinden.

[5] https://www.dcmr.nl/sites/default/files/2021-10/Eindrapportage%20Cybervolwassenheidsonderzoek%20DCMR%20v1.1.pdf
[6] https://www.ad.nl/binnenland/russisch-parlementslid-hint-op-rotterdamse-haven-als-doelwit-op-staatstelevisie~a626aece/

3.2 Weerbaarheid: Kwalitatieve en kwantitiatieve doelstellingen

"Van bewustwording naar weerbaarheid".

Onder deze noemer - 'van bewustwording naar weerbaarheid' - is stichting FERM begin 2021 van start gegaan. Doelstelling van FERM is om door samenwerking aan de weerbaarheid van het Rotterdamse Haven Industrieel Complex te werken.

Dreigingen veranderen, mogelijkheden en best-practices ontwikkelen zich ook. Daarbij merken we dat we blijvend moeten werken aan het voortschrijdend inzicht, dus blijvend aan 'awareness' werken.
Tegelijkertijd worden er steeds meer stappen naar 'weerbaarheid' gezet; zoals ook uit onderstaande paragrafen blijkt.

<u>Kwalitatieve doelstelling:</u>

Onder de participanten van FERM - dit blijkt ook uit de cyberweerbaarheidsscans – zien we dat 'identify' en 'protect' voldoende zijn en de basis maatregelen zijn doorgevoerd. Dit is een ánder beeld dan in het Cyberbeeld Nederland en het Cyberbeeld van de Gemeente Rotterdam komt.
Hieruit kan geconcludeerd worden dat de organisaties die participant zijn van FERM het gemiddeld meer op orde hebben dan niet-participanten van FERM.

<u>Kwantitatieve doelstelling:</u>

Stichting FERM heeft als opdracht en is uitgerust om te groeien. Hierbij liggen we op schema van de gestelde doelstelling bij oprichting van de stichting.

Daarbij 'voelen' we dat als gevolg van de groeiende dreiging de verwachting voor weerbaarheid ook groeit. We zetten ons in om - door middel van aanvullende projecten - inhoud te geven aan deze verwachtingen.

3.3 Incident Response en het belang van oefenen

Door te oefenen kan tijdens een echte digitale crisis sneller en adequater gehandeld worden.

Er zijn afgelopen jaar in diverse settings oefeningen gedaan, bij bedrijven en ook bij samenwerkingen als in ketenafhandeling. Een voorbeeld van de laatste is de Cybernautics oefening van het Havenbedrijf, waar geoefend wordt met het Haven Crisis Team en de ISPS bedrijven (bedrijven die onder de ISPS wetgeving vallen; de International Ship & Port facility Security).

Hierbij valt procesmatig op dat de gekozen methodieken bij de bedrijven en instanties overeenkomt (gebaseerd op de BOB-methode; Beeldvorming, Oordeelsvorming en Besluitvorming), dit maakt het werken in verschillende samenstellingen intuïtief uitvoerbaar.

Inhoudelijk zien we met regelmaat de volgende bevindingen terugkomen:

- liaisons:
  Veel crisisoefeningen worden ‘centraal’ gecoördineerd of er wordt geoefend in een setting waarbij de informatie en eindbeslissing in hand van het crisisteam ligt.
  Hierbij is er onvoldoende oog voor informatie die er in het ecosysteem aanwezig is.

  Advies: zet in je Incident Response Plan een overzicht van de contactpersonen die als liason kunnen helpen in geval van crisis met communicatie en brengen/halen van informatie elders. Voor onze participanten is FERM is daar natuurlijk één van.

- Informeren van stakeholders
  Crisisteams informeren in de oefening vaak wel enkele, maar lang niet alle stakeholders. Voorbeelden van stakeholders die vergeten worden zijn de Autoriteit Persoonsgegevens, de politie, het haven-cyber-meldpunt of collega-bedrijven uit de haven.

  Advies: maak een lijst - inclusief telefoonnummers, e-mailadressen - zowel zakelijk als privé - van de contactpersonen en print deze op papier uit.

- Escalatie
  Eén incident is een incident, twee kan duiden op een structureel probleem. Wanneer wordt de crisis ‘te groot’ voor dit crisisteam en escaleer je, bijvoorbeeld naar de veiligheidsregio?

  Advies: maak de escalatiepunten in het Incident Response Plan vooraf duidelijk en beschouw de Veiligheidsregio als stakeholder, zodat je ze gedurende een crisis tijdig informeert.

3.4 Cyberweerbaarheidsscans

Er zijn vanuit FERM afgelopen jaar verschillende Cyberweerbaarheidsscans bij bedrijven uitgevoerd. Deze scans - nulmetingen die participanten krijgen aangeboden op het moment dat ze gaan participeren - bekijken een organisatie van binnenuit langs de ISO 27001 standaard en richtlijnen. De organisaties die hebben meegewerkt zijn divers in sector en grootte.

Hierbij zijn de voornaamste bevindingen:

- De overall score is hoger zodra er management commitment is voor cybersecurity,

- De score is ook hoger als cybersecurity wordt opgepakt door dedicated professionals waarmee het management kan sparren over cybersecurity. Afhankelijk van de organisatiegrootte kunnen deze cybersecurity medewerkers gerust deeltijd en inhuur zijn, zolang de cybermaatregelen maar worden geïmplementeerd, opgevolgd en nagejaagd. Het effect hiervan wordt na circa 2 jaar pas goed zichtbaar.

- Daar tegenover staat dat de overall score van de Cyberweerbaarheidsscan lager uitvalt als cybersecurity als “bijgerecht” wordt opgepakt door de reguliere IT medewerkers;
  - In kleinere organisaties speelt dit minder omdat het daar gemakkelijker is om overzicht te houden en in control te blijven.
  - Zodra de organisatie groter is, wordt het moeilijker om cybersecurity bij de verschillende vestigingen goed door te voeren en te volgen. Vaak hebben dat soort organisaties wel een CISO en/of Security Office, en daarmee hun cybersecurity policy en procedures op orde, maar zij hebben moeite om lokaal management te overtuigen.

- Op technisch vlak scoren organisaties hoger als zij een nieuwe infrastructuur hebben en niet te veel legacy systemen.

- Asset: Verder is registratie van alle hardware en software in een asset register essentieel; je kunt niet beschermen waarvan je niet weet dat je het hebt.

- De bescherming (“Protect”) is in het algemeen goed ingericht bij de FERM participanten, wat betekent dat nu geïnvesteerd moet worden in het monitoren van gebeurtenissen (“Detect”) en vooral in de weerbaarheid en veerkracht van de organisatie als het desondanks tot een incident komt (“Respond” en “Recover”).

- Inside threats:
  Tenslotte is het lastig voor organisaties om cybersecurity en waakzaamheid tussen de oren van medewerkers te houden.

Overigens is de medewerking aan de Cyberweerbaarheidsscans zeer goed, waarbij de participanten de tijd nemen om de vragen goed te begrijpen en te beantwoorden. Daarbij zijn zij eerlijk en realistisch, soms zelfs kritisch, over de eigen cybersecurity en -weerbaarheid.

3.5 Cyber Kracht Meting

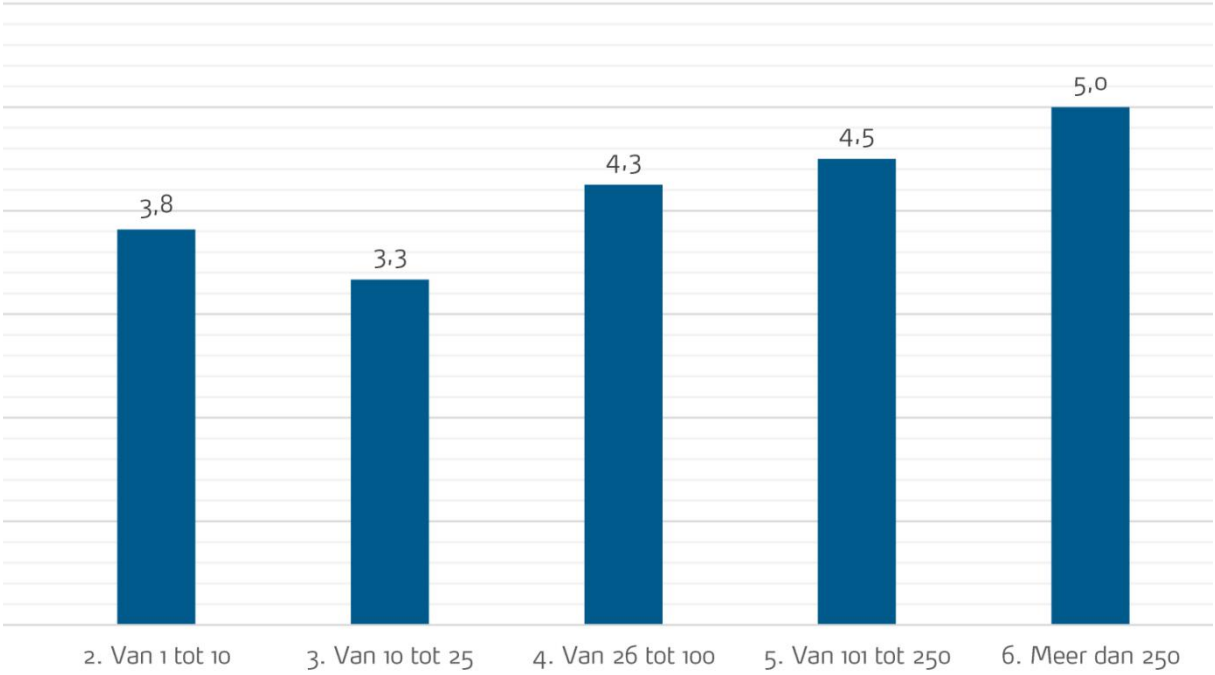
De Cyber Kracht Meting is een meting die is uitgevoerd op 536 bedrijven in de Rotterdamse Haven. Het is een meting die gebruik maakt van publiekelijk aanwezige informatie over de domeinnaam - zowel met betrekking tot de website als het e-mailverkeer.

De meting is tot stand gekomen op basis van uitvraag van openbare bronnen op het internet, gekoppeld aan de domeinnaam. Er zijn dus geen ethische hackers ingeschakeld die geprobeerd hebben om digitaal bij de organisaties binnen te komen. Er is alleen op basis van een domeinnaam van een afstand gekeken of er “ramen of deuren open staan” waar cybercriminelen kans zien om binnen te komen.

Deze is bedoeld om richtinggevend inzicht te geven; de meting kan gezien worden als een eerste, laagdrempelige aanzet waarmee organisaties direct hun informatiebeveiliging en digitale weerbaarheid kunnen versterken.

Het gaat voor dit beeld te ver in detail om alle elementen op te sommen waar op gecontroleerd is, maar in hoofdlijnen is gecontroleerd op gebruik van de juiste securityprotocollen voor websites (zoals gebruik “https”, DNSsec maar ook afdwingen van protocollen, openstaande poorten en het voorkomen op blacklists), E-mail configuratie instellingen (zoals DKIM, SPF en DMARC) en of er informatie zoals gebruikersnamen en wachtwoorden van medewerkers publiek bekend is.

Hierbij valt op dat er flinke verbeteringen zijn te behalen, met name in de organisaties met een aantal FTE tussen de 10-25.



3.6 Vraagbundeling

Participanten vanuit FERM bepalen de inhoudelijke agenda, mede door vragen die worden gesteld op het community-portal.

Volgend uit deze vragen, lag de focus op de respons - en daarmee de aandacht in de beantwoording van vragen op deze drie onderwerpen:

- de cloud
- third party risk management
- identity en access management

Dit zijn ook punten zijn die veelal misbruikt worden door kwaadwillenden, die aandacht krijgt van vele autoriteiten en regulerende instanties; niet in de laatste plaats omdat in deze punten organisaties ook nog te kort schieten.

Het is belangrijk dat je de juiste controls voor je eigen organisatie kiest na gedegen onderzoek van de eigen situatie. Meer dan vanuit druk van derde partijen zoals overheden, regulerende instanties, klanten, leveranciers, etc.. Juist als er een intrinsieke behoefte is vanuit een organisatie, d.m.v. risico assessments, merk je dat het bewustzijn en daarmee management commitment sterk bevorderd wordt.

3.7 Juridisch / Legal en contractuele zorgen

We verwachten - mede als gevolg van de implementatie van de NIB-2 directive (internationaal NIS-2 directive genoemd)- een toename van de juridische en contractuele aspecten met betrekking tot cyberweerbaarheid en schadeafhandeling. Iets wat rondom cyberverzekeringen al langer waargenomen wordt.

4.Handelingssuggesties / adviezen

Cyberweerbaarheid is een zaak van de lange adem.
Cyberweerbaarheid is een gezamenlijke verantwoordelijkheid.

Gezien het huidige beeld van de cyberweerbaarheid van het Rotterdamse Haven Industrieel Complex geven we hierbij de volgende handelingssuggesties / adviezen.

4.1 Individuele organisaties

- Zorg dat je de basis op orde[7] hebt.
  Analyseer de mogelijke risico's, niet alleen aan de hand van de impact op je eigen organisatie maar ook die van je omgeving. Doe gedegen onderzoek naar controls die voor jouw organisatie belangrijk en effectief zijn; dat is een sterkere stuurfactor dan dat controls opgelegd wordt vanuit derde partijen.

- Maak een meerjarenplan en geef daar in ieder geval aandacht aan: 'cloud', 'third party risk management' en 'identity en access management'.

- Richt je organisatie in op de 'long haul': scheidt IT en de cybersecurity in rol, voor minimaal 2 jaar. Hou de eindverantwoordelijkheid voor cybersecurity in eigen huis. Als er geen functionaris beschikbaar is, maak gebruik van part-time 'CISO-as-a-service' .

- Onder de participanten zien we dat 'identify' en 'protect' voldoende zijn. Werk aan 'detect' en bereid je voor op 'response' en 'recover'. Zorg voor een eigen Incident Response Plan en neem daarin de escalatie naar het ecosysteem mee, zoals bijvoorbeeld het Haven Cybermeldpunt 010 – 252 1005[8]

- Als er een afhankelijkheid is van bedrijven om je heen, bevraag hen - je ketenpartners - op hun cybermaatregelen en stimuleer hen om ook stappen te zetten om gezamenlijk veilig te blijven.
  Indien mogelijk neem de rol als 'leaderfirm' voor je omgeving.

  Er zijn regelingen die je hierbij kunnen helpen; zoals bijvoorbeeld de voucher regeling voor cybersecurityscans voor MKB 0-50 FTE in de provincie Zuid Holland. Daarnaast biedt FERM voor de kleinere bedrijven CYRA aan, waarmee integraal ketenveiligheid aangepakt kan worden.

- Oefen aan de hand van je eigen Incident Response Plan.

[7] https://www.ferm-rotterdam.nl/nl/basishygiene
[8] https://www.ferm-rotterdam.nl/nl/meldpunten

4.2 Ecosysteem- ketenpartners en beleidsmakers

Net als voor individuele bedrijven, geldt ook voor beleidsmakers en ecosysteempartners dat ‘management commitment’ noodzakelijk is voor een weerbare haven.

- Maak “cyberveiligheid” een randvoorwaarde bij alle grote onderwerpen die spelen.
  Bij alle projecten en initiatieven die gegund worden; maak ‘cyber’ een in te vullen randvoorwaarde. Of het nu gaat om energietransitie, ondermijning of verregaande digitalisering, stel als eis dat het cyberveilig is.
  Gebruik het netwerk van FERM indien gewenst als “CISO Haven”, met een adviesrol hierin

- Een risico waar individuele bedrijven mee te maken hebben is het tekort aan voldoende cyberkundig gekwalificeerd personeel.
  Stuur op:
  - digitale skills van individuen (en daarmee - potentiële - medewerkers).
  - Het zorgdragen voor voldoende opgeleide en beschikbare functionarissen die als security officers kunnen functioneren.

- Maak van MKB een prioriteit. Niet alleen in woord maar maak het ook voor hen attractief om cyber als randvoorwaarde in te vullen. Dit advies is niet eenvoudig of enkelvoudig in te vullen. Zet daarom breed in.

  Naast bestaande dienstverlening van FERM kun je denken aan faciliteren op het gebied van een meldpunt voor zachte en harde signalen, verder delen van voorbeelden, maar ook: hoe selecteer ik leveranciers en waar kan ik naar toe met hulp bij een incident.

  Zet in op haven breed gebruik, voor alle organisaties die actief zijn in het havengebied.

- Doe onderzoek naar het IT landschap en de onderliggende kwetsbaarheden, zoals bijvoorbeeld informatie- of netwerk knooppunten in de haven.

- Oefen cyber gevolgbestrijding

4.3 Stichting FERM

De stichting FERM heeft een Raad van Toezicht en een Raad van Advies. Deze laatste kan het bestuur gevraagd en ongevraagd van advies voorzien. Het bestuur legt de richting en inhoud ook voor aan deze Raad van Advies.

Heb je na het lezen van dit rapport vragen en/of een advies voor stichting FERM?

Neem gerust contact op via contact@ferm-rotterdam.nl en meld als onderwerp “Advies nav cyberbeeld 2022”.