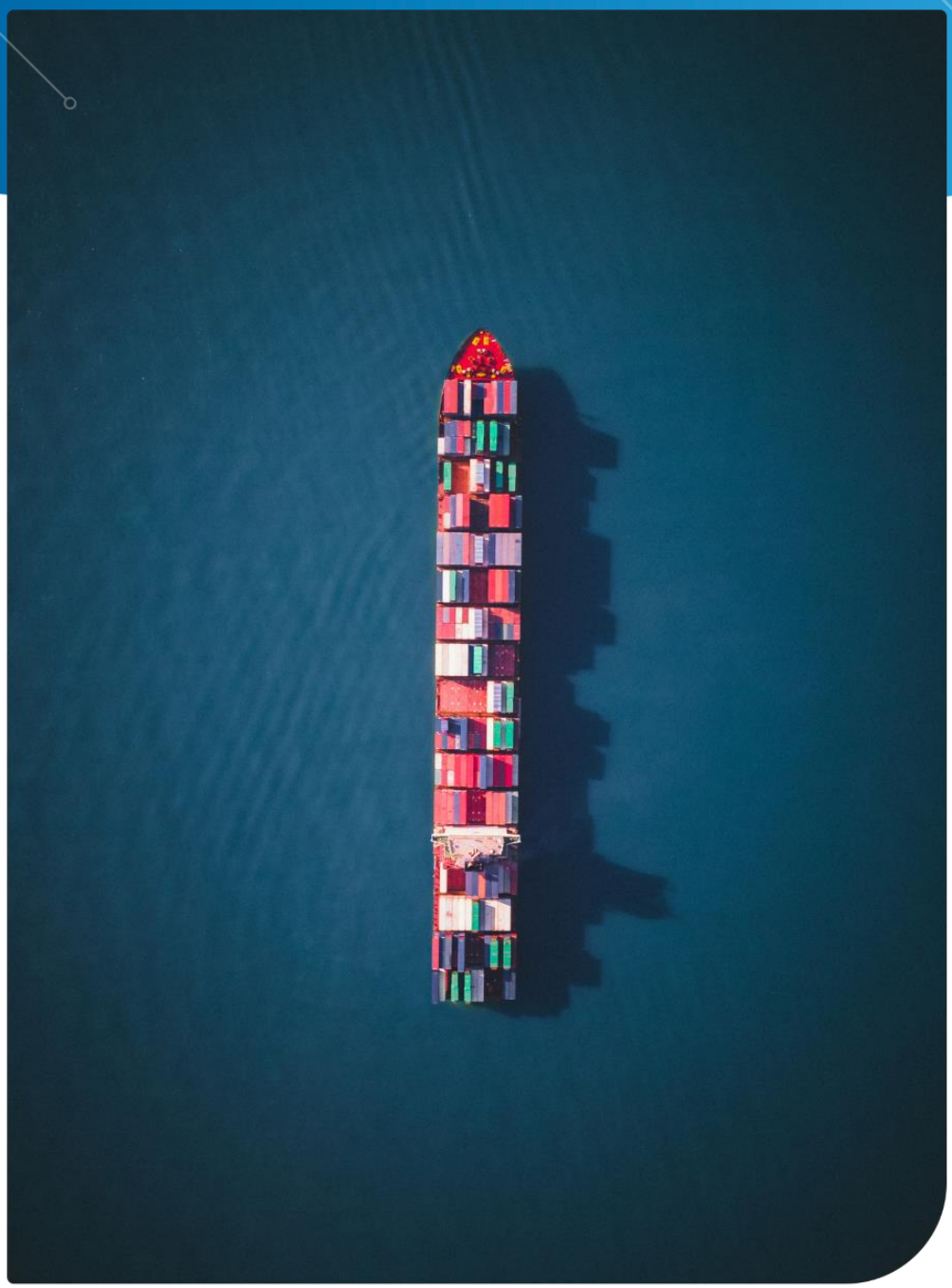
Cyberweerbaarheid in de maritieme sector

Frank van Summeren

Projectleider cyberweerbaarheid in de logistieke sector namens Security Delta



HSD

securitydelta.nl

HSD
securitydelta.nl

Inhoudsopgave

1. Programma cyberweerbaarheid van ondernemers

De Metropoolregio Rotterdam Den Haag (MRDH) erkent het belang van digitalisering als belangrijke voorwaarde voor economische innovatie. Nieuwe technologische ontwikkelingen zoals artificial intelligence, internet of things en blockchain geven een impuls aan de economie in de regio. De 23 gemeenten in de Metropoolregio Rotterdam Den Haag zetten al een aantal jaar in op een goede digitale bereikbaarheid en (nieuwe) digitale technologieën. Digitalisering levert naast economische kansen (zoals kostenbesparing door efficiëntie en nieuwe producten en diensten door innovatie) ook dreigingen op. Digitalisering zorgt immers voor een sterkere afhankelijkheid van digitale processen en netwerken. Digitale processen raken steeds meer verweven en verbonden met fysieke processen en apparaten. Dit betekent dat een cyberaanval de continuïteit van een (digitaal en/of fysiek) proces kan verstoren met de mogelijke gevolgen van dien voor de getroffen onderneming(en) en de maatschappij. Een weerbare economie is zodoende gebaat bij cyberweerbaarheid van ondernemers.

Bedrijven staan dagelijks bloot aan cyber security risico's zoals bedrijfsspionage en afpersing door hackers die met ransomware computersystemen vergrendelen waardoor vitale bedrijfsprocessen niet meer (optimaal) werken met verlies van omzet en reputatieschade tot gevolg. Desondanks nemen bedrijven nog niet altijd de noodzakelijke maatregelen om zich voldoende te beschermen tegen cybercriminaliteit. In 2020 is, in opdracht van de Economic Board Zuid-Holland, een onderzoek verricht naar de impact van cyberonveiligheid. Uit het onderzoek kwam naar voren dat jaarlijks ongeveer 20% van de MKB bedrijven slachtoffer wordt van een cyberbaanval. De indicatieve kosten van cyberonveiligheid in de provincie Zuid-Holland bedragen jaarlijks tussen de 2 tot 4 miljard euro. De verwachting is dat het slachtofferschap onder ondernemers en de daarbij horende schade in de toekomst beide gaan stijgen door de vergaande en versnelde digitalisering (Cybergereedheid Provincie Zuid-Holland, Koen Gijsbers, 2020).

De (digitale) processen, toegepaste technologieën, (potentiële) kwetsbaarheden en daaruit voortkomende cyber security risico's verschillen per sector. Dit betekent dat een sectorale aanpak het meest voor de hand ligt om de cyberweerbaarheid van ondernemers in verschillende sectoren te bevorderen. De Security Delta start daarom een programma om de cyberweerbaarheid van ondernemers in zes essentiële sectoren (life sciences & health, water, logistiek, maakindustrie, maritiem, lucht- en ruimtevaart) in de regio Zuid-Holland te bevorderen. Dit initiatief wordt mede mogelijk gemaakt door de Metropoolregio Rotterdam Den Haag subsidie Sectoraal Digitaal Veilig.

In deze rapportage wordt ingegaan op de cyberweerbaarheid van ondernemers in de maritieme sector. Hierbij wordt aandacht besteed aan actuele vraagstukken op het terrein van cyber security in de maritieme sector. Ook wordt er ingegaan op lopende initiatieven om de cyberweerbaarheid van ondernemers in de maritieme sector te bevorderen en worden er suggesties gedaan om deze waar mogelijk en gewenst met elkaar te verbinden en te versterken.

2. Maritieme sector

De maritieme sector is met ondermeer de Haven van Rotterdam van groot belang voor de Nederlandse economie en werkgelegenheid. De maritieme sector is onder te verdelen in een aantal deelsectoren waaronder zeevaart, binnenvaart, waterbouw, scheepsbouw, toeleveranciers, dienstverlening, offshore, baggerindustrie, visserij, watersport en havens. Er zijn in Nederland ruim 21.000 bedrijven actief in de maritieme sector. Daarnaast werken ruim 250.000 medewerkers in de maritieme sector en de toegevoegde economische waarde is ruim 23 miljard euro. Dit maakt maritiem een belangrijke economische sector.

Om toonaangevend en concurrerend te blijven wordt er geïnvesteerd in innovatie in de maritieme sector waaronder in digitalisering. Zo wordt er ingezet op smart maintenance en autonoom varen. In de Haven van Rotterdam wordt geïnvesteerd in digitale infrastructuur om logistieke ketens (nog) efficiënter te laten verlopen. Zo leveren inmiddels meer dan 125 operators hun data aan de digitale planningstool Routescanner die kan helpen bij het vinden van de meest duurzame route voor container logistiek. In de binnenvaart wordt voor het plannen gebruikt gemaakt van de digitale service Nextlogic. Deze ontwikkelingen brengen kansen, maar ook risico's met zich mee ondermeer op het terrein van cyber security.

Zuid-Holland is het grootste maritieme knooppunt in West-Europa. Dit is mede het gevolg van de aanwezigheid van de Haven van Rotterdam die behoord tot de grootste havens van de wereld en die in Nederland direct en indirect werk biedt aan ruim 550.000 medewerkers. De Haven van Rotterdam is het grootste haven- en industriecomplex van Europa dat bestaat uit verschillende havenbekkens en bedrijfsterreinen die ten dienste staan van de aan- en afvoer van goederen (zoals aardolie, chemicaliën, kolen en ertsen) van de aan de haven gevestigde (petro)chemische en andere industrieën, en de op- en overslag van goederen van derden voor verder transport. In 2021 werden er meer dan 15 miljoen containers in de Haven van Rotterdam overgeslagen. Een groot deel daarvan wordt via multimodale inlandterminals overgeslagen. Dit zijn knooppunten waar verbindingen over het water, de weg, het spoor en/of buisleidingen samenkomen en waar goederen kunnen worden overgeslagen van de ene op de andere modaliteit. Er is zodoende sprake van ketenafhankelijkheid. Dit betekent dat wanneer er ergens in de keten een (cyber security) incident plaatsvindt, dit aanzienlijke gevolgen kan hebben voor de gehele keten. Dit betekent dat cyberweerbaarheid niet alleen betrekking heeft op afzonderlijke bedrijven, maar op gehele logistieke processen en ketens.

Gezien de toegevoegde economische waarde van de maritieme sector en de afhankelijkheid van andere sectoren van ondermeer de Haven van Rotterdam vormt maritiem een van de zes essentiële sectoren waarop het programma cyberweerbaarheid van de Security Delta zich richt. In deze rapportage wordt expliciet ingegaan op maritieme bedrijvigheid. Hierbij wordt beperkt aandacht besteed aan overslag naar andere modaliteiten, zoals verbindingen over de weg en het spoor. Dit komt omdat in een andere rapportage expliciet wordt ingegaan op de cyberweerbaarheid van ondernemers in de logistieke sector. Ook wordt er beperkt aandacht besteed aan organisaties die zich richten op watermanagement, omdat er in een andere rapportage expliciet wordt ingegaan op cyberweerbaarheid van ondernemers in de sector water.

3. Onderzoeksopzet

In dit hoofdstuk wordt beschreven op welke wijze de opzet en de uitvoering van het onderzoek hebben plaatsgevonden naar de cyberweerbaarheid van ondernemers in de maritieme sector. Er wordt ondermeer ingegaan op de gehanteerde onderzoeksstrategie en de methoden van onderzoek die zijn toegepast.

De vraagstelling die centraal staat in dit onderzoek in het kader van de rapportage betreft: wat is de cyberweerbaarheid van ondernemers in de maritieme sector? Wat zijn actuele vraagstukken op het terrein van cyber security in de maritieme sector? Welke lopende initiatieven zijn er om de cyberweerbaarheid van ondernemers in de maritieme sector te bevorderen? En hoe kunnen deze worden versterkt en/of aangevuld met nieuwe initiatieven om de cyberweerbaarheid van ondernemers in de maritieme sector te bevorderen?

Er is gestart met het verrichten van literatuuronderzoek naar cyberweerbaarheid van ondernemers in zijn algemeenheid en in de maritieme sector in het bijzonder. Vervolgens zijn organisaties en bedrijven in de sector maritiem in de MRDH regio in kaart gebracht. Hierna zijn deze organisaties en bedrijven benaderd om een afspraak te maken voor een interview. In de interviews is ingegaan op vitale bedrijfsprocessen en daarbij horende (potentiële) kwetsbaarheden en daaruit voortkomende cyber security risico's bij ondernemers in de maritieme sector. Daarnaast is geïnventariseerd welke cyber security vraagstukken zich voordoen in de sector. Op basis van het verkregen beeld is waar mogelijk de verbinding gelegd met de Security Delta zodat zij desgewenst partners uit haar netwerk kan positioneren die beschikken over de benodigde kennis, ervaring, referenties en innovatieve (technologische) oplossingen voor de betreffende cyber security vraagstukken. Tevens zijn lopende initiatieven op het terrein van de bevordering van cyberweerbaarheid van ondernemers in kaart gebracht. Tot slot is geïnventariseerd hoe lopende initiatieven waar mogelijk en gewenst met elkaar kunnen worden verbonden en/of versterkt.

In het kader van het onderzoek is gesproken met bedrijven in de maritieme sector, branche organisaties, publiek private samenwerkingsverbanden, lokale, regionale en nationale overheden. Aan het onderzoek hebben de volgende organisaties geparticipeerd en een bijdrage geleverd: Provincie Zuid-Holland, Innovation Quarter, gemeente Rotterdam, politie eenheid Rotterdam, Veiligheidsregio Rotterdam Rijnmond, Regionaal Informatie en Expertise Centrum Rotterdam, DCRM Milieudienst Rijnmond, Platform Veilig Ondernemen Rotterdam, Veiligheidsalliantie Regio Rotterdam, Resilient Rotterdam, Havenbedrijf Rotterdam, FERM, iTanks, Maritime Delta, gemeente Dordrecht, Cybernetwerk Zuid-Hollandse Eilanden, Werkgevers Drechtsteden, Cybernetwerk Drechtsteden, Nationaal Cyber Security Center, Digital Trust Center, Adviescentrum Bescherming Vitale Infrastructuur, Port Security Center, Vereniging van Nederlandse Gemeenten, ministerie van Justitie en Veiligheid, Centrum voor Criminaliteitspreventie en Veiligheid, VNO NCW, MKB Nederland, IRO, Koninklijke Vereniging van Nederlandse Reders, DigiShape, Transport en Logistiek Nederland, Evofenedex, gemeente Den Haag, Platform Veilig Ondernemen Den Haag, Regionaal Samenwerkingsverband Integrale Veiligheid, Resilient The Hague, Centre of Expertise Cybersecurity en de politie eenheid Den Haag. Van de afgenomen interviews met stakeholders zijn gespreksverslagen gemaakt welke de basis vormen voor de rapportage over de cyberweerbaarheid van ondernemers in de maritieme sector.

4. Cybercriminaliteit in de maritieme sector

In dit hoofdstuk wordt ingegaan op de aard, omvang en verschijningsvormen van cybercriminaliteit in de maritieme sector. Bedrijven in de maritieme sector lopen een niet gering risico om slachtoffer te worden van cybercriminaliteit door de aard van hun bedrijfsactiviteiten, de producten en diensten die ze vervoeren voor derden en/of de mogelijke buit die er bij hun te halen is.

Het worst case scenario voor bedrijven in de maritieme sector is dat de informatievoorziening voor de bedrijfsvoering wordt uitgeschakeld of overgenomen waardoor de continuïteit van de bedrijvigheid in het geding komt. Een voorbeeld hiervan is de cyberaanval waarvan Maersk in 2017 slachtoffer werd. De computersystemen van Maersk waren geïnfecteerd door het Petya virus. Dit betreft gijzelsoftware waarmee computersystemen door hackers worden overgenomen en doorgaans pas worden vrijgegeven zodra er losgeld is betaald. Het gevolg was dat twee van de vijf grote containerterminals in de Haven van Rotterdam ruim een week buiten bedrijf waren. Vanzelfsprekend had dit een enorme impact op de keten. Het heeft ongeveer een jaar gekost voordat alle containers weer terecht waren. Maersk heeft daarnaast noodgedwongen nieuwe computersystemen moeten aanschaffen. De geschatte kosten van de cyberaanval voor ondermeer Maersk betreft enkele honderden miljoenen euro's.

Daarnaast lopen de bedrijven in de maritieme sector het risico dat ze door criminele netwerken actief in de georganiseerde (drugs)criminaliteit worden misbruikt om onbewust illegale goederen te vervoeren. Deze criminele netwerken hebben geen baat bij het verstoren van de bedrijfsvoering, maar willen inzicht en/of invloed hebben op de logistieke keten rond een lading waarin hun illegale goederen (zoals drugs) ongezien vervoerd worden. Nederland, waaronder de Haven van Rotterdam, speelt een belangrijke rol als doorvoerhaven van ondermeer cocaïne. In 2020 werd er ruim 40.000 kilo cocaïne in beslag genomen door het Hit And Run Cargo team (HARC) van de politie, douane en de FIOD. Naar verwachting is dit slechts het topje van de ijsberg. De inschatting is dat tussen de 20% en 30% van de drugstransporten wordt ontdekt en vervolgens vernietigd. Criminele netwerken infiltreren in systemen en in bedrijven in de maritieme sector om hun drugs ongezien te transporteren. Dit heeft een grote impact op de bedrijvigheid in ondermeer de Haven van Rotterdam. De bedrijven die actief zijn in de maritieme sector moeten zich zowel wapenen tegen dreigingen van buitenaf en van binnenuit. Enerzijds moeten zij voorkomen dat criminele netwerken van buitenaf kunnen infiltreren in hun informatievoorziening ten behoeve van logistieke processen om deze vervolgens te manipuleren. Anderzijds moeten zij voorkomen dat criminele netwerken hun medewerkers als handlangers misbruiken om hun logistieke processen aan te wenden voor drugssmokkel.

"Drugscriminelen proberen door in logistieke processen te infiltreren hun drugstransporten te beschermen en ongezien te laten passeren. Als relatief kleine ondernemer in de logistieke sector ben je voor dit soort criminelen heel aantrekkelijk om te misbruiken en is het heel ingewikkeld om je hier tegen te wapenen en doe je niet snel genoeg om dit te voorkomen." (Respondent interview)

Tot slot is er in de Haven van Rotterdam regelmatig sprake van storage spoofing. Het betreft alle vormen van verkoop van fictieve opslagcapaciteiten en voorraden van grondstoffen en goederen in terminals in de Haven van Rotterdam. Het doelwit van deze vorm van fraude zijn de potentiële kopers van grondstoffen en goederen die vanuit de Haven van Rotterdam lijken te worden aangeboden. De slachtoffers betalen onbewust voor niet bestaande opslagcapaciteiten en voorraden van grondstoffen en goederen. Daarnaast leidt dit tot mogelijke imago en reputatieschade voor de bedrijven die in de Haven van Rotterdam gevestigd zijn wiens naam wordt misbruikt door fraudeurs om slachtoffers op te lichten. Veelal bevindt zowel de dader als het slachtoffer van storage spoofing zich in het buitenland, waardoor het onderzoek naar deze vorm van fraude vaak moeizaam verloopt.

Ondanks dat de bedrijven in de maritieme sector met regelmaat worden geconfronteerd met cyber security incidenten wordt hier slechts in beperkte mate melding van gemaakt. Er wordt door bedrijven relatief vaak voor gekozen om af te zien van aangifte van een strafbaar feit bij de politie. Hieraan liggen verschillende oorzaken ten grondslag. Zo zijn bedrijven terughoudend om kenbaar te maken dat ze slachtoffer zijn van een cyber security incident omdat als dit in de openbaarheid komt mogelijk kan leiden tot imago en reputatieschade. Daarnaast bestaat het beeld dat de belangen van een bedrijf kunnen conflicteren met die van de politie. Zo heeft het bedrijf er belang bij dat de informatievoorziening zo spoedig mogelijk weer operationeel is om de continuïteit van de bedrijfsvoering te waarborgen terwijl de politie mogelijk prioriteit geeft aan de opsporing van de daders van het cyber security incident. Tot slot is het voor bedrijven niet altijd duidelijk wat ze waar wanneer moeten melden en bestaat er twijfel over de opvolging en het mogelijke resultaat daarvan.

"De meldingsbereidheid van cyber security incidenten is laag. Hierdoor is er geen compleet beeld van cybercriminaliteit. Bedrijven wordt aangeraden om aangifte te doen bij slachtofferschap van cybercriminaliteit, maar de kans is aanwezig dat er geen adequate opvolging aan kan worden gegeven door schaarse capaciteit en druk op de strafrechtketen. Daarom is het van belang om de schaarse capaciteit en middelen gericht in te zetten tegen cybercriminelen die verantwoordelijk zijn voor omvangrijke cybercriminaliteit met veel impact. Daarnaast kunnen op basis van ontwikkelingen ondernemers worden geïnformeerd om toekomstig slachtofferschap te reduceren." (Respondent interview)

Om cybercriminaliteit in de maritieme sector gericht te kunnen aanpakken is inzicht vereist in de aard, omvang, verschijningsvormen, slachtoffers, kwetsbaarheden, daders en werkwijzen. Om dit te bewerkstelligen is het van belang dat de meldingsbereidheid van slachtofferschap van cybercriminaliteit wordt bevorderd. FERM, dat zich inzet voor cyber security in de Haven van Rotterdam, heeft op haar website een pagina met meldpunten waar bedrijven terecht kunnen wanneer ze slachtoffer zijn geworden van cybercriminaliteit. Afhankelijk van de aard van de cyberaanval en de aard van de werkzaamheden van een bedrijf is deze soms ook verplicht om te melden. Ondanks de pagina met meldpunten wordt slachtofferschap van cybercriminaliteit nog niet altijd gemeld. Er wordt ook de mogelijkheid geboden om anoniem te melden. Hier wordt nog (te) weinig gebruik van gemaakt.

Bij het in 2018 geopende Haven Cybermeldpunt kunnen bedrijven melding maken van IT-verstoringen met een effect op het aan- en afmeren van schepen, overslag van goederen of de veiligheidsmaatregelen in het kader van de Havenbeveiligingswet. Bedrijven die moeten voldoen aan de International Ship & Port facility Security (ISPS) zijn verplicht tot het nemen van maatregelen voor het beveiligen van schepen en havenvoorzieningen en geldt een meldplicht van cyber security incidenten. Anderen bedrijven die niet ISPS plichtig zijn worden aangemoedigd om vrijwillig cyber security incidenten te melden. In 2020 ontving het Haven Cybermeldpunt meerdere meldingen. Naar aanleiding hiervan zijn er maatregelen getroffen om de doorgang van scheepvaart- en wegverkeer te waarborgen. Er is een beeld van de cyber security van activiteiten in de Haven van Rotterdam. Daarnaast is er zicht op logistieke processen die de haven inkomen. Er is een minder goed beeld van de cyber security van logistieke processen wanneer deze de haven verlaten.

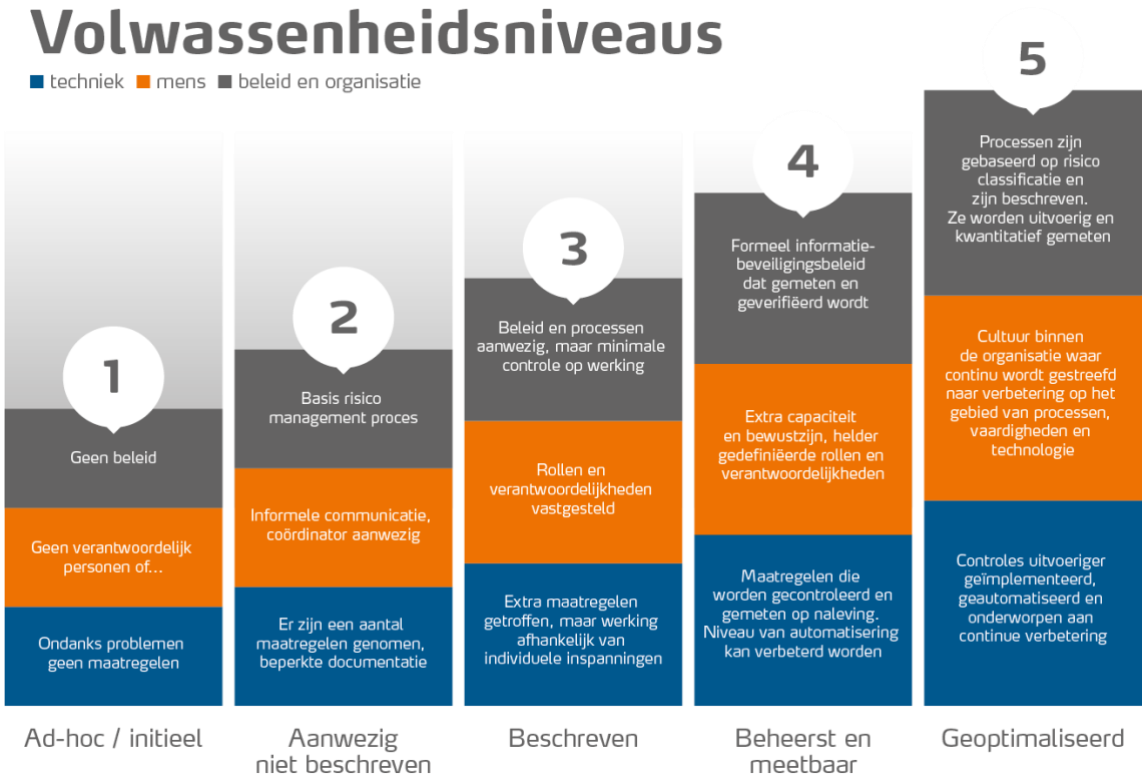
Het toezicht op bedrijven in de maritieme sector is versnipperd. In de Haven van Rotterdam houdt het Havenbedrijf toezicht op maritiem. De douane is toezichthouder op logistiek en DCRM Milieudienst Rijnmond is toezichthouder op Brzo-bedrijven die werken met grote hoeveelheden gevaarlijke stoffen. Het streven is om in de toekomst te gaan werken met één gemeenschappelijk toetsingskader op het terrein van cyber security. Het Havenbedrijf is verantwoordelijk voor het beheer en exploitatie van de Haven van Rotterdam en het handhaven van de snelle en veilige afhandeling. De douane houdt toezicht op de invoer, de uitvoer en het vervoer van goederen. DCMR

Milieudienst Rijnmond is de gezamenlijke omgevingsdienst van de provincie Zuid-Holland en vijftien gemeenten in de regio Rijnmond en is verantwoordelijk voor de vergunningverlening, het toezicht en de handhaving bij ongeveer 140 Brzo-bedrijven (zoals raffinaderijen, chemiebedrijven en bedrijven die gevaarlijke stoffen opslaan). Een aanzienlijk deel van deze Brzo-bedrijven bevindt zich in (de omgeving van) de Haven van Rotterdam. Er is nog geen toezicht vanuit DCMR Milieudienst Rijnmond op de cyber security van Brzo-bedrijven. Hiervoor ontbreekt het mandaat omdat cyberweerbaarheid niet is opgenomen in de SEVESO richtlijn die Brzo-bedrijven verplicht om in de bedrijfsvoering extra aandacht te besteden aan externe veiligheidsaspecten vanwege de aanwezigheid van bepaalde hoeveelheden gevaarlijke stoffen. Omdat het mandaat ontbreekt kan DCMR Milieudienst Rijnmond geen toezicht houden en niet handhaven op het terrein van cyber security bij Brzo-bedrijven. Daarom zet DCMR Milieudienst Rijnmond (via FERM) in op het informeren van ondernemers en wil zij hun op deze manier bewust maken van de cyber security risico's zodat zij geactiveerd worden om hun cyberweerbaarheid te verhogen. Mogelijk wordt in de toekomst de wet- en regelgeving aangepast waardoor er wel mogelijkheden zijn om de cyberweerbaarheid te reguleren. In dat geval zal dit eerst kenbaar worden gemaakt voordat er tot toezicht en handhaving zal worden overgegaan.

Om in de toekomst toezicht te kunnen uitoefenen op de cyberweerbaarheid van Brzo-bedrijven en indien nodig te handhaven is kennis en expertise vereist van cyber security. Deze kennis en expertise ontbreekt nu (nog) bij DCMR Milieudienst Rijnmond. Bij Brzo- inspecteurs bij DCMR Milieudienst Rijnmond is er nu nog geen of weinig kennis en expertise aanwezig over cyber security. De insteek ligt nu nog vooral op safety en in mindere mate op security (waaronder cyber security).

5. Cyberweerbaarheid in de maritieme sector

In dit hoofdstuk wordt ingegaan op cyberweerbaarheid van ondernemers in de maritieme sector. Om de cyberweerbaarheid van ondernemers in de maritieme sector te duiden is gebruik gemaakt van de cyber security routekaart van Threadstone (een partner van de Security Delta). Het gaat erom in welke mate ondernemers (beleidsmatige, technische en/of personele) maatregelen hebben genomen om cyber security risico's (waar mogelijk) te voorkomen en (waar nodig) te reduceren om de continuïteit van hun bedrijfsvoering te waarborgen. Hierbij een voorbeeld van het Havenbedrijf Rotterdam om dit toe te lichten. Het proces van het afwikkelen van het scheepvaartverkeer in de Haven van Rotterdam is in hoge mate afhankelijk van ICT systemen. Het Havenbedrijf Rotterdam investeert continue in technische maatregelen om de cyber security van haar ICT systemen te waarborgen. Daarnaast wordt er met personele maatregelen ingezet op cyber security awareness bij medewerkers. Tot slot worden er organisatorische maatregelen getroffen om goed voor bereid te zijn



op een (dreigend) cyber security incident, bijvoorbeeld door het testen van herstelprocedures.

Beleid en organisatie

Bedrijven in de maritieme sector kunnen beleidsmatige en organisatorische maatregelen nemen om de kans op slachtofferschap en impact van een mogelijke cyberaanval te reduceren. Uit de gesprekken met respondenten blijkt dat een groot deel van de ondernemers (met name de kleinere bedrijven) in de maritieme sector zich onvoldoende bewust is van de kans op slachtofferschap van cybercriminaliteit en de mogelijke impact daarvan op hun bedrijfsvoering en eventuele gevolgschade. Doordat de kans op slachtofferschap van cybercriminaliteit en de mogelijke impact van een cyberaanval wordt onderschat worden er door hun niet altijd de benodigde (beleidsmatige en organisatorische) maatregelen genomen om de cyberweerbaarheid te bevorderen.

Bij sommige bedrijven in de maritieme sector ontbreekt het aan cyber security beleid en zijn taken, verantwoordelijkheden en bevoegdheden ten aanzien van cyber security niet (duidelijk) belegd bij functionarissen in de organisatie. Daarnaast ontbreekt het bij diverse bedrijven aan protocollen en procedures wat betreft de omgang met cyber security dreigingen. Grotere bedrijven geven over het algemeen een hogere prioriteit aan cyber security binnen de organisatie. Dit komt (deels) doordat zij vanwege de omvang van hun organisatie en de aard van hun werkzaamheden eerder een gericht doelbewust target kunnen vormen van kwaadwillenden, wat vraagt om betere bescherming. Grotere bedrijven hebben doorgaans de beschikking over meer kennis, expertise, capaciteit en middelen voor cyber security. Hierdoor zijn zij over het algemeen, betere dan kleinere bedrijven, in staat om externe cyber security dreigingen buiten de deur te houden. Daar staat tegenover dat interne dreigingen (ook bij grotere bedrijven) soms worden verwaarloosd.

Een aanzienlijk deel van de bedrijven in de maritieme sector heeft hun IT hardware volledig buitenshuis geplaatst bij een externe organisatie. Veel kleinere bedrijven kiezen er al dan niet noodgedwongen voor om hun ICT te outsourcen. Bedrijven kunnen zich hierdoor richten op hun primaire bedrijfsvoering en hebben geen directe bemoeienis meer met het onderhoud en beheer van ICT. Dit betekent dat ze niet alleen voor hun ICT maar ook voor de cyber security (voor een deel) afhankelijk zijn van een externe organisatie. In sommige gevallen zijn er in dit geval ook geen concrete afspraken gemaakt over cyber security (waaronder monitoring, detectie, incident response, recovery). Dit komt bijvoorbeeld doordat de ondernemer er vanuit gaat dat dit met het outsourcen van de ICT geregeld is zonder dat cyber security expliciet met de externe organisatie is besproken. Daarnaast krijgt cyber security, doordat de ICT bij een externe organisatie is belegd, niet altijd de aandacht die het verdient in een bedrijf omdat dit door het extern uitbesteden uit het gezichtsveld is verdwenen en hierdoor minder gesprek van onderwerp is in de organisatie.

Techniek

Bedrijven nemen verschillende technische maatregelen om kwaadwillenden (waar mogelijk) buiten te houden en (waar nodig) de schade te beperken wanneer zij toch infiltreren. Er wordt gebruik gemaakt van toegangsbeheer ondermeer door middel van authenticatie waarmee een systeem kan vaststellen wie een gebruiker is. Een voorbeeld hiervan is het inloggen met een gebruikersnaam en wachtwoord waarmee een gebruiker toegang krijgt tot gegevens en/of kan werken in een systeem. Deze technische maatregel wordt regelmatig ondermijnd door dat medewerkers van een afdeling of in sommige gevallen zelfs van de gehele organisatie gebruik maken van één en hetzelfde account en wachtwoord voor een systeem. Enige jaren geleden was dit ook het geval bij een systeem van Portbase dat door verschillende bedrijven in de Haven van Rotterdam werd gebruikt door middel van één bedrijfsaccount voor alle medewerkers. Via het Port Community System biedt *Portbase* meer dan 40 verschillende services aan circa 3600 klanten in alle sectoren van de Nederlandse havens. De ambitie van Portbase is om via één loket de logistieke ketens van de Nederlandse havens zo aantrekkelijk mogelijk te maken. Portbase verbindt hiertoe alle partijen in de logistieke ketens van de Nederlandse havens. Via het Port Community System faciliteert Portbase datadeling tussen bedrijven en informatie-uitwisseling met overheden om sneller, efficiënter en tegen lagere kosten te kunnen werken.

“Binnen de Haven van Rotterdam wordt gebruik gemaakt van de systemen van Portbase. Als zij toestaan dat bedrijven één gezamenlijk bedrijfsaccount gebruiken met meerdere medewerkers dan wordt dit ook gedaan. Nu moet iedere medewerker een persoonlijk account gebruiken met een authenticator.” (Respondent interview)

Wanneer alle medewerkers van een afdeling of organisatie ongeacht hun functie en/of werkzaamheden ongelimiteerd en ongecontroleerd toegang krijgen tot data en/of systemen vergroot dit de kans op een insider threat. In een dergelijke situatie worden technische maatregelen te niet gedaan door een gebrek aan organisatorische maatregelen (ontbreken van of geen naleving van protocollen en procedures ten aanzien van toegang tot data en systemen) en/of personele maatregelen (niet rechtmatig en doelmatig omgaan met data en systemen). Er is bij diverse bedrijven geen scheiding/segmentatie van processen en data en geen compartimentering en

codering van informatie om bijvoorbeeld ladingen op te halen. Hierdoor is de kans aanwezig dat de betreffende informatie in de verkeerde handen valt, waardoor een lading kan worden ontvreemd door een kwaadwillende.

"Het aantal medewerkers wat ongezien bij informatie kon om containers op te halen was groot. Sommige bedrijven hebben dit verbeterd. In het verleden waren er honderden incidenten. Een aantal bedrijven hebben het opgepakt. Dit heeft geresulteerd in het gebruik van versleutelde nummers en minder medewerkers die hier toegang toe hebben." (Respondent interview)

De mate waarin bedrijven in staat zijn om cyber security risico's te identificeren verschilt. Bedrijven die over een Security Operations Center (SOC) beschikken zijn hier over het algemeen beter toe in staat. Vanuit het SOC kunnen afwijkingen worden gesignaleerd. Op basis daarvan kunnen maatregelen worden getroffen. Bedrijven die hun ICT buitenshuis hebben geplaatst kunnen mogelijk een beroep doen op een SOC van de betreffende externe organisatie.

Daarnaast verschilt ook de mate waarin bedrijven in staat zijn om cyber security dreigingen te detecteren. Hiervoor is een detectiesysteem nodig. De software, onderhoud en beheer hiervan zijn doorgaans kostbaar. Opvallend is dat wanneer de ICT extern is belegd, er niet altijd expliciet afspraken zijn gemaakt over de detectie van cyber security dreigingen.

Er zijn bedrijven die geen logging hebben, waardoor ze niet kunnen monitoren wie wanneer waar welke handeling (heeft) verricht. Ook is er geen monitoring of er vanuit vreemde locaties, op vreemde tijdstippen afwijkende handelingen worden verricht.

Ook als het gaat om het reageren op cyber security incidenten zijn er verschillen waar te nemen tussen bedrijven. Over het algemeen hebben grotere bedrijven met een SOC doorgaans een crisisplan waardoor zij in staat worden gesteld om adequaat te reageren op een (dreigend) cyber security incident.

Tot slot verschilt de mate waarin bedrijven kunnen terugvallen op een backup wanneer zij (ondanks de andere getroffen technische maatregelen) slachtoffer worden van een cyberaanval. Een backup zorgt ervoor dat niet alle informatie verloren gaat als een bedrijf bijvoorbeeld wordt getroffen door een ransomware aanval waarmee computersystemen worden vergrendeld waardoor bedrijfsprocessen niet meer (optimaal) werken.

"Een backup is niet altijd goed geregeld. Vaak staat ook niet alles in de cloud waar er een backup wordt gemaakt, maar staat er onbedoeld en onbewust ook een deel op de externe harde schijf." (Respondent interview)

Medewerkers

Medewerkers die cyber security aware zijn kunnen een belangrijke rol spelen in het weren van cyber security dreigingen. Daar staat tegenover dat medewerkers (onbewust) ook organisatorische en/of technische maatregelen te niet kunnen doen waardoor zij een risico vormen voor de cyberweerbaarheid van een onderneming. Een voorbeeld hiervan is het niet toepassen van het vier ogen principe door medewerkers in verschillende bedrijven in de maritieme sector wat de kans op slachtofferschap van CEO fraude vergroot.

Bedrijven in de maritieme sector lopen het risico dat ze door criminele netwerken actief in de georganiseerde (drugs)criminaliteit worden misbruikt om onbewust illegale goederen te vervoeren. Bedrijven moeten zich zowel wapenen tegen dreigingen van buitenaf en van binnenuit. Enerzijds moeten bedrijven voorkomen dat criminele netwerken van buitenaf kunnen infiltreren in hun informatievoorziening ten behoeve van logistieke processen om deze vervolgens te manipuleren om

de lading waarin hun illegale goederen (zoals drugs) zitten ongezien te transporteren buiten het gezichtsveld van ondermeer de politie en de douane. Anderzijds moeten bedrijven voorkomen dat criminele netwerken hun medewerkers als handlangers misbruiken om hun logistieke processen aan te wenden voor drugssmokkel.

Er is sprake van veel dreigingen van binnenuit, ook wel insider threats genoemd. Het hacken van systemen is vaak niet nodig door corrupte medewerkers bij bedrijven. Er vindt veel corruptie onderzoek plaats naar medewerkers van bedrijven. Hier is zelf een apart team voor binnen de politie. Er wordt desgewenst informatie verstrekt aan bedrijven die slachtoffer zijn geworden van een misdrijf zodat ze corrupte medewerkers in ieder geval kunnen ontslaan in afwachting van het onderzoek." (Respondent interview)

Er moet continue geïnvesteerd worden in de cyber security awareness van goedwillende medewerkers. Daarnaast is het van belang dat kwaadwillenden niet in dienst (kunnen) treden bij bedrijven. Dit kan bijvoorbeeld door sollicitanten (voor met name sleutelfuncties op kwetsbare vitale posities) te screenen tijdens hun sollicitatieprocedure, voorlichting te verzorgen richting medewerkers over mogelijke misstanden en door te werken met een integriteitscoördinator waar vermoedens van corruptie en integriteitsschendingen door medewerkers (anoniem) kunnen worden gemeld.

Cyberweerbaarheid van ondernemers en ketens

Goederen die in de havens binnenkomen worden voor een groot deel via multimodale inlandterminals overgeslagen. Hier komen verbindingen over het water, de weg, het spoor en/of buisleidingen samen en worden goederen overgeslagen van de ene op de andere modaliteit. Er is zodoende sprake van ketenafhankelijkheid. Bedrijven in de maritieme sector zijn zich in toenemende mate bewust van de ketenafhankelijkheid. Zij onderkennen dat de cyberweerbaarheid niet alleen afhankelijk is van de inspanningen van hun eigen organisatie, maar ook (in toenemende mate) van die van hun samenwerkingspartners in de keten. Desondanks wordt er tussen bedrijven in ketens nog niet altijd samengewerkt aan cyberweerbaarheid, terwijl een cyber security incident ergens in de keten ook aanzienlijke gevolgen kan hebben voor de gehele keten.

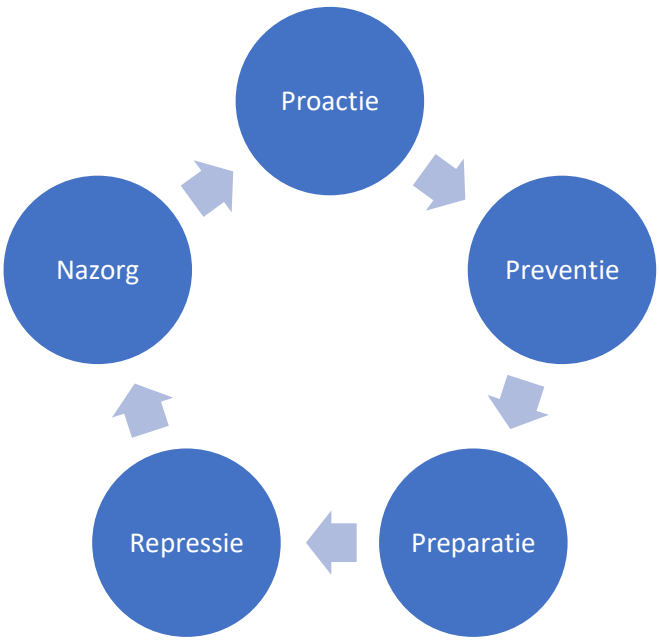
"Er zijn stappen genomen in de bevordering van de cyberweerbaarheid van ondernemers in de maritieme sector. Er is gestart met het op de kaart zetten van het probleem en het inzichtelijk maken van de urgentie daarvan. Verschillende bedrijven zijn naar aanleiding hiervan aan de slag gegaan met cyber security. Tegelijkertijd zien we dat veel ondernemers vooral voor zichzelf bezig zijn, een gezamenlijke aanpak ontbreekt. De keten is zo sterk als de zwakste schakel. Dit betekent dat bedrijven samen de cyberweerbaarheid moeten verhogen en dit gebeurt (nog) niet voldoende. Organisaties zijn huiverig om kwetsbaarheden en incidenten te delen, met name vanwege imagoschade." (Respondent interview)

"De marges in de logistiek zijn soms flinterdun, waardoor er weinig kan worden geïnvesteerd in security waaronder cyber security, waar we ons vanzelfsprekend zorgen over maken. De logistiek is ongeveer 70% van de bedrijvigheid in de haven. Als het ergens mis gaat in de logistieke keten kan dat gevolgen hebben voor de rest. Er is sprake van ketenafhankelijkheid. De hele keten is zo sterk als de zwakste schakel. Een voorbeeld hiervan is het incident in het verleden bij APM terminals waardoor het logistieke proces in de haven van Rotterdam vastliep." (Respondent interview)

Integrale benadering van cyberweerbaarheid

Cyberweerbaarheid staat voor het vermogen van ondernemers om cyber security dreigingen te herkennen en hier adequaat op te anticiperen. De aanname is dat iedere ondernemer in de loop der tijd te maken krijgt met een cyber security incident. Dit betekent dat ondernemers zich niet alleen moeten richten op preventieve maatregelen om een cyber security incident te voorkomen, maar ook op detectie en respons. De veiligheidsketen is een methode voor een integrale benadering van

cyber security risico's. De veiligheidsketen bestaat uit vijf fasen of schakels. Het betreft proactie, preventie, preparatie, repressie en nazorg. Proactie is het wegnemen van structurele oorzaken van onveiligheid. Te denken valt aan het bewaren van cruciale informatie op een server die niet verbonden is met het internet. Het voordeel van proactie is dat het risico (grotendeels) wordt weggenomen. Het nadeel is dat het de bedrijfsvoering bemoeilijkt en/of dat er hoge (extra) kosten aan verbonden (kunnen) zijn. Preventie is het nemen van maatregelen vooraf om de risico's zo klein mogelijk te houden en de mogelijke gevolgen te beperken indien deze zich toch voordoen. Te denken valt aan toegangsbeheer en netwerksegmentatie. Preparatie is de voorbereiding om (pogingen tot) beveiligingsinbreuken te kunnen bestrijden. Voorbeelden hiervan zijn het opstellen van plannen en procedures, het opleiden van personeel en het houden van oefeningen. Voorbereiding is nodig, omdat er altijd een kans is dat preventieve maatregelen niet of onvoldoende werken. Het is echter waarschijnlijker dat preventieve maatregelen niet correct worden getroffen (bijvoorbeeld door menselijke fouten). Repressie is de daadwerkelijke bestrijding van (pogingen tot) beveiligingsinbreuken. De belangrijkste voorwaarde voor succesvol repressief optreden is kennis en ervaring. Daar doet zich tegelijkertijd het grootste probleem voor. Cyberaanvallen doen zich in vele vormen voor. Tegelijkertijd is er niet altijd voldoende bekend over (nieuwe) vormen van cyberaanvallen waardoor beslissingen moeten worden genomen op basis van beperkte informatie.



Uit het onderzoek komt naar voren dat het merendeel van de bedrijven in de maritieme sector zich in zekere mate bewust is van de cyber security risico's waarmee zij te maken (kunnen) krijgen. Door veel bedrijven zijn er zodoende (beleidsmatige, technische en/of personele) maatregelen genomen om cyber security risico's (waar mogelijk) te voorkomen en (waar nodig) te reduceren om de continuïteit van hun bedrijfsvoering te waarborgen. Het ontbreekt hierbij soms aan een integrale blik waardoor de getroffen maatregelen zich concentreren op één of enkele schakels van de veiligheidsketen. Het mogelijke gevolg is dat er bijvoorbeeld aanzienlijk wordt geïnvesteerd in preventie, maar minder in repressie. Of andersom. Ook worden beleidsmatige of technische maatregelen soms teniet gedaan door menselijk falen. Om de cyberweerbaarheid van een onderneming substantieel te bevorderen is een integrale blik vereist waarbij maatregelen worden getroffen in alle fasen van de veiligheidsketen.

“Er is een basislevel waar bedrijven in de haven aan moeten voldoen om weerbaar te zijn. Dit gaat niet alleen om cyber security maar ook om fysieke beveiliging. Een integrale blik is nodig. Oog voor vitale processen, kwetsbaarheden en maatregelen. Aandacht voor dreigingen van buitenaf bijvoorbeeld met een pentest en van binnenuit bijvoorbeeld met social engineering. Hierover kunnen veel meer best practices en lessons learned worden gedeeld.” (Respondent interview)

Daarnaast is het van belang dat een bedrijf bij het bevorderen van de cyberweerbaarheid verder kijkt dan de eigen organisatie en waar mogelijk en gewenst ook de samenwerking opzoekt met andere organisaties in de keten om de gezamenlijk de cyberweerbaarheid te bevorderen.

“Misschien moeten we ons bij het bevorderen van de cyberweerbaarheid niet alleen richten op de bedrijven zelf, maar ook op de ICT leveranciers die hun ICT beheren en onderhouden. Een suggestie is om professionele standaarden op het terrein van cyber security met elkaar af te spreken die ook van toepassing zijn voor ICT leveranciers.” (Respondent interview)

6. Initiatieven op cyberweerbaarheid

In dit hoofdstuk wordt ingegaan op het speelveld van (publieke en branche) organisaties, (lokale, regionale en nationale) samenwerkingsverbanden en initiatieven (in de maritieme sector) op het terrein van cyber security in de MRDH regio.

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) opereert als zelfstandige dienst van het ministerie van Justitie en Veiligheid en is het nationale expertisecentrum voor cybersecurity dat als doel heeft om de Nederlandse samenleving en in het bijzonder de vitale infrastructuur digitaal weerbaarder te maken. Het NCSC is het nationale knoop- en informatiepunt op het gebied van cybersecurity en deelt kwetsbaarheden, incidenten en dreigingen die op nationaal niveau spelen. Primair heeft het NCSC tot taak om aanbieders van vitale processen, producten en/of diensten en organisaties binnen de rijksoverheid te informeren en adviseren over (dreigende) cyber security incidenten en daarvoor analyses en technisch onderzoek te verrichten. De Haven van Rotterdam behoort tot de vitale infrastructuur en valt hierdoor onder de verantwoordelijkheid van het NCSC. De overige havens worden niet als vitale infrastructuur aangemerkt en vallen hierdoor onder de verantwoordelijkheid van het Digital Trust Center (DTC). Het NCSC beschikt regelmatig over informatie over digitale dreigingen of incidenten die ook relevant is voor bedrijven in de maritieme sector die actief zijn in andere havens (dan de Haven van Rotterdam). Momenteel ontbreekt het (nog) aan de wettelijke basis om deze informatie te verstrekken aan organisaties die geen onderdeel uitmaken van de vitale infrastructuur (www.ncsc.nl).

Digital Trust Center

Het Digital Trust Center (DTC) heeft als doel om ongeveer 2 miljoen Nederlandse bedrijven cyberweerbaar te maken die niet tot de vitale sectoren behoren (en hierdoor niet tot de primaire doelgroep van het NCSC behoren). Het DTC probeert ondernemers op verschillende manier te bereiken. Zo biedt het DTC op haar website op een laagdrempelige manier kennis, informatie en advies aan ondernemers hoe zij hun cyberweerbaarheid kunnen bevorderen. Voorbeelden hiervan zijn de basisscan cyberweerbaarheid waarmee ondernemers de cyberweerbaarheid van hun eigen onderneming kunnen toetsen en de 5 basisprincipes van veilig digitaal ondernemen die bedrijven als leidraad kunnen gebruiken om de basale digitale cyber security maatregelen op orde te krijgen. Daarnaast heeft het DTC een online community in het leven geroepen waar ondernemers opgedane kennis en ervaring kunnen uitwisselen op het terrein van cyber security. Ook verspreidt het DTC via de online community actuele informatie over cyber security dreigingen vanuit het NCSC. Het DTC is niet in staat om alle ondernemers te bereiken. Om haar bereik te vergroten werkt het DTC samen met brancheorganisaties en (publieke en/of private) samenwerkingsverbanden die ondernemers bijstaan om hun cyberweerbaarheid te bevorderen. Deze samenwerkingsverbanden kunnen samenwerken in een keten, sector, branche en/of regio (lokaal, regionaal, nationaal). Een voorbeeld van een dergelijk samenwerkingsverband in de maritieme sector is FERM, een stichting die zich inzet voor de cyberweerbaarheid van bedrijven die actief zijn in het Rotterdams havengebied. FERM wordt ondersteund door het DTC (www.digitaltrustcenter.nl).

Security Delta

Security Delta (HSD) is hét nationale veiligheidscluster waar ongeveer 275 bedrijven, overheidsorganisaties en kennisinstellingen samenwerken aan de cyberweerbaarheid van de digitaliserende samenleving. Dit doet de HSD door de kennis van haar partners te delen en samen te werken aan innovatieve veiligheidsoplossingen. De focus ligt hierbij op cybersecurity & -weerbaarheid, data & AI/intel en slimme veilige samenlevingen. De Security Delta biedt bedrijven toegang tot kennis over cyber security, toegang tot innovatie op het terrein van vooruitstrevende

(technologische) oplossingen voor complexe vraagstukken, toegang tot de markt door het matchen van probleemeigenaren met probleemoplossers, toegang tot kapitaal voor de financiering van oplossingen en toegang tot cyber security talent (www.securitydelta.nl).

Centrum voor Criminaliteitspreventie en Veiligheid

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een stichting die zich inzet om veiligheidsproblemen in kaart te brengen en op te lossen. Daarvoor biedt het CCV kennis, instrumenten, keurmerken, voorlichtingsmateriaal en advies op maat gericht op onder andere cyber security aan overheden en bedrijven met preventie als uitgangspunt. Het CCV biedt op haar website kennis, informatie en advies aan ondernemers hoe zij hun cyberweerbaarheid kunnen bevorderen. Daarnaast brengt het CCV frequent een (online) nieuwsbrief en vakblad uit over veiligheidsvraagstukken (ondermeer op het terrein van cyber security). Tevens brengt het CCV handreikingen uit over de aanpak van cyber security vraagstukken. Ook organiseert en verzorgt het CCV webinars, fysieke bijeenkomsten en trainingen op het terrein van cyber security. Tot slot geeft het CCV advies op maat aan ondernemers ten aanzien van de bevordering van cyberweerbaarheid (www.hetccv.nl).

VNO NCW MKB Nederland

De werkgeversorganisaties VNO NCW en MKB Nederland hebben met het initiatief Samen Digitaal Veilig de handen in een geslagen om de cyberweerbaarheid van ondernemers te bevorderen. Samen Digitaal Veilig is een praktische tool om MKB bedrijven en medewerkers op te leiden in digitale veiligheid. Medewerkers worden getraind via korte opleidingsvideo's en vragen. Via een automatische uitvraag ziet de ondernemer of zijn IT-leverancier de zaken goed heeft geregeld. Na het invullen van een veiligheidsscan door de ondernemer komen alle resultaten en voortgang van de organisatie, leveranciers en medewerkers in één veiligheids-dashboard te staan. Het platform Samen Digitaal Veilig wordt uitgerold via een groot aantal branche- en ondernemersverenigingen (www.samendigitaalveilig.nl).

Transport en Logistiek Nederland

Transport en Logistiek Nederland (TLN) is een brancheorganisatie voor ondernemers in de logistieke sector waar ook bedrijven die actief zijn in havens onderdeel van uit (kunnen) maken. Ondernemers kunnen bij TLN kennis en expertise inwinnen over uiteenlopende thema's op het terrein van logistiek. TLN heeft zelf niet (meer) de kennis en expertise in huis op het terrein van cyber security. Wanneer ondernemers met vragen over cyber security terecht komen bij TLN dan worden zij veelal doorverwezen naar het DTC. Ook wordt door TLN doorverwezen naar Samen Digitaal Veilig van VNO NCW MKB Nederland aangezien ongeveer 75% van de leden van TLN een MKB onderneming betreft (www.tln.nl).

Evofenedex

Evofenedex is een ondernemersvereniging en netwerk van Nederlandse handels- en productiebedrijven met een logistieke of internationale operatie waar ook bedrijven die actief zijn in havens onderdeel van uit (kunnen) maken. Evofenedex heeft ongeveer 12.000 leden die continue te maken hebben met veranderingen in hun (logistieke) ketens. Ook is er sprake van toenemende concurrentie waardoor verdienmodellen onder druk (kunnen) komen te

staan. Een van de speerpunten van Evofenedex is de digitalisering van de bedrijfsprocessen van ondernemers in hun sector. Digitalisering levert naast economische kansen (zoals kostenbesparing door efficiëntie en nieuwe producten en diensten door innovatie) ook cyber security risico's op. Tot dus ver is er vooral aandacht voor de kansen en minder voor de risico's van digitalisering (www.evofenedex.nl).

IRO

IRO is de brancheverenigingvoor Nederlandse toeleveranciers in de offshore energie industrie. IRO heeft ongeveer 400 leden. In eerste instantie waren die met name actief in olie en gas, maar nu ook in waterstof en windmolens (op zee). De activiteiten van IRO omvatten het verlenen van ondersteuning op het gebied van vertegenwoordiging aan overheden en potentiële opdrachtgevers, het bevorderen van export, het ontwikkelen van nieuwe technologieën en het bieden van informatievoorzieningen. Cyberweerbaarheid wordt af en toe belicht door IRO richting haar leden. Zo heeft IRO in het verleden met het Innovation Quarter een workshop gehad bij de Security Delta (Campus). Gezien de mate van cyberweerbaarheid van (een aanzienlijk deel van) de leden van IRO is het van belang om hier in de toekomst frequent aandacht aan te (blijven) besteden. IRO gaat hiervoor in principe graag de samenwerking aan met anderen organisaties, netwerken en samenwerkingsverbanden (www.iro.nl).

Deltalinqs

Deltalinqs vertegenwoordigd als ondernemersvereniging meer dan 95% van alle logistieke, haven en industriële bedrijven in de Haven van Rotterdam. Het betreft ruim 700 bedrijven uit verschillende sectoren. Deltalinqs zet zich ondermeer in voor de thema's infrastructuur en bereikbaarheid, veiligheid en security. Deltalinqs organiseert hierover ook diverse trainingen en bijeenkomsten. Daarnaast kunnen bedrijven de website van Deltalinqs raadplegen, hun nieuwsbrief ontvangen en podcast beluisteren (www.deltalinqs.nl).

FERM

FERM is onderdeel van het Port Cyber Resilience Programma. Doel van het programma is het stimuleren van samenwerking tussen bedrijven in de Haven van Rotterdam en het verhogen van het bewustzijn met betrekking tot cyber security risico's om zo de best digitaal beveiligde haven van de wereld te worden. Het programma is een initiatief van gemeente Rotterdam, Havenbedrijf Rotterdam, Veiligheidsregio Rotterdam Rijnmond, DCMR Milieudienst Rijnmond, Provincie Zuid-Holland, Zeehavenpolitie en Deltalinqs. FERM legt zich steeds meer toe op het bevorderen van de cyberweerbaarheid (in navolging op het bevorderen van het bewustzijn ten aanzien van cyber security risico's). FERM wordt/is zodoende omgevormd naar een organisatie die actief cyberweerbaarheidsdiensten aanbiedt aan de bedrijven actief in de Haven van Rotterdam. FERM deelt op haar website actuele nieuwsberichten over cyber security die relevant zijn voor bedrijven die actief zijn in de Haven van Rotterdam. Ook worden er tools gedeeld en een overzicht van gespoofde websites die potentiële kopers proberen op te lichten met fictieve opslagcapaciteiten en voorraden van grondstoffen en goederen in terminals in de Haven van Rotterdam. Daarnaast organiseert FERM ongeveer 5 keer per jaar een Port Cyber Café waar bedrijven onderling opgedane kennis en ervaringen kunnen uitwisselen op het terrein van cyber security. Ook organiseert FERM jaarlijks een gezamenlijke cybercrisisoefening 'Cybernautics' waar bedrijven en veiligheidspartners uit de Haven van Rotterdam aan deelnemen. Tevens is het Haven Cybermeldpunt in gebruik voor het melden van

IT-verstoringen met invloed op het laden en lossen, aan- en afmeren en op veiligheidsmaatregelen in het kader van de Havenbeveiligingswet. Deelnemers van FERM krijgen een nulmeting op het terrein van cyberweerbaarheid. Daarnaast zijn ongeveer 700 bedrijven in de haven van Rotterdam passief gescand door Threadstone (een partner van de Security Delta).

FERM heeft de OKTT-status toegewezen gekregen. Het NCSC kan vanuit zijn wettelijke grondslag alleen informatie over dreigingen en incidenten delen met een samenwerkingsverband dat objectief kenbaar tot taak (OKTT) heeft andere organisaties of het publiek te informeren. Dankzij de toekenning van de OKTT-status kan het NCSC FERM voorzien in tijdige, actuele en relevante dreigingsinformatie die FERM op haar beurt kan delen met bedrijven in de Haven van Rotterdam die lid zijn van het samenwerkingsverband van FERM.

FERM staat open voor samenwerking, bijvoorbeeld met de Security Delta. FERM richt zich op bedrijven actief in het Rotterdamse havengebied. De Security Delta richt zich op alle bedrijven ongeacht de sector of de regio waarin deze actief zijn. Zo zou nieuwe technologie op het terrein van cyber security die wordt ontwikkeld met betrokkenheid van de Security Delta als pilot kunnen worden toegepast in het Rotterdamse havengebied onder begeleiding van FERM. Hiervoor zou gezamenlijk kunnen worden opgetrokken bij het werven van het benodigd budget voor een dergelijke pilot middels het aanvragen van subsidies. Ook kan er gezamenlijk een rondetafel worden georganiseerd over een actueel cyber security vraagstuk gerelateerd aan de maritieme sector. Een suggestie voor een onderwerp voor een rondetafel is de omgang met storage spoofing.

Haven Information Sharing and Analysis Centre

Het Haven Information Sharing and Analysis Centre (ISAC) is een sectoraal overleg van bedrijven en organisaties actief in de maritieme sector. Het doel van het Haven ISAC is door uitwisseling van opgedane kennis en ervaring de digitale weerbaarheid van de afzonderlijke bedrijven en de maritieme sector in zijn geheel te bevorderen. Deelnemende bedrijven en organisaties kunnen leren van cyber security incidenten die zich elders hebben voorgedaan en van maatregelen die door andere organisaties zijn getroffen om zodoende soortgelijke cyber security incidenten in de eigen organisatie te voorkomen dan wel te beperken.

iTanks

iTanks is een kennis- en innovatieplatform voor de haven gerelateerde industrie. iTanks verbindt bedrijven, kennisinstituten en industrie experts met elkaar en introduceert deze partijen met nieuwe technologie van binnen en buiten de sector. iTanks heeft recent een bijeenkomst georganiseerd voor ondernemers over cyber security, zodat ze ook bekend raken met de risico's die gepaard (kunnen) gaan met digitalisering (www.itanks.eu.nl).

Maritieme Delta

Maritime Delta is een samenwerkingsverband tussen bedrijven**,** onderwijs- en kennisinstellingen**,** brancheorganisaties en overheden in het maritieme cluster van Zuid**-**Holland. Maritime Delta draagt bij aan de vorming van samenwerkingsverbanden en het realiseren van innovatiedoelstellingen van consortia van bedrijven, waaronder digitalisering (www.maritimedelta.nl).

Koninklijke Vereniging van Nederlandse Reders

De Koninklijke Vereniging van Nederlandse Reders (KVNR) vertegenwoordigt de in Nederland gevestigde reders die actief zijn in de zeevaart. Het doel van de KVNR is dat de reders wereldwijd onbelemmerd en veilig kunnen varen. De KVNR is al een aantal jaren actief op het thema cyber security. Vanaf begin 2021 zijn er verplichtingen op het terrein van cyber security voor managementsystemen waar reders aan moeten voldoen. Er is sprake van een gevarieerd ledenbestand van de KVNR op wie dit betrekking heeft: van geavanceerde schepen tot low tech schepen. Schepen gaan gemiddeld ruim 30 jaar mee. Een schip wordt regelmatig uitgebreid met nieuwe techniek. Dit betekent dat er door de jaren heen een stapeling van techniek plaatsvindt wat de complexiteit ervan vergroot.

De KNVR is in gesprek met het DTC en haar leden over het opzetten van een Information Sharing and Analysis Centre (ISAC) voor reders met zeeschepen. FERM legt de focus op het Rotterdamse havengebied (de wal), terwijl de KVNR zich focust op de activiteit op zee. Daarnaast werkt een vakgroep samen met de Stenden Hogeschool die systemen van zeeschepen inventariseert op het terrein van cyber security op basis waarvan algemene richtlijnen en handleidingen kunnen worden opgesteld (www.knvr.nl).

DigiShape

DigiShape is een open innovatieplatform van en voor bedrijven, kennisinstellingen en overheden, die samen de grote potentie van digitalisering voor de watersector willen benutten. Door slim gebruik te maken van data-innovaties en digitalisering kan de watersector kosten besparen, de kwaliteit verhogen en risico's beperken. Overheden, bedrijfsleven en kennisinstellingen zijn dan ook bezig om data vanuit verschillende bronnen slimmer in hun bedrijfsprocessen te integreren. Desondanks worden data, technieken en kennis nog onvoldoende met elkaar gedeeld. DigiShape is opgericht om al lopende initiatieven op het gebied van data science te koppelen en veelbelovende nieuwe technieken te signaleren, uittesten en implementeren. Digishape fungeert als proeftuin onder de Topsector Water & Maritiem. DigiShape zou in de toekomst aandacht kunnen besteden aan security bij design en ketenafhankelijkheid (www.digishape.nl).

Platform Veilig Ondernemen Rotterdam

Het Platform Veilig Ondernemen (PVO) Rotterdam zet zich in regio van de politie eenheid Rotterdam ondermeer in voor de bevordering van de cyberweerbaarheid van ondernemers. Deelnemers van het PVO Rotterdam zijn: MKB Nederland, VNO NCW, ondernemersverenigingen, gemeenten, politie en Openbaar Ministerie. Het PVO faciliteert 25 gemeenten en hun (veiligheids)partners die op hun beurt met (lokale) ondernemersverenigingen samenwerken om ondernemers te bereiken. Door het organiseren van ondermeer (online en fysieke) bijeenkomsten wordt getracht om ondernemers te informeren over cyber security risico’s en vervolgens te activeren om hun cyberweerbaarheid te bevorderen.

De focus van het PVO Rotterdam ligt hierbij met name op MKB bedrijven omdat deze hiertoe over het algemeen minder goed zelfstandig in staat zijn dan grotere bedrijven en zodoende doorgaans meer ondersteuning nodig hebben om hun cyberweerbaarheid te bevorderen. Het PVO Rotterdam faciliteert waar mogelijk en gewenst publiek-private samenwerkingsverbanden op het terrein van cyber security in de regio Rotterdam. Een voorbeeld hiervan is het Cybernetwerk Zuid Hollandse Eilanden (ZHE).

VeiligheidsAlliantie regio Rotterdam

De VeiligheidsAlliantie regio Rotterdam (VAR) is een samenwerkingsverband van 25 gemeenten, de politie en het Openbaar Ministerie binnen de regio van de politie eenheid Rotterdam. De VAR functioneert binnen de regio als platform om kennis en ervaring te delen rond veiligheidsvraagstukken (waaronder cyberweerbaarheid). Daarnaast ondersteunt de VAR regionale samenwerking tussen partners door actief te signaleren, agenderen, initiëren en verbinden. De VAR zet zich ondermeer in voor de aanpak van cybercriminaliteit in haar regio. De VAR heeft zich bij de Vereniging van Nederlandse Gemeenten (VNG) sterk gemaakt om de voorkoming en aanpak van cybercriminaliteit een plek te geven in het kernbeleid veiligheid die als handreiking dient voor gemeenten bij de ontwikkeling van hun integraal veiligheidsbeleid. Zodoende is het focusblad digitale veiligheid ontwikkeld dat onderdeel uitmaakt van kernbeleid veiligheid. Het focusblad biedt gemeenten handvatten bij het opnemen en uitwerken van het thema digitale veiligheid in het lokale integraal veiligheidsplan (IVP). Het focusblad beschrijft de te onderscheiden veiligheidsrisico's, de rol van de gemeente rond deze risico's en het aanbevolen pad voor de uitwerking van dit thema in het integraal veiligheidsplan. Daarnaast biedt de VAR gemeenten ondersteuning bij het initiëren van activiteiten om de cyberweerbaarheid van ondermeer ondernemers te bevorderen. Op deze manier kunnen gemeenten ook daadwerkelijk invulling geven aan digitale veiligheid uit hun integraal veiligheidsplan (www.veiligheidsalliantie.nl).

Cybernetwerk Zuid Hollandse Eilanden

Het Cybernetwerk Zuid Hollandse Eilanden (ZHE) is opgericht om MKB bedrijven te helpen maatregelen te nemen tegen cybercriminaliteit om mogelijk slachtofferschap te voorkomen. Het Cybernetwerk ZHE is een publiek-privaat samenwerkingsverband wat actief is op de Zuid-Hollandse Eilanden: Hoeksche Waard, Voorne Putten en Goeree-Overflakkee. Partners zijn onder andere gemeenten, Rabobank, VeiligheidsAlliantie regio Rotterdam, MKB Rotterdam en Platform Veilig Ondernemen (PVO) Rotterdam. Het cybernetwerk ZHE organiseert (fysieke) kennisbijeenkomsten, online seminars en online trainingen voor haar doelgroep. Daarnaast brengt zij een nieuwsbrief uit en stelt zij tools beschikbaar. Ook worden nulmetingen verricht op het terrein van cyberweerbaarheid en worden nepadvertenties op sociale media geplaatst om de bewustwording ten aanzien van cyber security risico's te bevorderen.

Het betreft een veelzijdig aanbod waar ondernemers (kosteloos) gebruik van (kunnen) maken. Voor een deel gaat het om het opnieuw delen van reeds bestaande handvatten, zoals tools die door een andere organisatie zoals het DTC zijn ontwikkeld en beschikbaar zijn gesteld. Het DTC kan haar tools via het Cybernetwerk ZHE bij de doelgroep terecht laten komen zodat ze hier kennis van kunnen nemen en hier desgewenst ook gebruik van gaan maken (www.cybernetwerkzhe.nl).

Platform Veilig Ondernemen Den Haag

Het Platform Veilig Ondernemen (PVO) Den Haag zet zich in de regio van de politie eenheid Den Haag ondermeer in voor de bevordering van de cyberweerbaarheid van ondernemers. Het PVO Den Haag faciliteert 28 gemeenten en hun (veiligheids)partners. PVO Den Haag valt in deze regio samen met het Regionaal Samenwerkingsverband Integrale Veiligheid (RSIV). Het PVO Den Haag heeft zich de afgelopen jaren ingezet voor het weerbaarder maken van ondernemers tegen cybercriminaliteit, bijvoorbeeld met trainingen. Ook is er door het PVO Den Haag geïnvesteerd in het opzetten van publiek private samenwerkingsverbanden, bijvoorbeeld rond bedrijventerreinen en winkelcentra.

Nederland beschikt over tien PVO's. Iedere politie eenheid beschikt over een PVO. Door het kabinet is ongeveer 10 miljoen euro beschikbaar gesteld om de PVO's te versterken. Een deel van het budget komt terecht bij het CCV dat een landelijk netwerk inricht waar de PVO's informatie met elkaar kunnen uitwisselen, zodat niet in ieder PVO het wiel opnieuw hoeft te worden uitgevonden. Het overige overgrote deel van het budget komt bij de tien PVO's terecht, waaronder het PVO Den Haag. Het PVO Den Haag is voornemens om een deel van dit budget aan te wenden voor de bevordering van cyberweerbaarheid van ondernemers (waaronder die actief zijn in de logistieke sector).

Regionaal Samenwerkingsverband Integrale Veiligheid

Het Regionaal Samenwerkingsverband Integrale Veiligheid (RSIV) bestaat uit 27 gemeenten, de politie en het Openbaar Ministerie. Het RSIV zet zich in op gezamenlijke prioriteiten op regionaal niveau (waaronder de aanpak van cybercriminaliteit). Het betreft veiligheidsvraagstukken die in het merendeel van de gemeenten spelen, waarop een gezamenlijke integrale aanpak gewenst is en waarover bestuurlijk draagvlak is om hierover op regionaal niveau afspraken te maken. De prioriteiten voor de komende vier jaar staan in het Regionaal Beleidsplan (RBP) 2019-2022. Inmiddels zijn ook de eerste voorbereidingen gestart voor het Regionaal Beleidsplan 2023-2026. De nieuwe regionale prioriteiten zullen voor een belangrijk deel worden bepaald door het Algemeen Veiligheidsbeeld van de eenheid Den Haag 2021. De belangrijkste doelstelling van het RSIV is het praktisch ondersteunen van de netwerkpartners bij het uitvoeren van het Regionaal Beleidsplan, bijvoorbeeld door het organiseren van regionale kennis- en netwerkbijeenkomsten en het ontwikkelen van concrete beleidsinstrumenten (www.rsiv.nl).

Cyber Netwerk Drechtsteden

Het Cyber Netwerk Drechtsteden (CND) is een samenwerkingsverband dat cyberweerbaarheid onder de aandacht brengt bij MKB bedrijven in de regio Drechtsteden. Partners van het CND zijn HBO Drechtsteden, IMC, VitrumNet, Hoek en Blok IT. Het doel van CND is om bedrijven in de regio bewust te maken van de risico's die digitalisering en cyberbedreigingen voor de bedrijfsvoering kunnen vormen. Door het beschikbaar stellen van middelen en tools geeft het CND bedrijven in de Drechtsteden handvatten om de cyberweerbaarheid te bevorderen. Zo biedt het CND een toolkit en pentesten aan richting bedrijven (www.cybernetwerk.nl).

Centre of Expertise Cybersecurity

Het Centre of Expertise Cybersecurity (CoECS) van de Haagse Hogeschool zet zich in voor het versterken van de cyberweerbaarheid van publieke en private organisaties die zelf in mindere mate zijn toegerust op cyber security dreigingen. Het CoECs verricht onderzoek op drie deelgebieden: mens, organisatie en techniek. In het onderzoek wordt ingegaan op welke menselijke, organisatorische en technische aspecten de cyberweerbaarheid van ondermeer ondernemers beïnvloeden en hoe deze desgewenst kunnen worden verbeterd.

Regionaal Informatie en Expertise Centrum

In het Regionaal Informatie en Expertise Centrum (RIEC) werken onder andere gemeenten, politie, openbaar ministerie en de douane samen aan de aanpak van ondermijnende georganiseerde

criminaliteit zoals drugssmokkel. Iedere politie eenheid heeft de beschikking over een RIEC. Zo is er binnen de MRDH regio een RIEC Rotterdam en RIEC Den Haag. Hiermee kan de samenwerking worden gezocht als het gaat om de aanpak van criminele netwerken die misbruik maken van logistieke processen van bedrijven in de maritieme sector om ongezien drugs te transporten (www.riec.nl).

1. Conclusies en aanbevelingen

Dit hoofdstuk vormt het sluitstuk van de rapportage over cyberweerbaarheid in de maritieme sector. Er wordt antwoord gegeven op de vraagstelling die centraal staat in het onderzoek in het kader van de rapportage. Daarnaast worden aanbevelingen gegeven voor (de versterking van initiatieven ten behoeve van) de bevordering van cyberweerbaarheid van ondernemers in de maritieme sector.

Cyberweerbaarheid van ondernemers in de maritieme sector

Bedrijven in de logistieke sector lopen een niet gering risico om slachtoffer te worden van cybercriminaliteit door de aard van hun bedrijfsactiviteiten, de producten en diensten die ze vervoeren voor derden en/of de mogelijke buit die er bij hun te halen is. Het worst case scenario voor bedrijven in de maritieme sector is dat de informatievoorziening voor de bedrijfsvoering wordt uitgeschakeld of overgenomen waardoor de continuïteit van de bedrijvigheid in het geding komt. Een voorbeeld hiervan is de cyberaanval waarvan Maersk in 2017 slachtoffer werd. Daarnaast lopen de bedrijven in de maritieme sector het risico dat ze door criminele netwerken actief in de georganiseerde (drugs)criminaliteit worden misbruikt om onbewust illegale goederen te vervoeren. Deze criminele netwerken hebben geen baat bij het verstoren van de bedrijfsvoering, maar willen inzicht en/of invloed hebben op de logistieke keten rond een lading waarin hun illegale goederen (zoals drugs) ongezien vervoerd worden. Tot slot is er in de Haven van Rotterdam regelmatig sprake van storage spoofing waarbij potentiële kopers worden opgelicht met fictieve opslagcapaciteiten en voorraden van grondstoffen en goederen in terminals in de Haven van Rotterdam.

Ondanks dat de bedrijven in de maritieme sector met regelmaat worden geconfronteerd met cyber security incidenten wordt hier slechts in beperkte mate melding van gemaakt ondermeer uit angst voor imago en reputatieschade, mogelijke belangenconflicten voortkomend uit strafrechtelijk onderzoek die de bedrijfsvoering (kunnen) frustreren en onduidelijkheid over wat waar wanneer gemeld kan of moet worden naar aanleiding van een (dreigend) cyber security incident. Om cybercriminaliteit in de maritieme sector gericht te kunnen aanpakken is inzicht vereist in de aard, omvang, verschijningsvormen, slachtoffers, kwetsbaarheden, daders en werkwijzen. Om dit te bewerkstelligen is het van belang dat de meldingsbereidheid van slachtofferschap van cybercriminaliteit wordt bevorderd, bijvoorbeeld met de pagina op de website van FERM met alle meldpunten.

Het toezicht op bedrijven in de maritieme sector is versnipperd en daarnaast ontbreekt het mandaat om te handhaven op het terrein van cyber security. In de Haven van Rotterdam houdt het Havenbedrijf toezicht op maritiem. De douane is toezichthouder op logistiek en DCRM Milieudienst Rijnmond is toezichthouder op Brzo-bedrijven die werken met grote hoeveelheden gevaarlijke stoffen. Het streven is om in de toekomst te gaan werken met één gemeenschappelijk toetsingskader op het terrein van cyber security.

Ketenafhankelijkheid ten aanzien van cyberweerbaarheid

Het merendeel van de bedrijven in de maritieme sector is zich in zekere mate bewust van de cyber security risico's waarmee zij te maken (kunnen) krijgen. Door veel bedrijven zijn er zodoende (beleidsmatige, technische en/of personele) maatregelen genomen om cyber security risico's (waar

mogelijk) te voorkomen en (waar nodig) te reduceren om de continuïteit van hun bedrijfsvoering te waarborgen. Het ontbreekt hierbij soms aan een integrale blik waardoor de getroffen maatregelen zich concentreren op één of enkele schakels van de veiligheidsketen. Ook worden beleidsmatige of technische maatregelen soms teniet gedaan door menselijk falen wat de kans op insider threats verhoogt. Om de cyberweerbaarheid van een onderneming substantieel te bevorderen is een integrale blik vereist waarbij maatregelen worden getroffen in alle fasen van de veiligheidsketen.

Daarnaast wordt er tussen bedrijven in ketens nog niet altijd samengewerkt aan cyberweerbaarheid, terwijl een cyber security incident ergens in de keten ook aanzienlijke gevolgen kan hebben voor de gehele keten. Dit is een gemiste kans omdat door informatie over kwetsbaarheden, dreigingen, (bijna) incidenten, best practices en lessons learned te delen de cyberweerbaarheid van afzonderlijke bedrijven en daarmee van de gehele keten kan worden bevorderd.

Initiatieven om de cyberweerbaarheid te bevorderen

In de MRDH regio zijn verschillende samenwerkingsverbanden actief die zich inzetten voor de bevordering van cyberweerbaarheid van ondernemers. Het overgrote deel van deze samenwerkingsverbanden richt zich op alle ondernemers ongeacht de sector waarin zij actief zijn. FERM onderscheidt zich hierin door zich te focussen op het bevorderen van de cyberweerbaarheid van bedrijven die actief zijn in het Rotterdamse havengebied. Bij bedrijven in andere havens is er ook behoefte aan (sectorale) samenwerking en informatiedeling ten behoeve van de cyberweerbaarheid. Hier zou door FERM (desgewenst in samenwerking met andere regionale en sectorale samenwerkingsverbanden) in kunnen worden voorzien door opgedane kennis en ervaringen in het Rotterdamse havengebied ook te delen met (bedrijven actief in) andere havens in de regio.

Ondernemers activeren om de cyberweerbaarheid te bevorderen

Ondanks de niet geringe kans op slachtofferschap van cybercriminaliteit treffen bedrijven in de maritieme sector (nog) niet altijd de benodigde (beleidsmatige, technische, personele) maatregelen om cyber security risico's (waar mogelijk) te voorkomen en (waar nodig) te reduceren om de continuïteit van hun bedrijfsvoering te waarborgen. Om de cyberweerbaarheid van afzonderlijke bedrijven en de gehele keten te bevorderen is het van belang dat ondernemers worden geactiveerd om daadwerkelijk maatregelen te treffen.

Ondernemers kunnen worden geactiveerd om te investeren in cyber security door ze te wijzen op cyber security dreigingen en de mogelijke impact daarvan. Daarnaast kunnen bedrijven als opdrachtgever samenwerkingspartners aansporen en/of voorschrijven (middels samenwerkingsvoorwaarden) om hun cyber security op orde te hebben. Tot slot kan in de toekomst regulering en toezicht en handhaving op wet- en regelgeving door overheden vanuit één gemeenschappelijk toetsingskader op het terrein van cyber security bedrijven aansporen om hun cyberweerbaarheid te bevorderen.

In de sector maritiem wordt geïnvesteerd in innovatie en digitalisering van bedrijfsprocessen, maar hierbij wordt niet altijd voldoende nagedacht over de bijkomende cyber security risico's. Dat hangt nauw samen met een gebrek aan medewerkers binnen de sector die op het gebied van cybersecurity tijdig dreigingen kunnen signaleren en verhelpen. Als er bestuurlijk of operationeel aandacht is voor cybersecurity dan is dat vaak nog niet verankerd in de bedrijfsvoering, functies en ontwikkeling. Er zijn twee Security Delta hulpmiddelen die gericht zijn op het vervullen van de

behoefte aan relevant opgeleide cybersecurity werknemers, namelijk cybersecuritywerkt.nl (zij instroom/omscholing/ startersfuncties) en securitytalent.nl (vacatures/opleidingen/beroepsprofielen/ arbeidsmarkt).

Bestaande medewerkers binnen de sector met een interesse in cybersecurity zijn de meest toegankelijke resources. Deze medewerkers hebben al de nodige kennis van en ervaring in de sector, maar als hen een kans wordt aangeboden, zijn ze waarschijnlijk bereid om zich om- of bij te scholen op het gebied van cybersecurity binnen de betreffende sector. Om deze doelgroep meer beeld te geven bij de arbeidsmogelijkheden, kan gebruik gemaakt worden van het platform www.cybersecuritywerkt.nl: gericht op het laten doorstromen naar startersfuncties en passende bij-of omscholingstrajecten.

Als er onvoldoende medewerkers zijn met een interesse voor om- of bijscholing, moet er extern geworven worden en daar dient het platform www.securitytalent.nl voor. Dit is meer gericht op specialisten en het behouden en doorontwikkelen binnen security. Een platform waar vacatures, opleidingen en werkgevers staan op het gebied van (digitale) veiligheid.

Aanbevelingen ten aanzien van cyberweerbaarheid

Afsluitend worden onderstaand de belangrijkste aanbevelingen ten aanzien van de bevordering van cyberweerbaarheid in de maritieme sector op een rij gezet.

Er in (meer) inzicht vereist in de aard, omvang, verschijningsvormen, slachtoffers, kwetsbaarheden, daders en werkwijzen om cybercriminaliteit in de maritieme sector gericht te kunnen aanpakken. Om de informatiepositie te verbeteren dient de meldingsbereidheid van slachtofferschap van cybercriminaliteit te worden bevorderd.

Het toezicht op bedrijven in de maritieme sector is versnipperd en daarnaast ontbreekt het mandaat om te handhaven op het terrein van cyber security. Investeer zodoende in het werken met één gemeenschappelijk toetsingskader op het terrein van cyber security.

Getroffen maatregelen richten zich nog te vaak of slecht één of enkele schakels van de veiligheidsketen. Bevorder een integrale blik bij ondernemers waarbij maatregelen worden getroffen in alle fasen van de veiligheidsketen om de cyberweerbaarheid van een onderneming substantieel te bevorderen.

Er is sprake van een grote mate van ketenafhankelijkheid in de maritieme sector ten aanzien van cyberweerbaarheid. Daarom dient te worden ingezet op het onderling delen van informatie over kwetsbaarheden, dreigingen, (bijna) incidenten, best practices en lessons learned waarmee de cyberweerbaarheid van afzonderlijke bedrijven en daarmee van de gehele keten kan worden bevorderd.

Een sectorale aanpak lijkt het meest effectief en efficient daar waar het gaat om de bevordering van de cyberweerbaarheid van ondernemers in de maritieme sector. FERM voorziet hierin daar waar het gaat om ondernemers actief in het Rotterdamse havengebied. Verken wat de mogelijkheden zijn om de opgedane kennis en ervaring van FERM te ontsluiten naar (bedrijven actief in) andere havens (in de regio), zodat zij hier ook hun voordeel mee kunnen doen om hun cyberweerbaarheid te bevorderen.