Cybersecurity

Een advies van de RMB aan de gemeente Rotterdam

Erasmus UPT

Maart 2023

UPT Erasmus
ERASMUS CENTRE FOR
URBAN, PORT AND TRANSPORT ECONOMICS

Colofon

Dit onderzoek is uitgevoerd door het Erasmus Centre for Urban, Port and Transport Economics (Erasmus UPT) in opdracht van de Rotterdam maritime board. De Rotterdam maritime board heeft Erasmus UPT gevraagd haar te begeleiden bij het opstellen van een advies aan het college van B&W ten aanzien van cybersecurity. Dit onderzoek is uitgevoerd onder begeleiding van een klankbordgroep met vertegenwoordigers van FERM, Kotug, Cornelder Holding, Marsh en gemeente Rotterdam. Voor dit onderzoek is gebruik gemaakt van gesprekken met diverse vertegenwoordigers van overheid en bedrijfsleven. De juistheid van de inhoud van deze rapportage is voor verantwoordelijkheid van Erasmus UPT. Wij zeggen de ondervraagde experts onze grote dank voor de bereidheid hun inzichten met ons te delen. Deze rapportage is bedoeld voor de Rotterdam maritime board ter ondersteuning van haar advies. Erasmus UPT aanvaardt geen aansprakelijkheid van derden voor het gebruik van deze rapportage.

Erasmus Centre for Urban, Port and Transport Economics

Auteurs: Albert Veenstra en Martijn Streng

Voor meer informatie kunt u contact opnemen via veenstra@rsm.nl of streng@ese.eur.nl
Bezoekadres Erasmus UPT: Burgemeester Oudlaan 50, Rotterdam, Mandeville Gebouw, kamer T19-13

Samenvatting

De afgelopen decennia is de digitalisering van de wereld in snel tempo toegenomen, waarbij tegenwoordig vrijwel elk proces en activiteit in meer of mindere mate digitaal is. Deze toegenomen digitalisering biedt vele voordelen, maar er zitten ook risico's aan. In dit onderzoek richten wij ons op de cybersecurity-component van dit speelveld.

De Rotterdam maritime board heeft aan Erasmus UPT gevraagd haar te begeleiden bij het opstellen van een advies aan de gemeente Rotterdam ten aanzien van cybersecurity. Het beeld in de Rotterdam maritime board is dat cybersecurity een belangrijk thema zou moeten zijn voor de maritieme community in en rondom de haven en het maritieme cluster in de regio Rotterdam, maar dat dit het om allerlei redenen nog niet is. De Rotterdam maritime board is voornemens om dit thema steviger op de agenda te zetten bij de gemeente Rotterdam. Om dit te realiseren voert Erasmus UPT dit onderzoek uit waarin een viertal elementen worden uitgewerkt:

1. **Definitie en context**. Wat verstaan we precies onder cybersecurity en welke elementen moeten in gedachten gehouden worden bij de verdere rapportage.
2. **Inventarisatie en overzichten**. Het overzicht van de belangrijkste stakeholders, initiatieven en documenten verduidelijkt welke stappen waar al gezet worden en hoe verschillende zaken complementair zijn of wellicht overlappen.
3. **Positie en behoefte.** De positie en de behoefte die verschillende stakeholders op dit moment hebben beantwoorden de vragen waar verschillende stakeholders staan op het gebied van cybersecurity, maar ook waar ze naar toe zouden willen.
4. **Rollen en aanbevelingen.** Tot slot werken wij concreter uit welke rollen de verschillende stakeholders zouden kunnen pakken? Hierbij worden enerzijds concrete acties gedefinieerd, waarbij anderzijds meer hoog over richtingen worden aangegeven.

Cybersecurity is urgent

Op 6 maart 2023 werd Royal Dirkzwager getroffen door een cyberaanval. De diensten Ship2Report, ISPS, Pax en ROAM zijn verstoord en niet beschikbar. Het systeem Ship2Report wordt gebruikt door zo'n 800 bedrijven in de maritieme sector.

Het onderzoek naar de oorzaak en het opnieuw opstarten van de systemen duurde enkele dagen. De systemen waren uiteindelijk op 12/13 maart weer in de lucht.
Als vervanging voor de verstoorde systemen was op 9 maart uitgeweken naar Portcall Web als alternatief voor Ship2Report. Ook voor het systeem Pax was binnen twee dagen een workaround beschikbaar, in nauwe samenwerking met de havenpolitie en Portbase.

De berichtgeving op dit moment (14 maart) is dat systemen het weer doen, maar dat de gevolgen van de aanval nog niet helemaal verdwenen zijn. Een aantal deelsystemen werken nog niet, en de stabiliteit van beschikbare systemen kan nog lager zijn dan gewenst. Een inschatting van de financiële consequenties is er nog niet.

Bron: https://dirkzwager.com/nieuws/royal-dirkzwager-victim-of-cyber-attack/

Definitie en context

De schets van definitie en context leidt tot een vijftal aandachtgebieden voor het Rotterdamse haven- en maritieme cluster, inclusief de stakeholders:

- De stand van zaken, en mogelijke voortrekkersrol van het maritieme complex in de directe weerbaarheid ten aanzien van cybersecurity.
- De cyberweerbaarheid van het MKB in de maritieme sector. Deze bedrijven werken wel in ketens en netwerken samen met heel veel andere bedrijven, en hun cyberkwetsbaarheid is daarmee wel relevant.
- De cyberweerbaarheid van de gemeente zelf is een dimensie.
- Tenslotte is er de dimensie van individuen, consumenten, medewerkers, werknemers waarvoor de bewustwording van cyberrisico's in hun eigen omgeving, zowel wonen en werken, meer aandacht zou moeten krijgen.
- De verbondenheid van bedrijven in het ontwikkelen van complexe maritieme productie en dienstverlening is een extra risico in het cybersecuritydomein.

Overzicht stakeholders, beleid en initiatieven

Deze aandachtspunten komen voor een beperkt gedeelte al terug in de huidige overzichten van stakeholders en initiatieven en/of beleid. Vanuit de wetgeving is de EU wetgeving, specifiek de NIB richtlijnen, dominant; deze worden vervolgens doorvertaalt in soortgelijke nationale Nederlandse wetgeving. De hoeveelheid en scope van de partijen die onder de NIB2 vallen ten opzichte van de oorspronkelijke richtlijn neemt flink toe. Qua stakeholders is een breed beeld zichtbaar van type partijen die zich bezig houden met cybersecurity. Zowel op publiek niveau, als ook op publiek-privaat en privaat niveau zijn diverse partijen bezig met cybersecurity en de verschillende componenten daarvan. Door middel van kennisdeling, risico analyses en preventieve maatregelen wordt het thema benaderd, al dan niet vanuit een commerciële invalshoek. Deze stakeholders voeren een diverse set aan initiatieven uit, welke voor een deel gekaderd worden door diverse documenten die uitgewerkt worden door deze stakeholders.

Positie en behoefte

De meest directe manier om te komen tot een ambitie om de maritieme sector in de Rotterdamse regio op de kaart te zetten met een effectieve cybersecurity-aanpak is door het grootste hiaat in de gezamenlijke kennis van bedrijven, overheid en kennispartijen in te gaan vullen: wat is nu een ideaal niveau van cybersecurity?

De Rotterdamse maritieme sector is zo rijk geschakeerd dat juist hier in Rotterdam die vraag beantwoord kan en moet worden. Daarvoor is het nodig om de bestaande kennis beter te laten circuleren, en uit te wisselen, en om de unieke kennis in de rest van de Nederlandse economie te benutten, zoals de CYRA-aanpak in Eindhoven. De introductie van de NIB2-regelgeving zal ervoor zorgen dat een groot aantal bedrijven rechtstreeks met cybersecurity-eisen geconfronteerd gaan worden. Hiermee is al een goede start gemaakt via FERM en initiatieven van onder andere het Havenbedrijf Rotterdam. Aanvullend hierop is het nodig om steeds goed te borgen dat de hele keten en de hele maritieme sector uiteindelijk door deze maatregelen geraakt wordt. Deze verantwoordelijkheid is in het ecosysteem nog niet belegd.

Het is ook van belang dat zowel lokaal als nationaal er voldoende begrip is bij de overheid en volksvertegenwoordiging dat cybersecurity in de Rotterdamse regio bijzondere aspecten heeft vanwege het economische belang van haven en maritieme activiteiten, en vanwege de complexe

bedrijfsnetwerken. Dit betekent niet dat 'Rotterdam' helemaal zelf een cyberaanpak moet bedenken. Maar in de manier waarop in Rotterdam de cybersecurity-initiatieven vanuit nationaal niveau worden geadopteerd moet de bijzondere positie van de maritieme sector in Rotterdam wel meegewogen worden. Deze bijzondere positie kenmerkt zich bijvoorbeeld door de sterke ketenverbondenheid, maar ook door de waarde van lading of economische gefaciliteerde waarde die groter is dan de eigen (bedrijfs)waarde. Dit maakt deze sector bijzonder in economische zin, maar dit houdt ook een bijzondere kwetsbaarheid in.

Om deze bijzondere positie te bestendigen is het nuttig om de verschillende lijnen van een effectieve cyberaanpak (governance, kennis, verdediging) in een institutie in de regio bij elkaar te laten komen. Dit zou een organisatie moeten zijn die zoveel mogelijk voortbouwt op en integreert wat er al is.

Ons advies

Deze elementen leiden tot het volgende advies:

Advies: Versterk het cyberweerbaarheidsinitiatief in voor de Rotterdamse maritieme sector

Onze belangrijkste aanbeveling is om voor de maritieme sector in Rotterdam de bestaande cyberweerbaarheidsinitiatieven, waarin FERM en het Havenbedrijf Rotterdam belangrijke rollen hebben, te versterken en uit te bouwen. Daarbij kan de aandacht vooral uitgaan naar de betrokkenheid van het brede maritieme MKB, door middel van het toepassen en uitbouwen van een werkbare MKB cyberveiligheidsstandaard voor de maritieme sector. Uiteindelijk moet het cyberweerbaarheidsinitiatief de volgende componenten bevatten:

1. Een governance structuur. Hierbij adviseren wij tenminste te onderzoeken in hoeverre de bestaande en goed werkende ISPS-governance structuur bruikbaar is, of uitgebreid kan worden om de toezichtsfunctie voor cybersecurity in onder te brengen. Binnen de ISPS structuur zijn in Rotterdam, voor de operaties in de haven, al specifieke initiatieven (cyber meldpunt) genomen. Tegelijkertijd dekt de huidige ISPS-structuur momenteel maar een beperkt deel van de brede maritieme sector af.
2. Een kennisinfrastructuur van en voor bedrijven. De functie van deze kennisinfrastructuur heeft een aantal componenten: allereerst is kennis nodig over het actuele niveau van kwetsbaarheden bij bedrijven, daarnaast is het nodig om een certificeringsmodel voor bedrijven (self-scan, audits, begeleiding voor het implementeren van maatregelen, gericht op het streven naar ISO 27001 niveau) uit te kunnen voeren, en er is kennis nodig over allerlei oplossingen die door dienstverleners worden aangeboden aan MKB bedrijven. FERM voert nu al een deel van deze rollen uit. Het verdient daarom aanbeveling om de mogelijkheden voor uitbreiding van het takenpakket van FERM, alsmede langjarige financiering te verkennen.
3. De derde onmisbare component is de cyberverdedigingscomponent. De invulling van dit deel van een cyberweerbaarheidsinstitutie wordt op dit moment onderzocht, door Deloitte, FERM en het Havenbedrijf Rotterdam. Vanuit dit onderzoek is een belangrijke vraag of een gezamenlijke verdedigingsstructuur zo kan worden ingericht dat die ook voor aanvallen op kleinere bedrijven ingezet kan worden.

Het advies om het cyberweerbaarheidsinitiatief uit te bouwen leidt tot het benoemen van een aantal prioriteiten.

1. Binnen de bestaande ISPS governance structuur moet worden besproken of de uitbreiding van de verantwoordelijkheid naar het hele maritieme cluster en het brede cybersecurityveld wenselijk en

mogelijk is. Hierbij zijn er rollen voor de gemeente (burgemeester, wethouder), de Port Security Officer (de havenmeester) en andere betrokkenen.

2. Voor de uitbreiding van de kennisinfrastructuur en de rol die FERM daarin speelt moet een verkenning worden gestart over middelen en mogelijkheden. Vooral de financiering op de langere termijn is daarbij een belangrijke voorwaarde voor succes. Dit vereist overleg tussen de founding fathers van FERM, de betrokken publieke partners, en de FERM organisatie.
3. Voor wat de inrichting van de cyberverdediging betreft: omdat hier al een onderzoek loopt doen we daar geen uitspraken over. Wel stellen wij voor dat dit onderzoek na afronding breed wordt neergelegd in de maritieme sector, om een goede vervolgdiscussie te krijgen over de verdediging van de hele maritieme sector.

Advies: Besteed binnen de Rotterdamse maritieme cyberweerbaarheid bijzondere aandacht aan ketenafhankelijkheden

Een bijzonder aspect van de situatie in Rotterdam is dat de nadruk van alle drie de componenten sterk zien op de ketenstructuur van het maritieme cluster. Deze structuur wordt gekenmerkt door grote complexiteit, en door een gebrek aan een duidelijke hiërarchie. Rotterdam wordt gekenmerkt door een relatief *groot* aantal leader firms. De druk op kleinere bedrijven om meer aan cybersecurity te doen zal vooral ontstaan vanuit de verplichtingen van NIB-2, en het risico is daarbij dat dat door elk bedrijf anders wordt ingevuld, en dat kleinere bedrijven met verschillende eisen worden geconfronteerd. Dit inzicht, en de specifieke mechanismen om hiermee om te gaan zullen de aanpak in de Rotterdamse maritieme sector onderscheidend maken. Het lijkt onvermijdelijk dat hiervoor een wat sterkere institutionele structuur moet worden ingericht dan in de Brainport Eindhoven.

Naast het inrichten van een meer collectieve aanpak die werkt voor de Rotterdamse situatie is ook nader onderzoek nodig naar de precieze invulling van ketenafhankelijkheden. Dit soort onderzoek is een uitbreiding van het kwetsbaarheidsonderzoek dat nu door de gemeente is uitgezet. Dit onderzoek kijkt vooral naar kwetsbaarheden in publiek toegankelijke IT-omgevingen zoals websites en email. Nader onderzoek is nodig om de digitale relaties tussen de partijen in de maritieme sector beter te begrijpen en de kwetsbaarheden die hiermee samenhangen beter in kaart te krijgen. Daarbij gaat het om informatieuitwisseling (al of niet als onderdeel van een handelsrelatie), updaterechten van IT leveranciers, wederzijdse data-aanpassingsrechten bij partijen, enzovoort.

Advies: Versterk het politieke draagvlak voor de Rotterdamse maritieme cyberweerbaarheid

Naast ons voorstellen voor de inrichting van deze cyber-institutionele structuur voor de Rotterdame maritieme sector zien wij nog een belangrijke randvoorwaarde. Het is van groot belang dat in de gemeente Rotterdam de dreiging ten aanzien van cybersecurity in de maritieme sector op waarde wordt geschat. We stellen daarom voor om de wethouder te adviseren om hier ook met de gemeenteraad over in gesprek te gaan. Daarin zou, naast een overzicht van nationale en internationale ontwikkelingen, vooral de bijzondere positie en kwetsbaarheid van de Rotterdamse maritieme sector centraal moeten staan, en de gedachten over het inrichten van een cyberweerbaarheidsinitiatief waarmee Rotterdam zich internationaal kan onderscheiden.

Advies: Vergeet niet om breed voorlichting te blijven geven aan bedrijven, personeel en leidinggevenden in de Rotterdamse maritieme sector

De Rotterdam maritime board heeft op een heel aantal dossiers een klokkenluidersrol. Dat is ook voor cybersecurity het geval. Dit onderzoek, en het daarop gebaseerde advies, is daar een invulling van. Het is

van belang dat de board die rol blijft vervullen, en samen met de gemeente invulling blijft geven aan de informerende, inspirerende en activerende rol die de gemeente als ambitie in het MKB actieprogramma heeft geformuleerd. Daarbij speelt een belangrijke rol dat ondanks de aandacht voor cybersecurity in bepaalde delen van de maritieme sector en daarbuiten, nog heel veel individuele bedrijven, personeel en leidinggevenden maar een heel beperkt begrip hebben van de ontwikkelingen, oplossingen, mogelijkheden en formele eisen. Velen realiseren zich ook nog onvoldoende hoe cybersecuritykwetsbaarheden zich manifesteren in complexe netwerken en hoe zij zich daartegen moeten wapenen. Informatievoorziening en voorlichting blijft daarom een heel belangrijk wapen tegen cyberkwetsbaarheid. Wij adviseren om als gemeente met bedrijven samen dit soort voorlichting, liefst ingevuld met concrete casussen van bedrijven, te blijven aanbieden. De Rotterdam maritime board kan hier een coördinerende en stimulerende rol in spelen. De continuïteit van een dergelijk activiteiten kan ook goed verzekerd worden via een stabiel, goed gefinancierd cyberweerbaarheidsinitiatief. Vanuit de gemeente sluit de cybersecurity-problematiek ook goed aan bij de ambities die geformuleerd zijn in het Rotterdamse MKB Actieprogramma[1] dat voor 2023 gelanceerd is. De gemeente ziet voor zichzelf een rol in het helpen organiseren van activiteiten voor en door ondernemers, die als doel hebben het informeren, inspireren en activeren van ondernemers.

[1] https://www.watdoetdegemeente.rotterdam.nl/begroting2023/programmas/economische-ontwikkeling2/3-doel1/

Inhoudsopgave

Colofon 2

Samenvatting 3

1. Aanleiding en opzet van het onderzoek 9

2. Definitie en context 11

3. Inventarisatie en overzichten 13

4. Positie en behoefte 21

5. Aanbevelingen en prioriteiten 28

Bijlage 31

NOTEN 33

1. Aanleiding en opzet van het onderzoek

De afgelopen decennia is de digitalisering van de wereld in snel tempo toegenomen, waarbij tegenwoordig vrijwel elk proces en activiteit in meer of mindere mate digitaal is. Deze toegenomen digitalisering biedt vele voordelen, maar er zitten ook risico's aan. In de haven- en maritieme sector zijn diverse voorbeelden van deze voor- en nadelen te vinden. Het continue monitoren van processen door middel van sensoren en hierbij gebruik maken van artificial intelligence om te werken naar een systeem van predictive maintenance is een voorbeeld van hoe verschillende componenten van digitalisering en technologie activiteiten beter laten plaats vinden. Anderzijds is de afgelopen jaren vrijwel elke grote containerrederij slachtoffer geworden van een ransomware aanval, waarbij digitale aanvallers IT systemen platleggen. Dit zijn slechts enkele voorbeelden van een breed en divers thema, waarbij het in kaart brengen van dit speelveld een onderzoek an sich is. In dit onderzoek richten wij ons op de cybersecurity-component van dit speelveld. Het cybersecurity & infrastructure security agency definieert cybersecurity als *"the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information".* Ook deze definitie laat nog een breed speelveld zien, waarin verschillende elementen terugkomen. Het is hierom dat wij -na deze aanleiding en opzet- dit onderzoek beginnen met een definitie en context uitwerking waarin wij scherper definiëren hoe wij cybersecurity zien.

APM terminals en het Petya virus

Een van de grootste cyberaanvallen in de haven van Rotterdam, en een van de best gedocumenteerde, is de PETYA-virus aanval op een aantal APM-terminals in Nederland en andere landen, in juni 2017. Dit was een vervolg op eerdere aanvallen met het Petya virus, en wordt daarom ook wel de non-Petya aanval genoemd. Dit betrof een ransomware-aanval waarbij bestanden 'op slot' werden gezet tot betaling van losgeld in bitcoin was ontvangen. De ingang voor het virus was een Oekraïens accountancy systeem genaamd MeDoc.

Deze aanval op de APM-terminals was onderdeel van een veel grotere aanval, die primair gericht was op systemen in de Oekraïne. Vooral bedrijven in de Oekraïne en in Duitsland werden getroffen, maar ook partijen in Italië, Verenigd Koninkrijk, Polen, Frankrijk en Nederland. TNT Express werd ook getroffen door de aanval. Microsoft rapporteerde dat er ongeveer 20000 apparaten getroffen werden. Volgens een expert van McAfee was het expliciet de bedoeling om met de aanval kritische infrastructuur en transport- en mobiliteitsknooppunten te raken.

De gevolgen voor APM waren ingrijpend: de beide terminals kwamen stil te liggen. Hoewel de overslag na ongeveer een dag weer kon worden hervat op de APM RTM terminal, bleef APM MVII langer dicht. De ICT-ondersteuning was na een week weer min of meer operationeel. Deze situatie, waarbij operaties wel konden worden hervat, maar niet volledig, heeft nog ongeveer een week geduurd. Vooral de verder geautomatiseerde terminal APM MVII had veel last van de cyberaanval, en werd uiteindelijk als laatste terminal in het APM netwerk weer volledig operationeel.

De cyberaanval op de APM terminals had ook verdergaande gevolgen voor de afhandeling van containers via de Rotterdamse haven: schepen konden een tijdje niet terecht en moesten uitwijken naar andere havens.

APM terminals en het Petya virus - vervolg

Ook aan de landzijde waren er verstoringen en wachtrijen voor vrachtwagens en binnenvaartschepen. Binnen het Maersk concern had de hack ook gevolgen voor allerlei applicaties zoals de uitwisseling van documenten, en de boekingsportals.

De financiële schade voor Maersk is uiteindelijk becijferd op zo'n 250 mln dollar. In het hele Maersk concern, inclusief de terminal-tak, moest de hele IT-infrastructuur worden vervangen (4000 servers, 45000 pc's, 2500 applicaties). In Rotterdam werd de schade geschat op enkele tientallen miljoenen, alleen al voor de twee terminals. Verassend genoeg is de schade voor de ondernemers in het achterland (binnenvaart, wegvervoer, achterlandterminals) veel minder goed gedocumenteerd dan de schade voor Maersk.

In 2018 werd een ander onderdeel van het Maersk concern – Svitzer sleepdiensten - getroffen door een cyberaanval die leidde tot een data lek van zo'n 60.000 mails. De IT van Svitzer staat los van de rest van Maersk, en de hack was beperkt tot de operatie in Australië.

Dit onderzoek voeren wij uit op verzoek van de Rotterdam maritime board. De Rotterdam maritime board heeft aan Erasmus UPT gevraagd haar te begeleiden bij het opstellen van een advies aan de gemeente Rotterdam ten aanzien van cybersecurity. Het beeld in de Rotterdam maritime board is dat cybersecurity een belangrijk thema zou moeten zijn voor de maritieme community in en rondom de haven en het maritieme cluster in de regio Rotterdam, maar dat dit het om allerlei redenen nog niet is. De Rotterdam maritime board is voornemens om dit thema steviger op de agenda te zetten bij de gemeente Rotterdam. Om dit te realiseren voert Erasmus UPT dit onderzoek uit, waarin een viertal elementen worden uitgewerkt:

1. **Definitie en context**. In deze sectie wordt een korte definitie en context geschetst. Wat verstaan we precies onder cybersecurity en welke elementen moeten in gedachten gehouden worden bij de verdere rapportage.
2. **Inventarisatie en overzichten**. In deze tweede sectie wordt een overzicht geschetst van de belangrijkste stakeholders, initiatieven en documenten. Hiermee wordt verduidelijkt welke stappen waar al gezet worden en hoe verschillende zaken complementair zijn of wellicht overlappen.
3. **Positie en behoefte.** In deze sectie wordt de positie die verschillende stakeholders op dit moment hebben in kaart gebracht en worden de behoeftes gedefinieerd. Hiermee beantwoorden wij de vragen waar verschillende stakeholders staan op het gebied van cybersecurity, maar ook waar ze naar toe zouden willen.
4. **Rollen en aanbevelingen.** In deze laatste sectie werken wij concreter uit welke rollen de verschillende stakeholders zouden kunnen pakken? Hierbij worden enerzijds concrete acties gedefinieerd, waarbij anderzijds meer hoog over richtingen worden aangegeven.

Dit onderzoek wordt uitgevoerd door middel van een deskresearch gecombineerd met interviews met diverse experts. Voor deze studie zijn experts en betrokkenen vanuit -in alfabetische volgorde- het CYRA initiatief, Erasmus Universiteit Rotterdam, FERM, gemeente Rotterdam, Havenbedrijf Rotterdam, Kotug, Marsh, Ministerie van Infrastructuur en Waterstaat en Oceanco gesproken.

2. Definitie en context

Er zijn behoorlijk wat definities van het begrip cybersecurity in omloop, maar de centrale gedachte is dat cybersecurity gaat over het beschermen van data, en systemen tegen schadelijke aanvallen. Door deze insteek gaat de discussie over cybersecurity ook vooral over wat voor soorten aanvallen er zouden kunnen worden uitgevoerd, en welke verdediging daartegen mogelijk is. Op dit vlak zijn er veel ontwikkelingen die gevoerd worden op een hoog-technische niveau. Een alternatief is de zogenaamde AIC Triad, die beschrijft dat het bij elk informatiesysteem gaat om de combinatie van continuïteit, integriteit en beschikbaarheid.[2] Maar dit levert een hele algemene kijk op informatiesystemen op.

Een meer praktische aanpak van de cybersecurity discussie is het denken in kwetsbaarheden. Door de complexiteit van digitalisering in onze maatschappij, en door de beperkte mate waarin burgers/medewerkers begrijpen hoe de digitale technologie waar zij mee werken, precies functioneert, sluipen kwetsbaarheden op allerlei manieren in ons dagelijks handelen binnen.

Het kan ook voor komen dat kwetsbaarheden meekomen met individuele werknemers van bedrijven. Dit is vergelijkbaar met de manier waarop criminele organisaties op dit moment bedrijven in de haven en de maritieme sector infiltreren. Zij maken daarbij gebruik van de sociale kwetsbaarheid van mensen. Via sociale media en via de ingangen in bedrijfssystemen die lopen via individuen in een organisatie kunnen nieuwe kwetsbaarheden worden gecreëerd die vervolgens leiden tot cybersecurity-aanvallen. Er is dus mogelijk een relatie tussen het cybersecurity-domein en ondermijning, waar op dit moment in Rotterdam ook veel aandacht voor is.

Voor de bedrijfssystemen is inmiddels wel duidelijk dat een aantal basale maatregelen, zoals update, back-up en wachtwoordbeleid, geen bedrijfs- maar individuele accounts en multifactor-authenticatie[3], het hebben van een centrale verantwoordelijke, al veel problemen kunnen voorkomen. Dit zijn dan ook de voorwaarden die verzekeraars van cybersecurity verzekeringen stellen, en dit komt ook overeen met de handreikingen in de documentatie van het Nederlandse Nationaal Cyber Security Center.

Als we de context op deze manier neerzetten, dan zijn er voor de gemeente in grote lijnen de volgende aandachtsgebieden:

- De stand van zaken, en mogelijke voortrekkersrol van het maritieme complex in de directe weerbaarheid ten aanzien van cybersecurity. Dit raakt vooral de grotere bedrijven. Op dit vlak is veel in beweging op nationale en regionale schaal, en hier komen wij op terug in het volgende hoofdstuk;
- De cyberweerbaarheid van het MKB in de maritieme sector. Naast een aantal MKB-bedrijven die onder de verplichte cybersecurity-maatregelen vallen, zullen er vele bedrijven zijn die niet direct door maatregelen geraakt worden. Deze bedrijven werken wel in ketens en netwerken samen met heel veel andere bedrijven, en hun cyberkwetsbaarheid is daarmee wel relevant. Voor deze bedrijven kan een regionale aanpak worden ontwikkeld waarmee Rotterdam zich onderscheidend kan opstellen in het cybersecurity-veld.

[2] https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. (CIA slaat niet op de Amerikaanse spionagedienst, maar is een acroniem van de drie concepten.)

[3] Bij Portbase, bijvoorbeeld, is het sinds juli 2022 alleen nog mogelijk om door middel van multi-factor autenticatie in te loggen. Dit betekent dat er alleen nog maar individuele accounts zijn, en dat de identiteitsverificatie van de persoon die inlogt geverifieerd wordt met een app op de eigen telefoon.

- De cyberweerbaarheid van de gemeente zelf is een dimensie. Op dit moment gebeurt er veel op nationaal niveau, en de ontwikkelingen zijn complex, verdeeld over een aantal ministeries, en geborgd in diverse – deels nieuwe – organisaties. Het verdient aanbeveling om vanuit het perspectief van Rotterdam eigen prioriteiten te blijven stellen, zowel aan de zijde van de politiek, als aan de zijde van de stadse economie;
- Tenslotte is er de dimensie van individuen, consumenten, medewerkers, werknemers waarvoor de bewustwording van cyberrisico's in hun eigen omgeving, zowel wonen en werken, meer aandacht zou moeten krijgen.

De context van dit onderzoek is uiteindelijk: het belang voor de stad Rotterdam. Voor de stad is het belangrijk dat het economische klimaat gekenmerkt wordt door aantrekkelijkheid en robuustheid, waardoor zowel bedrijven als burgers/werknemers zich staande kunnen houden.

Onvoldoende bescherming op cybergebied brengt dit mogelijk in gevaar. Daarbij is niet alleen een directe aanval op een bedrijf of installatie een probleem, maar ook de kettingreactie die zo'n aanval kan veroorzaken bij andere bedrijven; ook wel systeemrisico genoemd. In het maritieme complex zijn veel bedrijven door middel van transactionele relaties en gezamenlijk gebruik van infrastructuur aan elkaar verbonden. De mogelijke olievlekwerking van een cyberaanval is daarmee voor het maritieme complex in en rondom Rotterdam een significant risico.

Vanuit nationale regelgeving op cybersecuritygebied krijgen de grotere bedrijven zorgplicht voor hun ketenpartners. Het is echter niet zomaar aannemelijk dat die bedrijven precies weten wie hun ketenpartners zijn, zeker als dat complexe ketens en netwerken zijn. Daarnaast blijft die ketenverantwoordelijk snel beperkt tot de directe ketenpartners, terwijl ketens, zeker in transport en logistiek, vaak complexer in elkaar zitten.

In aanvulling op de vier prioriteiten hierboven, is er daarom nog een vijfde:

- De verbondenheid van bedrijven in het ontwikkelen van complexe maritieme productie en dienstverlening is een extra risico in het cybersecuritydomein en vereist daarom bijzondere aandacht. Deze verbondenheid dient in kaart te worden gebracht om de zorgplicht die de grotere bedrijven krijgen vanuit nationale cybersecuritywetgeving maximaal te kunnen laten renderen.

3. Inventarisatie en overzichten

In deze sectie maken wij een inventarisatie en overzicht van een drietal componenten rondom cybersecurity:

1. Wetgeving
2. Stakeholders
3. Initiatieven

1. Wetgeving

Gezien de grote hoeveelheid initiatieven en onderdelen die zich bezig houden met cybersecurity, richten wij ons op de belangrijkste wetgeving. Op het gebied van wetgeving richten wij ons allereerst op de Europese wetgeving en richtlijnen, waarna wij vervolgens de belangrijkste nationale wetgeving in kaart brengen. Tot slot richten we ons nog op haven- en maritieme specifieke wetgeving en richtlijnen.

EU

Het strategisch kader waarbinnen de EU opereert op het gebied van cybersecurity wordt gevormd door de EU cybersecurity strategy, welke in december 2020 gepubliceerd is.[1] Deze EU-strategie inzake cyberbeveiliging voor het digitale tijdperk vormt een cruciaal aspect van de zaken die de digitale toekomst van Europa vormgeven en draagt daarnaast bij aan een flink aantal andere strategieën en plannen. In de strategie is uiteengezet hoe de EU haar mensen, ondernemingen en instellingen zal beschermen tegen cyberdreigingen, hoe zij de internationale samenwerking zal bevorderen en hoe zij het voortouw zal nemen bij het beveiligen van een mondiaal en open internet.

De belangrijkste wetgeving die vanuit de EU op het gebied van cybersecurity opgesteld is, is de ***netwerk- en informatiebeveiliging richtlijn*** (vanaf nu: NIB) richtlijn.[4] In juli 2016 is de eerste richtlijn opgesteld, waarin de beveiliging van netwerk- en informatiesystemen van aanbieders van essentiële diensten (AED's) en van digitale dienstverleners (DSP's) wordt geregeld, onder meer door hen te laten voldoen aan een zorg- en meldplicht. Deze essentiële dienen door de lidstaten zelf te worden aangewezen.[2] Voor het haven en maritieme cluster in de regio Rotterdam is alleen de scheepvaartafwikkeling gekwalificeerd als vitaal proces.[3] Dat wil overigens niet zeggen dat alleen de scheepvaartafwikkeling aan de NIB richtlijn moet voldoen. Onder de huidige NIB-richtlijn zijn aanbieders van essentiële diensten (zoals banken, drinkwater, energie) en digitale partijen (zoals clouddiensten, online marktplaatsen) door de Rijksoverheid al aangewezen om maatregelen te nemen voor hun digitale veiligheid en ernstige cyberincidenten te melden. Daarmee zijn er -naast de scheepvaartafwikkeling- nog een aantal partijen in het haven- en maritieme cluster die vallen onder de huidige NIB richtlijn en maatregelen op het gebied van cybersecurity moeten nemen.

Omdat de digitale wereld sinds 2016 flink veranderd is, is de NIB richtlijn toe aan herziening, iets waar de EU eerder in 2022 een akkoord over bereikt heeft en de implementatie momenteel in volle gang is. Deze NIB2 richtlijn moderniseert het bestaande rechtskader, rekening houdend met de toegenomen digitalisering van de interne markt in de afgelopen jaren en een zich ontwikkelend bedreigingslandschap voor cyberbeveiliging.[4] Een belangrijk element wat verandert in de NIB2 richtlijn ten opzichte van de oorspronkelijke NIB richtlijn is voor welke publieke en private stakeholders en processen deze richtlijn van

[4] In het Engels heet deze richtlijn voluit Directive on Security of Network and Information Systems, en wordt deze afgekort tot NIS. In deze studie gebruiken wij de Nederlandse afkorting, maar in de documenten waar naar verwezen wordt, wordt vaak NIS gebruikt.

toepassing is. In de NIB2 richtlijn worden essentiële en belangrijke entiteiten gedefinieerd voor wie de NIB2 richtlijn geldt. Deze essentiële entiteiten worden flink uitgebreid ten opzichte van de huidige lijst en daarnaast zijn ook binnen momenteel gedefinieerde sectoren diverse subsectoren toegevoegd. In de NIB2 richtlijn gaat het voor **essentiële entiteiten** om de volgende sectoren en subsectoren vallen:

- Energie
    - Elektriciteit
    - Stadsverwarming en -koeling
    - Aardolie
    - Aardgas
    - Waterstof
- Vervoer
    - Lucht
    - Spoor
    - Water
    - weg
- Bankwezen
- Infrastructuur voor de financiële markt
- Gezondheidszorg
- Drinkwater
- Afvalwater
- Digitale infrastructuur
- Overheidsdiensten
- Ruimtevaart

Daarnaast gaat het om de volgende **belangrijke entiteiten**:

- Post- en koeriersbedrijven
- Afvalstoffenbeheer
- Vervaardiging, productie en distributie van chemische stoffen
- Productie, verwerking en distributie van levensmiddelen
- Vervaardiging
    - Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor invitrodiagnostiek
    - Vervaardiging van informaticaproducten en van elektronische en optische producten
    - Vervaardiging van elektrische apparatuur
    - Vervaardiging van machines, apparaten en werktuigen, n.e.g.
    - Vervaardiging van transportmiddelen
    - Vervaardiging van meubelen; overige industrie; reparatie en installatie van machines en apparaten
- Digitale aanbieders

In de volledige specificatie zijn ook soorten entiteit die in deze sectoren en subsectoren actief zijn gedefinieerd.[5] Belangrijk element wat verschilt met de oorspronkelijke richtlijn is dat, waar in de eerste richtlijn de essentiële diensten door de nationale overheden bepaald werden, de soorten entiteiten actief in de (sub)sectoren zoals gespecificeerd, in principe automatisch allemaal onder de NIB2 richtlijn vallen. Bij de essentiële aanbieders, vooral partijen uit Nederlandse vitale sectoren, is het toezicht straks

proactief. Bij de belangrijke aanbieders vindt het toezicht achteraf plaats, als er aanwijzingen zijn dat er sprake is van een incident. Dit zijn voornamelijk (middel)grote partijen, waarbij verstoring geen zeer ernstige maatschappelijke of economische gevolgen zal hebben. Behalve voldoen aan de meldplicht moeten alle aanbieders die onder de herziene richtlijn gaan vallen ook veiligheidsmaatregelen nemen: de zorgplicht. Het gaat dan onder andere om het verhogen van de beveiliging van hun toeleveringsketen en het op orde brengen van de wijze van afhandeling van cyberincidenten. Naast dat partijen in het haven- en maritieme cluster dus hun eigen cybersecurity -voor zover nog niet het geval- op orde moeten brengen, moeten ze dus ook de beveiliging van hun toeleveringsketen in kaart brengen en verhogen. Hoe dit precies uitwerkt is momenteel volop in ontwikkeling en wordt mede bepaald door de omzetting naar nationale wetgeving, die in 2024 verwacht wordt. Maar de conclusies dat er veel meer partijen in het haven- en maritieme cluster onder de NIB2 richtlijn gaan vallen en dat deze partijen (veel) meer moeten gaan doen op het gebied van cybersecurity is wel duidelijk. Wel is de NIB2 richtlijn erg sectoraal ingericht, waarbij sector overstijgende ketens en ketenafhankelijkheden nog een aandachtspunt is.

Naast de NIB richtlijnen zijn er nog twee EU wetgevingselementen die we willen uitlichten in deze context. Eerste element is de EU cybersecurity act, waarin een EU breed cybersecurity kader voor cyberbeveiligingscertificering voor ICT-producten, -diensten en -processen wordt geïntroduceerd. Bedrijven die zaken doen in de EU zullen er baat bij hebben om hun ICT-producten, -processen en -diensten slechts één keer te certificeren en hun certificaten in de hele Europese Unie te erkennen.[6] Daarnaast wordt in deze act, de positie van Enisa (het Agentschap van de EU voor cyberbeveiliging) versterkt. Enisa zal een sleutelrol spelen bij het opzetten en in stand houden van het Europees kader voor cyberbeveiligingscertificering door de technische basis voor specifieke certificeringsregelingen voor te bereiden. Concreet specificeert deze cybersecurity act de eisen waarin producten op het gebied van cybersecurity moeten voldoen.
Tweede element wat we willen uitlichten is de cyber resilience act, een voorstel voor een verordening betreffende cyberbeveiligingsvereisten voor producten met digitale elementen, bekend als de wet inzake cyberveerkracht, versterkt de cyberbeveiligingsregels om te zorgen voor veiliger hardware- en softwareproducten.[7] Hierin worden de eisen die aan hardware- en softwareproducten gesteld worden vastgesteld.

Nationaal
De nationale wetgeving op het gebied van cybersecurity is in lijn met de Europese wetgeving en vooral nationale uitwerking van de NIB richtlijn. Belangrijkste wetgeving in Nederland is de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) welke, sinds eind 2018 in werking is. In lijn met de NIB richtlijn hebben vitale aanbieders en aanbieders van essentiële diensten (AED's) in geval van ernstige incidenten een meldplicht bij het NCSC en bij hun sectorale toezichthouder. Digitale dienstverleners melden bij het Computer Security Incident Response Team (CSIRT). Daarnaast bevat de wet de zorgplicht voor AED's en DSP's. Zij moeten maatregelen nemen om de kansen en gevolgen van digitale incidenten te verkleinen. De Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) is in de Wbni opgenomen.[8] Naast de Wbni zijn er nog een aantal wetten en richtlijnen waarin cybersecurity in meer of mindere mate een rol speelt, zoals de Wet op de inlichtingen- en veiligheidsdiensten 2017 of de wet veiligheidsregio's.[9] Deze zijn van substantieel minder belang dan de Wbni.

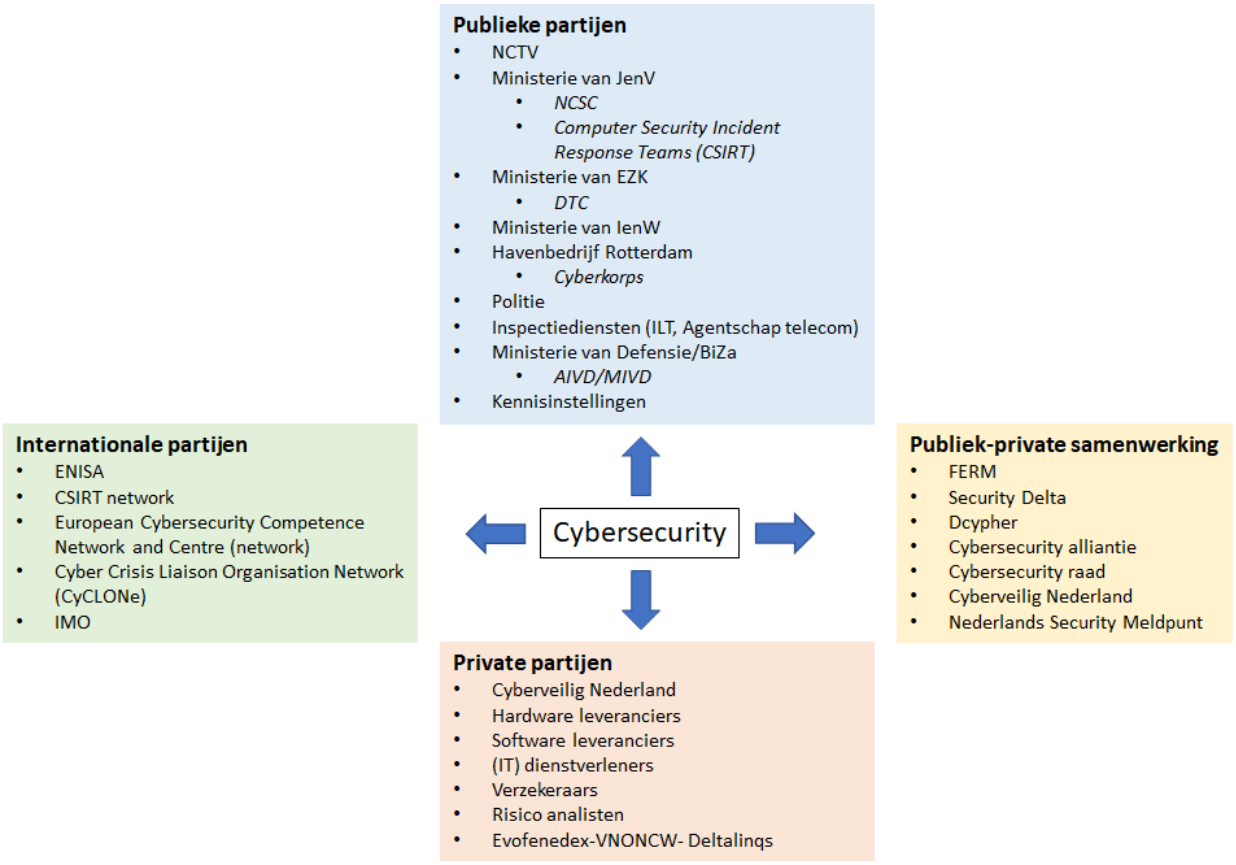
Haven- en maritieme context
De fysieke veiligheid van havens wordt geregeld door middel van de International Ship and Port Facility Security (ISPS) Code. De code beschrijft de verantwoordelijkheden van overheden, rederijen, personeel

aan boord van schepen en personeel van havenfaciliteiten met betrekking tot het detecteren van bedreigingen van de veiligheid. Daarnaast beschrijft de code het nemen van preventieve maatregelen om incidenten op het gebied van veiligheid te voorkomen, die een bedreiging vormen voor schepen en havenfaciliteiten.[10] In 2021 is vanuit havenpartijen een set aan richtlijnen ter overweging richting de IMO gestuurd op het gebied van cybersecurity, om mogelijk op te nemen in de ISPS. Sowieso is al een gedeeltelijke verbreding zichtbaar van de insteek van ISPS, naar een breder veiligheidsperspectief.[11] Op dit moment is er -voor zover de onderzoekers hebben kunnen achterhalen- nog geen expliciete opname van cybersecurity in deze wetgeving. Wel heeft de IMO een resolutie aangenomen in juni 2017 met als titel 'Maritime Cyber Risk Management in Safety Management Systems'. In deze resolutie worden regeringen aangemoedigd om te zorgen dat cyberrisico's op passende wijze worden aangepakt in bestaande veiligheidsbeheersystemen.[12] Daarnaast heeft de IMO in juli 2017 richtlijnen op het gebied van management van maritieme cyberrisico's uitgegeven. De richtlijnen bevatten aanbevelingen -op hoog niveau- over maritiem cyberrisicobeheer om de scheepvaart te beschermen tegen huidige en opkomende cyberdreigingen en kwetsbaarheden. Daarnaast bevatten deze richtlijnen functionele elementen die effectief cyberrisicobeheer ondersteunen.[13]

2. Stakeholders

Het speelveld op het gebied van cybersecurity qua stakeholders is breed en divers. Zeker aan de private kant is er een grote diversiteit en hoeveelheid van partijen die een vorm van dienstverlening op het gebied van (cyber)veiligheid aanbieden. Onderstaande Figuur 1 geeft een globaal overzicht van de belangrijkste stakeholders in de verschillende categorieën. Belangrijke opmerking hierbij is dat het overzicht niet volledig beoogd te zijn, maar dat het een beeld geeft van een flink aantal van de relevante stakeholders.

Figuur 1: globaal overzicht stakeholders in het cybersecurity speelveld (zie ook deze link)



Publiek

Aan de publieke kant zijn er een aantal belangrijke organisaties. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) beschermt Nederland tegen bedreigingen die de maatschappij kunnen ontwrichten en richt zich daarmee op een breder speelveld dan alleen cybersecurity. Specifiek op cybersecurity is er het Nationaal Cyber Security Centrum (NCSC). Het NCSC heeft onder andere als doel om vitale aanbieders en onderdelen van het Rijk bij te staan bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen en te informeren en adviseren over dreigingen en incidenten voor netwerk- en informatiesystemen van vitale aanbieders en het Rijk.[14] Daarnaast is er vanuit het ministerie van EZK het Digital Trust Center (DTC) opgericht. Waar het NCSC zich voornamelijk richt op de vitale aanbieders, richt het DTC zich breder op alle bedrijven die niet tot de vitale sectoren behoren. Dit doen ze onder andere door kennisdeling, het ontwikkelen van tools en het delen van dreigingsinformatie met bedrijven. Het NCSC en het DTC hebben in september 2022 aangekondigd samen te gaan in één centraal expertisecentrum.

Publiek-privaat

In de publiek-private samenwerkingshoek zijn er diverse initiatieven die in meer of mindere mate hetzelfde doen. Voor het Rotterdamse haven- en maritieme cluster is FERM de belangrijkste partij; FERM brengt bedrijven en kennis bij elkaar en faciliteert het onderling uitwisselen van dreigingsinformatie, oplossingen en best-practices. Op nationaal niveau is er een vergelijkbaar initiatief in de zin van de Security Delta (HSD), waarin 275 bedrijven, overheidsorganisaties en kennisinstellingen sinds 2013 samen werken om het verschil te maken in de veiligheid van onze digitaliserende samenleving. Dit doen zij door hun kennis te delen en samen te werken aan innovatieve veiligheidsoplossingen, die zowel binnen als buiten Nederland opgeschaald kunnen worden.[15] Het Nederlands Security Meldpunt bevordert de cyber weerbaarheid van alle organisaties in Nederland door de uitwisseling van informatie over kwetsbaarheden, zwakke configuraties en dreigingsinformatie aan vertrouwde partijen te bevorderen en te faciliteren. Eind september 2022 hebben FERM en NSM besloten de krachten te bundelen.

Naast deze drie enigszins vergelijkbare initiatieven zijn er nog twee elementen die we hier willen uitlichten. De cybersecurity alliantie is het platform van de publiek-private samenwerking voor een weerbaar en digitaal veilig Nederland. De cybersecurity alliantie is een aanjager voor projecten die concrete doorbraken kunnen realiseren en daarmee het streven naar een digitaal weerbaar Nederland helpen te bereiken.[16] De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen.

Privaat

De private sector is op het gebied van cybersecurity enorm breed en divers. Het valt buiten de scope van dit onderzoek om een volledig beeld te schetsen van het hele speelveld van alle aanbieders. Daarom beperken we ons in deze uitwerking tot een overzicht van de belangrijkste type partijen die van belang zijn op het gebied van cybersecurity. Ten eerste zijn er leveranciers van hardware en software, welke een belangrijke rol spelen op het gebied van cybersecurity. Vrijwel elk bedrijf in het haven- en maritieme cluster maakt gebruik van deze hardware- en software leveranciers. Enerzijds gaat het om duidelijke en simpele voorbeelden als computers of besturingssystemen, maar anderzijds gaat het ook om specifieke ‘programmable logic controllers’ (PLC), robuuste industriële computers die geschikt zijn voor de besturing en automatisering van productieprocessen waar specifieke eisen aan gesteld worden. Daarnaast is er een grote hoeveelheid nationale en internationale partijen die we binnen de categorie IT dienstverleners scharen. Het gaat hier bijvoorbeeld enerzijds om partijen die werkzaamheden zoals monitoring van IT

systemen en digitale processen uitvoeren voor klanten. Anderzijds gaat het om partijen die diensten en producten op het gebied van digitale preventie, analyse en herstel aanbieden; denk hierbij aan cybersecurity scans of digitale risico analyses. Derde type private partijen wat we identificeren zijn de verzekeraars en risico analisten. Dit zijn partijen die diensten en producten aanbieden om risico's in kaart te brengen, te kwantificeren en vervolgens ook kunnen afdekken. Laatste type private partijen die we identificeren zijn brancheorganisaties en belangenverenigingen. Dit zijn verzamelingen van private partijen die samenwerken of (sub)sectoren vertegenwoordigen. Deze partijen doen zelf niet altijd veel uitvoerend werk, maar vertegenwoordigen of verspreiden de boodschap van leden of andere partijen.

Internationaal

Op de internationale stakeholders gaan wij kort in, omdat deze ten dele vergelijkbaar zijn met de nationale publieke partijen. Enige partij die wij hier wel willen uitlichten is Enisa; het agentschap dat bijdraagt aan het cyberbeveiligingsbeleid van de EU en -naar eigen zeggen- Europa helpt voor te bereiden op de cyberuitdaging van morgen. Door middel van kennisdeling, capaciteitsopbouw en bewustmaking werkt Enisa samen met zijn belangrijkste belanghebbenden om het vertrouwen in de digitale economie te versterken, de veerkracht van de infrastructuur van de Unie te vergroten en uiteindelijk te zorgen voor de digitale veiligheid van de Europese samenleving en burgers.[17] In die zin is Enisa dus vergelijkbaar met nationale partijen binnen Nederland, zowel publiek als publiek-privaat.

3. Initiatieven

Binnen de wetgevende kaders ontplooien de genoemde stakeholders een hele set aan initiatieven en worden een diversiteit aan documenten gepubliceerd. Net als voor de wetgeving en stakeholders focussen wij ons ook hier op de hoofdlijnen en belangrijkste initiatieven.

Belangrijk kader voor veel van de activiteiten in Nederland is de recent (oktober 2022) gepubliceerde nationale cybersecurity strategie. In deze studie staan de ambities voor de komende 6 jaar en in het bijgevoegde actieplan de acties om deze ambities te realiseren.[18] Deze nationale strategie bouwt voort op de Nederlandse cybersecurity agenda uit 2018. Als onderdeel van de strategie wordt het landelijk dekkend stelsel (LDS) van cybersecuritysamenwerkingsverbanden waarmee organisaties van beveiligingsadvies worden voorzien versterkt. Het landelijk dekkend stelsel is een stelsel waarin het NCSC en het DTC samenwerken met publieke- en private organisaties om informatie en kennis uit te wisselen. Organisaties die hierin participeren worden aangewezen als CERT (Computer Emergency Response Team) of OKTT (Objectief Kenbaar Tot Taak).[19] Op dit moment zijn er 11 CERTs en/of OKTTs voor verschillende doelgroepen zoals Nederlandse gemeenten, zorginstellingen of organisaties in de Rotterdamse haven (FERM). Het uitbreiden en versterken hiervan voor verschillende sectoren in het haven- en maritieme cluster kan helpen voor het vergroten van de cyberweerbaarheid in het cluster, maar moet tegelijkertijd ook niet leiden tot een versplintering.

Op het gebied van informatie delen en communicatie gebeuren er diverse dingen. Door middel van het organiseren van kennissessies, maar ook door middel van communicatie verspreiden een diversiteit aan organisaties kennis en vestigen ze aandacht op het thema. Dit varieert van simpele basiscommunicatie tot diepgaande sessies waarin specifiek op 1 onderwerp wordt ingezoomd.[20] In het haven- en maritieme cluster wordt ook in zogeheten 'information sharing and analysis centers' (ISAC) overlegd door diverse publieke en private partijen. Deze haven ISAC worden vanuit het NCSC gefaciliteerd en partijen kunnen hier met elkaar spreken over onder andere cybersecurity en cyberdreigingen.

Verschillende type partijen ontplooien ook verschillende soorten initiatieven op het gebied van cybersecurity. Publieke partijen richten zich -onder meer- op het delen van kennis en het maken van overkoepelende beelden en analyses. Zo hebben zowel FERM, gemeente Rotterdam[21], de NCTV[22] als het havenbedrijf in 2022 een cyberbeeld gepubliceerd. Deze beelden geven een overzicht van kansen en bedreigingen op het gebied van cybersecurity. Private initiatieven die we hier kort willen benoemen zijn onderdeel van een veel bredere set aan producten en diensten die private stakeholders aanbieden op het gebied van cybersecurity. Er worden vele varianten van cyberscans aangeboden; ook FERM biedt bedrijven diverse diensten die bedrijven weerbaarder maken tegen cyberincidenten. Wij lichten nog 1 specifieke pilot uit, welke in maart 2017 werd aangekondigd. AON, in combinatie met de gemeente Rotterdam voerden een pilot uit waarbij zestig Mkb'ers uit Rotterdam gebruik konden maken van het pakket, dat onder meer bestaat uit een veiligheidsscan, directe cybersecurity-oplossingen en een cybersecurityverzekering.[23] Het is de onderzoekers niet duidelijk geworden of deze pilot doorgezet is, maar de essentie en gedachte zijn zeker een voorbeeld geweest voor hoe momenteel veel partijen met cybersecurity (diensten) omgaan.

FERM Maritieme Bedrijvenscan

In opdracht van gemeente Rotterdam is onlangs een scan uitgevoerd over de digitale kwetsbaarheid van 336 maritieme bedrijven. De spreiding van bedrijven was breed gekozen: van handelsbedrijven, tot jachtbouw, zakelijke dienstverlening en offshore. Van de bedrijven was niet alleen het type bedrijf maar ook de omvang in termen van personeel meegenomen in het onderzoek. De scan omvat een overzicht van een groot aantal digitale kwetsbaarheden die gekoppeld zijn aan de websites van de bewuste bedrijven. Het ging daarbij om de bereikbaarheid van de website, de kwetsbaarheden in de website, veiligheid van emailverkeer, en mogelijkheden om de website van buitenaf te manipuleren.

De belangrijkste inzichten uit dit onderzoek zijn dat de scores overall laten zien dat er nog wel wat werk aan de winkel is. Het gemiddelde van de scores is 4.5 op een schaal van 10. Daarnaast laat het onderzoek duidelijk zien dat er een relatie is tussen de hoogte van de score en de omvang van de onderneming. Grotere bedrijven doen het beduidend beter dan kleinere bedrijven. Dit bevestigt ons inziens dat met name aandacht voor het MKB nodig is.

Bron: Onderzoeksrapport cyberscan

Laatste soort initiatieven in het haven- en maritieme cluster wat we hier willen toelichten zijn de simulaties van crisissituaties, oefeningen en preventie van schade als gevolg van een cyberincident. Vanuit FERM wordt elk jaar een gezamenlijke cybercrisisoefening Cybernautics uitgevoerd, waarin diverse stakeholders (nautisch dienstverleners, Rotterdamse havenbedrijven en veiligheidspartners). Vanuit het NCSC wordt ISIDOOR georganiseerd, een grootschalige cyberoefening, waarbij structuren en processen uit het nationaal crisisplan digitaal worden geoefend.[24]

Samenvattend overzicht

Deze sectie geeft een algemeen overzicht van de belangrijkste wetgeving, stakeholders en initiatieven. Dit overzicht pretendeert niet om een volledig beeld te geven van alle componenten en onderdelen, maar schetst een aantal belangrijke onderdelen. Vanuit de wetgeving is de EU wetgeving, specifiek de NIB

richtlijnen, dominant; deze worden vervolgens doorvertaald in soortgelijke nationale Nederlandse wetgeving. De hoeveelheid en scope van de partijen die onder de NIB2 vallen ten opzichte van de oorspronkelijke richtlijn neemt flink toe. Qua stakeholders is een breed beeld zichtbaar van type partijen die zich bezig houden met cybersecurity. Zowel op publiek niveau, als ook op publiek-privaat en privaat niveau zijn diverse partijen bezig met cybersecurity en de verschillende componenten daarvan. Door middel van kennisdeling, risico analyses en preventieve maatregelen wordt het thema benaderd, al dan niet vanuit een commerciële invalshoek. Deze stakeholders voeren een diverse set aan initiatieven uit, welke voor een deel gekaderd worden door diverse documenten die uitgewerkt worden door deze stakeholders.

4. Positie en behoefte

In deze sectie lichten wij een drietal componenten uit die van belang zijn voor de bepaling van de positie en de behoefte op het gebied van cybersecurity in het maritieme cluster in de regio Rotterdam:

1. Demografisch overzicht bedrijven
2. Cybersecurity risico's in het maritieme cluster
3. Huidige positie en behoefte ten aanzien van cybersecurity

1. Demografisch overzicht bedrijven

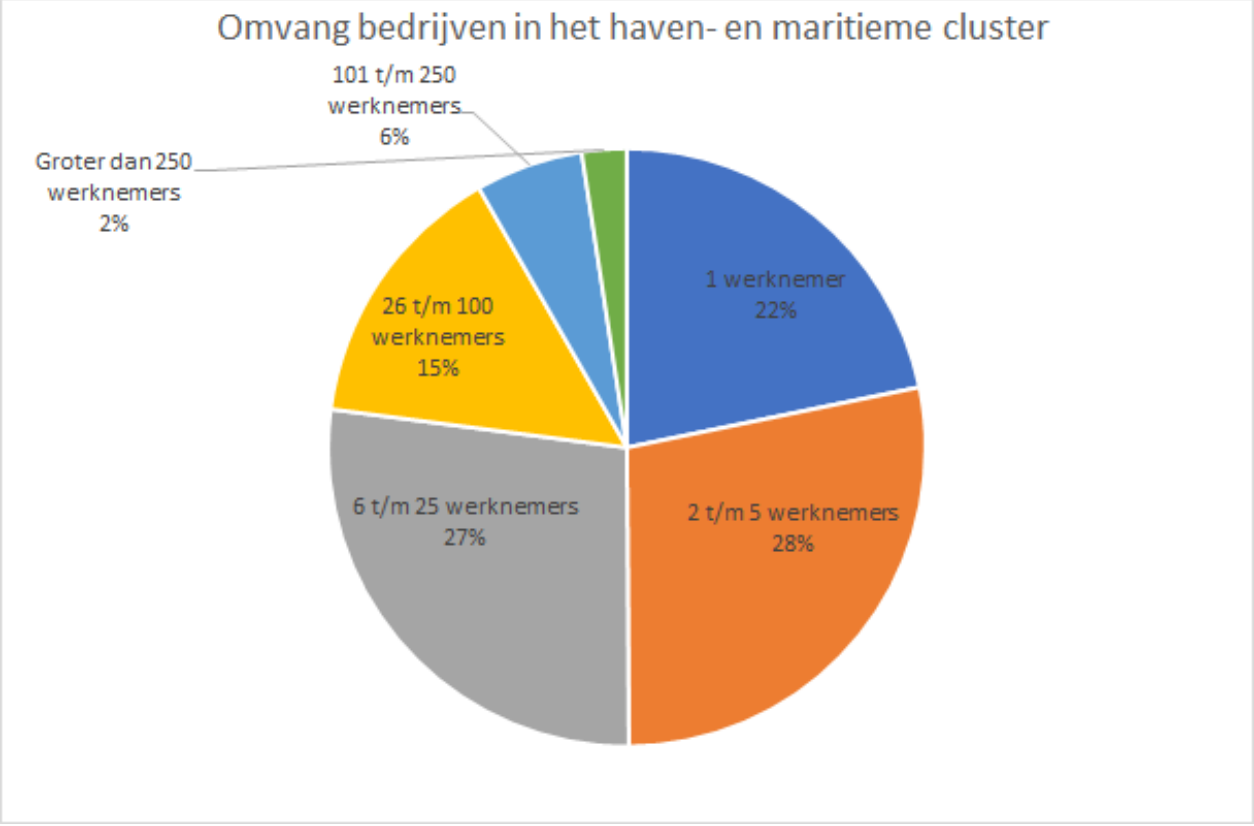
De mate waarin partijen bezig zijn met cybersecurity en het risico wat partijen lopen heeft met meerdere kenmerken te maken. In deze sectie bekijken wij de populatie bedrijven in het haven- en maritieme cluster vanuit twee perspectieven:

1. Omvang
2. Activiteiten/sectoren

Hiervoor maken wij gebruik van de populatie bedrijven uit de havenmonitor op basis van data van stichting LISA.[25] Hierbij nemen wij alle bedrijven die in de havenmonitor worden meegenomen in Rotterdam, Noordoever Nieuwe Waterweg, Overig Rijnmond en de Drechtsteden.

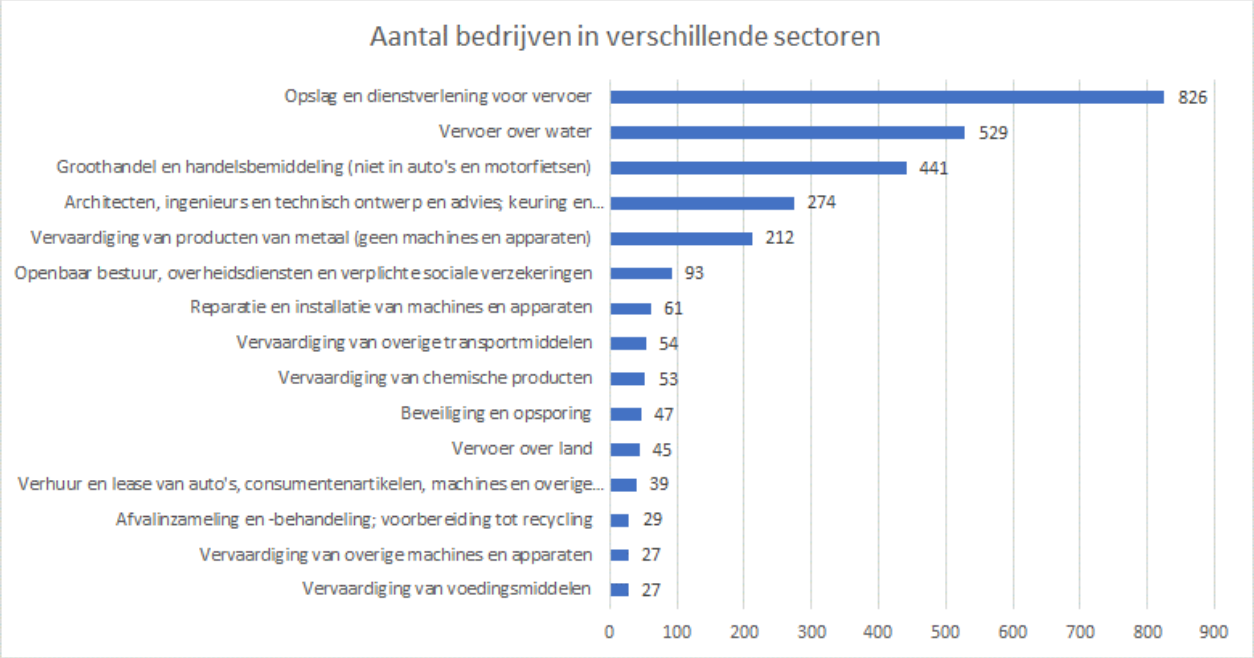
Van de bijna 3000 bedrijven is meer dan 77% tussen de 1 en 25 werknemers. Slechts 8% van de bedrijven is groter dan 100 werknemers. Dit betekent dus dat de bedrijven in het haven- en maritieme cluster voor het grootste gedeelte relatief klein zijn.

Figuur 2: omvang bedrijven in het haven- en maritieme cluster (hele populatie bedrijven)



Tweede element wat wij hier uitlichten is de sector waarin bedrijven hun activiteiten uitvoeren. Hiervoor gebruiken wij de SBI codes van de bedrijven. In Figuur 3 is een overzicht van de aantallen bedrijven in de verschillende sectoren, waarbij een minimum van 20 bedrijven actief in deze sectoren is genomen. Het volledige overzicht is opgenomen in de bijlage.

Figuur 3: aantal bedrijven in verschillende sectoren (tenminste 20 bedrijven actief in de sector), van groot naar klein



In Figuur 4 hebben wij een verdere uitsplitsing gemaakt van Figuur 3. Hierbij zijn de aantallen bedrijven uitgesplitst in de verschillende grootteklasses. Tot slot hebben wij in onderstaande tabel het totaal aantal werknemers opgenomen in de sectoren, wederom waarin tenminste 20 bedrijven actief zijn.

Tabel 1: aantal werknemers totaal per sector (tenminste 20 bedrijven actief in de sector), van groot naar klein

Sector	Aantal wn
Opslag en dienstverlening voor vervoer	24823
Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)	11861
Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen	10821
Vervaardiging van chemische producten	6483
Vervoer over water	6284
Vervaardiging van overige transportmiddelen	4025
Vervaardiging van producten van metaal (geen machines en apparaten)	3803
Vervaardiging van voedingsmiddelen	3409
Architecten, ingenieurs en technisch ontwerp en advies; keuring en controle	3188
Vervoer over land	2558
Vervaardiging van overige machines en apparaten	1813
Afvalinzameling en -behandeling; voorbereiding tot recycling	1482
Reparatie en installatie van machines en apparaten	1111
Verhuur en lease van auto's, consumentenartikelen, machines en overige roerende goederen	484
Beveiliging en opsporing	100

Figuur 4: uitsplitsing aantal bedrijven in verschillende grootteklasses (sectoren met tenminste 20 bedrijven actief in de sector), oplopende SBI volgorde

Sector	1 werknemer	2 t/m 5 werknemers	6 t/m 25 werknemers	26 t/m 100 werknemer	101 t/m 250 werknemers	Groter dan 250 werknemers
Vervaardiging van voedingsmiddelen	3	1	1	13	7	2
Vervaardiging van chemische producten	1	2	10	15	19	6
Vervaardiging van producten van metaal (geen machines en apparaten)	92	39	46	25	9	1
Vervaardiging van overige machines en apparaten	2	4	11	5	4	1
Vervaardiging van overige transportmiddelen	8	12	13	12	6	3
Reparatie en installatie van machines en apparaten	33	3	15	7	3	0
Afvalinzameling en -behandeling; voorbereiding tot recycling	0	5	7	13	2	2
Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)	60	123	157	72	22	7
Vervoer over land	0	6	17	15	5	2
Vervoer over water	128	273	86	28	9	5
Opslag en dienstverlening voor vervoer	86	249	304	139	35	13
Architecten, ingenieurs en technisch ontwerp en advies; keuring en controle	140	62	53	10	6	3
Verhuur en lease van auto's, consumentenartikelen, machines en overige roerende goederen	15	9	8	7	0	0
Beveiliging en opsporing	37	6	4	0	0	0
Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen	5	11	17	28	19	13

2. Cybersecurity risico's in het maritieme cluster

Cybersecurity raakt onze hele maatschappij. Ook in Rotterdam betekent dit dat de stad een grote opgave heeft ten aanzien van cybersecurity, in een heel breed maatschappelijk domein. Onze opdracht is echter voor de Rotterdam maritime board. Het is daarom zinnig om stil te staan bij de specifieke risico's in het Rotterdamse haven- en maritieme ecosysteem.

Als we kijken naar de recente ontwikkeling van zakelijke diensten ten aanzien van cybersecurity, dan volgt daar onmiddellijk een denkwijze uit over het bijzondere karakter van de maritieme en transport sector. Aanbieders van cybersecurity-verzekeringen beschouwen alle bedrijven die bezig zijn met transport en productie, maar ook ICT-ondernemingen, als bedrijven met een bijzonder risico die zich niet zomaar voor cyber-risico's kunnen verzekeren. De reden daarvoor is dat het bedrijven zijn die vanwege hun bedrijfsactiviteit activiteiten faciliteren die een waarde vertegenwoordigen die groter is dan hun eigen bedrijfswaarde. In gewone woorden: bijna elke vervoerder rijdt of vaart rond met lading die een waarde vertegenwoordigd die groter is dan de vrachtauto of het schip waar het in zit.

Dit aspect kan je ook op het niveau van de hele haven en/of het maritieme complex beschouwen: de economische waarde die deze sector faciliteert voor Nederland, en Europa, is veel groter dan de economische waarde van de verzameling bedrijven in deze regio. Dit maakt deze sector bijzonder in economische zin, maar dit houdt ook een bijzondere kwetsbaarheid in. Onze regio heeft daarom een bijzondere verantwoordelijkheid die maakt dat je naast de toepassing van het nationale cybersecurity-beleid in Rotterdam meer tijd en energie een gedragen cybersecuritybeleid voor de maritieme sector zou moeten besteden.

In de recente periode is gebleken dat we steeds meer inzicht krijgen in cybersecurity-kwetsbaarheden. Naast kwetsbaarheid voor cyber-aanvallen rechtstreeks op infrastructuur en bedrijven, schuilen er ook grote kwetsbaarheden in de complexiteit van bedrijfssystemen en bedrijfsnetwerken. Veel van de aandacht gaat inmiddels uit naar de rol van IT en de mogelijkheden die IT-leveranciers hebben om hun producten beter te maken.

Kwetsbaarheden als gevolg van de complexiteit van bedrijfsnetwerken of logistieke ketens krijgt steeds meer, maar nog steeds onvoldoende, aandacht. Het Solarwinds incident in 2020[5] heeft de cyber-community getriggerd. In deze aanval is gebruik gemaakt van IT-update rechten van een IT-leverancier (Solarwinds) bij heel veel van haar klanten. Op deze manier kon malware bij zo'n 30.000 bedrijven worden geïntroduceerd. Dit lijkt op de situatie die in Rotterdam met het Petya virus in Oekraïense software bij containerterminal APM-T in 2017 (zie het kader eerder in deze studie). Daar was sprake van een ransomware-aanval, die hele grote gevolgen had voor de operaties op de terminals van APM en die uiteindelijk leidde tot de volledige vervanging van alle ICT -systemen van het Maersk-concern. Het wegmasseren van de operationele gevolgen van deze situatie in Rotterdam heeft maanden geduurd, en heeft de Maersk Groep uiteindelijk wereldwijd €200-300 mln gekost (het betrof 17 terminals wereldwijd). In de al eerder genoemde NIB2-regelgeving is het aspect van ketenafhankelijkheden wel opgenomen, maar beperkt tot de directe ketenpartners. Daarbij blijft de definitie van ketens ook sterk binnen sectoren, en dit doet daarmee onvoldoende recht aan de complexiteit van maritieme ketens.

[5] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

In het innovatieve ecosysteem rondom Eindhoven is dit ketenrisico onderkend. In dit ecosysteem is het effectief functioneren van het hele netwerk van leveranciers voor partijen als ASML van cruciaal belang. Voor dit netwerk, dat uit meerdere lagen toeleveranciers bestaat, is daarom een systeem geformuleerd waarmee alle bedrijven, en niet alleen de bedrijven die door NIB2 geraakt worden, handvaten krijgen voor informatiebeveiliging en privacymaatregelen[6]. Hiermee wordt invulling gegeven aan het vertalen van de ISO 27001 standaard, maar op een manier die ook geschikt is voor het MKB. In de kern bestaat de aanpak uit het onderscheiden van drie beveiligingsniveaus en een verzameling controles. Het startpunt is een self assessment door ondernemers, waarmee ondernemers een handelingsperspectief krijgen ten aanzien van hun eigen cyberkwetsbaarheid. Omdat dit in het hele netwerk op dezelfde manier wordt uitgerold krijgt ASML ook zicht op de stand van zaken in het hele netwerk. De gekozen naam voor deze aanpak is Cyber Rating, ofwel CYRA.

Een belangrijke kwalificatie hierbij is wel dat dit hele suppliers-netwerk natuurlijk een sterke hiërarchie heeft. In de maritieme sector in de Rotterdamse regio is die hiërarchie er veel minder. Dat neemt niet weg dat ook in de maritieme sector de ketenafhankelijkheden groot zijn. Het is daarom ook in Rotterdam zinvol om tot een aanpak te komen die daar expliciet invulling aan geeft. De CYRA-aanpak in de Brainport regio doet qua organisatie sterk denken aan de ISPS aanpak die na 9/11 in de Rotterdamse haven is uitgerold. Ook toen was er een grote noodzaak om alle betrokken partijen (126 terminals die zeeschepen konden ontvangen) heel snel compliant te krijgen met de ISPS-regels. Met een collectieve aanpak, waarbij ondernemers gefaciliteerd werden, maar waarin ook de standaard op regio-niveau werd vastgesteld, is dat toen heel effectief uitgevoerd.

Huidige positie en behoefte

Naast de formulering van bijzondere kwetsbaarheden in de Rotterdamse maritieme sector zijn de vervolg vragen: waar we nu staan, en is dat al voldoende? Onze gesprekken met experts en stakeholders leveren het volgende beeld op:

- Los van de aandacht die cyberscecurity nu krijgt in de wetenschap (via de Topsectoren, bijvoorbeeld), en bij de nationale overheid, zijn er nog veel partijen – daaronder ook het management van essentiële bedrijven – die nog heel weinig zicht hebben op de problematiek. Het verhogen van de kennis over cybersecurity, met in achtneming van de bijzondere risico's in de Rotterdamse regio, blijft dus nog steeds belangrijk. Hierbij speelt ook de politieke aandacht in bijvoorbeeld de Rotterdamse gemeenteraad, en de manier waarop cybersecurity in de gemeenteorganisatie belegd is een belangrijke rol.
- De NIB2-regelgeving gaat ervoor zorgen dat een significant aantal bedrijven (waarschijnlijk enkele honderden in de maritieme sector) met hun cyberveiligheid aan de gang moeten, onder toezicht van de overheid (maar met sectoren die verdeeld zullen worden over diverse ministeries). Een aantal scans is al gedaan, en daaruit volgt dat veel bedrijven met de 'hygiëne-maatregelen' al goed op streek zijn, maar dat er ook nog wel werk te doen is. Portbase, het IT- platform voor de haven, heeft vorig jaar (2022) bij al haar gebruikers multi-factor-authenticatie ingevoerd. Het is vooralsnog onduidelijk hoe ketenpartners, anders dan directe toeleveranciers, betrokken zullen raken in dit proces. Daarnaast is er onvoldoende zicht op de mate waarin daarmee dan het hele

[6] Zie het verslag van het Cybercafe van Ferm van 21 april 2022 over Cyra en ASML

maritieme ecosysteem afgedekt wordt, of dat er een soort witte vlekken blijven met bedrijven die niets doen aan cybersecurity.

- Er is eigenlijk geen invulling van een ideaalbeeld voor bedrijven ten aanzien van cybersecurity, noch bij wetenschappers, overheid (nationaal of lokaal) of bedrijven. Dit betekent dat veel bedrijven onzeker blijven of ze voldoende doen, en dit houdt ook een risico in dat bedrijven te veel doen. Dit laatste maakt hen duurder dan concurrenten, en tast uiteindelijk de concurrentiepositie van de maritieme sector aan.
- Er worden brede, geautomatiseerde scans uitgevoerd om bepaalde standaard-kwetsbaarheden in kaart te krijgen. Dit is in lijn met de laatste gedachten over hoe onder grote groepen bedrijven een basaal niveau van cyberverdediging kan worden geïntroduceerd. Momenteel zijn dit nog ad hoc initiatieven, maar experts adviseren om dit soort scans onderdeel te maken van een sectorale aanpak en ze met enige regelmaat uit te voeren in delen van de maritieme sector.
- Terwijl bedrijven nog zoeken naar de eisen, eenvoudige maatregelen, en hun witte vlekken, zijn er al veel leveranciers van technische, zakelijke en organisatorische oplossingen. Om te beoordelen of die oplossingen nuttig en redelijk geprijsd zijn is een gezamenlijke kennisinfrastructuur nodig voor de Rotterdamse maritieme sector waar vooral MKB-bedrijven laagdrempelig terecht kunnen met vragen over tools, oplossingen, en kennisvragen. Deze kennisinfrastructuur is in aanleg aanwezig via FERM, maar haar langdurig bestaan is nog niet gezekerd.
- Op het vlak van cyberverdediging tegen daadwerkelijke aanvallen wordt in Rotterdam een gezamenlijke infrastructuur overwogen, een zogenaamd Security Operations Center (SOC) voor de haven. Dit onderzoek loopt, dus het is goed om de resultaten hiervan af te wachten. Verschillende partijen geven wel aan dat zo'n SOC liefst op bestaande structuren geënt zou moeten worden. Daarbij lijken de governance-structuur van ISPS, de kennisbasis van FERM, en de bestaande cyberverdediging van het havenbedrijf voor de hand liggende componenten.

Conclusie: waar moeten we naar toe?

Bij een initiële discussie over dit advies is gesproken over de achterliggende ambitie om de maritieme sector in de Rotterdamse regio op de kaart te zetten met een effectieve cybersecurity-aanpak. De meest directe manier om daartoe te komen is om het grootste hiaat in de gezamenlijke kennis van bedrijven, overheid en kennispartijen in te gaan vullen: wat is nu een ideaal niveau van cybersecurity?

De Rotterdamse maritieme sector is zo rijk geschakeerd dat juist hier in Rotterdam die vraag beantwoord kan en moet worden. Daarvoor is het nodig om de bestaande kennis beter te laten circuleren, en uit te wisselen, en om de unieke kennis in de rest van de Nederlandse economie te benutten, zoals de CYRA-aanpak in Eindhoven. De introductie van de NIB2-regelgeving zal ervoor zorgen dat een groot aantal bedrijven rechtstreeks met cybersecurity-eisen geconfronteerd gaan worden. Hiermee is al een goede start gemaakt via FERM en initiatieven van onder andere het Havenbedrijf Rotterdam. Aanvullend hierop is het nodig om steeds goed te borgen dat de hele keten en de hele maritieme sector uiteindelijk door deze maatregelen geraakt wordt. Deze verantwoordelijkheid is in het ecosysteem nog niet belegd.

Het CYRA initiatief in de Brainport Eindhoven
Het initiatief Cyber Rating (CYRA) is een programma van het Cyberweerbaarheidscentrum Brainport Eindhoven. Het programma is gericht op het ondersteunen van het MKB in de regio Eindhoven om tot een vergelijkbaar niveau van cybersecurity te komen als de nieuwe standaard ISO 27001. Het programma is gericht op het introduceren van de 'basis hygiëne' maatregelen voor cybersecurity. Het is gebaseerd op een drie-stap maturity model, waarbij bij grotere bedrijven meer maatregelen worden genomen. Voor het behalen van de gewenste niveaus worden certificaten vertrekt (op basis van een geaccrediteerde audit).

Dit programma bevat een dashboard oplossing, waarbij informatie over alle betrokken bedrijven anoniem kan worden weergegeven, en een benchmark aanpak, waarbij de maatregelen bij bedrijven kunnen worden vergeleken met 'peers'. Daarnaast is er een self-assessment faciliteit die door de bedrijven zelf gebruikt kan worden om te controleren waar zij staan.
Het certificeringstraject is onderdeel van het lidmaatschap van het cyberweerbaarheidscentrum. Lidmaatschap komt met een eerste scan en audit, op basis waarvan het 'basis' certificaat wordt uitgereikt.

Het CWB is een samenwerking van de provincie Noord-Brabant, Metropoolregio Eindhoven, Brainport Industries, BDO advisory, en de Ministeries van EZK en J&V. Gegeven de specifieke situatie in de provincie Noord-Brabant, en de trekkende rol van de provincie is in dit initiatief de rol van de gemeente Eindhoven beperkt.

Bron: cwbrainport.nl/nieuws/wat-is-cyra

Het is ook van belang dat zowel lokaal als nationaal er voldoende begrip is bij de overheid en volksvertegenwoordiging dat cybersecurity in de Rotterdamse regio bijzondere aspecten heeft vanwege het economische belang van haven en maritieme activiteiten, en vanwege de complexe bedrijfsnetwerken. Dit betekent niet dat 'Rotterdam' helemaal zelf een cyberaanpak moet bedenken. Maar in de manier waarop in Rotterdam de cybersecurity-initiatieven vanuit nationaal niveau worden geadopteerd moet de bijzondere positie van de maritieme sector in Rotterdam wel meegewogen worden. Om deze bijzondere positie te bestendigen is het nuttig om de verschillende lijnen van een effectieve cyberaanpak (governance, kennis, verdediging) in een institutie in de regio bij elkaar te laten komen. Dit zou een organisatie moeten zijn die zoveel mogelijk voortbouwt op en integreert wat er al is.

Om te kunnen toetsen of de 'Rotterdamse aanpak' op internationaal niveau overeind blijft is een internationale benchmark ook belangrijk. Vergelijkend onderzoek in geavanceerde havenregio's zoals Los Angeles, Singapore en Busan is daarbij noodzakelijk.

Tenslotte is een bijzondere uitdaging gelegen in het feit dat de maritieme sector in Rotterdam voor een deel bestaat uit Nederlandse vestigingen van internationale bedrijven. Een deel van deze bedrijven is gelegen in, of geassocieerd met, bekende statelijke agressors in het cyberdomein. Dit roept vragen op over de manier waarop in de Rotterdamse maritieme sector alle bedrijven op dezelfde manier betrokken zouden moeten zijn bij initiatieven en maatregelen. Dit thema vraagt gespecialiseerde aandacht van partijen als Clingendael, HCSS en/of de AIVD, en ontstijgt in belang dit onderzoek.

5. Aanbevelingen en prioriteiten

In Hoofdstuk 4 hebben we aangegeven waarom het in het Rotterdamse maritieme cluster een noodzaak is voor een 'Rotterdamse' aanpak voor cybersecurity. Het strategisch en economische belang van de maritieme sector, de diversiteit in soorten bedrijven en activiteiten alsmede de complexe structuur van het maritieme cluster vraagt om een specifieke aanpak. Tegelijkertijd is er op nationaal en internationaal niveau een uitgebreide ontwikkeling ingezet op het vlak van de ontwikkeling van regelgeving (NIB-2) en het inrichten van instituties (NCSC, enzovoort). Deze ontwikkeling vormt de context waarbinnen de Rotterdamse initiatieven vorm moeten krijgen. Tenslotte heeft bijvoorbeeld een recente bedrijvenscan in de maritieme sector in Rotterdam laten zien dat de grootte van het bedrijf een belangrijke indicator is voor de mate waarin men cybersecuritymaatregelen neemt.

De cybersecurity-problematiek sluit goed aan bij de ambities die geformuleerd zijn in het Rotterdamse MKB Actieprogramma[7] dat voor 2023 gelanceerd is. In dat programma is expliciet aandacht voor het inrichten van toekomstgerichte bedrijfsvoering, die schoon, innovatief, digitaal en circulair moet zijn. De gemeente ziet voor zichzelf een rol in het helpen organiseren van activiteiten voor en door ondernemers, die als doel hebben het informeren, inspireren en activeren van ondernemers.

Advies: Versterk het cyberweerbaarheidsinitiatief in voor de Rotterdamse maritieme sector

Onze belangrijkste aanbeveling is om voor de maritieme sector in Rotterdam de bestaande cyberweerbaarheidsinitiatieven, waarin FERM en het Havenbedrijf Rotterdam belangrijke rollen hebben, te versterken en uit te bouwen. Daarbij kan de aandacht vooral uitgaan naar de betrokkenheid van het brede maritieme MKB, door middel van het toepassen en uitbouwen van een werkbare MKB cyberveiligheidsstandaard voor de maritieme sector. Uiteindelijk moet het cyberweerbaarheidsinitiatief de volgende componenten bevatten:

4. Een governance structuur. Hierbij adviseren wij tenminste te onderzoeken in hoeverre de bestaande en goed werkende ISPS-governance structuur bruikbaar is, of uitgebreid kan worden om de toezichtsfunctie voor cybersecurity in onder te brengen. Binnen de ISPS structuur zijn in Rotterdam, voor de operaties in de haven, al specifieke initiatieven (cyber meldpunt) genomen. Tegelijkertijd dekt de huidige ISPS-structuur momenteel maar een beperkt deel van de brede maritieme sector af.
5. Een kennisinfrastructuur van en voor bedrijven. De functie van deze kennisinfrastructuur heeft een aantal componenten: allereerst is kennis nodig over het actuele niveau van kwetsbaarheden bij bedrijven, daarnaast is het nodig om een certificeringsmodel voor bedrijven (self-scan, audits, begeleiding voor het implementeren van maatregelen, gericht op het streven naar ISO 27001 niveau) uit te kunnen voeren, en er is kennis nodig over allerlei oplossingen die door dienstverleners worden aangeboden aan MKB bedrijven. FERM voert nu al een deel van deze rollen uit. Het verdient daarom aanbeveling om de mogelijkheden voor uitbreiding van het takenpakket van FERM, alsmede langjarige financiering te verkennen.
6. De derde onmisbare component is de cyberverdedigingscomponent. De invulling van dit deel van een cyberweerbaarheidsinstitutie wordt op dit moment onderzocht, door Deloitte, FERM en het Havenbedrijf Rotterdam. Vanuit dit onderzoek is een belangrijke vraag of een gezamenlijke

[7] https://www.watdoetdegemeente.rotterdam.nl/begroting2023/programmas/economische-ontwikkeling2/3-doel1/

verdedigingsstructuur zo kan worden ingericht dat die ook voor aanvallen op kleinere bedrijven ingezet kan worden.

Het advies om het cyberweerbaarheidsinitiatief uit te bouwen leidt tot het benoemen van een aantal prioriteiten.

4. Binnen de bestaande ISPS governance structuur moet worden besproken of de uitbreiding van de verantwoordelijkheid naar het hele maritieme cluster en het brede cybersecurityveld wenselijk en mogelijk is. Hierbij zijn er rollen voor de gemeente (burgemeester, wethouder), de Port Security Officer (de havenmeester) en andere betrokkenen.
5. Voor de uitbreiding van de kennisinfrastructuur en de rol die FERM daarin speelt moet een verkenning worden gestart over middelen en mogelijkheden. Vooral de financiering op de langere termijn is daarbij een belangrijke voorwaarde voor succes. Dit vereist overleg tussen de founding fathers van FERM, de betrokken publieke partners, en de FERM organisatie.
6. Voor wat de inrichting van de cyberverdediging betreft: omdat hier al een onderzoek loopt doen we daar geen uitspraken over. Wel stellen wij voor dat dit onderzoek na afronding breed wordt neergelegd in de maritieme sector, om een goede vervolgdiscussie te krijgen over de verdediging van de hele maritieme sector.

Advies: Besteed binnen de Rotterdamse maritieme cyberweerbaarheid bijzondere aandacht aan ketenafhankelijkheden

Een bijzonder aspect van de situatie in Rotterdam is dat de nadruk van alle drie de componenten sterk zien op de ketenstructuur van het maritieme cluster. Deze structuur wordt gekenmerkt door grote complexiteit, en door een gebrek aan een duidelijke hiërarchie. Rotterdam wordt gekenmerkt door een relatief *groot* aantal leader firms, en dat betekent dat het uitzetten van een gecoördineerde aanpak minder eenvoudig is dan in de brainport regio Eindhoven. De druk op kleinere bedrijven om meer aan cybersecurity te doen zal vooral ontstaan vanuit de verplichtingen van NIB-2, en het risico is daarbij dat dat door elk bedrijf anders wordt ingevuld, en dat kleinere bedrijven met verschillende eisen worden geconfronteerd. Dit inzicht, en de specifieke mechanismen om hiermee om te gaan zullen de aanpak in de Rotterdamse maritieme sector onderscheidend maken. Het lijkt onvermijdelijk dat hiervoor een wat sterkere institutionele structuur moet worden ingericht dan in de Brainport Eindhoven.

Deze institutionele oplossing maakt het wel goed mogelijk om, om te gaan met de grote aantallen kleine bedrijven die deel uitmaken van het maritieme cluster. Door de combinatie van self-assessment, auditing en certificering en het toezicht daarop kunnen grote groepen MKB bedrijven meegenomen worden in het op zijn minst inrichten van de cyber hygiëne maatregelen. Benut hierbij ook vooral het mechanisme van NIB-2, maar maatregelen dienen geformuleerd te worden vanuit een gezamenlijke visie op ketenafhankelijkheden.

Naast het inrichten van een meer collectieve aanpak die werkt voor de Rotterdamse situatie is ook nader onderzoek nodig naar de precieze invulling van ketenafhankelijkheden. Dit soort onderzoek is een uitbreiding van het kwetsbaarheidsonderzoek dat nu door de gemeente is uitgezet. Dit onderzoek kijkt vooral naar kwetsbaarheden in publiek toegankelijke IT-omgevingen zoals websites en email. Nader onderzoek is nodig om de digitale relaties tussen de partijen in de maritieme sector beter te begrijpen en de kwetsbaarheden die hiermee samenhangen beter in kaart te krijgen. Daarbij gaat het om

informatieuitwisseling (al of niet als onderdeel van een handelsrelatie), updaterechten van IT leveranciers, wederzijdse data-aanpassingsrechten bij partijen, enzovoort.

Advies: Versterk het politieke draagvlak voor de Rotterdamse maritieme cyberweerbaarheid

Naast ons voorstellen voor de inrichting van deze cyber-institutionele structuur voor de Rotterdame maritieme sector zien wij nog een belangrijke randvoorwaarde. Het is van groot belang dat in de gemeente Rotterdam de dreiging ten aanzien van cybersecurity in de maritieme sector op waarde wordt geschat. We stellen daarom voor om de wethouder te adviseren om hier ook met de gemeenteraad over in gesprek te gaan. Dit zou kunnen door het schrijven van een beleidsbrief maritieme cybersecurity door de wethouder aan de gemeenteraad. Daarin zou, naast een overzicht van nationale en internationale ontwikkelingen, vooral de bijzondere positie en kwetsbaarheid van de Rotterdamse maritieme sector centraal moeten staan, en de gedachten over het inrichten van een cyberweerbaarheidsinitiatief waarmee Rotterdam zich internationaal kan onderscheiden.

Advies: Vergeet niet om breed voorlichting te blijven geven aan bedrijven, personeel en leidinggevenden in de Rotterdamse maritieme sector

De Rotterdam maritime board heeft op een heel aantal dossiers een klokkenluidersrol. Dat is ook voor cybersecurity het geval. Dit onderzoek, en het daarop gebaseerde advies is daar een invulling van. Het is van belang dat de board die rol blijft vervullen, en samen met de gemeente invulling blijft geven aan de informerende, inspirerende en activerende rol die de gemeente als ambitie in het MKB actieprogramma heeft geformuleerd.

Daarbij speelt een belangrijke rol dat ondanks de aandacht voor cybersecurity in bepaalde delen van de maritieme sector en daarbuiten, nog heel veel individuele bedrijven, personeel en leidinggevenden maar een heel beperkt begrip hebben van de ontwikkelingen, oplossingen, mogelijkheden en formele eisen. Velen realiseren zich ook nog onvoldoende hoe cybersecuritykwetsbaarheden zich manifesteren in complexe netwerken en hoe zij zich daartegen moeten wapenen. Informatievoorziening en voorlichting blijft daarom een heel belangrijk wapen tegen cyberkwetsbaarheid. Wij adviseren om als gemeente met bedrijven samen dit soort voorlichting, liefst ingevuld met concrete casussen van bedrijven, te blijven aanbieden. De Rotterdam maritime board kan hier een coördinerende en stimulerende rol in spelen. De continuïteit van een dergelijk activiteiten kan ook goed verzekerd worden via een stabiel, goed gefinancierd cyberweerbaarheidsinitiatief.

Bijlage

1. Overzicht activiteiten/sectoren bedrijven haven- en maritieme cluster

SBI2	Omschrijving	Aantal bedrijven
52	Opslag en dienstverlening voor vervoer	826
50	Vervoer over water	529
46	Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)	441
71	Architecten, ingenieurs en technisch ontwerp en advies; keuring en controle	274
25	Vervaardiging van producten van metaal (geen machines en apparaten)	212
84	Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen	93
33	Reparatie en installatie van machines en apparaten	61
30	Vervaardiging van overige transportmiddelen	54
20	Vervaardiging van chemische producten	53
80	Beveiliging en opsporing	47
49	Vervoer over land	45
77	Verhuur en lease van auto's, consumentenartikelen, machines en overige roerende goederen	39
38	Afvalinzameling en -behandeling; voorbereiding tot recycling	29
10	Vervaardiging van voedingsmiddelen	27
28	Vervaardiging van overige machines en apparaten	27
45	Handel in en reparatie van auto’s, motorfietsen en aanhangers	18
42	Grond-, water- en wegenbouw (geen grondverzet)	17
19	Vervaardiging van cokesovenproducten en aardolieverwerking	16
35	Productie en distributie van en handel in elektriciteit, aardgas, stoom en gekoelde lucht	16
81	Facility management, reiniging en landschapsverzorging	16
29	Vervaardiging van auto's, aanhangwagens en opleggers	13
24	Vervaardiging van metalen in primaire vorm	12
27	Vervaardiging van elektrische apparatuur	11
23	Vervaardiging van overige niet-metaalhoudende minerale producten	9
43	Gespecialiseerde werkzaamheden in de bouw	9
9	Dienstverlening voor de winning van delfstoffen	8
74	Industrieel ontwerp en vormgeving, fotografie, vertaling en overige consultancy	8
94	Levensbeschouwelijke en politieke organisaties, belangen- en ideële organisaties, hobbyclubs	8
64	Financiële instellingen (geen verzekeringen en pensioenfondsen)	7
8	Winning van delfstoffen (geen olie en gas)	6
91	Culturele uitleencentra, openbare archieven, musea, dieren- en plantentuinen, natuurbehoud	6
26	Vervaardiging van computers en van elektronische en optische apparatuur	5
62	Dienstverlenende activiteiten op het gebied van informatietechnologie	5
70	Holdings (geen financiële), concerndiensten binnen eigen concern en managementadvisering	4
31	Vervaardiging van meubels	3
68	Verhuur van en handel in onroerend goed	3
41	Algemene burgerlijke en utiliteitsbouw en projectontwikkeling	2
3	Visserij en kweken van vis en schaaldieren	1
16	Primaire houtbewerking en vervaardiging van artikelen van hout, kurk, riet en vlechtwerk (geen meubels)	1
22	Vervaardiging van producten van rubber en kunststof	1
32	Vervaardiging van overige goederen	1
39	Sanering en overig afvalbeheer	1
51	Luchtvaart	1
66	Overige financiële dienstverlening	1
78	Arbeidsbemiddeling, uitzendbureaus en personeelsbeheer	1

NOTEN

[1] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52020JC0018&from=NL
[2] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[3] https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen
[4] https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0006.02/DOC_1&format=PDF
[5] https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0006.02/DOC_2&format=PDF
[6] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32019R0881&from=EN
[7] https://digital-strategy.ec.europa.eu/nl/library/cyber-resilience-act
[8] https://www.ncsc.nl/onderwerpen/wettelijke-taak
[9] https://open.overheid.nl/repository/ronl-ec4dde7f-d0b3-46dc-83f7-174c42584100/1/pdf/tk-bijlage-overzicht-wet-en-regelgeving-cybersecurity.pdf
[10] https://puc.overheid.nl/nsi/doc/PUC_2396_14/
[11] Interview Port of Rotterdam, 14 december 2022
[12] https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
[13] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf
[14] https://www.ncsc.nl/over-ncsc/wettelijke-taak
[15] https://securitydelta.nl/nl/over/over-hsd
[16] https://www.cybersecurityalliantie.nl/over-csa/
[17] https://www.enisa.europa.eu/about-enisa/about/nl
[18] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022---2028/Nederlandse+Cybersecuritystrategie+2022+-+2028.pdf
[19] https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds
[20] https://www.ncsc.nl/onderwerpen/basismaatregelen/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen
[21] https://vng.nl/sites/default/files/2022-03/Cyberbeeld%20Rotterdam%202022.pdf
[22] https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022
[23] https://www.resilientrotterdam.nl/rotterdamse-cybersecurity-pilot-mkb/
[24] https://www.ncsc.nl/onderwerpen/isidoor
[25] Erasmus UPT (2022) Havenmonitor 2022 via www.havenmonitor.nl