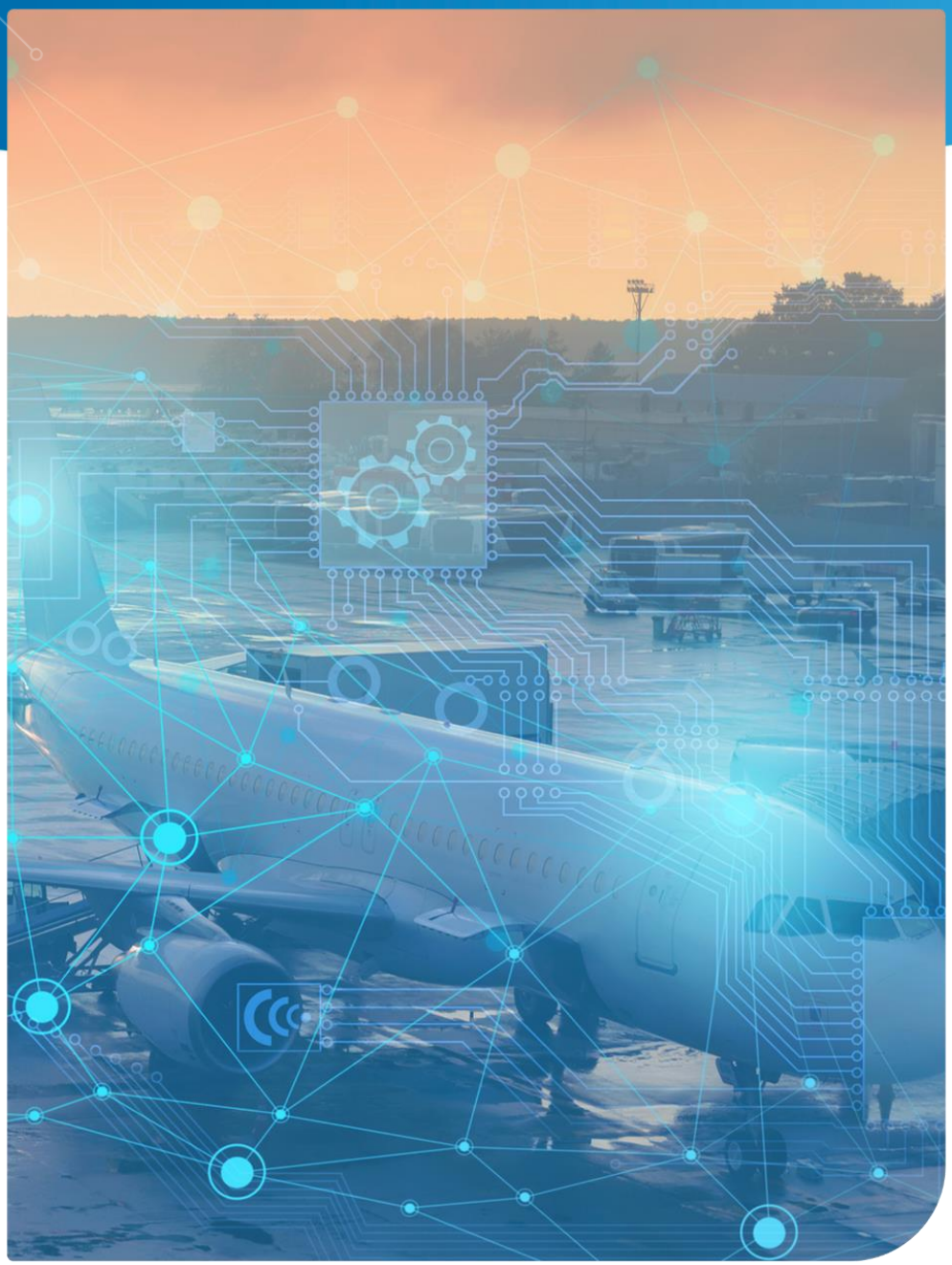
Analyserapport

Cyber Security en samenwerking in de Lucht- en ruimtevaart-keten in de provincie Zuid-Holland

Armando Lorenzo, projectleider onderzoek Cyber Security in de sector Lucht- en Ruimtevaart. Security Delta



HSD

securitydelta.nl

Inhoudsopgave

Inleiding

In de *Roadmap verbeteren weerbaarheid Zuid-Holland* lezen we dat "Digitale transformatie versnelt, en daarmee de maatschappelijke en economische afhankelijkheid van digitale netwerken en diensten. Tegelijkertijd neemt het aantal cybersecurity incidenten dagelijks toe. De Provincie Zuid-Holland toont haar betrokkenheid om de digitale weerbaarheid en veerkracht te vergroten en wil een aanzet geven voor regionale programmering om cybersecurity (verder) in de economie in te bedden door middel van de Road Map *Verbeteren Weerbaarheid Digitale Economie* als basis voor effectieve maatregelen, beleid, en verbeterde processen om het geïdentificeerde risico te beheersen.

Overigens zijn er naast zorgen ook kansen. Immers digitaal weerbaarheid van de economie is een goed uithangbord voor het aantrekken van nieuwe bedrijven. Een robuuste en veilige ICT-infrastructuur, goede dienstverlening om cyber incidenten te voorkomen en te verhelpen, een hoge mate van cyber awareness bij het MKB waarvan grotere bedrijven afhankelijk zijn en een cyber-ready workforce nemen zorgen weg en dragen bij aan een goed vestigingsklimaat.
Ook zijn er goede kansen voor cyberinnovatie en voor cybersecurity ondernemingen in de regio. Er is immers al een goede basis rondom Security Delta (HSD). Binnen de ICT is cybersecurity de snelst groeiende sector, naast toepassing van Artificial Intelligence (AI) en blockchain. Hoe beter ondernemingen samen met en voor de regionale economie relevante cyberproducten ontwikkelen en
hoe meer deze regionaal worden verkocht, hoe meer groei van deze cybersecuritybedrijven zal worden gerealiseerd, terwijl de regionale economische sectoren ook nog eens beter zijn voorbereid op cyberaanvallen. Samenwerking met academische instelling, R&D-organisaties, volwassen ICT-dienstverleners en de overheid als klant versterkt zo'n cluster verder." [Bron: 1]

De Metropoolregio Rotterdam Den Haag (MRDH) erkent het belang van digitalisering als belangrijke voorwaarde voor economische innovatie. Weerbare economische en digitale sectoren ontstaan alleen als de cyberveerkracht van die sectoren wordt vergroot.
In de ontwikkeling van nieuwe technologieën is veiligheid en privacy niet altijd meegenomen. Bovendien neemt het aantal cyberaanvallen en incidenten flink toe. Dit heeft niet alleen impact op de organisatie die daarvan het slachtoffer is, maar ook op organisaties die hiermee in verbinding staan. Kwetsbaarheden kunnen met het vergroten van digitale kennis en vaardigheden worden opgelost, zodat een digitaal weerbare economie ontstaat. De cyberveiligheidsrisico's en veiligheidsaanpak verschillen per sector omdat deze samenhangen met de manier waarop digitale technologie en kennis in de sector worden toegepast. 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 is daarom een programma gestart 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 ondernemingen in de sector Lucht- en Ruimtevaart in de provincie Zuid-Holland. Het huidige volwassenheidsniveau van weerbaarheid wordt gegeven volgens de maturity-tabel (bijlage 1) en de bereidheid van de ondernemingen deze weerbaarheid zo mogelijk in gezamenlijkheid te versterken.
Ook geeft het rapport antwoord of er concrete vraagstukken zijn ten aanzien van cyber security en of bedrijven bekend zijn met HSD als partner om deze vragen te beantwoorden.

1. Onderzoek

Door de toenemende dreiging van cyberaanvallen zoals met gijzelsoftware of ransomware, is het voor bedrijven een uitdaging om de ICT-infrastructuur goed te beheren en maximaal te benutten. De provincie Zuid Holland heeft als uitdaging de economie en de werkgelegenheid in de regio te versterken door bedrijven te laten samenwerken en zo weerbaarder te worden. (https://www.economicboardzuidholland.nl/cybersecurity)

Daarom is een onderzoek gestart naar de huidige situatie omtrent cyber-weerbaarheid en wordt bedrijven gepolst naar de mogelijkheid samen te werken in de bestrijding en weerbaarheid van Cyber security. Het doel is de cyber-weerbaarheid en professionaliteit van bedrijven te vergroten en daarmee de economie te versterken.

In de eerste fase worden verschillende stakeholders, netwerk- en samenwerkingspartners benaderd om nader inzicht te krijgen in de digitalisering van de sector, de veiligheid ervan en de belangrijke spelers daarbinnen. In opdracht van Security Delta (HSD) is daartoe deze analyse voor de Metropoolregio Rotterdam Den Haag opgesteld van de Cyber Security binnen de sector Lucht- en Ruimtevaart (Aerospace) in met name Zuid Holland.

Interviews

Het onderzoek is uitgevoerd door het bij diverse bedrijven afnemen van interviews die zijn opgebouwd rondom drie vraagstukken. Een vierde vraag is toegevoegd om via de geïnterviewde organisatie doorverwezen te worden naar een directe leverancier of klant uit de keten die ook in de sector Lucht & Ruimtevaart opereert en gevestigd is in Zuid-Holland.

1. Wat is de Cyber Security volwassenheid van de organisatie (weerbaarheid, awareness).
2. Leven er concrete cyber veiligheidsvraagstukken (bv. compliance, crisispreparatie technologie of andere vragen over online kwetsbaarheden)?
3. Hoe staat het bedrijf tegenover een samenwerking binnen de sector om in gezamenlijkheid cybersecurity tot een hoger niveau tillen door de mogelijkheid om de verworven veiligheidskennis en -kunde ter beschikking te stellen aan andere ketenpartners.
4. Welke bedrijven met contactpersonen die het bedrijf kent (bijvoorbeeld als klant of leverancier binnen de supply-chain) kan opvolgend aan dit interview worden benaderd als onderdeel van de sector Lucht- en Ruimtevaart-keten in de provincie Zuid-Holland?

De voor het onderzoek later beschikbaar gestelde *maturity*-tabel (Bijlage 1) bleek een goed en praktisch instrument voor het beantwoorden van de eerste vraag en voor het starten van een open gesprek. De vraag hoe het gesteld is met Cybersecurity leidt soms tot enige weerstand in concrete beantwoording, maar door vooraf een mail te sturen met deze tabel in de bijlage, konden bedrijven ter voorbereiding op voorhand nadenken over het veiligheidsniveau in hun bedrijfsproces en de hadden zij hiermee een beter idee over de bedoeling van de vraag en de toegepaste waarderingsnorm.

De vierde vraag gaf de mogelijkheid om, op voorzet van de relatie, opvolgend andere bedrijven in de sector Aerospace te benaderen. Door deze vraag kwamen ook minder *usual suspects*-bedrijven in zicht zoals toeleveranciers of afnemers van specifieke of minder opvallende onderdelen of services

in de keten. Naast enkele andere contacten in de markt reikte *Innovation Quarters* een eerste groep aan van drie organisaties in de sector Aerospace waarmee het onderzoek van start is gegaan.

Van de interviews is een kort geanonimiseerd verslag gemaakt. Enkele bedrijven gaven te kennen geen bezwaar te hebben tegen naamsvermelding of vulden bij de gerectificeerde tekst zelf de namen in.

2a. Cybervolwassenheid

Dit onderzoek en de interviews moeten niet beschouwd worden als gedetailleerde weerslag van de cybersecurity situatie bij de bevraagde organisaties. Zowel het aantal geïnterviewde bedrijven als de type vraagstelling is daarvoor te beperkt.
Ter vergelijking werden bij een veiligheidsonderzoek cybersecurity in de Rotterdams Haven dat is uitgevoerd door de Haagsche Hogeschool in samenwerking met VeiligheidsAlliantie regio Rotterdam (VAR), FERM en het Havenbedrijf, 738 onderzocht en was er concreet resultaat van 93 respondenten met een veelvoud aan vragen over veiligheidsmaatregelen [bron: 2].

Bij de gevoerde gesprekken in dit onderzoek is als maatstaf de *maturity*-tabel (bijlage 1) gehanteerd, wat een hulpzaam instrument bleek bij de interviews. Het geeft een goed en eenvoudig beeld voor de globale normering van de volwassenheid van de cyberveiligheid bij het geïnterviewde bedrijf. (De tabel is licht aangepast voor gebruik bij dit onderzoek).
De organisaties hadden met deze tabel een duidelijk beeld hoe het volwassenheidsniveau van hun weerbaarheid was en in welke richting (op het gebied van infrastructuur, organisatie en beleid) systematisch stappen gezet kunnen worden voor verbetering (groei in volwassenheidsniveau).
Er was bij de bedrijven die een laag maturity-niveau hadden vaak ook het besef (*'ik zal wel laag zitten'*). Het concrete vraagstuk dat hieruit voortvloeit is, dat er behoefte is aan een roadmap die eenvoudig bruikbaar is en aangeeft welke acties op aandachtspunten (zoals die als voorbeeld zijn opgenomen in bijlage 3) te nemen zijn om naar het volgende niveau te groeien.

Gebruik digitale middelen en cybervolwassenheid

De sector Aerospace blijkt in hoge mate gedigitaliseerd en daarmee rijp voor de door de provincie geïdentificeerde bedreigingen, maar dus ook voor de genoemde kansen met cybersecurity. De geïnterviewde organisaties leveren digitale producten en services of zijn er in hoge mate van afhankelijk. De bedrijven zijn alle afhankelijk van ICT of gebruiken IoT in het bedrijf of bij de geleverde diensten en producten en dragen dus ook het digitale risico. De *awareness* bij de organisaties is daarmee evident hoog. Dit wordt mede veroorzaakt door de sectorcultuur waarbij bedrijven gewoon zijn om gecertificeerd te zijn (bijvoorbeeld volgens de ISO-normering) of te voldoen aan door handelspartners gestelde voorwaarden.

De bedrijven kennen alle mogelijke dreigingen van bijvoorbeeld (vreemde) e-mails en de grote impact als er op een verkeerde link wordt gedrukt of van andere vormen van Cyberrisico's. In een enkel geval waren zij er ook slachtoffer van of ondervonden daar (bijna) schade van. Concrete ervaringen werden evenwel relatief weinig genoemd.

Het nemen van (met name technische) maatregelen staat op het netvlies en wordt bij de bedrijven overal wel in enige basale vorm toegepast (zoals tweetraps verificaties, de afweging om servers en data intern of extern op te nemen in de infrastructuur en een gedegen backup-beleid). Bedrijven kennen vrijwel alle een volwassenheidsniveau van weerbaarheid op minimaal niveau 2 (bijlage 6). Wat bij veel bedrijven ontbreekt is een cyber securitybeleid en bij die bedrijven is cyber security niet goed ingebed in de organisatie. Daar ontbreekt dan bijvoorbeeld de verdeling in taken en verantwoordelijkheden, budgettering en voldoende tijd om aandacht te besteden aan cybersecurity. Het protocol voor de aanpak bij een concrete aanval ontbrak bij de meeste bedrijven. Bij grotere bedrijven was dit beter ingevuld en was er soms ook een Chief Information Security Officer (CISO). Bij grotere bedrijven was er beter de mogelijkheid om tijd hiervoor in te plannen en personen en

taken toe te bedelen. Bij kleine of jonge bedrijven was het vaak de oprichter of directeur die bijvoorbeeld de rol van cybercoördinator vervult.

Groeien in volwassenheidsniveau

Verbeteringen zijn hier vooral te behalen in de extra te nemen technische maatregelen, de professionalisering van processen (zoals vastlegging van taken en rolverdelingen) en opname van cybersecurity in het beleid, met permanente acties gericht op weerbaarheid in een integrale aanpak (bewustzijn, bewaking, treffen van maatregelen).
Bedrijven beseffen dat er nooit 100% veiligheid zal zijn maar zij willen zich evenwel zo weerbaar mogelijk maken tegen digitale aanvallen en de Cybersecurity zo goed mogelijk professionaliseren. De bereidheid bij bedrijven te groeien in volwassenheidsniveau blijkt groot. De voordelen die daarbij ook mogelijk ontstaan zoals een beter eigen imago en daarmee de mogelijke economische voordelen worden door de bedrijven niet genoemd.

Genoemde weerstanden bij bedrijven waar geen volwassen beleid op cyberweerbaarheid is, zijn:

1. **Onbekendheid**
   Men is niet bekend met de materie of mogelijke te nemen stappen naar volwassenheid. Er is geen heldere route tot verbetering of de afweging van de baten tegen de risico's. De impact is onduidelijk en is soms gestoeld op onvolledige aannames.
2. **Geen core-business**
   Cyberveiligheid is niet ingebed in de bedrijfsprocessen, men acht zich nog in een te vroeg stadium van ontwikkeling van het bedrijf of men neemt aan dat de extern ingeschakelde organisatie voor systeembeheer of voor cyber-monitoring de cyberveiligheid actief, doeltreffend en afdoende aanbiedt. Er is geen verdere aandacht voor verbetering.
3. **Tijd**
   Met name bij kleinere organisaties zonder eigen systeembeheerder of cyber-kennis is geen tijd of geen tijd ingeruimd voor cyberveiligheid.
4. **Geld**
   Cyberweerbaarheid wordt niet gebudgetteerd in de bedrijfsuitgaven. Op dit vlak wordt de wens uitgesproken om onder laagdrempelige voorwaarden met subsidies of vouchers te worden ondersteund door gemeente, provincie of het rijk.

Het is met deze signalen duidelijk dat een gerichte ondersteuning nuttig is om cyberweerbaarheid bij die organisaties te bevorderen.

Extern beheer

Bij meerdere bedrijven is (een deel van) de ICT uitbesteed, waaronder het beheer van de ICT-infrastructuur. In die gevallen wordt in voorkomende gevallen aangenomen dat de cybersecurity ook op orde is, in sommige gevallen zonder dat hierover expliciete afspraken over zijn gemaakt, zoals het periodiek monitoren van het systeem, het verzorgen van protocollen en rolverdelingen of het borgen van een goede actuele backup.
Ook wordt bij het nemen van maatregelen binnen de eigen organisatie niet gekeken of de externe ICT leverancier eveneens voldoet aan de gestelde eisen voor samenwerken met ketenpartners.
Het is daarom goed om bij het programma om de cyberweerbaarheid van bedrijven te vergroten, de externe ICT-bedrijven daar nauw te betrekken.

Normering en certificering

Goede beveiliging is van groot belang. Er is een gevoel van de risico's en de impact en men is over het algemeen bekend met meerdere mogelijkheden van te nemen maatregelen (bijlage 3), maar er is geen kennis over de integrale samenhang of een helder stappenplan.
Mede door de eigenschappen typisch voor de sector Lucht & Ruimtevaart, zijn de organisaties alle bekend met eisen die gesteld worden met bijvoorbeeld de in de sector vaak gehanteerde ISO-normen (onder *Safety*) waaraan moet worden voldaan. Deze worden alle ter hand genomen, waarmee bescherming van privacy-gegevens en andere veiligheidseisen ook leidt tot een zekere mate van basis-cyberveiligheid.
Leveranciers worden daarbij soms beoordeeld door (herhaald) naar certificering te vragen, maar in sommige gevallen worden zij slechts beoordeeld eenvoudig op basis van het (betrouwbare) beeld dat over de bedrijven bestaat (groot in omvang, geografische reikwijdte, leeftijd of langdurige relatie).

Het invoeren van een beveiligingsclassificatie van bedrijven in de vorm van bijvoorbeeld een certificering in de sector leek veel bedrijven nuttig voor de gehele sector en de supply-chain. Er werd de kanttekening gemaakt, dat voorkomen moet worden dat dit kostbaar wordt of tot een hoge administratieve belasting leidt.

2b. Samenwerken in een Regionaal Cyber-weerbaarheidscentrum

Alle geïnterviewde bedrijven zien voordeel in samenwerking met andere bedrijven om zo weerbaarder te zijn. De verwachting is dat in een op te richten regionaal cyber weerbaarheidscentrum (bijlage 7) informatie, technieken, kennis, ervaringen en *best practices* onderling (kunnen) worden uitgewisseld. Er is binnen bedrijven expertise die ook voor andere bedrijven in de sector interessant kan zijn. Zo is het latent aanwezige risico bekend bij het gebruik van chinese producten of het gebruik van externe opslag bij externe datacenters, waarvan het voor anderen interessant kan zijn deze kennis te delen.
Er was bij de bedrijven geen indruk dat men nadelen van een dergelijke samenwerking voorzag, op grond van bijvoorbeeld concurrentie en een enkeling vroeg zich daarbij af of de aanpak van Cybersecurity sectoraal moest worden ingedeeld, omdat cyber security feitelijk een generieke zorg betreft.

De meeste bedrijven hebben het idee dat een cybercentrum de functie moet hebben hen vérder te brengen in cyber security met antwoorden op vraagstukken als:

1. Waar zijn gedegen en juiste tools verkrijgbaar?
2. Hoe is cyberweerbaarheid haalbaar (betaalbaar en uitvoerbaar)?
3. En hoe is het praktisch implementeerbaar zonder (core-)processen te verzwaren?

In dergelijke centra zou, zo is de verwachting, kennis worden opgedaan en ervaring worden gedeeld over:

- Hoe werkt verzekeren tegen schade bij cyberaanvallen en hoe is de assistentie die verzekeraars bieden bij incidenten.
- Cybersecurity verbeteren is een cyclisch proces. Hoe kan dit continue gecontroleerd (bijv. met jaarlijks beoordeling) en aangepast worden; worden er scans aangeboden?
- De kennis over de bedrijfsprocessen is belangrijk om alles te kunnen herstellen als het fout gaat. Hoe kan een dergelijk informatiedocument opgezet worden.
- Incidenten dienen gemeld te worden en het vervolg moet teruggekoppeld worden aan de melder. Hoe wordt dit proces het best opgezet?
- Er moeten draaiboeken geschreven worden voor gebruik bij calamiteiten. Hoe stel je de protocollen op en hoe wordt dit geoefend?
- Wat zijn de voordelen van het instellen van een cyber-team in de organisatie?

Actieve participatie

Op de vraag of er interesse is voor actieve deelname, om gezamenlijk de sector als geheel te versterken op het gebied van cyberweerbaarheid wordt afwachtend gereageerd.
Voor de op te richten weerbaarheidscentra is het raadzaam de meerwaarde en de implicaties voor de sector en de participant goed aan te geven (bijlage 7).

Overwegingen die genoemd zijn om niet actief te participeren zijn:

1. Er bestaan al meerdere soortgelijke initiatieven zoals het Digital Trust Center (DTC) en het nationaal cyber security centrum (NCSC).
2. De beperkte meerwaarde voor het eigen bedrijf.
3. De (verwachte jaarlijkse) kosten.
4. De geografische afstand.
5. De benodigde frequentie en inzet van mankracht voor de participatie.
6. De beperkte eigen cyberkennis *(heeft actieve deelname dan nut?).*

Bedrijven met een kleine omvang lijken a priori weinig tijd en geld te willen steken in het initiatief; de meerwaarde voor hen moet duidelijk(er) zijn tegenover de investering in tijd en geld.
Enkele grote bedrijven zijn meer geïnteresseerd. Zij herkennen er eerder commerciële meerwaarde in of zien het voordeel voor de sector als geheel, als meerdere bedrijven in de sector weerbaar-volwassen zijn.

Hoewel de bedrijven onderkennen dat een sterke weerbaarheid goed is voor elk bedrijf individueel binnen de sector, lijkt er weinig behoefte aan het gezamenlijk versterken van de sector. Bedrijven zijn in het algemeen niet (dusdanig) afhankelijkheid van andere bedrijven in de sector, dat een zwakke schakel in de keten negatieve invloeden heeft op de andere bedrijven in de keten. Een gezamenlijk aanpak om de keten als geheel te versterken lijkt niet de geschikte aanpak.
Er lijkt niet voldoende draagvlak voor het oprichten van een eigen cybercentrum voor de sector Aerospace. De functie kan mogelijk ondergebracht worden bij één van de gelijksoortige initiatieven in de andere sectoren of bestaande initiatieven. De sector Lucht- en ruimtevaart (Aerospace) is aangewezen als *categorie B* vitale sector door de Nationaal Coördinator Terrorismebestrijding en Veiligheid [Bron 3] en valt daarmee in het aandachtsgebied van het DigitalTrustCenter (DTC) https://www.digitaltrustcenter.nl/.

In de sector wordt bij samenwerkingen veel gewerkt met (ISO-)certificeringen, onder andere op het gebied van veiligheid (waar cybersecurity onderdeel van uitmaakt), of er wordt gewerkt met door partners opgestelde voorwaarden en eisen waaraan klanten of leveranciers dienen te voldoen en waar cybersecurity onderdeel van kan uitmaken.

Zo bezien biedt een programma voor samenwerking voor verbetering van de sector als geheel geen overtuigende meerwaarde en wordt de handelsketen in de sector het best versterkt door een aanpak, waarbij de verbindingen tussen de schakels onderling gericht geregeld en versterkt wordt.
In dat geval zou de ondersteuning gericht moeten zijn op de afzonderlijke bedrijven waarbij de bedrijven kunnen groeien in volwassenheid van cyberweerbaarheid, bijvoorbeeld door het bieden van scans, waarbij op basis van de uitkomsten daarvan ondersteuning geboden wordt bij het implementeren van maatregelen waarmee het bedrijf groeit in cyberweerbaarheid.
Het vastleggen van de maturity met een certificaat past daarbij binnen de huidige cultuur van samenwerken binnen de sector. Samenwerking bij verbeteringen kan mogelijk plaatsvinden door concreet ondersteuning te bieden bij het bewerkstelligen van samenwerkingen tussen ketenpartners, waarbij oplossingen worden aangedragen op het vlak van cybersecurity vraagstukken. Hiermee wordt cyber security versterkt en wordt samenwerking bewerkstelligd.

2c. Concrete vraagstukken

HSD onderzoekt of er concrete vraagstukken (digitale veiligheidsvraagstukken over bijvoorbeeld compliance, crisispreparatie of technologie) zijn voor marktconsultaties. Kennis delen is ontzettend belangrijk. Dat is een van de redenen waarom HSD aangesloten wil zijn en daar actief aan wil bijdragen, zodat de digitale veiligheid in Nederland op een hoger niveau komt te liggen.
De bedrijven in dit onderzoek is gevraagd of er concrete vraagstukken zijn die voorgelegd kunnen worden aan HSD en haar partners. In bijlage 8 staan enkele in de interviews genoemde vraagstukken die potentieel tot een marktconsultancies kunnen leiden.

Kleinere bedrijven zien te weinig meerwaarde bij assistentie om concrete vraagstukken te beantwoorden, of zagen op dit moment, of in de huidige fase van bedrijfsontwikkeling, geen concrete vraagstukken die van voldoende groot formaat of complexiteit werden ingedacht voor de aangeboden marktconsultatie. Bij bedrijven zonder eigen cyber-experts in huis, kan je verwachten dat vraagstukken over bijvoorbeeld crisismanagement, het opstellen van een bedrijfscontinuïteitsplan of een crisisscenario evenwel reëel aanwezig zullen zijn. In de praktijk blijken de bedrijven bij dergelijke voorkomende vragen vooral hun externe ICT bedrijf of de consultants van de verzekering te consulteren voor het verbeteren van de cyberweerbaarheid.

Vraagstukken bij bedrijven ontstaan wellicht bij een concreet aanbod, waarbij maatregelen getroffen worden om de weerbaarheid op een hoger niveau te brengen, waarbij het bedrijf ondersteund wordt bij:

- Systematisch roadmap om organisatie en beleid op een volwassen niveau te brengen, inclusief de naast technische maatregelen.
- Proofs of Concepts voor cyber-startups.
- Standaard procedures en *Best Practices.*
- Uitleg bij de betekenis van bepaalde termen in de maturity-tabel.
- Het besef dat cybersecurity een terugkerend proces is, dat vast ingebed moet worden in de processen van de organisatie.
- Risicoscans, -analyses en trainingen.
- Subsidies en andere R&D-middelen.
- Infrastructurele afwegingen, zoals de keuze in huis of extern implementeren.
- Het beoordelen van leveranciers (certificering).

Wellicht zullen door het aanbieden van sessies over dergelijke onderwerpen concrete vraagstukken ontstaan waarbij de vraag naar marktconsultaties kan ontstaan. Ook het aanbieden van scans (zoals pentests) kan vraagstukken voortbrengen bij aangetoonde tekortkomingen van de beveiliging.

De grotere bedrijven, die zelf cybersecurity in het beleid van de organisatie ingebed hebben en budget, tijd en personeel alloceren, lossen zelf voorkomende vraagstukken op. Zij hebben een professioneel proces waarbij de organisatie continue bewaakt wordt en passende maatregelen worden getroffen.
In dit onderzoek is ook gesproken met een bedrijf dat zélf ook vraagstukken voor bedrijven beantwoordt en zodoende een gelijksoortige dienst als HSD lijkt aan te bieden.

3. Conclusies en aanbevelingen

In bijlage 6 is het volwassenheidsniveau van weerbaarheid van de bedrijven in een tabel opgenomen.
In bijlage 5 staan de uitkomsten samengevat van de reacties bij de interviews over de bekendheid van de organisatie met HSD en de reacties op het initiatief voor een CyberWeerbaarheidscentrum.

Cyberweerbaarheid volwassenheidsniveau

Geen van de bedrijven had, om risico's te voorkomen, cybersecurity als *doel* in het bedrijfsbeleid. En geen van de bedrijven hanteert het als *uithangbord* met positieve uitstraling, zoals de provincie dat voorziet ('*wij bieden en zorgen voor een veilig product en dienst volgens een veilig proces'*) om aldus voordeel te behalen uit een beter imago of mogelijk voorkeur te genieten bij aanbestedingen, offertes en het verkoopproces.

Alle bedrijven zijn zich bewust van de ontwikkelingen en de risico's van cybersecurity en nemen het onderwerp Cybersecurity serieus, ondanks dat het aantal genoemde incidenten waarbij de bedrijven in de sector concreet ervaring hadden met cyberaanvallen, relatief laag is. De sectorcultuur, waarbij vaak certificeringen binnen de keten benodigd zijn op bijvoorbeeld het gebied van veiligheid en de privacywetgeving dragen bij aan de grote *awareness*.
Alle bedrijven hanteren een basale vorm van veiligheidsmaatregelen en zijn in dit onderzoek bijna alle gewaardeerd met een volwassenheidsniveau 2 of hoger (bijlage 6). Enkele bedrijven van voldoende groot formaat, of die een cyberexpert in huis hebben, kennen een hoger volwassenheidsniveau.
Met name de kleinere bedrijven of de bedrijven die zich (nog) in een vroeg stadium van de bedrijfsontwikkelingsfase bevinden, scoorden lager en kunnen ondersteuning gebruiken bij de groei in het volwassenheidsniveau. Bij die bedrijven ontbreekt het vaak aan tijd of geld om op continue basis de benodigde aandacht te besteden aan cybersecurity en bij deze bedrijven vormt cyberveiligheid geen vast onderdeel van het bedrijfsbeleid.

Het nut wordt erkend van een vorm van certificering in maturity van cyberweerbaarheid om leveranciers, klanten en het bedrijf zelf goed te kunnen kwalificeren. Het strekt tot aanbeveling bedrijven concreet handvatten te bieden om te groeien in de maturity-tabel en om instrumenten aan te reiken, dit continue en regelmatig te monitoren en waar mogelijk actie op te ondernemen.

Binnen de sector is verbetering van het volwassenheidsniveau en versterking van de weerbaarheid mogelijk. Ook bedrijven met een hoog maturityniveau zullen blijvend aandacht moeten houden op security en bedrijfsprocessen steeds, waar nodig aan moeten passen.
Ondersteuning in tijd(mankracht), met financiële middelen of door het aanbieden van praktische handvatten om professioneel en beleidsmatig invulling te geven, lijkt hierbij de sleutel. Er is *awareness*, maar de focus ligt bij sommige bedrijven te weinig op het *continue* vergroten of verbeteren van het cybersecurityniveau.

Het aanbieden van betaalbare *cyberscans* (zoals pentests) door externe partijen zou een probaat middel kunnen zijn. Dit aanbod met scans kan dan, in combinatie met het tonen van tekortkomingen

in de beveiliging en het aanbieden van effectieve maatregelen, mogelijk een passende drijvende kracht zijn ter ondersteuning, om op deze wijze volwassener en weerbaarder te worden. Een dergelijk proactief aanbod is er niet (of is niet bekend) vanuit bijvoorbeeld het DTC of andere initiatieven.

Ook kan het invoeren van een cybercertificaat gekoppeld aan een periodieke controle een goed middel zijn om de aandacht van bedrijven regelmatig gericht te sturen op cybersecurity. Een certificaat kan ook een voordeel zijn ten behoeve van kwalificaties bij onderling handelen met ketenpartners binnen de sector en kan het imago positief versterken.
Een certificering (vergelijkbaar met het CYRA-certificaat in bijlage 2) wordt door de bedrijven, zolang het administratief en financieel niet teveel bezwarend is, omarmt (met name door de bedrijven van beperkte omvang - voor de grotere bedrijven met internationale klanten, zijn dergelijke certificaten een goede indicatie maar van minder belang). Bedrijven wijzen daarbij op de wens om voor certificering financieel gesteund te worden (bijvoorbeeld met vouchers).

Bij het programma om de cyberweerbaarheid van bedrijven te vergroten is het raadzaam om de ICT bedrijven, die als externe partij zijn aangetrokken voor ICT-diensten en -beheer, nauw te betrekken. Daarbij is een service waarbij gecontroleerd wordt op afwijkingen in (het gebruik van) data over internet aan te bevelen.

Samenwerken

De voordelen van kennis en informatie delen binnen de sector en gezamenlijk optrekken om elkaar weerbaarder te maken wordt door alle bedrijven omarmt. De bedrijven die een hoog volwassenheidsniveau kennen en cyberkennis in huis hebben, lijken meer bereid te participeren, maar bedrijven zijn terughoudend wat betreft *actieve* participatie bij een op te richten CyberWeerbaarheidscentrum (CWC).

De bedrijven zien niet direct of niet voldoende meerwaarde voor hen (*'kennis brengen'*). Wel is men enthousiast in passieve participatie (*'informatie halen'*), maar tijd en geld zijn ook hier zeker factoren die overwogen worden. Wellicht evident, gezien het feit dat cyberweerbaarheid niet in het beleid is ingebed en er in de huidige situatie ook geen tijd en geld geïnvesteerd wordt voor een structurele volwassen aanpak van weerbaarheid.

Hoewel de bedrijven zien dat een sterke weerbaarheid goed is voor elk bedrijf binnen de sector afzonderlijk, lijken de bedrijven niet zodanig afhankelijkheid van andere bedrijven in de sector, dat een zwakke schakel in de keten negatieve invloed heeft op andere bedrijven in de sector. Een gezamenlijk aanpak om de keten als geheel te versterken lijkt daarom niet de juiste aanpak.

Er wordt gewerkt met ISO-certificeringen op het gebied van veiligheid of voor aan partners gestelde voorwaarden en eisen waaraan klanten of leveranciers dienen te voldoen, waarbinnen cybersecurity is opgenomen. Zo bezien wordt de keten in de sector versterkt door de verbindingen tussen de schakels onderling te regelen. In dat geval zou het concreet, afzonderlijk ondersteunen van bedrijven bij het (gaan) voldoen aan door ketenpartners gestelde eisen, passen binnen de huidige cultuur van samenwerken binnen de sector, wat mogelijk leidt tot concrete samenwerkingen. Samenwerkingen die dan ook kunnen bestaan uit schakels in de keten die andere schakels vooruit helpen.

De bedrijven die hulp kunnen gebruiken wensen een cyber weerbaarheids-informatiepunt waar handvatten te verkrijgen zijn om te groeien in de maturity-tabel. Hiervoor kan wellicht beter samenwerking gezocht worden met andere initiatiefnemers.

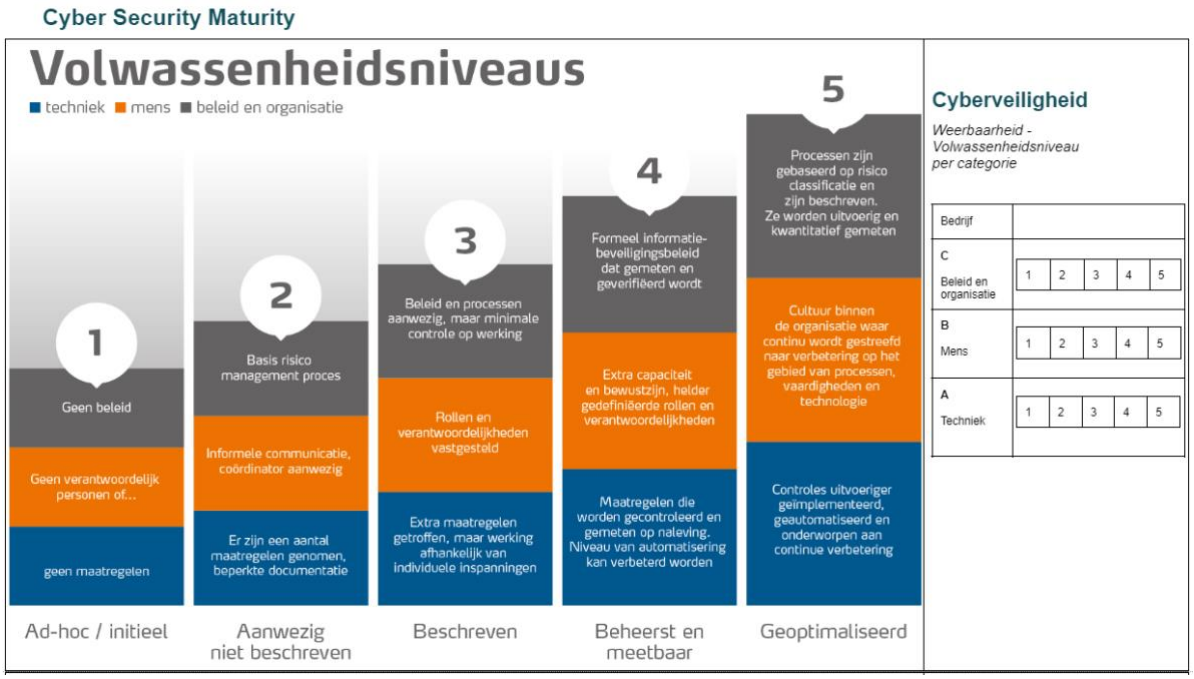
Concrete vraagstukken

Ruim de helft van de bedrijven in dit onderzoek is bekend met Security Delta. Enkele konden een concreet vraagstuk beschrijven. Die beschrijvingen zijn opgenomen in bijlage 8. De meeste hadden (nog) geen behoefte aan een oplossing die geleverd wordt met hulp van partners van HSD bij een complex vraagstuk. Cybervraagstukken worden of zelf opgelost bij bedrijven met cyberexpertise in huis of voorgelegd aan de externe systeembeheerder. Bij het ontbreken van een strategisch plan richting volwassen cyberweerbaarheid, komen dergelijke vraagstukken waarschijnlijk ook niet op.

HSD zou een schets of onderdelen van een dergelijk strategisch plan kunnen voorleggen aan bedrijven. Een dergelijk richtinggevend aanbod en resultaten uit de eerder genoemde aan te bieden scans kunnen ook een opstap zijn naar concrete vraagstukken uit de markt.
In bijlage 8 staan enkele in de interviews genoemde vraagstukken die potentieel tot marktconsultancies kunnen leiden.

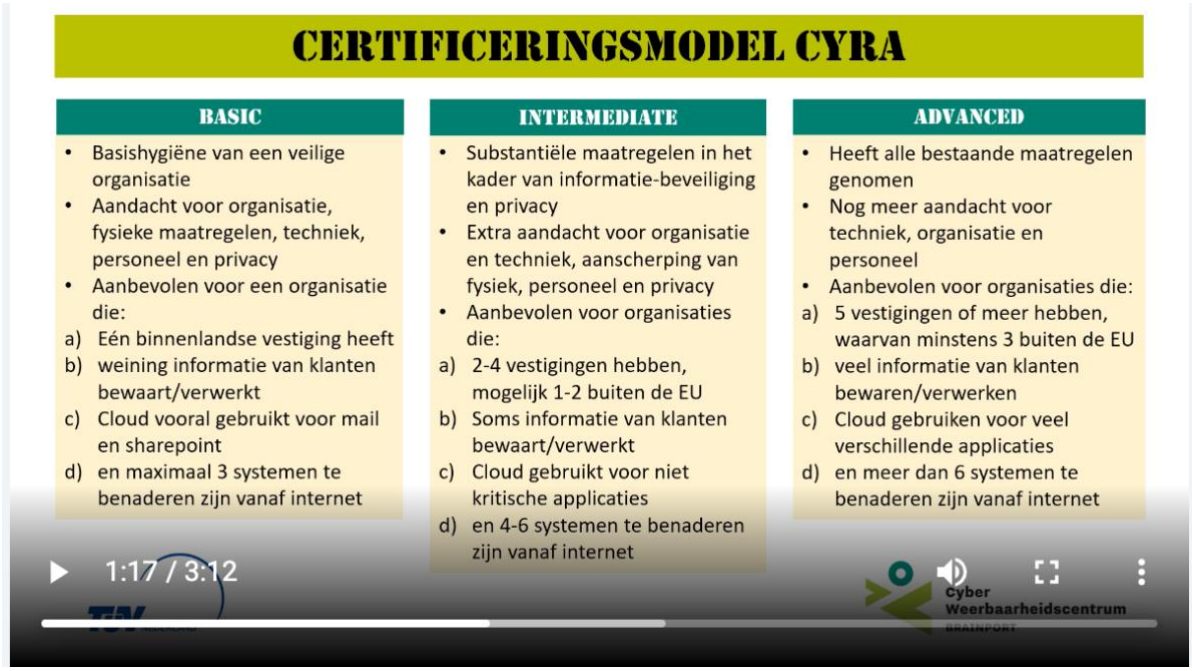
Bijlagen

Bijlage 1: Cyber Security Maturity



Note: Deze tabel is aangepast voor gebruik bij dit onderzoek, omdat dit bij sommige organisaties tot vragen leidde. Bij Techniek, niveau 1 staat in de oorspronkelijke tabel: “Ondanks problemen, geen maatregelen”. [Bron: 4]

Bijlage 2: CYRA certificaat

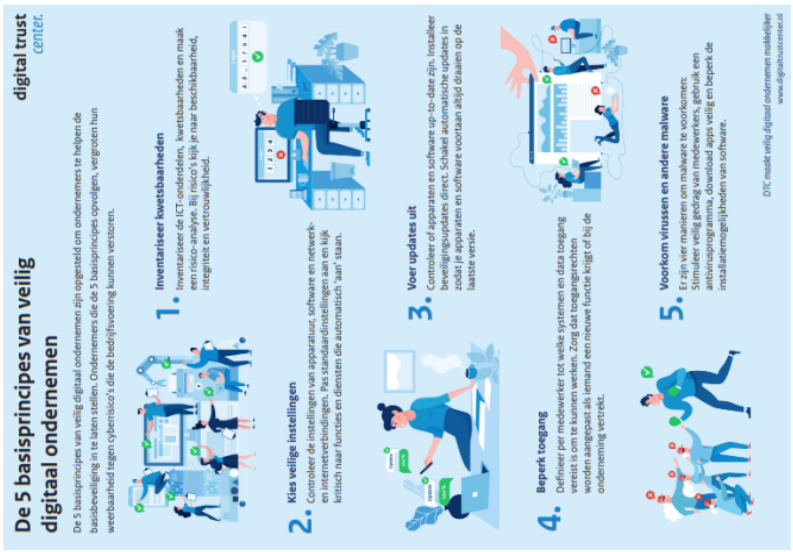


Bijlage 3: Aandachtspunten cyberweerbaarheid

1. Is het bedrijf zelf slachtoffer geworden van CyberCrime
2. Wel eens mislukte pogingen ervaren
3. Wordt er gebruik gemaakt van back-ups
4. Virusscanners
5. Software up-to-date
6. Firewalls
7. Bedrijfssoftware
8. Autorisatieschema
9. Monitoring/logging
10. Encryptie
11. Biometrische
12. E-mail openen
13. Omgaan met vertrouwelijke gegevens
14. Wijzigen wachtwoorden
15. Sterke wachtwoorden
16. Bewust online risico's
17. Bewust en regels online betalingen
18. Gevoelige informatie op internet verstrekken
19. Veiligheidsaudits
20. Informatieveiligheidsbeleid
21. Afgeven bedrijfsgegevens
22. Omgaan met onbekende bestanden
23. Schriftelijke weergave ICT Infrastructuur
24. ICT privé- en thuisgebruik
25. Protocollen hoe te handelen bij aanval

[Bron: 2]

Bijlage 4: Kamer van Koophandel – Goodiebag



[Bron 5]

Bijlage 5: Bedrijvenoverzicht

Bedrijf	HSD	Concreet vraagstuk	RCWC nuttig	Actieve participatie RCWC
1.	Onbekend	Nee	Ja	Ja
2.	Bekend	Nee, in toekomst wel verwacht	Ja	Nee
3.	Onbekend	Ja	Ja	(Ja)
4.	Bekend	Ja	-	(Nee)
5.	Bekend	Nee	Ja	Nee
6.	Onbekend	Nee	Ja	(Ja)
7.	Onbekend	(Ja)	Ja	Nee
8.	Bekend	Nee	Ja	Nee
9.	Onbekend	Nee	Ja	(Ja)
10.	Bekend	Ja	(Ja)	Nee
11.	Bekend	Nee	Ja	Ja*
12.	Onbekend	(Ja)	Ja	Nee
13.	Bekend	Nee	Ja	Ja
14.	Bekend	Nee	Ja	(Ja)
15.	Bekend	Nee	Ja	Nee

RCWC = Op te richten Regionaal Cyber WeerbaarheidsCentrum. (zie Bijlage 7)

* = interesse voor initiële gesprek ten behoeve van de oprichting, actieve participatie daarna onzeker

Bijlage 6: Maturity-normering

Bedrijf	Techniek	Mens	Beleid & organisatie
1.	5	5	5
2.	2	2	2
3.	2	2	1
4.	3	4	3
5.	4	3	3-4
6.	5	4	3
7.	2	2	2
8.	5	5	5
9.	2	3	3
10.	2	2	2
11.	4	5	4
12.	3	3	3
13.	3	5	4
14.	5	5	5
15.	2	2	2

Waardering van de bedrijven volgens de Maturity-tabel (bijlage 1).

Bijlage 7: Regionaal Cyberweerbaarheidscentrum (CWC)

Context

Cyberincidenten zijn aan de orde van de dag en door toenemende digitalisering krijgen steeds meer ondernemers te maken met incidenten. De cyberrisico's voor ondernemers zijn divers en lopen uiteen van het betalen van losgeld om weer toegang te krijgen tot het eigen bedrijfsnetwerk, tot de uitval van faciliteiten waardoor de continuïteit van de onderneming in gevaar komt.
Omdat door het internet alles met iedereen is verbonden wordt het belang van goede cybersecurity ook een gezamenlijk vraagstuk, waarbij de keten zo sterk is als de zwakste schakel. Door een cyberweerbaarheidscentrum op te richten, eenvoudig gezegd een vorm van samenwerking van een groep bedrijven, kan de keten in gezamenlijkheid werk maken van cybersecurity en zaken goed op elkaar afstemmen. Samenwerken en het bieden van handelingsperspectief voor de sector rondom cybervraagstukken staan hierin centraal.

Randvoorwaarden en stappen

Er zijn veel mogelijkheden om samen te werken aan cybersecurity, maar om te spreken van een Cyberweerbaarheidscentrum zijn een aantal randvoorwaarden te onderscheiden die hier in ieder geval onderdeel van uitmaken.

1. Er is sprake van een sector: eenzelfde soort bedrijven met een overeenkomstig economische en/ of maatschappelijk belang, een afhankelijkheid en een wil om samen te werken;
2. Er is een hoge mate van digitalisering en er wordt veelvuldig gebruik gemaakt van datasets;
3. Er is besef van de risico's op de digitale infrastructuur (netwerk, mobiel, datacenters) en er wordt actief gewerkt aan een digitaal veilige omgeving;
4. Er zijn plannen (in voorbereiding) voor de aanpak van cyberincidenten en of continuïteit;
5. Cyberveiligheid is een onderwerp in de 'boardroom' en de kwetsbaarheid hierop worden erkent. Een CWC is een 'coalition of the willing';
6. Er is een verbinding vanuit de sector naar het DTC en de landelijke structuur van het NCC;
7. Een CWC is vrijwillig, maar zeker niet vrijblijvend ;
8. Een CWC is een ecosysteem waarbij iedereen iets brengt en iets haalt en zo samen bestaat;
9. Een CWC heeft het doel om binnen 3 jaar zelfstandig te opereren;
10. Een CWC heeft tot doel om bij dreiging of incident samen te werken en kennis en kunde te delen om zo beter voorbereid te zijn op cyberincidenten en beter en adequater te kunnen acteren in geval van een cyberincidenten.

Wat is een CWC?

Een Cyberweerbaarheidscentrum (CWC) is een expertisecentrum en informatieknooppunt rond cybersecurity-vraagstukken. Door samen te werken met bedrijven en organisaties die een belangrijke plek hebben in de ketenregie, kennisinstellingen, overheden en cybersecurity-dienstverleners. Ofwel: de kracht van het collectief. De voornaamste functies van het cyberweerbaarheidscentrum hebben betrekking op:

1. Opstarten van specifiek programma's rondom bewustwording waardoor gedragsverandering van ondernemers en CeO's, managers en medewerkers plaatsvindt.
2. De meeste cyberincidenten worden door menselijk handelen veroorzaakt;
3. Opstellen en delen van beveiligingsadvies ten aanzien van kwetsbaarheden in hardware en software;
4. Faciliteren van expert-overleggen voor kennisdeling en netwerking speciaal voor deze sector;
5. Oprichten van een digitaal loket voor raad, advies en slachtofferhulp. Een Centrum waar ondernemers terecht kunnen voor digitale opvang om te voorkomen dat ze slachtoffer

worden van een cyberincident of te helpen wanneer ze slachtoffer zijn geworden: detectie, preventie en respons.

6. Tevens een centrum waar men kan leren van elkaars fouten met speciale aandacht voor de kenmerken van deze sector.
7. Het verstrekken van relevante en duidelijke (dreigings)informatie op strategisch, tactisch en operationeel niveau over actuele cyberdreigingen die van toepassing zijn op de bedrijven werkzaam in deze sector. Hierbij maakt het cyberweerbaarheidscentrum onder andere gebruik van informatie van de overheid (de zogenaamde OKTT status bij het NCSC om dreigingsinformatie te kunnen ontvangen);
8. Waar gewenst, het gezamenlijk inkopen van cybersecurity-dienstverlening in de markt (zoals ondersteuning van onder andere security monitoring via shared service inkoop) waarbij specifieke kennis van de sector essentieel is.

Bijlage 8: Concrete vraagstukken

Bedrijf	Vraagstuk
3	Graag zien zij een soort Cyber Security-certificering die alle bedrijven moeten bezitten, waartoe een programma moet worden opgezet om te bewerkstelligen dat bedrijven een dergelijk certificaat kunnen behalen en behouden (opleiding, checklist en regelmatige monitoring). Concreet is er een vraagstuk of er bedrijven op dit vlak ervaring hebben of kunnen assisteren bij het opzetten van een dergelijk Cyber Security certificeringstraject, waarbij aandacht komt op het gebied van data awareness, data security en privacy.
4	Met de pandemische periode is het bedrijf meer gebruik gaan maken van thuiswerken. Daar opent zich een mogelijk veiligheidsrisico, omdat de infrastructuren niet in eigen beheer zijn. Wenselijk zou zijn als daar een scan of certificering op mogelijk zou zijn. Dit vraagstuk wordt voorgelegd aan de eigen ICT beheerder, maar is wellicht ook een concrete vraag die aan HSD voorgelegd kan worden. Voor bedrijven in de keten (klant/leverancier) zou een standaard cyberweerbaarheid certificering moeten komen zoals met de AVG voor verenigingen die zij hanteren om de weerbaarheid van bedrijven te graderen. Is een dergelijk traject actief in ontwikkeling?
7	Wel is er de vraag bij de *maturity-tabel* of er ook een roadmap is waaruit is te lezen welke aanpassingen nodig zijn om op een volgend, hoger niveau te komen. Dat vraagstuk is er feitelijk ook bij een algemene veiligheidscertificering die klanten zouden kunnen gaan stellen in de toekomst. Een roadmap naar het volgende niveau zou een praktische leidraad voor de groei van de organisatie zijn.
10	Een oplossing (monitor of scan) om inzicht te krijgen in de type digitale aanvallen die plaatsvinden en de intensiteit ervan zou een concreet vraagstuk kunnen zijn.
12	Geen concreet vraagstuk maar zijn wel geïnteresseerd in oplossingen die hen verder helpt: Zijn er vouchers of subsidie waarmee zij de maturity van het bedrijf naar een volgend level kunnen tillen en is daar een roadmap voor?

Bronnen

1. Economic Board Zuid-Holland, Roadmap verbeteren weerbaarheid ZH
   Koen Gijsbers, Cyber4Board, Oktober 2020

2. Veiligheidsonderzoek en nulmeting cybersecurity in de Rotterdamse Haven
   Documentatie HSD, Nieuwsbericht 24 oktober 2019

3. Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Justitie en Veiligheid. Overzicht vitale processen | Vitale infrastructuur | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl). https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

4. Routekaart van Threadstone
   https://www.threadstone.eu/routekaart, 2022

5. Kamer van koophandel, Meetups
   Goodiebag-Cybersecurity_tcm109-459983.pdf (kvk.nl), 2022

HSD
securitydelta.nl

Security Delta (HSD)
Wilhelmina van Pruisenweg 104
2595 AN The Hague
070 204 41 80

info@securitydelta.nl
www.securitydelta.nl
@HSD_NL