Sterke schakels versterken de keten

Een ontwerponderzoek naar samenwerking in de keten tussen high tech MKBs op gebied van cybersecurity

Lectoraat Digitalisering en Veiligheid
Ben Kokkeler
Steven van den Oord
Esger ten Thij
Quinn Vollenberg

Mei 2023

Samenvatting

In dit praktijkonderzoek onderzoeken we op welke manier waardeketens ondersteund kunnen worden om de informatiebeveiliging van het innovatief ecosysteem Brainport Eindhoven te verbeteren. Naast literatuuronderzoek is praktijkonderzoek gedaan op basis van een serie interventies bij 16 bedrijven. Via een validatieworkshop samen met de deelnemende bedrijven en een ontwerpworkshop met bedrijven en experts van veiligheidsorganisaties zijn condities en kenmerken voor samenwerking, in het bijzonder voor shared functies cyberexpert en CISO, geformuleerd.
De algehele conclusie is dat er goede kansen zijn voor samenwerking, dat er de noodzaak is omwille van de efficiency en de leerfunctie voor ondernemers, en dat het verkennen van publiek-private samenwerking in schaalbare vervolgpilots gewenst is.

Het onderzoek werd uitgevoerd in samenwerking tussen het Cyber Weerbaarheidscentrum Brainport, het Regiobureau Integrale Veiligheid Oost-Brabant, en het Avans lectoraat Digitalisering en Veiligheid, met medewerking van ASML en Cyber4Z, en werd gesubsidieerd door het CCV Programma Lokale Cyberweerbaarheid en het Digital Trust Centre (DTC).

Inhoudsopgave

2 Introductie

Wereldwijd zien we steeds meer organisaties die zoeken naar meer structurele beveiliging tegen cyberaanvallen. Zij zoeken niet alleen slimme oplossingen voor de eigen organisatie, maar ook innovatie manieren om veilig samen te werken. Het is noodzakelijk aan andere organisatie- en samenwerkingsmodellen te werken die samenwerking tussen organisaties centraal stellen en meerwaarde daarvoor bieden.
Dit ontwerponderzoek is gericht op beleidsmakers, bestuurders en directies van organisaties in het innovatief ecosysteem Brainport Eindhoven. Het rapport biedt inzicht in praktische aspecten van cybersecurity in ketens van MKB, mede gebaseerd op een pilot samen met 16 bedrijven. De conclusies en aanbevelingen zijn gericht op de creatie van shared cyberexpertise functies en CISO-functies, als onderdeel van een door het lectoraat Digitalisering en Veiligheid ontwikkeld ontwerp van digitaal veilige organisatienetwerken, gevalideerd met experts uit het innovatief ecosysteem Brainport Eindhoven.
Naar verwachting zijn de conclusies en aanbevelingen ook relevant voor andere regio's die in ketens en clusters willen samenwerken aan cybersecurity.

2.1 Het innovatie ecosysteem Brainport

In dit praktijkonderzoek onderzoeken we op welke manier waardeketens ondersteund kunnen worden om de weerbaarheid van het innovatief ecosysteem Brainport Eindhoven te verbeteren. We voeren een pilotonderzoek uit met als doel de praktische haalbaarheid van ketenbeveiliging in het ecosysteem te evalueren. Op basis van de onderzoeksresultaten kan nagegaan worden welke manier van ketenbeveiliging een geschikt initiatief is om de weerbaarheid van het innovatief ecosysteem Brainport Eindhoven te verbeteren.

Brainport Eindhoven is een innovatief ecosysteem in Zuidoost-Brabant. Met een sterke high tech maakindustrie, een bijzondere designsector en een uniek samenwerkingsmodel. De kennisintensieve maakindustrie kenmerkt zich door productie in kleine volumes van technisch complexe producten. Daarnaast is er een levendige creatieve industrie met volop ruimte voor innovatieve startups (Brainport Eindhoven, z.d.).

Binnen dit ecosysteem neemt ASML als high techbedrijf een belangrijk rol in. ASML maakt lithografiesystemen: ingewikkelde machines die door andere bedrijven gebruikt worden om hun computerchips te produceren. Uiteindelijk belanden deze chips in smartphones en computers, maar ook in auto's, vliegtuigen en huishoudelijke apparaten die dagelijks worden gebruikt door mensen overal ter wereld.

Om snellere, betere en goedkopere chips te produceren, vernieuwt ASML steeds haar machines door middel van open innovatie: "het combineren van bronnen en middelen van verschillende organisaties binnen en buiten het ecosysteem voor zowel de ontwikkeling als het op de markt brengen van nieuwe technologieën, producten en diensten (Chesbrough, 2003)." Open innovatie brengt voordelen met zich mee omdat een organisatie niet alle kennis en middelen in huis heeft om onderzoek en ontwikkeling in een of meerdere waardeketens te organiseren.

ASML ontwikkelt complexe machines met meer dan 180.000 elementen van allerlei verschillende leveranciers (NCSC Magazine, 2020). Deze samenhangende activiteiten zijn gebaseerd op onderlinge samenwerkingsverbanden tussen (maak)bedrijven, toeleveranciers, kennisinstellingen, opleiders, overheden, en andere organisaties die in verschillende

organisatienetwerken binnen het ecosysteem van Brainport Eindhoven informatie delen, kennis uitwisselen en andere activiteiten uitvoeren om meerwaarde te creëren. Dit brengt echter ook risico's met zich mee zoals datalekken, cyberaanvallen, bedrijfs- of industriële spionage, en bedreigingen van open, vrije samenwerking. Cyberaanvallen bijvoorbeeld via gijzelsoftware vaak in combinatie met afpersing kan grote gevolgen hebben voor de getroffen organisatie, maar ook voor haar klanten, leveranciers of partners. Een ander voorbeeld is dat (gedeelde) clouddiensten worden overgenomen waardoor diensten kunnen worden misbruikt. De impact is dat cruciale bedrijfsprocessen kunnen uitvallen of worden verstoord met grootschalige gevolgen voor de getroffen organisaties en het ecosysteem waarin de organisatie is ingebed. Bijgevolg is de weerbaarheid – het vermogen om weerstand te bieden tegen bekende en onbekende vormen van dreigingen – een gedeeld belang van het gehele ecosysteem.

Het strategisch doel van bedrijven is vervolgens het voorkomen en verminderen van kwetsbaarheden binnen het ecosysteem van Brainport Eindhoven. Een ecosysteem is een gemeenschap van onderlinge afhankelijke organisaties die relaties onderhouden met als streven om meerwaarde te leveren aan klanten (Moore, 1997). Binnen het ecosysteem wordt continu in veranderende organisatienetwerken de krachten van organisaties gebundeld om producten of diensten te ontwikkelen en aan te bieden op de markt. Organisatienetwerken zijn groepen van organisaties die in wisselende samenstelling met elkaar samenwerken om een doel te bereiken dat afzonderlijk
Dit gebeurt zowel in samenwerking als concurrentie in waardeketens. Op basis van aaneenschakeling van meerdere handelingen of gebeurtenissen komen organisaties tot op elkaar afgestemde economische activiteiten, die uiteindelijk een product of dienst opleveren.

2.2 Beoogde resultaten van het onderzoek

De overall beoogde resultaten van het project waren praktisch georiënteerd. De ambitie was het betrekken van vijftien - minstens tien - bedrijven bij de pilot (een serie gerichte cyberweerbaarheidsinterventies) en het vergroten van hun cyberveiligheid. Binnen dit praktijkgerichte kader was de opdracht voor het Avans onderzoeksteam om een aantal zaken op te leveren in de vorm van een onderzoekrapport.

- Bevindingen en conclusies over de effectiviteit van hands-on ondersteuning en inzet van een shared cyberprofessional, zoals deze in de pilot heeft plaatsgevonden.
- Aanbevelingen over de mogelijkheden voor samenwerking in ketens en netwerken van bedrijven, daarbij de inzet van shared cyberprofessionals en shared CISO's.

Dit praktijkonderzoek moest op basis van deze resultaten op twee manieren bijdragen aan het versterken van de weerbaarheid van het high tech ecosysteem Brainport Eindhoven. De eerste bijdrage is het delen van geleerde lessen over hoe grote spelers kleinere toeleveranciers kan ondersteunen in het versterken van de ketenbeveiliging. De tweede bijdrage is het schetsen van handelingsperspectieven over hoe de weerbaarheid van het ecosysteem kan worden versterkt.

2.3 De organisatie van het onderzoek

Het onderzoek werd uitgevoerd in samenwerking tussen het Cyber Weerbaarheidscentrum Brainport, het Regiobureau Integrale Veiligheid Oost-Brabant en het Avans lectoraat

Digitalisering en Veiligheid, met medewerking van ASML en Cyber4Z, en werd gesubsidieerd door het CCV Programma Lokale Cyberweerbaarheid.

3 Methoden van onderzoek

Voor dit onderzoek is ervoor gekozen om gebruik te maken van een samenhangend pakket van kwalitatieve methoden die passen bij de aard van het ontwerponderzoek.

3.1 Literatuuronderzoek

Er is begonnen met het uitvoeren van een literatuuronderzoek middels Google Scholar om te bepalen wat er de afgelopen jaren is gepubliceerd op het gebied van supply chain in combinatie met cyber security, security, hacking, tools, threaths en framework. De resultaten die hieruit zijn voortgekomen zijn een voor een geanalyseerd en hieruit is een set bronnen voortgekomen die hebben geleid tot een aantal use cases. Deze use cases zijn specifiek gericht op cyberincidenten in de supply chain van de afgelopen vijf jaar.
Daarnaast is er een literatuuronderzoek uitgevoerd naar waarde creatie in de high tech maakindustrie.

3.2 Semigestructureerde interviews

Om te bepalen hoe bedrijven omgaan met cyberincidenten zijn er verdiepende interviews uitgevoerd met vier van de zestien bedrijven die deelnamen aan de pilot. De interviews zijn online afgenomen met behulp van een topic-lijst die mede op basis van de literatuur review werd opgesteld. De topic-lijst focuste zich op de volgende onderwerpen: risicobepaling, veiligheid en het rapporteren van incidenten, kritische organisaties waarmee u samenwerkt en communicatie. Naast het maken van aantekeningen tijdens de interviews zijn deze ook opgenomen. Naderhand zijn deze uitgewerkt en zijn de beide aantekeningen met elkaar vergeleken om zo tot een eenduidig verhaal te komen.

3.3 Ontwerp- en validatieworkshop

Ter afronding van dit onderzoek, is er een ontwerp- en validatieworkshop gehouden om met de deelnemers van de pilot en externe partners te kijken naar de resultaten en te bepalen wat vervolgstappen kunnen zijn. De opgehaalde inzichten zijn verwerkt in de conclusies en aanbevelingen.

3.4 Interventies in bedrijven

Gedurende de pilot en het onderzoek heeft het bedrijf Cyber4Z interventies uitgevoerd bij de deelnemende bedrijven binnen de pilot. Zij hebben de bedrijven eerst een vragenlijst toegestuurd om te bepalen hoe de situatie eruitziet. In overleg met de bedrijven is vervolgens gekeken naar interventies om te bepalen waar nog mogelijkheden waren. Elk bedrijf heeft tien uur toegewezen gekregen om deze inventarisatie mogelijk te maken en succes te laten hebben. De aanpak en tussentijdse inzichten uit de interventies zijn in online overleggen tussen consultants van Cyber4Z en de Avans onderzoekers gedeeld.

4 Conceptualisering – de literatuur over cybersecurity in ketensamenwerking

Een uitgebreide literatuurstudie is voor dit onderzoek niet uitgevoerd. Enerzijds omdat de scope van het onderzoek primair gericht was op het aansluiten bij en kritisch analyseren van de gerichte cyberweerbaarheidsinterventies onder 16 – primair high tech - bedrijven. Anderzijds omdat de empirische literatuur over cyberweerbaarheid in ketens en netwerken van (high tech) Mkb's nog redelijk beperkt is. Er is daarom gekozen voor een gerichte studie rond een vijftal concepten.

Op basis van literatuur over samenwerking in de high tech maakindustrie schetsen wij de specifieke kenmerken van het ecosysteem waarin de resultaten en opvolging van een pilot als 'sterke schakels versterken de keten' zou kunnen landen.
Vervolgens schetsen wij de risico's en impact van cyberaanvallen.
De literatuur over organisatienetwerken is behulpzaam bij de concretisering van ketensamenwerking. Allereerst voor samenwerking in lerende netwerken, of zelfs van pps-netwerken waarin bedrijven en publieke organisaties gezamenlijk werken aan het vergroten van cybersecurity. Deze lerende (pps)netwerken zijn belangrijk voor het organiseren van een cyberveilig ecosysteem voor veilig ondernemen en innovatie.
Met behulp van literatuur over weerbaarheid en ketenbeveiliging bieden wij een volgende stap van concretisering van het voorbereid zijn op het hanteren van cyberrisico's in die lerende netwerken en ketens.
Tenslotte behandelen wij literatuur over crisis governance, met focus op de situatie waarin netwerken van bedrijven rond cybercrime zich bevinden, t.w. als een situatie van min of meer permanente crisis, waarbij de realiteit is dat niet alleen preventie, maar juist ook het herstel tijdens een crisis om tijdige aandacht vraagt.

4.1 Waardecreatie in de high tech maakindustrie

Het creëren van waarde in de high tech maakindustrie is een complex proces dat niet langer het traditionele lineaire waardecreatieproces volgt. Waar er vroeger sprake was van een waardecreatieproces waarbij het ene bedrijf aan het andere leverde, zien we nu dat verschillende bedrijven samenwerken om gezamenlijk een product of dienst te leveren.
Er ontstaan clusters in ecosystemen die ook spelers bevat buiten de traditionele waardeketens (Iansiti, M & Levien, R, 2004). Voor cybersecurity is relevant dat het bijvoorbeeld gaat om softwareleveranciers die productiebedrijven ondersteunen en daarmee een schakel worden in een netwerk van bedrijven met veelal horizontale relaties (Moore, 1997). Noties als 'industrie' en 'ketens' zijn daarmee minder van toepassing, en een notie als 'bedrijfsecosysteem' neemt in betekenis toe.

In een bedrijfsecosysteem kan een enkele entiteit invloed hebben op de prestaties van de gehele eenheid of keten. "In een bedrijfsecosysteem werken actoren samen en concurrerend om nieuwe producten te creëren, aan de behoeften van de klant te voldoen, en gezamenlijk capaciteiten rond innovatie te ontwikkelen (Moore, 1997)". Zeker in de high tech maakindustrie zien we dat veel bedrijven niet alleen afhankelijk zijn van elkaar maar ook – op innovaties - met elkaar concurreren of aan andere ecosystemen verbonden zijn, hetgeen extra kwetsbaarheden kan veroorzaken die niet volledig worden afgedekt door samenwerking in een keten. Mocht een van de bedrijven onverhoopt wegvallen door een cyberaanval dan kan dit grote gevolgen hebben voor de rest van de keten. Vanuit dit oogpunt kunnen

bedrijfsecosystemen dus worden gezien als complexe adaptieve systemen die relatief veel onafhankelijke onderdelen bevatten en in hoge mate onderling verbonden en interactief zijn (Brons, 2016).

4.2 Risico en impact van cyberaanvallen op ketens en netwerken van bedrijven

De statistieken over cyberaanvallen op supply chains zijn alarmerend. In 2018 alleen al zijn de aanvallen op ketens met 78% toegenomen en dat percentage blijft alleen maar stijgen (Symantec, 2019). Een 'software supply chain' aanval is te definiëren als een inbreuk uitgevoerd door hackers die software van derden beschadigen. Hierbij slaagt een kwaadwillende actor erin toegang te krijgen tot het systeem van een organisatie via malware die geïnstalleerd is op software van een externe leverancier. De malware wordt vervolgens verspreid onder alle geassocieerde actoren, zoals klanten, partners en leveranciers van de getroffen organisatie. De meest bekende hierbinnen is de cyberaanval op SolarWinds (Jeferson, Martinez & Javier M, Duran, 2021).

SolarWinds is een Amerikaans bedrijf dat software ontwerpt voor bedrijven om hun netwerken, systemen en infrastructuur voor informatietechnologie te helpen beheren. In december 2020 had SolarWinds ongeveer 300.000 klanten waaronder bijna alle Fortune 500-bedrijven en talrijke internationale agentschappen. De cyberaanval op de software supply chain, vond plaats gedurende een aantal maanden in 2020 en trof 18.000 klanten. APT29, alias Cozy Bear, werkzaam voor de Russische buitenlandse inlichtingendienst (SVR), zou achter de aanval van 2020 zitten (Nakashima & Timberg, 2020). Slachtoffers van deze aanval zijn onder meer; de cybersecurity firma FireEye, US Treasury Department, US Department of Homeland Security, NATO, European Parliament, UK Ministry of Defence, NHS en AstraZeneca. Microsoft president Brad Smith beschreef het als volgt: "Vanuit een software engineering perspectief, is het waarschijnlijk eerlijk om te zeggen dat dit de grootste en meest geavanceerde aanval is die de wereld ooit heeft gezien," (Cerules, 2021). De impact van dit soort aanvallen is vaak gigantisch evenals de bijkomende kosten om systemen te kunnen herstellen.

Over de mate van impact is op basis van de literatuur aan bedrijven nog weinig houvast te bieden. Veel grotere casussen die in de literatuur naar voren komen spelen zich af in het buitenland of in multinationals. Wel is er een groeiend aantal ondernemers die – nadat ze slachtoffer geworden zijn – naar buiten treden en hun verhaal houden. In kwalitatieve zin is het gangbaar om een risico-impact matrix te hanteren om een indruk te bieden van mogelijke impact. Zeer recent heeft TNO i.s.m. het NCSC een eerste handreiking uitgebracht om cyberrisico's te calculeren (NCSC, TNO; 2023).

4.3 Ecosysteem, netwerken en ketens

Om beter te begrijpen hoe ketens, netwerken en ecosystemen in elkaar steken en van elkaar afhankelijk zijn, is het van belang deze begrippen nader uit te leggen. Van een keten is sprake als er tussen verschillende organisaties (in een netwerk) een overeenkomst bestaat om gezamenlijk een product en/of dienst te leveren (Goedee & Entken, 2008). In de overeenkomst wordt beschreven welke organisatie wat doet in de keten en wie voor welk onderdeel verantwoordelijk is (Goedee & Entken, 2008).Op deze manier wordt duidelijk welke toegevoegde waarde deze organisatie in de totale keten realiseert (Goedee & Entken, 2008). Het grote verschil tussen een organisatienetwerk en een keten is dat het (samen)werken in

een keten niet vrijblijvend is, in tegenstelling tot het (samen)werken in een organisatienetwerk (Goedee & Entken, 2008).

We spreken van een netwerk als er sprake is van een begrensde groep van minimaal drie actoren tussen wie er bepaalde relaties zijn: meer of minder sterk, soms tijdelijk niet aanwezig. Een netwerk behelst het sociaal kapitaal van één persoon, groep of organisatie waarmee relaties worden onderhouden. Wanneer we spreken over sociale netwerken doelen we dan op familieleden, vrienden, kennissen, collega's of buren. Bij (inter)professionele netwerken kijken we naar het sociaal kapitaal (netwerken) van werknemers en de hulpbronnen die via dat netwerk gemobiliseerd kunnen worden. Organisatienetwerken daarentegen verbinden en delen informatie, middelen en competenties van soevereine en unieke organisaties om samen een resultaat te realiseren die geen van de organisaties afzonderlijk kan bereiken. Dit soort type netwerken zijn vaak formeel en organisaties kunnen op basis van verschillende relaties met elkaar verbonden zijn. Relaties tussen organisaties zijn vaak multilateraal en niet-hiërarchisch (Provan, Fish & Sydow, 2007). Dat wil zeggen dat er tussen organisaties geen relaties zijn op basis van een arbeidscontract zoals in een individuele organisatie (Gulati, Puranam & Tushman, 2012). Daardoor hebben organisaties die participeren in een organisatienetwerk een behoorlijke mate van operationele autonomie (Provan, Fish & Sydow, 2007) en maken ze gebruik van coördinatiemechanismen op basis van informele autoriteit.

Die informele autoriteit kan voor het creëren van clusters van bedrijven (en publieke partijen) die willen samenwerken aan cyberweerbaarheid van groot belang zijn. In een bedrijfsecosysteem "(…) ontwikkelen bedrijven hun capaciteiten en rollen, en hebben ze de neiging zich aan te passen aan de koers die door een of meer centrale bedrijven wordt uitgezet. De bedrijven die een leiderschapsrol vervullen, kunnen in de loop van de tijd veranderen, maar de functie van ecosysteemleider wordt door de gemeenschap gewaardeerd omdat het de leden in staat stelt naar gedeelde visies toe te werken, hun investeringen op elkaar af te stemmen en wederzijds ondersteunende rollen te vinden" (Brons, 2016).

4.4 Weerbaarheid, betrouwbaarheid en ketenbeveiliging

Voor het begrijpen van ketensamenwerking onder extreme omstandigheden – zoals grootschalige cyberattacks op bedrijven in een netwerk of keten – is de literatuur over High Reliability Organisations (HRO's) relevant. HRO's zijn technologisch complexe organisaties die werken in omgevingen met een hoog risico, waarin zelfs kleine storingen dramatische gevolgen kunnen hebben (b.v. kerncentrales, vliegdekschepen of chemische bedrijven). In dergelijke organisaties heeft het voorkomen van storingen de hoogste prioriteit en is betrouwbaarheid van de prestaties belangrijker dan productiviteit. Centrale noties in de HRO-literatuur zijn het ontwikkelen van competenties rond zowel anticiperend vermogen als rond het herstel na (grotere) incidenten. Het anticiperende vermogen betekent dat een bedrijf is uitgerust om onvoorziene tegenslagen het hoofd te bieden en klaar is om onverwachte kansen te benutten (Legnick-Hall & Beck, 2009). De veerkracht en weerbaarheid van organisaties ontwikkelt zich in de loop der tijd en komt voort uit het proces van omgaan met bedreigende situaties en onverwachte gebeurtenissen (Linnenluecke et al, 2012). Deze gebeurtenissen kunnen enerzijds voortkomen uit fysieke bedreigende situaties zoals een brand of overstromingen, maar ook uit digitale bedreigingen zoals een ransomware aanval, of een cyberaanval. De literatuur over business continuity management (Elliott et al, 1999) biedt inzichten in hoe organisaties zich kunnen voorbereiden op kritieke gebeurtenissen; bijvoorbeeld hoe organisaties geschikte herstelplannen kunnen ontwikkelen voor eerder

geïdentificeerde kritieke bedrijfsactiviteiten (Randeree et al, 2012). Een dergelijk voorbereidingsvermogen kan worden ontwikkeld "door het uitbreiden van algemene kennis en technische faciliteiten, en gegeneraliseerde controle over middelen" (Wildavsky, 1991).

4.5 Crisis Governance

Literatuur over HRO en business continuity vragen dus aandacht voor het voorbereid zijn, met name voor de situatie waarin een bedrijf of keten van bedrijven een groot incident ondergaat en zich daaruit herstelt. Juist waar het clusters of netwerken betreft, is dan de literatuur over crisis governance van belang.
Berx definieert crisis governance als: hoe een organisatie als systeem vormen en structuren van autoriteit en samenwerking inzet om activiteiten te coördineren, middelen toe te wijzen, en conflict te bemiddelen om zo een gemeenschappelijk doel te behalen, iets waar leden van het systeem op zichzelf niet toe in staat zijn (Marynissen & van den oord, 2021).
Brugghemans et al pleiten voor een definitie over keuzes die gemaakt worden wanneer het grondig mis loopt en het voortbestaan van het bedrijf bepalen (Brugghemans, Pieters, & Marynissen, 2021). Crisis governance is een essentieel onderdeel binnen de incubatie theorie van Turner (1976) die beschrijft hoe je van een “near miss” naar een incident gaat en hier uiteindelijk van leert (Turner, 1976). Herstelplannen zijn een belangrijk onderdeel van crisis governance. Hierin beschrijf je niet alleen hoe je de productie weer opstart, maar ook hoe de communicatie geregeld is, waar de verantwoordelijkheden liggen, hoe de back-up situatie geregeld is, etc. Elke organisatie krijgt op termijn te maken met een crisis en dient de juiste voorbereidingen te treffen.

4.6 Conclusies uit de literatuurstudie

In de voorgaande paragrafen is een samenvattende beschrijving gegeven van relevante literatuur, de volledige lijst van geraadpleegde literatuur en andere bronnen is te vinden in de bijlage.
Naast deze literatuur zijn er de voorschriften en protocollen vanuit het kwaliteitsdomein, het stelsel van ISO-normen, die in deze literatuurstudie verder niet zijn meegenomen, ze zijn bekend bij high tech ondernemers, brancheorganisaties en adviseurs.

De samenvattende beschrijvingen, en de onderliggende literatuur, vormen een goede bron voor de verdere uitwerking van vervolgstappen van deze pilot. Wij noemen hier een aantal voorbeelden.

De opvolging van de pilot ‘sterke schakels versterken de keten’ zou weliswaar de praktische focus kunnen richten op een of meer ketens van bedrijven. Maar voor het beklijven van resultaten en voor het begrijpen van het belang van horizontale relaties met bedrijven die niet in de lineaire productieketen staan – zoals IT-leveranciers – is het noodzakelijk van een ecosysteem uit te gaan. Er is inmiddels veel bekend over soorten en verschijningsvormen van cybercriminaliteit die het mogelijk maken anticiperende risicoanalyses en actieplannen te maken om de preventie zo goed mogelijk te organiseren.
Bij de wijze van organiseren in organisatienetwerken is het belangrijk ook aandacht te schenken aan samenwerking in lerende netwerken. Naast samenwerking tussen bedrijven kan het hier ook gaan om pps-netwerken waarin bedrijven en publieke organisaties gezamenlijk werken aan het vergroten van cybersecurity als onderdeel van het organiseren van een cyberveilig ecosysteem voor veilig ondernemen en innovatie.

5 Netwerk- en ketenbeschrijving van de deelnemende bedrijven in context

Om een beeld te kunnen schetsen van de netwerken en ketens waarin de deelnemende 16 bedrijven opereren, zijn er vier interviews afgenomen met verschillende bedrijven uit twee verschillende ketens die een inkijkje gaven in hoe wordt omgaan met onderwerpen zoals: risicobepaling, veiligheid en het rapporteren van incidenten, kritische organisaties waarmee wordt samengewerkt, en communicatie. Er is voor deze specifieke bedrijven gekozen omdat ze niet alleen in verschillende branches actief zijn, maar ook verschillende groottes hebben, om verschillende interventies hebben gevraagd en een goede doorsnede geven van zowel het MKB als deelnemende bedrijven binnen deze pilot

Om een goed beeld te kunnen schetsen van deelnemende bedrijven ketens zullen eerst de branches beschreven worden waarin de 16 bedrijven actief zijn.

5.1 Deelnemende bedrijven en interventies

Uiteindelijk hebben er 16 bedrijven deelgenomen aan de pilot in twee delen. Eerst hebben er negen bedrijven deelgenomen, voornamelijk leden partijen van de Koninklijke Metaalunie (KMU). De andere zeven bedrijven komen uit de keten van ASML. De branches waarbinnen de verschillende bedrijven actief zijn:

- Advisering, onderzoek en overige specialistische zakelijke dienstverlening
- Industrie
- Bouwnijverheid
- Groot- en detailhandel
- Verhuur van roerende goederen en overige zakelijke dienstverlening
- Vervaardiging van metalen constructiewerken en delen daarvan

De bedrijven konden vervolgens kiezen uit een palet aan interventies die door Cyber4Z konden worden uitgevoerd. Dit waren; externe scan & consult, privacy in een dag, ISO 27001 interne audit, neoforce servicemanagement tool, phishing campagne & awareness, wachtwoord beveiligingscheck, mobile device managementO365, O365/ Azure beveiligingscheck, CYRA assessment, securitytraining in een dag en een korte pentest.

5.2 Risicobepaling

De vragen achter risicobepaling focusten zich op de impact van risico's en de frequentie hiervan. Vanuit de interviews kwam naar voren dat hierin een verschil zit tussen de verschillende bedrijven. Er zijn drie niveaus te zien. Sommige bedrijven zijn helemaal niet bezig op cybergebied maar hebben wel fysieke risico's zoals brand in beeld. Andere bedrijven zijn door de interventies op de hoogte gebracht van de risico's en pakken deze nu aan. Als laatste zijn er de bedrijven die zich bewust zijn van hun risico's en deze actief aanpakken. Dit kan enerzijds intern zijn maar ook in samenwerking met de IT-leverancier.

5.3 Veiligheid en het rapporteren van incidenten aan ketenpartners

De vragen rondom veiligheid en het rapporteren van incidenten waren gefocust op het achterhalen hoe bedrijven omgaan met een incident en aan wie ze dat melden als er toch wat gebeurt. Hier komt naar voren dat intern rapporteren bij vrijwel alle bedrijven duidelijk is. Bij bijna alle bedrijven is er sprake van rapporteren naar boven, ofwel naar een manager of naar

de directeur. Hoe er naar klanten of leveranciers gecommuniceerd wordt is niet altijd duidelijk. Bij het ene bedrijf loopt dit via de directie en bij de andere wordt dit helemaal niet gecommuniceerd. Drie van de vier bedrijven moet hiervoor nog een plan opstellen.

Op het gebied van interne communicatie over veiligheid komt naar voren dat er goed gecommuniceerd wordt met de werknemers op de werkvloer. Het ene bedrijf neemt hiervoor meer tijd dan de andere, maar over het algemeen is deze communicatie goed en komen werknemers ook zelf naar de ICT'er toe wanneer zij een verdachte mail of andere situatie zien. Daarnaast proberen de bedrijven op het gebied van veiligheid niet alleen te kijken naar digitale veiligheid maar ook naar fysieke veiligheid. Het een kan niet zonder het andere en een stukje locatie beveiliging wordt zeker meegenomen.

5.4 Kritische samenwerkingspartners en datastromen

Bij het bepalen van de kritische organisaties waarmee wordt samengewerkt, draaide deze vraag vooral om het vaststellen met welke externe leveranciers er wordt samengewerkt en welke diensten en producten zij leveren. Uit de verschillende interviews komt naar voren dat er vier soorten primaire partners zijn waarmee wordt samengewerkt, namelijk; klanten, leveranciers van grondstoffen, leveranciers van software veelal voor machines en een IT-leverancier. De hoeveelheid klanten is sterk verschillend binnen de verschillende bedrijven, sommige hebben er enkele, anderen hebben er aanzienlijk veel en sommige zitten alleen met de grote spelers in de high tech sector om de tafel zoals ASML, Philips, Signify maar ook NXP. Ook de hoeveelheid leveranciers van grondstoffen is sterk verschillend; er zijn partijen die alles in house maken of juist afhankelijk zijn van andere leveranciers voor onderdelen en grondstoffen. Deze diversiteit brengt een extra uitdaging mee op het gebied van cybersecurity in de keten, leveranciersmanagement wordt dan een belangrijk onderwerp.

Daarnaast is er bij sommige bedrijven sprake van een datastroom van CAD-tekeningen voor productie. Veelal is er een NDA gekoppeld aan de tekeningen die voortkomen uit CAD of soortgelijke software. Klanten leveren deze zelf aan en vervolgens worden deze gebruikt voor de productie. Op dit gebied is er te zien dat bedrijven of met een of meerdere speler in de high Tech industrie data uitwisselen en dus direct of indirect onderdeel zijn van meerdere supply chains.

Uit de analyse van softwareleveranciers en IT-leveranciers komt een vrij eenduidig beeld naar voren. Vrijwel alle bedrijven maken gebruik van een extern ICT-bedrijf voor een deel of voor de volledige infrastructuur. Enkele bedrijven kiezen ervoor om vrijwel alles in house te ontwikkelen. Deze hebben weinig externe connecties, uitgezonderd voor ofwel basale software of specialistische software voor machines.

6 De pilot in de vorm van een serie gerichte cyberweerbaarheidsinterventies

6.1 Inleiding

De praktische kern van het onderzoek was een serie gerichte cyberweerbaarheidsinterventies, uitgevoerd door een cyberconsultancy team. Het onmiddellijke doel van de interventies was uiteraard de cyberweerbaarheid te vergroten van de deelnemende bedrijven. Elk bedrijf kreeg een begeleiding aangeboden van 10 consultancy uren. Waar het streven was 15 bedrijven deel te laten nemen, werden uiteindelijk 16 bedrijven geworven, die ook het gehele traject hebben doorlopen.

De werving werd verzorgd door het Cyber Weerbaarheidscentrum Brainport (CWB) met ondersteuning van ASML.

Op deze plaats geven wij een korte samenvatting van de uitgevoerde interventies, de onmiddellijke resultaten en de bevindingen.

6.2 Proces

Het CWB benaderde de beoogde deelnemende bedrijven; een deel van die bedrijven maken deel uit van de leveranciersketen van ASML, waarbij ASML ondersteuning verleende om deze bedrijven te bereiken.
Nadat het CWB een bedrijf eenmaal had vastgelegd ondernam het cyberconsultancy team de volgende stappen:

1. **Vragenlijst**: vooraf werd een vragenlijst toegestuurd met vragen over het bedrijf, betreffende de grootte, activiteiten, IT-middelen en volwassenheidsniveau van IT-organisatie.
2. **Intake**: een gesprek van ca. een half uur waarbij het consultancy team samen met het bedrijf aan de hand van de vragenlijst bepalen waar de cyberprofessional het beste ingezet kan worden. Daarnaast werd de planning besproken en randvoorwaarden om de opdracht te kunnen starten: bijvoorbeeld, bij een netwerktest is er een actieve netwerkpoort nodig voor de tester.
3. **Uitvoering:** op een daarvoor vastgelegd moment voerde een cyberconsultant de afgesproken activiteiten uit. Soms was dit op locatie, soms op afstand.
4. **Evaluatie:** veelal ontvingen de deelnemers een rapport of een evaluatie. Daarnaast had Avans de rol om de pilot en de rol van security in de keten te evalueren met de deelnemers.

Deze uitvoering van deze processtappen wordt hieronder kort besproken.

6.3 Reflectie op de vragenlijst

De vragenlijst bestond uit algemene informatie, keteninformatie, vragen over informatiebeveiliging en stellingen over informatiebeveiliging.
Tijdens de intakegesprekken bleek dat vooral het deel informatiebeveiliging soms lastig was om in te vullen. Kennis van informatiebeveiliging is beperkt bij veel ondernemers, deels omdat men dit nog niet als kernactiviteit beschouwd, maar ook omdat ‘de IT’ vaak uitbesteed

is qua uitvoering. Daarmee vervalt natuurlijk niet de verantwoordelijkheid voor de bescherming van data en informatie, maar dat inzicht is niet overal aanwezig.

6.4 Reflectie op de intake

De intakegesprekken zijn goed verlopen en 30 minuten was in alle gevallen voldoende om te bepalen waar de cyberprofessional ingezet kon worden. In ongeveer 50% van de gevallen had de contactpersoon zelf al een idee waar de professional ingezet kon worden. Het regelen van de randvoorwaarden (opzetten gesprek, NDA's, vrijwaringen, bevestiging, planning) na de intake kostte relatief veel tijd ten opzichte van de inhoudelijke uitvoering ervan.

6.5 Reflectie op de uitvoering

De volgende activiteiten zijn uitgevoerd:

- Phishing campagne van het personeel (2)
- Technische test van het bedrijfsnetwerk (9)
- Verbeteren IT-beveiliging (vpn) (1)
- CYRA-assessment (2)
- Opstellen beleid (1)
- NIS2 assessment (1)

Wat opvalt is dat er relatief veel technische testen zijn uitgevoerd. Tijdens de intake kwam naar voren dat ondernemers vooral benieuwd zijn wat een potentiële aanvaller zou kunnen aanrichten wanneer hij zich toegang verschaft tot het bedrijfsnetwerk.
Omdat veel deelnemers de IT hadden uitbesteed aan een derde partij, is een technische test van het netwerk meer een controle van de beveiliging zoals de IT partij deze heeft opgezet.

Het oorspronkelijke doel van de pilot was om de beveiliging direct te verbeteren door middel van implementatie van maatregelen. In de praktijk was de uitvoering van de testen en andere interventies vooral een vorm van controle op de bestaande situatie. Deelnemende bedrijven dienen dan wel zelf – vaak via hun IT-leverancier - na de oplevering van het rapport over phishing of een netwerkcontrole actie te nemen.
De lering uit deze pilot is dan ook dat het lastig is om voorgestelde maatregelen direct – aansluitend op een test- en adviestraject - te implementeren. Er is overleg nodig met de onderneming zelf, vaak ook met de IT-leverancier; en er is maatwerk vereist, in die zin dat een implementatieplan moet aansluiten bij de IT-infrastructuur en de werkwijze van het bedrijf (en zijn IT-dienstverlener).

Op basis van de netwerktesten kan geconstateerd worden dat het niveau van beveiliging wisselend is. Er zijn deelnemers waar bijna geen kwetsbaarheden zijn gevonden en waarbij geconcludeerd kan worden dat zij de beveiliging goed op orde hebben. Er zijn echter ook deelnemers waarbij een complete domein takeover is gerealiseerd: ergo, waar een aanvaller vrijuit zijn gang kan gaan in het IT-netwerk.

6.6 Resultaten en bevindingen uit de interventies samengevat

Een belangrijk resultaat is dat alle deelnemende bedrijven open staan voor de rapportages, de bevindingen goed ontvangen hebben, en deze gaan opvolgen.

In een volgende pilot zouden de vragen en stellingen over informatiebeveiliging concreter en simpeler gesteld moeten worden.
Het regelen van de randvoorwaarden (opzetten gesprek, NDA's, vrijwaringen, bevestiging, planning) na de intake moet niet onderschat worden, dit kost relatief veel tijd ten opzichte van de daadwerkelijke interventies.
Een volgende keer kan een interventietraject nader gefaseerd worden. In de eerste fase kan redelijk gestandaardiseerd het intake- en adviestraject doorlopen worden. Vervolgens is er dan de implementatie die een maatwerkaanpak vereist.
In het vervolg zouden ook de IT-leveranciers betrokken moeten worden, omdat deze een belangrijke rol spelen in de beveiliging.

Als algehele conclusie kan de pilot als geslaagd betiteld worden. Alle deelnemers hebben meer inzicht in beveiliging gekregen; zij kunnen en willen zich weerbaarder (laten) maken tegen cybercriminaliteit.

7 De afsluitende validatie- en ontwerpworkshops

Intro
De oorspronkelijke opzet was om afzonderlijke workshops te organiseren op verschillende data. Dit zou de onderzoekers de tijd en ruimte bieden om resultaten uit de eerste – validatie – workshop te verwerken als basis voor de tweede – ontwerp – workshop. Aan de eerste workshop zouden de bedrijven deelnemen die ook bij de pilot betrokken waren. De tweede workshop zou primair georganiseerd worden met medewerking van experts uit organisaties op gebied van cybersecurity en MKB.
Uiteindelijk is besloten beide workshops op een dag plaats te laten vinden. Belangrijkste overweging hiervoor was de bedrijven de kans te bieden om aan beide workshops deel te nemen. Wel is vastgehouden aan de onderscheiden doelen van beide workshops, d.w.z. de onderzoekers hebben tijdens de pauze de bevindingen uit de eerste workshop geresumeerd, en deze als vertrekpunt voor de tweede workshop gepresenteerd.
Beide workshops vonden plaats op donderdag 13 april in verschillende zalen van Brainport Development.

7.1 De validatie workshop

Voor de validatieworkshop is anderhalf uur uitgetrokken. Deelnemers waren de bedrijven die betrokken waren bij de interventies en bij het onderzoek, naast experts van het CWB. Presentaties werden verzorgd door onderzoekers van het lectoraat en door consultants van Cyber4Z. In de presentaties zijn de inzichten en voorlopige conclusies uit de literatuurstudie, de expertinterviews en uit de interventies kritisch tegen het licht gehouden. De daaropvolgende dialoog leverde verdiepte inzichten op over de condities voor samenwerking, en over de vorm en timing van interventies gericht op cyberweerbaarheid. De uitkomsten van deze validatieworkshop vormden vervolgens het vertrekpunt voor de ontwerpworkshop.

7.2 De ontwerpworkshop

Aan de ontwerpworkshops namen – naast een aantal ondernemers die ook aan de voorgaande validatieworkshop deelnamen – een aantal experts deel vanuit het CWB, Brainport Development, de Provincie N-Brabant, Platform Veilig Ondernemen N-Brabant & Limburg, het Regiobureau Integrale Veiligheid Oost-Brabant, de KvK, Koninklijke Metaalunie, Cyberveiligheid Breda, Datacoaches, Fontys, Cyber4Z.

Uitgaande van de voorlopige conclusies uit de validatieworkshop is er aan de hand van een aantal kenmerken die de onderzoekers aandroegen uitgebreid gesproken over de condities en kenmerken waaraan shared functies als die van cyberexpert en CISO zouden moeten voldoen.

De resultaten uit beide workshops zijn verwerkt in de conclusies en aanbevelingen van dit onderzoeksrapport.

8 Conclusies en aanbevelingen

8.1 Conclusies

De Avans onderzoekers formuleren hier een aantal conclusies die gebaseerd zijn op (i) het monitoren van de interventies tijdens de voorbereiding en uitvoering ervan door het cyberconsultancy team van Cyber4Z, (ii) de tussentijdse overleggen met het Cyber Weerbaarheidscentrum Brainport (CWB), het Regiobureau Integrale Veiligheid Oost-Brabant, de interventieconsultants van Cyber4Z, en (iii) de expertinterviews met een aantal deelnemende bedrijven, en voorbereidende bron- en literatuurstudies. De tussentijdse bevindingen en concept-conclusies zijn tevens besproken in een klankbordgroep binnen het lectoraat waarin onder meer experts deelnamen op gebied cybersecurity interventies binnen bedrijven, samenwerking tussen Mkb's, pps-constructies in het veiligheidsdomein, organisatienetwerken en netwerkorganisaties, en de ontwikkeling en uitvoering van een CISO-functie.

De overall conclusie is dat de pilot geslaagd is: in de zin dat het gelukt is 16 bedrijven bij de interventies en de adviestrajecten te betrekken, en het voornemen van die bedrijven om de adviezen ook op te volgen door maatregelen te treffen – al dan niet samen met hun IT-leveranciers. Een deel van deze bedrijven nam ook actief deel in de overall evaluatie in de vorm van de validatie- en ontwerpworkshops.
De projectpartners – de experts van het Regiobureau Integrale Veiligheid Oost-Brabant, ASML en van het CWB, de consultants van Cyber4Z, en de Avans onderzoekers hebben productief kunnen samenwerken.
Meer in detail terugkijkend naar het verloop van de pilot zijn een aantal conclusies te trekken over de resultaten van de interventies tijdens de pilot, mogelijke vervolgstappen om het concept 'sterke schakels versterken de keten' verder te ontwikkelen en concretiseren, o.a. in de vormgeving van de rollen van de cyberprofessional(s) en de shared CISO.

8.1.1 Resultaten van de interventies tijdens de pilot

De interventies door het cyberconsultancy team van Cyber4Z hebben plaatsgevonden. Het is gelukt 16 bedrijven bij de interventies te betrekken. Dit betreft zowel bedrijven die leveranciers zijn van ASML, als ook andere bedrijven. Een bereik van 100% van het geplande aantal deelnemende bedrijven is dus gerealiseerd.
Bij al deze bedrijven kon het volledige pakket van interventies worden uitgevoerd, waarbij uiteraard per bedrijf andere prioriteiten zijn gesteld naar gelang de behoeftes van een bedrijf. De impact van de interventies is beperkter in reikwijdte dan bij de voorbereiding van het project was voorzien. Alle deelnemende bedrijven zijn weliswaar van een actiegericht maatwerkadvies voorzien dat men wil gaan uitvoeren; dat is een concreet resultaat. Maar de (eerste stappen van) implementatie ervan maakte uiteindelijk geen deel uit van de interventies.
Het beschikbare aantal consultancy uren in de pilot voor elk bedrijf (max. 10 uur) en de korte doorlooptijd van de interventies als geheel (vier maanden) waren toereikend voor een maatwerk-adviestraject. Een veelvoud van begeleidingsuren is echter vereist voor de implementatie, en de totale doorlooptijd van implementatie van het maatwerkadvies bedraagt – incl. tussentijdse besluitvorming binnen een bedrijf – enkele maanden tot een jaar.

Een tweede positief resultaat van de pilot is dat een MKB beter voorbereid is gerichte kritische vragen te stellen aan zijn IT-leverancier, over de mate waarin deze leverancier zelf cyber secure is. Dit is in het bijzonder van belang voor Mkb's die al jarenlang samenwerken met dezelfde IT-leverancier. In de pilot is het gesprek tussen enkele deelnemende ondernemers en hun brancheorganisaties verder op gang gebracht, hoe een IT-leverancier met wie al langer wordt samengewerkt, geconfronteerd kan worden met nieuwe eisen en wensen. Het is voor veel Mkb's een onderdeel van hun eigen organisatiecultuur dat er een wijze van samenwerking is die berust op onderling professioneel – en soms ook sociaal – vertrouwen. Het behoort dan tot de cultuurverandering van een bedrijf om niet alleen zelf cyber secure te worden, maar ook een 'trusted IT supplier' hierop aan te spreken.

8.1.2 Mogelijke vervolgstappen voor het concept 'sterke schakels versterken de keten'

De pilot resulteert in een aantal concrete beelden over te nemen mogelijke vervolgstappen. Wij geven deze hier kort weer; tijdens de afrondende workshops onder leiding van Avans onderzoekers is er door aanwezigen, waaronder experts van het CWB, de Provincie, PVO Zuid, het Regiobureau Integrale Veiligheid Oost-Brabant en KMU meer in detail gesproken over mogelijke vormen van vervolg en hun eigen betrokkenheid daarin.

De algehele conclusie is dat een opvolging in de vorm van schaalbare pilots gewenst is om het concept 'sterke schakels versterken de keten' verder te ontwikkelen en concretiseren.

In de voorbereiding op die pilots moet een verdere uitwerking plaatsvinden van de business case voor elk van de (beoogde) deelnemende bedrijven.

Er zouden roadmaps beschikbaar moeten komen voor de (te nodigen) deelnemende bedrijven, die de deelnemers houvast bieden bij de uitvoering, en waarmee de bedrijven de timing en het tempo van te nemen stappen kunnen afstemmen op hun beschikbare resource: geld waar het om inhuur van (implementatie)consultants of om inhuur van een andere IT-leverancier gaat, uren waar het gaat om training en bijscholing van personeel gaat, uren waar het om interne (implementatie)projectleiding gaat.

Ondernemers maken zich zorgen over een (nieuw) oerwoud aan certificaten, en het onderhoud ervan dat erachter wegkomt. Standaardisatie via toepassing van toolkits van brancheorganisaties, CYRA en van DTC zouden door certificatieorganisaties geaccepteerd moeten worden

Samenwerking in de keten wordt gezien als een goede kans. Ook is geopperd samenwerking in pps-constructen te verkennen. Onderdeel van die samenwerking zou kunnen zijn bepaalde functies te delen. Van de functies shared cyberprofessional(s) en shared CISO geven we in de volgende sectie de belangrijkste kenmerken mee.

8.1.3 Kenmerken van shared functies cyberprofessional en shared CISO

De hier geschetste kenmerken gelden voor wat wij hier kortheidshalve 'shared functies' noemen. Dit is een aanduiding van de verantwoordelijkheid van de betrokken functionarissen. In de praktijk zal het niet gaan om 1 persoon, maar om teams. Hiervoor zijn een aantal redenen te geven: (i) er zijn verschillende specialisaties en vakbekwaamheden vereist die niet in 1 persoon te verenigen zijn; (ii) het gaat functies die kritisch zijn voor de business continuity, uitval is geen optie en inzet bij meerdere bedrijven tegelijkertijd kan vereist zijn;

(iii) de shared functies vervullen een belangrijke rol in het stimuleren van praktijkleren en reflectie op en het actief delen van good practices.

Allereerst gaat het om de shared functie van cyberexpert, waarbij de volgende inhoudelijke en organisatorische kenmerken aan de orde zijn.

- Het gaat om uiteenlopende expertises en vaardigheden, bijv.: risico-analist en adviseur, softwarespecialist, implementatie projectleider. Daarnaast kan het gaan om specialismen rond AVG, databases, specifieke cyberattacks.
- Naast de primair taakstelling, operationele bijstand van de samenwerkende bedrijven, is er ook een proactieve en lerende taak, om good practices te delen en om actuele inzichten uit de vakwereld rond cyberattacks snel te delen. Een aandachtspunt daarbij is de vertrouwensrelatie tussen het team en de samenwerkende bedrijven, en uiteraard de bedrijven onderling.
- Qua organisatie lijkt een onafhankelijk team de beste optie, waarbij er een meerjarige afspraak is met een groep bedrijven op basis van een strippenkaartformule, met een jaarlijkse minimale inzet voor periodieke controles.
- Er zijn varianten op voorgaand model, t.w.:
    - Een pps-construct waarbij publieke partners zoals PVO Zuid-Nederland en/of gemeenten participeren en expertises inbrengen
    - Een OEM neemt deel en brengt expertises in

  Bij beide varianten zin er ook aandachtspunten. De overheid heeft ook een controlerende taak, en met OEMs is er een economische afhankelijkheidsrelatie.
- De laagdrempelige toegang tot de shared functie, het team, is belangrijk. Varianten hierop zijn regelmatige (online) bijpraatmomenten of spreekuren op locatie, op bedrijventerreinen.

De inhoudelijke en organisatorische vormgeving van de shared CISO-functie bouwt voort op bovengenoemde kenmerken, waarbij er een aantal aanvullende kenmerken zijn, gezien de positie van deze functie.

- Deze functie heeft rechtstreeks toegang tot de directie (en/of de bestuurder) van een bedrijf, heeft doorzettingsmacht om ook ongevraagd en niet vrijblijvend te adviseren.
- Deze functie staat daartoe in contact en heeft vertrouwensrelaties met zowel de meer technische als de meer business- en organisatiegerichte directieleden, en cyberexperts.
- De bijdrage aan het leren in netwerken en ketens van bedrijven is een bijzondere taak, waarbij deze shared CISO-functie stuwend en organiserend is, bijv. door het organiseren en modereren van leerkringen voor directieleden en voor cyberexperts.

8.1.4 Limitaties

In de opzet van het onderzoek is niet gestreefd naar representativiteit. Gegeven de vraagstelling van het onderzoek ging het om de selectie van een populatie van high tech bedrijven die samenwerken in ketens rond de OEMs in en rond Eindhoven.

8.2 Aanbevelingen

Er is bij de deelnemende bedrijven, bij de betrokken experts vanuit de Koninklijke Metaal Unie, de Provincie en bij het CWB een sterke interesse om een gezamenlijke planmatige opvolging te geven aan deze pilot. Ook vanuit Avans als kennispartner in deze pilot, is er

nadrukkelijk interesse. Er liggen voor de praktijk belangrijke en voor de wetenschappelijke interessante vraagstukken die om nader onderzoek vragen.

Bij het verder planmatig uitwerken van die opvolging zijn een aantal zaken die aandacht vergen.

Allereerst moet het nadrukkelijk gaan op opschaling, anders gezegd om het verder ontwikkelen en testen van schaalbare aanpakken en toepassingen.

Voor de deelnemende bedrijven en koepelorganisatie is daarbij een vereiste, dat er een of meer varianten van een roadmap beschikbaar komt.
Aan de hand van die roadmap kan een cluster van bedrijven, of een (groter) bedrijf in een keten, bepalen op welk moment ze in werk tempo welke stappen gaan realiseren. Waarbij het van belang is dat die stappen 'behapbaar' zijn: de impact op de workload van leidinggevende en uitvoerende professionals moet zoveel mogelijk (tijdig) in te plannen zijn, om de bedrijfsvoering zo min mogelijk te belasten, en ook om een leidinggevende die parttime een cybersecurity implementatie aanstuurt, tijdig voor een bepaalde 'blokreservering' van uren en weken kan zorgen.
'Timing' is een andere vereiste vanuit de bedrijven, beter gezegd: advies over het moment waarop een bedrijf of cluster van bedrijven het beste in de realisatie van een roadmap kan inhaken. Om dus tijdig human resources in te kunnen plannen, maar vooral om effectief te kunnen zijn.

Een andere meer algemene eis is de business case analyse die voorafgaat aan de invulling van de roadmap planning, en die tijdens de realisatie en de evaluatie van de eenmaal doorlopen roadmap plaatsvindt.
Het ontbreekt bedrijven aan houvast bij het in beeld brengen van alle kosten en baten, zeker waar het gaat om onbekende kosten en baten in termen van kansen op nieuwe producten of diensten. Recent hebben TNO en NCSC hiervoor een handreiking uitgebracht[1].

De daadwerkelijke invoering van de NIS-2 wet- en regelgeving vormt op termijn een business driver voor bedrijven om te investeren in cybersecurity. Het is onduidelijk op welke termijn dit gaat spelen. Wel is duidelijk dat NIS-2 dwingend zal zijn voor IT-leveranciers. Dit biedt kansen voor bijvoorbeeld een groep bedrijven die dezelfde IT-leverancier hebben i.c. gaan inhuren, zouden deze leverancier kunnen 'aansporen' nu al actie te nemen.

Een interessante kans tenslotte, is de mogelijke inbedding van cybersecurity roadmaps als onderdeel van projecten rond procesinnovatie. Waar investeringen in cybersecurity vaak gezien worden, en ook min of meer worden gepresenteerd als een 'verplicht nummer' met allerlei nieuwe verplichtingen rond rekenschap en verantwoording, ligt er een kans om maatregelen op gebied van cybersecurity te benutten om bedrijfsvoering, samenwerking met andere bedrijven in de keten, en procesinnovaties te ontwikkelen en door te voeren.

---

1 https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ncsc.nl%2Fonderzoek%2Fdocumenten%2Fpublicaties%2F2023%2Fapril%2F17%2Faan-de-slag-met-het-kwantificeren-van-cyberrisicos&data=05%7C01%7Cbjm.kokkeler%40avans.nl%7C340021b1992647157d7f08db40f2da36%7C87c50b582ef2423da4db1fa7c84efcfa%7C0%7C0%7C638175184009880242%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=LkdftYIV6jkdaWyBnFn%2BD%2FG9TbVBZLjXRuEKYp9e1gY%3D&reserved=0

Met het oog op de centrale vraag rond de effectiviteit van versterking van schakels in een keten, is een belangrijke aanbeveling, dat de samenwerking wellicht privaat-publiek moet zijn. Om effectief te zijn voor de publieke taak, te weten het creëren van een veilige en productieve omgeving voor business continuity en innovatie. En om efficiënt te zijn voor ondernemers. In vergelijkbare domeinen is te zien dat deze nieuwe vormen van pps-en 'werken'. Het organiseren van shared functies van teams van cyberexperts en teams van CISO's zouden hierin een plek kunnen krijgen.
Juist voor het innovatie ecosysteem dat zich in Zuid-Nederland verder ontwikkelt, liggen hier kansen om de eerder bepleitte schaalbare vervolgpilots als pps-constructen te organiseren.

9 Bibliografie

Brainport Eindhoven. (z.d.). *Samenwerking tussen overheid, bedrijfsleven en onderwijs- en kennisinstellingen*. Opgehaald van Brainport Eindhoven: https://brainporteindhoven.com/nl/ontdek/strategie

Brons, D. A. (2016). *Success within the innovation ecosystem.* Amsterdam: Amsterdam Business School.

Brugghemans, B., Pieters, S., & Marynissen, H. (2021). Alles onder controle. In B. Brugghemans, S. Pieters, & H. Marynissen, *Alles onder controle* (pp. 46-47). Leuven: Lannoo Campus.

Cerules, L. (2021, Februari 15). *SolarWinds is 'largest' cyberattack ever, Microsoft president says* . Opgehaald van Politico: https://www.politico.eu/article/solarwinds-largest-cyberattack-ever-microsoft-president-brad-smith/

Chesbrough, H. W. (2003). *Open Innovation: The New Imperative for Creating and Profiting from Technology.*

Elliott et al. (1999). In D. E. Elliott, *Just waiting for the next big bang: Business continuity planning in the UK finance sector* (pp. 43-60). Journal of Applied Management Studie.

Goedee & Entken. (2008). In J. &. Goedee, *(Ont)keten. Implementeren van werken in ketens.* Lemma.

Gulati, Puranam & Tushman. (2012). Geen eenheid in command en control op basis van formele autoriteit. . In R. P. Gulati, *Meta-organization design: Rethinking design in interorganizational and community contexts.* (pp. 571-586.). Strategic management journal.

Iansiti, M & Levien, R. (2004). In M. &. Iansiti, *The Keystone Advantage.* Massachusetts: Hardvard Business School Press.

Jeferson, Martinez & Javier M, Duran. (2021, Oktober 12). *Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study.* Opgehaald van International Information and Engineering Technology Association: https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.110505

Legnick-Hall & Beck. (2009). In C. A. Lengnick-Hall, *Resilience capacity and strategic agility: Prerequisites for thriving in a dynamic environment. In Resilience engineering perspectives, Volume 2. Preparation and restoration* (pp. 39-70). Aldershot: Ashgate Publishing.

Linnenluecke et al. (2012). In M. K. Linnenluecke, *Extreme weather events and the critical importance of anticipatory adaptation and organizational resilience in responding to impacts.* (pp. 17–32). Business Strategy and the Environment.

Marynissen, H., & van den oord, S. (2021). De kunst om het vuur aan te wakkeren. *Machtig vuur: over de kracht van vuur en de beheersing ervan in sterk verander(enn)de tijden.* (pp. 117-144). Antwerpen: Provincie Antwerpen.

Moore, J. F. (1997). The Death of Competition. In J. F. Moore, *The Death of Competition.* New York: Harper Collins Publishers.

Nakashima, E., & Timberg, C. (2020, December 14). *Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce*. Opgehaald van The Washington Post: https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

NCSC Magazine. (2020, December 16). *Eendracht maakt macht: Cybersecurity in het ecosysteem*. Opgehaald van NCSC: https://magazines.ncsc.nl/ncscmagazine/2020/02/lds-cwb

Provan, Fish & Sydow. (2007). Eigenschappen van organisatienetwerken geciteerd op pagina 482. In K. G. Provan, *nterorganizational networks at the network level: A review of the empirical literature on whole networks.* (pp. 479-516.). Journal of management.

Randeree et al. (2012). In K. A. Randeree, *A business continuity management maturity model for the UAE banking sector.* (pp. 472–492). Business Process Management Journal .

Symantec. (2019). *2019 Internet Security Threat Report.* Opgehaald van Symantec: https://docs.broadcom.com/doc/istr-24-executive-summary-en

Turner. (1976). In B. A. Turner, *The organizational and interorganizational development of disasters.* (pp. 378-397). Administrative science quarterly.

Wildavsky. (1991). In A. B. Wildavsky, *Searching for Safety* (p. 221). New Brunswick: Transaction.