Verkenning behoefte cyberweerbaarheidscentrum Life Sciences & Health Sector Zuid-Holland

Uitgevoerd in opdracht van:
Security Delta
Stichting Leiden BioScience Park
Metropoolregio Rotterdam Den Haag

Buck Consultants International
Nijmegen, 18 oktober 2022

Inhoudsopgave

Hoofdstuk 1 Inleiding

1.1 Achtergrond

Cyberincidenten zijn aan de orde van de dag. De jaarlijkse schade door cybercrime voor de Nederlandse economie bedraagt inmiddels meer dan 10 miljard euro. In 2019 is ruim 55% van het midden- en klein bedrijf minstens één keer slachtoffer geworden van cybercrime. De schade door een digitale aanval loopt snel op, vanwege het (deels) stil vallen van werkprocessen, verlies van relevante data, kostbare hersteloperaties en imagoschade.

Het Nationale Cyber Security Centrum (NCSC) biedt vitale sectoren ondersteuning bij het in beeld brengen en beheersen van risico's. Voor Zuid-Holland belangrijke sectoren als tuinbouw en life sciences & health worden nog niet tot deze vitale sectoren gerekend en ontberen een dergelijke ondersteuning. In opdracht van provincie Zuid-Holland is in 2020 een onderzoek uitgevoerd naar de mate waarin de provinciale economie bestand is tegen cyberaanvallen. Uit dit onderzoek blijkt onder meer dat de Life- en BioScience sector in hoge mate is gedigitaliseerd en kwetsbaar is voor cyberdreigingen als het stelen van IP en het lekken van persoonsdata. Binnen de sector bestaan grote verschillen in mate van digitaal risicomanagement, waarbij middelgrote en vooral kleine bedrijven en instellingen de risico's vaak wel zien, maar niet weten hoe ze hiermee om moeten gaan. Deze groep heeft behoefte aan gerichte ondersteuning.

In navolging van een vergelijkbaar initiatief voor de Greenport West-Holland hebben Security Delta (HSD) en Leiden BioScience Park (LBSP) samen met andere stakeholders het initiatief genomen voor het opzetten van een cyberweerbaarheidscentrum/-programma voor de Life Sciences & Health (LSH) sector. Het gaat om een regionaal expertisecentrum en informatieknooppunt rond cybersecurity vraagstukken, met als voornaamste functies het stimuleren van bewustwording, advisering, het faciliteren van expertoverleg en kennisdeling, en het oprichten van een loket voor raad, advies en slachtofferhulp. Om te komen tot zo'n centrum heeft HSD een stappenplan uitgewerkt dat bestaat uit drie delen:

1 Basisanalyse: in deze analyse wordt de behoefte aan een cyberweerbaarheidscentrum verkend, door contactpersonen bij een aantal relevante bedrijven en sectorale organisaties te identificeren en de behoeften aan ondersteuning binnen de sector na te gaan.
2 Daarnaast wordt door Hogeschool Leiden met steun van de Haagse Hogeschool ook gewerkt aan een sectorale nulmeting van het cyberweerbaarheidsniveau van LSH-bedrijven en instellingen in de regio.
3 Ervan uitgaande dat deze analyses voldoende perspectief bieden, wordt op basis van een 'go-beslissing' gewerkt aan het opzetten van het cyberweerbaarheidscentrum. De

werkzaamheden bestaan uit het ontwikkelen van een bassistructuur, verdere uitwerking van de benodigde ondersteuning en hulpmiddelen die aansluiten op de resultaten van de nulmeting, organisatie van awareness sessies en uitwerking van het businessplan, inclusief financiering van het Cyberweerbaarheidscentrum.

Deze rapportage beschrijft de uitkomsten van de basisanalyse.

1.2 Aanpak basisanalyse

Deze verkenning van de behoefte aan een cyberweerbaarheidscentrum bestond uit de volgende onderdelen:

- Samenstellen van een overzicht van contactpersonen bij bedrijven en sectorale organisaties uit de hele regio waarbij veiligheidsvraagstukken op het bord belanden.
- Benaderen van deze organisaties om de behoeften in de sector te achterhalen, waarbij in principe minimaal 2 cyberveiligheidsvraagstukken worden opgehaald. Het benaderen van deze organisaties gebeurt in nauw overleg met Hogeschool Leiden/Haagse Hogeschool om duplicatie te voorkomen.
- Vastlegging van de resultaten in een beknopte rapportage. Het voorziene resultaat van de basisanalyse is een beknopt document met:
  - een overzicht van de kernspelers in de LSH-sector in Zuid-Holland (ketenregisseurs, brancheorganisaties, bedrijven en instellingen),
  - de belangrijkste behoeften van LSH-bedrijven en instellingen op het vlak van cyberweerbaarheid, en
  - de eerste contouren van de programmering van het cyberweerbaarheidscentrum en een indicatie van mogelijke financieringsbronnen.

In totaal zijn in de eerste helft van 2022 ruim 25 (mede vanwege Covid digitale) interviews gehouden met relevante organisaties en bedrijven (zie bijlage 1 voor geanonimiseerd overzicht van geïnterviewde partijen). Daarnaast hebben 14 bedrijven niet op het verzoek voor een interview gereageerd of dit geweigerd. Als belangrijkste redenen voor deze non-respons werden genoemd: gebrek aan tijd of interesse, het voldoende op orde hebben van de eigen systemen, en het geen behoefte hebben aan (extra) ondersteuning vanuit een cyberweerbaarheidscentrum.

De wel geïnterviewde bedrijven en instellingen zijn gevraagd naar de aandacht voor cyberweerbaarheid in hun eigen bedrijfsvoering, hun belangrijkste veiligheidsvraagstukken en hun behoefte aan ondersteuning. Overheden en intermediairs zijn bevraagd op het belang van cyberweerbaarheid in de LSH-sector binnen hun werkgebied en mogelijk interessante bedrijven en instellingen die in het kader van deze verkenning zouden kunnen worden benaderd.

1.3 Leeswijzer

Hoofdstuk 2 gaat in op de aard en omvang van de Life Sciences & Health sector in Zuid-Holland, als potentiële doelgroep van het op te richten cyberweerbaarheidscentrum. Hoofdstuk 3 beschrijft de resultaten van de interviews. Op basis van deze resultaten wordt in hoofdstuk 4 het gewenste aanbod van een cyberweerbaarheidsprogramma geschetst. Tot slot worden in hoofdstuk 5 de belangrijkste conclusies en aanbevelingen van deze verkenning weergegeven.

Hoofdstuk 2 LSH-sector Zuid-Holland

2.1 Inleiding

De Life Sciences & Health (LSH) sector bestaat uit een scala van uiteenlopende bedrijven en instellingen. Enerzijds omvat het de Life- en BioScience sector die zich bezighoudt met R&D en productie van o.a. medicijnen, vaccins, biomarkers, etc. en veelal internationaal opereert. Anderzijds betreft het onderzoek, ontwikkeling en productie van medische technologie (Medtech), zowel hoogwaardige apparaten voor bijvoorbeeld OK's en IC's in klinieken, als medium en low tech producten voor zorg in en om huis. Beide deelsectoren bedienen grotendeels een (inter-)nationale markt en zijn daarmee 'stuwend' voor de economie van Zuid-Holland. Tot slot omvat de Health-kant van de sector een veelheid van zorginstellingen (zowel cure als care) en gezondheidsondersteunende diensten, die primair ten goede komt aan de eigen inwoners van de provincie. Al deze bedrijven en instellingen opereren binnen ketens van toeleveranciers, dienstverleners en afnemers c.q. eindgebruikers, die vaak de provinciegrens overstijgen. Omdat cyberdreigingen zowel gericht kunnen zijn op de eigen organisatie als op de zwakste schakels in de waardeketen, is voor het bestrijden van incidenten een ketenbenadering belangrijk.

De Life-& BioSciences en Medtech sector in Zuid-Holland behoort tot de top van de wereld op het gebied van wetenschappelijk onderzoek en ondernemerschap. In 2020 telt deze sector in totaal 2.147 bedrijven met 68.461 werkzame personen[1].

Leiden, Delft en Rotterdam zijn de drie focusgebieden in de provincie Zuid-Holland voor de ontwikkeling van innovatieve toepassingen en technologie in de Life- en BioScience en Medtech sector. Zo bevindt zich in Leiden het grootste BioScience cluster van Nederland waar meer dan 400 innovatieve Life Sciences bedrijven actief zijn in de biotech/farma en de ontdekking en ontwikkeling van geneesmiddelen. In de Rotterdam Science Tower zijn organisaties werkzaam in niches als virologie, diagnostiek en genomics, terwijl op de TU Delft Science Park bedrijven actief zijn in de niches Medtech, e-health, devices en robotics. Een aantal voorbeelden van leidende BioSciences en Medtech bedrijven actief in Zuid-Holland zijn ThermoFisher, 3M, Astellas, DSM, Biomarin, WelchAllyn, Janssen, Pfizer, Galápagos en Toshiba.

Naast tal van innovatieve bedrijven beschikt de regio over drie gerenommeerde universiteiten, twee Universitair Medische Centra en vier Life Sciences incubators/accelerators. Dit alles maakt dat de provincie Zuid-Holland een uitermate geschikte omgeving heeft voor het doen van klinische proeven en het verder ontwikkelen en het testen van nieuwe geneesmiddelen.

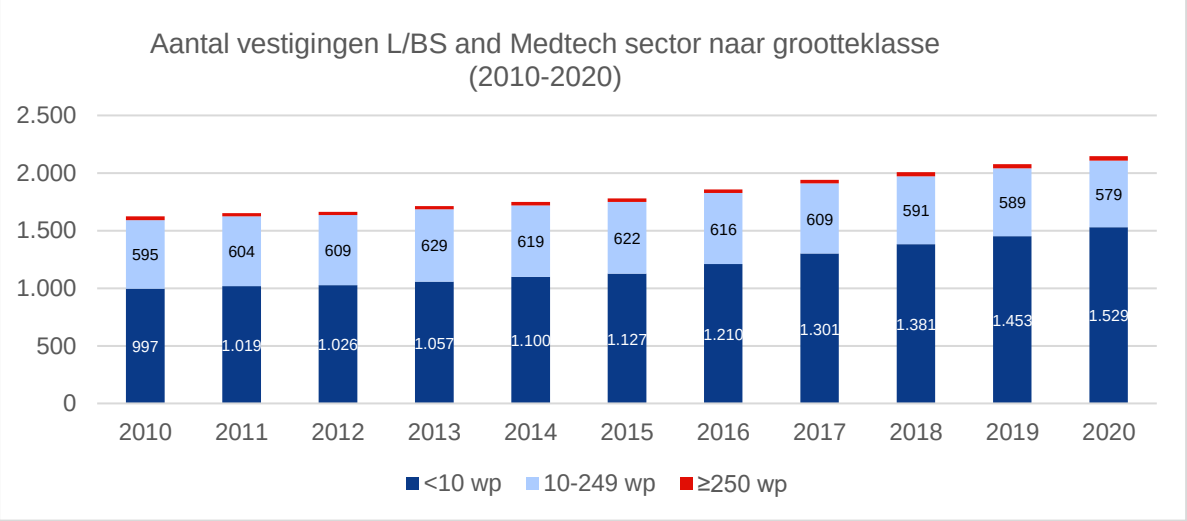
[1] Bron: Zuid-Holland in Zicht (data: LISA, regionale vestigingsregisters)

Enkele voorbeelden van succesvolle innovaties die afkomstig zijn uit het Zuid-Hollandse cluster:

- Crucell heeft het eerste internationaal verkrijgbare volledig vloeibare vaccin Quinvaxem ontwikkeld dat antigenen combineert voor bescherming tegen de vijf kinderziekten
- Jansen Biologics heeft Remicade ontwikkeld voor de behandeling van auto-immuunziekten
- Royal DSM is verantwoordelijk voor de eerste doorbraakanalyse van de DNA-sequentie van de schimmel Penicillium chrysogenum.

2.2 Ontwikkeling van Life-/BioScience en Medtech sector

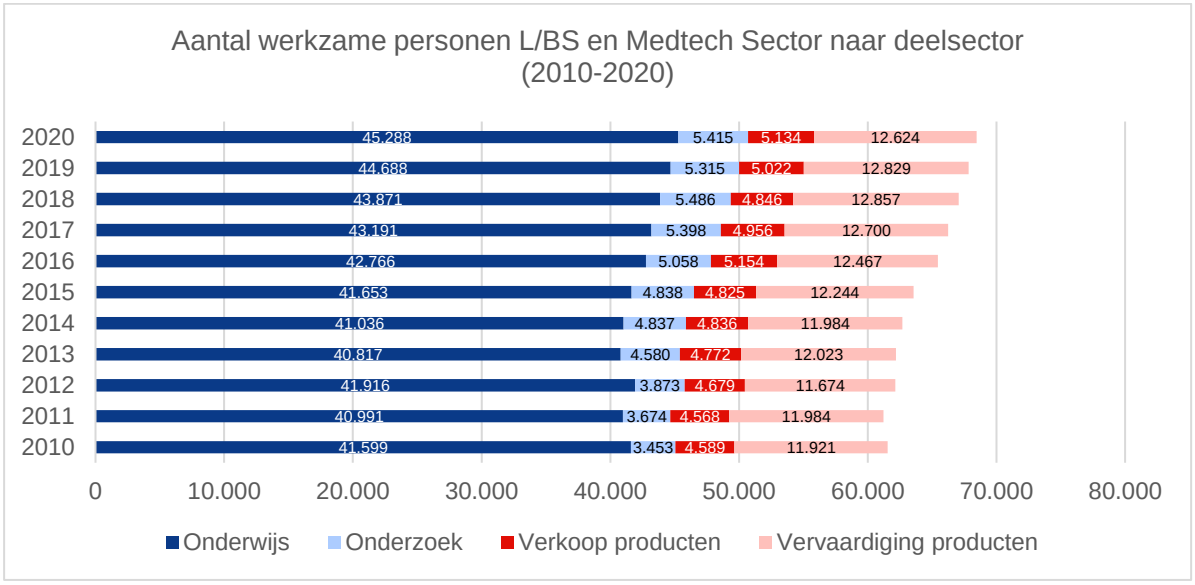
In de periode 2010-2020 is het aantal vestigingen in de Life- & BioScience en Medtech sector in Zuid-Holland sterk gegroeid, namelijk met 32%. Als gekeken wordt naar het aantal vestigingen naar grootteklasse blijkt dat de sector voor het grootste gedeelte bestaat uit bedrijven met minder dan 10 werkzame personen. Dit is ook de groep bedrijven die in de periode 2010-2020 het sterkst is gegroeid (+53% | +532 bedrijven). Het aantal bedrijven met 250 of meer werkzame personen is in dezelfde periode gestegen met 18% (+6 bedrijven), terwijl het aantal organisaties met 10-249 werkzame personen licht is afgenomen (-3% | -16 bedrijven).



Bron: Zuid-Holland In Zicht (data: LISA)

Relatief gezien blijft de groei van het aantal werkzame personen in de afgelopen 10 jaar wat achter bij de groei in het aantal vestigingen. Ten opzichte van 2010 is het aantal werkzame personen met 11% toegenomen van 61.562 werkzame personen naar 68.461 werkzame personen in 2020. Als gekeken wordt naar de groei van het aantal werkzame personen in de

verschillende deelsectoren[2], blijkt dat de deelsector onderzoek relatief gezien het sterkst gegroeid is. In de afgelopen 10 jaar zijn er 1.962 onderzoek gerelateerde banen bij gekomen wat gelijk staat aan een groei van 57%. In de andere drie deelsectoren te weten onderwijs, verkoop van producten en vervaardiging van producten is de werkgelegenheid in zelfde periode licht toegenomen.

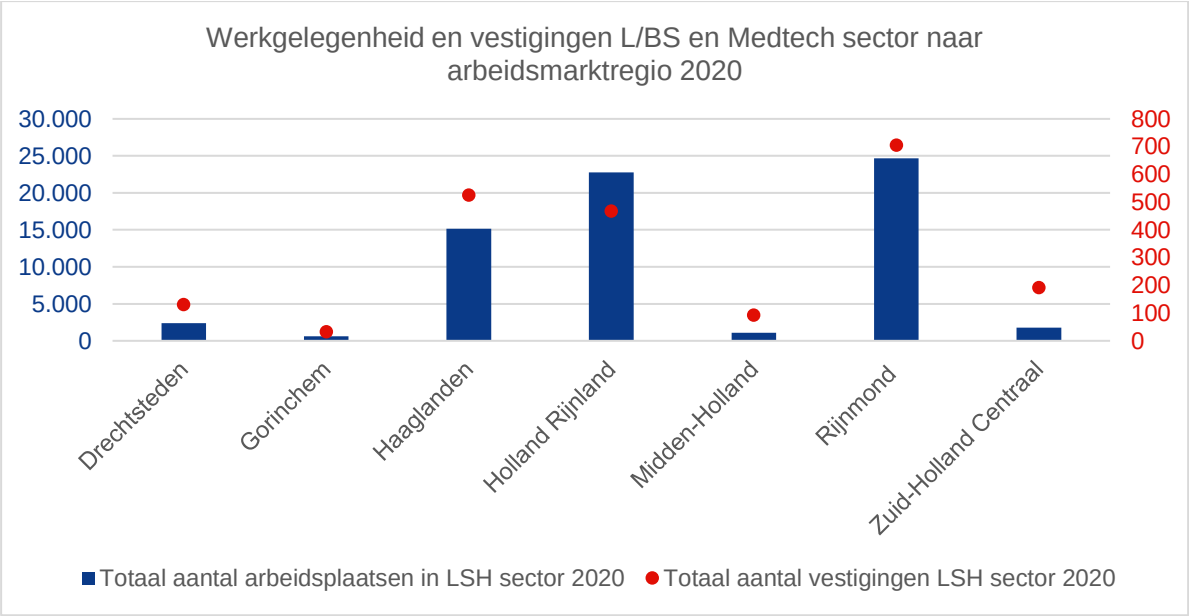


Bron: Zuid-Holland In Zicht (data: LISA)

Indien het aantal vestigingen en aantal werkzame personen uitgesplitst wordt naar de verschillende arbeidsmarktregio's in de provincie Zuid-Holland, blijkt dat het grootste LSH cluster aanwezig is in de regio Holland Rijnland (gemeten als percentage van totaal aantal arbeidsplaatsen en totaal aantal vestigingen in de arbeidsmarktregio), waartoe ook Leiden behoort. Dit cluster is in die regio in de afgelopen 10 jaar ook sterk gegroeid, zowel het aantal vestigingen (+43%) als het aantal arbeidsplaatsen (+23%).

Daarnaast is er in de afgelopen 10 jaar veel dynamiek te zien in de LSH sector in Haaglanden, Gorinchem, Midden-Holland en Zuid-Holland Centraal. Dit komt voornamelijk door een sterke toename in het aantal vestigingen, de groei in het aantal werkzame personen blijft meestal wat achter. Bij de regio's Zuid-Holland Centraal en Midden-Holland is zelfs een afname te zien in het aantal werkzame personen in deze deelsector in de afgelopen 10 jaar.

[2] Om een beeld te kunnen vormen van de opbouw binnen de sector Life- & BioSciences en Medtech worden in de statistieken vier deelsectoren onderscheiden, te weten: onderzoek, onderwijs, verkoop producten en vervaardiging producten. De opbouw van de verschillende deelsectoren in de Life- & BioSciences, Medtech en Zorg aan de hand van SBI-labels wordt weergegeven in bijlage 2.



Bron: Zuid-Holland In Zicht (data: LISA)

Uit onderstaande tabel blijkt dat de Life & BioScience en Medtech sector in de regio Leiden met 9% het grootste aandeel heeft in de totale werkgelegenheid, gevolgd door Rijnmond (inclusief Delft) met 3,6% en Haaglanden met 3,3%.

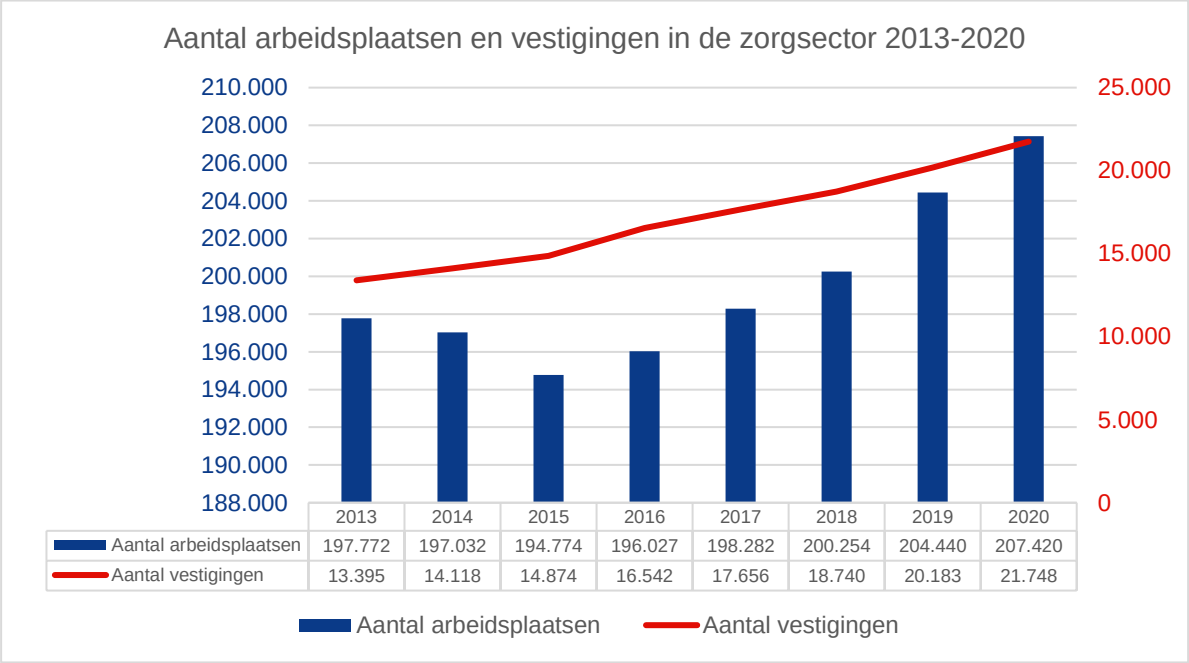
Tabel 2.1 Vestigingen en werkgelegenheid Life-/BioScience en Medtech sector naar arbeidsmarktregio

Arbeidsmarkt-regio	Totaal aantal arbeidsplaat-sen in LS en Medtech sec-tor 2020	Δ% groei t.o.v. 2010	% van totale werkgelegen-heid 2020 (per regio)	Totaal aantal vestigingen LS/Medtech sector 2020	Δ% groei t.o.v. 2010	% van totaal aantal vesti-gingen 2020 (per regio)
Drechtsteden	2.374	-2,1%	1,7%	131	9,2%	0,6%
Gorinchem	621	27,5%	1,5%	33	32,0%	0,4%
Haaglanden	15.131	17,1%	3,3%	525	49,1%	0,6%
Holland Rijnland	22.769	22,7%	9,0%	468	42,7%	0,9%
Midden-Holland	1.107	-10,4%	1,3%	93	24,0%	0,5%
Rijnmond	24.678	3,4%	3,6%	705	18,1%	0,6%
Zuid-Holland Centraal	1.781	-14,2%	1,3%	192	50,0%	0,6%
Provincie Zuid-Holland	**68.461**	**11,2%**	**3,8%%**	**2.147**	**32,1%**	**0,6%**

Bron: Zuid-Holland In Zicht (data: LISA)

2.3 Ontwikkelingen van de zorgsector

Aangezien veel LSH-bedrijven toeleveranciers en klanten/afnemers hebben in de algehele zorgsector wordt de dynamiek van deze sector ook nader belicht. In 2020 zijn er totaal 21.748 vestigingen met 207.420 arbeidsplaatsen aanwezig in de zorgsector. Ten opzichte van 2013 is de totale werkgelegenheid gemeten in het aantal arbeidsplaatsen tot 2020 toegenomen met slechts 5%, terwijl het aantal vestigingen in dezelfde periode is gestegen met 62%.



Bron: Zuid-Holland In Zicht (data: LISA en regionale vestigingsregisters)

Indien het aantal vestigingen en aantal werkzame personen uitgesplitst wordt naar de verschillende arbeidsmarktregio's in de provincie Zuid-Holland, blijkt dat in absolute getallen het grootste zorgcluster in de provincie Zuid-Holland aanwezig is in de regio Rijnmond. In totaal zijn er in die regio Rijnmond in 2020 7.580 organisaties actief die gezamenlijk ruimte bieden aan 79.595 arbeidsplaatsen. De arbeidsmarktregio's Haagland en Holland Rijnland zijn twee regio's die na de regio Rijnmond de meeste vestigingen en werkzame personen hebben in de zorgsector.

Bron: Zuid-Holland In Zicht (data: LISA en regionale vestigingsregisters)

2.4 Conclusie

De LSH-sector in Zuid-Holland is een omvangrijke sector met in totaal circa 23.900 bedrijven en instellingen en ruim 275.000 arbeidsplaatsen. Hiervan behoort 9% van de vestigingen tot de Life-/BioScience en Medtech bedrijvigheid en 91% tot de zorg. Deze Life-/BioScience en Medtech bedrijvigheid neemt bijna 25% van de totale werkgelegenheid in de LSH in Zuid-Holland voor haar rekening. De sector bestaat uit een groot aantal deelsectoren, met elk hun eigen waardeketens van toeleveranciers, dienstverleners, co-producenten en afnemers/eind-gebruikers.

Hoofdstuk 3 Cyberweerbaarheid in de LSH-sector

3.1 Resultaten interviews

Cyberweerbaarheid belangrijk, maar ….

In de interviews met betrokken partijen wordt het belang van cyberweerbaarheid voor de LSH-sector breed onderkend. De sector werkt met grote hoeveelheden data van patiënten, medische processen en onderzoek, die optimaal moeten worden beschermd. Bij de zorg gaat het daarbij vooral om privacy en veilige uitwisseling van persoonsdata. Bij bedrijven en onderzoeksinstellingen gaat het daarnaast om bescherming van concurrentiegevoelige data. De hacks die afgelopen jaren bij onder meer Universiteit Maastricht (eind 2019), bedrijven (o.a. in haven) en gemeenten plaatsvonden waren voor velen een belangrijke wake-up call om ook naar de eigen cyberweerbaarheid te kijken. Nu digitale criminaliteit een steeds groter aandeel in de totale criminaliteit vormt en er steeds meer ruchtbaarheid wordt gegeven aan bedrijven en instellingen die getroffen worden door cybercrime, neemt ook binnen deze sector de aandacht voor het tegengaan van cyberdreigingen toe. Maar tegelijkertijd vormt cybercrime voor een aanzienlijk deel van de sector een ‘ver van het bed’ fenomeen, omdat het belang van de data en de kwetsbaarheid van de eigen organisatie vaak niet worden erkend. Bedrijven en instellingen binnen de sector lopen sterk uiteen in mate van digitalisering, de kwetsbaarheid voor cyberaanvallen resp. hun bewustzijn van de dreiging.

Kleinere bedrijven en instellingen vaak (on)bewust onbekwaam

De respons van de bijna 20 benaderde bedrijven op het verzoek om een interviews was laag. De grote en innovatieve bedrijven gaven aan hun systemen op orde te hebben, hetgeen bijvoorbeeld wordt bevestigd via een ISO27001 en/of NEN7510 certificering. De veiligheidsstandaarden voor o.a. medicijnontwikkeling en medische technologie liggen hoog en dit uit zich ook in een hoog bewustzijn van mogelijke cyberdreigingen. Ook is een deel van de bedrijven onderdeel van een multinational, die hoge standaarden hanteert om in verschillende markten (waaronder de USA) te kunnen opereren. Deze hoge eisen worden door vertaald naar toeleveranciers, maar bijvoorbeeld ook naar stagiairs.

Daarentegen onderkennen veel kleinere bedrijven en zorginstellingen het belang van cyberweerbaarheid lang niet altijd. Een deel van hen vertaalt de dreiging louter in bescherming van persoonsgegevens: “We voldoen aan AVG, dus hebben de systemen op orde.” Bovendien

wordt de waarde van hun data vaak onderschat: “Wie zou er nu geïnteresseerd zijn in onze data? Ook hebben veel bedrijven en instellingen geen idee van de kosten van bijvoorbeeld een dag niet functioneren door een cyberaanval, zowel in euro’s, noch in het bedienen van hun patiënten of klanten. Deze bedrijven en instellingen zijn ‘onbewust onbekwaam’ en dienen via voorlichting en eenvoudige doorlichtingen meer bewust te worden gemaakt van mogelijke cyberdreigingen.

Een ander deel van de bedrijven erkent haar kwetsbaarheid, maar weet in de praktijk niet waar te beginnen: “We moeten er iets mee, maar wat ….?” Ze zijn nauwelijks in staat om hun vragen goed te articuleren en bijpassende ondersteuning te zoeken. Vaak wordt de IT-staf gevraagd de beveiliging op orde te brengen, terwijl de kwetsbaarheid niet louter in de techniek zit, maar vooral in de gebruikers. Een omvattend en breed gedragen beleid met continue aandacht voor het tegengaan van cyberdreigingen ontbreekt. Sommige van de ‘bewust onbekwame’ geïnterviewden hebben wel belangrijke stappen gezet in het voorkomen van cybercrime, maar vonden hun aanpak niet efficiënt: “We hebben zelf het wiel uitgevonden, terwijl andere bedrijven om de hoek waarschijnlijk nuttige voorbeelden en tips hadden kunnen geven. Een laagdrempelige omgeving voor kennisuitwisseling zou ons erg hebben geholpen.” Tot slot maken veel kleinere bedrijven een kosten-baten afweging: “We kunnen niet alles tegelijk oppakken en zijn vooral bezig met vernieuwing van onze producten en het uitbreiden van onze klantenkring en daarbij staat cyberweerbaarheid lager op de prioriteitenlijst.”

De geïnterviewde kleinere bedrijven hebben de volgende behoefte aan ondersteuning voor versterking van hun cyberweerbaarheid geuit:

- Best practices van collega’s: waaraan moeten we denken (awareness, vraagarticulatie), hoe wat aanpakken, in welke volgorde en wat zijn betrouwbare toeleveranciers?
- Afweging van investeringen: prioriteiten, risico’s versus kosten, meerjarenplanning
- Inhuur van een parttime medewerker (CISO) uit een pool van betrouwbare aanbieders, die ondersteunt bij het vergroten van de cyberweerbaarheid.
- Binnen uiteenlopende digitale omgevingen faciliteren van een goede afscherming van patiënten data, plus onderhoud van de beveiliging van systemen.
- Inzicht in betrouwbare manieren van data delen binnen open source omgeving.
- Generieke informatie waarop te letten om cybercrime te voorkomen, plus specifieke informatie voor beveiliging van de eigen bedrijfsprocessen.
- Regelmatige informatie over nieuwe bedreigingen.
- Periodieke trainingen van personeel.
- Een protocol c.q. faciliteit (helpdesk, EHBO) voor incident respons (wanneer wat doen).

Nog veel te winnen in de zorg

De aandacht voor cyberweerbaarheid bij zorginstellingen is eveneens sterk wisselend. Grote instellingen hebben hun systemen veelal op orde, hoewel er wel risico’s blijven bestaan door verknoping van uiteenlopende systemen, overdracht van data uit verschillende bronnen en onachtzaamheid van medewerkers vanwege werkdruk en beperkte digitale vaardigheid. Kleinere instellingen, thuiszorg e.d. hebben vaak eenvoudige digitale systemen en zijn relatief

weinig digitaal vaardig en nauwelijks bezig met cyber risico's. Volgens een gesprekspartner is het 'voordeel' van de zorg op het vlak van cyber security de grote pluriformiteit van systemen en opslag van data, waardoor ze deels minder goed verknoopt en kwetsbaar zijn. Tegelijkertijd neemt het aantal computer gestuurde apparaten (meetinstrumenten) en toepassingen (implantaten, etc.) in de zorg exponentieel toe, waardoor professionals en patiënten steeds kwetsbaarder zijn voor cyber incidenten en top veiligheid vereist is. Dit vergt vergaande 'compartimentalisering' van systemen, veilige uitwisselingsmogelijkheden en hoge toegangseisen (multifactor autorisatie). Voor een zorgprofessional betekent dit de noodzaak van een hoog risicobewustzijn, beschikbaarheid over basale vaardigheden en zeer praktische tools om met cyberdreigingen bezig te zijn. Deze zijn in een aanzienlijk deel van de werksituaties nog niet aanwezig. Maar er zijn ook instellingen die intensief samenwerken om de veiligheid van de zorg, ook op het gebied van cyberweerbaarheid, te vergroten, zoals uit het volgende voorbeeld blijkt.

Gezamenlijke aanpak van cyberweerbaarheid
De Samenwerkende Rijnmond Ziekenhuizen (SRZ) hebben in 1972 de handen ineen geslagen om de kwaliteit en veiligheid van de zorg te verbeteren. Eén van de thema's waar SRZ zich op richt, is cyberveiligheid & gegevensbescherming. In dit kader is er een werkgroep voor cybersecurity, waarin door de aangesloten ziekenhuizen samen met partners als gemeente Rotterdam, politie en Z-CERT wordt gewerkt aan kennisuitwisseling, een cyber responsplan en oefeningen om dit plan te toetsen. Knelpunten die de werkgroep in de praktijk tegenkomt, zijn o.a.:

- *Verschillen in techniek (apparatuur, infrastructuur) en software, waardoor kwetsbaarheden uiteenlopen en verschillende oplossingen voor vergelijkbare problemen nodig zijn.*
- *Sterk verschillend digitaal volwassenheidsniveau van betrokken instellingen.*
- *Cyberdreigingen worden niet altijd gesignaleerd en incidenten regelmatig onder de pet gehouden.*
- *Z-CERT levert een 'overkill' aan dreigingsinformatie waarop instellingen niet altijd (adequaat) kunnen reageren.*

Dankzij de inzet van deskundigen uit de verschillende instellingen worden veel problemen voorkomen en heeft men niet echt behoefte aan een nieuw cyberweerbaarheidscentrum. De gesprekspartners geven echter aan wel behoefte te hebben aan:

- *Op maat toegespitste dreigingsinformatie.*
- *Eenduidige toepassing van de GRIP (Gecoördineerde Regionale Incidentbestrijdingsprocedure) systematiek, wanneer de respons moet worden opgeschaald naar een hoger niveau.*
- *Vertaling van het cyber responsplan (volgens bob-systematiek: beeldvorming – oordeelsvorming – besluitvorming) in een handzame infographic/A4 wat wel/niet doen bij incident.*
- *Activiteiten voor bewustwording van eindgebruikers (zorgprofessionals, patiënten).*
- *Toegang tot aanvullende capaciteit en deskundigheid op het vlak van cyberweerbaarheid.*

Bron: Groepsinterview CISO's ziekenhuizen en gemeente Rotterdam

Kennisinstellingen veel eigen expertise en peer learning

Kennisinstellingen als universiteiten, UMC's en hogescholen in Zuid-Holland hebben veel expertise op het gebied van cyberweerbaarheid in huis en leren veel van elkaar in netwerken. Bij de bescherming tegen cybercrime gaat het zowel om bescherming van patiënt-, student-

en medewerkersdata, als om veilige uitwisseling van onderzoeks- en onderwijsgegevens, onder meer in open source systemen.

De ingrijpende hack bij Universiteit Maastricht eind 2019 was voor de meeste instellingen een wake-up call om nog intensiever te gaan werken aan een uitgebreid pakket van maatregelen om de cyberweerbaarheid te vergroten. Hierbij wordt aandacht besteed aan zowel aanscherping van beleid en governance, als aan veilige informatie-uitwisseling binnen en buiten de organisatie, differentiatie in toegang van personeel tot beschikbare functionaliteiten, en verfijning van voorwaarden in contracten met toeleveranciers en afnemers. De meeste instellingen hanteren hierbij een proactieve, 'holistische' benadering, op basis van een meerjarige investeringsagenda. Ze beschikken over 'dedicated' menskracht om systemen continu te verbeteren. Bovendien maken ze bij de uitwerking en implementatie van hun cyberweerbaarheidsstrategie intensief gebruik van de landelijke SURF-organisatie en van collega's (CISO's) van andere universiteiten, UMC's of hogescholen in regio of Nederland met wie ze regelmatig overleggen.

(Semi-)publieke inzet voor LSH-sector versnipperd en weinig bekend

Binnen intermediaire organisaties en grotere gemeenten in Zuid-Holland zijn diverse medewerkers actief voor structuurversterking van de LSH-sector resp. voor de stimulering van initiatieven rond digitalisering en cybersecurity. De communicatie tussen deze sector- en ICT-specialisten is echter – zoals ze zelf aangeven – ad hoc en beperkt. Cyberweerbaarheid staat nog niet prominent op de agenda, noch binnen LSH-versterking/zorginnovatie, maar ook beperkt binnen digitale strategieën. Op initiatief van de provincie is binnen Zuid-Holland recent uitwisseling tussen betrokken medewerkers van gemeenten, kennispartners en intermediairs op het vlak van digitale economie gestart, maar de gezamenlijke aanpak en revenuen moeten zich nog uitkristalliseren.

Landelijk worden door het Nationaal Cyber Security Center (NCSC), onderdeel van het Ministerie van Justitie en Veiligheid, gericht op vitale sectoren en het Digital Trust Center (DTC), onderdeel van het Ministerie van Economische Zaken, gericht op overige bedrijven dreigingsinformatie verstrekt, informatie over beveiligingsmogelijkheden en tools uitgewisseld en advies gegeven. Deze informatie en dienstverlening dringen echter nog weinig door tot de geïnterviewde LSH-bedrijven en instellingen in de regio, zoals blijkt uit uitspraken als: "Niet bekend met DTC" of "Nooit gehoord van Z-CERT" (zie onder). Het landelijke Digital Trust Center is zeer geïnteresseerd in dit initiatief in Zuid-Holland en wil het graag breder promoten.

Sectorale initiatieven cyberweerbaarheid

Op de website van DTC staat een groot aantal sectorale, regionale en brancheorganisatie-samenwerkingsverbanden genoemd. De voor de LSH-sector belangrijkste samenwerkingsverbanden zijn Z-CERT en Digitale Veiligheid in de Zorg.

Stichting Z-CERT is in 2017 door de Nederlandse Vereniging van Ziekenhuizen, Nederlandse Federatie van UMC's en GGZ Nederland opgericht als expertisecentrum op het gebied van cybersecurity in de zorg. Z-CERT heeft specifieke kennis van medische hard- en software, ondersteunt zorginstanties bij een digitaal incident en vergroot de weerbaarheid van de sector op het gebied van cybersecurity. Z-CERT is vooral gericht op grote bedrijven en instellingen (> 250 wp).

Digitale Veiligheid in de Zorg is in 2019 opgericht en wil instellingen helpen om stapsgewijs een solide organisatie op te tuigen voor cyberveiligheid. Het doel is om voor zorg- en ziekenhuis instellingen een digitale standaard te ontwikkelen, met bijbehorend awareness- en opleidingsprogramma waardoor zorginstellingen meer cyberweerbaar worden. In een standaardkaart in de vorm van een infographic staan rollen, verantwoordelijkheden en procedures beschreven. Met elke organisatie onderzoekt Digitale Veiligheid in de Zorg hoe de standaardkaart past in hun eigen situatie. Vervolgens gaan ze de daarin beschreven procedures ook echt testen en scenario's trainen. De standaardkaart bevat een online toolkit met bijvoorbeeld instructies, bellijsten en trainingen. Zo kunnen instellingen er zelf actief mee werken en kunnen ze de jaarlijks werking ervan checken.

Bron: www.digitaltrustcenter.nl/samenwerkingsverbanden

Niet alleen vraag, maar ook aanbod vanuit de regio

Diverse geïnterviewde partijen hebben aangeboden deel uit te gaan maken van het op te zetten cyberweerbaarheidscentrum voor de LSH-sector. Zo geven de betrokken hogescholen aan een grote pool van IT-studenten te kunnen inzetten, die scans kunnen verrichten en/of tijdens stages verbeterprojecten kunnen uitvoeren. Ook gemeenten en intermediairs bieden aan ondersteuning te geven bij programmaonderdelen, onder andere het werven van mogelijk geïnteresseerde bedrijven en instellingen, het organiseren van bijeenkomsten, het verspreiden van informatie en tools, of subsidiëring van initiatieven. Tot slot heeft een start-up een e-learning cursus ontwikkeld gericht op bewustwording van het belang van cybersecurity en basale concepten om ermee aan de slag te gaan.

3.2 Conclusies

De afgelopen decennia is de samenleving steeds verder gedigitaliseerd en zijn digitale technologieën en toepassingen in vrijwel alle aspecten van het leven doorgedrongen. Ook de zorg is in toenemende mate gedigitaliseerd, variërend van hoogwaardige sensoren en informatie-uitwisseling in OK, IC en implantaten (bijvoorbeeld pacemakers) tot wearables en apps om de eigen gezondheid en inspanningen te monitoren. Dankzij snelle manieren om grote hoeveelheden data te verwerken, wordt gerichter onderzoek naar bijvoorbeeld de effectiviteit en bijwerkingen van medicijnen of vaccins mogelijk. Digitalisering biedt ongelofelijke kansen, maar brengt ook risico’s met zich mee, zoals aantasting van privacy, aanvallen op computersystemen, verspreiding van desinformatie (bijvoorbeeld over ziekten) en stelen van concurrentiegevoelige data. De afgelopen jaren zijn de cyberdreigingen fors toegenomen, waarbij het lekken van persoonsdata, de continuïteit van de zorg en het stelen van IP als belangrijkste risico’s worden gezien.

Het belang van cyberweerbaarheid binnen zowel de Life- & BioScience en Medtech als de Zorgsector wordt breed onderkend, maar de benaderde bedrijven waren terughoudend in het aangaan van een gesprek over de mogelijkheden van een gezamenlijke aanpak voor de LSH-

sector. Grote bedrijven zijn vaak – mede door hun buitenlandse moederorganisaties - streng gereguleerd en hebben hun cyberbeveiliging goed op orde. Dit geldt ook voor grote ziekenhuizen en kennisinstellingen, die weliswaar een complexe ICT-architectuur hebben, maar proactief en systematisch aandacht besteden aan beveiliging van hun systemen. Daarentegen is bij veel middelgrote en kleinere bedrijven en instellingen het bewustzijn over cyber risico's laag, of weten ze niet hoe ze dreigingen aan kunnen pakken. Ze schatten de risico's vaak laag in en gaan pas aan de slag als zich een incident voordoet. Dit wordt bevestigd door de eerste resultaten van de nulmeting van Hogeschool Leiden/Haagse Hogeschool. Uit een doorlichting van 9 bedrijven op Leiden BioScience Park blijkt dat ze overschatten hoe weerbaar ze voor cyberaanvallen zijn. Een andere groep bedrijven en instellingen is zich wel bewust van de risico's, maar weet niet hoe hiermee om te gaan. Ze zijn sterk afhankelijk van de kennis van de eigen IT-afdeling of leveranciers, waaraan ze vaak niet de juiste vragen weten te stellen.

Mede door de vergrijzing, sterk toenemende zorgkosten en personeelstekorten is de komende decennia een transitie in de zorg nodig, met meer accent op preventie, zelfredzaamheid en minder zorg in instellingen en meer in de thuissituatie. In deze transitie spelen digitale oplossingen een belangrijke rol. Een randvoorwaarde is dat de digitale uitwisseling van gegevens, verzameling en gebruik van data, en diagnose en behandeling in een uiterst veilige omgeving moeten plaatsvinden. De mate van digitalisering, inschatting van omvang en urgentie van cyber risico's, en de volwassenheid van digitaal risicomanagement lopen binnen de LSH-sector zeer sterk uiteen. Omdat de weerstand tegen dreigingen wordt bepaald door de zwakste schakel in een keten, is een ketenaanpak om de cyberweerbaarheid van de sector te vergroten wenselijk. Deze kan starten met de dominante spelers binnen een waardeketen, maar zal ook moeten kijken naar relevante toeleveranciers, dienstverleners en afnemers. Zo'n ketenaanpak kan deels generieke interventies omvatten min of meer voor alle bedrijven en instellingen gelden, maar zal ook rekening moeten houden met specifieke aspecten van de verschillende deelketens en dus maatwerk vergen.

Deze verkenning laat zien dat in de sector het belang van digitale veiligheid uiterst groot is, maar dat veel kleinere bedrijven en instellingen de risico's als beperkt inschatten of niet weten hoe hiermee om te gaan. De behoefte aan een cyberweerbaarheidscentrum is vaak hooguit latent aanwezig en wordt pas manifest als de gesprekspartners – liefst door collega's ('peers') - gewezen worden op de negatieve consequenties van incidenten voor hun bedrijfsvoering of de mogelijkheden die bestaan om dreigingen tegen te gaan. Vooral kleinere bedrijven en instellingen hebben vaak een slecht beeld hoe ze qua cyberweerbaarheid ervoor staan. Als ze wel bewust zijn van de risico's die ze lopen, weten ze vaak niet hoe ze ermee aan de slag moeten gaan. Er is dus een noodzaak van meer bewustwording van cyber risico's en vervolgens behoefte aan ondersteuning om deze risico's te beperken. In het volgende hoofdstuk wordt ingegaan op de gewenste bouwstenen van een eventueel cyberweerbaarheidsprogramma die door de gesprekspartners zijn aangedragen.

Hoofdstuk 4 Onderdelen cyberweerbaarheidsprogramma LSH sector

Op basis van de gevoerde gesprekken zijn de volgende programma-ideeën voor een cyberweerbaarheidscentrum voor de LSH-sector naar voren gekomen:

1 Stimuleren van ***bewustwording*** over de cyber-risico's die bedrijven en instellingen lopen. Hierbij wordt benadrukt dat cyberweerbaarheid niet alleen een zaak is van de IT-medewerkers, maar van het hele bedrijf vanaf bestuur en management tot en met de werkvloer. Hoewel de mate van digitalisering en kwetsbaarheid in bijvoorbeeld de thuiszorg of huisartsenpraktijk veel geringer is dan van een ziekenhuis, hogeschool of eHealth-bedrijf, zijn de kosten van incident door bijvoorbeeld het niet kunnen leveren van adequate zorg of lekken van persoonsdata ongekend hoog. Bewustwordingsactiviteiten zullen zich moeten richten op zowel partijen die de risico's niet onderkennen (zgn. onbewust onbekwamen) als op bedrijven en instellingen die wel risico's zien, maar niet weten hoe hiermee om te gaan ('bewust onbekwamen'). Deze laatste staan meer open voor de onderstaande activiteiten. Bij de bewustwording kan gebruik worden gemaakt van tal van goede voorbeelden die bijvoorbeeld al door het Digital Trust Center zijn verzameld. Ook voorlichting of peer-to-peer uitwisselingen binnen ondernemersverenigingen kunnen nuttig zijn.
2 Uitrol van een ***basisscan*** voor screening van de digitale zwakten binnen een bedrijf of instelling. Hiervoor kan gebruik worden gemaakt van diverse zelfevaluatie tools van het DTC, maar ook van een beknopte doorlichting door studenten of een externe deskundige.
3 Voor het tegengaan van de geconstateerde zwakten dienen laagdrempelige ***stappenplannen*** beschikbaar te zijn, variërend van een set van maatregelen om een systeem veilig in te stellen tot een protocol hoe te handelen bij een incident.
4 Voor een meer gestructureerde aanpak van digitaal risicomanagement dienen uiteenlopende ***trainingen*** beschikbaar te zijn, variërend van basistrainingen voor uiteenlopende typen medewerkers met generieke aandachtspunten tot op de specifieke bedrijfsvoering gerichte maatwerkoplossingen voor verschillende onderdelen van bedrijf of instelling.
5 Diverse keren werd benadrukt dat zo'n centrum het wiel niet opnieuw moet worden uitgevonden, maar dat het een belangrijke taak is om ***bestaande tools*** toegankelijk maken c.q. te vertalen naar de LSH-sector.
6 Een laagdrempelige vorm van bewustwording en informatievoorziening die wordt gesuggereerd is het stimuleren van ***kennisdeling tussen vergelijkbare bedrijven***, bijvoorbeeld in de vorm van cybercafés met pitches van best practices dan wel vragen die bij een bedrijf leven.
7 Aangezien 'cyber digibeten' moeite hebben om de benodigde informatie op internet te vinden, is een telefonische ***helpdesk*** of chatfunctie voor beantwoording van basale vragen wenselijk.
8 Indien een bedrijf of instelling wordt getroffen door bijvoorbeeld ransomware is het cruciaal om een soort ***EHBO*** ('slachtofferhulp', 'Rapid Respons Functie') te kunnen

raadplegen om te kunnen sparren hoe met dit incident kan worden omgegaan, de effecten zo snel mogelijk te mitigeren en hoe het best hierover te communiceren (voor het tegengaan van imagoschade).

9 Aangezien een cyber dreiging zich niet beperkt tot een bedrijf of instelling zelf, maar ook afkomstig kan zijn van de rest van de keten, is een deskundige ***doorlichting van leverancierscontracten*** of gerelateerde software systemen een wens. In dit kader kunnen ook standaard voorwaarden worden voorgesteld, bijvoorbeeld hoe in inkoopvoorwaarden een eis kan worden opgenomen dat een aanbieder zijn cybersecurity op orde heeft.

10 Aangezien voor veel kleinere bedrijven en instellingen een specialist in cybersecurity geen fulltime functie is, wordt ook gepleit voor het opzetten van een ***pool*** van gekwalificeerde cyber-experts, die organisaties tijdelijk of parttime kunnen inhuren (bijv. parttime Information Security of Privacy Officer).

Om een programma voor vergroting van de cyberweerbaarheid in de LSH-sector van de grond te trekken, is in eerste instantie externe financiering nodig. Omdat veel bedrijven en instellingen zich niet bewust zijn van de risico's en – als ze zich dat wel zijn – vaak niet weten waar te beginnen, zullen ze pas bereid zijn tot betaling voor diensten als de waarde ervan duidelijk is. Een opstartfase mede gefinancierd door de overheid, lijkt dan ook onvermijdelijk. Tijdens deze opstartfase zullen andere vormen van financiering moeten worden gezocht om het programma toekomstbestendig te maken, bijvoorbeeld in de vorm van abonnementen met uiteenlopende service pakketten. Ook kan worden gekeken naar de rol van verzekeraars hierbij.

Hoofdstuk 5 Conclusies en aanbevelingen

5.1 Conclusies

De Life Sciences & Health sector is met bijna 24.000 vestigingen en 275.000 werkzame personen een omvangrijke en belangrijke sector in Zuid-Holland. Hiervan behoort ruim 90% van de vestigingen en 75% van de arbeidsplaatsen tot de zorg, terwijl de rest wordt gevormd door Life- & BioScience en Medtech bedrijvigheid. Tussen en binnen deelsectoren bestaan grote verschillen in activiteiten, waardeketens en geografische reikwijdte.

Zo neemt Zuid-Holland (en met name Leiden en Rotterdam) een vooraanstaande positie in qua wetenschappelijk onderzoek en ondernemerschap op het vlak van Life- & BioSciences. Deze sector is sterk internationaal georiënteerd, zeer kennisintensief en data- en IP-gedreven, met hoge veiligheidseisen en een intensieve ketensamenwerking tussen innovatieve start-ups, toeleverend MKB en grote multinationals. Ook op het gebied van Medtech is de regio (o.a. rond Delft) (inter-)nationaal toonaangevend.

De sector is sterk gedigitaliseerd en het belang van digitale technologieën en toepassingen neemt exponentieel toe. De digitale volwassenheid binnen de sector is echter zeer verschillend, hetgeen onder andere blijkt uit het omgaan met cyber dreigingen. Terwijl de grote bedrijven en instellingen zich terdege bewust zijn van de risico's en veel investeren om hun weerbaarheid op orde te brengen en houden, zijn veel kleinere partijen daar nauwelijks mee bezig. Hen ontbreekt het aan bewustzijn, kennis, menskracht en middelen om dreigingen te onderkennen resp. ze het hoofd te bieden. Voor veel van deze bedrijven en instellingen zou een cyberweerbaarheidsprogramma een belangrijke rol kunnen spelen, maar ze zijn vaak moeilijk te bereiken of weten niet wat ze moeten doen. De respons van bedrijven en zorginstellingen om mee te doen aan deze verkenning is dan ook laag.

Een conclusie van deze verkenning zou kunnen zijn dat er bij bedrijven en instellingen uit de LSH-sector geen draagvlak bestaat om met cyberweerbaarheid aan de slag te gaan. Daarentegen kan ook worden geconcludeerd dat cyber security voor bedrijven en instellingen in deze sector juist heel belangrijk is en steeds relevanter wordt om veilig (medische) informatie uit te wisselen, de privacy van patiënten en medewerkers te borgen, en IP van innovatieve producten te beschermen. Gezien het maatschappelijke en economische belang van deze sector voor de provincie en Nederland, is het van belang om te pogen de latent aanwezige behoefte aan ondersteuning om de cyberweerbaarheid te verbeteren door samen met koplopers een programma op te zetten en in de praktijk onder kleinere bedrijven en instellingen te testen. Daarbij moet worden onderkend dat de LSH-keten veel gevarieerder en complexer is dan bijvoorbeeld de tuinbouw/Greenport waar eerder een programma voor is opgezet. Dit

houdt in dat in zo'n programma gerichter wordt gekeken naar relevante deelsectoren/ketens, waarin ondersteuning het meest urgent is c.q. de meeste impact kan hebben.

5.2 Aanbevelingen

Voor de start van een succesvol programma om de cyberweerbaarheid in de LSH-sector te versterken, is het van belang om gestructureerd te werk te gaan door:

1 'Bottom-up' te starten met een kerngroep van een aantal koplopers uit de sector die belang heeft bij een gestructureerde aanpak om de cyberdreigingen te reduceren en wil fungeren als meedenker en ambassadeur van een toegespitst cyberweerbaarheidsprogramma. Deze kunnen komen uit de nulmeting van Hogeschool Leiden/Haagse Hogeschool en uit andere geïnteresseerde MKB'ers uit bestaande regionale netwerken.
2 Tegelijkertijd 'top down' te beginnen met het identificeren van koplopers en mogelijk geinteresseerde partijen in relevante deelketens, die specifiek worden benaderd met een toegespitst aanbod.

Via deze bottom-up en top down aanpak wordt gedurende een proefperiode van 2-3 jaar een laagdrempelig programma voor kleinere bedrijven en instellingen ontwikkeld, waarbij zoveel mogelijk gebruik wordt gemaakt van bestaande voorbeelden en tools van onder andere DTC, studenten en docenten van de aanwezige hogescholen en goede voorbeelden van bedrijven en instellingen zelf. Dit programma bestaat voor een aanzienlijk deel uit generieke informatie en tools die voor alle sectoren gelden, maar daarnaast ook uit op de LSH-sector en specifieke deelsectoren toegespitste interventies en maatwerkoplossingen.

Belangrijke aandachtspunten tijdens de startfase van het cyberweerbaarheidscentrum voor de LSH-sector zijn:

- Het bereiken van een aanzienlijk deel van de potentiële doelgroepen. Hierbij gaat het niet om de zorg als geheel, maar ligt de focus op nog niet bediende deelsectoren, waaronder R&D- en services bedrijven binnen de Life-/BioScience en Medtech.
- Een kosteneffectieve inzet van tools en instrumenten door aanpassing van bestaande aan de situaties in de LSH-sector.
- Het uitwerken van een financieringsvorm voor de voortzetting van het programma met een evenredige verdeling van de kosten over de verschillende typen belanghebbenden.

Bijlage 1 Geïnterviewde organisaties

A Bedrijven en instellingen
- Start-ups (3)
- Biopartner Leiden
- Samenwerkende Ziekenhuizen Rijnmond
- Non-respons: 14

B Kennisinstellingen
- Universiteit Leiden
- LUMC (2)
- CHDR
- Hogeschool Leiden (2)
- Hogeschool Rotterdam
- CIV BioScience
- Externe deskundige

C Intermediairs
- Innovation Quarter
- Medical Delta
- Stichting Leiden BioScience Park
- Ondernemersverenging BioScience Park
- The Hague Tech
- Digital Trust Center

D Overheden
- Ministerie EZK
- Provincie Zuid-Holland
- Gemeente Leiden
- Gemeente Rotterdam (2)
- Gemeente Den Haag (2)

Bijlage 2 Afbakening Life- & BioScience en Zorg sector

Life- & BioSciences en Medtech sector

Onderzoek

1 Biotechnologisch speur- en ontwikkelingswerk op het gebied van agrarische producten en processen.
2 Biotechnologisch speur- en ontwikkelingswerk op het gebied van medische producten en farmaceutische processen en van voeding.
3 Biotechnologisch speur- en ontwikkelingswerk voor overige toepassingen.
4 Speur- en ontwikkelingswerk op het gebied van gezondheid en voeding (niet biotechnologisch).
5 Medische laboratoria, trombosediensten en overig behandelingsondersteunend onderzoek.

Verkoop producten:

1 Groothandel in farmaceutische producten.
2 Groothandel in medische en tandheelkundige instrumenten, verpleeg- en orthopedische artikelen en laboratoriumbenodigdheden.

Vervaardiging producten

1 Apotheken.
2 Vervaardiging van farmaceutische grondstoffen.
3 Vervaardiging van farmaceutische producten (geen grondstoffen).
4 Vervaardiging van meet-, regel-, navigatie- en controleapparatuur.
5 Vervaardiging van bestralingsapparatuur en van elektromedische en elektrotherapeutische apparatuur.
6 Vervaardiging van optische instrumenten en apparatuur.
7 Vervaardiging van medische instrumenten en hulpmiddelen (geen tandtechniek).

Onderwijs

1 Middelbaar beroepsonderwijs.
2 Volwassenen onderwijs.
3 Niet-universitair hoger onderwijs.
4 Universitair hoger onderwijs.
5 Universitair medische centra.

Zorg sector

1 Ziekenhuizen.
2 Geestelijke gezondheids- en verslavingszorg.
3 Medische en tandheelkundige praktijken.
4 Paramedische praktijken.
5 Overige gezondheidszorg.