Verhogen cyberweerbaarheid bij bedrijven in de Zuid-Hollandse maakindustrie

Verkenning in opdracht van Security Delta (HSD) en met ondersteuning van Metropoolregio Rotterdam Den Haag (MRDH)

HSD

securitydelta.nl

Verhogen cyberweerbaarheid bij bedrijven in de Zuid-Hollandse maakindustrie

Verkenning in opdracht van Security Delta (HSD) en met ondersteuning van Metropoolregio Rotterdam Den Haag (MRDH).

30 mei 2022

Verkenning uitgevoerd door ir. Erik Knol (Qeam) in opdracht van Security Delta (HSD).

Citatiesuggestie: Knol, E. (2022). *Verhogen cyberweerbaarheid bij bedrijven in de Zuid-Hollandse maakindustrie.* Verkenning in opdracht van Security Delta (HSD) en met ondersteuning van Metropoolregio Rotterdam Den Haag (MRDH).

Inhoudsopgave

1. Inleiding

Deze notitie vormt een onderdeel van het programma ‘Sectoraal digitaal veilig’ dat tot doel heeft om de cyberweerbaarheid (digitale weerbaarheid) van organisaties in zes essentiële sectoren in de regio Zuid-Holland te vergroten: life sciences en health, water, logistiek, maakindustrie, maritiem / haven en lucht- en ruimtevaart. Het programma is een initiatief van Security Delta (HSD)[1] mede op basis van voorbereidingen[2] en wordt mede mogelijk gemaakt door de Metropoolregio Rotterdam Den Haag (MRDH).

Deze notitie is het resultaat van een beknopte verkenning naar cyberweerbaarheid in de maakindustrie in Zuid-Holland. Een twintigtal organisaties heeft informatie aangereikt voor deze verkenning via telefonische/online gesprekken. Het overgrote deel van de betrokken organisaties zijn bedrijven gevestigd in de regio Zuid-Holland. Het gaat daarbij om zowel kleine bedrijven, middelgrote bedrijven als grote bedrijven. Bijlage 1 geeft een geanonimiseerd overzicht van de betrokken organisaties.

Het doel van de notitie is om vervolgstappen op het vlak van cyberweerbaarheid in de regionale maakindustrie scherper te krijgen. De notitie heeft de volgende aandachtspunten: 1) maakindustrie in Zuid-Holland, 2) digitale veiligheid en de maakindustrie, 3) reflecties t.a.v. het ondersteunen van maakbedrijven in Zuid-Holland met digitale weerbaarheid en 4) conclusies en aanbevelingen.

Om minder ingevoerde lezers op het vlak van maakindustrie en/of cyberweerbaarheid mee te nemen, is gekozen om deze onderwerpen hier en daar uitvoeriger te beschrijven en/of te ondersteunen met additionele informatie in de bijlagen (bijvoorbeeld van het Digital Trust Center en Cyber Kracht).[3]

[1] Security Delta (2021), Sectoraal digitaal veilig: een regionale aanpak.

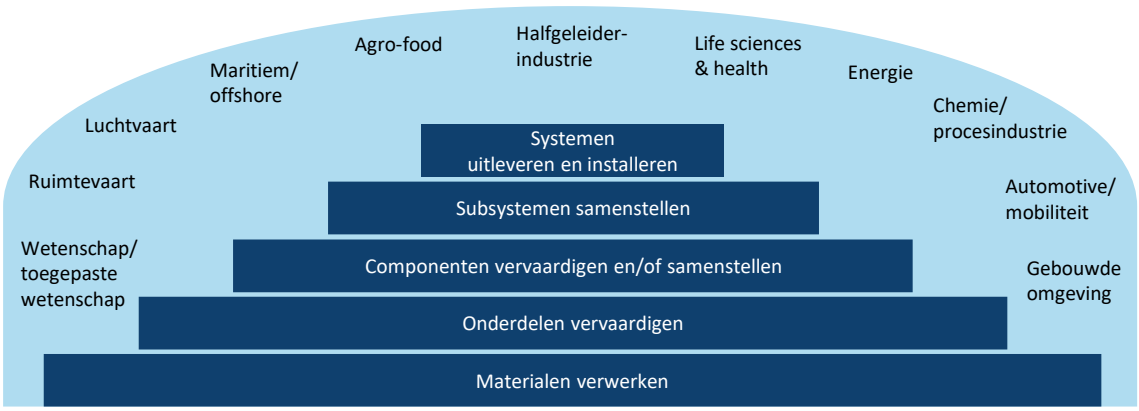
[2] Zie publicatie van de Provincie Zuid-Holland en de Economic Board Zuid-Holland.: 1) Roadmap Verbeteren Weerbaarheid Digitale Economie en 2) Cybergereedheid economie provincie Zuid-Holland: een strategische luchtfoto en handelingsperspectief.

[3] Het Digital Trust Center (DTC), onderdeel van het ministerie van Economische Zaken en Klimaat, heeft als missie om Nederlandse bedrijven weerbaarder te maken tegen digitale dreigingen. Activiteiten zijn o.a. het uitwisselen van kennis (via de website www.digitaltrustcenter.nl), het ontwikkelen en aanreiken van instrumenten (o.a. controlelijsten en Basisscan Cyberweerbaarheid), het stimuleren van samenwerking en het delen van dreigingsinformatie met individuele bedrijven.

2. Maakindustrie in Zuid-Holland

2.1 Wat omvat de maakindustrie?

Bedrijven in de maakindustrie vormen een subset van de totale industriesector en deze beslaat binnen deze verkenning: basismetaalindustrie (SBI24)[4], metaalproductenindustrie (SBI25), elektrotechnische industrie (SBI26), elektrische apparatenindustrie (SBI27), machine-industrie (SBI28), auto- en aanhangwagenindustrie (SBI29), overige transportmiddelenindustrie (SBI30) en reparatie en installatie van machines (SBI33). Deze indeling van de maakindustrie wordt veelvuldig gebruikt in onderzoeken en inventarisaties (zie ook bijlage 2).



Figuur 1: Schematische weergave van de keten van de maakindustrie (van materiaalverwerking tot het samenstellen en uitleveren van systemen) en voorbeelden van sectoren die worden gediend door de maakindustrieketens.

Bedrijven in de maakindustrie maken onderdeel uit van diverse ketens die een veelheid aan sectoren bedienen. Figuur 1 geeft een versimpelde impressie van de keten van de maakindustrie: van verwerken van materialen tot het uitleveren en installeren van systemen. De diversiteit aan producten en activiteiten is zeer groot: veren (stansen, lasersnijden, draadbuigen), metalen trappen (lasersnijden, lassen, poedercoaten), industriële elektronica (ontwerpen, printplaten bestukken, schakelkasten bouwen, assembleren, sensoren en actuatoren configureren), mechatronica-systemen (ontwerpen, simuleren, (laten) fabriceren van componenten, componenten reinigen, assembleren in cleanrooms, instellingen configureren, integreren met andere systemen) etc. Figuur 1 geeft ook een niet-uitputtende indruk van sectoren die door de maakindustrieketens bediend worden.

2.2 Verschillende type bedrijven in de maakindustrie

Bedrijven in de maakindustrie zijn divers kijkend naar verschillende dimensies zoals:

- Omvang van de maakbedrijven: micro, klein, middelgroot en groot.[5]
- Aard van de producten en diensten van de bedrijven: producerende bedrijven (enkelstuks, kleine series, grote series), system suppliers (neemt verantwoordelijkheid op het gebied

[4] De SBI-codering (standaard bedrijfsindeling) is opgesteld door het Centraal Bureau voor Statistiek (CBS).

[5] Microbedrijf: minder dan 10 medewerkers; kleinbedrijf: tussen 10 en 50 medewerkers; middenbedrijf: tussen 50 en 250 medewerkers; grootbedrijf: meer dan 250 medewerkers. Zie ook bijlage 3.

van productontwikkeling, procesontwikkeling, serieproductie en end of life management) en OEM-bedrijven (original equipment manufacturer: zelfscheppende bedrijven die eigen producten in de markt zetten; voorbeelden: Berg Hortimotive, Lely, ASML en Vanderlande).

- Positie van de bedrijven in de keten(s): OEM-bedrijf, tier 1, tier 2 en tier 3 toeleveranciers.
- Mate van vernieuwingsgezindheid van de bedrijven: koplopers, ontwikkelaars en toepassers.
- Mate van aandacht voor duurzaamheid en circulariteit door de bedrijven.[6]
- Mate en wijze van organisatie van IT/OT[7] en cyberweerbaarheid door de bedrijven: voorbeelden van relevante instrumenten en normen zijn de 5 basisprincipes van veilig digitaal ondernemen (Digital Trust Center; zie bijlagen 4 en 6), ISO 9001, ISO 27001 / ISO 27002 niveaus, CIS Controls niveaus en IEC 62443.[8]

2.3 Maakindustrie in Zuid-Holland

De maakindustrie in de regio Zuid-Holland is omvangrijk en levert belangrijke bijdragen aan regionale, nationale en internationale ketens die te relateren zijn aan onder meer logistiek (o.a. transportwerktuigen en -middelen), maritiem/offshore (o.a. onderdelen van en apparatuur voor schepen en offshore installaties), lucht- en ruimtevaart (o.a. constructieonderdelen en communicatie- en observatie-apparatuur), halfgeleiderindustrie (o.a. inspectie-apparatuur), medisch (o.a. beeld-vormende apparatuur) en agro-food (o.a. regelsystemen en robotica-oplossingen).[9]

In Nederlandse industrie zijn circa 950.000 personen werkzaam, waarvan ongeveer 420.000 werkzaam in de maakindustrie.[10] Ongeveer 65.000 personen zijn werkzaam in de Zuid-Hollandse maakindustrie. Een zeer groot deel daarvan werkt bij zogenaamde microbedrijven (bedrijven met minder dan 10 medewerkers). Circa 87% van de bedrijven in de maakindustrie zijn microbedrijven. Zie bijlage 3.

Ruim 7.100 bedrijfsvestigingen in Zuid-Holland zijn onderdeel van de maakindustrie en dat is circa 20% van het totaal aantal bedrijfsvestigingen in de Nederlandse maakindustrie. Binnen de Zuid-Hollandse maakindustrie is de metaalproductenindustrie sterk vertegenwoordigt: ruim 3.350 bedrijfsvestigingen. Zie bijlage 3.

De metaalproductenindustrie (SBI25) - het grootste segment in de Zuid-Hollandse maakindustrie qua aantal vestigingen - is sterk vertegenwoordigt onder de leden van de brancheverenigingen

---

[6] TNO (2021), *De impact van slim èn circulair: hoe innovaties in de maakindustrie bijdragen aan een lagere footprint*.

[7] IT is de afkorting voor informatietechnologie en staat in nauw verband met ICT (informatie- en communicatie-technologie). OT is de afkorting van operationele technologie en omvat systemen die worden gebruikt voor het beheer van operationele processen zoals het aansturen en monitoren van (industriële) apparatuur. Nauw verwant zijn ICS (industrial control systems) en SCADA (supervisory control and data acquisition).

[8] ABB (2021), *Differentiation of the IT security standard series ISO 27000 and IEC 62443: a view of automation systems in the manufacturing and process industries*.

[9] Zie o.a. PZH-EBZH (2019), *Van investeren in Zuid-Holland plukt Nederland de vruchten: het Zuid-Hollandse perspectief op missiegedreven innovatiebeleid*. EBZH-MRDH (2021), *Groeiagenda Zuid-Holland*. PZH (2021), *Programma Zuid-Hollandse economie 2021-2025*. MRDH (2022), *Strategische agenda Metropoolregio Rotterdam Den Haag*.

[10] CBS (2022). Diverse statistische gegevens van het Centraal Bureau voor de Statistiek, https://opendata.cbs.nl/statline.

Koninklijke Metaalunie. De spreiding van deze leden in de regio Zuid-Holland (bijlage 3) laat zien dat de metaalproductenindustrie sterke clusters heeft in het Westland, Groot Rotterdam, Drechtsteden en Hoekse Waarde & Goeree-Overflakkee. In de regio Groot Den Haag is de maak-industrie ook sterk vertegenwoordigd met daarbij nadruk op geavanceerde materialen, meet- en detectietechnologie, ruimtevaart en onderhoud & reparatie.[11]

In Zuid-Holland zijn veel maakbedrijven verbonden aan of onderdeel van de ketens van de regionale maritieme clusters[12] en de regionale horticultuursector.[13]

De maakindustrie in de regio Zuid-Holland is verweven met regionale innovatiebevorderende initiatieven zoals fieldslabs en publiek-private samenwerkingen (PPS).[14] Diverse regionale fieldlabs zijn verbonden aan het smart industry programma van Zuid-Holland SMITZH.

Voorbeelden van regionale fieldlabs zijn Big Data Innovatiehub (o.a. digitale veiligheid), Digital Factory Composites (opschaling composietenproductie), Dutch Growth Factory (digitalisering en verduurzaming van de maakindustrie), Dutch Optics Centre (DOC; opto-mechatronica), Duurzaamheidsfabriek (o.a. maritieme automatisering), RAMLAB (3d printing), RoboHouse (robotica), SAM|XL (productie van lichtgewicht (composiet)constructies) en SMASH (slim onderhoud van schepen).

Enkele relevante PPS-en op het vlak van leven lang ontwikkelen relevant voor de Zuid-Hollandse maakindustrie zijn Civ Maintenance en Procestechniek Rijnmond, Civ Smart Technology, Expertise Centrum Precisietechniek, High Tech Centre Delft, Leidse instrumentmakers School (o.a. instrumentatie voor ruimtevaart en -onderzoek, medische precisietechniek), Maritiem Techplatform, Masterplan Techniek Zuid-Holland en RDM Centre of Expertise.

[11] Birch (2019), *Versterking economische structuur: achtergrond, analyse en beleidsopties voor de gemeente Den Haag*.

[12] Ecorys (2020), *Nederlandse maritieme cluster: monitor 2020*. InnovationQuarter (2021), *Regionale maritieme agenda: Zuid-Holland 2030*.

[13] LEI Wageningen UR (2021), *Tuinbouwtoeleveranciers: veroveren de wereld: resultaten enquête onder AVAG Plus-leden*. TNO (2019), *Samen innoveren in de glastuinbouw*.

[14] Zie o.a. PZH et al. (2017), *Slim gemaakt in Zuid-Holland* - een gezamenlijke publicatie van Provincie Zuid-Holland, InnovationQuarter, Kamer van Koophandel, TNO, FME, Metaalunie en de Gemeente Delft. PBT (2018), *Regioanalyse Zuid-Holland: een sterkere provincie door vernieuwende publiek-private samenwerking in het beroepsonderwijs*.

3. Digitale veiligheid en de maakindustrie

3.1 Waarom is digitale veiligheid relevant in de maakindustrie?

De afgelopen decennia hebben ontwikkelingen op het vlak van informatietechnologie en productie-automatisering de productiviteit in de Nederlandse maakindustrie aanzienlijk verhoogd. Tevens maakten deze technologieën het mogelijk om als maakindustrie meer complexe onderdelen, componenten en systemen te ontwikkelen en te vervaardigen. Dit laatste is onder andere goed te zien in de ketens die bijdragen leveren aan de realisatie van geavanceerde systemen (lithografie-machines van ASML, elektronenmicroscopen van Thermo Fisher Scientific, metrologiesystemen van Nearfield Instruments, hijsoplossingen van Huisman Equipment en melkveehouderijsystemen van Lely).

Digitale veiligheid (cyberweerbaarheid) heeft een hoge relevantie voor bedrijven actief in de maakindustrie. In zijn algemeenheid kan gesteld worden dat het aantal cyberdreigingen met de jaren is toegenomen. Uit de interviews blijkt dat het cyberdreigingsniveau als hoog tot zeer hoog wordt omgeschreven voor de maakindustrie. Dit heeft te maken met het feit dat cybercriminelen steeds meer en laagdrempelige instrumenten tot hun beschikking hebben (ransomware-as-a-service, brute-kracht-aanvallen, gerichte aanvallen en reeds gehackte (toegangs)informatie beschikbaar op 'ondergrondse' fora) om cyberaanvallen uit te voeren en/of resultaten van eerdere cyberaanvallen van anderen crimineel te gebruiken.[15]

Cyberincidenten zijn zeer frustrerend voor bedrijven in de maakindustrie en voor OEM-bedrijven die sterk afhankelijk zijn van de toeleverende maakindustrie:

1. Ondermijnen van de bedrijfscontinuïteit door IT-systemen (tijdelijk) plat te leggen (chantage en het eisen van losgeld)
2. Ontvreemden van intellectueel eigendom door in te breken in IT-systemen (technische tekeningen, software, broncode, data)
3. Ondermijnen of ontvreemden van specifiek data- en/of informatieverkeer (bijvoorbeeld geautomatiseerd dataverkeer van technische systemen tussen klant en OEM-bedrijf)
4. Verzwakken van het imago van het bedrijf vanwege cyberincidenten.

Door de hoge mate van ketenintegratie zijn steeds meer bedrijven in de maakindustrie digitaal met elkaar verbonden. *"Gaandeweg lijkt het alsof we meer een IT-bedrijf zijn geworden, dan een verspaningsbedrijf"*, aldus een geïnterviewd directielid van een middelgroot verspanend bedrijf. De sterke afhankelijkheid van digitale informatie-uitwisseling (binnen de bedrijfsgrenzen en daarbuiten) betekent dat cyberveiligheid en cyberweerbaarheid niet alleen het domein is van één bedrijf, maar steeds meer het domein is van samenwerkende bedrijven in de keten. Een voorbeeld: technische tekeningen van een geavanceerd component van een hightech systeem – waar intellectueel eigendom op berust – wordt door meerdere schakels in de toeleverketen digitaal gedeeld, opdat uiteindelijk een specialistisch maakbedrijf die componenten vanaf tekening kan gaan maken. Het is zaak dat de gehele keten voldoende maatregelen neemt om te zorgen dat die technische tekeningen digitaal veilig worden gedeeld, gebruikt en opgeborgen. Een relevante ontwikkeling in de maak-industrie is het Smart Connected Supplier Network (SCSN) dat zich richt op de (technische) uitrol van digitaal berichtenverkeer in de toeleverketen.[16]

[15] Group IB (2021), *Hi tech crime trends*.

[16] https://smart-connected.nl/_asset/_public/SCSN-Technology-Update-Brainport-Industries-20200514.pdf.

3.2 Drie gebieden van digitale veiligheid bij bedrijven actief in de maakindustrie

Binnen de maakindustrie en bij OEM-bedrijven sterk afhankelijk van de maakindustrie zijn op globaal niveau drie gebieden van digitale veiligheid te onderscheiden: 1) informatietechnologie, 2) productie-systemen en productieautomatisering en 3) producten met digitale netwerkverbindingen.[17]

1. Informatietechnologie

Digitale veiligheid t.a.v. informatietechnologie (IT) heeft voor een groot deel te maken met het digitaal veiliger maken van 'kantoorsystemen': ERP-systemen, administratiesystemen, salaris-systemen, emailservers, webservers, netwerksystemen, CAD-software, CAM-software, simulatie-software etc. Over het algemeen hebben fabrikanten van IT-systemen en software veel aandacht voor digitale veiligheid en bieden periodiek de nodige updates en nieuwe versies aan om de systemen digitaal veilig te houden.

2. Productiesystemen en productieautomatisering

Digitale veiligheid t.a.v. van operationele technologie (OT) heeft de maken met productiesystemen die gaandeweg steeds meer verbonden worden met digitale netwerken en IT-systemen: draai- en freesmachines, draadvonksystemen, lassystemen, robotinstallaties, transportsystemen, meet-instrumenten etc. Productiesystemen zijn vele jaren in gebruik en brengen met de jaren meer digitale veiligheidsrisico's met zich mee omdat de ingebouwde hardware en software (tot voorkort) relatief weinig digitale update/upgrade-aandacht kregen of kon krijgen van fabrikanten. Echter, OT krijgt steeds meer aandacht van maakbedrijven en het zoeken naar de meest optimale digitale veiligheid staat bij maakbedrijven en fabrikanten van productiesystemen steeds hoger op de agenda.

3. OEM-producted met digitale technieken en netwerkverbindingen

Digitale veiligheid t.a.v. 'embedded systems' en 'connected products' speelt hoofdzakelijk bij OEM-bedrijven (onderdeel van de maakindustrie) die producten leveren aan klanten waarin vormen van elektronica, regelsystemen, digitale technieken, netwerkverbindingen en data-uitwisseling aan de orde zijn. De digitale technieken bieden het OEM-bedrijf goede mogelijkheden om aanvullende (digitale) diensten aan te bieden, denk aan onderhoudsvoorspelling (predictive maintenance) en betalen naar gebruik (equipment-as-a-service; pay-per-use). Voorbeelden van producten die steeds meer digitale (online) functionaliteit omvatten zijn melkrobots met diermonitoringsfuncties en geautomatiseerde systemen voor oogstprognose, oogsten en logistiek in de agro-food.

[17] Zie o.a.: Deloitte (2019), *Cyber risk in advanced manufacturing*. ABN-AMRO (2021), *Ondernemers onderschatten het risico op cybercriminaliteit.*

3.3 Indicatie van digitale weerbaarheid bij maakbedrijven in Zuid-Holland

Een twintigtal organisaties hebben kwalitatieve informatie aangereikt voor deze verkenning. Diverse type bedrijven uit Zuid-Holland zijn betrokken geweest, van kleine verspanende bedrijven tot grote OEM-bedrijven met veel toeleveranciers in de (regionale) maakindustrie.

Over het algemeen is het beeld dat de betrokken Zuid-Hollandse maakbedrijven digitale weerbaarheid erkennen als belangrijk en dat veel van de gesproken bedrijven – binnen de organisatorische en budgettaire mogelijkheden – stappen ondernemen om de digitale weerbaarheid te verhogen (zie bijlage 6). Vele geïnterviewden onderschrijven dat het niet een kwestie is *óf* een bedrijf in de maakindustrie te maken krijgt met een cyberincident, maar *wanneer*. Het is opvallend dat enkele kleine producerende bedrijven (verspaners) betrokken bij de verkenning zeer bewust aandacht hebben voor digitale veiligheid, mede omdat de bedrijfseigenaren redeneren dat bedrijfscontinuïteit van hun familiebedrijf erg belangrijk is. Neemt niet weg dat ook wordt aangegeven door diverse geïnterviewden - die een goede en brede kijk hebben op de maakindustrie - dat nog veel bedrijven in de (regionale) maakindustrie op het vlak van (onderdelen van) digitale veiligheid nog onbewust onbekwaam zijn. Over het algemeen gaat het hier om de kleinere maakbedrijven. Diverse ondernemers / managers van kleinere bedrijven hebben te kennen gegeven dat het interview (voor deze verkenning) de bewustwording bij hen over cyberweerbaarheid verder heeft aangewakkerd.

Tijdens de gesprekken met de bedrijven is op globaal niveau de opzet van IT, OT en cyberweerbaarheid doorgenomen om betere beelden te krijgen. Deze informatie is van waarde geweest voor de verkenning. De diepgang van het onderzoek was te beperkt om de gesproken bedrijven te positioneren in een zogenaamd cyberweerbaarheid-volwassenheidsmodel (cyber security maturity model).

- 50% van de bedrijven vreest dat hun bedrijf binnen 12 maanden slachtoffer wordt van een cyberaanval.
- 48% voert zelden tot nooit updates uit.
- 32% van de bedrijven scant hun netwerk op kwetsbaarheden.
- 48% van de respondenten zegt niet over kennis te beschikken als ze geconfronteerd worden met een cyberaanval.
- 34% heeft een beleid dat zowel IT als operationele technologie (OT) dekt.
- 55% van de respondenten geeft aan geen standaarden te gebruiken of te overwegen met betrekking tot cybersecurity van de operationele technologie.
- 40% van de bevraagde bedrijven schenkt geen aandacht aan cybersecurity bij industriële aankopen.
- 35% werkt met PLC's (programmable logic controllers; programmeerbare logische sturing) van tien jaar of ouder.
- 77% test de beveiliging van de operationele technologie nooit.

Tabel 1: Enkele resultaten van een onderzoek bij 77 Belgische industriële maakbedrijven naar cyberweerbaarheid (Agoria et al, 2021)

Een recent Belgisch onderzoek laat zien dat veel Belgische maakbedrijven serieuze stappen dienen te nemen op het gebied van cyberweerbaarheid (zie tabel 1).[18] Inschatting is dat dit Belgische beeld voor een groot deel ook geldt voor de Nederlandse en Zuid-Hollandse maakbedrijven. De juiste stappen zetten is uitdagend, zeker voor de kleinere bedrijven. Een geïnterviewde ondernemer van een klein maakbedrijf met kennis en kunde van IT en digitale beveiliging verwoordde het als volgt: "*Ondanks het feit dat ik weet waar mijn bedrijf naar toe moet op het vlak van digitale beveiliging en ik continu maatregelen tref op het vlak van digitale veiligheid, heb ik nog steeds het idee dat ik in de mist rijd. Je rijdt in de mist en je weet en ziet niet wanneer je digitaal flink geraakt wordt of gaat worden. Dat is erg frustrerend.*" Aangereikte suggesties om bijvoorbeeld deze ondernemer te ondersteunen zijn o.a. kennisdeling, veiligheidsanalyse (scan) en dreigingsinformatie.

Het beeld bij de gesproken Zuid-Hollandse middelgrote en grote bedrijven is duidelijk: zij zijn over het algemeen intensief bezig om op strategisch, tactisch en operationeel niveau maatregelen te nemen op het vlak van cyberweerbaarheid. Sommige van die grote ondernemingen zijn actief bezig om de ISO 27001-certificering te behalen. Andere middelgrote en grootbedrijven hebben een ISO 27001-certificering en maken verbeterstappen in het borgen en onderhouden van de ISO 27001-certificering.

Het mkb actief in de maakindustrie heeft over het algemeen (onderdelen van) de IT uitbesteed aan IT-dienstverleners. Vaak nemen deze IT-dienstverleners ook digitale veiligheid onder hun hoede voor klanten. De opmerking valt tijdens de uitgevoerde verkenning dat digitale veiligheid (cyber-security) een specialisme is en dat met name kleine maakbedrijven in Zuid-Holland zich moeten vergewissen of en hoe sterk digitale veiligheid is geregeld door de betrokken IT-dienstverlener. Behulpzaam zijn controlelijsten voor (maak)bedrijven om samen met de IT-dienstverlener afspraken over digitale veiligheid na te lopen. Een voorbeeld is de controlelijst van het Digital Trust Center (bijlage 5).

De afstemmingen tussen kleine maakbedrijven en hun IT-dienstverleners leiden tot communicatie-uitdagingen. Enerzijds omdat de medewerkers van de kleinere maakbedrijven geen tot beperkte kennis hebben van IT en digitale veiligheid en anderzijds omdat de IT-dienstverleners (nog) te vaak in jargon communiceren. Zoals enkele gesproken ondernemers uit maakindustrie ook aangaven: *"De IT-dienstlener praat voor mij in geheimtaal"* en *"Als ik met de IT-dienstverlener om tafel zit dan heb ik het idee dat ik in de Matrix ben beland; de IT-Matrix"*.

Het algemene beeld is dat voorgevallen cyberincidenten bij organisaties (zoals vernomen via de media of via netwerken) het nodige losmaken bij de maakbedrijven in Zuid-Holland. Binnen de (regionale) maakindustrie heeft de cyberaanval op de VDL Groep[19] de bewustwording over de noodzaak van digitale weerbaarheid bij maakbedrijven prompt vergroot. Vele geïnterviewden geven duidelijk aan dat het cyberincident bij de VDL Groep de ogen (verder) geopend. Enkele gesproken (maak)bedrijven hebben bedrijfsmatig daadwerkelijk hinder ondervonden van de cyberaanval op de VDL Groep.

Voor bedrijven in de maakindustrie is het van belang om voldoende goed opgeleide professionals te kunnen aantrekken om cyberweerbaarheid binnen het bedrijf op niveau te brengen en te houden. Met name middelgrote en grote bedrijven hebben eigen afdelingen die zich (onder andere) richten op cybersecurity en cyberweerbaarheid. Enkele geïnterviewden geven aan dat het van belang is voor de regionale maakindustrie om goede verbindingen te hebben met het regionaal onderwijs op het vlak van informatietechnologie en cybersecurity. Ook initiatieven dragen bij aan het meer en

[18] Agoria, Howest, UGent en Sirris (2021), *Cybersecurity in de maakindustrie: welke bedrijven spelen het slim?*

[19] VDL Groep nieuwsbericht *'VDL Groep weer in bedrijf na cyberaanval'*, 8 november 2021, https://www.vdlgroep.com/nl/nieuws/vdl-groep-weer-in-bedrijf-na-cyberaanval.

beter opleiden van professionals op het vlak van cybersecurity: stimuleren zij-instroom (‘Cybersecurity werkt’) en weergave van vacatures, opleidingen en werkgevers (‘Security Talent’) (zie bijlage 7).

3.4 Vraagstukken op het vlak van digital veiligheid bij maakbedrijven

Tijdens de telefonische / online gesprekken is geprobeerd om een beeld te krijgen van eventuele vraagstukken die er leven bij de bedrijven op het vlak van digitale veiligheid. De intentie vanuit Security Delta is om bedrijven te ondersteunen met het helder krijgen van de vraagstukken of het (deels) oplossen van de vraagstukken door deze vraagstukken vrijblijvend in behandeling te laten nemen door een geselecteerde groep partners van Security Delta.

De interviews laten zien dat over het algemeen de middelgrote en grote bedrijven goed geoutilleerd (lijken te) zijn om vraagstukken op te pakken in samenwerking met bestaande IT- en cybersecurity-partners en specialisten. De bedrijven maken meerjarenplannen op het vlak van cybersecurity en daarmee is er een relatief duidelijke routekaart om bepaalde vraagstukken en uitdagingen – in lijn met gebruikte normen – op te pakken. Vooralsnog is het beeld dat deze bedrijven in de maak-industrie beperkte intenties hebben om vraagstukken voor te leggen aan het netwerk van Security Delta. De indruk is dat tijd, relaties en vertrouwen nodig zijn om vraagstukken uit de maakindustrie relevant voor het Security Delta-netwerk boven water te krijgen. Deze verkenning en de gevoerde gesprekken hebben bijgedragen aan de verdere positionering van Security Delta. Het is goed om als Security Delta blijvend kenbaar te maken dat het netwerk van Security Delta een kwalitatieve bijdrage kan leveren aan het wegen en oppakken van vraagstukken.

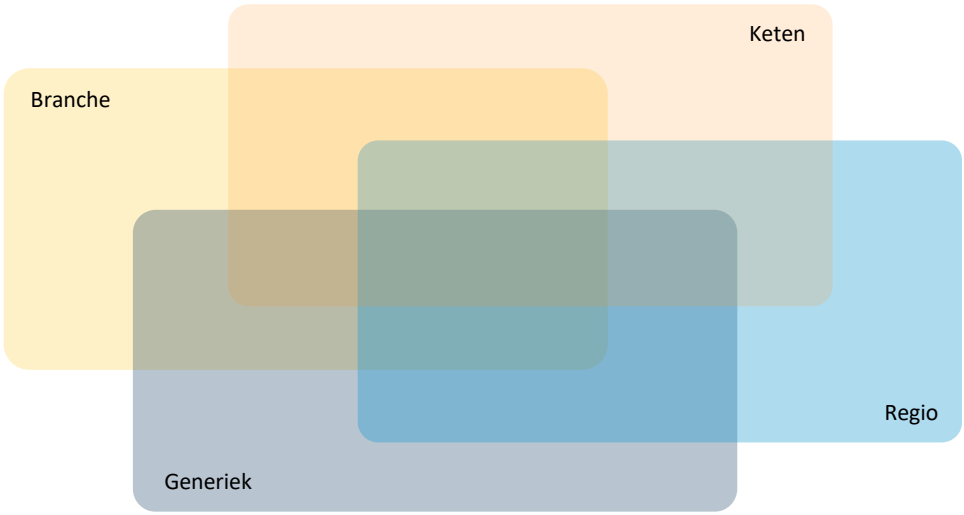
De kleinere bedrijven zijn meer zoekende qua maatregelen op het vlak van digitale weerbaarheid. Zoals eerder aangegeven in deze notitie geven betrokkenen aan dat over het algemeen de kleinere bedrijven meer onbewust onbekwaam zijn waar het gaat om cyberweerbaarheid. De vraagstukken die leven bij de kleinere bedrijven zijn over het algemeen meer standaard vraagstukken (virus-protectie, firewalls, veilige dataopslag, software in de cloud).

Toch hebben diverse bedrijven uit de maakindustrie aangegeven dat er de komende periode meer aandacht gericht zal zijn op de digitale beveiliging van met name operationele technologie. Eén bedrijf zoekt naar oplossingen om CNC-machines met verouderde operating systems via veilige koppelingen aan het digitale bedrijfsnetwerk te koppelen. Een ander bedrijf zoekt naar mogelijk-heden om persoonsauthenticatie in te voegen in het aanstuurproces van geautomatiseerde productiesystemen. Verdere afstemmingen met deze bedrijven kunnen mogelijk leiden naar vervolgacties om het netwerk van Security Delta oplossingsrichtingen te laten aanreiken.

4. Reflecties t.a.v. het ondersteunen van maakbedrijven in Zuid-Holland met digitale weerbaarheid

4.1 Digitale weerbaarheid adresseren vanuit verschillende aanvliegroutes

Dit hoofdstuk gaat over de verschillende opties en denkrichtingen om maakbedrijven in Zuid-Holland (sterker) te ondersteunen met digitale weerbaarheid. De afbakeningen, opties en denkrichtingen zijn met name gebaseerd op de verkregen informatie tijdens de gesprekken met de betrokken organisaties. De intentie is niet om met dit hoofdstuk een uitputtend overzicht te geven.



Figuur 2: Bedrijven in de maakindustrie aanspreken op het vlak van om cyberveiligheid en cyberweerbaarheid: vanuit een brancheperspectief, vanuit een ketenperspectief en/of vanuit een regionale invalshoek.

Vanuit verschillende aanvliegroutes kunnen en worden bedrijven in de maakindustrie aangesproken om cyberveiligheid en cyberweerbaarheid (sterker) te overwegen of (sterker) onderdeel te laten zijn van de bedrijfsvoering. In het kader van deze verkenning zijn – kijkend naar de sectorale en regionale focus en de informatie verkregen van de geïnterviewden - die verschillende invalshoeken beperkt tot de volgende drie: 1) branches, 2) ketens en 3) regio (figuur 2).

Overige invalshoeken (actoren), zoals de IT- en security-dienstverleners, verzekeraars, accountants, Kamer van Koophandel-organisatie, overheden (nationale, regionaal en lokaal), zijn in deze verkenning buiten beschouwing gelaten. Deze actoren zouden in het kader van deze verkenning geschaard kunnen worden onder de rubriek ‘generiek’ in figuur 2.

4.2 Vanuit de branche cyberweerbaarheid adresseren

Uit de gesprekken blijkt sterk dat bedrijven in de maakindustrie zich sterk verbonden voelen met de branche. Dit maakt ook dat veel bedrijven de brancheorganisatie zien als een belangrijke organisatie om cyberweerbaarheid te adresseren. De brancheorganisatie begrijpt de business, begrijpt de

bedrijven in de branche en spreekt de taal van de ondernemers. Ondernemersbijeenkomsten en ondernemersnetwerken meer vanuit de branche aangevlogen worden positief ontvangen door de ondernemers / managers vanwege de herkenbaarheid van knelpunten en oplossingen die spelen bij de bedrijven. Brancheorganisaties die als relevant worden gezien door de geïnterviewden zijn onder meer de Koninklijke Metaalunie, FME, NEVAT, AVAG, Netherlands Maritime Technology (NMT) en FHI. Mogelijk dat meerdere brancheorganisatie hieraan toegevoegd kunnen worden. Individuele brancheorganisaties zijn actief op het vlak van cyberweerbaarheid. Ook werken brancheorganisaties en koepels gericht op de industrie samen aan initiatieven (bijvoorbeeld Samen digitaal veilig en Certificering cyberweerbaarheid).

Tijdens de verkenning zijn diverse leden van de Metaalunie gesproken. Deze brancheverenigingis sterk vertegenwoordigd in de Zuid-Hollandse maakindustrie (zie hoofdstuk 2 en bijlage 3). De gesproken leden zien de periodieke bulletins van de Metaalunie als waardevol voor het verspreiden van inzichten en actuele informatie over cyberweerbaarheid. Ook geven enkelen aan dat vanuit de branche georganiseerde bijeenkomsten over cyberweerbaarheid als potentieel interessant wordt gezien. De gesprekken hebben niet tot een robuust beeld geleid hoe specifiek of omvangrijk het ‘cyberweerbaarheidspakket’ van een brancheorganisatie zou moeten zijn naast bijvoorbeeld werken aan bewustwording, uitwisselen van kennis en het stimuleren van contacten en vervolgstappen.

De Europese Unie werkt aan een nieuwe cybersecurityrichtlijn genaamd NIS2 (‘network and information security directive’).[20] Deze richtlijn zal de oude NIS-richtlijn uit 2016 vervangen. Een belangrijk aspect is dat ook de vervaardigingsindustrie in de NIS2-richtlijn meer aandacht krijgt.[21] De exacte effecten van NIS2 voor de Nederlandse industrie zijn nog niet duidelijk, maar het kan gaan betekenen dat individuele bedrijven in de (maak)industrie verplicht worden om cyber-beveiligingsrisico's in toeleveringsketens en inzake relaties met leveranciers aan te pakken. De NIS2-richtlijn zal daardoor in de diverse branches gerelateerd aan de maak- en hightech industrie – ook in de regio Zuid-Holland - structurele aandacht krijgen.

4.3 Keten(s) en cyberweerbaarheid

Ketenrelaties spelen een belangrijke rol in het stimuleren van cyberweerbaarheid in de keten (zie ook de bovengenoemde ontwikkelingen t.a.v. de NIS2-richtlijn). Klanten van maakbedrijven hebben en kunnen de nodige invloed uitoefenen om toeleverende bedrijven aan te zetten om (meer) werk te maken van cyberweerbaarheid. Twee routes worden daarbij onderscheiden: 1) met behulp van inkoopvoorwaarden de toeleverende maakbedrijven stimuleren om verbeterstappen te maken en 2) toeleverende maakbedrijven meer vanuit betrokkenheid en maatschappelijk verantwoord ondernemen helpen met cyberweerbaarheid (bewustwording, kennisuitwisseling, best practices, trainingen, gezamenlijk optrekken). De twee routes zijn complementair.

Het valt op dat een groot deel van de gesproken grootbedrijven nog niet de aandacht heeft om de toeleverketen actief te helpen met cyberweerbaarheid (vooruitlopend op de NIS2-richtlijn), behoudens inkoopvoorwaarden over bijvoorbeeld continuïteit en kwaliteit van de leveringen en geheimhouding van bepaalde informatie. Deze bedrijven zijn actief om bedrijfsintern – volgens

[20] Europese Commissie (2020), *Proposal (and annexes) for a directive of the european parliament and of the council on the resilience of critical entities*.

[21] De volgende sectoren worden als essentieel bestempeld: energie, vervoer, bankwezen, financiële markten, gezondheid, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur en ruimtevaart. Belangrijke sectoren: post- en koeriersdiensten, afvalbeheer, productie en distributie van chemische producten, productie, verwerking en distributie van levensmiddelen, vervaardigingsindustrie en digitale dienstverleners.

plannen en standaarden – de cyberweerbaarheid te verhogen. Wel verwachten ze de komende periode meer aandacht te kunnen richten op de toeleverketens.

Toch zijn er ook grootbedrijven die op structurele wijze de toeleverketen ondersteunen met cyber-weerbaarheid. ASML heeft bijvoorbeeld een helder pakket aan maatregelen en instrumenten om (in eerste instantie) de grotere toeleveranciers (system supplier; tier 1 leveranciers) te bewegen via de geschetste twee routes. Maar ook de minder grote toeleveranciers in het ASML-ecosysteem worden meegenomen. Het belang van ASML is hierbij aanzienlijk: intellectueel eigendom van ASML dient zeer goed beveiligd te zijn in de keten en ketencontinuïteit is van uiterst belang gezien de hoge complexiteit van de lithografiemachines van ASML.[22] Ook is ASML een actieve aanjager van initiatieven zoals het Cyberweerbaarheidscentrum Brainport en CYRA (een instrument om de cyberweerbaarheid van bedrijven vast te stellen en certificeringen mogelijk te maken).[23] De aanpak van ASML is zeer inspirerend en bruikbaar voor middelgrote en grote (OEM-)bedrijven actief in de industrie in de regio Zuid-Holland.

Het is opvallend dat over het algemeen de kleinere bedrijven in de regio Zuid-Holland nog niet actief of specifiek benaderd zijn door industriële klanten om meer werk te maken van cyberweerbaarheid. Geïnterviewden geven aan dat ze dat een volstrekt logische aanpak zouden vinden van klanten en hebben zeker de intentie om (samen met klanten) aan de slag te gaan met het versterken van de cyberweerbaarheid.

4.4 Vanuit de regio cyberweerbaarheid adresseren

De insteek om bedrijven aan te spreken en onder te steunen met cyberweerbaarheid vanuit een branche of in ketenperspectief staat relatief dicht bij de inhoudelijke business van de ondernemer. Desalniettemin wordt ook door middelgrote en kleinere bedrijven aangegeven dat de regionale netwerken van bedrijven ook waardevol zijn om kennis en kunde over cyberweerbaarheid uit te wisselen. Met name de persoonlijke netwerken van ondernemers / managers lijken (mogelijk) van waarde. Deze netwerken zijn bijvoorbeeld gerelateerd aan lokale ondernemersverenigingen in Zuid-Holland of regionale koepels en verenigingen zoals Hi Delta. Initiatieven op het vlak van cyberweerbaarheid vanuit deze netwerken worden gewaardeerd, maar sommige meer technisch-georiënteerde ondernemers en bedrijfsleiders van met name kleinere maakbedrijven in de regio Zuid-Holland zijn minder genegen om actief deel te nemen aan lokale en regionale netwerken die meer gericht zijn op ondernemen en business development. Deze ondernemers / managers voelen zich meer thuis in branchegerelateerde netwerken.

Regionale ontwikkelingsorganisaties spelen een actieve rol om regionaal bijdragen te leveren aan bijvoorbeeld internationalisering en innovatie. Ook zijn deze organisaties vaak gericht op thema's die te maken hebben met de maakindustrie: smart industry en cyberveiligheid. De afgelopen jaren zijn in en vanuit diverse regio's in Nederland (regionaal-georiënteerde) loketten en publiek-private initiatieven opgezet om bedrijven te ondersteunen met smart industry en cyberweerbaarheid. Voorbeelden zijn SMITZH (gerelateerd aan onder andere InnovationQuarter) gericht op smart industry in met name Zuid-Holland (zie hoofdstuk 2 met een indicatie van de regionale fieldlabs), FERM (gericht op cyberweerbaarheid in de ketens in en rond de Rotterdamse haven), Cyberweer-

[22] Ter indicatie: de EUV-machine van ASML heeft ruim 100.000 onderdelen. Zie artikel *'Waarom ASML straks 4,5 miljoen onderdelen nodig heeft voor EUV'*, https://www.made-in-europe.nu/2020/01/waarom-asml-straks-45-miljoen-onderdelen-nodig-heeft-voor-euv/.

[23] CYRA ('cyber rating') is een certificeringsmodel dat het Cyberweerbaarheidscentrum Brainport samen met TÜV Nederland en ASML heeft ontwikkeld om het volwassenheidsniveau van de digitale weerbaarheid in beeld te brengen bij bedrijven en handvatten aan te reiken om een hoger cyberweerbaarheidsniveau te behalen.

baarheidscentrum Greenport (horticultuursector en toeleverketens; opstartfase), BOOST (smart industry; Oost-Nederland), Cybersecurity Centrum Maakindustrie (gerelateerd aan Novel-T; Oost-Nederland), MKB Cyber Campus in Noord-Nederland, Expertise Centrum Cyberweerbaarheid in Zuid-Nederland en het Cyberweerbaarheidscentrum Brainport (gestart in de regio Brainport, maar gaandeweg landelijk opererend). Deze opsomming is niet uitputtend. De regionale initiatieven op het vlak van cyberweerbaarheid laten de afgelopen maanden meer stappen zien in samenwerking, bijvoorbeeld met TÜV Nederland om gezamenlijk te werken aan onafhankelijke certificering van bedrijven op het gebied van cybersecurity.[24]

De dienstverlening van de (regionale) cyberweerbaarheidsloketten en -centra zijn divers en niet alle initiatieven zijn specifiek gericht op de (maak)industrie. Bepaalde initiatieven richten zich nadrukkelijker op kleinere bedrijven met toegankelijke en kortdurende diensten (denk aan bijeenkomsten en scans). Andere initiatieven zoals bijvoorbeeld het Cyberweerbaarheidscentrum Brainport (CWB) biedt een uitgebreid pakket aan diensten – in eerste instantie gericht op middelgrote en grote bedrijven in de maak- en hightech industrie – op basis van een abonnement (kennissessies, dreigingsinformatie, besloten app, besloten fora voor kennisuitwisseling, scans en certificeringstrajecten). Inmiddels zijn ruim 75 bedrijven uit de industrie participant van het CWB, waarbij het aandeel bedrijven buiten de regio Brainport één-derde is en toeneemt. De ambitie van het CWB is om eind 2022 een forse sprong te maken in het aantal participanten.

Enkele geïnterviewden geven aan dat het track-record van het CWB zich inmiddels heeft opgebouwd en dat het zinvol is om bewezen initiatieven naar de regio Zuid-Holland te halen. Een geïnterviewde ziet interessante mogelijkheden om het dienstenpakket van het CWB met bijvoorbeeld een sectorale of regionale kleuring in de regio Zuid-Holland te positioneren. Daarmee wordt het mogelijk om bijvoorbeeld regionale of sectorale 'hulpposten' op te zetten op basis van het fundament ('backbone') van het CWB. Dit schept regionale en/of sectorale mogelijkheden voor branches en koepels actief in of gericht op de maakindustrie. Geïnterviewden refereren ook naar FERM als een initiatief met een track record waarvan geleerd kan worden. Ook wordt gerefereerd naar het Cyberweerbaarheidscentrum Greenport dat als relevant wordt gezien voor bedrijven in de maakindustrie die actief zijn in de toeleverketen van de horticultuur.

Door geïnterviewden wordt aangegeven dat de diensten zoals die worden aangeboden door het CWB mogelijk nog niet geheel afgestemd zijn voor de kleinere bedrijven en daar liggen verdere kansen voor samenwerking. Enkele kleinere bedrijven die aan de verkenning hebben bijgedragen vinden de meerwaarde van cyberweerbaarheidsdiensten van loketten en centra lastig in te schatten en laten blijken dat de bestaande IT-dienstverleners als belangrijk aanspreekpunt wordt gezien voor cyberweerbaarheidsuitdagingen en -oplossingen. De prijsstelling van de cyberweerbaarheidsdiensten speelt daarbij een rol volgens de kleinere bedrijven. Daarentegen redeneren geïnterviewden ook dat de financiële schade door productiestilstand door cyberincidenten goed meegenomen moet worden in de budgettaire afwegingen van (kleinere) bedrijven die de inkoop van (additionele) diensten op het vlak van cyberweerbaarheid complex, lastig of te duur vinden.

Een ontwikkeling in de Europese regio's en ook in de regio Zuid-Holland zijn de zogenaamde EDIH's (European digital innovation hubs).[25] Deze regionale hubs worden (mede) gefinancierd door de Europese Commissie en hebben tot doel om het regionaal bedrijfsleven en regionale overheden

[24] https://www.certificering-keuring.nl/t%C3%BCv-nederland-en-het-cybersecurity-centrum-maakindustrie-van-novel-t-sluiten-partnership, https://www.certificering-keuring.nl/aantoonbare-cyberweerbaarheid-dankzij-samenwerking-tuv-nederland-ferm-rotterdam en https://mkbcybercampus.nl/mkb-cyber-campus-en-tuv-nederland-tekenen-samenwerkingsovereenkomst/

[25] Europese Commissie (2021a), *Digital Europe Work Programme 2021-2022*. Europese Commissie (2021a), *Digital Europe - EDIH Work Programme 2021-2023*. Europese Commissie (2021c), *Digital Europe - Cybersecurity Work Programme 2021-2022*.

(via loketten en doorverwijzingen) te ondersteunen met het inzetten van nieuwe digitale technieken. Voor deze verkenning gaat het te ver om het Europese EDIH-initiatief uit te diepen, echter de komende jaren zal in de regio Zuid-Holland naar alle waarschijnlijkheid een EDIH opgebouwd worden om regionale bedrijven te helpen met digitale innovaties, mogelijk ook gerelateerd aan cybersecurity. Onder andere InnovationQuarter is betrokken om de EDIH-ambities in de regio Zuid-Holland vorm te geven (medio 2022 komt meer helderheid over de financiering; in theorie zal het initiatief vanaf 2023 van start kunnen gaan). Geïnterviewden geven aan dat het EDIH-initiatief zou kunnen aansluiten op de (bestaande) cyberweerbaarheidsloketten en -centra, door bijvoorbeeld nieuwe technieken en concepten op het vlak van cybersecurity en cyberweerbaarheid in de praktijk te (laten) testen. Het is voor bepaalde geïnterviewden op dit moment niet geheel helder hoe de Nederlandse EDIH's van waarde gaan worden voor bedrijven in de maakindustrie.

4.5 Afrondend

De voorgaande paragrafen hebben laten zien dat bedrijven in de maakindustrie vanuit verschillende aanvliegroutes aangesproken en/of bediend (kunnen) worden op het vlak van cyberweerbaarheid. Meerdere geïnterviewden geven aan dat in Nederland en ook in de regio Zuid-Holland er een drukte is aan initiatieven, projecten, platformen en activiteiten die zich richten op het bedrijfsleven (mkb) eventueel in combinatie met thema's als digitalisering, smart industry en/of cybersecurity. Ook wordt aangegeven dat het voor bedrijven in de maakindustrie moeilijk is en/of steeds moeilijker wordt om door de bomen het bos te zien kijkend naar de veelheid aan initiatieven en acties om het bedrijfsleven aan te spreken, te laten participeren, te betrekken, te ondersteunen etc. Dit zegt trouwens nog niets of deze initiatieven en acties voldoende of passend zijn voor het bedrijfsleven.

Deze constateringen scheppen ook mogelijkheden voor verschillende instanties, partijen en initiatieven om samen te werken en vanuit een gezamenlijke routekaart (roadmap) bedrijven in de regionale maakindustrie te ondersteunen met cyberweerbaarheid. De branche-insteek lijkt daarbij een belangrijke rol te spelen.

Ook komt vooralsnog naar voren dat het niet eenduidig is of een nieuw op te zetten centrum voor cyberweerbaarheid voor de Zuid-Hollandse maakindustrie opportuun is. Interessanter is het wellicht om vanuit een bestaand centruminitiatief met een track-record, betrokken participanten en specifiek gericht op de maakindustrie – bijvoorbeeld het CWB – te kijken naar een regionale en/of sectorale inkleuring (CWB-hulpposten) om bedrijven in Zuid-Holland te ondersteunen. Duidelijk komt ook naar voren dat nu het moment is om een sneeuwbaleffect (multiplier) in gang te zetten, met elkaar, om digitale weerbaarheid bij bedrijven in de maakindustrie – onder andere in de regio Zuid-Holland - te verhogen. Benut daarbij de hoge betrokkenheid van grotere bedrijven uit de industrie.

5. Conclusies en aanbevelingen

5.1 Conclusies

1. De maakindustrie is alom aanwezig in de regio Zuid-Holland.

De maakindustrie (SBI24 - SBI30 en SBI33) is in Zuid-Holland met ruim 7.100 bedrijfsvestigingen vertegenwoordigd. Inschatting is dat ongeveer 65.000 personen werkzaam zijn in de regionale maakindustrie. Ongeveer 87% van de bedrijven in de maakindustrie heeft minder dan 10 medewerkers. Clusters zijn onder meer te vinden in het Westland, Groot Rotterdam, Drechtsteden, Hoekse Waarde & Goeree-Overflakkee en Groot Den Haag.

2. Het is relevant om te onderkennen dat de maakindustrie uit vele type bedrijven bestaat.

De Zuid-Hollandse maakindustrie bestaat uit een veelheid aan type bedrijven die een grote verscheidenheid aan sectoren bedienen. Dimensies die bedrijven in de maakindustrie kunnen typeren zijn bijvoorbeeld omvang (o.a. op basis van aantal medewerkers), aard van de producten en diensten, positie in de keten, vernieuwingsgezindheid en mate en wijze van organisatie van informatietechnologie, operationele technologie en cyberweerbaarheid. In het kader van regionale cyberweerbaarheidsinitiatieven is het van belang om die diversiteit aan bedrijven te onderkennen.

3. Cyberweerbaarheid is sterk van belang in de maakindustrie.

De maakindustrie is sterk gedigitaliseerd de afgelopen jaren en toeleverketens zijn afhankelijk van digitale gegevensuitwisseling. Verstoringen van de toeleverketens en het ontvreemden van intellectueel eigendom door cyberincidenten hebben grote gevolgen voor individuele bedrijven en ketenpartners. De cyberdreiging in de maakindustrie wordt getypeerd als hoog tot zeer hoog. Dit maakt dat cyberweerbaarheid sterk van belang is.

4. Cyberweerbaarheid heeft aandacht bij de maakbedrijven.

De cyberdreiging in de maakindustrie wordt als hoog tot zeer hoog getypeerd en cyberincidenten kunnen aanzienlijke schade veroorzaken bij bedrijven en in ketens actief in de maakindustrie.

Over het algemeen is het beeld dat de regionale bedrijven in de maakindustrie aandacht hebben voor cyberweerbaarheid. Grote en middelgrote bedrijven zijn actief om volgens normen en certificeringen cyberweerbaarheid met name bedrijfsintern op goed niveau te krijgen.

Een deel van de kleinere bedrijven is (op onderdelen) onbewust onbekwaam ten aanzien van cyberweerbaarheid. Toch is ook het beeld dat de kleine en microbedrijven het belang van cyberweerbaarheid onderkennen, echter ze zijn (over het algemeen) zoekende hoe dat opgepakt moet worden. Het is voor kleine en microbedrijven een lastig vraagstuk, ook als ze gebruik maken van de diensten van een IT-dienstverlener.

Recente cyberincidenten in de industrie – zoals bij de VDL Groep – hebben de bewustwording prompt op scherp gezet bij alle bedrijven in de maakindustrie – van groot tot klein. Ook deze verkenning heeft met name bij de kleinere bedrijven de bewustwording verder aangescherpt.

5. Drie relevante aanvliegroutes om cyberweerbaarheid te adreseren bij maakbedrijven: vanuit de branch, vanuit de keten en vanuit de regio.

Uit de gesprekken blijkt dat bedrijven in de maakindustrie zich sterk verbonden voelen met de branche. Vanuit de branche bedrijven attenderen op en ondersteunen met cyberweerbaarheid lijkt daarmee relevant.

Ook de ketenbenadering is van belang en een goed voorbeeld is de wijze hoe ASML ketenpartners en ecosystemen meeneemt in cyberweerbaarheid. De nieuwe NIS2-richtlijn (cyberveiligheid) lijkt van belang voor de maakindustrie en gaat effecten hebben op hoe bedrijven cyberweerbaarheid in de toeleverketen dienen te organiseren.

De regionale benadering speelt een rol: bedrijven en hun ondernemers / bedrijfsleiders / managers zijn ingebed in lokale en regionale netwerken die van waarde zijn om kennis uit te wisselen.

6. Bepaalde bestaande cyberweerbaarheidsinitiatieven zijn interessant voor de Zuid-Hollandse maakindustrie.

In Nederland zijn reeds diverse cyberweerbaarheidscentra en -loketten actief en (deels) ook gericht op de (maak)industrie. De diensten van deze centra en loketten zijn divers. Enkele cyberweerbaarheidsinitiatieven zijn interessant voor de Zuid-Hollandse maakindustrie, gezien de focus op de maakindustrie, het track-record en de bereidheid tot afstemmingen. Voorbeelden zijn het Cyberweerbaarheidscentrum Brainport (CWB) en CYRA (certificeringsmodel).

Er is in Nederland en in de regio Zuid-Holland een drukte aan initiatieven gericht op industriële bedrijven kijkend vanuit het perspectief van de maakbedrijven; met name de kleinere bedrijven zien steeds minder door de bomen het bos. Voorkomen moet worden dat in de regio Zuid-Holland het wiel opnieuw wordt uitgevonden en het is vanuit nationaal perspectief wellicht beter om vanuit bestaande initiatieven een sneeuwbaleffect op gang te brengen die ook de maakbedrijven in de regio Zuid-Holland positief gaat beïnvloeden.

7. Intentie bij bedrijven om vraagstukken op het vlak van cyberweerbaarheid aan te reiken aan het Security Delta-netwerk is vooralsnog beperkt.

Middelgrote en grote bedrijven in de maakindustrie lijken over het algemeen goed geoutilleerd te zijn om bepaalde interne vraagstukken op het vlak van cyberweerbaarheid intern en met bestaande IT- en securitypartners op te pakken. De kleinere bedrijven zijn meer zoekende qua maatregelen op het vlak van digitale weerbaarheid, waarbij de inschatting is dat het over het algemeen gaat om standaard vraagstukken.

Tijd, relaties en vertrouwen lijken nodig om vraagstukken mogelijk relevant voor het Security Delta-netwerk door maakbedrijven te laten delen. Potentiële vraagstukken vanuit de maakbedrijven voor het Security Delta-netwerk zullen onder andere gaan over operationele technologie (productiesystemen binnen de maakbedrijven).

5.2 Aanbevelingen

1. Sluit aan bij het bestaande Cyberweerbaarheidscentrum Brainport om maakbedrijven in de regio Zuid-Holland te ondersteunen met cyberweerbaarheid.

De cyberdreiging in de maakindustrie is hoog tot zeer hoog en dat maakt dat met urgentie stappen moeten worden gezet om de cyberweerbaarheid bij Zuid-Hollandse maakbedrijven te verhogen, bij voorkeur op basis van bestaande initiatieven.

Een relevant initiatief interessant voor maakbedrijven in de regio Zuid-Holland is het Cyberweer-baarheidscentrum Brainport (CWB). Het CWB richt zich op de hightech en maakindustrie en opereert steeds meer landelijk kijkend naar het (groeiend) aantal participanten van buiten de Brainport regio.

Een aanbeveling is om met het CWB de mogelijkheden voor Zuid-Hollandse maakbedrijven af te stemmen, bij voorkeur in samenwerking met (regionale vertegenwoordigen van) brancheorganisaties in de maakindustrie. Een scenario is het opzetten van (branche) CBW-hulpposten die gebruik maken van het fundament (‘backbone’) van het CWB. Overleg met en over het CBW zal moeten uitwijzen wat het meest aantrekkelijke scenario is voor de regionale bedrijven. Daarbij zal ook goed gekeken moeten worden hoe op basis van de CBW-formule kleinere bedrijven in de maakindustrie bediend zouden moeten worden.

Het Cyberweerbaarheidscentrum Greenport is een initiatief in de opstartfase dat relevant is voor bedrijven in de maakindustrie die actief zijn in de toeleverketen van de horticultuur. Het is van belang om het Cyberweerbaarheidscentrum Greenport en FERM (cyberweerbaarheidscentrum gericht op de Rotterdamse haven) te betrekken voor het uitwisselen van inzichten en ervaringen.

Concrete actie: een overleg tussen Security Delta en CWB en indien mogelijk inclusief één of meerdere relevante brancheorganisaties zoals Koninklijke Metaalunie én exclusief andere organisaties.

2. Breng belanghebbenden bij elkaar om samen op te trekken in het bedienen van Zuid-Hollandse maakbedrijven op het vlak van cyberweerbaarheid.

Voor een krachtig sneeuwbaleffect en met voorkoming van het opnieuw uitvinden van het wiel is het zaak dat diverse belanghebbenden (nationaal en regionaal) samen (sterker) gaan optrekken. Daarbij is het goed om initieel goed te kijken naar ambities en ontwikkelingen buiten de regio Zuid-Holland (bijvoorbeeld de ambities van de brancheorganisaties die weerslag hebben in de regio Zuid-Holland of de ambities en kracht van het CWB).

De voorkeuren zijn om 1) Zuid-Hollandse cyberweerbaarheidsstappen voor de maakindustrie sterk van een brancheperspectief aan te vliegen mede door sterke inhoudelijke inbreng en betrokkenheid van brancheorganisaties, 2) sterk rekening te houden met het feit dat de Zuid-Hollandse maak-industrie voor een zeer groot deel uit kleinere bedrijven bestaat en 3) initiatieven efficiënt en effectief op te zetten.

Concrete belanghebbenden voor afstemmingen zijn brancheorganisaties (o.a. Metaalunie, AVAG, NMT, NEVAT, FME, FHI), aanjagers van cyberweerbaarheid in de maakindustrie (o.a. Security Delta, ASML Security Office, Cyberweerbaarheidscentrum Brainport, Cyberweerbaarheidscentrum Greenport, Brainport Industries) en regionale organisaties (Hi Delta, InnovationQuarter).

Ook is het van belang om de grote en middelgrote bedrijven uit de Zuid-Hollandse maakindustrie te betrekken; zij hebben sterk belang bij digitaal veilige toeleveringsketens, ook kijkend naar de komende NIS2-richtlijn. Enkele namen zonder uitputtend te zijn: Lely, Huisman Equipment, Damen,

IHC, Priva, Berg Hortimotive, Kind Technologies, Batenburg Techniek, Boers & Co en Hittech Group.

Concrete actie: rondetafelgesprek met uitsluitend Security Delta en relevante brancheorganisaties om de contouren van ‘samen optrekken’ te bespreken.

Concrete actie: rondetafelgesprek met een grotere groep: Security Delta, brancheorganisaties, aanjagers (denk aan CWB en ASML Security Office), enkele (grotere) bedrijven uit Zuid-Holland en regionale organisaties om ‘samen optrekken’ te bespreken, waarbij aanvliegen van branche-perspectief aan te bevelen is mede door een sterke inhoudelijk inbreng van brancheorganisaties.

Concrete actie: onderlinge afstemming tussen middelgrote en grote (OEM-)bedrijven uit Zuid-Holland om de potentie van ‘samen optrekken’ op het vlak van cyberweerbaarheid in de toe-leveringsketen (implicaties NIS2-richtlijn) te bespreken, bij voorkeur inclusief de aanwezigheid van grote (OEM-)bedrijven die voorgang boeken met cyberweerbaarheid in de keten / het ecosysteem (o.a. ASML). Een eerste afstemming zou kunnen plaatsvinden tijdens een HSD Café over het onderwerp NIS2-richtlijn.

3. Houd bij het opzetten en uitrollen van activiteiten op het vlak van cyberweerbaarheid rekening met de grote diversiteit aan regionale maakbedrijven en betrek bij de activiteiten verschillende type funcionarissen verbonden aan de maakbedrijven.

De maakindustrie is zeer divers qua type bedrijven en de markten die bediend worden. Een aanbeveling aan cyberweerbaarheidsinitiatieven gericht op de Zuid-Hollandse maakindustrie is om rekening te houdend met deze grote diversiteit en de zeer grote populatie van microbedrijven.

Deze diversiteit speelt aan de inhoudelijke kant van cyberweerbaarheidsactiviteiten (redeneren en zaken aanpakken vanuit de specifieke business van de bedrijven) en bij de communicatie (segmen-teren bij het werven, aanspreken en betrekken van bedrijven bij de activiteiten).

Spreek bij activiteiten en informatie over cyberweerbaarheid de directeur-eigenaren / directie / bestuurders van bedrijven aan op hun verantwoordelijk om cyberweerbaarheid te organiseren binnen hun bedrijf en/of bedrijven.

Betrek (indien relevant of mogelijk) op gesegmenteerde wijze meerdere type functionarissen verbonden aan de (middelgrote en grote) maakbedrijven bij regionale / sectorale activiteiten die te maken hebben met cyberweerbaarheid: directie, management, inkoop, productie, kwaliteit, IT, cybersecurity, communicatie etc.

Concrete actie: houd initiatieven (inhoud en communicatie) van bijvoorbeeld Security Delta die gericht zijn op het bedrijfsleven en specifiek de maakindustrie tegen het licht, kijkend naar 1) de grote diversiteit aan type bedrijven in de maakindustrie, 2) de noodzaak om directie / bestuurders van maakbedrijven aan te spreken op hun verantwoordelijkheid ten aanzien van cyberweerbaarheid en 3) het belang van het betrekken van meerdere type functionarissen bij maakbedrijven op het vlak van cyberweerbaarheid.

4. Werk aan het structureel positioneren van Security Delta en de toegevoegde waarde van het netwerk van Security Delta in de maakindustrie.

Cyberweerbaarheid verhogen binnen maakbedrijven betekent in meerdere bedrijfsdomeinen (strategie, organisatie, techniek etc.) stappen ondernemen en borgen. Het netwerk van Security Delta omvat vele organisaties die generieke en specialistische diensten en producten leveren op het vlak van cybersecurity / cyberweerbaarheid.

Om de toegevoegde waarde van het netwerk voor de maakindustrie kenbaar te maken en te laten landen is het structureel positioneren van Security Delta en het netwerk van Security Delta van belang. Een aandachtsgebied voor de (middelgrote en grote) bedrijven in de maakindustrie is de cyberweerbaarheid op het vlak van operationele technologie (productiesystemen, productie-automatisering). Een aandachtspunt voor OEM-bedrijven in de maakindustrie met producten die digitale technieken en digitale verbindingen hebben is de digitale beveiliging van deze digitaal verbonden (‘connected’) producten.

Concrete actie: organiseer voor (middelgrote en grote) maakbedrijven kennisdeling over cyber-veiligheid op het vlak van operationele technologie (OT), ook om te zorgen dat deze bedrijven van elkaar kunnen leren. Deze kennisdeling kan verlopen via het lerende netwerk ‘Community of practice OT’ (een initiatief van Security Delta).

Concrete actie: organiseer voor OEM-bedrijven in de maakindustrie die digitaal verbonden (‘connected’) producten ontwikkelen kennisdeling over digitale beveiliging van digitaal verbonden producten, ook om te zorgen dat deze bedrijven van elkaar kunnen leren.

Bijlagen

Bijlage 1: Overzicht (geanonimiseerd) van organisaties betrokken bij de verkenning

Betrokken organisatie	Omschrijving belangrijkste activiteiten
Bedrijven 1, 2 en 3	Microbedrijven met verspanende activiteiten voor diverse sectoren.
Bedrijven 4 en 5	Kleine bedrijven met verspanende activiteiten inclusief (module-)assemblage voor diverse sectoren.
Bedrijven 6 en 7	Middelgrote bedrijven met verspanende activiteiten inclusief (module-)assemblage voor diverse sectoren.
Bedrijf 8	Kleinbedrijf op het vlak van ontwikkeling, productie en verkoop van toolingproducten voor de maakindustrie.
Bedrijf 9	OEM bedrijf (middelgroot) gericht op de ontwikkeling, productie en verkoop van productiesystemen voor de maakindustrie.
Bedrijf 10	OEM bedrijf (middelgroot) gericht op de ontwikkeling, productie en verkoop van systemen voor met name de horticultuur.
Bedrijf 11	OEM bedrijf (grootbedrijf) gericht op de ontwikkeling, productie en verkoop van systemen voor o.a. horticultuur en gebouwmanagement.
Bedrijf 12	Bedrijvengroep (grootbedrijf) actief in vele technologische disciplines met een nadruk op mechatronica en system integration.
Bedrijf 13	OEM machinebouwer (grootbedrijf) voor met name de zuivel-producerende industrie.
Bedrijf 14	OEM machinebouwer (grootbedrijf) voor met name de verpakkingsindustrie.
Bedrijf 15	OEM machinebouwer (grootbedrijf) voor de halfgeleiderindustrie.
Bedrijf 16	OEM machinebouwer (grootbedrijf) voor de maritieme/offshore industrie.
Organisatie 1	Stichting actief op het vlak van cyberweerbaarheid.
Organisatie 2	Coöperatie van 1e, 2e of 3e lijns hightech toeleveranciers.
Organisatie 3	Vereniging van regionale bedrijven en organisaties.
Organisaties 4 en 5	Twee organisaties gericht op regionale ontwikkeling, met o.a. activiteiten op het vlak van smart industry en cyberweerbaarheid.
Organisaties 6, 7 en 8	Drie brancheorganisaties (metaal, instrumentatie & automatisering en greenhouse technology).

Bijlage 2: Afbakeningen maakindustrie

Veel gebruikte afbakening van de maakindustrie	Ruimere afbakening van de maakindustrie
Basismetaalindustrie (SBI24) Metaalproductenindustrie (SBI25) Elektrotechnische industrie (SBI26) Elektrische apparatenindustrie (SBI27) Machine-industrie (SBI28) Auto- en aanhangwagenindustrie (SBI29) Overige transportmiddelenindustrie (SBI30) Reparatie en installatie van machines (SBI33)	Vervaardiging van tabaksproducten (SBI12) Vervaardiging van textiel (SBI13) Vervaardiging van kleding (SBI14) Vervaardiging van leer, lederwaren en schoenen (SBI15) Primaire houtbewerking en vervaardiging (SBI16) Vervaardiging papier- en kartonwaren (SBI17) Drukkerijen, reproductie van opgenomen media (SBI18) Vervaardiging van chemische producten (SBI20) Vervaardiging producten van rubber en kunststof (SBI22) Vervaardiging niet-metaalhoudende minerale producten (SBI23) Vervaardiging van metalen in primaire vorm (SBI24) Vervaardiging van producten van metaal (SBI25) Vervaardiging van computers en van elektronische en optische apparatuur (SBI26) Vervaardiging van elektrische apparatuur (SBI27) Vervaardiging van overige machines en apparaten (SBI28) Vervaardiging auto's, aanhangwagens en opleggers (SBI29) Vervaardiging van overige transportmiddelen (SBI30) Vervaardiging van meubels (SBI31) Vervaardiging van overige goederen (SBI32) Reparatie en installatie van machines en apparaten (SBI33) Reparatie van computers en consumentenartikelen (SBI95)

Bijlage 3: Specifieke tabellen over de maakindustrie

Omvang van de bedrijven in de Nederlandse maakindustrie op basis van aantal medewerkers

De onderstaande tabel geeft inzicht in de hoeveelheid bedrijven in de Nederlandse maakindustrie kijkend naar de vier groepen: microbedrijven, kleine bedrijven, middelgrote bedrijven en grote bedrijven.

Het overgrote deel van de bedrijven in de maakindustrie (87%) zijn zogenaamde microbedrijven (bedrijven met minder dan 10 medewerkers). Ongeveer één op de tien bedrijven valt in de categorie kleine bedrijven. Rond de 3,5% van de bedrijven hebben meer dan 50 medewerkers; daarvan heeft 0,5% meer dan 250 medewerkers. Deze nationale verspreiding geldt min of meer ook voor de regio Zuid-Holland.

Aantal medewerkers	Bedrijven in de Nederlandse maakindustrie	
	Aantal	Percentage
Microbedrijven (minder dan 10 medewerkers)	29.580	87%
Kleine bedrijven (10 - 50 medewerkers)	3.190	9,5%
Middelgrote bedrijven (50 - 250 medewerkers)	1.000	3%
Grote bedrijven (meer dan 250 medewerkers)	150	0,5%
Totaal aantal bedrijven in de maakindustrie	33.920	100%

Tabel 2: Omvang van de bedrijven in de Nederlandse maakindustrie (CBS, 2022).

Aantal bedrijfsvestigingen in de maakindustrie in Nederland en Zuid-Holland

De onderstaande tabel geeft inzicht in de hoeveelheid bedrijfsvestigingen in de maakindustrie (Nederland en Zuid-Holland) per segment. De meeste bedrijven zijn te relateren aan het segment ‘metaalproductieindustrie’ (SBI25).

Segment	Aantal bedrijfsvestigingen in Nederland	Aantal bedrijfsvestigingen in Zuid-Holland
Basismetaalindustrie (SBI24)	430	105
Metaalproductenindustrie (SBI25)	14.510	3.365
Elektrotechnische industrie (SBI26)	1.575	325
Elektrische apparatenindustrie (SBI27)	1.160	185
Machine-industrie (SBI28)	3.540	570

Auto- en aanhangwagenindustrie (SBI29)	880	115
Overige transportmiddelenindustrie (SBI30)	1.480	285
Reparatie en installatie van machines (SBI33)	11.615	2.230
Totaal aantal vestigingen in de maakindustrie	35.190	7.180
Totaal aantal vestigingen in de industrie	81.440	14.975

Tabel 3: Aantal bedrijfsvestigingen in de maakindustrie in Nederland en in Zuid-Holland (CBS, 2022).

Regionale spreiding van Metaalunie-leden in Zuid-Holland

De Koninklijke Metaalunie is een brancheorganisatie voor mkb-bedrijven actief in de metaalindustrie. De vereniging heeft meer dan 14.000 leden, waarvan er circa 2.560 gevestigd zijn in Zuid-Holland.

De onderstaande tabel geeft de regionale spreiding van Metaalunie-leden in Zuid-Holland weer, waarbij uitsluitend de gemeenten zijn weergegeven met meer dan 50 Metaalunie-leden.

Zuid-Hollandse gemeente met meer dan 50 Metaalunie-leden	Aantal Metaalunie-leden	Zuid-Hollandse gemeente met meer dan 50 Metaalunie-leden	Aantal Metaalunie-leden
Westland	298	Zwijndrecht	60
Rotterdam	218	Sliedrecht	60
Hoekse-Waard	142	Hardinxveld-Giessendam	60
Alphen aan den Rijn	113	Ridderkerk	58
Dordrecht	103	Pijnacker-Nootdorp	58
Lansingerland	85	Vlaardingen	53
Krimpenerwaard	73	Nieuwkoop	53
Goeree-Overflakkee	66	Barendrecht	51
Schiedam	62		
Totaal aantal leden in Zuid-Hollandse gemeenten met meer dan 50 Metaalunie-leden	1.551	Totaal aantal Metaalunie-leden in Zuid-Holland	2.562

Tabel 4: Spreiding van Metaalunie-leden in Zuid-Holland (Metaalunie, 2022)

Bijlage 4: 5 basisprincipes van veilig digitaal ondernemen

Het Digital Trust Center (DTC) is onderdeel van het ministerie van Economische Zaken en Klimaat en heeft voor ondernemers 5 basisprincipes van veilig digitaal ondernemen opgesteld. Bedrijven/ondernemers die de 5 basisprincipes opvolgen, vergroten de weerbaarheid tegen cyberrisico's die de bedrijfsvoering kunnen verstoren.

1. Inventariseer kwetsbaarheden	Inventariseer de IT-onderdelen, kwetsbaarheden en maak een risico-analyse. Bij risico's wordt gekeken naar beschikbaarheid, integriteit en vertrouwelijkheid.
2. Kies veilige instellingen	Controleer de instellingen van apparatuur, software en netwerk- en internetverbindingen. Pas standaardinstellingen aan en kijk kritisch naar functies en diensten die automatisch 'aan' staan.
3. Voer updates uit	Controleer of apparaten en software up-to-date zijn. Installeer beveiligingsupdates direct. Schakel automatische updates in zodat apparaten en software voortaan altijd draaien op de laatste versie.
4. Beperk toegang	Definieer per medewerker tot welke systemen en data toegang vereist is om te kunnen werken. Zorg dat toegangsrechten worden aangepast als iemand een nieuwe functie krijgt of bij de onderneming vertrekt.
5. Voorkom virussen en andere malware	Er zijn 4 manieren om malware te voorkomen: 1) stimuleer veilig gedrag van medewerkers, 2) gebruik een antivirusprogramma, 3) download apps veilig en 4) beperk de installatiemogelijkheden van software.

Meer informatie: https://www.digitaltrustcenter.nl

Een ander hulpmiddel is de website van Cyber Kracht: https://ikhebcyberkracht.nl/. Deze website is voor ondernemers in Zuid-Holland die meer willen weten over cybersecurity en over het digitaal veiliger maken van het bedrijf.

Bijlage 5: checklist voor het maken van afspraken met een IT- leverancier

Bedrijven in de maakindustrie besteden over het algemeen IT-gerelateerde zaken uit aan IT-dienstverleners. Met name voor kleinere bedrijven is het uitdagend om heldere en inzichtelijke afspraken (service level agreement – SLA) te maken met de IT-dienstverlener, zeker op het gebied van cyberweerbaarheid. Het Digital Trust Center (DTC) heeft voor bedrijven/ondernemers een checklijst gemaakt voor het maken van afspraken met een IT-leverancier.

1. Producten- en dienstenoverzicht	Wat gaat de IT-dienstverlener leveren qua IT-diensten en/of IT-apparatuur? Is het helder voor welke producten en diensten je zelf nog verantwoordelijk bent?
2. Onderhoud	Door wie wordt onderhoud uitgevoerd en om welk onderhoud gaat het dan precies? Welke regelmaat is er qua onderhoud? Word het onderhoud uitgevoerd op momenten dat het geen invloed heeft op de bedrijfscontinuïteit?
3. Preventieve beveiliging	Zijn alle apparaten voorzien van antivirussoftware? Is het netwerk voorzien van een firewall? Worden kritieke systemen extra beschermd (tweefactorauthenticatie)? Wie is voor welke beveiligingsmaatregelen verantwoordelijk? Vinden er periodieke controles plaats om zeker te stellen dat de beveiligingsmaatregelen functioneren?
4. Werkplekken	Is afgesproken wie verantwoordelijk is voor het opstellen en uitvoeren van het werkplekbeveiligingsbeleid? Worden medewerkers verplicht om een sterk wachtwoord te gebruiken? Worden gegevens op computers, laptops en andere mobiele apparaten versleuteld opgeslagen?
5. Gegevensbescherming	Waar wordt de bedrijfsinformatie opgeslagen, in de cloud of lokaal? Als het in de cloud wordt opgeslagen, is de informatie dan versleuteld? Wie heeft toegang tot de in de cloud opgeslagen data? Worden er back-ups gemaakt van informatie die niet in de cloud, maar lokaal wordt opgeslagen?
6. Cyberaanvallen en andere incidenten	Weet je bij wie je terecht kunt als er zich een cyberprobleem voordoet? Is vastgelegd binnen welke tijd de IT-dienstverlener moet reageren op een incidentmelding (response time) en binnen welke tijd een oplossing moet worden geboden (oplostijd)? Wat is de beschik-baarheid van de ondersteuning; heeft de leverancier een 24x7 service?
7. Prestatie-eisen	Wat wordt er in de afspraken toegezegd over de beschikbaarheid (uptime) van de systemen/software? Wat staat er in het SLA over hoe lang een dienst offline mag zijn voor bijvoorbeeld onderhoud of door storingen (downtime)?
8. Contractbreuk	Wat is de vergoeding als de overeengekomen afspraken niet worden nagekomen of niet (voldoende) worden nageleefd? Wat zijn de afspraken m.b.t. schadevergoedingen? Zijn er afspraken over aansprakelijkheid vastgelegd?

Meer informatie: https://www.digitaltrustcenter.nl/

Bijlage 6: Belangrijkste stappen met betrekking tot cyberweerbaarheid

1. Bewustwording	Verhogen van de bewustwording dat cyberweerbaarheid van belang is voor het bedrijf en de keten waarin het bedrijf zich bevindt.
2. Kennis vergaren	Vergaren van kennis om inhoudelijk beter te begrijpen waarom en hoe cyberweerbaarheid binnen het bedrijf vorm moet krijgen en/of verder geoptimaliseerd moet worden.
3. Identificatie	Verkrijgen van inzicht in welke mate cybersecurity risico's worden beheerst kijkend naar onder andere IT-systemen, OT-systemen, organisatie en data.
4. Bescherming	Het nemen van beschermende maatregelen op het vlak van cyberweerbaarheid: strategie, organisatie, techniek etc.
5. Detectie	Continu vaststellen of er sprake is van digitale dreiging (cyberdreiging) en hoe een eventuele cyberdreiging effect heeft of kan hebben op het bedrijf.
6. Reactie	Het beperken van de impact van een cybersecurity-incident op het bedrijf.
7. Herstel	Herstellen van beschadigde onderdelen van het bedrijf (IT, data, productie etc.) vanwege een voorgevallen cybersecurity-incident en het opstellen en uitvoeren van plannen om de cyberweerbaarheid van het bedrijf structureel te vergroten.

Bijlage 7: Twee voorbeelden gericht op human capital in cybersecurity

Voldoende goed opgeleide professionals zijn nodig om bij te dragen aan het vergroten van de cyberweerbaarheid van onder andere het bedrijfsleven actief in de maakindustrie. Security Delta heeft op dit vlak twee initiatieven opgezet:

1) Stimuleren van zij-instroom in cybersecurity

De website www.cybersecuritywerkt.nl is een hulpmiddel om zij-instroom en omscholing in cybersecurity te stimuleren en informatie aan te reiken over onder andere arbeidsmogelijkheden en bij- en omscholingstrajecten.

2) Vacatures in cybersecurity

De website www.securitytalent.nl is een hulpmiddel om vacatures, opleidingen, werkgevers actief op het gebied van (digitale) veiligheid en loopbaaninformatie te presenteren.

Publicatie informatie
Verhogen cyberweerbaarheid bij bedrijven in de Zuid-Hollandse maakindustrie

Een publicatie van
Security Delta (HSD)
Wilhelmina van Pruijsenweg 104
2595 AN Den Haag
T + 31 (0)70 2045180
Info@securitydelta.nl
www.securitydelta.nl
@HSD_NL

Auteur
Erik Knol

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

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