Cyberweerbaarheid in de logistieke sector

Frank van Summeren

Projectleider cyberweerbaarheid in de logistieke sector namens Security Delta

HSD

securitydelta.nl

HSD
securitydelta.nl

Inhoudsopgave

1. Programma cyberweerbaarheid van ondernemers 3
2. Logistieke sector 4
3. Onderzoeksopzet 5
4. Cybercriminaliteit in de logistieke sector 6
5. Cyberweerbaarheid in de logistieke sector 7
   - Beleid en organisatie 7
   - Techniek 9
   - Medewerkers 10
   - Cyberweerbaarheid van ondernemers en ketens in de logistiek 11
   - Behoeften van ondernemers in de logistieke sector ten aanzien van cyberweerbaarheid 11
   - Integrale benadering van cyberweerbaarheid 12
6. Initiatieven op cyberweerbaarheid 14
   - Nationaal Cyber Security Centrum 14
   - Digital Trust Center 14
   - Security Delta 14
   - Centrum voor Criminaliteitspreventie en Veiligheid 15
   - VNO NCW MKB Nederland 15
   - Transport en Logistiek Nederland 15
   - Evofenedex 15
   - IRO 16
   - Platform Veilig Ondernemen Rotterdam 16
   - VeiligheidsAlliantie regio Rotterdam 16
   - Cybernetwerk Zuid Hollandse Eilanden 17
   - Platform Veilig Ondernemen Den Haag 17
   - Regionaal Samenwerkingsverband Integrale Veiligheid 18
   - Cyber Netwerk Drechtsteden 18
   - Centre of Expertise Cybersecurity 18
7. Conclusies en aanbevelingen 19
   - Cyberweerbaarheid van ondernemers in de logistieke sector 19
   - Ketenafhankelijkheid ten aanzien van cyberweerbaarheid 19

Initiatieven om de cyberweerbaarheid te bevorderen 20
Ondernemers activeren om de cyberweerbaarheid te bevorderen 20
Cyberweerbaarheidscentrum 21
Aanbevelingen ten aanzien van cyberweerbaarheid 21

1. Programma cyberweerbaarheid van ondernemers

De Metropoolregio Rotterdam Den Haag (MRDH) erkent het belang van digitalisering als belangrijke voorwaarde voor economische innovatie. Nieuwe technologische ontwikkelingen zoals artificial intelligence, internet of things en blockchain geven een impuls aan de economie in de regio. De 23 gemeenten in de Metropoolregio Rotterdam Den Haag zetten al een aantal jaar in op een goede digitale bereikbaarheid en (nieuwe) digitale technologieën. Digitalisering levert naast economische kansen (zoals kostenbesparing door efficiëntie en nieuwe producten en diensten door innovatie) ook dreigingen op. Digitalisering zorgt immers voor een sterkere afhankelijkheid van digitale processen en netwerken. Digitale processen raken steeds meer verweven en verbonden met fysieke processen en apparaten. Dit betekent dat een cyberaanval de continuïteit van een (digitaal en/of fysiek) proces kan verstoren met de mogelijke gevolgen van dien voor de getroffen onderneming(en) en de maatschappij. Een weerbare economie is zodoende gebaat bij cyberweerbaarheid van ondernemers.

Bedrijven staan dagelijks bloot aan cyber security risico's zoals bedrijfsspionage en afpersing door hackers die met ransomware computersystemen vergrendelen waardoor vitale bedrijfsprocessen niet meer (optimaal) werken met verlies van omzet en reputatieschade tot gevolg. Desondanks nemen bedrijven nog niet altijd de noodzakelijke maatregelen om zich voldoende te beschermen tegen cybercriminaliteit. In 2020 is, in opdracht van de Economic Board Zuid-Holland, een onderzoek verricht naar de impact van cyberonveiligheid. Uit het onderzoek kwam naar voren dat jaarlijks ongeveer 20% van de MKB bedrijven slachtoffer wordt van een cyberbaanval. De indicatieve kosten van cyberonveiligheid in de provincie Zuid-Holland bedragen jaarlijks tussen de 2 tot 4 miljard euro. De verwachting is dat het slachtofferschap onder ondernemers en de daarbij horende schade in de toekomst beide gaan stijgen door de vergaande en versnelde digitalisering (Cybergereedheid Provincie Zuid-Holland, Koen Gijsbers, 2020).

De (digitale) processen, toegepaste technologieën, (potentiële) kwetsbaarheden en daaruit voortkomende cyber security risico's verschillen per sector. Dit betekent dat een sectorale aanpak het meest voor de hand ligt om de cyberweerbaarheid van ondernemers in verschillende sectoren te bevorderen. De Security Delta start daarom een programma om de cyberweerbaarheid van ondernemers in zes essentiële sectoren (life sciences & health, water, logistiek, maakindustrie, maritiem, lucht- en ruimtevaart) in de regio Zuid-Holland te bevorderen. Dit initiatief wordt mede mogelijk gemaakt door de Metropoolregio Rotterdam Den Haag subsidie Sectoraal Digitaal Veilig.

In deze rapportage wordt ingegaan op de cyberweerbaarheid van ondernemers in de logistieke sector. Hierbij wordt aandacht besteed aan actuele vraagstukken op het terrein van cyber security in de logistieke sector. Ook wordt er ingegaan op lopende initiatieven om de cyberweerbaarheid van ondernemers in de logistieke sector te bevorderen en worden er suggesties gedaan om deze waar mogelijk en gewenst met elkaar te verbinden en te versterken.

2. Logistieke sector

Nederland is toonaangevend in de logistiek met haar diverse mainports zoals de Haven van Rotterdam en Schiphol. Dit zorgt ervoor dat Nederland een aantrekkelijke vestigingslocatie is voor ondernemers. De logistieke sector draagt steeds meer bij aan de Nederlandse economie. Zo werken er ruim 800.000 medewerkers in de logistieke sector en is de toegevoegde economische waarde jaarlijks ruim 30 miljard euro (volgens een onderzoek dat in 2020 is verricht door Buck Consultants International in opdracht van Prologis). Logistiek is bovendien onmisbaar voor andere sectoren zoals de voedsel en maakindustrie. Dit maakt logistiek een belangrijke economische sector. Om de toonaangevende positie in de logistiek te behouden wordt er geïnvesteerd in innovatie waaronder digitalisering van de sector.

Zuid-Holland is de transportprovincie bij uitstek. Dit is mede het gevolg van de aanwezigheid van de Haven van Rotterdam, de Greenports Oost en Westland, de Bollenstreek en Boskoop, een aantal grote bedrijven(terreinen) en de grote stedelijke gebieden. Voor de economische bedrijvigheid in de MRDH regio is de aan- en afvoer van goederen en grondstoffen essentieel. De logistieke sector biedt in de regio werkgelegenheid voor ongeveer 50.000 medewerkers. Om toonaangevend te blijven in de logistiek worden bedrijfsprocessen continue vernieuwd en worden er samenwerkingen in de logistieke keten aangegaan. Informatie in en tussen bedrijven, opdrachtgevers en opdrachtnemers (zoals klantgegevens en voertuigposities) wordt steeds meer via internet gedeeld. Het digitaal delen van informatie ten behoeve van het logistieke proces is eenvoudiger, sneller en efficiënter, maar dit maakt ondernemingen in deze sector ook kwetsbaar voor cyber security risico’s.

Gezien de toegevoegde economische waarde van de logistieke sector en de afhankelijkheid van andere sectoren van logistieke processen vormt logistiek een van de zes essentiële sectoren waarop het programma cyberweerbaarheid van de Security Delta zich richt. De logistieke sector bestaat uit goederenvervoer en personenvervoer. Transport vindt plaats over de weg, het spoor, het water en de lucht. Hierbij wordt gebruik gemaakt van een logistieke keten. Het betreft de gehele organisatie, planning en uitvoering van de stroom van producten en diensten. Informatievoorziening is cruciaal voor het beheersingsproces van personen- en goederenbewegingen. Deze is doorgaans gedigitaliseerd. Belangrijke schakels in de logistieke keten ten aanzien van goederenvervoer zijn de aanvoer, productie, opslag, overslag en distributie. Er is zodoende sprake van een ketenafhankelijkheid van de verschillende bedrijven die actief zijn in de logistieke keten. Dit betekent dat wanneer er ergens in de keten een (cyber security) incident plaatsvindt, dit aanzienlijke gevolgen kan hebben voor de gehele keten. Dit betekent dat cyberweerbaarheid niet alleen betrekking heeft op afzonderlijke bedrijven, maar op gehele logistieke processen en ketens.

In deze rapportage wordt expliciet ingegaan op bedrijven in de logistieke sector die zich richten op personen- en/of goedervervoer over de weg en/of over het spoor. Dit komt doordat er in het programma cyberweerbaarheid onderscheid wordt gemaakt tussen de sectoren logistiek, maritiem, lucht- en ruimtevaart. In twee andere rapportages wordt expliciet ingegaan op de cyberweerbaarheid van ondernemers in de maritieme sector en in de sector lucht- en ruimtevaart.

3. Onderzoeksopzet

In dit hoofdstuk wordt beschreven op welke wijze de opzet en de uitvoering van het onderzoek hebben plaatsgevonden naar de cyberweerbaarheid van ondernemers in de logistieke sector. Er wordt ondermeer ingegaan op de gehanteerde onderzoeksstrategie en de methoden van onderzoek die zijn toegepast.

De vraagstelling die centraal staat in dit onderzoek in het kader van de rapportage betreft: wat is de cyberweerbaarheid van ondernemers in de logistieke sector? Wat zijn actuele vraagstukken op het terrein van cyber security in de logistieke sector? Welke lopende initiatieven zijn er om de cyberweerbaarheid van ondernemers in de logistieke sector te bevorderen? En hoe kunnen deze worden versterkt en/of aangevuld met nieuwe initiatieven om de cyberweerbaarheid van ondernemers in de logistieke sector te bevorderen?

Er is gestart met het verrichten van literatuuronderzoek naar cyberweerbaarheid van ondernemers in zijn algemeenheid en in de logistieke sector in het bijzonder. Vervolgens zijn organisaties en bedrijven in de sector logistiek in de MRDH regio in kaart gebracht. Hierna zijn deze organisaties en bedrijven benaderd om een afspraak te maken voor een interview. In de interviews is ingegaan op vitale bedrijfsprocessen en daarbij horende (potentiële) kwetsbaarheden en daaruit voortkomende cyber security risico's bij ondernemers in de logistieke sector. Daarnaast is geïnventariseerd welke cyber security vraagstukken zich voordoen in de sector. Op basis van het verkregen beeld is waar mogelijk de verbinding gelegd met de Security Delta zodat zij desgewenst partners uit haar netwerk kan positioneren die beschikken over de benodigde kennis, ervaring, referenties en innovatieve (technologische) oplossingen voor de betreffende cyber security vraagstukken. Tevens zijn lopende initiatieven op het terrein van de bevordering van cyberweerbaarheid van ondernemers in kaart gebracht. Tot slot is geïnventariseerd of er bereidheid is om te participeren in een mogelijk op te richten cyberweerbaarheidscentrum voor de sector en/of een bijdrage te leveren om deze (mede)mogelijk te maken.

In het kader van het onderzoek is gesproken met bedrijven in de logistieke sector, branche organisaties, publiek private samenwerkingsverbanden, lokale, regionale en nationale overheden. Aan het onderzoek hebben de volgende organisaties geparticipeerd en een bijdrage geleverd: Provincie Zuid-Holland, Innovation Quarter, gemeente Rotterdam, politie eenheid Rotterdam, Veiligheidsregio Rotterdam Rijnmond, DCRM Milieudienst Rijnmond, Platform Veilig Ondernemen Rotterdam, Veiligheidsalliantie Regio Rotterdam, Resilient Rotterdam, gemeente Dordrecht, Cybernetwerk Zuid-Hollandse Eilanden, Werkgevers Drechtsteden, Cybernetwerk Drechtsteden, Nationaal Cyber Security Center, Digital Trust Center, Adviescentrum Bescherming Vitale Infrastructuur, Vereniging van Nederlandse Gemeenten, ministerie van Justitie en Veiligheid, Centrum voor Criminaliteitspreventie en Veiligheid, VNO NCW, MKB Nederland, IRO, Transport en Logistiek Nederland, Evofenedex, PostNL, ProRail, Nederlandse Spoorwegen, gemeente Den Haag, Platform Veilig Ondernemen Den Haag, Regionaal Samenwerkingsverband Integrale Veiligheid, Resilient The Hague, Centre of Expertise Cybersecurity en de politie eenheid Den Haag. Van de afgenomen interviews met stakeholders zijn gespreksverslagen gemaakt welke de basis vormen voor de rapportage over de cyberweerbaarheid van ondernemers in de logistieke sector.

4. Cybercriminaliteit in de logistieke sector

In dit hoofdstuk wordt ingegaan op de aard, omvang en verschijningsvormen van cybercriminaliteit in de logistieke sector. Ongeveer 20% van de bedrijven actief in de logistieke sector is slachtoffer geweest van een cyberaanval. Bij ongeveer een vijfde van deze bedrijven is vanwege de cyberaanval de informatievoorziening en daarmee het bedrijfsproces tijdelijk verstoord waardoor deze niet naar behoren kon functioneren. Dit is ook de grootste angst van bedrijven actief in de logistieke sector omdat dit direct raakt aan hun bedrijfsvoering De informatievoorziening is van cruciaal belang voor het beheersingsproces van personen- en goederenbewegingen.

Bedrijven in de logistieke sector lopen een niet gering risico om slachtoffer te worden van cybercriminaliteit door de aard van hun bedrijfsactiviteiten, de producten en diensten die ze vervoeren voor derden en/of de mogelijke buit die er bij hun te halen is. Daarnaast lopen de bedrijven in de logistieke sector het risico dat ze door criminele netwerken in de georganiseerde (drugs)criminaliteit worden misbruikt om onbewust illegale goederen te vervoeren. Deze criminele netwerken hebben geen baat bij het verstoren van de bedrijfsvoering, maar willen inzicht en/of invloed hebben op de logistieke keten rond een lading waarin hun illegale goederen (zoals drugs) ongezien vervoerd worden.

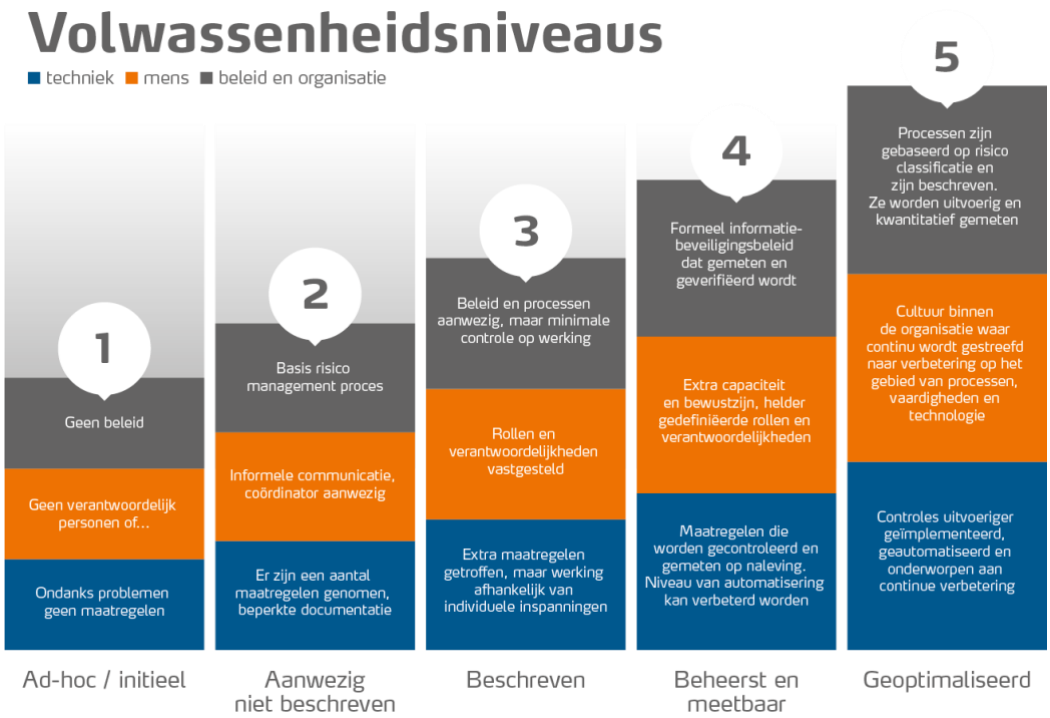
De meest voorkomende verschijningsvormen van cybercriminaliteit zijn malware, ransomware, DDoS aanvallen, onderschepte betalingen, factuurfraude en CEO fraude. Wat opvalt is dat kwaadwillenden zich vaak voordoen als een klant, collega of leverancier om bepaalde informatie te verkrijgen van een organisatie. In sommige gevallen is er sprake van doelbewuste gerichte pogingen waarbij het ging om specifieke functies, medewerkers en/of bedrijfsonderdelen. Het worst case scenario voor bedrijven in de logistieke sector is dat de informatievoorziening voor de bedrijfsvoering wordt uitgeschakeld of overgenomen waardoor de continuïteit van de bedrijvigheid in het geding komt. Daarnaast zijn bedrijven op hun hoede voor diefstal en/of het manipuleren van gevoelige vertrouwelijke informatie (Cybersecurity in de logistieke keten, Robin de Veer en Robert Wezeman, 2020).

Het merendeel van bedrijven actief in de logistieke sector werkt samen met tientallen andere bedrijven. Veelal wordt er in ieder onderdeel van het gehele operationele proces samengewerkt met een of meerdere ketenpartners. Er wordt informatie gedeeld tussen en met ketenpartners ten behoeve van productontwikkeling en/of dienstverlening. Zo wordt er gebruik gemaakt van pincodes om ondermeer goederen af te halen. De werkwijze met pincodes is niet waterdicht. Pincodes zijn regelmatig zwak en/of worden (te) gemakkelijk met (te) veel andere partijen gedeeld via verschillende soms onveilige communicatiekanalen (zoals email). Hierdoor is de kans aanwezig dat pincodes in de verkeerde handen vallen, waardoor bijvoorbeeld een lading kan worden ontvreemd door een kwaadwillende. Er wordt over het algemeen onderling met ketenpartners niet of nauwelijks informatie gedeeld over slachtofferschap van een cyberaanval en/of cyber security risico's. Terwijl dit de cyberweerbaarheid van de gehele keten zou kunnen bevorderen omdat er in dat geval kan worden geleerd van cyber security incidenten die zich elders (in de keten) reeds hebben voorgedaan waarna hiervoor de benodigde maatregelen kunnen worden genomen om slachtofferschap in de toekomst te voorkomen.

In de logistieke sector wordt regelmatig door een afdeling of zelfs door een geheel bedrijf gebruik gemaakt van één en hetzelfde algemeen account en bijbehorend wachtwoord om toegang te krijgen tot een systeem. Op deze manier kunnen (te)veel (voormalig) medewerkers toegang krijgen tot gevoelige informatie, terwijl een deel van hen deze mogelijkerwijs niet (meer) nodig heeft voor de uitvoering van hun werkzaamheden. Daarnaast kan op deze manier niet worden gemonitord wie op welk moment op welke plek met welk doel welke informatie raadpleegt. Vanzelfsprekend verhoogt dit de kans op een insider threat waardoor het voor een kwaadwillende niet eens nodig is om van buitenaf te infiltreren om bepaalde gewilde informatie te bemachtigen omdat deze met geringe inspanningen ook van binnenuit kan worden verkregen

5. Cyberweerbaarheid in de logistieke sector

In dit hoofdstuk wordt ingegaan op cyberweerbaarheid van ondernemers in de logistieke sector. Het gaat erom in welke mate zij (beleidsmatige, technische en/of personele) maatregelen hebben genomen om cyber security risico's (waar mogelijk) te voorkomen en (waar nodig) te reduceren om de continuïteit van hun bedrijfsvoering te waarborgen. Om de cyberweerbaarheid van ondernemers in de logistieke sector te duiden is gebruik gemaakt van de cyber security routekaart van Threadstone (een partner van de Security Delta).



Beleid en organisatie

Bedrijven in de logistieke sector lopen een niet gering risico om slachtoffer te worden van cybercriminaliteit door de aard van hun bedrijfsactiviteiten, de producten en diensten die ze vervoeren voor derden en/of de mogelijke buit die er bij hun te halen is. Een groot deel van de ondernemers in de logistieke sector is zich onvoldoende bewust van de kans op slachtofferschap van cybercriminaliteit en de mogelijke impact daarvan op hun bedrijfsvoering. In sommige gevallen leidt een cyberaanval zelfs het einde van een onderneming in. Doordat de kans op slachtofferschap van cybercriminaliteit en de mogelijke impact van een cyberaanval wordt onderschat door met name kleinere bedrijven worden er door hun niet altijd de benodigde (beleidsmatige en organisatorische) maatregelen genomen om de cyberweerbaarheid te bevorderen. De grotere bedrijven schatten de dreiging van cybercriminaliteit over het algemeen hogere in dan kleinere bedrijven en zien cyber security (beleid) vaak ook als een essentieel onderdeel van hun bedrijfsvoering. Met name grotere bedrijven stellen ook steeds vaker eisen op het terrein van cyber security aan de bedrijven met wie zij (digitaal) samenwerken en informatie delen. Zij zijn zich ervan bewust dat de cyberweerbaarheid niet alleen afhankelijk is van de inspanningen van hun eigen organisatie, maar ook (in toenemende mate) van die van hun samenwerkingspartners. In dit geval vraagt een bedrijf bijvoorbeeld inzage in het cyber security beleid van haar samenwerkingspartners met bijbehorende certificeringen (zoals ISO 27001) of wordt er een verwerkingsovereenkomst opgesteld voor de onderlinge uitwisseling van informatie.

Cyber security is bij grotere bedrijven veelal belegd bij een Chief Information Security Officer die (mede afhankelijk van de grootte van de organisatie en de aard van de werkzaamheden) al dan niet wordt bijgestaan door een CISO office. Het CISO office heeft veel kennis en expertise op het terrein van cyber security doorgaans zelf in huis. Daar waar nodig wordt specifieke gespecialiseerde kennis en expertise van buiten naar binnen gehaald. Hiervoor wordt samengewerkt met (een consortium van) cyber security bedrijven die wanneer gewenst specifieke gespecialiseerde kennis en expertise inbrengen. Bepaalde type specialismen zijn dermate kostbaar dat de betreffende experts niet vast in dienst kunnen worden genomen. Bij kleinere bedrijven is cyber security veelal de verantwoordelijkheid van een directeur, manager en/of systeembeheerder die dit naast hun andere reguliere werkzaamheden invulling (proberen te) geven.

Een aanzienlijk deel van de bedrijven in de logistieke sector heeft hun IT hardware volledig buitenshuis geplaatst bij een externe organisatie. Veel kleinere bedrijven kiezen er al dan niet noodgedwongen voor om hun ICT te outsourcen. Bedrijven kunnen zich hierdoor richten op hun primaire bedrijfsvoering en hebben geen directe bemoeienis meer met het onderhoud en beheer van ICT. Dit betekent dat ze niet alleen voor hun ICT maar ook voor de cyber security (voor een deel) afhankelijk zijn van een externe organisatie. In sommige gevallen zijn er in dit geval ook geen concrete afspraken gemaakt over cyber security (waaronder monitoring, detectie, incident response, recovery). Dit komt bijvoorbeeld doordat de ondernemer er vanuit gaat dat dit met het outsourcen van de ICT geregeld is zonder dat cyber security expliciet met de externe organisatie is besproken. Daarnaast krijgt cyber security, doordat de ICT bij een externe organisatie is belegd, niet altijd de aandacht die het verdient in een bedrijf omdat dit door het extern uitbesteden uit het gezichtsveld is verdwenen en hierdoor minder gesprek van onderwerp is in de organisatie.

Grotere bedrijven geven over het algemeen aan dat cyber security hoge prioriteit heeft binnen de organisatie. Daarnaast zijn zij van oordeel dat de kosten van cyber security opwegen tegen de baten en dat hun bedrijf goed is beveiligd tegen kwaadwillenden door de (beleidsmatige en organisatorische) maatregelen die zijn getroffen. Daar staat tegenover dat zij door de omvang van hun organisatie en de aard van hun werkzaamheden eerder een gericht doelbewust target kunnen vormen van kwaadwillenden, wat vraagt om betere bescherming. Grotere bedrijven hebben doorgaans de beschikking over meer kennis, expertise, capaciteit en middelen voor cyber security. Hierdoor zijn zij over het algemeen, betere dan kleinere bedrijven, in staat om externe cyber security dreigingen buiten de deur te houden. Daar staat tegenover dat interne dreigingen (ook bij grotere bedrijven) soms worden verwaarloosd. Er wordt regelmatig door een afdeling of zelfs door een geheel bedrijf gebruik gemaakt van één en hetzelfde algemeen account en bijbehorend wachtwoord om toegang te krijgen tot een systeem. Op deze manier kunnen (te) veel (voormalig) medewerkers toegang krijgen tot gevoelige informatie, terwijl een deel van hen deze niet (meer) nodig heeft voor de uitvoering van hun werkzaamheden. Ook pincodes om ondermeer goederen af te halen zijn regelmatig zwak en/of worden (te) gemakkelijk met (te) veel andere partijen gedeeld via verschillende soms onveilige communicatiekanalen (zoals email). Hierdoor is de kans aanwezig dat pincodes in de verkeerde handen vallen, waardoor bijvoorbeeld een lading kan worden ontvreemd door een kwaadwillende.

Ruim de helft van de bedrijven beschikt over een crisisplan dat in werking kan treden wanneer er zich een cyber security incident voordoet. Een derde van de bedrijven heeft (nog) geen crisisplan voor een cyberaanval. Het overgrote deel van deze bedrijven is wel voornemens om op termijn een crisisplan op te stellen waardoor zij in staat worden gesteld om adequaat te reageren op een (dreigend) cyber security incident. Punt van aandacht is dat een deel van de bedrijven die over een crisisplan beschikken deze (nog) niet in de praktijk hebben getest. Bij een deel van de bedrijven zijn de medewerkers ook niet bekend met het crisisplan. Door te gaan oefenen met het crisisplan kan een bedrijf zich voorbereiden op een cyber security incident waarmee ze in de toekomst (mogelijk) te maken (kunnen) krijgen en wordt er bovendien voor gezorgd dat medewerkers hiermee bekend zijn/raken.

“Een cyberaanval is regelmatig einde bedrijf, tenzij je een plan b hebt. Daarmee kun je een cyberaanval overleven. Hiervoor is het belangrijk dat een bedrijf zijn vitale primaire bedrijfsprocessen in kaart brengt en bedenkt hoe de continuïteit daarvan ten alle tijden kan worden gewaarborgd. Dit betekent dat een ondernemer moet begrijpen waar zijn afhankelijkheden zitten.” (Respondent interview)

Techniek

Bedrijven in de logistieke sector lopen een niet gering risico om slachtoffer te worden van cybercriminaliteit. Bedrijven die zich hiervan bewust zijn hebben doorgaans meer technische maatregelen getroffen dan bedrijven die in de veronderstelling zijn dat ze een minder prominente rol spelen in de logistieke keten. Bedrijven die cyber security een hoge prioriteit geven zijn over het algemeen van oordeel dat hun organisatie door de getroffen technische maatregelen goed is beschermd tegen cyber security dreigingen.

Het overgrote deel van de bedrijven hanteert toegangsbeheer voor met name vertrouwelijke en gevoelige informatie. Het betreft hier bijvoorbeeld bedrijfsgevoelige informatie of privacy gevoelige informatie van klanten. Het gebruik van toegangsbeheer moet ervoor zorgen dat vertrouwelijke en gevoelige informatie alleen toegankelijk is voor medewerkers met bepaalde rechten die deze data voor legitieme doelen moeten gebruiken. Dit betekent dat medewerkers die deze data niet of slechts in geringe mate nodig hebben voor de uitoefening van hun werkzaamheden niet of slechts in beperkte mate toegang hebben tot deze data. De data wordt in dit geval bijvoorbeeld geclassificeerd aan de hand van een risicoanalyse. Er wordt, door met name grotere bedrijven, gebruik gemaakt van een access control list waarmee wordt bepaald wie op welk moment toegang heeft tot welke informatie vanaf welke locatie. Om toegang te krijgen moet een medewerker een wachtwoord invoeren die is gekoppeld aan bij voorkeur zijn persoonlijke account. Daarnaast wordt bij verschillende bedrijven Multi Factor Authenticatie gehanteerd waarbij de betreffende medewerker via bijvoorbeeld een authenticatie app op zijn mobiele telefoon een extra code moet opgeven om toegang te krijgen. Een andere mogelijkheid is dat de biometrische gegevens van een medeweker hem of haar toegang verschaffen. Bij verschillende bedrijven wordt iedere handeling in een systeem gelogd. Zo kan er altijd worden teruggezocht wie op welk moment vanaf welke locatie welke data heeft opgevraagd, ingezien en/of heeft gemuteerd. Door loggegevens en gebruikersactiviteiten te monitoren kunnen afwijkende handelingen (vroegtijdig) worden gedetecteerd.

Mocht data ondanks de genomen technische maatregelen toch in het bezit komen van een kwaadwillende dan kan met encryptie ervoor worden gezorgd dat de data onleesbaar en hierdoor onbruikbaar is. Verschillende bedrijven anonimiseren en/of pseudonimiseren privacy gevoelige data. Ook wordt privacy gevoelige data door bedrijven afgeschermd met behulp van encryptie. Tot slot wordt privacy gevoelige data die niet meer benodigd is vernietigd.

Veel bedrijven maken gebruik van netwerksegmentatie waarmee de schade van een mogelijke cyberaanval (zoals een ransomware of DDoS aanval) kan worden beperkt mocht deze zich voordoen (ondanks andere getroffen technische maatregelen). Bij netwerksegmentatie wordt het netwerk van een bedrijf verdeeld in verschillende zones waardoor mogelijkerwijs kan worden voorkomen dat een virus of een indringer zich (verder) kan verspreiden in het gehele netwerk. Zo beperkt het cyber security incident zich waarschijnlijk tot een deel van het netwerk en blijven andere delen van het netwerk onaangetast. De verschillende zones kunnen worden gedefinieerd met firewalls en access control lists. Bij het definiëren van zones kan ook onderscheid worden gemaakt tussen de gevoeligheid en vertrouwelijkheid van data.

Tot slot maakt het overgrote deel van de bedrijven gebruik van backups, waardoor niet alle informatie verloren gaat als zij bijvoorbeeld worden getroffen door een ransomware aanval waarmee computersystemen worden vergrendeld waardoor bedrijfsprocessen niet meer (optimaal) werken. Backups vinden veelal minimaal dagelijks plaats en worden vaak op verschillende plaatsen opgeslagen (zowel online in de cloud als offline in een fysieke omgeving). Bedrijven zien backups als een essentiële maatregel om snel weer up and running te zijn wanneer zij (ondanks andere

getroffen technische maatregelen) slachtoffer worden van een cyberaanval. Op deze manier kan de continuïteit van de bedrijfsvoering worden gewaarborgd.

Verschillende met name kleinere bedrijven kiezen er soms noodzakelijkerwijs voor om hun ICT te outsourcen. In dat geval zijn er niet altijd duidelijke afspraken gemaakt over cyber security en te nemen technische maatregelen. Soms is onduidelijk wie wat beheerd en wie verantwoordelijk is voor de continuïteit van processen ten behoeve van de bedrijfsvoering.

Medewerkers

Medewerkers kunnen de sterkste maar ook de zwakste schakel vormen wat betreft de cyberweerbaarheid van een onderneming. Met technische maatregelen kunnen met name cyber security dreigingen van buitenaf worden geweerd. Maar zonder cyber security awareness bij medewerkers loopt een bedrijf (nog steeds) een verhoogd risico op een cyber security incident (van binnenuit). Een voorbeeld hiervan zijn medewerkers die zich (onbewust) niet houden aan het cyber security beleid en technische maatregelen omzeilen uit efficiëntie overwegingen. Medewerkers die onbewust onbekwaam op cyber security zijn vormen een risico wat betreft cyberweerbaarheid. Terwijl medewerkers die bewust bekwaam zijn een belangrijke rol (kunnen) spelen in het bevorderen van de cyberweerbaarheid van een onderneming. Een voorbeeld hiervan is het hanteren van het vier ogen principe om de kans op slachtofferschap van CEO fraude te reduceren.

Bedrijven proberen cyber security awareness te creëren bij hun medewerkers door ze te wijzen op het cyber security beleid bij indiensttreding. Daarnaast worden er door bedrijven cursussen op het terrein van cyber security aangeboden aan hun medewerkers. Ook wordt er gecontroleerd of medewerkers zich houden aan de protocollen en procedures op het terrein van cyber security. Een voorbeeld hiervan is het delen van een test phishing email die door een ethical hacker is opgesteld en is gedeeld met medewerkers. Bij een dergelijke test in de regio werd door ongeveer 30% op de phishing email geklikt en ongeveer 15% vulde de gevraagde gegevens in. Wanneer dit een poging was geweest van een kwaadwillende had dit tot aanzienlijke economische en/of reputatieschade kunnen leiden. Tot slot informeren bedrijven hun medewerkers (bijvoorbeeld via een nieuwsbrief) over actuele cyber security dreigingen (waarbij ook regelmatig wordt verwezen naar cyber security incidenten die zich elders voordeden).

Bij verschillende bedrijven is er (te) weinig aandacht voor insider threats. Dit geldt zowel voor kleinere als grotere bedrijven. Er zijn verschillende voorbeelden van misstanden bij bedrijven waarbij (voormalig) medewerkers (nog steeds) toegang hebben tot data, terwijl zij die voor de uitoefening van hun werkzaamheden niet (meer) nodig hebben, en deze informatie misbruiken om achter de locatie van bijvoorbeeld een container te komen waarna de inhoud daarvan kan worden ontvreemd. Op deze manier worden de getroffen maatregelen die een onderneming heeft genomen om (externe) cyber security dreigingen buiten de deur te houden te niet gedaan door cyber security dreigingen van binnenuit. Een kwaadwillende kiest waar mogelijk veelal voor de weg van de minste weerstand en in dit geval is de mens de zwakste schakel in de cyberweerbaarheid van een onderneming. Verschillende bedrijven hebben processen ingericht rondom de uitdiensttreding van medewerkers zodat automatisch gebruikersrechten worden uitgeschakeld van de betreffende medewerker wanneer degene daar niet meer werkzaam is.

“Cyberweerbaarheid is sterk afhankelijk van menselijk gedrag. Bij verschillende bedrijven is de cyber security goed geregeld, maar wordt er voor een systeem door alle medewerkers wel gebruik gemaakt van één en hetzelfde account en wachtwoord. In dit geval geef je in feite de sleutel van je bedrijf weg.” (Respondent interview)

Er moet continue geïnvesteerd worden in de cyber security awareness van medewerkers. Wanneer dit niet gebeurt dan neemt deze gedurende de tijd vaak af. Bij sommige bedrijven wordt een (intern of extern) cyber security incident aangewend om cyberweerbaarheid (weer) top of mind te maken bij hun medewerkers. Veelal wordt er dan verwezen naar cyber security incidenten (en hun economische en/of maatschappelijke gevolgen) die zich elders hebben voorgedaan.

“Cyber security moet richting ondernemers niet alleen worden ingestoken via ICT, maar ook via menselijk gedrag. ICT is relatief ingewikkeld voor ondernemers, terwijl menselijk gedrag eenvoudiger is te duiden. Daar komt bij dat veel cyber security incidenten ontstaan door menselijk gedrag. De grootste winst is te behalen met het laaghangend fruit. Hierbij gaat het ondermeer om wachtwoordbeleid, backups en een backup plan.” (Respondent interview)

Cyberweerbaarheid van ondernemers en ketens in de logistiek

Het merendeel van bedrijven actief in de logistieke sector werkt samen met tientallen andere bedrijven. Veelal wordt er in ieder onderdeel van het gehele operationele proces samengewerkt en informatie gedeeld met een of meerdere ketenpartners. Bedrijven in de logistieke sector zijn zich bewust van de ketenafhankelijkheid. Zij onderkennen dat de cyberweerbaarheid niet alleen afhankelijk is van de inspanningen van hun eigen organisatie, maar ook (in toenemende mate) van die van hun samenwerkingspartners in de keten. Desondanks wordt er tussen bedrijven nog niet of nauwelijks samengewerkt en informatie gedeeld op het terrein van cyber security. Dit is een gemiste kans omdat door informatie over kwetsbaarheden, dreigingen, (bijna) incidenten, best practices en lessons learned te delen de cyberweerbaarheid van afzonderlijke bedrijven en daarmee van de gehele logistieke keten kan worden bevorderd.

Behoeften van ondernemers in de logistieke sector ten aanzien van cyberweerbaarheid

Het slachtofferschap van cybercriminaliteit onder ondernemers in de logistieke sector is aanzienlijk. Het is zodoende van belang om de cyberweerbaarheid van ondernemers in de logistieke sector te bevorderen. Er doen zich twee barrières voor die ervoor zorgen dat het verhogen van de cyberweerbaarheid van ondernemers (nog) niet optimaal verloopt. De eerste barrière vormt het überhaupt bereiken van de ondernemers. Ondernemers in de logistieke sector verkrijgen informatie (over cyber security) ondermeer via het nieuws van media, websites, nieuwsbrieven, bijeenkomsten, brancheorganisaties, (publieke en/of private) samenwerkingsverbanden en andere ondernemers. De tweede barrière vormt het gedrag van ondernemers. Ondernemers laten zich niet zomaar aanzetten om te investeren in cyber security maatregelen. Dit komt mede doordat ondernemers het risico op slachtofferschap van cybercriminaliteit en de mogelijke gevolgen daarvan onderschatten en/of omdat ze onvoldoende kennis hebben om hun cyberweerbaarheid daadwerkelijk te bevorderen. Dit betekent dat ondernemers enerzijds behoefte hebben aan de inzichten van andere ondernemers (bij voorkeur uit de logistieke sector) over cyber security dreigingen zodat zij deze op waarde kunnen schatten voor hun eigen bedrijf. Anderzijds hebben ondernemers behoefte aan concrete handvatten om gerichte (beleidsmatige, technische, personele) maatregelen te nemen om cyber security risico’s (waar mogelijk) te voorkomen en (waar nodig) te reduceren om de continuïteit van hun bedrijfsvoering te waarborgen.

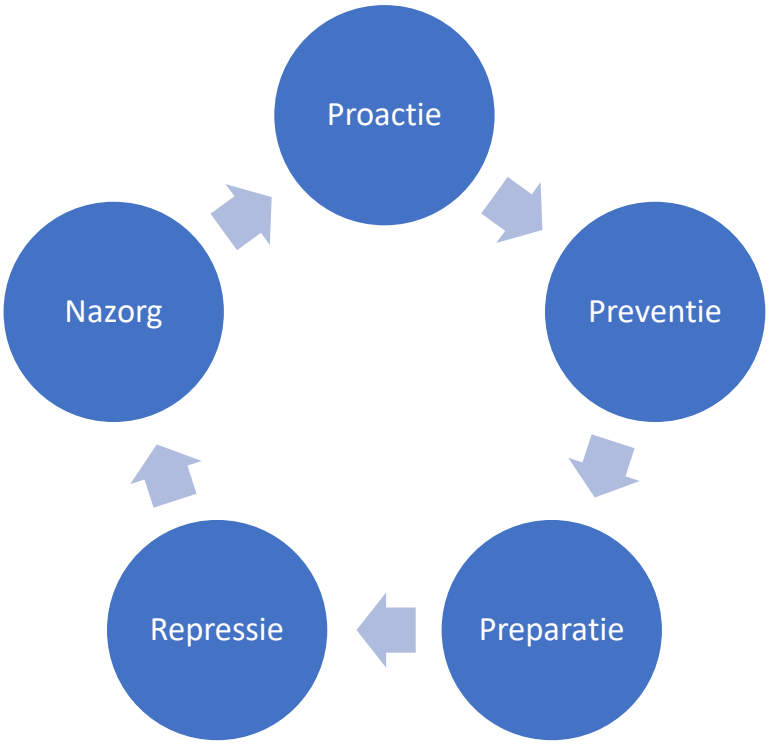
“Het beeld is dat het nog niet goed gesteld is met de cyberweerbaarheid van ondernemers. We zien het aantal cyberaanvallen toenemen en het aantal slachtoffers ook. We zitten nog steeds in de fase dat ondernemers bewust moeten worden gemaakt van de risico’s en mogelijke gevolgen. De vraag is wat er nodig is om ondernemers tot actie aan te zetten. De tools zijn er namelijk al, maar worden nog niet altijd ingezet door ondernemers. Er is al veel materiaal beschikbaar op het terrein van preventie en het voorkomen van slachtofferschap van cybercriminaliteit. Daar staat tegenover dat er nog minder beschikbaar is voor repressie en nazorg wat ondernemers handvatten geeft wat te doen als ze toch zijn gehackt of de fase na het slachtofferschap als de organisatie weer moet worden opgestart. Een ondernemer kan zich met de basismaatregelen niet volledig beschermen tegen met name een gerichte cyberaanval. Wat moet een ondernemer doen als deze ondanks alle inspanningen op het terrein van cyber security toch slachtoffer wordt.” (Respondent interview)

Verschillende bedrijven zouden meer inzicht willen verkrijgen in de kwetsbaarheden van hun organisatie (bijvoorbeeld via een scan) om de mate van cyberweerbaarheid van hun organisatie in te schatten. Ook zouden verschillende bedrijven graag best practices en lessons learned van andere ondernemers (bij voorkeur uit de logistieke sector) ontvangen om op basis daarvan (beleidsmatige,

technische en/of personele) maatregelen te nemen ten behoeve van de cyberweerbaarheid van hun organisatie. Tevens bestaat er behoefte bij bedrijven om (bij voorkeur gezamenlijk met andere ondernemers uit de logistieke sector) bijeenkomsten, workshops en trainingen op het terrein van cyber security bij te wonen om hun kennis te vergroten en te leren van anderen zodat hun organisatie hier zijn voordeel mee kan doen. Daarnaast is er behoefte aan een centraal meldpunt voor cyber security incidenten. Afhankelijk van de aard van de werkzaamheden van het bedrijf, de cyberaanval en de opgelopen schade kan/moet er een melding worden gedaan bij een of meerdere verschillende instanties. Het is voor bedrijf niet altijd duidelijk waar wanneer waarover wat gemeld moet worden naar aanleiding van een (dreigend) cyber security incident. Tot slot is er behoefte aan een helpdesk waar men als bedrijf terecht kan voor hulp bij een acute cyber security dreiging.

Integrale benadering van cyberweerbaarheid

Cyberweerbaarheid staat voor het vermogen van ondernemers om cyber security dreigingen te herkennen en hier adequaat op te anticiperen. De aanname is dat iedere ondernemer in de loop der tijd te maken krijgt met een cyber security incident. Dit betekent dat ondernemers zich niet alleen moeten richten op preventieve maatregelen om een cyber security incident te voorkomen, maar ook op detectie en respons. De veiligheidsketen is een methode voor een integrale benadering van cyber security risico's. De veiligheidsketen bestaat uit vijf fasen of schakels. Het betreft proactie, preventie, preparatie, repressie en nazorg. Proactie is het wegnemen van structurele oorzaken van onveiligheid. Te denken valt aan het bewaren van cruciale informatie op een server die niet verbonden is met het internet. Het voordeel van proactie is dat het risico (grotendeels) wordt weggenomen. Het nadeel is dat het de bedrijfsvoering bemoeilijkt en/of dat er hoge (extra) kosten aan verbonden (kunnen) zijn. Preventie is het nemen van maatregelen vooraf om de risico's zo klein mogelijk te houden en de mogelijke gevolgen te beperken indien deze zich toch voordoen. Te denken valt aan toegangsbeheer en netwerksegmentatie. Preparatie is de voorbereiding om (pogingen tot) beveiligingsinbreuken te kunnen bestrijden. Voorbeelden hiervan zijn het opstellen van plannen en procedures, het opleiden van personeel en het houden van oefeningen. Voorbereiding is nodig, omdat er altijd een kans is dat preventieve maatregelen niet of onvoldoende werken. Het is echter waarschijnlijker dat preventieve maatregelen niet correct worden getroffen (bijvoorbeeld door menselijke fouten). Repressie is de daadwerkelijke bestrijding van (pogingen tot) beveiligingsinbreuken. De belangrijkste voorwaarde voor succesvol repressief optreden is kennis en ervaring. Daar doet zich tegelijkertijd het grootste probleem voor. Cyberaanvallen doen zich in vele vormen voor. Tegelijkertijd is er niet altijd voldoende bekend over (nieuwe) vormen van cyberaanvallen waardoor beslissingen moeten worden genomen op basis van beperkte informatie. Nazorg is al hetgeen nodig is om zo snel mogelijk naar de 'normale' situatie terug te keren, zoals herstel van veroorzaakte schade. Een voorbeeld hiervan is een backup waardoor een organisatie na een cyberaanval haar primaire werkprocessen weer spoedig kan hervatten.
Uit het onderzoek blijkt er al veel tools beschikbaar zijn voor ondernemers op het terrein van preventie en het waar mogelijk voorkomen van slachtofferschap van cybercriminaliteit. Daar staat tegenover dat er minder tools voorhanden zijn voor ondernemers op het terrein van repressie en nazorg. Het gaat om handvatten voor ondernemers om te reageren op een (dreigende) cyber security aanval en om de bedrijfsvoering weer te hervatten zodra het cyber security incident achter de rug is. Een crisisplan kan een ondernemer hiervoor van dienst zijn. Ruim de helft van de bedrijven beschikt over een crisisplan dat in werking kan treden wanneer er zich een cyber security incident voordoet. Een derde van de bedrijven heeft (nog) geen crisisplan voor een cyberaanval. Het overgrote deel van deze bedrijven is wel voornemens om op termijn een crisisplan op te stellen waardoor zij in staat worden gesteld om adequaat te reageren op een (dreigend) cyber security incident. Dit voorbeeld laat zien dat hier richting ondernemers nog in een behoefte kan worden voorzien.



In het volgende hoofdstuk wordt ingegaan op lopende initiatieven om de cyberweerbaarheid van ondernemers in de logistieke sector te bevorderen en wordt er een overzicht gegeven van de (publieke en branche) organisaties en (lokale, regionale en nationale) samenwerkingsverbanden die zich hiervoor inzetten.

6. Initiatieven op cyberweerbaarheid

In dit hoofdstuk wordt ingegaan op het speelveld van (publieke en branche) organisaties, (lokale, regionale en nationale) samenwerkingsverbanden en initiatieven (in de logistieke sector) op het terrein van cyber security in de MRDH regio.

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) opereert als zelfstandige dienst van het ministerie van Justitie en Veiligheid en is het nationale expertisecentrum voor cybersecurity dat als doel heeft om de Nederlandse samenleving en in het bijzonder de vitale infrastructuur digitaal weerbaarder te maken. Het NCSC is het nationale knoop- en informatiepunt op het gebied van cybersecurity en deelt kwetsbaarheden, incidenten en dreigingen die op nationaal niveau spelen. Primair heeft het NCSC tot taak om aanbieders van vitale processen, producten en/of diensten en organisaties binnen de rijksoverheid te informeren en adviseren over (dreigende) cyber security incidenten en daarvoor analyses en technisch onderzoek te verrichten. Hierdoor beschikt het NCSC regelmatig ook over informatie over digitale dreigingen of incidenten die relevant is voor andere organisaties, waaronder bedrijven in de logistieke sector. Momenteel ontbreekt het (nog) aan de wettelijke basis om deze informatie te verstrekken aan organisaties die geen onderdeel uitmaken van de vitale infrastructuur (www.ncsc.nl).

Digital Trust Center

Het Digital Trust Center (DTC) heeft als doel om ongeveer 2 miljoen Nederlandse bedrijven cyberweerbaar te maken die niet tot de vitale sectoren behoren (en hierdoor niet tot de primaire doelgroep van het NCSC behoren). Het DTC probeert ondernemers op verschillende manier te bereiken. Zo biedt het DTC op haar website op een laagdrempelige manier kennis, informatie en advies aan ondernemers hoe zij hun cyberweerbaarheid kunnen bevorderen. Voorbeelden hiervan zijn de basisscan cyberweerbaarheid waarmee ondernemers de cyberweerbaarheid van hun eigen onderneming kunnen toetsen en de 5 basisprincipes van veilig digitaal ondernemen die bedrijven als leidraad kunnen gebruiken om de basale digitale cyber security maatregelen op orde te krijgen. Daarnaast heeft het DTC een online community in het leven geroepen waar ondernemers opgedane kennis en ervaring kunnen uitwisselen op het terrein van cyber security. Ook verspreidt het DTC via de online community actuele informatie over cyber security dreigingen vanuit het NCSC. Het DTC is niet in staat om alle ondernemers te bereiken. Om haar bereik te vergroten werkt het DTC samen met brancheorganisaties en (publieke en/of private) samenwerkingsverbanden die ondernemers bijstaan om hun cyberweerbaarheid te bevorderen. Deze samenwerkingsverbanden kunnen samenwerken in een keten, sector, branche en/of regio (lokaal, regionaal, nationaal). Er is (nog) geen cyberweerwaarheidsnetwerk specifiek voor de logistieke sector. Een dergelijk initiatief zou mogelijk door het DTC kunnen worden gefaciliteerd en/of gefinancierd (www.digitaltrustcenter.nl).

"Het DTC heeft veel kennis, ervaring en tools tot haar beschikking, maar niet alle ondernemers in ondermeer de logistieke sector zijn bekend met het DTC waardoor ze vooralsnog geen kennis kunnen nemen en gebruik kunnen maken van de tools van het DTC om hun cyberweerbaarheid te bevorderen." (Respondent interview)

Security Delta

Security Delta (HSD) is hét nationale veiligheidscluster waar ongeveer 275 bedrijven, overheidsorganisaties en kennisinstellingen samenwerken aan de cyberweerbaarheid van de digitaliserende samenleving. Dit doet de HSD door de kennis van haar partners te delen en samen te werken aan innovatieve veiligheidsoplossingen. De focus ligt hierbij op cybersecurity & -weerbaarheid, data & AI/intel en slimme veilige samenlevingen. De Security Delta biedt bedrijven toegang tot kennis over cyber security, toegang tot innovatie op het terrein van vooruitstrevende

(technologische) oplossingen voor complexe vraagstukken, toegang tot de markt door het matchen van probleemeigenaren met probleemoplossers, toegang tot kapitaal voor de financiering van oplossingen en toegang tot cyber security talent (www.securitydelta.nl).

Centrum voor Criminaliteitspreventie en Veiligheid

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een stichting die zich inzet om veiligheidsproblemen in kaart te brengen en op te lossen. Daarvoor biedt het CCV kennis, instrumenten, keurmerken, voorlichtingsmateriaal en advies op maat gericht op onder andere cyber security aan overheden en bedrijven met preventie als uitgangspunt. Het CCV biedt op haar website kennis, informatie en advies aan ondernemers hoe zij hun cyberweerbaarheid kunnen bevorderen. Daarnaast brengt het CCV frequent een (online) nieuwsbrief en vakblad uit over veiligheidsvraagstukken (ondermeer op het terrein van cyber security). Tevens brengt het CCV handreikingen uit over de oplossing van cyber security vraagstukken. Ook organiseert en verzorgt het CCV webinars, fysieke bijeenkomsten en trainingen op het terrein van cyber security. Tot slot geeft het CCV advies op maat ten aanzien van de bevordering van cyberweerbaarheid (www.hetccv.nl).

VNO NCW MKB Nederland

De werkgeversorganisaties VNO NCW en MKB Nederland hebben met het initiatief Samen Digitaal Veilig de handen in een geslagen om de cyberweerbaarheid van ondernemers te bevorderen. Samen Digitaal Veilig is een praktische tool om MKB bedrijven en medewerkers op te leiden in digitale veiligheid. Medewerkers worden getraind via korte opleidingsvideo's en vragen. Via een automatische uitvraag ziet de ondernemer of zijn IT-leverancier de zaken goed heeft geregeld. Na het invullen van een veiligheidsscan door de ondernemer komen alle resultaten en voortgang van de organisatie, leveranciers en medewerkers in één veiligheids-dashboard te staan. Het platform Samen Digitaal Veilig wordt uitgerold via een groot aantal branche- en ondernemersverenigingen (www.samendigitaalveilig.nl).

Transport en Logistiek Nederland

Transport en Logistiek Nederland (TLN) is een brancheorganisatie voor ondernemers in de logistieke sector. Ondernemers kunnen bij TLN kennis en expertise inwinnen over uiteenlopende thema's op het terrein van logistiek. TLN heeft zelf niet (meer) de kennis en expertise in huis op het terrein van cyber security. Wanneer ondernemers met vragen over cyber security terecht komen bij TLN dan worden zij veelal doorverwezen naar het DTC. Ook wordt door TLN doorverwezen naar Samen Digitaal Veilig van VNO NCW MKB Nederland aangezien ongeveer 75% van de leden van TLN een MKB onderneming betreft (www.tln.nl).

Evofenedex

Evofenedex is een ondernemersvereniging en netwerk van Nederlandse handels- en productiebedrijven met een logistieke of internationale operatie. Evofenedex heeft ongeveer 12.000 leden die continue te maken hebben met veranderingen in hun (logistieke) ketens. Ook is er sprake van toenemende concurrentie waardoor verdienmodellen onder druk (kunnen) komen te staan. Een van de speerpunten van Evofenedex is de digitalisering van de bedrijfsprocessen van ondernemers in hun sector. Digitalisering levert naast economische kansen

(zoals kostenbesparing door efficiëntie en nieuwe producten en diensten door innovatie) ook cyber security risico's op. Tot dus ver is er vooral aandacht voor de kansen en minder voor de risico's van digitalisering. Zodoende is Evofenedex (mede naar aanleiding van het programma cyberweerbaarheid van de Security Delta) voornemens om ook meer aandacht te besteden aan de cyber security risico's die gepaard gaan met digitalisering. Evofenedex zou (indien mogelijk in samenwerking met de Security Delta) graag een bijeenkomst voor haar leden willen organiseren over cyber security (www.evofenedex.nl).

IRO

IRO is de brancheverenigingvoor Nederlandse toeleveranciers in de offshore energie industrie. IRO heeft ongeveer 400 leden. In eerste instantie waren die met name actief in olie en gas, maar nu ook in waterstof en windmolens. De activiteiten van IRO omvatten het verlenen van ondersteuning op het gebied van vertegenwoordiging aan overheden en potentiële opdrachtgevers, het bevorderen van export, het ontwikkelen van nieuwe technologieën en het bieden van informatievoorzieningen. Cyberweerbaarheid wordt af en toe belicht door IRO richting haar leden. Zo heeft IRO in het verleden met het Innovation Quarter een workshop gehad bij de Security Delta (Campus). Gezien de mate van cyberweerbaarheid van (een aanzienlijk deel van) de leden van IRO is het van belang om hier in de toekomst frequent aandacht aan te (blijven) besteden. IRO gaat hiervoor in principe graag de samenwerking aan met anderen organisaties, netwerken en samenwerkingsverbanden (www.iro.nl).

Platform Veilig Ondernemen Rotterdam

Het Platform Veilig Ondernemen (PVO) Rotterdam zet zich in regio van de politie eenheid Rotterdam ondermeer in voor de bevordering van de cyberweerbaarheid van ondernemers. Deelnemers van het PVO Rotterdam zijn: MKB Nederland, VNO NCW, ondernemersverenigingen, gemeenten, politie en Openbaar Ministerie. Het PVO faciliteert 25 gemeenten en hun (veiligheids)partners die op hun beurt met (lokale) ondernemersverenigingen samenwerken om ondernemers te bereiken. Door het organiseren van ondermeer (online en fysieke) bijeenkomsten wordt getracht om ondernemers te informeren over cyber security risico's en vervolgens te activeren om hun cyberweerbaarheid te bevorderen. De focus van het PVO Rotterdam ligt hierbij met name op MKB bedrijven omdat deze hiertoe over het algemeen minder goed zelfstandig in staat zijn dan grotere bedrijven en zodoende doorgaans meer ondersteuning nodig hebben om hun cyberweerbaarheid te bevorderen. Het PVO Rotterdam faciliteert waar mogelijk en gewenst publiek-private samenwerkingsverbanden op het terrein van cyber security in de regio Rotterdam. Een voorbeeld hiervan is het Cybernetwerk Zuid Hollandse Eilanden (ZHE).

VeiligheidsAlliantie regio Rotterdam

De VeiligheidsAlliantie regio Rotterdam (VAR) is een samenwerkingsverband van 25 gemeenten, de politie en het Openbaar Ministerie binnen de regio van de politie eenheid Rotterdam. De VAR functioneert binnen de regio als platform om kennis en ervaring te delen rond veiligheidsvraagstukken (waaronder cyberweerbaarheid). Daarnaast ondersteunt de VAR regionale samenwerking tussen partners door actief te signaleren, agenderen, initiëren en verbinden. De VAR zet zich ondermeer in voor de aanpak van cybercriminaliteit in haar regio. De VAR heeft zich bij de Vereniging van Nederlandse Gemeenten (VNG) sterk gemaakt om de voorkoming en aanpak van cybercriminaliteit een plek te geven in het kernbeleid veiligheid die als handreiking dient voor

gemeenten bij de ontwikkeling van hun integraal veiligheidsbeleid. Zodoende is het focusblad digitale veiligheid ontwikkeld dat onderdeel uitmaakt van kernbeleid veiligheid. Het focusblad biedt gemeenten handvatten bij het opnemen en uitwerken van het thema digitale veiligheid in het lokale integraal veiligheidsplan (IVP). Het focusblad beschrijft de te onderscheiden veiligheidsrisico's, de rol van de gemeente rond deze risico's en het aanbevolen pad voor de uitwerking van dit thema in het integraal veiligheidsplan. Daarnaast biedt de VAR gemeenten ondersteuning bij het initiëren van activiteiten om de cyberweerbaarheid van ondermeer ondernemers te bevorderen. Op deze manier kunnen gemeenten ook daadwerkelijk invulling geven aan digitale veiligheid uit hun integraal veiligheidsplan (www.veiligheidsalliantie.nl).

Cybernetwerk Zuid Hollandse Eilanden

Het Cybernetwerk Zuid Hollandse Eilanden (ZHE) is opgericht om MKB bedrijven te helpen maatregelen te nemen tegen cybercriminaliteit om mogelijk slachtofferschap te voorkomen. Het Cybernetwerk ZHE is een publiek-privaat samenwerkingsverband wat actief is op de Zuid-Hollandse Eilanden: Hoeksche Waard, Voorne Putten en Goeree-Overflakkee. Partners zijn onder andere gemeenten, Rabobank, VeiligheidsAlliantie regio Rotterdam, MKB Rotterdam en Platform Veilig Ondernemen (PVO) Rotterdam. Het cybernetwerk ZHE organiseert (fysieke) kennisbijeenkomsten, online seminars en online trainingen voor haar doelgroep. Daarnaast brengt zij een nieuwsbrief uit en stelt zij tools beschikbaar. Ook worden nulmetingen verricht op het terrein van cyberweerbaarheid en worden nepadvertenties op sociale media geplaatst om de bewustwording ten aanzien van cyber security risico's te bevorderen. Het betreft een veelzijdig aanbod waar ondernemers (kosteloos) gebruik van (kunnen) maken. Voor een deel gaat het om het opnieuw delen van reeds bestaande handvatten, zoals tools die door een andere organisatie zoals het DTC zijn ontwikkeld en beschikbaar zijn gesteld. Het DTC kan haar tools via het Cybernetwerk ZHE bij de doelgroep terecht laten komen zodat ze hier kennis van kunnen nemen en hier desgewenst ook gebruik van gaan maken (www.cybernetwerkzhe.nl).

Platform Veilig Ondernemen Den Haag

Het Platform Veilig Ondernemen (PVO) Den Haag zet zich in de regio van de politie eenheid Den Haag ondermeer in voor de bevordering van de cyberweerbaarheid van ondernemers. Het PVO Den Haag faciliteert 28 gemeenten en hun (veiligheids)partners. PVO Den Haag valt in deze regio samen met het Regionaal Samenwerkingsverband Integrale Veiligheid (RSIV). Het PVO Den Haag heeft zich de afgelopen jaren ingezet voor het weerbaarder maken van ondernemers tegen cybercriminaliteit, bijvoorbeeld met trainingen. Ook is er door het PVO Den Haag geïnvesteerd in het opzetten van publiek private samenwerkingsverbanden, bijvoorbeeld rond bedrijventerreinen en winkelcentra.

Het PVO Den Haag start met het project evidence based cybersecurity gedragsinterventie. Hiervoor is door het ministerie van Justitie en Veiligheid in het kader van de CityDeal Lokale Weerbaarheid 50.000 euro toegekend. Een groot deel van bestaande initiatieven en projecten die zich richten op het bevorderen van de cyberweerbaarheid van ondernemers zijn niet evidence based. Het gevolg is dat niet altijd duidelijk is wat wel/niet werkt onder welke omstandigheden. Zodoende is het PVO Den Haag met het Centre of Expertise Cybersecurity (CoECS) het project evidence based cybersecurity gedragsinterventie gestart.

Nederland beschikt over tien PVO's. Iedere politie eenheid beschikt over een PVO. Door het kabinet is ongeveer 10 miljoen euro beschikbaar gesteld om de PVO's te versterken. Een deel van het budget komt terecht bij het CCV dat een landelijk netwerk inricht waar de PVO's informatie met elkaar kunnen uitwisselen, zodat niet in ieder PVO het wiel opnieuw hoeft te worden uitgevonden. Het overige overgrote deel van het budget komt bij de tien PVO's terecht, waaronder het PVO Den Haag. Het PVO Den Haag is voornemens om een deel van dit budget aan te wenden voor de bevordering van cyberweerbaarheid van ondernemers. De PVO Den Haag gaat graag gezamenlijk met de Security Delta verkennen welke toekomstige samenwerkingsmogelijkheden er liggen bij de bevordering van cyberweerbaarheid van ondernemers. De gedachte hierachter is dat het PVO Den Haag en de Security Delta samen meer impact kunnen maken door activiteiten op elkaar af te stemmen en op elkaar te laten aansluiten. Er zou door de Security Delta en het PVO Den Haag bijvoorbeeld kunnen worden samengewerkt aan een of meerdere (op te richten) sectorale cyberweerbaarheidscentra (waaronder voor de logistieke sector) waarbij de tools en trainingen van het PVO Den Haag worden ondergebracht en aangeboden bij de doelgroep.

Regionaal Samenwerkingsverband Integrale Veiligheid

Het Regionaal Samenwerkingsverband Integrale Veiligheid (RSIV) bestaat uit 27 gemeenten, de politie en het Openbaar Ministerie. Het RSIV zet zich in op gezamenlijke prioriteiten op regionaal niveau (waaronder de aanpak van cybercriminaliteit). Het betreft veiligheidsvraagstukken die in het merendeel van de gemeenten spelen, waarop een gezamenlijke integrale aanpak gewenst is en waarover bestuurlijk draagvlak is om hierover op regionaal niveau afspraken te maken. De prioriteiten voor de komende vier jaar staan in het Regionaal Beleidsplan (RBP) 2019-2022. Inmiddels zijn ook de eerste voorbereidingen gestart voor het Regionaal Beleidsplan 2023-2026. De nieuwe regionale prioriteiten zullen voor een belangrijk deel worden bepaald door het Algemeen Veiligheidsbeeld van de eenheid Den Haag 2021. De belangrijkste doelstelling van het RSIV is het praktisch ondersteunen van de netwerkpartners bij het uitvoeren van het Regionaal Beleidsplan, bijvoorbeeld door het organiseren van regionale kennis- en netwerkbijeenkomsten en het ontwikkelen van concrete beleidsinstrumenten (www.rsiv.nl).

Cyber Netwerk Drechtsteden

Het Cyber Netwerk Drechtsteden (CND) is een samenwerkingsverband dat cyberweerbaarheid onder de aandacht brengt bij MKB bedrijven in de regio Drechtsteden. Partners van het CND zijn HBO Drechtsteden, IMC, VitrumNet, Hoek en Blok IT. Het doel van CND is om bedrijven in de regio bewust te maken van de risico's die digitalisering en cyberbedreigingen voor de bedrijfsvoering kunnen vormen. Door het beschikbaar stellen van middelen en tools geeft het CND bedrijven in de Drechtsteden handvatten om de cyberweerbaarheid te bevorderen. Zo biedt het CND een toolkit en pentesten aan richting bedrijven (www.cybernetwerk.nl).

Centre of Expertise Cybersecurity

Het Centre of Expertise Cybersecurity (CoECS) van de Haagse Hogeschool zet zich in voor het versterken van de cyberweerbaarheid van publieke en private organisaties die zelf in mindere mate zijn toegerust op cyber security dreigingen. Het CoECs verricht onderzoek op drie deelgebieden: mens, organisatie en techniek. In het onderzoek wordt ingegaan op welke menselijke, organisatorische en technische aspecten de cyberweerbaarheid van ondermeer ondernemers beïnvloeden en hoe deze desgewenst kunnen worden verbeterd.

7. Conclusies en aanbevelingen

Dit hoofdstuk vormt het sluitstuk van de rapportage over cyberweerbaarheid in de logistieke sector. Er wordt antwoord gegeven op de vraagstelling die centraal staat in het onderzoek in het kader van de rapportage. Daarnaast worden aanbevelingen gegeven voor (de versterking van initiatieven ten behoeve van) de bevordering van cyberweerbaarheid van ondernemers in de logistieke sector.

Cyberweerbaarheid van ondernemers in de logistieke sector

Bedrijven in de logistieke sector lopen een niet gering risico om slachtoffer te worden van cybercriminaliteit door de aard van hun bedrijfsactiviteiten, de producten en diensten die ze vervoeren voor derden en/of de mogelijke buit die er bij hun te halen is. De meest voorkomende verschijningsvormen van cybercriminaliteit zijn malware, ransomware, DDoS aanvallen, onderschepte betalingen, factuurfraude en CEO fraude. Uit het onderzoek komt naar voren dat de mate van cyberweerbaarheid van ondernemers in de logistieke sector sterk verschilt. Een belangrijke oorzaak hiervan is dat een deel van de ondernemers zich onvoldoende bewust is van de kans op slachtofferschap van cybercriminaliteit en de mogelijke impact daarvan op hun bedrijfsvoering. Een andere oorzaak is dat het bij een deel van de ondernemers ontbreekt aan kennis, capaciteit en/of middelen om hun cyberweerbaarheid daadwerkelijk te bevorderen. Hierdoor worden er (met name door de kleinere bedrijven) niet altijd de benodigde (beleidsmatige, technische en/of personele) maatregelen genomen om de cyberweerbaarheid te bevorderen. Tot slot worden door medewerkers al dan niet bewust (bijvoorbeeld uit efficiëntie overwegingen) basisregels van het cyber security beleid genegeerd wat de kans op insider threats verhoogd. Dat hangt nauw samen met een gebrek aan medewerkers binnen de sector die op het gebied van cybersecurity tijdig dreigingen kunnen signaleren en verhelpen. Als er bestuurlijk of operationeel aandacht is voor cybersecurity dan is dat vaak nog niet verankerd in de bedrijfsvoering, functies en ontwikkeling. Er zijn twee Security Delta hulpmiddelen die gericht zijn op het vervullen van de behoefte aan relevant opgeleide cybersecurity werknemers, namelijk cybersecuritywerkt.nl (zij-instroom/omscholing/startersfuncties) en securitytalent.nl (vacatures/opleidingen/beroepsprofielen/arbeidsmarkt).

Bestaande medewerkers binnen de sector met een interesse in cybersecurity zijn de meest toegankelijke resources. Deze medewerkers hebben al de nodige kennis van en ervaring in de sector, maar als hen een kans wordt aangeboden, zijn ze waarschijnlijk bereid om zich om- of bij te scholen op het gebied van cybersecurity binnen de betreffende sector. Om deze doelgroep meer beeld te geven bij de arbeidsmogelijkheden, kan gebruik gemaakt worden van het platform www.cybersecuritywerkt.nl: gericht op het laten doorstromen naar startersfuncties en passende bij-of omscholingstrajecten.

Als er onvoldoende medewerkers zijn met een interesse voor om- of bijscholing, moet er extern geworven worden en daar dient het platform www.securitytalent.nl voor. Dit is meer gericht op specialisten en het behouden en doorontwikkelen binnen security. Een platform waar vacatures, opleidingen en werkgevers staan op het gebied van (digitale) veiligheid.

Ketenafhankelijkheid ten aanzien van cyberweerbaarheid

Het merendeel van bedrijven actief in de logistieke sector werkt samen met tientallen andere bedrijven. Veelal wordt er in ieder onderdeel van het gehele operationele proces samengewerkt en informatie gedeeld met een of meerdere ketenpartners. Bedrijven in de logistieke sector zijn zich bewust van de ketenafhankelijkheid. Zij onderkennen dat de cyberweerbaarheid niet alleen afhankelijk is van de inspanningen van hun eigen organisatie, maar ook (in toenemende mate) van die van hun samenwerkingspartners in de keten. Desondanks wordt er tussen bedrijven in de

logistieke sector nog niet of nauwelijks samengewerkt en informatie gedeeld op het terrein van cyber security. Dit is een gemiste kans omdat door informatie over kwetsbaarheden, dreigingen, (bijna) incidenten, best practices en lessons learned te delen de cyberweerbaarheid van afzonderlijke bedrijven en daarmee van de gehele logistieke keten kan worden bevorderd. De totstandkoming van een cyberweerbaarheidscentrum specifiek voor de logistieke sector zou een impuls kunnen geven aan de onderlinge samenwerking en informatiedeling en daarmee aan de bevordering van cyberweerbaarheid van ondernemers en de gehele keten.

Initiatieven om de cyberweerbaarheid te bevorderen

In de MRDH regio zijn verschillende samenwerkingsverbanden actief die zich inzetten voor de bevordering van cyberweerbaarheid van ondernemers. Zij hebben gemeen dat ze zich richten op ondernemers ongeacht de sector waarin deze actief zijn. Het voordeel van de brede benadering die wordt gehanteerd is dat er veel ondernemers uit allerlei sectoren worden bereikt en dat er kruisbestuiving plaatsvindt tussen sectoren. Daar staat tegenover dat er hierdoor geen recht wordt gedaan aan de verschillen tussen sectoren ten aanzien van cyber security. De (digitale) processen, toegepaste technologieën, (potentiële) kwetsbaarheden en daaruit voortkomende cyber security risico's in de logistiek verschillen met die in andere sectoren. Dit betekent dat een sectorale aanpak van toegevoegde waarde kan zijn om de cyberweerbaarheid van ondernemers in de logistiek (verder) te bevorderen. Op dit moment wordt hier in de MRDH regio (of op een andere schaal) voor de logistieke sector nog niet in voorzien.

Ondernemers activeren om de cyberweerbaarheid te bevorderen

Er doen zich twee barrières voor die ervoor zorgen dat het verhogen van de cyberweerbaarheid van ondernemers (nog) niet optimaal verloopt. De eerste barrière vormt het überhaupt bereiken van de ondernemers. De tweede barrière vormt het gedrag van ondernemers. Ondernemers laten zich niet zomaar aanzetten om te investeren in cyber security maatregelen. Dit komt mede doordat ondernemers het risico op slachtofferschap van cybercriminaliteit en de mogelijke gevolgen daarvan onderschatten en/of omdat ze onvoldoende kennis hebben om hun cyberweerbaarheid daadwerkelijk te bevorderen.

Dit betekent dat ondernemers enerzijds behoefte hebben aan de inzichten van andere ondernemers (bij voorkeur uit de logistieke sector) over cyber security dreigingen zodat zij deze op waarde kunnen schatten voor hun eigen bedrijf. Anderzijds hebben ondernemers behoefte aan concrete handvatten om gerichte (beleidsmatige, technische, personele) maatregelen te nemen om cyber security risico's (waar mogelijk) te voorkomen en (waar nodig) te reduceren om de continuïteit van hun bedrijfsvoering te waarborgen. Voor het reduceren van de bovengenoemde barrières ligt een sectorale aanpak ten behoeve van de cyberweerbaarheid van ondernemers in de logistiek voor de hand.

"Ondernemers zijn moeilijk te activeren. Het zou goed zijn als ondernemers in ieder geval de basisregels op het terrein van cyber security hanteren. Als er een keer iets misgaat staat soms zelfs het voorbestaan van de onderneming op het spel. Bijvoorbeeld een ransomware aanval kan de continuïteit van een onderneming ernstig in gevaar brengen. Daarom is het belangrijk om veel aandacht te geven aan cyberweerbaarheid van ondernemers. Ondernemers luisteren doorgaans alleen naar andere ondernemers, niet of nauwelijks naar de overheid en iets meer naar een brancheorganisatie. Daarom is het belangrijk om de taal van de sector te spreken en sectorale samenwerkingen aan te gaan." (Respondent interview)

Cyberweerbaarheidscentrum

Er is bij verschillende stakeholders geïnventariseerd of er behoefte en bereidheid is om te participeren in een mogelijk op te richten cyberweerbaarheidscentrum voor de logistieke sector. Hier werd door het overgrote deel van de relevante respondenten positief op gereageerd. Het merendeel onderkent het belang van een sectorale aanpak voor de cyberweerbaarheid van ondernemers in de logistiek en is ook bereid om met zijn of haar organisatie een bijdrage te leveren om een mogelijk op te richten cyberweerbaarheidscentrum (mede)mogelijk te maken. Daarnaast is er ook geïnventariseerd onder de stakeholders wat de mogelijke toekomstige activiteiten van een dergelijk cyberweerbaarheidscentrum zouden kunnen/moeten zijn. Er worden mogelijkheden gezien voor een gecombineerde response en recovery unit, het (waar mogelijk en gewenst) gezamenlijk opleiden van cyber security professionals, het onderling kennis en ervaringen uitwisselen op gezamenlijke bijeenkomsten, een gecombineerd SOC, basisniveau van cyberweerbaarheid door middel van certificering naar aanleiding van criteria op het terrein van cyber security en controle van belangrijkste gedeelde ICT leveranciers. Belangrijk uitgangspunt is dat door gezamenlijk producten en diensten extern in te kopen op het terrein van cyber security hoogwaardige(re) kwaliteit kan worden verkregen en/of kostenbesparingen kunnen worden gerealiseerd.

Uit de interviews met respondenten kwam naar voren dat verschillende bedrijven meer inzicht zouden willen verkrijgen in de kwetsbaarheden van hun organisatie (bijvoorbeeld via een scan) om de mate van cyberweerbaarheid van hun organisatie in te schatten. Ook zouden verschillende bedrijven graag best practices en lessons learned van andere ondernemers (bij voorkeur uit de logistieke sector) ontvangen om op basis daarvan (beleidsmatige, technische en/of personele) maatregelen te nemen ten behoeve van de cyberweerbaarheid van hun organisatie. Tevens bestaat er behoefte bij bedrijven om (bij voorkeur gezamenlijk met andere ondernemers uit de logistieke sector) bijeenkomsten, workshops en trainingen op het terrein van cyber security bij te wonen om hun kennis te vergroten en te leren van anderen zodat hun organisatie hier zijn voordeel mee kan doen. Daarnaast is er behoefte aan een centraal meldpunt voor cyber security incidenten. Tot slot is er behoefte aan een helpdesk waar men als bedrijf terecht kan voor hulp bij een acute cyber security dreiging. Bovenstaande behoeften bij ondernemers in de logistieke sector kunnen mogelijk ook door een mogelijk op te richten cyberweerbaarheidscentrum worden gefaciliteerd.

Tot slot wordt door de respondenten als belangrijke randvoorwaarde genoemd voor een mogelijk op te richten cyberweerbaarheidscentrum dat hierbij (waar mogelijk en gewenst) de verbinding wordt gemaakt met reeds bestaande samenwerkingsverbanden en lopende initiatieven. Door deze te verbinden en te versterken wint het cyberweerbaarheidscentrum aan draagvlak. Bovendien kan er door kennis, capaciteit en middelen te combineren gezamenlijk meer worden bereikt ten aanzien van de bevordering van cyberweerbaarheid van ondernemers in de logistieke sector.

Aanbevelingen ten aanzien van cyberweerbaarheid

Afsluitend worden onderstaand de belangrijkste aanbevelingen ten aanzien van de bevordering van cyberweerbaarheid in de logistieke sector op een rij gezet.

Ondernemers moeten niet alleen geinformeerd maar met name geactiveerd worden om hun cyberweerbaarheid te bevorderen. Het meest effectief en efficient is om ondernemers in sectoraal verband elkaar te laten informeren en aan te laten zetten tot het nemen van cyber security maatregelen.

Medewerkers kunnen de sterkste maar ook de zwakste schakel vormen wat betreft de cyberweerbaarheid van een onderneming. Investeer zodoende in de cyberweerbaarheid van medewerkers en daarmee ook van de organisatie.

Er is sprake van een grote mate van ketenafhankelijkheid in de logistieke sector ten aanzien van cyberweerbaarheid. Daarom dient te worden ingezet op het onderling delen van informatie over kwetsbaarheden, dreigingen, (bijna) incidenten, best practices en lessons learned waarmee de

cyberweerbaarheid van afzonderlijke bedrijven en daarmee van de gehele keten kan worden bevorderd.

Een sectorale aanpak lijkt het meest effectief en efficient daar waar het gaat om de bevordering van de cyberweerbaarheid van ondernemers in de logistieke sector. Een mogelijk op te richten cyberweerbaarheidscentrum specifiek voor de sector logistiek kan hierin voorzien. Zodoende dient met stakeholders te worden verkend wat het doel, de werkwijze, de doelgroep, het werkgebied, de activiteiten, de partners en de wijze van financiering van een dergelijk samenwerkingsverband zou kunnen zijn. Hierbij kan worden voortgeborduurd op reeds bestaande initiatieven (in de regio).

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

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