Digitale weerbaarheid in het midden –en kleinbedrijf

Het is moeilijk, kost tijd, geld en capaciteit maar het is wel nodig

Naam: Adam van den Ende
Studentnr.: s2075628
Eerste lezer: Dr. Jelle Brands /
Tweede lezer: Dr. Elina van ’t Zand-Kurtovic
Datum: 29-07-18

Scriptie geschreven in het kader van de Master Criminologie & Veiligheidsbeleid aan de Faculteit der Rechtsgeleerdheid, Universiteit Leiden

Inhoud

Samenvatting 3

1. Inleiding 4

1.1 Cybercrime, cybersecurity en digitale weerbaarheid 6

1.2 Doelen 8

1.3 Hoofdvraag, deelvragen en leeswijzer 10

2. Theoretisch kader 11

2.1 Conceptuele discussie over weerbaarheid 11

2.2 Interventies en het COM-B model 15

3. Methoden 19

3.1 Deelnemers 19

3.2 Instrumenten 19

3.3 Procedure 21

3.4 Analyse 23

4. Resultaten 25

4.1 Wat is digitale weerbaarheid? 25

4.1.1 Experts 25

4.1.2 Midden –en kleinbedrijf 27

4.1.3 Vergelijking 30

4.2 Interventies 31

4.2.1 Obstakels bij het toepassen van interventies 31

4.2.2 Maatwerk en behoeften 35

4.2.3 Voorlichting 39

5. Conclusie en discussie 43

5.1 Conclusie 43

5.2 Discussie 45

6. Literatuurlijst 48

6. Bijlagen 53

6.1 Topiclijst 53

6.2 Lijst van respondenten 56

Samenvatting

In deze scriptie is onderzoek gedaan naar digitale weerbaarheid binnen het midden –en kleinbedrijf (mkb). Eén van de doelen bestond uit het verzamelen van kennis over het begrip digitale weerbaarheid, de achterliggende concepten en om, waar mogelijk, de tot nu toe bestaande definities aan te vullen. Een tweede doel was gericht op het vinden van nieuwe interventies die gebruikt kunnen worden om digitale weerbaarheid binnen het mkb te versterken. Daarbij is gekeken naar obstakels die door de respondenten genoemd zijn die de effectiviteit van deze interventies mogelijk belemmeren. Om deze doelen te bereiken zijn 12 semigestructureerde kwalitatieve interviews afgenomen onder cybersecurity experts, mkb-ondernemers en respondenten uit mkb brancheverenigingen. Uit de resultaten is naar voren gekomen dat mkb'ers het begrip nauw beschrijven en digitale weerbaarheid vooral zien als het treffen van beschermende en preventieve maatregelen. Experts zien het begrip in breder perspectief en beschrijven concepten zoals herstel, veerkracht en het leren van incidenten. Daarnaast is gebleken dat 'offline' definities en concepten van weerbaarheid van toepassing zijn op de digitale variant. Uiteindelijk is een definitie van digitale weerbaarheid, op basis van de interviewresultaten, geformuleerd. Eén van de belangrijkste bevindingen is het feit dat experts afhankelijk zijn van mkb'ers en diens behoeften voor het ontwikkelen van interventies. Mkb'ers hebben echter geen expliciet behoeftebeeld waardoor er sprake is van een kennistekort bij experts. Experts weten (nog) niet welke interventies geschikt zijn. Een oorzaak hiervan kan zijn dat er te weinig bewustzijn onder mkb'ers is over het belang van digitale weerbaarheid. Capaciteitsgebrek en prioritering zijn andere oorzaken. Opgemerkt moet worden dat verschillende partijen toch bezig zijn met het in kaart brengen van de behoeften van mkb'ers via verschillende onderzoeken. Het is aan te bevelen deze resultaten samen te brengen zodat het mkb hier van kan profiteren. Uit de data zijn impliciet wel een aantal behoeften naar voren gekomen waar toekomstig beleid zich op zou kunnen richten. Mkb'ers hebben hulp nodig bij het kiezen van de juiste ICT leveranciers en producten. Ook hechten zij waarde aan sectorspecifieke informatie omdat niet iedere mkb-onderneming hetzelfde is. Via deze sectorspecifieke informatieverspreiding is het eveneens nuttig om incidenten uit te lichten. Duidelijk is geworden dat geïnformeerd worden over incidenten van collega mkb'ers een goede manier is om het belang van digitale weerbaarheid te benadrukken en ondernemers te motiveren om te investeren in digitale weerbaarheid. Publiek-private samenwerkingsverbanden kunnen op deze behoeften inspelen.

1. Inleiding

Cybercrime is een relatief nieuw fenomeen en komt steeds meer in het nieuws. Onlangs kopte het Algemeen Dagblad (AD) dat burgers 'nu hun wachtwoord moesten veranderen' (Boeschoten & Rosman, 2018). Reden voor deze oproep was het feit dat e-mailadressen en wachtwoorden van zo'n 3.3 miljoen Nederlanders op straat waren komen te liggen. Dat cybercrime een *hot item* is, is niet meer te ontkennen. Een Google nieuws zoekopdracht naar de term levert al snel 292.000 resultaten op. Overheidsinstanties en private partijen (zoals het AD) waarschuwen voor de gevaren van cybercrime en proberen burgers en bedrijven zo goed mogelijk te informeren over deze vorm van criminaliteit en manieren om de kans op slachtofferschap te verkleinen. Volgens het Centraal Bureau voor de Statistiek (CBS) is één op de negen Nederlanders in 2015 slachtoffer geweest van identiteitsfraude, hacken, koop- en verkoopfraude of cyberpesten. Ook merkt het CBS op dat bijna driekwart van de cybercrimedelicten niet gemeld wordt. Dit houdt in dat het aantal slachtoffers in Nederland hoger ligt dan nu geschat wordt (CBS, 2017a: 32-34).

Niet alleen burgers worden slachtoffer van cybercrime. Het bedrijfsleven krijgt er ook mee te maken en het probleem lijkt te groeien (Van Wees, 2015). Uit een rapportage van het CBS blijkt dat één op de vijf bedrijven met minstens tien werknemers in 2016, te maken heeft gehad met de gevolgen van cybercrime.Vooral de gezondheids- en welzijnszorg heeft er veel mee te maken terwijl horecagelegenheden relatief gezien weinig last hebben (CBS, 2017b). Volgens een onderzoeksrapport van Deloitte bedragen de kosten van cybersecurity gerelateerde incidenten in het Nederlandse bedrijfsleven zo'n tien miljard euro (Deloitte, 2016). Voor het midden en klein bedrijf (mkb) bedraagt dit één miljard euro (Deloitte, 2017). Het mkb in Nederland vormt het grootste deel van het aantal bedrijven in Nederland. 99.8% van de Nederlandse bedrijven bestaan uit mkb-ondernemingen en 64.4% van de werkende bevolking werkt bij mkb-ondernemingen. Dit houdt in dat bijna twee derde van alle werkgelegenheid ingevuld wordt door het mkb. Gemiddeld genomen werken er 3.3 personen bij een mkb-onderneming (European Comission, 2017). Een mkb wordt veelal gedefinieerd op basis van het aantal personeelsleden. De EU hanteert als indicator dat een bedrijf met minder dan 250 werknemers gezien wordt als mkb, een kleinbedrijf heeft minder dan 50 werknemers en een microbedrijf heeft minder dan tien werknemers (Harris & Patten, 2014; European Commission, 2017). In deze scriptie wordt de mkb definitie van de EU gehanteerd.

Concrete statistieken over slachtofferschap van cybercrime in het mkb zijn schaars. Wel zijn er een aantal studies gedaan om meer inzicht te krijgen in dit soort statistieken. Uit

onderzoek van Veenstra, Zuurveen, & Stol (2015) is naar voren gekomen dat in 2012, 28,5% van de 343 ondervraagde bedrijven slachtoffer is geworden van een of meer vormen van cybercrime. Daarnaast stellen de auteurs dat cybercrime onder bedrijven bijna even vaak voorkomt als traditionele criminaliteit onder bedrijven. Uit een ander onderzoek is gebleken dat van de 800 respondenten uit het mkb, 20% slachtoffer is geweest, 21% een poging heeft ondervonden maar geen slachtoffer is geworden en 8% niet weet of ze slachtoffer zijn geweest (Notté & Slot, 2016). Wel is het zo dat incidenten pas na een lange tijd ontdekt worden waardoor deze percentages hoger kunnen uitvallen. De voormalig minister van Economische Zaken, Henk Kamp, heeft in een kamerbrief (2017: 1) benadrukt dat het niet als vitaal aangemerkte deel van het bedrijfsleven […] steeds vaker digitaal [wordt] aangevallen' en dat deze groep zich 'vaak niet bewust is van dreigingen in het digitale domein en hoe zich daartegen te beschermen'. Het mkb valt hieronder en moet volgens Kamp ondersteund worden. Dit is dan ook een van de functies en doelstellingen van het inmiddels opgerichte Digital Trust Center (DTC). Het DTC adviseert ondernemers over cybersecurity (Ministerie van Economische Zaken en Klimaat, 2018).

De gevolgen van cybercriminaliteit voor mkb bedrijven zijn omvangrijk. Gedacht kan worden aan reputatieschade wanneer bekend is geworden dat een bedrijf slachtoffer is geweest. Het verliezen van klanten en het draaien van minder omzet zijn mogelijke gevolgen (Van der Meulen, 2015). Andere gevolgen kunnen bestaan uit productiviteitsverlies (Tawileh, 2007), verlies van bedrijfskennis zoals intellectuele eigendommen, hogere beveiligingskosten (Watkins, 2014), onderzoekskosten van bijvoorbeeld forensisch onderzoek en kosten van PR campagnes om reputatieschade te beperken (Romanosky, 2016). Ondanks deze gevolgen investeren bedrijven weinig in cybersecurity (Kshetri & Murugesan, 2013). Daarnaast vormt bij een klein deel van de bedrijven cybersecurity een integraal onderdeel van de bedrijfsvoering (Asllani, White, & Ettkin, 2013). Volgens het Cybersecuritybeeld Nederland investeren bedrijven niet omdat er sprake zou zijn van 'marktfalen' en economische prikkels om te investeren in cybersecurity ontbreken (NCTV, 2017a). Ook wordt cybersecurity beleid bij bedrijven gekenmerkt door 'underinvestment' of onderinvestering (Rowe & Gallagher, 2006; Gordon, Loeb, Lucyshyn, & Zhou, 2015). Bedrijven zijn niet bereid te investeren in cybersecurity omdat ze in kosten-batenanalyses bijvoorbeeld geen rekening houden met externe kosten zoals 'spillover'. Dit houdt in dat wanneer een bedrijf geïnfecteerd wordt met een virus, de kans bestaat dat dit virus overslaat naar andere bedrijven omdat beide bedrijven toegang hebben tot elkaars informatiesystemen (vgl. Taliweh e.a., 2008). Bij de kosten-baten analyse wordt met deze kostenpost geen rekening gehouden, terwijl de kosten voor beide

bedrijven hoog kunnen uitvallen. Het gevolg is dat er te weinig geïnvesteerd wordt in cybersecurity terwijl dit wel gewenst is (Gordon, e.a., 2005). Meestal wordt er pas na grote incidenten geïnvesteerd.

Redenen waarom mkb'ers veelal slachtoffer worden van cybercrime zijn als volgt te omschrijven. Ze hebben bijvoorbeeld het idee dat er minder strenge en strikte regels gelden in vergelijking met grotere bedrijven. Ook spelen de relatief hoge kosten van het beveiligen van digitale informatie een beperkende rol (Tawileh, Hilton, & McIntosh, 2007). Volgens Tawileh e.a. (2007) vormt het mkb ook een risico voor de informatiebeveiliging van grotere bedrijven omdat er sprake is van 'interdependence' of onderlinge afhankelijkheid. Grote bedrijven zijn wel eens afhankelijk van de diensten van kleinere bedrijven. De kleinere bedrijven moeten soms toegang hebben tot de informatiesystemen van de grotere bedrijven om te voldoen aan bedrijfscontracten. Doordat ze toegang krijgen, maken ze deel uit van het bedrijfsnetwerk van grotere bedrijven. Mkb-ondernemingen zijn vaak de zwakste schakel op dit netwerk en zijn daarom een aantrekkelijk doelwit om toegang te krijgen tot de netwerken van de grotere bedrijven die wel waardevolle informatie bezitten.

Al met al kan gesteld worden dat het mkb een aantrekkelijk doelwit kan zijn voor cybercriminelen, het probleem voor deze sector groeiende is en dat de gevolgen omvangrijk en negatief zijn. In deze scriptie staat het mkb als doelgroep centraal. Door bovengenoemde redenen is het van belang dat deze sector goed bestand is tegen cybercrime. Daarnaast ziet de de overheid ook in dat het probleem groeiende is en heeft daarom het DTC opgericht.

1.1 Cybercrime, cybersecurity en digitale weerbaarheid

Het is nuttig om cybercrime enigszins te definiëren omdat het een breed begrip is dat op verschillende manieren ingevuld kan worden. Leukfeldt en Yar (2016) definiëren het als misdrijven die afhankelijk zijn van het gebruik van nieuwe technologische communicatiemiddelen om gepleegd te kunnen worden. Verder wordt er in de literatuur een tweedeling gemaakt. Volgens Leukfeldt (2017: 19) ontstaan er enerzijds nieuwe vormen van criminaliteit die gericht zijn op ICT en gepleegd worden door gebruik te maken van ICT ('*cyber-dependent crimes*'). Anderzijds bestaan de meer traditionele vormen van criminaliteit die niet gericht zijn op ICT maar waar ICT een substantiële bijdrage levert bij het plegen van de misdaad ('*cyber-enabled crimes'*). Cybercrime is volgens Leukfeldt een paraplubegrip dat gebruikt wordt voor beide categorieën (2017: 19). Voorbeelden van *cyber-dependent crimes* zijn DDoS aanvallen en ransomware. Fraude en stalking met een ICT component zijn

voorbeelden van *cyber-enabled crimes*. Individuen, bedrijven en overheidsorganisaties kunnen allemaal in verschillende mate slachtoffer worden van deze (nieuwe) vormen van criminaliteit. De kans om slachtoffer te worden van een DDoS aanval is bijvoorbeeld groter voor een bedrijf dan voor een individueel persoon.

Zoals preventie bescherming kan bieden tegen bepaalde vormen van traditionele criminaliteit, zo moet cybersecurity bescherming bieden tegen cybercrime. Cybersecurity moet er voor zorgen dat de kans op digitaal slachtofferschap onder bedrijven, individuen en overheidsorganisaties afneemt. Het probleem bij dit begrip is dat er geen eenduidige definitie van de term bestaat omdat cybersecurity een maatschappelijke uitdaging vormt. Maatschappelijke uitdagingen zijn volgens Van der Meulen altijd onderwerp van discussie en de definitie van cybersecurity vormt hier geen uitzondering op. Verschillende partijen hebben namelijk verschillende opvattingen over het begrip. Omdat er geen eenduidige definitie bestaat wordt het ontwikkelen van beleid of het verzamelen van kennis bemoeilijkt (Van der Meulen, 2015). De verschillen in definities kunnen kort geïllustreerd worden door een aantal voorbeelden te benoemen. De NCTV definieert cybersecurity in de Nationale Cyber Security Strategie (2017b: 13) als volgt:

Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan. De schade kan bestaan uit: aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie.

De Cyber Security Raad (2017) deelt cybersecurity op in drie aspecten die een rol spelen: de beschikbaarheid van ICT systemen, het bewaken van de integriteit van informatie en het bewaren van de vertrouwelijkheid van toegang tot ICT systemen en gegevens. Volgens Von Solms & Van Niekerk (2013) wordt cybersecurity in de literatuur veelal gezien als een containerbegrip. Zo wordt het gedefinieerd als *'measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack'*. Lodder en Toet omschrijven cybersecurity als 'een streven naar, of een staat van, bescherming tegen onrechtmatig verwerken van elektronische gegevens of onrechtmatig gebruik van computersystemen (2013: 136). Wat al deze definities in ieder geval gemeen hebben is dat de digitale omgeving beveiligd moeten worden tegen (digitale) gevaren van buitenaf door verschillende middelen in te zetten. Deze middelen kunnen zowel technisch (firewalls) als organisatorisch (instructies naar personeel) van aard zijn (Kaur & Mustafa, 2013). De

definitie van de NCTV (2017b) is een stuk breder dan degene van Von Solms & Niekerk (2013) en van Loeder en Toet (2013) omdat de NCTV verschillende aspecten aanhaalt die niet alleen draaien om bescherming. Dit kan problematisch zijn bij het verzamelen van kennis en het ontwikkelen van beleid zoals Van der Meulen (2015) aankaart. Moet beleid dan alleen gericht zijn op bescherming of vallen andere aspecten zoals herstel hier ook onder?

In deze scriptie staat één onderdeel van cybersecurity centraal: digitale weerbaarheid. Digitale weerbaarheid of *digital resilience* kan ook gezien worden als de verzamelnaam voor allerlei verschillende middelen en manieren om cybercrime tegen te gaan en cybersecurity te verhogen (Rothrock, 2017). In het Cyber Security Beeld (2017: 31) wordt weerbaarheid gedefinieerd als 'de mate waarin maatregelen zijn getroffen om de kwetsbaarheid voor beveiligingsproblemen te verminderen'. Deze maatregelen kunnen gericht zijn op de mens, de techniek en de organisatie. Het fundamentele verschil met cybersecurity is dat digitale weerbaarheid er van uit gaat dat een bedrijf slachtoffer wordt en dat maatregelen niet alle dreigingen kunnen tegengaan (Rothrock, 2017; De Crespigny, 2012).

1.2 Doelen

Digitale weerbaarheid is een erg breed begrip. Het is daarom van belang om een strakke afbakening te maken en de onderwerpen te beschrijven die in deze scriptie aan bod komen. In de Nederlandse vakliteratuur is weinig bekend over digitale weerbaarheid als begrip of over achterliggende concepten. De term wordt wel genoemd in beleidsdocumentatie van de overheid (zoals in het voorgenoemde Cyber Security Beeld) en in de grijze literatuur (Kokkeler, 2017: 23; Akerboom, 2012; Zielstra & Krabbendam-Hersman, 2013; Ministerie van Economische Zaken en Klimaat, 2018). Opvallend is dat het begrip, een uitzondering daargelaten, niet wordt uitgelegd, uiteengezet en duidelijk wordt gedefinieerd. In de buitenlandse (grijze) literatuur lijkt dit vaker te gebeuren (Rothrock, 2017; De Crespigny, 2012; Accenture, 2018). Dit zal verder uiteengezet worden in de conceptuele discussie in het theoretisch kader. Het is opvallend dat overheidspartijen inzetten om de 'digitale weerbaarheid' van bedrijven te verhogen zonder dat hier, voor zover bekend, een duidelijke Nederlandse definitie van bestaat. Ook is er weinig bekend over de achterliggende concepten van digitale weerbaarheid. Daarnaast is niet bekend wat (mkb) bedrijven zelf denken wat digitale weerbaarheid is of in zou moeten houden. Ook dit kan waardevol zijn omdat (overheids)partijen dan beter in kunnen spelen op de behoeften of denkbeelden van ondernemers. In deze scriptie wordt daarom aandacht gegeven aan de definitie en

achterliggende concepten van digitale weerbaarheid en wat het volgens experts en mkb ondernemers is. Het doel is om meer kennis te verzamelen over de term, een poging doen om bestaande definities uit te breiden, erachter te komen hoe mkb ondernemers en experts er over denken en om te onderzoeken of 'offline' concepten en definities van weerbaarheid overgenomen kunnen worden door de 'online' variant. De verschillen tussen experts en mkb'ers kunnen waardevolle en nuttige inzichten opleveren. Op deze manier komt er inzicht in mogelijke kloven die bestaan tussen beide partijen. Mkb'ers hebben bijvoorbeeld bepaalde ideeën bij het begrip en stemmen activiteiten hier op af. Anderzijds kunnen experts andere ideeën hebben en van mening zijn dat mkb'ers meer zouden moeten doen op het gebied van digitale weerbaarheid. Wanneer deze (mogelijke) kloven in kaart gebracht zijn, dan kan hier op ingespeeld worden door middel van beleid.

Ook wordt er aandacht besteed aan (nieuwe) manieren om mkb'ers digitaal weerbaarder te maken. In de literatuur is geschreven over interventies om het cybersecurityniveau van ondernemingen en personen te vergroten (Abawajy, 2014; Shaw, Chen, Harris, & Huang, 2009; McCrohan, Engel, & Harvey, 2010; Khan, Algathbar & Khan, 2011) terwijl er weinig is geschreven over specifieke interventies gericht op het versterken van digitale weerbaarheid. Zoals naar voren is gekomen zit er een verschil tussen beide concepten. Deze scriptie is op dit gebied van waarde omdat met dit onderzoek inzichtelijk wordt welke manieren volgens mkb'ers en experts in theorie effectief kunnen zijn om de digitale weerbaarheid binnen het mkb te versterken. Ook hier kunnen kloven zitten tussen beide partijen. Experts kunnen bijvoorbeeld van mening zijn dat bepaalde interventies goed werken terwijl deze mening niet gedeeld wordt door mkb'ers. Een interventie die niet aansluit op de doelgroep zal waarschijnlijk weinig kans van slagen hebben. Opgemerkt moet worden dat het gaat om een inventarisatie van mogelijke manieren en interventies. De effectiviteit van deze interventies wordt niet onderzocht en vormt geen onderzoeksonderwerp van deze scriptie. Verder wordt er aandacht besteed aan de voorwaarden die gelden bij het ontwikkelen van interventies. Ook zal er gekeken worden naar obstakels die het implementeren en ontwikkelen van interventies mogelijk bemoeilijken.

Het digitaal weerbaar maken van mkb'ers vormt, zoals in de inleiding is besproken, één van de doelen van het DTC. Daarnaast zet een overheidspartij zoals de VeiligheidsAlliantie regio Rotterdam (VAR) zich ook in om het mkb weerbaarder te maken tegen digitale criminaliteit. De VAR is een regionaal samenwerkingsverband van 32 gemeenten, de politie en het OM. Het voornaamste doel van de VAR is het verzamelen en delen van kennis en ervaring over verschillende onderwerpen zoals geweld,

jeugdproblematiek en veilig wonen en cybercrime. Eén van de sporen waar de VAR zich op richt is het vergroten van het bewustzijn over cybercrime en het weerbaarder maken van het mkb tegen deze vorm van criminaliteit. Dit doen zij bijvoorbeeld door het organiseren van voorlichtingsavonden voor mkb'ers in de gemeenten van de regio Rotterdam. Deze en andere projecten vallen onder het overkoepelende project 'Digitaal Veilig'. Deze scriptie is geschreven tijdens mijn stageperiode bij de VAR en kan van waarde zijn door mogelijk (nieuwe) interventies te beschrijven die gebruikt kunnen worden om de digitale weerbaarheid van mkb'ers te vergroten.

Al met al kan er op basis van het bovenstaande geconcludeerd worden dat het van belang is dat het mkb in Nederland zich goed kan weren tegen cybercrime. Het probleem lijkt groter te worden en kan vele negatieve gevolgen met zich mee brengen. Het onderhavige onderzoek is tweedelig in de zin dat twee onderdelen van digitale weerbaarheid onderzocht worden. Inzicht in deze onderdelen zou moeten leiden tot een betere digitale weerbaarheid binnen het mkb.

1.3 Hoofdvraag, deelvragen en leeswijzer

Op basis van de bovenstaande doelen is de volgende hoofdvraag geformuleerd:

Welke aspecten spelen een rol bij digitale weerbaarheid binnen het mkb volgens cybersecurity experts en mkb-ondernemers?

De bijhorende deelvragen zijn als volgt:

1. Wat is digitale weerbaarheid volgens cybersecurity experts en mkb'ers?
2. Hoe kan digitale weerbaarheid binnen het mkb volgens cybersecurity experts en mkb'ers verhoogd worden?
3. In hoeverre bestaan er verschillen of overeenkomsten tussen cybersecurity experts en mkb'ers in de mogelijkheden die zij zien om digitale weerbaarheid binnen het mkb te verbeteren en wat zij verstaan onder het begrip?

De scriptie is als volgt opgebouwd. In hoofdstuk 2 worden verschillende theorieën uiteen gezet die centraal staan in deze scriptie. Daarna volgt een beschrijving van de gehanteerde methoden (hoofdstuk 3). Vervolgens worden de resultaten in hoofdstuk 4 besproken. Hoofdstuk 5 bevat de conclusie waarin de hoofdvraag wordt beantwoord.

2. Theoretisch kader

In dit hoofdstuk worden de verschillende theoretische benaderingen besproken die centraal staan in deze scriptie. Allereerst wordt het begrip 'weerbaarheid' conceptueel uiteengezet waarbij er ook kort aandacht besteed wordt aan digitale weerbaarheid zoals beschreven in de buitenlandse literatuur. Vervolgens volgt er een kort literatuur overzicht van bestaande interventies gericht op cybersecurity en een beschrijving van het COM-B model.

2.1 Conceptuele discussie over weerbaarheid

Zoals in de inleiding naar voren is gekomen is er in de Nederlandse literatuur vrij weinig consensus over de definitie van digitale weerbaarheid. In de buitenlandse literatuur is hier meer over geschreven. Digitale weerbaarheid is volgens Rothrock pessimistisch van aard omdat het er van uit gaat dat bedrijven slachtoffer worden van cybercrime, dat beveiligingsmaatregelen nooit alle dreigingen tegen kunnen gaan en dat het management van een bedrijf zich moet richten op het beperken van de impact van aanvallen. Wanneer dit laatste gebeurt dan is de kans groter dat het bedrijf blijft voortbestaan en zich kan herpakken. Daarnaast is het, als de digitale weerbaarheid van een bedrijf sterk is, mogelijk om tijdens aanvallen te blijven functioneren. De Crespigny (2012) stelt dat een bepaalde mate van onzekerheid onderdeel uitmaakt van digitale weerbaarheid. Voor bedrijven is het lastig om een risicoinventerasiatie te maken van cyber gerelateerde dreigingen. Deze kunnen erg snel ontstaan en ze worden steeds geavanceerder waardoor het moeilijk is om hier passende maatregelen voor te treffen. Ook De Crespigny gaat er van uit dat bedrijven ooit slachtoffer worden van cybercrime en dat het daarom van belang is om weerbaar te worden zodat het bedrijf kan voort blijven bestaan, vooral nadat het aangevallen is. Een goede balans moet gevonden worden tussen de kosten van maatregelen om de digitale weerbaarheid te verhogen en de kosten die een aanval met zich mee brengt. Naast de voorgaande korte discussie is het waardevol om naar het begrip 'weerbaarheid' of *resilience* in breder perspectief te kijken. In combinatie met de verzamelde data is het dan mogelijk om te zeggen of definities en concepten over dit 'offline' begrip door te trekken zijn naar de 'online' variant.

Volgens Cavelty, Kaufmann & Kristensen (2015) is weerbaarheid als concept steeds populairder geworden in de wetenschappelijke gemeenschap. Weerbaarheid is gericht op het beschrijven van de mechanismen die nodig zijn om stabiliteit, overleving en veiligheid te behouden. Deze mechanismen zijn op individuele, gemeenschapelijke, natuurlijke en technische systemen toe te passen. Weerbaarheid is dus een erg breed begrip en hoeft niet

beperkt te worden tot beveiliging of veiligheid alleen. Op het gebied van veiligheid biedt weerbaarheid wel de oplossing voor het probleem dat niet alle dreigingen op tijd gedetecteerd, voorspeld of weggenomen kunnen worden. Weerbaarheid accepteert namelijk het idee van een onstabiele en onvoorspelbare omgeving waarin incidenten gebeuren. Het zo goed mogelijk herstellen na een negatieve gebeurtenis zoals een aanval staat centraal. Daarnaast stellen de auteurs dat weerbaarheid zowel kijkt naar de toekomst als naar het verleden. Op het gebied van de toekomst wordt uitgegaan van onzekerheid en traumatische gebeurtenissen. Hier moet men zich op voor kunnen bereiden. Dit is mogelijk door naar het verleden te kijken en te leren van eerdere gebeurtenissen en incidenten. Verder zorgt weerbaarheid voor een verschuiving van verantwoordelijkheden. Niet alleen de overheid is verantwoordelijk voor weerbaarheid, ook burgers worden verantwoordelijk gehouden. Degene die weerbaar gemaakt moet worden, bijvoorbeeld burgers, zijn dus niet passief en hoeven niet volledig beschermd te worden. Ze worden gezien als actieve subjecten die een bijdrage kunnen leveren aan veiligheid. Toegespitst op dit onderzoek is het subject van weerbaarheid de mkb'er. Deze moet ook zelf een bijdrage leveren aan de eigen weerbaarheid en mag niet alleen vertrouwen op de overheid. De meest beperkte definitie die Cavelty, Kaufmann & Kristensen (2015) aanhalen is dat weerbaarheid gezien kan worden als een reactie op iets dat gebeurd is in het verleden. Aanpassingsprocessen en reorganisatie worden ingezet om een gevoel van veiligheid te creëren. Afsluitend stellen de auteurs dat weerbaarheid uit gaat van een verstorend verleden, een mogelijk verstorende toekomst en voortdurende verstoringen in het heden en de reacties op deze verstoringen (Cavelty, Kaufmann & Kristensen, 2015: 9).

Bourbeau stelt eveneens dat *resilience* veel aandacht heeft gekregen van psychologen, criminologen en maatschappelijk werkers. Een overeenkomend kenmerk van weerbaarheid in deze disciplinces is het idee van '*bouncing back'* (2013: 6). Weerbaarheid gaat dan om het vermogen dat iemand of een bedrijf heeft om te herstellen en zich makkelijk aan te passen aan pech, tegenslagen, conflicten, mislukking of verandering. Verder beschrijft Bourbeau (2013: 9) verschillende defnities van weerbaarheid die veelvuldig in de literatuur gebruikt worden. '*Engineering resilience*' kijkt naar de mate waarin een systeem veranderd, verplaatst of verschoven kan worden van een vast evenwichtspunt en nog steeds terug kan keren naar dit evenwichtspunt nadat een verstoring heeft plaats gevonden. Een bepaald incident zorgt dus voor een verstoring in het evenwicht. Weerbaarheid is dan de mogelijkheid van een bedrijf om terug te keren naar dit evenwichtspunt en weer stabiel te worden. '*Ecological resilience*' wordt gedefinieerd als de capaciteit van een systeem om een verstoring te ondervinden maar lopende functies toch te behouden. Het systeem ervaart dus een verstoring maar kan alsnog

voort blijven bestaan en ligt niet volledig stil. '*Socio-ecological resilience'* is een mengvorm van de vorige twee. Deze vorm van weerbaarheid wordt gedefinieerd als de hoeveelheid verstoring die een systeem kan opvangen, maar alsnog kan blijven functioneren. Daarbij hoort de mate waarin een systeem in staat is om de capaciteit te vergroten om van het incident te leren en zich aan te passen aan (toekomstige) incidenten. Weerbaarheid draait dan niet alleen om sterk zijn tegen verstoringen maar ook om de kansen die ontstaan op het gebied van reorganisatie, herschikking en het onstaan van nieuwe paden. Weerbaarheid brengt dan ook kansen voor vernieuwing.

Coaffee & Fussey (2015) kijken gerichter naar weerbaarheid en veronderstellen dat het draait om het weerstaan, opvangen en herstellen van verstoringen. Daarnaast vinden deze auteurs ook dat er geen eenduidige definitie van weerbaarheid bestaat en dat dit niet erg is. Beargumenteerd kan worden dat het belangrijker is om te begrijpen wat weerbaarheid doet en hoe het werkt in plaats van te weten wat het nu precies is. Als er gekeken wordt naar mkb'ers dan is het voor te stellen dat zij hier hetzelfde over denken. Misschien zijn zij niet geïnteresseerd in een definitie omdat ze alleen willen weten hoe ze hun bedrijf weerbaar moeten maken zonder dat ze zich druk hoeven te maken over wat het inhoudt. Verder beschrijven Coaffee & Fussey (2015) hoe het begrip in het Verenigd Koninkrijk door de jaren heen, als gevolg van allerlei ontwikkelingen zoals terrorisme en de angst die hierdoor onstaat, is veranderd en verbreed. Als gevolg van terrorisme was weerbaarheid allereerst reactief van aard en maatregelen werden bedacht die de dreiging van terrorisme tegen moest gaan. Weerbaarheid werd erg breed ingevuld en was vooral gericht op het versterken van zowel de fysieke omgeving als van de mensenlijke en technologische surveillance mogelijkheden. Vervolgens vond er een verschuiving plaats waar meer nadruk werd gelegd op de voorbereidende en preventieve aspecten van weerbaarheid. Er werd dus niet meer alleen gekeken naar het vermogen om incidenten op te vangen. De nationale overheid ging ook steeds meer samenwerken met lokale en regionale autoriteiten en verschillende andere overheidspartijen. Deze samenwerkingsdrang past volgens de auteurs in een langer gaande ontwikkeling in het Verenigd Koninkrijk en is niet alleen gerelateerd aan weerbaarheid. De derde en laatste ontwikkeling is dat weerbaarheid geïntegreerd werd in het alledaagse leven. Hierbij werd verwacht dat bedrijven, overheden en gemeenschappen gezamenlijk steeds meer onregelmatigheden (*shocks)* probeerden te voorspellen zodat hier op gereageerd kan worden. De verantwoordelijkheid voor weerbaarheid lag niet langer bij de overheid alleen, ook niet-overheidspartijen werden verantwoordelijk gemaakt. Samengevat zou op basis van deze drie ontwikkelingen weerbaarheid dus gedefinieerd kunnen worden als het vermogen om

incidenten te voorspellen, hier preventieve en reactieve maatregelen voor te bedenken en zonodig de gevolgen van incidenten te verminderen waarbij de verantwoordelijkheid voor deze acties zowel ligt bij de nationale en lokale overheid als bij het bedrijfsleven, de gemeenschap en waarbij weerbaarheid een integraal onderdeel vormt van het dagelijks leven.

Een uniek punt wordt aangedragen door Helm (2015). Deze zegt dat weerbaarheid de oplossing is voor de beperkingen die spelen bij risico-inschattingsmodellen. Beperkingen van deze modellen bestaan uit het hebben van te weinig informatie over de kans, grootte en effecten van bekende maar zeldzame gevaren. Daarnaast bestaan er onbekende grootschalige ongelukken die niet te voorspellen zijn, ook zijn er erg veel mogelijke gebeurtenissen die een ramp kunnen veroorzaken. Het is bijna onmogelijk om voorbereidingen voor al deze gebeurtenissen en diens onvoorspelbare effecten te treffen. Alleen het treffen van proactieve maatregelen is niet voldoende om veiligheid te garanderen. Weerbaarheid geeft een uitweg omdat het, onder andere, draait om het maken van aanpassingsplannen die in werking treden wanneer een incident plaatsvindt. Ook Helm erkent dat er nog geen universeel geaccepteerde definitie bestaat. Wel wordt weerbaarheid veelal gezien als 'a behavioural property of a system as it responds to and recovers from shock' (Helm, 2015: 102). Het is dus een manier om te reageren op en te herstellen van verstoringen. Daarnaast haalt hij een aantal definities aan van overheidsinstanties in het Verenigd Koninkrijk. Weerbaarheid wordt dan gedefinieerd als het vermogen om verstorende uitdagingen (*disruptive challenges)* te detecteren, te voorkomen en er zonodig mee om te kunnen gaan en er van te herstellen. Weerbaarheid wordt ook gedefinieerd als het vermogen om je voor te bereiden op nadelige gebeurtenissen, deze te kunnen absorberen, hiervan te kunnen herstellen en je er succesvol op aan te passen. (Helm, 2015: 102). Er zijn dus verschillende definities van weerbaarheid maar volgens Helm bevat weerbaarheid altijd twee componenten: *robustness* (robuustheid, sterkte) en *adaption* (aanpassing). Een weerbaarheidssysteem moet dus dermate sterk zijn dat functies blijven functioneren en het moet mogelijk zijn om grote aanvallen (*shocks)* op te vangen, hier snel op te reageren, hier op aan te passen en er uiteindelijk beter van worden door van het incident te leren (Helm, 2015: 108). Weller & Anderson (2013: 54) stellen dat *reisilience* veelal gedefinieerd wordt volgens de definitie van Hollin: 'the capacity of a system to absorb disturbances and reorganise while undergoing change, so as to retain essentially the same function, structure, identity and feedbacks'. Het kunnen opvangen van incidenten speelt een grote rol. Daarnaast is het vermogen van het systeem om te veranderen en op die manier dezelfde functies en structuur te behouden van belang.

De bovenstaande uiteenzetting van het begrip weerbaarheid laat zien dat de term op uiteenlopende manieren ingevuld wordt. De verschillende auteurs zijn het er over eens dat weerbaarheid er van uit gaat dan incidenten gebeuren en dat het van belang is om tijdens incidenten te blijven functioneren. Daarbij komt dat herstel na een incident van groot belang is. Verder moet er op het gebied van weerbaarheid naar het verleden gekeken worden om van incidenten te leren. Maar ook naar de toekomst, om incidenten enigszins te voorspellen. Op basis van deze punten kan een definitie gevormd worden. Dit is overigens niet altijd nodig omdat de genoemde punten laten zien hoe weerbaarheid werkt en wat het doet waardoor een definitie niet altijd nodig is (Coaffee & Fussey, 2015).

2.2 Interventies en het COM-B model

Interventies worden gebruikt om gedrag te veranderen. In de literatuur zijn voor zover bekend weinig onderzoeken gedaan naar interventies op het gebied van het verbeteren van digitale weerbaarheid van bedrijven of individuen. Wel zijn er verschillende onderzoeken gedaan naar het vergroten van bewustzijn met betrekking tot cybersecurity en welke interventies hiervoor geschikt en effectief zijn (Abawajy, 2014; Shaw, Chen, Harris, & Huang, 2009; Cone, Irvine, Thompson, & Nguyen, 2007; Choi, Levy, & Hovav, 2013). Abawajy (2014) stelt bijvoorbeeld dat *information security awareness* trainingen voor minder digitale incidenten zorgen. Dit soort trainingen worden gegeven om het gedrag en de attitude van werknemers over informatiebeveiliging en cybersecurity te beïnvloeden. Security awareness kan volgens Abawajy op verschillende manieren vergroot worden. Zo bestaan er conventionele manieren (posters, nieuwsbrieven, flyers), presentaties en seminars die verzorgd worden door experts, online methoden (blogs, e-mail, internetfora, screensavers), *game-based* methoden waarbij awareness vergroot wordt door een spel te spelen, e-learning en simulaties (phisingoefeningen). De auteur concludeert dat een mix van de verschillende methoden gewenst is om security awareness te verhogen. Ook Shaw e.a. (2009) hebben onderzoek gedaan naar information security awareness en methoden om dit te verbeteren. Zij hebben onderscheid gemaakt in drie typologieën: hypermedia (interactieve methoden bestaande uit een combinatie van audio, video, tekst en hyperlinks waarbij de gebruiker zelf beslist wat hij bekijkt), multimedia (combinatie van tekst, beeld, geluid, animatie waarbij de gebruiker niet zelf kan beslissen wat hij bekijkt) en hypertext (normale tekst met hyperlinks). Uit deze studie kwam naar voren dat het gebruik van hypermedia de voorkeur verdient omdat dit de perceptie, het begrip en het voorspellend vermogen van individuen met betrekking tot

informatiebeveiliging positief beinvloedt. Ook is er onderzoek gedaan naar het gebruik van een digitaal stripboek om cybersecurity te verbeteren (Zhang-Kennedy, Chiasson, & Biddle, 2016). Uit dit onderzoek komt naar voren dat de interactieve elementen van een digitaal stripboek positief werken om de kennis en het bewustzijn van gebruikers over informatiebeveiliging te verbeteren. De auteurs concluderen dat het versimpelen van beveiligingsinformatie door middel van grafische communicatie goed werkt om informatie over te brengen. Daarnaast bood het digitale stripboek entertainment waardoor gebruikers geïnteresseerd bleven. Ook kwam naar voren dat het stripboek voor gedragsverandering zorgde. Gebruikers werden bijvoorbeeld voorzichtiger en deelden de informatie met familieleden. Khan, Alghathbar & Khari (2011) hebben vanuit psychologisch oogpunt gekeken naar een aantal methoden om het bewustzijn met betrekking tot informatiebeveiliging te vergroten. Zij komen tot de conclusie dat groepsdiscussies het beste werken, gevolgd door educatieve presentaties. Deze twee methoden bieden kennis aan en zorgen voor gedragsverandering. Posters, nieuwsbrieven en e-mail berichten lijken het minst effectief omdat hier alleen eenzijdig informatie wordt aangeboden waardoor er weinig tot geen gedragsverandering plaatsvindt.

Zoals aangegeven moeten interventies gedrag veranderen en daarvoor moeten zij effectief zijn. Idealiter wordt, voordat een interventie wordt ingezet, (theoretisch) onderzocht of deze effectief kan zijn. Willen interventies effectief zijn dan moeten deze aansluiten op de doelgroep en de context waarin de interventie wordt toegepast. Het is van belang om de doelgroep en de context goed te analyseren, veelal gebeurt dit niet (Michie, Van Stralen, & West, 2011). Michie, Van Stralen & West (2011) hebben daarom het COM-B model ontwikkeld die gebruikt kan worden om de doelgroep (in deze scriptie het mkb) te analyseren en zo te bepalen welke interventies het meest geschikt zijn om gedragsverandering te bewerkstelligen. Het model wordt in deze scriptie als raamwerk gebruikt om de verzamelde data van de respondenten te analyseren. Hierdoor is het mogelijk om theoretisch te zeggen waarom interventies wel of niet zullen werken om de digitale weerbaarheid te versterken.

Het COMB-B model veronderstelt dat er drie componenten zijn die aanzetten tot gedrag. De *capabilities* (bekwaamheid), *opportunities* (kansen) en *motivations* (motivaties) van de doelgroep interacteren met elkaar en leiden zo tot bepaald *behaviour* (gedrag). Bekwaamheid draait om de psychologische en fysieke capaciteit waar een individu over moet beschikken om deel te nemen aan de activiteit die de interventie voorstelt. Het gaat hier ook om het hebben van de benodigde kennis (begrip en redenering) en vaardigheden. Toegespitst

op het mkb is het bijvoorbeeld mogelijk dat mkb'ers weinig kennis hebben van digitale weerbaarheid, denken dat het niet belangrijk is en daarom het nut niet inzien van het volgen van interventies zoals voorlichting. Andersom is het ook mogelijk dat mkb'ers wel veel kennis hebben en dus inzien dat interventies nuttig zijn. Motivatie wordt gezien als alle mentale processen die gedrag sturen. Het draait om gewoonten, emotionele reacties en het analytisch maken van keuzes door bijvoorbeeld keuzes te evalueren. Uit de data kan mogelijk naar voren komen dat mkb'ers weinig (of veel) motivatie hebben om zich te verdiepen in digitale weerbaarheid. Wanneer er voldoende motivatie is dan is het aannemelijk dat een interventie werkt. Bij weinig motivatie is dit niet het geval en zal er gezocht moeten worden naar manieren om mkb'ers te motiveren om aan de slag te gaan met digitale weerbaarheid. De term kansen wordt gedefinieerd als alle factoren (fysieke of sociale) die buiten de invloed van een individu liggen en die het gedrag mogelijk maken of in werking kunnen stellen. Gedacht kan worden aan alle mogelijke interventies (zoals voorlichtingsbijeenkomsten) die (semi) overheidsinstanties en private bedrijven aan mkb'ers aanbieden. Wanneer dit veel gebeurt dan zijn er voldoende kansen beschikbaar voor mkb'ers om bekend te raken met digitale weerbaarheid, hier het belang van inzien en vervolgens te investeren indien zij dat nodig vinden. De auteurs merken op dat de drie componenten elkaar kunnen beïnvloeden. De geboden kansen kunnen bijvoorbeeld tot meer of minder motivatie leiden. Een interventie kan dus gericht zijn op één component (bijv. motivatie), dit component kan dan de andere componenten (kansen en bekwaamheid) beïnvloeden. Deze drie componenten vormen dus de lens waarmee de verzamelde data geanalyseerd wordt. Kijkend vanuit dit model is het mogelijk om te bepalen of mkb'ers over voldoende motivatie en bekwaamheid beschikken en of zij voldoende kansen geboden krijgen om digitale weerbaarheid binnen de organisatie tot een hoger niveau te tillen. Door deze analyse te maken wordt duidelijk waarom, vanuit theoretisch oogpunt bezien, bepaalde interventies wel of niet zullen werken.

Volgens Michie, Van Stralen & West (2011) moet ook onderzocht worden welk type gedrag gewenst is en welke componenten van het COMB-B systeem daarvoor gemanipuleerd moeten worden. Voorlichtingsbijeenkomsten en trainingen worden bijvoorbeeld veelvuldig gebruikt om het bewustzijn over cybersecurity te verhogen (McCrohan, Engel, & Harvey, 2010; Bada & Sasse, 2014). Het is dan de vraag of deze bijeenkomsten de componenten bewkaamheid, kansen en motivatie dusdanig beïnvloeden dat het gewenste gedrag (meer bewustzijn over cybersecurity) bereikt wordt. Een voorlichting kan bijvoorbeeld zorgen voor meer bewkaamheid en kennis maar dit betekent niet dat een mkb'er daardoor ook gemotiveerd is om te investeren in digitale weerbaarheid. Voorafgaand aan de

voorlichtingsbijeenkomst moet er gekeken worden naar de te manipuleren componenten zodat het gewenste gedrag ontstaat. Een soortgelijke analyse zou volgens Michie, Van Stralen & West (2011) gedaan moeten worden voor iedere interventie. Hierbij merken de auteurs op dat een interventie niet altijd gericht hoeft te zijn op alle componenten. Het is ook mogelijk dat alleen de bekwaamheid via een interventie wordt vergroot omdat de doelgroep hier behoefte aan heeft en al gemotiveerd is.

3. Methoden

In dit hoofdstuk worden de gebruikte methoden beschreven. Allereerst wordt beschreven hoe respondenten zijn geselecteerd, vervolgens worden de gebruikte instrumenten beschreven. Daarna wordt uitgelegd welke procedure gebruikt is en hoe de data geanalyseerd is.

3.1 Deelnemers

Voor dit onderzoek zijn respondenten uit twee verschillende groepen benaderd en geïnterviewd. De eerste groep bestaat uit cybersecurity experts. Respondenten uit deze groep zijn op pragmatische wijze gekozen. Op internet is gezocht naar partijen die zich profileerden als experts. Voorafgaand aan het benaderen van experts is gezocht naar basale informatie (missie, doelstelling, werkzaamheden) over de instantie of het bedrijf. Deze informatie vormde de criteria om te beoordelen of de expert een geschikte partij was om te benaderen. Daarnaast is gebruik gemaakt van de eigen kennis van instanties en bedrijven en van eigen professionele netwerken. Uiteindelijk zijn zes diverse experts, werkzaam voor de overheid, private partijen en kennisinstituten, benaderd en geïnterviewd[1]. Alle experts zijn via de mail benaderd en is gevraagd of zij interesse hadden om mee te werken aan het onderzoek.

De andere groep bestaat uit mkb ondernemers of organisaties die mkb'ers vertegenwoordigen zoals brancheorganisaties. Ook deze respondenten zijn op pragmatische wijze geselecteerd en benaderd. Via zoekopdrachten op het internet, eigen kennis en persoonlijke en eigen professionele netwerken zijn respondenten benaderd. Omdat de focus van dit onderzoek op de gehele mkb sector ligt, is er niet gekozen om een onderscheid te maken tussen bedrijfstakken of branches. Uiteindelijk zijn, na het benaderen van ongeveer 25 mkb'ers, zes uiteenlopende respondenten (mkb-ondernemers, brancheverenigingen en kennisinstituten) uit de mkb wereld geïnterviewd.

3.2 Instrumenten

Er is gekozen voor interviews omdat beide groepen (mkb'ers en experts) gezien worden als waardevolle informatiebronnen. Via interviews is het mogelijk om de informatie waar deze groepen over beschikken te achterhalen. Volgens Beyens & Tournel (2010: 204-206) worden kwalitatieve interviews veelal gebruikt bij het beantwoorden van open vragen zoals waarom en hoe-vragen. Via kwalitatieve interviews is het mogelijk om de respondent te laten vertellen

[1] Zie bijlage voor een overzicht van de respondenten.

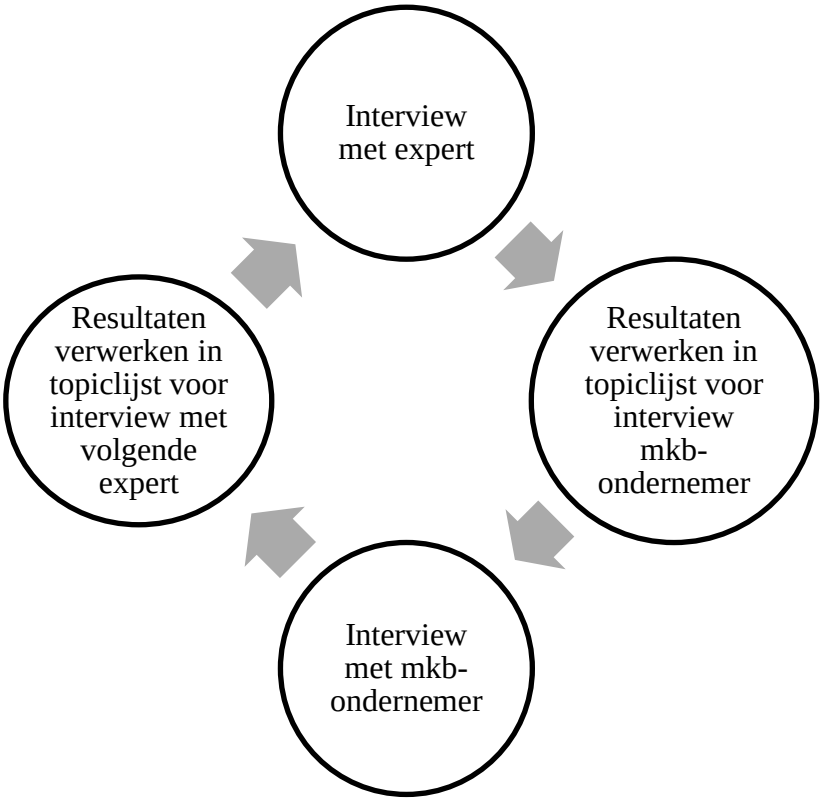
over het onderwerp dat onderzocht wordt. Semi gestructureerde interviews worden gezien als de meeste effectieve en geschikte manier om informatie te verzamelen. Daarnaast is dit type interview flexibel omdat afgeweken kan worden van de vragenlijst indien andere relevante onderwerpen ter sprake komen. Een groot voordeel van dit type interview is dat belangrijke en vaak verborgen informatie naar voren kan komen omdat de respondent vrijuit kan praten en de interviewer in kan spelen op de respondent. Deze kan de stijl, de snelheid en de volgorde van vragen aanpassen om de meest uitgebreide antwoorden uit de respondent te halen. Ook stelt het de respondent in staat om in zijn of haar eigen woorden antwoord te geven (Qu & Dumay, 2011). Digitale weerbaarheid en de wereld van cybersecurity zijn erg omvangrijk waardoor een open benadering gewenst is. De beweegredenen die mkb'ers en experts aankaarten komen sneller naar voren in kwalitatieve interviews omdat de respondent aan het woord gelaten wordt en er doorgevraagd kan worden wat bij enquêtes of andere methoden lastiger is. Verder staan gedachten en overwegingen van mkb'ers en experts centraal staan. Interviews zijn om deze redenen de meest geschikte onderzoeksmethode.

Voorafgaand aan het eerste interview is een topiclijst opgesteld. Globaal is er een driedeling gemaakt tussen de onderwerpen, te weten: inleidende topics, topics met betrekking tot digitale weerbaarheid en manieren om digitale weerbaarheid te vergroten. Bij ieder topic zijn een aantal open vragen en *probes* (Hennink, Hutter & Bailey, 2011: 119) opgesteld om er voor te zorgen dat overige belangrijke en gedetailleerde informatie verzameld kan worden. Dezelfde topiclijst is gebruikt voor beide groepen. De topics waren geselecteerd op basis van eigen ideeën en op basis van de literatuur. In de literatuur werden bijvoorbeeld mogelijke oorzaken aangedragen die een obstakel voor bedrijven vormden om te investeren in cybersecurity. Deze oorzaken werden als *probes* (Hennink, Hutter & Bailey, 2011: 119) gebruikt bij het vragen naar obstakels bij het investeren in digitale weerbaarheid. Daarnaast is, zoals eerder beschreven, gebleken dat er veel onduidelijkheid is over wat digitale weerbaarheid nu precies is. Een concrete vraag die gesteld werd in het interview was dan ook wat de respondent verstond onder het begrip digitale weerbaarheid. Ook zijn er effectstudies gedaan naar de inzet van verschillende interventies om het (digitale) veiligheidsbewustzijn te verhogen. Tijdens de interviews is dan ook gevraagd naar mogelijke (nieuwe) interventies of manieren die volgens de respondent effectief kunnen zijn in het verhogen van de digitale weerbaarheid. Verder moet worden opgemerkt dat de topiclijst gedurende de onderzoeksperiode is aangepast aan de hand van informatie van eerdere interviews. Het ging om onderwerpen die ter sprake waren gekomen tijdens het interview maar niet op de topiclijst stonden en wel relevant leken voor volgende interviews.

3.3 Procedure

De interviews zijn afgenomen op de locatie waar de respondent werkzaam was. Alle interviews vonden plaats in een aparte ruimte waardoor de kans op verstoring minimaal was. Eén interview met een mkb'er vond plaats in de zitgelegenheid van de onderneming waardoor klanten aanwezig waren en mee konden luisteren met het interview. Dit vormde echter geen obstakel. Voorafgaand is gevraagd of het gesprek opgenomen mocht worden en of de respondent geanonimiseerd wilde worden. Geen van de experts had behoefte om geanonimiseerd te worden. Eén interview is op aanvraag van de respondenten niet opgenomen, van dit interview is een verslag gemaakt. Eén mkb'er wilde anoniem blijven. Wanneer de topiclijst volledig was doorgelopen en er verder geen onderwerpen meer ter sprake kwamen, is gevraagd of de respondent nog aanvullingen had. Daarna is gestopt met interviewen. Gemiddeld genomen duurde een interview 75 minuten. Ook zijn vijf voorlichtingsbijeenkomsten van de VAR bijgewoond. Tijdens deze bijeenkomsten is gelet op de vragen en opmerkingen die mkb'ers tijdens de voorlichting stelden. Ook is er na iedere bijeenkomst een korte vragenlijst rondgestuurd naar de deelnemers waar bijvoorbeeld gevraagd werd naar de behoeften die zij hebben op het gebied van digitale weerbaarheid en cybersecurity. Deze vragenlijst is rondgestuurd naar ongeveer 140 mkb'ers. Uiteindelijk hebben tien ondernemers deze vragenlijst ingevuld.

De onderzoeksopzet bestond uit het afwisselend interviewen van expert en mkb'er. Eerst is een expert geïnterviewd, daarna een mkb-ondernemer. Op deze manier is het mogelijk een goede vergelijking te maken tussen beide partijen. De informatie uit het expertinterview kan direct gebruikt worden tijdens het interview met een mkb'er. Hierna is opnieuw gesproken met een andere expert waarbij de resultaten van het interview met de mkb'er meegenomen zijn indien dit relevant genoeg leek. Het was bijvoorbeeld mogelijk dat één van de groepen (mkb'er of expert) een interessant punt aankaartte waar de andere groep over bevraagd kon worden. Schematisch ziet het bovenstaande er als volgt uit:



Figuur 1: Schematische weergave van de onderzoeksmethodiek

De toegevoegde waarde van de vergelijking tussen expert en mkb'er is dat op deze manier de verschillende denkwijzen van beide groepen tegen elkaar afgezet kunnen worden. Vergelijkingen tussen experts en leken zijn eerder gedaan en hebben tot verschillende conclusies geleid (Isaacs & Clark, 1987; Fiske, Kinder, & Michael-Larter, 1983; Brand-Gruwel, Wopereis, & Vermetten, 2005). Zo is naar voren gekomen dat experts en leken bepaalde zaken anders beschrijven. Experts zijn bijvoorbeeld uitgebreider en denken na over achterliggende contexten terwijl leken dit niet doen (Hmelo-Silver & Green-Pfeffer, 2004). Daarnaast is gebleken dat het voor experts soms moeilijk is om informatie over te brengen op leken. Dit komt bijvoorbeeld omdat experts op een hoger en abstracter niveau communiceren waardoor het voor beginners moeilijk is om van experts te leren (Hinds & Pfeffer, 2002). Het vergelijken van experts met leken, of in dit geval mkb'ers zonder cybersecurity kennis, kan waardevolle inzichten opleveren. Door te vergelijken kan er gekeken worden waarom de kennis die experts hebben over cybersecurity of digitale weerbaarheid niet altijd overgenomen wordt door mkb'ers. Wanneer dit het geval is dan profiteren mkb'ers niet optimaal van de beschikbare kennis van experts. Daarnaast kunnen beide partijen verschillende opvattingen hebben over geschikte interventies. Als experts van mening zijn dat een interventie geschikt is terwijl deze mening niet gedeeld wordt door de mkb'er dan is het de vraag of de interventie

kans van slagen heeft omdat mkb'ers misschien niet gemotiveerd zijn. Inzicht in deze kloven kan dus waardevol zijn en wordt inzichtelijk gemaakt door beide groepen te interviewen.

3.4 Analyse

De getranscribeerde interviews zijn geanalyseerd met het kwalitatieve data analyse programma Atlas.ti. Bij kwalitatieve analyses wordt doorgaans gebruik gemaakt van open codering, gesloten codering of een combinatie. Een code is een onderwerp dat tijdens het interview ter sprake is gekomen of een onderwerp dat tijdens het analyseren van de data herkend wordt door de onderzoeker. Codes worden om verschillende redenen gebruikt. De meest voorkomende en belangrijke reden is dat codes gebruikt worden als indicatoren of bladwijzers van (veelvoorkomende) onderwerpen die terug komen in de data. Op deze manier is het voor de onderzoeker mogelijk om op een gemakkelijke manier ieder stukje data terug te vinden waar een bepaald onderwerp genoemd wordt (Hennik, Hutter & Bailey, 2011: 216-217). Hennik, Hutter & Bailey (2011) stellen dat er twee typen codes bestaan: deductieve en inductieve. Deductieve codes worden opgesteld door de onderzoeker en zijn afkomstig van de onderwerpen die terugkomen in de topiclijst. Inductieve codes worden geformuleerd door de data te analyseren en onderwerpen te identificeren die door respondenten worden besproken maar die niet op de topiclijst staan. Deze codes kunnen van belang zijn omdat ze afkomstig zijn van de respondenten zelf en niet van de onderzoeker. De onderzoeker kan bijvoorbeeld bij het opstellen van deductieve codes bepaalde onderwerpen over het hoofd gezien hebben die wel van belang zijn voor de respondenten. Het identificeren van inductieve codes verhelpt dit probleem. Het is dus van belang om beide typen codes te gebruiken bij kwalitatieve analyses (Hennik, Hutter & Bailey, 2011: 218).

In dit onderzoek is in eerste instantie gebruik gemaakt van deductieve codes omdat het onderzoek deels gericht van aard is, want er worden twee centrale concepten onderzocht worden. Daarna is, bij nadere analyse van de data, gebruik gemaakt van het inductief coderen van de data. Er lag nagenoeg evenveel nadruk op beide typen codes bij het analyseren van de data. Op het gebied van aangedragen interventies zijn deductieve codes gebruikt omdat interventies specifiek te coderen zijn. De vooraf opgestelde deductieve code 'interventie' is bijvoorbeeld zeer geschikt om tekstsegmenten te selecteren waarin de respondent vertelt over interventies. Inductieve codes zijn ook gebruikt. Vooral op het gebied van obstakels die de effectiviteit van een interventie bemoeilijken zijn deze codes gebruikt. Voor de vraag over digitale weerbaarheid is in dezelfde mate gebruik gemaakt van deductieve en inductieve

codes. Ook hier geldt dat een respondent zeer specifiek kan praten over digitale weerbaarheid waardoor een vooraf opgestelde code als ‘digitale weerbaarheid’ gebruikt kan worden. Achterliggende gedachten van de respondenten over het begrip zijn na verdere analyses inductief gecodeerd.

Voor het deductief coderen is gebruik gemaakt van een ‘top down’ analyse waarbij de data uit de interviews gecodeerd wordt op basis van het theoretisch kader en de twee centrale concepten. Omdat het onderzoek gericht is, is er voor gekozen om op basis van deze concepten deductieve codes op te stellen (Van Staa & Evers, 2010). Deze codes zijn vervolgens gebruikt om de data te analyseren. Hierbij wordt gebruik gemaakt van een mengvorm tussen de ‘search by code’ en ‘search by topic’ strategieën zoals beschreven door Hennink, Hutter & Bailey (2011: 235). Deze strategie houdt in dat een paar codes worden gekozen. Vervolgens wordt de tekst geanalyseerd waarbij gezocht wordt naar tekstsegmenten waar de codes op van toepassing zijn. Daarnaast is er veel ruimte gelaten om ook inductieve codes te identificeren in de data. Ook is gebruik gemaakt van de netwerkfunctie van het programma Atlas.ti. Met deze functie is het mogelijk om relaties tussen codes en tekstsegmenten inzichtelijk te maken en een duidelijk overzicht te creëren. Op deze manier is het mogelijk om overkoepelende thema’s te onderscheiden en te groeperen die gebruikt kunnen worden om invulling te geven aan het resultatenhoofdstuk.

4. Resultaten

In dit hoofdstuk worden de resultaten gepresenteerd. Allereerst wordt ingegaan op wat digitale weerbaarheid volgens de verschillende deelnemers is en welke factoren van invloed zijn. Vervolgens wordt ingegaan op geschikte interventies en welke randvoorwaarden spelen bij het formuleren van interventies.

4.1 Wat is digitale weerbaarheid?

Bij ieder interview is aan de respondent gevraagd wat hij of zij verstond onder het begrip 'digitale weerbaarheid'. Allereerst zal beschreven worden wat experts verstaan onder het begrip.

4.1.1 Experts

Op basis van de gesprekken met experts is naar voren gekomen dat het concept 'digitale weerbaarheid' uiteen valt in verschillende dimensies of thema's. Rick van der Kleij vertelt dat weerbaarheid bestaat uit vier vermogens waar een organisatie over moet beschikken. Het vermogen om te anticiperen op kansen en dreigingen, het vermogen om dreigingen te kunnen detecteren en monitoren, het vermogen om te reageren op incidenten en het vermogen om te leren van incidenten. Het vergroten van de capaciteit van deze vier vermogens zou dan moeten leiden tot een hoger niveau van digitale weerbaarheid (Van der Kleij, 2018). Deze vermogens worden hieronder als rode draad gebruikt.

Anticiperen op kansen en dreigingen

Het eerste vermogen is om te kunnen anticiperen op kansen en dreigingen en dat bedrijven moeten weten wat er speelt en wat er op het gebied van incidenten aan zit te komen. Als bedrijven dit weten dan kunnen ze zich voorbereiden op mogelijke incidenten. Deze anticiperende functie is van belang omdat niet alle incidenten volgens Van der Kleij te voorkomen zijn: *'maar je kunt het [incidenten] niet voorkomen zeg maar, er zal eens een keer iets misgaan je kunt niet alles buiten de deur houden'.* Bewustzijn over digitale criminaliteit kan het anticiperen op kansen en dreigingen vergemakkelijken. Peter Duin zegt bijvoorbeeld: *'Er komen steeds meer initiatieven in de maatschappij, als het alleen maar toeneemt en mensen raak daar meer geïnformeerd, de bewustwording wordt sterker, die weerbaarheid wordt sterker'.* Ook Leo Lans en Marieke van Leeuwen zijn van mening dat de anticiperende functie van weerbaarheid sterk samenhangt met bewustzijn. Zij vinden dat als mkb'ers zich

bewust zijn van de gevaren, zij ook weerbaarder worden. Verder kan preventie gezien worden als onderdeel van het anticiperen op dreigingen. Duin: *'Dat zegt ook resilience, je wilt voorkomen, is beter dan genezen. En om te voorkomen, zit ook in het woord, moet je aan de voorkant komen'.* Volgens Duin is het van belang dat fabrikanten van ICT producten, deze goed beveiligen zodat ze niet misbruikt kunnen worden door cybercriminelen. Daarnaast kunnen preventiemaatregelen zoals goed digitaal hang –en sluitwerk een belangrijke rol spelen bij het anticiperen op bedreigingen. Preventie is dus verbonden met anticipatie. Duin illustreert dit door het voorbeeld van het gevaar van slecht beveiligde ICT producten te noemen. Wanneer ondernemers weten dat ICT producten slecht beveiligd zijn (ze anticiperen op de gevaren), dan kunnen zij hier preventief op inspelen door deze producten niet te kopen.

Detecteren en monitoren

Het tweede vermogen houdt in dat bedrijven dreigingen moeten kunnen detecteren en monitoren. De technologische capaciteit moet hier wel beschikbaar voor zijn. Het treffen van maatregelen om te kunnen detecteren en monitoren maakt eveneens onderdeel uit van digitale weerbaarheid. Lans en Van Leeuwen vertellen dat bedrijven de mogelijkheid hebben om verschillende detectieve maatregelen te nemen. Deze (technische) maatregelen kunnen gericht zijn op mensen en processen. Ondanks dat door de respondenten niet veel verteld is over detectie en monitoring is het wel van belang om te benoemen dat het treffen van verschillende typen maatregelen onderdeel uitmaakt van dit vermogen.

Reageren op incidenten

Veerkracht maakt onderdeel uit van het reageren op incidenten. Zowel Van der Kleij als Duin onderkennen het belang van veerkracht. Volgens Duin moet veerkracht er voor zorgen dat het bedrijf snel weer terugkeert naar de normale bedrijfsvoering: *'Als ik jou heb weggedrukt hoe ga jij dan weer terugkomen naar mij, hoe weet jij dan weer terug te zijn in de markt. Cyber resilience gaat over continuïteit van de bedrijven […] zodat als je geraakt wordt door een cyberincident dat je bijvoorbeeld heel snel goede backups kan teruglezen dat je heel snel misschien je apparatuur kan vervangen, etc. Maar dat je dus heel snel terug bent in business.* Volgens Van der Kleij hangt veerkracht ook samen met *'het vermogen […] om adequaat te kunnen reageren om terug te veren op een snelle en goede manier'*. Een incident vindt plaats en het is aan de organisatie om hier op te reageren en terug te keren naar de oorspronkelijke situatie. Duin verwoordt het als volgt: *'Wat komt er nu op ons af als een projectiel, ja daar kan je niet meer, die moet je gewoon ontvangen en dan komt die veerkracht, laat dat*

projectiel maar inslaan en dan kijken hoe we hem gaan oplossen'. Anticiperen, detecteren en monitoren hangen volgens Duin dus samen met het vermogen om te reageren. Als een organisatie weet dat een incident onvermijdelijk is (anticipatie) dan is het vermogen om te reageren zeer belangrijk. Ook om te reageren op incidenten kunnen verschillende (technische) maatregelen genomen worden. Een concrete maatregel die Duin benoemt is het terugzetten van backups, Lans en Van Leeuwen spreken over responsieve maatregelen die ingezet worden als een incident plaatsvindt.

Leren van incidenten

Het vierde vermogen draait om het leren van incidenten. Bedrijven moeten weten wat er is gebeurd, snappen wat er is gebeurd en hiervan leren. Zo kunnen toekomstige incidenten worden voorkomen en kan hier beter op worden gereageerd. Deze lerende functie wordt ook benadrukt door Duin: *'Maar het is ook natuurlijk dat zo'n mkb'er naar zichzelf moet kijken en ook voor zichzelf moet bedenken van wat kan ik hier nou van leren. Hoe kan ik nou zorgen dat dit mij niet meer overkomt. Dus er moet ook een soort lerend vermogen komen binnen dat mkb bedrijfje, binnen die andere bedrijven dat ze sneller en beter leren van wat hun overkomen is'.* Daarnaast is hij van mening dat de lerende functie versterkt wordt als mkb'ers open zijn over cybercrime incidenten waar zij mee te maken hebben gehad. Andere mkb'ers kunnen hiervan profiteren. Duin verwoordt het als volgt: *'Dus dat als die mkb'er getroffen wordt en ook al schaamt hij zich er voor dan kan hij altijd anoniem zijn verhaal vertellen bijvoorbeeld aan de politie of aan een ander of aan misdaad anoniem […]. In elke aangifte of in elke melding zit wel een lessons learned. En als je die kan vertalen naar de taal van de doelgroep dan kan die doelgroep weer die maatregelen treffen'.* Communiceren over incidenten kan een wezenlijke bijdrage leveren aan het lerend vermogen onder bedrijven. Communicatie kan in de vorm van aangiften, meldingen of als collega's onder elkaar.

4.1.2 Midden –en kleinbedrijf

De antwoorden van de respondenten uit het mkb worden ingedeeld onder de vier verschillende vermogens zoals benoemd door Van der Kleij.

Anticiperen op kansen en bedreigingen

Op het gebied van het vermogen om te anticiperen op kansen en bedreigingen noemen de respondenten uit het mkb vooral bewustzijn als belangrijk onderdeel. Stefan Molleman zegt bijvoorbeeld: *'Ik denk bewustzijn van de risico's die je loopt en daar ook passende*

maatregelen op treffen'. Ook Tessa van Stiphout is van mening dat bewustzijn een wezenlijk onderdeel uitmaakt van digitale weerbaarheid: *'Dus bewustwording over, op het moment dat je dan digitaal bezig bent, al gaat het dus om je camerasysteem of je Wi-Fi netwerk. Het hoeft helemaal niet geavanceerd te zijn. Dat je bewust bent van de potentiële risico's, dat is al één'* Op basis van deze potentiële risico's is het aan de ondernemer om te bepalen tegen welke risico's hij of zij zich weert en tegen welke niet. Van Stiphout: *'En twee dat je dus ook bewust een keuze maakt van dit is het beveiligingsniveau dat ik aanga als ondernemer'.* De ondernemer neemt dan bewust de beslissing om digitale bedrijfsprocessen wel of niet te beschermen door het nemen van (preventieve) maatregelen. Volgens Van Stiphout bestaat digitale weerbaarheid dus enerzijds uit het bewust zijn van potentiële risico's die digitale systemen met zich mee brengen, anderzijds omhelst het begrip het nemen van preventieve maatregelen. Kees Boom ziet digitale weerbaarheid eveneens tweedelig: *'Nou ja denk ik inderdaad vooral kennis onder de mensen maar ook een stuk techniek. Wij hebben een VPN lijn […] dat geeft ons wel wat meer digitale weerbaarheid. Dus ik denk vooral aan kennis en aan hardware, hoe makkelijk is het om binnen te komen'.* Hier schuilt een deel preventie in omdat technische maatregelen (VPN) worden getroffen om oneigenlijke toegang tot het bedrijfsnetwerk te voorkomen. Madelon Janssen benoemt impliciet preventie en bewustzijn als onderdeel van het vermogen om te anticiperen op bedreigingen: *'Ja, gewoon als ik zeker weet dat ik daar niet op moet klikken of dat ik dat niet moet doen. Daar voorkom ik mee dat ik allerlei problemen nakrijg. Daar begint het mee'.* Ook Diederick Groeneveld kijkt vanuit preventief oogpunt naar digitale weerbaarheid en vertelt: *'Ja, het meest tastbare dat je meteen hebt is gewoon je wachtwoorden denk ik […] en daarna krijg je gewoon, ja we hebben een server, die staat ergens en het is gewoon belangrijk dat we met een partij zaken doen waar we op kunnen vertrouwen dat zij dat netjes hebben afgedicht'.* Digitale weerbaarheid bestaat volgens deze respondenten dus vooral uit preventie en het voorkomen van incidenten. Het vermogen om te anticiperen kan ook vergroot worden door bedrijfsbeleid en personeelsinstructies te hanteren. Organisaties proberen op die manier te voorkomen dat werknemers op verkeerde links klikken en leren goed om te gaan met informatie.

Detecteren en monitoren

Detectie en monitoring worden niet expliciet benoemd door de mkb'ers. Wel zeggen Janssen en Pieter van Klaveren dat het gezond verstand een rol speelt bij digitale weerbaarheid. Het hebben van gezond verstand kan gerelateerd worden aan het detecteren van dreigingen. Janssen vertelt bijvoorbeeld: *'Als ik mailtjes zie binnenkomen waarvan ik de origine niet ken*

dan zijn ze weg, die open ik echt niet […]. Maar ja, gewoon een beetje gezond verstand'. Volgens Van Klaveren moeten ondernemers ook een beetje logisch nadenken over gevaren. Dit logisch nadenken kan helpen bij het detecteren van gevaren. Gedacht kan worden aan het voorbeeld van Janssen. Logisch nadenken over onbekende mailtjes, en daarmee gevaren detecteren, kan een hoop ellende voorkomen. Voorlichting kan dit gezonde verstand vergroten alleen is hij ook van mening dat een aantal mensen nooit wijzer zullen worden. Verder kunnen collega's een rol spelen bij het detecteren van dreigingen. Volgens Boom moet er een soort meldcultuur ontstaan onder collega's wanneer iemand een dreiging denkt te zien. Boom: *'Kijk wat je eigenlijk wil is dat mensen elkaar gaan waarschuwen en dat gebeurde eigenlijk ook wel. Van joh, niet klikken wacht eventjes totdat we IT gesproken hebben wat dit is'.* In een meldcultuur zit ook een lerend element omdat werknemers van elkaar kunnen leren bepaalde dingen niet te doen, zoals het aanklikken van links. Daarnaast moeten werknemers wat wantrouwiger worden volgens Boom, ze moeten niet overal zomaar op klikken. Gezond verstand en personeel spelen volgens de respondenten dus een rol op het gebied van detectie en monitoring van dreigingen.

Reageren op incidenten

Impliciet wordt reageren op incidenten en het belang van veerkracht door verschillende respondenten genoemd. Janssen vertelt bijvoorbeeld over een situatie waarin de bestelsite niet functioneerde en klanten niet konden bestellen: *'Het begrip is nul eigenlijk bij klanten. Want ja, klant is koning dan moet er maar een andere oplossing komen. Dan heb je toch een back up server of je hebt toch een tweede webnet. Ja, is natuurlijk niet zo want dat kost klauwen vol met geld'*. Ondanks dat veerkracht volgens Janssen veel geld kost heeft ze wel geïnvesteerd in een back-up dongel zodat de Wi-Fi verbinding behouden blijft ingeval een storing. Ook Boom beschikt in het kader van veerkracht over back-ups. Interessant is dat een groot deel van de respondenten vertrouwt op zijn of haar ICT leverancier bij het reageren op incidenten. Van Stiphout vertelt: *'En daardoor een soort vertrouwen hebben in hun IT leverancier omdat vooral het echte kleinbedrijf is ook geen specialist in deze zaken. Dus ik denk nou, dit gaat mij ook te ver. Daarvoor heb ik toch een IT leverancier. Laat die het maar oplossen'.* Ook Groeneveld zegt dat ingeval van incidenten de IT leverancier snel wordt benaderd en dat de keuze om ICT uit te besteden een bewuste is geweest: *'Alleen op dit moment is het dus ook zo omdat we bij een andere partij zitten, dat het risico daar ook ligt. Dus als zij het verneuken dan is het ook hun probleem'.* Op de IT leverancier wordt vertrouwd om adequaat te reageren op incidenten en indien nodig veerkracht te bieden door back-ups terug te zetten. Naast

veerkracht en vertrouwen op IT leveranciers vertelt Janssen dat weerbaarheid bestaat uit bescherming. Janssen: *'Nou ja, weerbaarheid is in feite jezelf beschermen. Dus digitale weerbaarheid is jezelf beschermen op het digitale net dus alles wat in feite via de bits binnenkomt, naar buiten gaat. Dat je dat beschermd hebt, beveiligd hebt.* Daarnaast bestaat weerbaarheid uit het feit *'dat je in ieder geval weet hoe je er mee om moet gaan. Weerbaarheid is natuurlijk ook dat je weet hoe je er mee om moet gaan'*. Dit laatste hangt mogelijk weer samen met bewustzijn over het probleem. Als ondernemers weten wat ze kunnen doen, dan kunnen ze beter reageren op incidenten.

Leren van incidenten

Het lerend vermogen wordt vrijwel niet genoemd door de respondenten. Wel noemen verschillende respondenten dat incidenten aanleiding kunnen zijn om te investeren in digitale weerbaarheid. Mkb'ers kunnen als het ware leren van de incidenten van anderen. Groeneveld beschrijft het als volgt: *'Ja, er zijn bijna geen mkb bedrijven om mij heen gehackt. Als wij van onze klanten bijvoorbeeld zouden horen, of van andere uitzendbureaus zouden horen dat zij gehackt worden, dan wordt het voor ons een dingetje om er iets aan te gaan doen'.* Van Stiphout is eveneens van mening dat het nuttig is om mkb'ers attenderen op incidenten die bij collega ondernemers hebben plaatsgevonden: *'We hebben vaak geprobeerd om met ondernemers ook als soort voorbeelden te pitchen van kijk eens, nou deze ondernemer heeft zoveel schade opgelopen dus dat is wel iets wat in de communicatie goed werkt'.* Wel is er een probleem bij het naar buiten brengen van verhalen van mkb'ers die incidenten hebben meegemaakt. Ze vertelt: *'Maar het is echt taboe, ik ga echt niet aan de bühne vertellen dat er zoveel van mijn klantgegevens op straat lagen'.* Het vermogen om te leren van incidenten kan niet volledig benut worden omdat mkb'ers niet bereid zijn slachtofferverhalen naar buiten te brengen.

4.1.3 Vergelijking

Experts kijken breed naar het begrip door de vier vermogens te noemen en veel aandacht te besteden aan het lerend vermogen. De mkb'ers refereren impliciet aan de genoemde vermogens en praten meer over concrete maatregelen die zij hanteren om de digitale weerbaarheid van de organisatie vorm te geven. Vooral beschermende en herstellende maatregelen worden besproken. Experts doen dit minder maar benadrukken wel dat veerkracht van groot belang is. Daarnaast besteden veel mkb'ers digitale weerbaarheid uit aan ICT leveranciers en vertrouwen ze op deze partijen. Wellicht dat dit een reden is waarom

mkb'ers niet breed naar het begrip kijken. Het is een onderwerp waar ze zich niet altijd druk om maken omdat ze een andere partij verantwoordelijk hebben gemaakt. Volgens Hugo Leisink is dit juist gewenst: *'Betaal in godsnaam die 50 euro per maand. Dan heb je daar geen kopzorgen aan, ik bedoel je wilt ondernemen, jouw richting zit niet in de ICT dus jouw denkrichting zit ook niet in de ICT, ga dat dan ook niet erbij forceren. De kosten zijn echt niet die 50 euro, doe niet zo raar, ga niet zelf lopen prutten met een servertje ergens in de cloud hangen. Rot op'.*

4.2 Interventies

In deze paragraaf wordt ingegaan op de interventies die volgens de respondenten geschikt zijn om de digitale weerbaarheid van een bedrijf te vergroten. Allereerst wordt ingegaan op de obstakels en randvoorwaarden die genoemd worden bij het toepassen van interventies. Vervolgens wordt aandacht besteed aan het belang van maatwerk en het inspelen op behoeften. Daarna wordt de interventie voorlichting uitgelicht.

4.2.1 Obstakels bij het toepassen van interventies

Uit de analyses is naar voren gekomen dat beide partijen verschillende obstakels noemen die de inzet van interventies kunnen bemoeilijken. Het is van belang om inzicht in deze factoren te krijgen voordat interventies worden ingezet.

Experts

Van der Kleij vertelt dat er een kennistekort is op het gebied van interventies om de digitale weerbaarheid binnen mkb te verhogen. Kennis is volgens hem nodig om tot goede interventies te komen. Van der Kleij: *We zijn nu vooral bezig met het in kaart brengen van wat is dat weerbaarheid en hoe kan je dat meten, uit wat voor componenten bestaat dat en straks hebben we dan een beeld van hoe de situatie is en of er verschillen zijn en wat voor factoren daar een rol in spelen. Maar de stap die we daarna willen zetten is inderdaad het gaan bedenken van interventies voor het mkb. Afhankelijk van die kennis zou je daar goede suggesties over kunnen maken'.* Het uitvoeren van een goede analyse is volgens hem van belang om goede interventies te kunnen kiezen die toepasbaar zijn voor specifieke mkb sectoren of bedrijven. Ook vertelt Van der Kleij over studies die wel gedaan zijn naar interventies in het digitale domein en dat deze niet toereikend genoeg zijn. Van der Kleij: *' […]studies die zijn gedaan, dat zijn een soort one shot studies, je doet een interventie, je meet wat het effect direct is zonder echt te kijken naar wat dat over de tijd doet en wat het effect is*

van herhalingen. Dat wordt vaak niet gedaan dus daar is wel behoefte aan dat soort onderzoek'. Longitudinaal onderzoek is volgens hem nodig om interventies te kiezen waar het mkb op de lange termijn profijt van blijft hebben. Van der Kleij suggereert dat interventies uit het niet digitale domein mogelijk hergebruikt kunnen worden voor het digitale domein. Welke interventies dit zijn, weet hij (nog) niet. Het probleem van een kennistekort wordt ook benoemd door Molleman. Hij werkt voor het Centrum voor Criminaliteitspreventie (CCV) en vertelt dat ook zij bezig zijn met het verzamelen van kennis. Molleman: *'Wij hebben hier ook gedragsexperts dus we zijn aan het kijken hoe kunnen we nou met de expertise die we hebben met gedragsverandering, die training zo ontwikkelen dat het ook aanzet tot gedrag'*. Ook het DTC is bezig met het vergroten van de kennis over digitale weerbaarheid en interventies die hier geschikt voor zijn. Zij hebben, net als Het CCV, gedragswetenschappers in dienst die bezig zijn met het ontwikkelen van interventies.

Naast het genoemde kennistekort worden andere obstakels genoemd. Eén van deze obstakels is het feit dat mkb'ers het belang van digitale weerbaarheid en cybersecurity niet altijd inzien. Molleman vertelt: *'[…]ik gok dat zo'n CISO[2] 175 euro per uur kost. Als je dan het belang niet zo inziet, ja waarom ga je die dan in hemelsnaam inhuren'.* Het budget van een organisatie speelt volgens hem een belangrijke rol bij de inzet van een interventie zoals het inhuren van een CISO. Molleman: '*Een budget speelt natuurlijk ook mee, de bedragen voor dat soort jongens zijn gewoon ontzettend hoog. En ja, dat gaat een gemiddelde detaillist niet doen. Als je een advocaat, als het moet, als die in de ellende zit, nou ja oké, ik kom daar niet onderuit. Maar ja, zoiets waar ze het belang niet van inzien, dat gaan ze natuurlijk nooit doen'.* Samenhangend met het niet inzien van het belang, is dat er volgens de experts geen besef is over de noodzaak van digitale weerbaarheid onder mkb'ers. Leisink vertelt bijvoorbeeld: *'maar met digitaal, de mogelijkheden zijn zo enorm gegroeid dus de noodzaak om informatie te managen die is gigantisch toegenomen. Maar dat besef is er niet gekomen. We zien niet in dat we informatie moeten managen'.* Eén van de redenen voor het ontbreken van dit besef onder managers is volgens Leisink te wijten aan het feit dat managers geen techneuten zijn. Managers en ondernemers nemen risico's om het bedrijf te laten groeien en om winst te maken. Ondernemers beseffen alleen niet dat digitale informatie veel risico's met zich mee brengt. Leisink: *'De mogelijkheden wat je er mee kan doen [informatie] zijn enorm gegroeid maar dus ook wat er mis kan gaan. Alleen is dat nu natuurlijk een ander domein, het digitale domein, en daar hebben managers heel simpelweg geen verstand van'*. Ook meent

[2] Een CISO is een Chief Information Security Officer.

een aantal experts dat mkb'ers ten onrechte denken geen aantrekkelijk doelwit te zijn; Van der Kleij: *'Hoezo? Loop ik risico dan? Helemaal niet. Ik ben klein, waarom zouden ze mij moeten hebben, laat maar zitten'.* Dat dit beeld niet klopt wordt geïllustreerd door Molleman. Hij vertelt: *'Er zijn weinig cybercriminelen die zeggen van nou weet je wat, ik ga bakker Piet in Monster ga ik even heel gericht targetten. Nee, dat gaat niet gebeuren. Er valt niks te halen, niet interessant. Maar als zo'n cybercrimineel zegt van weet je wat, ik gooi eens zo'n sleepnet uit en ik kijk welke gegevens van wie dan ook ik binnen kan harken. Daar zitten ondernemers in, burgers wie dan ook. Ja, daar kun je wel slachtoffer worden.* Lans en Van Leeuwen denken verder dat het bewustzijnsniveau in het mkb *'bedroevend laag'* is. Een mkb'er heeft volgens hen andere prioriteiten dan informatiebeveiliging. Ook zijn zij van mening dat mkb'ers bewust onbekwaam zijn. Hiermee wordt bedoeld dat ondernemers er bewust voor kiezen geen informatie in te winnen over digitale veiligheid (onbekwaam blijven) omdat zij dan niet hoeven te investeren en zodoende geld denken te besparen. Het niet hebben van tijd en geld wordt het meest benoemd door de ondervraagde experts. Ook wordt door de experts geschat dat veel mkb'ers geen prioriteit toekennen aan digitale weerbaarheid. Duin antwoord bijvoorbeeld op de vraag waarom mkb'ers weinig doen aan digitale weerbaarheid: *'Waarschijnlijk tijdgebrek, misschien geldgebrek, capaciteitsgebrek, geen mensen genoeg voor. De waan van de dag, wel de intentie hebben, wel het op hun to-do lijstje hebben staan maar er knalt iedere keer weer iets anders door'.*

Midden –en kleinbedrijf

De grootste obstakels die genoemd worden door respondenten uit het mkb zijn tijd, prioritering, kennisgebrek en bewustzijn. Groeneveld vertelt: *'Het is bij ons natuurlijk ook zo, we zijn met zijn zevenen dus we moeten ook die dagtaak met zijn zevenen oplossen. Er is voor ons niet de ruimte of tijd om in cybersecurity te stoppen'.* Er komt naar voren dat bepaalde mkb'ers gewoonweg geen tijd (of geld) hebben om te investeren in digitale weerbaarheid in vergelijking met grotere mkb'ers. Boom vertelt: *'Kijk, ik kan op een gegeven moment vrijgespeeld worden maar ik kan me ook goed voorstellen als je geen dedicated IT persoon hebt dat, dat toch wat lastiger is om daar heen [voorlichtingsbijeenkomst] te gaan'.* De personele capaciteit van de mkb onderneming lijkt bepalend voor de effectieve inzet van interventies.

Verder komt naar meermaals naar voren dat het aangehaalde punt van de experts op het gebied van het niet vormen van een aantrekkelijk doelwit, bevestigd wordt door de mkb'ers. Van Klaveren zegt bijvoorbeeld: *'Ik denk als gemiddelde mkb'er denk je altijd van*

goh, wat moeten ze van mij, gaat mijn deur voorbij […] Het is ons wel bekend dat iedere ondernemer in Nederland eigenlijk al wel een keer gehackt is. Alleen niet iedereen is zich daar van bewust, eigenlijk is niemand zich daarvan bewust. Iedereen denkt wel: goh, het gaat mijn deurtje wel voorbij'. Ook heerst het idee dat cybercriminelen eerst de grotere bedrijven zullen aanvallen omdat deze meer en belangrijke informatie hebben. Groeneveld vertelt bijvoorbeeld: *'Ik denk dat het voor Nutricia en dat soort grote spelers, ja die zullen daar wel veel gevoeliger voor zijn. Dat zijn ook ja, die hebben veel meer informatie en dingen te verbergen'.*

Wat opvalt is dat een aantal mkb'ers wel over voldoende bewustzijn lijken te beschikken. Claire Wanneé vertelt bijvoorbeeld dat MKB Nederland in samenwerking met het DTC gratis cybersecurity scans heeft aangeboden aan ondernemers. Deze scans werden niet veel afgenomen door mkb'ers. Wanneé: *'Voordat je het kan doen [scan laten uitvoeren] moet je best wel veel van jou vrijgeven aan privacy informatie. Daar lopen ze al tegen aan'.* Dit laat zien dat een aantal mkb'ers inzien dat het weggeven van informatie niet zonder risico's is. De geïnterviewde mkb'ers lijken dit besef niet te hebben en onderschatten de waarde van de informatie die ze hebben. Groeneveld: *'We hebben hier een bankrekeningnummer en een kopie van een paspoort, misschien een verblijfsvergunning. Ik snap dat dat allemaal privacy is en dat niemand het moet hebben maar aan de andere kant denk ik ja, ik zou niet eens weten als ik een kopie van een paspoort van iemand zou hebben, wat daar mee mis zou kunnen gaan'.* Meerdere mkb'ers denken dat informatie datgene is waar cybercriminelen op uit zijn en dat kleinere mkb-ondernemingen daarom niet interessant zijn. Ook dit is opvallend omdat het stil leggen van het bedrijf, door middel van ransomware, een doel kan zijn van cybercriminaliteit. Het gaat cybercriminelen dan niet om de informatie van een bedrijf maar dat het bedrijf een bedrag moet betalen om weer operationeel te worden. Kennisgebrek en te weinig bewustzijn kunnen hier verklarend voor zijn.

Een laatste opvallend obstakel dat wordt aangekaart door een tweetal respondenten is vertrouwen. Van Klaveren: *'[…]ik denk dat wat dat betreft het een goed initiatief [voorlichtingsbijeenkomsten] is dat de overheid daar aan meehelpt maar ook met partijen zoals wij want als de overheid vertelt dan is het niet altijd waar. Maar als wij het vertellen dan is het al iets meer waar en als je het in principe van collega's hoort en met elkaar dan wordt iedereen zich steeds bewuster ervan'.* Ook Wanneé is er van overtuigd dat vertrouwen bepalend is: *'[…] ik denk dat trust de allerbelangrijkste is. Vertrouwen in wat ze te horen krijgen en wie het zegt, wie is de afzender'.* Interventies zouden dus van vertrouwde partijen moeten komen. Dit kunnen overheidspartijen zijn maar ook private partijen.

Vergelijking

Beide partijen identificeren min of meer dezelfde obstakels die mogelijk een rol spelen bij het inzetten van interventies. Vooral het investeren van tijd, geld en (personele) capaciteit zijn veel genoemde factoren. Te weinig bewustzijn kan eveneens een reden zijn waarom interventies niet zullen slagen. Belangrijker is het feit dat experts tot op heden over weinig (wetenschappelijke) informatie beschikken over digitale weerbaarheid en manieren om dit te verhogen. Door dit kennisgebrek is het lastig om interventies te bedenken die mogelijk nuttig zijn. Daarnaast lijken mkb'ers zich te zien als onaantrekkelijke doelwitten en denken dat zij geen slachtoffer zullen worden. Van Klaveren: *'Ze hebben wel enig idee van de risico's van digitale dreigingen maar betrekken ze niet op zichzelf. Het gebeurt altijd een ander en nooit jezelf, tot het een keer jezelf gebeurt'.* Volgens experts klopt dit beeld niet omdat cybercriminelen sleepnetten uitzetten waarin ze zoveel mogelijk potentiele slachtoffers proberen te bereiken. Niet iedere aanval is gericht op een specifiek (mkb) bedrijf. Leisink: *'[…] en dan zie je ontwikkelingen, dat de ransomware is en blijft lucratief. Er zijn nog genoeg partijen die er in trappen en als er maar 1 blijft intrappen dus dan moet je 100 pc's besmetten en eentje die gaat daadwerkelijk betalen'.* Het idee van mkb'ers dat ze oninteressant zijn is daarom enigszins opvallend. Gebrek aan kennis kan hier verklarend in zijn.

4.2.2 Maatwerk en behoeften

Nu mogelijke obstakels in kaart zijn gebracht, is het zaak om te beschrijven welke interventies mogelijk zijn en waar ze op gericht moeten zijn.

Experts

Verschillende experts zijn van mening dat interventies uiteindelijk moeten bestaan uit maatwerk en gebaseerd moeten zijn op de behoeften van mkb'ers. Wanneé[3]: *'Wij hebben ook met bedrijven gesproken die zich ook echt richten op gedragsbeïnvloeding en die zeiden ook ja, je moet echt naar een mkb'er toe, je moet de behoeften gaan peilen'.* Het probleem is dat er onder experts nog geen duidelijk beeld bestaat van waar mkb'ers behoefte aan hebben. Op de vraag waar mkb'ers behoeften aan hebben zegt Duin: *'Nou dat weten wij ook niet genoeg. Dat weten we met zijn allen niet goed en daarom gaan we ook die enquêtes doen […] Ja, langzaam moet ook, zij moeten aangeven wat is jullie behoefte'.* Als de behoeften van mkb'ers eenmaal inzichtelijk zijn gemaakt dan is het volgens Duin van belang om aan die behoeften te voldoen en hier actief mee aan de slag te gaan: *'Op het moment dat er toch*

[3] Wanneé is hier als expert aangemerkt omdat ze hier praat vanuit de werkzaamheden van het DTC.

iemand is die net een dingetje, dat je denkt maar dat is een goeie, dan moeten we hem ook kunnen oppakken. Dan moeten we ook geld hebben om het vertrouwen, want het gaat ook allemaal over vertrouwen, dat als je de mkb'er bevraagt van wat lopen jullie nou te willen, dat als er dan ook maar één dingetje naar boven komt drijven waar we ze mee kunnen helpen, dat we dat ook kunnen realiseren. Dan bouwen we dat vertrouwen'. Inspelen op de behoeften van het mkb of een individuele mkb'er is dus van groot belang bij het formuleren en bedenken van interventies. Omdat deze behoeften sterk uiteen kunnen lopen zullen interventies volgens Van der Kleij maatwerk moeten worden: *'en dan nog is er waarschijnlijk niet een soort gouden kogel, golden bullet, soort cure dat voor al die bedrijven gaat werken maar dat zal echt maatwerk moeten zijn'*.

Anderzijds geeft Molleman aan dat iedere mkb'er basismaatregelen zou moeten nemen: *'De basics, gewoon de basics, de basis die iedereen op elke training geeft. Pas je wachtwoord aan, pas het eens in de zoveel tijd aan. Maak daadwerkelijk een backup van je systeem en test het ook af en toe of het werkt'*. Daarnaast is hij van mening dat er een groot verschil bestaat tussen mkb'ers. Hoog risico mkb ondernemingen moeten andere beveiligingsmaatregelen treffen dan laagrisico ondernemingen. Molleman: *'Ik denk dat in de basis iedereen wel hetzelfde moet doen. De bakker moet ook zijn wachtwoord aanpassen en niet overal dezelfde gebruiken. Die accountant moet misschien wel iets meer omdat hij privacy gevoelige gegevens heeft. Die zal zijn beveiliging iets meer moeten opschroeven'.* Hij is van mening dat iedere mkb'er een risicoschatting moet maken van de potentiele digitale risico's die hij of zij loopt, de beveiligingsmaatregelen moeten daar op gebaseerd worden. Ook Leisink vindt dat een inschatting van de risico's waardevol is in het bepalen van de maatregelen: *'Dit is voor ons cruciale informatie, dat is wat minder, hiervan is de beschikbaarheid heel belangrijk want onze productstraat heeft dat continu nodig […]. Als je goed zicht hebt op je informatie dan kan je ook gaan bepalen welke beveiliging daar voor nodig is'.* Ook hieruit blijkt dat maatregelen maatwerk zullen zijn. Algemene interventies zoals cyber awareness trainingen zijn volgens Van der Kleij weggegooid geld en hij benadrukt weer het belang van maatwerk: *'Ik denk dat maatwerk nodig is want het alternatief is dat je het niet doet en wat er nu gebeurt. Dus iedereen doet maar een cyber awareness training. Ik denk dat dat nog meer weggegooid geld is want dat werk slechts in een beperkt aantal gevallen voor een beperkt aantal situaties'.* Deze trainingen zijn volgens hem alleen nuttig voor bepaalde personen die daar gevoelig voor zijn en die weinig kennis hebben.

In de analyses is wel een aantal behoeften naar voren gekomen. Duin zegt bijvoorbeeld dat mkb'ers behoefte hebben aan wat ze moeten doen ingeval van een incident in

de vorm van handelingsperspectief. Dit perspectief wordt veelal gegeven in tekstuele adviezen, alleen zijn deze in abstracte en moeilijke taal geschreven. Duin: *'[…]dat je ze ontzorgt, dat ze niet verdwalen in allerlei tekst en dat het gewoon snel en duidelijk en eenvoudig te behappen is en dat er ook een soort handelingsperspectief wordt aangeboden. Van oké, wat moet ik nu doen. Oh, dit moet ik doen, vijf stappen moet ik ondernemen of ik moet die bellen of ik moet naar die website en daar staat het dan in twintig stappen hoe ik het eenvoudig moet doen'.* Daarnaast is het volgens Duin van belang dat de taal van het mkb gesproken wordt zodat adviezen gemakkelijk overgenomen kunnen worden door de doelgroep. Wat deze taal precies inhoudt is onduidelijk. Van der Kleij vertelt dat mkb'ers behoefte hebben aan hulp bij het uitbesteden van digitale weerbaarheid: *'Ze weten vaak niet wat ze nodig hebben, daar zou je ze wel mee kunnen helpen of met ze mee gaan, soort bemiddelende rol hebben tussen enerzijds de IT leveranciers die diensten bieden en anderzijds de mkb'ers'.* Volgens Duin kan certificering van producten en leveranciers hier uitkomst in bieden. De consumentenbond of tech websites kunnen bijvoorbeeld rapporten uitbrengen. Mkb'ers weten dan welke producten en leveranciers betrouwbaar zijn en nemen dan gefundeerde beslissingen. Daarnaast is een 'winkel' een mogelijkheid om producten en leveranciers te beoordelen. Duin: *'Nou wat de bedoeling van zo'n winkel is dat er producten en services kunnen worden aangeboden, dat bedrijven zeg maar samen ook die mogelijk kunnen ranken en dat er vanzelf op een gegeven moment de goede bedrijven en de goede diensten, services en producten boven komen drijven'.*

Midden –en kleinbedrijf

Ook de respondenten uit het mkb erkennen dat een duidelijk beeld van de behoeften ontbreekt. Van Stiphout vertelt: *We hebben vaak focussessies georganiseerd met ondernemers om ook eens de vraag aan hen te stellen van wat heb je nou nodig. Hoe kunnen we jullie nou helpen om je beter te beschermen tegen cybercrime. Heel veel ondernemers weten het zelf ook niet'.* Daarnaast blijkt uit de korte rondvraag onder tien mkb ondernemers die deel hadden genomen aan de voorlichtingsbijeenkomsten, dat zij ook niet weten waar ze behoefte aan hebben. Wel noemt een ondernemer dat er behoefte is om regelmatig over de problematiek te lezen en bijeenkomsten bij te blijven wonen. Volgens Van Stiphout is het bieden van handelingsperspectief wel één van de zaken waar ondernemers wel behoefte aan hebben: *'Wat we ook heel erg zien is dat het moet niet alleen maar blijven bij informatie, het moet ook handelingsperspectief zijn. Dus oké, nou, ik ben me bewust van het dat ik misschien*

slachtoffer ben, wat moet ik nu doen'. Dit handelingsperspectief mist volgens haar nog bij overheidsinformatie.

Impliciet vertelt Groeneveld over het belang van maatwerk. Hij kaart aan dat iedere mkb'er anders is en andere maatregelen zou moeten nemen: *'Wij zijn een uitzendbureau, dat heeft natuurlijk hele andere prioriteiten en kwetsbaarheden als een ijzerhandel'.* Ook hieruit blijkt dat maatwerk een belangrijke factor is bij het ontwikkelen van interventies. Van Stiphout illustreert het door Groeneveld genoemde verschil: *'Daar zie je ook wel wat echt werkt en sectorspecifieke voorbeelden. Dus een horecagelegenheid die een Wi-Fi wachtwoord openbaar heeft, wat voor risico's levert dat op, ook voor je klanten. Dus wat betekent dat voor je gastvrijheid. Zo'n voorbeeld doet het heel goed voor horecaondernemers maar dat doe het helemaal niet bij de bouw of installatiebranche.* Het aanbieden van sectorspecifieke informatie is iets waar mkb'ers behoefte aan lijken te hebben. Janssen vertelt: *'Op het moment dat het voor mij van belang is, dat het gaat om dingen die spelen in mijn bedrijf vind ik dat vanuit de Kamer van Koophandel inderdaad zou kunnen komen. Want je bent ingeschreven onder een bepaald segment. Die weet precies wat voor jou van toepassing is. Dus, zonder dat zij hun gegevens bloot geven aan anderen kunnen zij die informatie gewoon verstrekken'.* Het is mogelijk dat een Kamer van Koophandel sectorspecifieke informatie opstuurt waardoor er een vorm van maatwerk ontstaat. Boom vertelt eveneens over het belang van sectorspecifieke informatie. Hij heeft bijeenkomsten van FERM[4] bijgewoond en zegt: *'je hebt als bedrijf natuurlijk zelf ook wel het een en ander lopen maar het is wel goed om te zien van dit is wat er nou specifiek aan de hand is in de haven'.* Ook is hij van mening dat het delen van informatie over incidenten met soortgelijke bedrijven waardevol is: *'Als er een incident is bij een soortgelijk bedrijf en je ziet dat er een incident ergens is, ja deel die informatie met dat type bedrijf en vertel ze van joh let op, het gebeurt wel degelijk in jouw sector'.* Ook lijkt er behoefte te zijn aan hulp bij het kiezen van ICT leveranciers en producten wanneer een mkb'er besluit zijn digitale weerbaarheid en cybersecurity uit te besteden. Voor veel mkb'ers is het echter lastig om te bepalen welke leverancier of welk product betrouwbaar is. Zo vertelt Janssen: *'[...] welke is dan wel veilig, welke is dan niet veilig, want iedereen zegt dat zijn systeem veilig is, iedereen zegt dat zijn programma veilig is maar waar is dat onafhankelijke bureau dat zegt nou dat programma en dat ding'.*

[4] FERM is een publiek-privaat samenwerkingsverband gericht op cyber resilience in de Rotterdamse haven

Vergelijking

Bij beide groepen komt naar voren dat er nog te weinig informatie en kennis beschikbaar is over de behoeften van mkb'ers. Volgens experts is het in kaart brengen van deze behoeften van groot belang omdat interventies gebaseerd moeten zijn op deze behoeften. Naast handelingsperspectief, sectorspecifieke informatie en hulp weten mkb'ers niet waar ze behoefte aan hebben op het gebied van digitale weerbaarheid. Omdat mkb'ers niet weten waar ze behoefte aan hebben, is het voor experts lastig om geschikte interventies te formuleren. Experts lijken gemotiveerd om het mkb te helpen maar het mkb lijkt niet gemotiveerd om duidelijk te maken waar ze behoefte aan hebben. Dit kan liggen aan de genoemde obstakels (tijd, prioritering, capaciteit etc.) in de vorige paragraaf.

4.2.3 Voorlichting

Voorlichting is bij uitstek de interventie die het meest genoemd is door zowel experts als mkb'ers als manier om digitale weerbaarheid te verhogen. Daarom wordt deze specifieke interventie uitgelicht.

Experts

Het 'ouderwets' voorlichten van bedrijfseigenaren en medewerkers wordt gezien als een manier om het bewustzijn en de kennis over digitale weerbaarheid te vergroten. Wanneer dit bewustzijn vergroot wordt dan zal een hoger niveau van digitale weerbaarheid bereikt worden. Wel stellen de experts dat voorlichting aan een aantal randvoorwaarden moet voldoen. Het is van groot belang dat voorlichting aangepast wordt op de doelgroep en de deelnemers van de voorlichtingsbijeenkomst. Als er bijvoorbeeld veel managers deelnemen aan de voorlichting dan is het volgens Leisink van belang om de voorlichting aan te passen op deze groep. Dit kan gezien worden als een concrete vorm van maatwerk zoals beschreven in de vorige paragraaf. Leisink: *'Want zij kunnen niks met het verhaal van, stel een firewall in en installeer antivirus want dat doen zij niet, daar zijn zij niet voor. Maar zij zijn wel voor de organisatie organiseren dus je moet directieleden aanspreken op het niveau van dat deel van de informatie beveiliging, alleen dat deel waar zij wat mee kunnen'.* Ook Molleman is van mening dat doelgroepgerichte voorlichtingen beter werken dan algemene voorlichtingsbijeenkomsten. Het mkb is volgens hem een erg brede doelgroep met uiteenlopende risicoprofielen. Een bakker loopt bijvoorbeeld andere risico's dan een advocatenkantoor zoals in de vorige paragraaf naar voren kwam. Op basis van deze risicoprofielen moeten voorlichtingen ontwikkeld worden. Het is volgens hem ook aan te

raden om voorlichting te geven op momenten dat bepaalde sectoren van het mkb bij elkaar samenkomen. Molleman: *'Misschien moet je bij die laag risico aansluiten bij een al bestaande bijeenkomst. Detailhandel, die is vaak georganiseerd in een ondernemingsvereniging, die komen één keer per maand misschien samen om de lokale problematiek te bespreken. Misschien moet je daar een keertje aanhaken, dan zijn ze al bij elkaar'.* Als een voorlichting tijdens deze bijeenkomsten gegeven kan worden dan kan de voorlichting direct toegepast worden op het risicoprofiel van deze specifieke mkb sector.

Duin is eveneens van mening dat voorlichtingsbijeenkomsten nuttig zijn maar geeft wel een aantal randvoorwaarden. Hij vertelt bijvoorbeeld: *'Natuurlijk proberen we in de sessies of de conferenties, proberen we juist ook mensen in de zaal uit te nodigen tot interactie. Ik denk wel dat je moet proberen het meer actief te maken. Dus meer interactie'.* De voorlichting mag niet alleen bestaan uit het zenden van informatie. Ook denkt hij dat deelnemers van de voorlichting de informatie die zij hebben meegekregen met collega ondernemers zullen delen. Duin: *'[…] dat er toch weer iemand van een bedrijf naar zo'n sessie is geweest die tegen zijn buurman zegt; het was eigenlijk wel heel interessant. Dan zegt die man misschien wel oh ja, shit, ik heb het wel eens gezien maar ik ben er nog niet naar toe gegaan'.* Verder benadrukt hij dat organisatoren van voorlichtingen niet te veel moeten kijken naar het aantal deelnemers: *'[…] en kan het zo zijn dat het kwalitatief gewoon heel erg goed is geweest, ook al waren er maar tien mensen, ook een sessie van 50 man kan kwalitatief goed zijn'.* Het idee is dat iedere deelnemer die is voorgelicht en meer bewust is, er één is.

Ook kunnen oefeningen gekoppeld worden aan voorlichting. Phisingoefeningen[5] kunnen bijvoorbeeld worden ingezet om werknemers bewuster te maken van de gevaren van dit soort criminaliteit. Het probleem van deze oefeningen is volgens Van der Kleij dat deze nauwelijks langdurig werken. Hij vertelt: *'Je ziet wel een heel kort durend effect, dat minder mensen dan klikken. Maar je ziet dat het effect, er is een effect, het wordt minder maar het wordt iets minder maar niet nul zullen we maar zeggen. En je ziet dat het effect van korte duur is, dus na verloop van tijd zie je dat het effect weer wegebt en dat mensen weer gewoon net zo vaak op die links klikken als voorheen.* Men zou dit soort oefeningen dan periodiek moeten herhalen om het bewustzijnsniveau hoog te houden. Ook geeft hij aan dat het uitvoeren van phisingoefeningen een onbedoeld negatief kortdurend neveneffect met zich mee brengt. Medewerkers worden te achterdochtig en klikken ook niet meer op goede links.

[5] Een bedrijf ondergaat vrijwillig een phisingaanval waarbij wordt gekeken hoe vaak werknemers gegevens verstrekken. Daarna worden de resultaten teruggekoppeld. De bedoeling is om het bewustzijn te vergroten.

Midden –en kleinbedrijf

Ook het mkb vindt dat voorlichting een nuttige interventie is om de digitale weerbaarheid van een onderneming naar een hoger niveau te tillen. Wel geeft Van Stiphout aan dat landelijke voorlichtings of bewustwordingscampagnes niet altijd veel impact kennen terwijl dit wel nodig is. *'Dan maak je zo'n hele grote bewustwordingscampagne, wat we nu via branches doen. Je bereik is veel groter maar je impact is niet per definitie groter en dat is wel iets wat je ziet bij het organiseren van lokale bijeenkomsten via onze regio's of andere ondernemingsverenigingen. Dat werkt soms het wel het best, dan heb je lokale ondernemers aan tafel'.* Ook vertelt ze dat het DTC bezig is met het opzetten van een helpdesk als vorm van informatievoorziening. Slachtoffers kunnen in de toekomst contact opnemen en vragen wat ze het beste kunnen doen. Dit kan gezien worden als een vorm van voorlichting. Groeneveld zegt dat het bewustzijn van een bedrijf ook verhoogd kan worden als een partij persoonlijk langsgaat en vertelt over cybercrime, digitale weerbaarheid en verwante onderwerpen. Groeneveld: *'Omdat jij nu ook gewoon langs bent geweest dan wordt gewoon je aandacht er op gevestigd'.* Van Klaveren is ook van mening dat voorlichtingen nodig zijn. *'Misschien is het wel een druppel op een gloeiende plaat maar als je ook niet druppelt dan gebeurt er helemaal niks. Dus uiteindelijk zal je het wel moeten doen, je moet het blijven herhalen he, de kracht van de boodschap zit toch in herhaling.* Het herhalen van de boodschap vanuit diverse kanten is nodig. Dit kunnen volgens hem overheidspartijen zijn maar ook private partijen. Janssen is echter minder positief over voorlichtingsbijeenkomsten. Ze vertelt: *'Bijeenkomsten, over het algemeen worden die niet bezocht want mensen hebben meer te doen dan alle bijeenkomsten af te gaan'* en *'over het algemeen zijn dat presentaties en wordt er alleen maar gepraat en verteld en wordt eigenlijk niet interactief gewerkt'*. Ook worden bijeenkomsten vaak te laat en op het laatste moment aangekondigd. Een agenda van een mkb'er staat vaak al snel vol waardoor voorlichtingsbijeenkomsten weinig bezocht worden. Zij heeft liever dat ze een presentatie, bijvoorbeeld in de vorm van e-learning, in haar eigen tijd kan bekijken en op die manier voorgelicht wordt. Oefeningen zoals phisingoefening zouden volgens haar ook effectief zijn. Het schrikeffect kan juist aanleiding geven om te investeren in digitale weerbaarheid. Boom heeft bij het bedrijf waar hij werkt een phisingoefening laten uitvoeren en de resultaten in de vorm van een security awareness training terug laten koppelen naar de werknemers. Hij merkt op: *In het begin is iedereen heel alert en dan krijg je bij wijze van spreken tien mailtjes per dag. […] Je merkt gewoon dat dat een beetje inzakt'.* Verder geeft hij aan dat voorlichting niet grootschalig hoeft te zijn. Mkb-ondernemingen met werknemers die verantwoordelijk zijn voor ICT kunnen werknemers

continu informeren over digitale veiligheid. Boom: *'Kijk, wij blijven wel constant mailtjes sturen naar iedereen van let op, let op waar je op klikt'.* Bij ondernemingen zonder vaste IT werknemers is dit lastiger. Bedrijven kunnen zich wel inschrijven voor nieuwsbrieven als een vorm van voorlichting maar hier kleven een aantal nadelen aan volgens Groeneveld: *'Je zou kunnen zeggen, die brancheorganisaties mails laten sturen maar als ik die binnenkrijg dan druk ik ook gewoon, selecteer ik en delete ik, dus dat is ook lastig'*. Nieuwsbrieven worden over het algemeen slecht gelezen.

Vergelijking

Ook hier zijn beide groepen in overeenstemming met het idee dat voorlichting nuttig is. De experts vinden dat voorlichtingsbijeenkomsten aangepast moeten worden op de doelgroep en op het risicoprofiel van de deelnemers. Zowel expert als mkb'er zijn het er over eens dat interactiviteit nodig is om een waardevolle voorlichtingsbijeenkomst te creëren. Daarnaast menen zowel Molleman als Van Stiphout dat het organiseren van lokale bijeenkomsten de impact van de bijeenkomst kan vergroten. Een belangrijk punt is dat mkb'ers het vaak druk hebben en niet altijd tijd hebben voor een voorlichtingsbijeenkomst.

5. Conclusie en discussie

5.1 Conclusie

Digitale weerbaarheid maakt onderdeel uit van cybersecurity maar verschilt op een belangrijk punt. Cybersecurity veronderstelt dat volledige bescherming tegen incidenten bestaat. Digitale weerbaarheid doet dit niet en treedt, onder andere in werking, gedurende of na een incident. Omdat er tot nu toe weinig wetenschappelijke aandacht is uitgegaan naar het onderwerp is in deze scriptie onderzoek gedaan naar twee aspecten van digitale weerbaarheid. Ten eerste is gekeken naar het begrip en de achterliggende concepten. Ten tweede is onderzocht welke interventies mogelijk geschikt zijn om digitale weerbaarheid binnen het mkb te versterken. De volgende onderzoeksvraag stond centraal: '*Welke aspecten spelen een rol bij digitale weerbaarheid volgens cybersecurityexperts en mkb-ondernemers?*

Digitale weerbaarheid is een breed begrip en als het argument van Van der Meulen (2015) gevolgd wordt is het definiëren van brede begrippen van belang voor het verzamelen van kennis en het vormen van toekomstig beleid. In tegenstelling tot het standpunt van Coaffee & Fussey (2015) is een definitie dus vanuit wetenschappelijk en beleidsmatig oogpunt van wezenlijk belang. Voor mkb'ers is een definitie waarschijnlijk minder belangrijk. Zij zijn vooral gericht op wat digitale weerbaarheid doet en hoe het werkt omdat ze praten over concrete maatregelen. Dit is niet erg want het mkb kan geholpen worden door de juiste maatregelen (op basis van kennis en beleid) aan te bieden zonder dat zij hoeven te weten wat digitale weerbaarheid precies inhoudt. Ondanks deze verschillende zienswijzen kunnen 'offline' definities en achterliggende concepten van weerbaarheid toegepast worden op de digitale variant. De belangrijkste concepten die digitale weerbaarheid als begrip 'maken' zijn de vier vermogens waar een bedrijf over zou moeten beschikken. Het vermogen om dreigingen te anticiperen, te detecteren, hier op te reageren en hiervan te leren. Als de door de respondenten genoemde vermogens en achterliggende concepten afgezet worden tegen de bestaande literatuur over weerbaarheid, dan valt op dat deze allen terug te vinden zijn in de denkbeelden van verschillende auteurs (Weller & Anderson, 2013; Cavelty, Kaufmann & Kristensen, 2015; Helm, 2015). Andere achterliggende concepten zijn dat incidenten niet te voorkomen zijn en dat herstel en veerkracht een grote rol van betekenis spelen. Ook deze punten zijn terug te vinden in de 'offline' weerbaarheidsliteratuur (Cavelty Kaufmann & Kristensen, 2015; Helm, 2015; Coaffee & Fussey, 2015; Bourbeau, 2013; Rothrock, 2017; De Crespigny, 2012). Rothrock (2017) veronderstelt dat weerbaarheid een verzamelnaam is van verschillende maatregelen die gebruikt worden om cybersecurity en digitale veiligheid te

verhogen. Uit de resultaten is gebleken dat vooral de mkb'ers digitale weerbaarheid relateren aan verschillende typen maatregelen waarbij de preventieve, herstellende en beschermende maatregelen de boventoon voeren. Een ander verschil is dat experts digitale weerbaarheid meer typeren als *socio-ecological resilience* omdat zij de lerende component sterk benadrukken. Mkb'ers doen dit in mindere mate en zien digitale weerbaarheid dus voornamelijk als *ecological resilience* (Bourbeau, 2013). Een antwoord op de deelvraag *'Wat is digitale weerbaarheid volgens cybersecurity experts en mkb'ers?'* is, na vergelijking tussen beide partijen dan ook: Digitale weerbaarheid is het idee dat digitale incidenten niet te voorkomen zijn en dat bedrijven verschillende soorten maatregelen inzetten om te kunnen reageren op deze incidenten, (snel) terug te kunnen keren naar de normale bedrijfsvoering en het vermogen moeten hebben om incidenten te anticiperen, te detecteren en hiervan te leren zodat toekomstige incidenten beter afgehandeld kunnen worden.

De tweede deelvraag: *'Hoe kan digitale weerbaarheid volgens cybersecurity experts en mkb'ers verhoogd worden?'* kan slechts deels beantwoord worden. Om tot goede interventies te komen moet er volgens experts kennis beschikbaar zijn en moet er een duidelijk behoeftebeeld zijn waar de interventies op moeten inspelen. Kennis over digitale weerbaarheid wordt nog verzameld en er bestaat geen duidelijk behoeftebeeld. De mkb'er weet niet waar hij of zij behoefte aan heeft. Daarnaast zien mkb'ers het belang beperkt in van digitale weerbaarheid omdat zij zichzelf niet als aantrekkelijk doelwit zien. Verder speelt de (beperkte) financiële capaciteit een rol bij de keuze om niet te investeren in digitale weerbaarheid. Deze factoren worden ook benoemd in de literatuur (bijv. Taliweh e.a., 2007; Kshteri & Murugesan, 2013; Rowe & Gallagher, 2006) en vormen obstakels bij het implementeren van interventies. Kijkend vanuit het COM-B model (Michie, Van Stralen & West, 2011) lijken mkb'ers dus niet gemotiveerd te zijn om aan de slag te gaan met digitale weerbaarheid. Daarnaast is er meermaals naar voren gekomen dat er een duidelijk kennisgebrek aanwezig is onder de mkb'ers en dat zij zich niet voldoende bewust zijn van het belang van digitale weerbaarheid (bekwaamheid). Verder lijkt het er op dat zij zelf niet in staat zijn om de digitale weerbaarheid van de eigen organisatie tot een hoger niveau te tillen. Dit hoeft echter geen obstakel te vormen omdat het vaak wordt uitbesteed. Het idee van mkb'ers is dat ICT leveranciers wel voldoende bekwaam zijn. Op het gebied van geboden kans moet geconcludeerd worden dat deze voldoende worden aangeboden door verschillende partijen. Gedacht kan worden aan gratis voorlichtingsbijeenkomsten en cybersecurity scans. Mkb'ers maken echter weinig gebruik van deze kansen. Waarschijnlijk komt dit door de hierboven genoemde obstakels. De toegevoegde waarde van het toepassen van dit model ligt

in het feit dat nu duidelijk is dat mkb'ers niet gemotiveerd zijn. Er moeten manieren gevonden worden om mkb'ers te motiveren digitale weerbaarheid prioriteit te geven en hier mee aan de slag te gaan. Niet iedere mkb'er kan een externe partij inhuren en zal dus zelf actie moeten ondernemen.

Ondanks dat mkb'ers geen expliciet behoeftebeeld hebben, kunnen wel een aantal impliciete behoeften onderscheiden worden. Op basis van de resultaten is vast te stellen dat mkb'ers hulp willen bij het kiezen van ICT leveranciers en producten. Certificering of de genoemde 'winkel' kunnen deze hulp bieden. Daarnaast hechten mkb'ers waarde aan sectorspecifieke informatie. Algemene informatie op het gebied van cyber security en digitale weerbaarheid is niet altijd relevant voor bepaalde sectoren. Het mkb kent veel verschillende segmenten en informatie zou per segment aangeboden moeten worden. Op deze manier is het ook mogelijk om sectorspecifiek te informeren over cyber incidenten. Incidenten kunnen een aanleiding zijn om te investeren in digitale weerbaarheid en het is daarom van belang dat er aandacht besteed wordt aan incidenten die plaatsvinden. Benadrukt moet worden dat mkb'ers open moeten en durven zijn over digitaal slachtofferschap zodat zijzelf en collega's hier van kunnen leren. Interventies kunnen op basis van dit kleine behoeftebeeld geformuleerd worden. De manier waarop deze interventies uitgevoerd moeten worden is lastig te zeggen. Het onder de aandacht brengen van certificering, het bieden van hulp bij het kiezen van ICT leveranciers en het aanbieden van sectorspecifieke informatie kan via seminars, presentaties of conventionele manieren zoals nieuwsbrieven (Abawajy, 2014). Theoretisch gezien werken educatieve presentaties goed, terwijl de effectiviteit van nieuwsbrieven laag is (Khan, Alghathbar & Khari, 2011). Presentaties in de vorm van voorlichtingsbijeenkomsten verdienen dus de voorkeur maar een combinatie van verschillende methoden blijft aanbevelingswaardig (Abawajy, 2014). Deze interventies spelen vooral in op de bekwaamheid van het mkb doordat kennis vergroot wordt en bewustzijn groeit. Het uitlichten van incidenten kan mkb'ers motiveren om digitale weerbaarheid prioriteit te geven.

5.2 Discussie

De resultaten uit dit onderzoek leveren een bescheiden bijdrage aan de (groeiende) kennis over digitale weerbaarheid en de manieren waarop het mkb zich digitaal weerbaarder kan maken. Een wetenschappelijke toevoeging van dit onderzoek is dat duidelijk is geworden dat de theoretische concepten uit de 'offline' weerbaarheidsliteratuur ook van toepassing zijn op de digitale variant. Opgemerkt moet worden dat er geen nieuwe wetenschappelijke inzichten

zijn vergaard op het gebied van een definitie van digitale weerbaarheid. De geformuleerde definitie en diens achterliggende concepten komen terug in al bestaande definities. Vanuit beleidsmatig oogpunt bezien kan de definitie wel gebruikt worden om het vormen van beleid over digitale weerbaarheid te vergemakkelijken. De definitie biedt voldoende aanknopingspunten waar beleid zich op zou kunnen richten. Zo zou beleid zich kunnen richten op het versterken van één van de vier vermogens of maatregelen formuleren die mkb'ers kunnen overnemen om de eigen organisatie digitaal weerbaarder te maken.

Daarnaast is duidelijk geworden dat de inbreng van mkb'ers om goede interventies te ontwikkelen van groot belang is. Het lijkt er op dat zij niet gemotiveerd zijn om deze inbreng te leveren. Hierdoor wordt het voor experts moeilijk om geschikte interventies te ontwikkelen. Mkb'ers hebben experts nodig om digitaal weerbaarder te worden maar experts hebben mkb'ers ook nodig. Voor toekomstig onderzoek is het interessant om het behoeftebeeld van het mkb duidelijk in beeld te brengen zodat interventies ontwikkeld kunnen worden. Met dit onderzoek is duidelijk geworden dat mkb'erswel impliciete behoeften hebben. Misschien ligt de oplossing voor het schetsen van dit behoeftebeeld in het afnemen van meerdere kwalitatieve interviews. Het recht op de man afvragen via enquêtes waarbij de mkb'er snel moet nadenken over zijn of haar behoeften werkt misschien beperkend. Een nadeel van meerdere kwalitatieve interviews is dat het erg tijdrovend is, zowel voor de onderzoeker als de mkb'er. Daarnaast vormt het geconstateerde motivatiegebrek een groot obstakel. Wellicht dat het uitlichten van incidenten hier een rol van betekenis kan spelen. Verder heeft Van der Kleij aangegeven dat het lectoraat Cybersecurity van de Haagse Hogeschool bezig is met het in kaart brengen van het behoeftebeeld. Daarnaast zijn andere partijen (DTC, FERM) eveneens informatie aan het verzamelen om dit behoeftebeeld duidelijk te krijgen. Het zou nuttig zijn als deze informatie gedeeld en bijeengebracht wordt zodat er een alomvattend beeld ontstaat. Het mkb kan hier alleen maar van profiteren.

Dit onderzoek kan ook aanknopingspunten bieden voor toekomstig beleid. Via publiek-private samenwerkingsverbanden kan ingespeeld worden op het kort geschetste behoeftebeeld. Daarnaast is het van belang om te benadrukken dat iedere mkb'er basismaatregelen moet treffen. Op basis van een risico-analyse moeten mkb'ers zelf beslissen om verdere maatregelen te nemen. Misschien is het mogelijk dat deze analyses via subsidieregelingen, dan wel vanuit de overheid of vanuit brancheverenigingen, aangeboden worden.

Afsluitend is het van belang om kritisch te kijken naar een aantal onderdelen van deze scriptie. Op het gebied van de betrouwbaarheid van de interviews moet gezegd worden dat de

topiclijst gedurende het onderzoeksproces uitgebreid is. Dit was de opzet van het onderzoek maar het heeft er ook toe geleid dat niet aan alle respondenten dezelfde vragen zijn gesteld. Dit vormt echter geen obstakel omdat het ging om een toevoeging van een klein aantal vragen en *probes*. Wel moet erkend worden dat er soms sturende vragen gesteld zijn tijdens de interviews. Wellicht dat dit ook ligt aan onervarenheid maar dit neemt niet weg dat hier in de toekomst extra op gelet moet worden. Dit leidde er echter toe dat de respondent misschien niet het antwoord wilde geven wat hij of zij in gedachten had, maar de gedachtegang van de onderzoeker overnam en het antwoord daar op baseerde. In hoeverre de resultaten hierdoor beïnvloed zijn is ook lastig te zeggen omdat er geen vergelijking mogelijk is met resultaten waarbij geen sturende vragen gesteld zijn. Wel kan er als voorbeeld gekeken worden naar de obstakels. Bij het stellen van de vraag werden al een aantal obstakels genoemd als *probes*. Deze *probes* werden echter overgenomen door de respondent en hij of zij vertelde hier over. Mogelijk zijn er dus andere obstakels van invloed die nu niet naar voren zijn gekomen. Ook moet genoemd worden dat gestart is met interviewen voordat volledig duidelijk was wat nu precies onderzocht ging worden. Uiteindelijk waren de resultaten van de eerdere interviews bruikbaar omdat een brede topiclijst was opgesteld waardoor er veel informatie verzameld kon worden. Voor soortgelijk toekomstig onderzoek is het belangrijk om van te voren duidelijk te hebben wat onderzocht wordt zodat de topiclijst gestructureerd en gericht opgesteld kan worden. Verder is gebleken dat het moeilijk was om mkb'ers te vinden die mee wilde werken aan dit onderzoek. Misschien dat dit komt omdat het onderwerp afschrikt en zij het idee hebben geen waardevolle informatie te kunnen geven omdat ze geen verstand (denken te) hebben van het onderwerp. Ook is het mogelijk dat het gaat om een drukbezette groep die gewoonweg geen tijd of zin heeft om mee te werken aan onderzoeken. Mkb brancheverenigingen waren weer wel bereid om mee te werken. Zij kunnen wel vanuit de mkb'er praten maar de echte betekenisgeving van de mkb'er komt dan niet volledig tot uiting. Voor toekomstig onderzoek zouden meerdere mkb'ers geïnterviewd moeten worden.

Al met al is er nog genoeg (wetenschappelijk) onderzoek te doen naar digitale weerbaarheid binnen het mkb. Vooral het in kaart brengen van het behoeftebeeld zodat geschikte interventies geformuleerd kunnen worden is een grote uitdaging en deze moet zeker worden aangegaan. Daarbij komt dat het mkb steeds vaker slachtoffer wordt van cybercrime en dat de kosten gemiddeld genomen één miljard euro bedragen voor deze sector. Digitale weerbaarheid moet en kan er voor zorgen dat dit bedrag niet oploopt. Het is daarom van belang dat er voldoende (wetenschappelijke) aandacht blijft uitgaan naar het onderwerp.

6. Literatuurlijst

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237-248.

Akerboom, E. (2012). Cyber security. Samenwerken voor een veilige en vitale cybersamenleving. *Militaire Spectator, 181*(12), 532-536.

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing Cybersecurity As A Public Good: The Role Of Governments, Business, And Individuals. *Journal of Legal, Ethical and Regulatory Issues, 1*(16), 7-14.

Beyens, K., & Tournel, H. (2010). Mijnwerkers of ontdekkingsreizigers? Het kwalitatieve interview. In T. Decorte, & D. Zaitch, *Kwalitatieve Methoden en Technieken in de Criminologie* (pp. 200-230). Leuven: Acco.

Boeschoten, T., & Rosman, C. (2018, 30 maart). *Verander nu je wachtwoord: 3,3 miljoen Nederlandse wachtwoorden eenvoudig te vinden*. Retrieved 07 mei, 2018, from Algemeen Dagblad: https://www.ad.nl/binnenland/verander-nu-je-wachtwoord-3-3-miljoen-nederlandse-wachtwoorden-eenvoudig-te-vinden~aef1faf3/

Bourbeau, P. (2013). Resiliencism: premises and promises in securitisation research. *Resilience, 1*(1), 3-17.

Brand-Gruwel, S., Wopereis, I., & Vermetten, Y. (2005). Information problem solving by experts and novices: Analysis of a complex cognitive skill. *Computers in Human Behaviour*(21), 487-508.

Cacioppo, J. T., & Freberg, L. A. (2013). *Discovering Psychology. The Science of Mind.* Belmont, Californië, Verenigde Staten: Wadsworth.

Cavelty, M. D., Kaufmann, M., & Kristensen, K. S. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue, 46*(1), 3-14.

CBS. (2017a). *Cybersecuritymonitor 2017.* Den Haag: CBS.

CBS. (2017b, 25 september). *Een op vijf bedrijven slachtoffer van cyberaanval*. Retrieved 14 juli, 2018, from Centraal Bureau voor de Statistiek: https://www.cbs.nl/nl-nl/nieuws/2017/39/een-op-vijf-bedrijven-slachtoffer-van-cyberaanval

Choi, M. S., Levy, Y., & Hovav, A. (2013). The Role of User Computer SElf-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. *Proceedings of the Eight Pre-ICIS Workshop on Information Security and Privacy*, (pp. 1-19). Milaan, Italië.

Coaffee, J., & Fussey, P. (2015). Constructing resilience through security and surveillance: The politics, practices and tensions of security-driven resilience. *Security Dialogue, 46*(1), 86-105.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A videogame for cyber security training and awareness. *Computers & Security*(26), 63-72.

de Crespigny, M. (2012). Building cyber-resilience to tackle threats. *Network Security*, 5-8.

Deloitte. (2016). *Cyber Valute at Risk in the Netherlands.* Deloitte.

Deloitte. (2017, 25 09). *Cybercriminaliteit kost Nederlands MKB jaarlijks een miljard*. Retrieved 26 april, 2018, from Deloitte: https://www2.deloitte.com/nl/nl/pages/about-deloitte/articles/cybercriminaliteit-kost-nederlands-mkb-jaarlijks-een-miljard.html

European Comission. (2017). *SBA Fact Sheet Netherlands.* Retrieved 02 februari, 2018, from European Comission: https://ec.europa.eu/docsroom/documents/26562

Fiske, S. T., Kinder, D. R., & Michael-Larter, W. (1983). The Novice and the Expert: Knowledge-Based Strategies in Political Cognition. *Journal of Experimental Psychology*(19), 381-400.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity, 1*(1), 3-17.

Harris, M. A., & Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114.

Helm, P. (2015). Risk and resilience: strategies for security. *Civil Engineering and Environmental Systems, 32*(1), 100-118.

Hennink, M., Hutter, I., & Bailey, A. (2011). *Qualitative Research Methods.* Los Angeles, Verenigde Staten: SAGE.

Hinds, P. J., & Pfeffer, J. (2002). Bothered by Abstraction: The Effect of Expertise on Knowledge Transfer and Subsequent Novice Perfromance. *Journal of Applied Psychology*(86), 1232-1243.

Hmelo-Silver, C. E., & Green-Pfeffer, M. (2004). Comparing expert and novice understanding of a complex system from the perspective of structures, behaviours and functions. *Cognitive Science*(28), 127-138.

Isaacs, E. A., & Clark, H. H. (1987). References in Conversation Between Experts and Novices. *Journal of Experimental Psychology, 6*(11), 26-37.

Kamp, H. G. (2017). *Oprichting van een Digital Trust Centre [Kamerbrief]*. Opgeroepen op 22 februari, 2018, van Rijksoverheid:

https://www.rijksoverheid.nl/documenten/kamerstukken/2017/09/23/kamerbrief-oprichting-van-een-digital-trust-centre

Kaur, J., & Mustafa, N. (2013). Examing the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME. *3rd International Conference on Research and Innovation in Information Systems (ICRIIS '13)*, (pp. 286-290). Maleisië.

Khan, B., Alghathbar, K., & Khari, K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management, 5*(26), 10862-10868.

Kokkeler, B. (2017). *Smart Public Safety. Leidersschap voor nieuwe verbindingen in de digi-sociale wereld.* Breda: Avans Hogeschool.

Kshetri, N., & Murugesan, S. (2013). EU and US Cybersecurity Strategies and Their Impact on Business and Consumers. *Computer*, 84-88.

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*(3), 5-7.

Leukfeldt, E. R. (2017). *Research Agenda: The Human Factor in Cybercrime And Cybersecurity.* Den Haag: Eleven International Publishing.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Emperical Analysis. *Deviant Behaviour, 37*(3), 263-280.

Lodder, A. R., & Toet, J. (2013). Cybersecurity: Europese Unie initiatieven voor een intrinsiek grensoverschrijdend fenomeen. *Tijdschrift voor Internetrecht, 5*(6), 135-140.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce, 9*(1), 23-41.

Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science, 6*(42), 1-11.

Ministerie van Economische Zaken en Klimaat. (2018, 16 maart). *Digital Trust Centre: Factsheet.* Retrieved 07 mei, 2018, from VNO-NCW: https://www.vno-ncw.nl/meer-informatie/factsheet-digital-trust-centre-dtc

NCTV. (2017a). *Cybersecuritybeeld Nederland 2017.* Den Haag: NCTV.

Notté, R., & Slot, L. (2016). *Cybersecurity in het mkb.* Retrieved 26 april, 2018, from De Haagse Hogeschool: https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management, 8*(3), 238-264.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121-135.

Rothrock, R. A. (2017). Digital Network Resilience: Surprising Lessons from the Maginot Line. *The Cyber Defense Review, 2*(3), 33-40.

Rowe, B. R., & Gallagher, M. P. (2006). Private Sector Cyber Security Investment Strategies: An Emperical Analysis. *Conference: Workshop on the Economics of Information Security (WEIS),* (pp. 1-23).

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52,* 92-100.

Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing information security in small and medium sized enterprises: A holistic approach. In Pohlmann, Reimer, & Schneider, *ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference* (pp. 331-339). Wiesbaden, Duitsland: Vieweg, Teubner Verlag.

Van der Kleij, R. (2018). Digitale weerbaarheid in het mkb: een serieus probleem? *Tijdschrift voor Human Factors, 43*(1), 19-32.

Van der Meulen, N. (2015). *Investeren in Cybersecurity.* Cambridge, Verenigd Koninkrijk: RAND Europe.

Van Staa, A., & Evers, J. (2010). 'Thick analysis': strategie om de kwaliteit van kwalitatieve data-analyse te verhogen. *KWALON, 15*(1), 5-12.

Van Velthoven, B. (2008). *Kosten-batenanalyse van criminaliteitsbeleid. Over de methodiek in het algemeen en Nederlandse toepassingen in het bijzonder.* Leiden: Universiteit Leiden.

Van Wees, R. (2015, 22 december). *MKB-bedrijven vaker slachtoffer van cybercrime*. Retrieved 14 juli, 2018, from Computable: https://www.computable.nl/artikel/nieuws/security/5667725/250449/mkb-bedrijven-vaker-slachtoffer-van-cybercrime.html

Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland.* Leeuwarden: NHL Hogeschool.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*(38), 97-102.

Watkins, B. (2014). *Briefing Paper: The Impact of Cyber Attacks on the Private Sector*. Praag, Tsjechië: Association for International Affairs.

Weller, M., & Anderson, T. (2013). Digital Resilience In Higher Education. *European Journal of Open, Distance, and e-Learning, 16*(1), 53-66.

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity. *International Journal of Human-Computer Interaction, 3*(32), 215-257.

Zielstra, A., & Krabbendam-Hersman, T. (2013). Cyber resilience in het jaarverslag? *Trends in Veiligheid*, 51-55.

6. Bijlagen

6.1 Topiclijst

De blauw gemarkeerde vragen en *probes* zijn gedurende de onderzoeksperiode toegevoegd.

Introductie in steekpunten

- Masterstudent Criminologie en Rechtshandhaving in Leiden: spoor Criminologie & Veiligheidsbeleid
- Stagiair bij de VeiligheidsAlliantie gemeente Rotterdam. Dit is een samenwerkingsverband van 32 gemeenten, politie en OM. Taken: kennis verzamelen, bundelen, delen over verschillende onderwerpen (veilig wonen, geweld, verwarde personen etc.).
- VAR heeft cyber in hun portfolio. 4 sporen waaronder het vergroten van cybersecurity en awareness bij MKB-ondernemers.
- Mijn onderzoek: Er achter komen welke aspecten een rol spelen bij digitale weerbaarheid volgens mkb'ers en experts. Onderzoek combineer ik met mijn scriptie.
- Interview duurt ongeveer een uurtje á anderhalf uur. Opnemen van het gesprek is gewenst. De opname gebruik ik voor mijn afstudeeronderzoek. De enige partijen die het in hand kunnen krijgen (indien nodig) zijn de VAR en de Universiteit Leiden. Het interview kan geanonimiseerd worden indien gewenst.

Inleidende vragen

- Kunt u iets vertellen over de organisatie / het bedrijf waar u werkt?

- In hoeverre hebben jullie te maken met cyber incidenten (informatiebeveiliging, cyber crime, cyber aanvallen etc.).
    - Hoe bepalen jullie risico –en dreigingen op dit gebied?
    - Maakt ICT beveiliging / cyber security een onderdeel uit van jullie bedrijfsvoering?
- Wat doen jullie in geval van een incident?
    - Welke handelingen ondernemen jullie?
    - Welke partijen benadert u? Waarom?
    - Hoe gaat u om met de gevolgen?

- Waar haalt u uw informatie m.b.t. cybersecurity vandaan?
    - Informatiebronnen? Experts? Internet? Nieuws? Collega's?
    - Wie moet deze informatie aanbieden?

Digitale weerbaarheid en verwante onderwerpen

- Wat verstaat u onder digitale weerbaarheid (verschil tussen MKB en expert).
    - Breedste zin van het woord, ieder idee dat bij u opkomt.

- Wat doen jullie zelf op het gebied van digitale weerbaarheid? Evt. cyber security.
    - Wat doen jullie om digitaal weerbaarder te zijn? Welke maatregelen hebben jullie getroffen? Technische of organisatorische maatregelen?
    - Uitbesteed of in huis? Hoe vaak contact met ICT aanbieder, zorgen zij voor bewustzijn? Hoe?
    - Vindt u uzelf / uw bedrijf digitaal weerbaar genoeg? Waarom wel / niet?
        - Werknemers, wat weten zij, doen zij?
    - Waarom doen jullie weinig (of veel) op dit gebied?

- Hebben jullie zicht op de verwachtte kosten van te weinig digitale weerbaarheid?
    - Waarom wel of niet? Hoe bepalen jullie dit?
    - Hoe maken jullie die kosten inzichtelijk?
    - Welke kosten? Niet alleen financieel?

- Wat is volgens u van invloed de digitale weerbaarheid van een bedrijf?
    - Beschrijving bedrijfscultuur, managementstijl, HR management?
    - Budget? Andere punten?
    - Waarom zijn de genoemde punten van invloed?

- Doen jullie (mkb'ers) aan informatie management?
    - Overzicht waar info staat, hoe het wordt verwerkt, wie kan er allemaal mee werken, wat gebeurt er met de info, wie is er verantwoordelijk voor.
    - Weten jullie welke info cruciaal is voor je bedrijf?
    - Waarom weten jullie dit wel of niet?

- Is cyber security / digitale weerbaarheid een groot probleem voor MKB-ondernemers?
    - Waarom?
    - Waarom doen mkb'ers er dan weinig aan?

- Wat is de grootste oorzaak van te weinig digitale weerbaarheid / cyber security incidenten?
    - Verschillen tussen grote bedrijven, MKB'ers en overheid?

Manieren om digitale weerbaarheid te vergroten

- Welke manieren zijn volgens u geschikt om digitaal weerbaar te worden / goed beschermd te zijn tegen cybersecurity? (awareness, bang maken, wijzen op gevolgen, pen tests etc.)
    - Welke zijn het meest effectief?
    - Welke juist niet?
    - Welke zijn technisch en financieel haalbaar?

- Wat zijn praktische tips of dingen die ondernemers kunnen doen om weer weerbaar te worden tegen cybercrime / incidenten?

Vragen m.b.t. VAR specifieke onderwerpen

- Huidig aanbod van de VAR: Voorlichtingsbijeenkomsten organiseren voor MKB-ondernemers in de gemeente. Presentatie bestaat uit een training / voorlichting over hoe om te gaan met cybercrime, praktische tips worden gegeven.
    - Denkt u dat dit effectief is? Waarom?
    - Aanvullingen op dit aanbod?

- Waar heeft u als MKB-ondernemer behoefte aan m.b.t. digitale weerbaarheid / cyber security?

6.2 Lijst van respondenten

Experts

Naam	Organisatie	Datum	Duur
Hugo Leisink	NCSC	07-03-18	1 uur 14 min.
Stefan Molleman[6]	Het CCV	04-04-18	56 min.
Leo Lans & Marieke van Leeuwen	Fox IT	06-04-18	n.b. ~1 uur 30 min.
Dr. Rick van der Kleij Senior researcher	Cybersecurity & SMEs Research Group aan de Haagse Hogeschool / Human Behavior & Organisational Innovations bij TNO	03-05-18	59 min.
Peter Duin	Zeehaven politie / FERM	17-05-18	1 uur 37 min.

Midden –en Kleinbedrijf

Naam	Organisatie	Datum	Duur
Tessa van Stiphout	MKB Nederland	05-04-18	56 min.
Stefan Molleman	Het CCV	04-04-18	56 min.
Diederick Groeneveld	StuD Uitzendbureau	18-04-18	46 min.
Madelon Janssen	Bakker Bart	19-04-18	1 uur 3 min.
Kees Boom	Een havenbedrijf	24-04-18	50 min.
Drs. Claire Wanneé	Digital Trust Center	05-05-18	1 uur 9 min.
Pieter van Klaveren	MKB Rotterdam Rijnmond	13-06-18	44 min.

[6] Stefan Molleman werd gezien als respondent die vanuit het mkb kon vertellen maar ook vanuit zijn positie als expert.