De ontwikkeling en evaluatie van het project “MKB Cyber Buddy’s”

Een effectieve interventie waarmee gemeenten handelingsverlegen mkb’ers kunnen helpen hun cyberweerbaarheid te verhogen?

Deelrapport werkpakket 4 (doelgroep mkb) van het project

‘Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime’

Colofon

Dit onderzoek is uitgevoerd door onderzoekers van het lectoraat Cybercrime & Cybersecurity van de Haagse Hogeschool:

Dr. Susanne van 't Hoff-de Goede[1]

Eline Brasker, MSc[1]

Luuk Bekkers, MSc[12]

Dr. Rutger Leukfeldt[13]

in samenwerking met de consortiumpartners binnen het project '*Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime*':

Hogeschool Saxion	Gemeente Utrecht
Gemeente Enschede	Gemeente Den Helder
Veiligheidsalliantie Regio Rotterdam	Regionale Veiligheidsstrategie Midden-Nederland
Noord-Holland Samen Veilig	Veiligheidsnetwerk Oost-Nederland
Gemeente Almere	Gemeente Amersfoort
Gemeente Apeldoorn	Gemeente Capelle a/d IJssel
Gemeente Dordrecht	Gemeente Zoetermeer
Gemeente Ede	Gemeente Rotterdam
Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)	Gemeente Haarlem

Dit onderzoek is medegefinancierd door Regieorgaan SIA, onderdeel van de Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO).

[1] De Haagse Hogeschool
[2] Saxion Hogeschool
[3] Nederlands Studiecentrum Criminaliteit en Rechtshandhaving

Inhoud

Samenvatting 5

1. Inleiding 10

1.1 Aanleiding 10

1.2 Doelstelling 11

1.3 Onderzoeksvraag en deelvragen 12

1.4 Leeswijzer 12

2. Eerder onderzoek en theorie 13

2.1 Ransomware in het mkb 13

2.2 Cyberweerbaarheid 13

2.2.1 Maatregelen tegen ransomware in het mkb 14

2.2.2 De benodigde vaardigheden voor weerbaarheid 14

2.2.3 Het verhogen van de cyberweerbaarheid in ondernemingen 16

3. De interventie “MKB Cyber Buddy’s” 18

3.1. Beschrijving van de interventie “MKB Cyber Buddy’s” 18

3.2 De onderdelen van de interventie 19

3.2.1 Onderdeel 1: De cyberscan 19

3.2.2 Onderdeel 2: Het adviesrapport 20

3.2.3 Onderdeel 3: Implementatiedagen 22

3.2.4 Onderdeel 4: Nameting 22

3.3 Betrokken partijen 23

3.3.1 De gemeente 23

3.3.2 De cybersecurity professional 24

3.3.3 De buddy’s 24

3.3.4 De mkb’ers 24

4. Verloop van de pilot 26

4.1 Werving en respons 26

4.2 Verloop van project stappen 27

4.3 Respondenten 28

4.4 Geleerde lessen 29

5. Methode voor de effectiviteitsmeting 33

5.1 Operationalisaties 33

5.2 Analyse 35

6. Resultaten van de pilot 36

6.1 Gemiddeld aantal gegeven en geïmplementeerde adviezen 36

6.2 Type adviezen dat wordt gegeven en ingevoerd 38

6.3 Risicoperceptie 42
6.4 Verschillen tussen groepen ondernemers in implementatie van adviezen 42
7. Ervaringen van betrokkenen van de pilot 45
7.1 Evaringen van mkb'ers 45
7.2 Ervaringen Buddy's 50
7.3 Gemeenten 51
8. Conclusie 53
8.1 Hoe is het uitvoeren van de pilot van de interventie "MKB cyber buddy's project" verlopen en hoe is deze uitvoering door betrokkenen ervaren? 53
8.2. In hoeverre beïnvloedt het "MKB cyber buddy's project" de cyberweerbaarheid van deelnemende ondernemingen tegen ransomware, met betrekking tot cybersecuritybeleid, technische maatregelen en weerbaarheid van medewerkers (human factor)? 54
8.3. Welke aanpassingen kunnen gemaakt worden om de interventie te verbeteren en geschikt te maken voor andere Nederlandse gemeenten? 56
8.4 Kanttekeningen bij het interpreteren van de resultaten 58
8.5 Is de interventie "MKB cyber buddy's project" een effectieve interventie om voor Nederlandse gemeenten om de cyberweerbaarheid van mkb'ers in hun gemeente rondom ransomware te bevorderen? 59
Literatuur 60
Bijlage 1: Op te vragen documenten 63
Bijlage 2: De cyberscan – voormeting 64
Bijlage 3: De cyberscan – nameting 73
Bijlage 4: Schematische weergave van het wervingsproces 86

Samenvatting

Aanleiding en doelgroep rapport

Cybercriminaliteit is een veelvoorkomend probleem geworden in Nederland (CBS, 2022). Nederlandse gemeenten hebben cybercrime dan ook breed als beleidsprioriteit opgepakt. Gemeenten geven daarbij aan behoefte te hebben aan handvaten om hun inwoners en ondernemers weerbaarder te maken tegen cybercriminaliteit. In het project "Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime" werken professionals uit twaalf[4] gemeenten en vier[5] regionale veiligheidsnetwerken samen met onderzoekers van de Haagse Hogeschool, Hogeschool Saxion en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) aan wetenschappelijk onderbouwde interventies waaromee ambtenaren openbare orde en veiligheid de cyberweerbaarheid van burgers en bedrijven binnen hun gemeente kunnen vergroten.

In dit rapport staat slachtofferschap van cybercriminaliteit onder mkb'ers centraal. Het midden- en kleinbedrijf (mkb) wordt relatief vaak slachtoffer van cybercriminaliteit en ondervindt hiervan in hoge mate schade (CBS, 2018; Notté et al., 2019). Met name de toename van slachtofferschap van ransomware binnen het mkb is een zorgelijke ontwikkeling. Het is van groot belang dat mkb'ers maatregelen nemen om een ransomware aanval te voorkomen en de schade zo veel mogelijk te beperken. Beschermende maatregelen worden echter door veel mkb'ers slechts in geringe mate ingezet (Bekkers et al., 2021; CBS, 2021; Notté et al., 2019; Veenstra et al., 2015). De cyberweerbaarheid van mkb'ers (*het vermogen van een organisatie om cyberincidenten te weerstaan, daarop te kunnen reageren en van te herstellen, zodat de organisatie operationeel blijft)* is daardoor te beperkt.

Doel en hoofdvraag rapport

In dit rapport presenteren we de ontwikkeling en evaluatie van een interventie genaamd "MKB Cyber Buddy's". Het doel van de interventie is om de weerbaarheid van mkb'ers tegen ransomware te vergroten. De interventie is er op gericht om mkb'ers niet alleen te informeren over cybercriminaliteit, maar ze ook door actieve deelname tot een positieve gedragsverandering te brengen. Onder mkb'ers verstaan we in dit onderzoek ondernemers met minimaal één en maximaal 250 werknemers. De hoofdvraag in dit rapport is: *Is de interventie "MKB cyber buddy's" een effectieve interventie voor*

[4] Almere, Amersfoort, Apeldoorn, Capelle a/d IJssel, Den Helder, Dordrecht, Ede, Enschede, Haarlem, Utrecht, Rotterdam, Zoetermeer.

[5] VeiligheidsAlliantie Rotterdam, Veiligheidsnetwerk Oost-Nederland, Noord-Holland Samen Veilig, Regionale Veiligheidsstrategie Midden-Nederland.

Nederlandse gemeenten om de cyberweerbaarheid van mkb'ers in hun gemeente met betrekking tot ransomware te bevorderen?

Het doel van dit rapport is tweeledig. Enerzijds beschrijft dit rapport de onderbouwing en ontwikkeling van de interventie "MKB Cyber Buddy's". Anderzijds beschrijft dit rapport de evaluatie van de pilot die is uitgevoerd in 2022, betreffende de effectiviteit, sterke kanten, valkuilen en onvoorziene gevolgen van de interventie. Hiermee zullen inzichten geboden worden in hoe de interventie verbeterd kan worden en in de toekomst op grotere schaal kan worden ingezet.

Beschrijving interventie en wetenschappelijke onderbouwing

In het "MKB Cyber Buddy's" project worden deelnemende mkb'ers gekoppeld aan een IT student die als buddy een aantal weken het bedrijf ondersteunt op het gebied van cybersecurity. De buddy neemt allereerst een cybersecurity scan af om het bedrijf en de huidige cybersecurity maatregelen (gericht op techniek, beleid en medewerkers) in kaart te brengen. Vervolgens schrijft de buddy op basis van de uitkomsten van de cyberscan een op maat gemaakt adviesrapport. Vervolgens stelt de buddy zich beschikbaar om tijdens twee meeloopdagen een bijdrage te leveren aan de implementatie van de aanbevelingen uit het adviesrapport. Tot slot wordt de cyberscan opnieuw afgenomen tijdens de nameting.

De interventie is op verschillende manier wetenschappelijk onderbouwd. Ten eerste werd op basis van resultaten uit werkpakket 3 risicocommunicatie opgenomen in het adviesrapport, waarmee wordt ingespeeld op twee wetenschappelijk onderbouwde factoren die bijdragen aan de motivatie van mkb'ers om maatregelen te nemen tegen ransomware, namelijk 'subjectieve norm' en 'affectieve respons'. Hoe meer ondernemers denken dat mensen in hun omgeving van ze verwachten dat ze maatregelen nemen (subjectieve norm), en hoe meer ondernemers zich zorgen maken over de risico's van ransomware (affectieve respons), hoe meer ze geneigd zijn zelf-beschermend gedrag te vertonen (Bekkers et al., 2021). Ten tweede richt de interventie zich op basis van eerder onderzoek niet alleen op cyberweerbaarheid door het nemen van technische maatregelen, maar ook maatregelen gericht op beleid en medewerkers. Bovendien wordt cyberweerbaarheid niet alleen opgevat als het vermogen om cyberincidenten te voorkomen (anticiperen) maar ook als het vermogen van bedrijven om aanvallen te detecteren, er vervolgens op te reageren en er ten slotte van te leren (Hollnagel, 2015). Ten slotte richt de interventie zich op cyberweerbaarheid onder medewerkers gebaseerd op het COM-B model, dat stelt dat medewerkers niet alleen kennis en vaardigheden (capaciteit) nodig hebben voor cyberveilig gedrag, maar ook gelegenheid en motivatie. De cyberscan brengt deze vermogens van bedrijven en hun medewerkers in kaart en het adviesrapport voorziet vervolgens de bedrijven van een handelingsperspectief gericht op specifieke onderdelen van cyberweerbaarheid op basis van de resultaten uit de cyberscan.

Resultaten van de pilot

De pilot is uitgevoerd van 1 februari 2022 tot en met 15 juli 2022. In totaal zijn gedurende deze pilot 498 mkb'ers benaderd om deel te nemen aan de interventie. Hiervan hebben 43 ook uiteindelijk de scan laten afnemen (6,4%). Uiteindelijk hebben 36 mkb'ers ook de nameting laten afnemen (83,7%).

Gemiddeld hebben de buddy's aan deelnemende mkb'ers 35.5 maatregelen geadviseerd, verdeeld over beleids-, technische- en medewerker maatregelen. Zeven weken later hebben de mkb'ers gemiddeld aangegeven 34,3% van de geadviseerde maatregelen ingevoerd te hebben. Dit percentage verschilt weinig tussen beleids-, technische- en medewerker maatregelen. In absolute aantallen implementeren bedrijven door hun deelname aan het project gemiddeld ongeveer drie technische maatregelen, vijf maatregelen gericht op medewerkers, twee maatregelen gericht op documentatie van cybersecuritybeleid en gemiddeld iets minder dan een halve maatregel gericht op cybersecurity management. Relatief minder vaak werden maatregelen ingevoerd die gericht waren op de vaardigheid van medewerkers om te leren van incidenten en de gelegenheid die hen geboden wordt om zich online veilig te gedragen. Bedrijven die gebruik maakten van de implementatiedagen hebben een groter aantal maatregelen ingevoerd (33-56%) dan bedrijven die hier geen gebruik van maakten.

Enkele van de meest ingevoerde beleidsmaatregelen zijn het verantwoordelijk maken van specifieke personen voor cybersecurity en een wachtwoordbeleid. De meest ingevoerde technische maatregelen zijn het beperken van IT-administratie rechten en het bijhouden en bijwerken van deze rechten. De meest ingevoerde maatregelen gericht op medewerkers waren medewerkers leren hoe ze een cyberaanval kunnen herkennen en hoe ze verdachte links op betrouwbaarheid kunnen checken.

Ook is nagegaan in hoeverre de risicoperceptie van deelnemende mkb'ers verschilt tussen de eerste en de tweede cyberscan. Gemiddeld bleek de risicoperceptie ongeveer gelijk te zijn gebleven. Het is onduidelijk in hoeverre het inspelen op de factoren 'affectieve respons' en 'subjectieve norm' in de risicocommunicatie heeft bijgedragen aan het verhogen van de motivatie van ondernemers om cybersecurity maatregelen te nemen.

Na afloop van het project is aan de deelnemende mkb'ers gevraagd wat de invloed van het project is geweest op hun onderneming en de toekomst van de cybersecurity van het bedrijf. Bijna twee derde van de respondenten heeft aangegeven dat zij op basis van het adviesrapport verbeteringen hebben doorgevoerd in de cybersecurity van hun onderneming. Redenen om geen maatregelen te implementeren waren onder andere dat ze er tijdens de looptijd van het project geen tijd voor hebben gehad, of dat uit het adviesrapport bleek dat alles al goed geregeld was. Vervolgens gaf de helft van de deelnemende mkb'ers aan het gevoel te hebben dat hun onderneming weerbaarder was geworden. Zo'n 60 procent van de respondenten voelde zich als gevolg van het project in staat om het bedrijf verder te ontwikkelen op het gebied van cybersecurity. Bovendien gaf ruim 60 procent

van de respondenten aan dat zij op basis van het adviesrapport op korte termijn (verdere) verbeteringen gaan doorvoeren in de cybersecurity van de onderneming.

Evaluatie van de pilot

Deelnemende mkb'ers waren gemiddeld tevreden over het project (gemiddeld 3.9, op een schaal van 1-5). Deelnemende mkb'ers waren het meest tevreden over het adviesrapport en het contact met de buddy (gemiddeld 4,2), dat als prettig en professioneel werd omschreven. Respondenten vonden bijvoorbeeld dat het adviesrapport in duidelijke taal geschreven was en veel inzichten bood in de kwetsbaarheden van het bedrijf. Enkele respondenten gaven aan dat ze het adviesrapport te lang vonden of dat het rapport nog meer op maat gemaakt had kunnen zijn. Een respondent leek de cyberscan relevanter voor grotere kantoren. Respondenten die tevreden waren met de cyberscan gaven aan dat er goede vragen gesteld werden. Volgens een van de respondenten leidde het invullen van de cyberscan op zichzelf al tot meer bewustwording en een intentie tot gedragsverandering. De respondenten die gebruik hebben gemaakt van de implementatiedagen waren daar gemiddeld tevreden over (gemiddeld 3,9). Respondenten gaven aan dat ze het fijn vonden dat er iemand met kennis kwam meekijken in het bedrijf.

De medewerkers vanuit de gemeenten waren over het algemeen positief over het project. Zij gaven aan dat zij vinden dat de kosten opwegen tegen de baten en dat het project aantrekkelijk kan zijn voor gemeentes die weinig medewerkers en tijd hebben voor het dossier cybersecurity. Ook gaven zij aan dat ze de samenwerking met zowel de andere gemeentes als met de onderzoekers prettig vonden verlopen. Ook waren ze tevreden over de opzet en onderbouwing van het project. Als minder positief aspect van het project gaven medewerkers aan dat het werven van de mkb'ers moeizamer ging dan verwacht. Een andere uitdaging voor gemeentemedewerkers was het vinden van voldoende buddy's om de stageplaatsen te vullen.

Buddy's ervaarden het als zeer uitdagend om mkb'ers te werven die mee wilden doen aan het project. Uit gesprekken tijdens het werven bleek bijvoorbeeld dat mkb'ers het vaak te druk hadden voor het project of cybersecurity niet als een prioriteit zagen. Ook hebben de buddy's vaak meegemaakt dat mkb'ers die meededen aan de cyberscan lastig te bereiken waren voor vervolgafspraken of niet kwamen opdagen voor de nameting. Wel vonden alle buddy's dit project als stage zeer leerzaam en interessant. De diversiteit aan bedrijven zorgde ervoor dat ze veel kennis uit hun studie hebben kunnen toepassen in de praktijk, waardoor ze veel hebben geleerd.

De evaluatie heeft een aantal geleerde lessen opgeleverd die inzicht bieden in hoe de interventie verbeterd kan worden en in de toekomst op grotere schaal kan worden ingezet. Deze hebben betrekking op het werven van respondenten, communicatie en verwachttingsmanagement met deelnemende mkb'ers, timing van de projectonderdelen, het afnemen van cyberscans en

schrijven van adviesrapporten en samenwerking en communicatie tussen uitvoerders. Het belangrijkste hieruit naar voren gekomen inzicht is dat het “koud” werven van mkb’ers (bij hen langsgaan zonder dat zij vooraf zijn geïnformeerd over het project) een zeer laag responspercentage oplevert, ondanks dat de interventie vanuit de gemeente werd aangeboden.

Conclusie

Is de interventie “MKB cyber buddy’s project” een effectieve interventie om voor Nederlandse gemeenten om de cyberweerbaarheid van mkb’ers in hun gemeente rondom ransomware te bevorderen? Alles bij elkaar genomen kan gesteld worden dat de interventie een effectieve tool is voor Nederlandse gemeenten om de cyberweerbaarheid van een specifieke groep mkb’ers in hun gemeente te bevorderen. Deze groep mkb’ers bestaat uit mkb’ers die handelingsonbekwaam zijn, behoefte hebben aan informatie en/of open staan voor een project om de cyberweerbaarheid van hun onderneming te toetsen en verbeteren. Deze mkb’ers hebben bijvoorbeeld zelf de gemeente benaderd met interesse om deel te nemen aan een project rondom cybersecurity of stonden hiervoor open nadat zij benaderd werden voor de buddy (6.4% van alle benaderde mkb’ers). Na deelname aan het project is er sprake van een hogere mate van cyberweerbaarheid, gezien de toename van het aantal cybersecurity maatregelen die deelnemende bedrijven lijken te nemen door hun deelname aan “MKB Cyber buddy’s”.

“MKB Cyber buddy’s” is een geschikte interventie voor gemeenten op zoek zijn naar een effectieve tool om mkb’ers die behoefte hebben aan informatie en hulp rondom cybersecurity in deze behoefte te voorzien. Wij raden aan het project te presenteren bij ondernemings-bijeenkomsten over cybersecurity, die door vele gemeenten reeds worden georganiseerd, waarbij ondernemers de optie geboden worden om zichzelf gelijk aan te melden voor “MKB Cyber buddy’s”.

1. Inleiding

1.1 Aanleiding

Cybercriminaliteit is een veelvoorkomend probleem geworden in Nederland (CBS, 2022). Nederlandse gemeenten hebben cybercrime dan ook breed als beleidsprioriteit opgepakt. Deze gemeenten geven daarbij aan behoefte te hebben aan handvaten om hun ondernemers weerbaarder te maken tegen cybercriminaliteit. In het project "Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime" werken professionals uit twaalf[6] gemeenten en vier[7] regionale veiligheidsnetwerken samen met onderzoekers van de Haagse Hogeschool, Hogeschool Saxion en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR) aan het volgende vraagstuk: *Met welke interventies kunnen ambtenaren openbare orde en veiligheid de cyberweerbaarheid van burgers en bedrijven binnen hun gemeente vergroten?* Hierbij is het overkoepelende doel te komen tot effectieve interventies die lokale overheden kunnen inzetten om de cyberweerbaarheid binnen hun gemeente te vergroten.

Op basis van inzichten uit zowel literatuur als interviews met gemeenten en experts, zijn in de eerste twee werkpakketten van dit project drie doelgroepen geïdentificeerd waarvoor het verhogen van hun cyberweerbaarheid het meest noodzakelijk is: 1) jongeren, 2) ouderen en 3) mkb'ers. Deze groepen lijken relatief vaak slachtoffer te worden van cybercriminaliteit en bovendien zijn de emotionele en/of financiële gevolgen van slachtofferschap groot. Toegepast op het huidige onderzoek, wordt cyberweerbaarheid benaderd vanuit de gedragingen of acties die iemand neemt om zichzelf te beschermen tegen deze cyberrisico's of de gevolgen daarvan, gebaseerd op het risicobewustzijn en bijbehorende verklarende factoren van gedrag.

Dit rapport richt zich op slachtofferschap van cybercriminaliteit onder mkb'ers. Het midden- en kleinbedrijf (mkb) wordt relatief vaak slachtoffer van cybercriminaliteit en ondervindt hier ook in hoge mate financiële en/of emotionele schade aan (CBS, 2018; Notté et al., 2019). Een zorgelijke ontwikkeling is de toename van slachtofferschap van ransomware binnen het mkb, mede vanwege de enorme financiële en emotionele impact die ransomware kan hebben voor organisaties, medewerkers en klanten.

In het derde werkpakket stond het Cyberweerbaarheidsmodel centraal (Bekkers et al., 2021; Misana-ter Huurne et al., 2021) dat als basis en als leidraad dient voor het inzichtelijk maken van de factoren die een rol spelen bij (intenties tot) zelfbeschermend gedrag ten aanzien van

[6] Almere, Amersfoort, Apeldoorn, Capelle a/d IJssel, Den Helder, Dordrecht, Ede, Enschede, Haarlem, Utrecht, Rotterdam, Zoetermeer.
[7] VeiligheidsAlliantie Rotterdam, Veiligheidsnetwerk Oost-Nederland, Noord-Holland Samen Veilig, Regionale Veiligheidsstrategie Midden-Nederland.

cybercriminaliteit onder eindgebruikers. Juist bij het bevorderen hiervan is het belangrijk om inzicht te krijgen in de percepties, beleving, behoeftes en (risicovolle) gedragingen van de doelgroep. Het doel is immers om (groepen) individuen daadwerkelijk in staat te stellen en te stimuleren om zichzelf (beter) te beschermen. Resultaten van werkpakket 3 suggereren dat mkb'ers gemotiveerd kunnen worden om meer zelfbeschermend gedrag te vertonen door de 'subjectieve norm' en 'affectieve respons' te verhogen: hoe meer ondernemers denken dat mensen in hun omgeving van ze verwachten dat ze maatregelen nemen, en hoe meer ondernemers zich zorgen maken over de risico's van ransomware, hoe meer ze geneigd zijn zelf-beschermend gedrag ge vertonen (Bekkers et al., 2021).

In dit rapport presenteren we de ontwikkeling en evaluatie van een interventie genaamd "MKB Cyber Buddy's". Het doel van de interventie is om de weerbaarheid van mkb'ers tegen ransomware te vergroten. Aan de hand van een cyberscan, een op maat gemaakt adviesrapport en werkbezoeken krijgen de ondernemers passend en toegankelijke adviezen van IT studenten. De cyberscan en de risicocommunicatie in de interventie zijn wetenschappelijk onderbouwd. De interventie is er op gericht om mkb'ers niet alleen te informeren over cybercriminaliteit, maar ze ook door actieve deelname tot een positieve gedragsverandering te brengen. Onder mkb'ers verstaan we in dit onderzoek ondernemers met minimaal één en maximaal 250 werknemers.

1.2 Doelstelling

Om te komen tot effectieve interventies voor ambtenaren openbare orde en veiligheid om de cyberweerbaarheid binnen hun gemeente te vergroten, is de centrale doelstelling opgedeeld in subdoelen: 1) Het in kaart brengen van de meest kwetsbare doelgroepen; 2) Het in kaart brengen van de vormen van cybercriminaliteit waarvan zij slachtoffer worden; 3) Het inzichtelijk maken van de onderliggende factoren en verklaringen van hun risicobewustzijn en preventieve gedrag ten aanzien van cybercriminaliteit; 4) Het ontwikkelen en implementeren van effectieve interventies die Nederlandse gemeenten kunnen inzetten om het risicobewustzijn en het preventieve gedrag rondom deze vormen cybercriminaliteit onder deze doelgroepen kunnen bevorderen.

De eerste drie subdoelen zijn reeds voldaan (zie geïntegreerd deelrapport werkpakketten 1 en 2 en deelrapport werkpakket 3). Hierbij zijn op basis van literatuuronderzoek en interviews de meest kwetsbare doelgroepen en de meest relevante vormen van cybercriminaliteit waarvan zij slachtoffer worden bepaald en is door middel van een vragenlijst onderzocht welke factoren ten grondslag liggen aan hun preventieve gedrag ten aanzien van die delicten.

Dit deelrapport richt zich op het vierde en tevens laatste subdoel, namelijk het ontwikkelen en implementeren van een effectieve interventie die Nederlandse gemeenten kunnen inzetten om het

risicobewustzijn en het preventieve gedrag rondom malware onder de doelgroep mkb te kunnen bevorderen. Hierbij staat gedragsverandering door middel van effectieve risicocommunicatie centraal.

Het doel van dit rapport is tweeledig. Enerzijds beschrijft dit rapport de onderbouwing en ontwikkeling van de interventie “MKB Cyber Buddy’s”, die lokale overheden kunnen inzetten om de cyberweerbaarheid van het mkb in hun regio te vergroten. Anderzijds beschrijft dit rapport evaluatie van de pilot die is uitgevoerd in 2022. Er zal hierbij verslag worden gedaan van de bevindingen die gedurende de pilot zijn opgedaan betreffende de effectiviteit, sterke kanten, valkuilen en onvoorziene gevolgen van de interventie. Hiermee zullen inzichten geboden worden in hoe de interventie verbeterd kan worden en in de toekomst op grotere schaal kan worden ingezet.

1.3 Onderzoeksvraag en deelvragen

In dit rapport staat de volgende onderzoeksvraag centraal:

Is de interventie “MKB cyber buddy’s” een effectieve interventie voor Nederlandse gemeenten om de cyberweerbaarheid van mkb’ers in hun gemeente met betrekking tot ransomware te bevorderen?

Deze zal beantwoord worden aan de hand van de volgende deelvragen:

1. Hoe is het uitvoeren van de pilot van de interventie “MKB cyber buddy’s project” verlopen en hoe is deze uitvoering door betrokkenen ervaren?
2. In hoeverre beïnvloedt het “MKB cyber buddy’s project” de cyberweerbaarheid van deelnemende ondernemingen tegen ransomware, met betrekking tot risicoperceptie en het nemen van maatregelen (gericht op beleid, techniek en medewerkers)?
3. Welke aanpassingen kunnen gemaakt worden om de interventie te verbeteren en geschikt te maken voor uitvoering door andere Nederlandse gemeenten?

1.4 Leeswijzer

In hoofdstuk 2 wordt een overzicht gegeven van de literatuur over ransomware in het mkb en wordt het theoretische Cyberweerbaarheidsmodel, waar de interventie “MKB cyber buddy’s project” op gestoeld is, toegelicht. In hoofdstuk 3 wordt de interventie beschreven en worden de gemaakte keuzes binnen het ontwerp van de interventie toegelicht. Vervolgens wordt in hoofdstuk 4 besproken hoe de pilot van de interventie is verlopen. Nadat in hoofdstuk 5 de methode van dit onderzoek wordt beschreven, worden de resultaten van de pilot beschreven in hoofdstuk 6 en de ervaringen van betrokkenen van de pilot in hoofdstuk 7. Dit rapport sluit af met de conclusies in hoofdstuk 8.

2. Eerder onderzoek en theorie

2.1 Ransomware in het mkb

Het mkb krijgt vaak te maken met cybersecurity incidenten. In de periode van 2016 tot en met 2020 had per jaar ongeveer 25 tot 60% van de mkb'ers te maken met cybersecurity incidenten van interne oorzaak en ongeveer 5 tot 25% met incidenten van externe oorzaak (CBS, 2021). In ongeveer de helft van deze gevallen leidden de incidenten tot economische schade. De Haagse Hogeschool onderzocht de prevalentie van slachtofferschap van cybercriminaliteit onder Nederlandse mkb'ers en vond dat 1 op de 5 mkb'ers in het verleden slachtoffer was geworden met (financiële of andere) schade tot gevolg (Notté et al., 2019). Dat cybercrime onder mkb's vaak voorkomt en tot veel schade leidt, blijkt ook uit gesprekken met experts (Misana-ter Huurne et al., 2021).

Eén van de meest voorkomende cyberdelicten in het mkb is ransomware (Datto, 2020; Notté et al., 2019), een vorm van malware die voor grote emotionele als economische schade kan leiden. Malware is een verzamelnaam voor kwaadaardige software (samentrekking van "malicious software"). In het geval van ransomware wordt data of een computer(systeem) versleutelt, waardoor de toegang tot die gegevens wordt ontzegd totdat het slachtoffer een geldbedrag betaalt (Richardson & North, 2017)(Al-rimy et al., 2018; Leukfeldt et al., 2015).

Slachtofferschap van ransomware kan grote gevolgen hebben voor bedrijven en medewerkers, zowel op financieel als emotioneel gebied (Button et al., 2021; Kamiya et al., 2021; Leukfeldt et al., 2018). Het losgeld dat cybercriminelen eisen loopt sterk uiteen, van bijvoorbeeld 5000 tot meer dan 100.000 euro, mogelijk afhankelijk van de omzet van aangevallen bedrijven (Chainalysis, 2022; Datto, 2020). Bovendien zijn kosten verbonden aan het tot stilstand komen van bedrijfsprocessen en het herstellen van de bedrijfsvoering (Brewer, 2016; Tuttle, 2020). Deze indirecte kosten zijn voor het mkb gemiddeld zelfs 23 keer hoger dan het geëiste losgeld (Datto, 2020). Daarnaast kan een cyberaanval als ransomware ook nog leiden tot schade aan de infrastructuren en reputatie van het bedrijf, met als gevolg bijvoorbeeld een afname in klanten en verkoop (Al-rimy et al., 2018; Brewer, 2016; Kamiya et al., 2021). Een deel van de bedrijven kiest er dan ook voor om het losgeld te betalen (Datto, 2020).

2.2 Cyberweerbaarheid

Experts geven aan dat het weerbaarder maken van mkb'ers tegen ransomware extra prioriteit verdient, aangezien deze vorm van cybercriminaliteit significant vaak voorkomt en tot zowel emotionele als economische schade kan leiden (Misana-ter Huurne et al., 2021). Deze paragraaf zal ingaan op de mate waarin mkb'ers maatregelen nemen tegen ransomware (2.2.1), wat wordt verstaan onder cyberweerbaarheid van mkb'ers (2.2.2) en hoe cyberweerbaarheid kan worden verhoogd

(2.2.3.). Inzicht in de cyberweerbaarheid in het mkb en welke factoren daar een rol bij spelen bieden aanknopingspunten voor de interventie die centraal staat in dit rapport.

2.2.1 Maatregelen tegen ransomware in het mkb

Het is van groot belang dat mkb'ers maatregelen nemen om een ransomware aanval te voorkomen en de schade van een infectie zo veel mogelijk te verkleinen. Mkb's kunnen zich bijvoorbeeld beschermen tegen ransomware met behulp van technische maatregelen, zoals firewalls, anti-malware programma's, automatische back-ups van bestanden en updates van software (Al-rimy et al., 2018; Brewer, 2016; Lopez et al., 2020; Tuttle, 2020; Zimba & Chishimba, 2019). Ransomware kan echter niet volledig voorkomen worden met enkel technische maatregelen, aangezien het vaak een systeem binnendringt als het gevolg van menselijke fouten (Hull et al., 2019; Leukfeldt, 2017; Levesque et al., 2014; Ovelgönne et al., 2017). Zo wordt er gebruik gemaakt van phishing en malware als eerste stap om bij data of een systeem te komen (Datto, 2020; Hull et al., 2019; Lévesque et al., 2018; Zimba & Chishimba, 2019). Technische maatregelen moeten dan ook worden aangevuld met (beleids)maatregelen die zich richten op medewerkers, zoals het trainen in het herkennen van verdachte mailtjes en onveilige bijlagen (Al-rimy et al., 2018; Lopez et al., 2020).

Hoewel er dus meerdere manieren zijn waarop mkb'ers zich kunnen beschermen tegen ransomware, worden beschermende maatregelen slechts in geringe mate ingezet (Bekkers et al., 2021; CBS, 2021; Notté et al., 2019; Veenstra et al., 2015). Dit kan mogelijk verklaard worden doordat mkb´ers minder prioriteit stellen aan cyberveiligheid dan grotere bedrijven, vanwege een gebrek aan middelen of lage risico inschatting (Alert Online, 2019; Notté et al., 2019; Wetzer, 2018). Onderzoek van het CBS (2021) laat bijvoorbeeld niet alleen zien dat mkb'ers minder beschermende maatregelen treffen dan grotere bedrijven, maar dat dit verschil ook groter is bij de moeilijkere maatregelen dan bij de gangbare maatregelen. Ondernemers zouden vooral beschermingsmaatregelen treffen die simpel te gebruiken zijn en zouden overtuigd moeten zijn dat die maatregel ook effectief is (Misana-ter Huurne et al., 2021; Zwilling et al., 2022). Bovendien hebben mkb'ers vaak een IT-leverancier, waardoor het risico ontstaat dat mkb'ers er onterecht van uitgaan dat de cybersecurity voor hen goed geregeld is. Een ruime meerderheid van de mkb'ers geeft aan dat de leverancier zorgplicht heeft over hun cybersecurity, terwijl slechts 22% van IT leveranciers aangeeft duidelijke afspraken hierover te hebben (Ipsos, 2018).

2.2.2 De benodigde vaardigheden voor weerbaarheid

In de literatuur zijn er verschillende perspectieven op het concept cyberweerbaarheid. Zo kan cyberweerbaarheid worden beschouwd als *het vermogen van een organisatie om cyberincidenten te*

weerstaan, daarop te kunnen reageren en van te herstellen, zodat de organisatie operationeel blijft (Hausken, 2020; Linkov & Kott A, 2018). In deze conceptualisatie spelen vier verschillende vaardigheden een rol (Hollnagel, 2015). Deze vaardigheden beschrijven oorspronkelijk weerbaarheid in het algemeen en lijken op basis van eerder onderzoek ook toepasbaar op het cyberdomein (Hausken, 2020; Linkov & Kott, A, 2018; Van der Kleij & Leukfeldt, 2019). Dit zijn anticiperen, detecteren, reageren en leren (Hollnagel, 2015).

- Anticiperen omvat de vaardigheid om voorbereid te zijn op potentiële gebeurtenissen, dreigingen of andere ontwikkelingen in de toekomst.
- Detecteren is het vermogen om situaties als dreigingen en ontwikkelingen als zodanig te kunnen herkennen.
- Reageren is het in staat zijn om te handelen na veranderingen en verstoringen, door middel van geplande acties of het aanpassen van het functioneren.
- Leren is het vermogen om de juiste les uit een gebeurde situatie te trekken.

Deze vier vaardigheden bepalen samen de (cyber)weerbaarheid van een organisatie; door te anticiperen weten organisaties welke veranderingen en verstoringen zij kunnen verwachten en wat zij in dat geval moeten doen, detecteren zorgt dat veranderingen en verstoringen ook daadwerkelijk worden opgemerkt, juist reageren zorgt ervoor dat de organisatie kan voortbestaan en daarmee de kans heeft om van de situatie te leren, waardoor toekomstige veranderingen en verstoringen effectiever zullen worden aangegaan.

De vier vaardigheden zijn toepasselijk op de schaal van de gehele organisatie, maar ook op het gebied van de individuele medewerkers (Van der Kleij & Leukfeldt, 2019). Het is voor de cyberweerbaarheid van een bedrijf van belang dat medewerkers anticiperen, monitoren, reageren en leren. Om te verklaren waarom ze dit wel of niet doen en hoe hier verandering in aangebracht kan worden, maken Van der Kleij en Leukfeldt (2019) gebruik van het COM-B model van Michie et al. (2011). In dit model worden capaciteit, gelegenheid en motivatie gezien als essentiële voorwaarden voor het plaatsvinden van een gedraging. Onder capaciteit valt zowel de fysieke als psychologische capabiliteit om een gedraging uit te voeren, zoals het hebben van de nodige kennis en vaardigheden. Gelegenheid heeft betrekking op alle factoren die buiten de invloed van een individu liggen en die bepaald gedrag mogelijk maken of het beïnvloeden. Een voorbeeld is de aanwezigheid van een cybersecuritybeleid. Motivatie omvat ten slotte alle interne processen die zowel bewust als onbewust een gedraging aansturen (Michie et al., 2011).

Door het COM-B model te combineren met de vier aspecten van weerbaarheid van Hollnagel (2015), vormt het model van der Kleij en Leukfeldt (2019) een theoretisch raamwerk voor cyberweerbaar gedrag (Tabel 1). Volgens dit raamwerk is dus de capaciteit, gelegenheid en motivatie

van belang voor ieder aspect van cyberweerbaarheid. Deze operationalisatie stelt onderzoekers en beleidsmakers in staat om cyberweerbaar gedrag binnen een bedrijf te meten en effectief beleid te voeren.

Tabel 1. Theoretische raamwerk voor cyberweerbaar gedrag (aangepast overgenomen uit Van der Kleij & Leukfeldt (2019))

	Capaciteit	Gelegenheid	Motivatie
Anticiperen	Weten wat je kunt verwachten	Middelen hebben om naar ontwikkelingen in de toekomst te kijken	Bereid zijn om te zoeken naar potentiële dreigingen
Detecteren	Weten waar je naar moet kijken	Middelen hebben om de werking en de omgeving van de organisatie te monitoren	Bereid zijn om te monitoren wat mogelijk een positieve of negatieve invloed kan hebben op de organisatie
Reageren	Weten wat je moet doen	Middelen hebben om voorbereide reacties uit te voeren	Bereid zijn om te reageren op veranderingen, dreigingen en mogelijkheden
Leren	Weten wat er gebeurd is	Middelen hebben om de juiste lessen uit een ervaring te halen	Bereid zijn om te leren van de ervaringen

2.2.3 Het verhogen van de cyberweerbaarheid in ondernemingen

Om de cyberweerbaarheid te verhogen onder mkb'ers en medewerkers, is het van belang om vast te stellen hoe mensen kunnen worden aangezet tot het aannemen van zelfbeschermend gedrag. Een ander perspectief op cyberweerbaarheid hanteert dan ook een meer sociaalpsychologische benadering. Hierbij wordt cyberweerbaarheid gedefinieerd als de combinatie van een voldoende hoge mate van risicobewustzijn en zelfbeschermend gedrag om slachtofferschap van cybercriminaliteit te voorkomen en/of mogelijk impact te voorkomen of verkleinen (Spithoven, 2020; Misana-ter Huurne et al., 2020). Onder zelfbeschermend gedrag verstaan wij acties of gedragingen die mensen uitvoeren om zichzelf te beschermen tegen risico's, gevaren of de gevolgen daarvan (inclusief (negatieve) emoties). (Floyd et al., 2000; Rogers, 1975)Deze opvatting over cyberweerbaarheid staat centraal in het conceptuele Cyberweerbaarheidsmodel van Spithoven (2020) en Misana-ter Huurne et al. (2020). In dit model worden verschillende factoren uit bestaande theorieën samengevoegd die een direct effect hebben op de intentie om cyberveilig gedrag te vertonen (e.g. Rogers, 1975

In het deelrapport van werkpakket 3 van het huidige project is door middel van een online vragenlijst onder meer dan 1000 mkb'ers onderzocht in welke mate de factoren uit het Cyberweerbaarheidsmodel bijdragen aan zelfbeschermend tegen ransomware onder mkb'ers (Bekkers et al., 2021). Het bleek dat hoe meer zorgen mkb'ers zich maken om slachtoffer te worden (affectieve respons) en hoe meer ze het gevoel hebben dat bedrijven in hun omgeving verwachten dat ze zichzelf beschermen (subjectieve norm), hoe meer ze aangeven geneigd te zijn om in de toekomst meer zelfbeschermende maatregelen te nemen. Mkb'ers zijn juist in mindere mate van plan hun bedrijf in de toekomst beter te beschermen als ze zichzelf daar momenteel al goed toe in staat achten (zelfeffectiviteit). Daarnaast bleek risicobewustzijn en risicoperceptie een indirect positief effect te hebben op de gedragsintentie, door tot een hogere affectieve respons te leiden. Samengenomen blijkt hieruit dat ondernemers kunnen worden gemotiveerden tot gedragsverandering, door in te spelen op de affectieve respons en de subjectieve norm. Deze factoren staan dan ook centraal in de risicocommunicatie in de interventie.

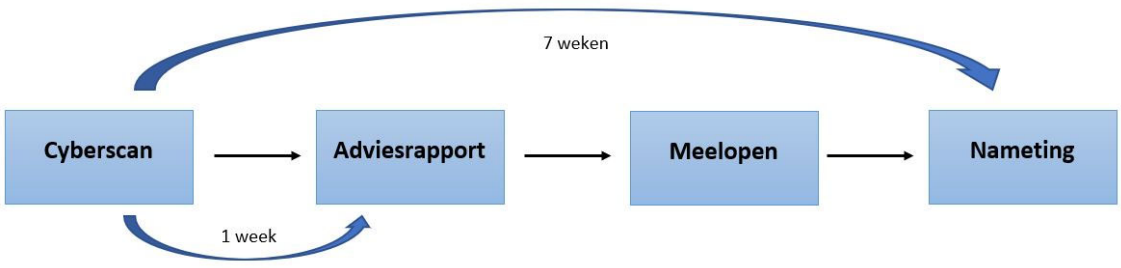
3. De interventie “MKB Cyber Buddy’s”

In dit hoofdstuk beschrijven we de interventie (3.1.), de onderdelen (3.2) en de betrokken partijen (3.3).

3.1. Beschrijving van de interventie “MKB Cyber Buddy’s”

In het “MKB Cyber Buddy’s” project worden deelnemende mkb’ers gekoppeld aan een IT student die als buddy een aantal weken het bedrijf ondersteunt op het gebied van cybersecurity. Het doel van de interventie is om de weerbaarheid van mkb’ers tegen ransomware te vergroten. De interventie is er op gericht om mkb’ers niet alleen te informeren over cybercriminaliteit, maar ze ook door actieve deelname tot een positieve gedragsverandering te brengen.

Aan de hand van een cyberscan, een op maat gemaakt adviesrapport en werkbezoeken krijgen de ondernemers passend en toegankelijke adviezen van IT studenten. De buddy neemt allereerst een cybersecurity scan af om het bedrijf en de huidige cybersecurity maatregelen (gericht op techniek, beleid en medewerkers) in kaart te brengen. Vervolgens schrijft de buddy op basis van de uitkomsten van de cyberscan een op maat gemaakt advies rapport. In dit rapport is risicocommunicatie opgenomen die inspeelt op twee wetenschappelijk onderbouwde factoren die bijdragen aan de motivatie van mkb’ers om maatregelen te nemen tegen ransomware (Bekkers et al., 2021). Vervolgens stelt de buddy zich beschikbaar om tijdens twee meeloopdagen een bijdrage te leveren aan de implementatie van de aanbevelingen uit het adviesrapport. Tot slot wordt de cyberscan opnieuw afgenomen tijdens de nameting. Alle onderdelen van het project zullen in paragraaf 3.2. nader beschreven worden.



Figuur 1. Tijdsplanning van de vier onderdelen van de interventie

De vier onderdelen van het project “MKB Cyber Buddy’s” (cyberscan, adviesrapport, meeloopdagen en nameting) vinden over een periode van zo’n negen weken plaats (figuur 1). Voor een optimale uitvoering en evaluatie van de interventie is het van belang dat deze verschillende stappen worden

uitgevoerd volgens deze planning. Dit betekent dat de buddy uiterlijk een week na de cyberscan het adviesrapport overhandigd aan de mkb'er. In de weken hierna kan de mkb'er gebruikmaken van de meeloopdagen. Zeven weken na de cyberscan vindt de nameting plaats.

Gemeenten en buddy's kunnen in overleg beslissen hoeveel mkb'ers maximaal gelijktijdig worden gescand, waarbij bij elk hierop volgende onderdeel genoeg tijd moet worden gereserveerd voor het tijdig opsturen van alle adviesrapporten en het plaatsvinden van de meeloopdagen. Denkbaar is bijvoorbeeld dat een buddy in de eerste week 10 verschillende mkb bedrijven scant, en buddy's kunnen gedurende hun stage steeds opnieuw aan een cyclus van 9 weken beginnen. Afhankelijk van het aantal mkb'ers dat gebruik maakt van meeloopdagen kunnen buddy's in deze periode alvast een nieuwe cyclus opstarten. De uitvoerende gemeente medewerker (ook wel coördinator genoemd) houdt het overzicht en waarborgt dat dit proces goed verloopt bij alle buddy's.

3.2 De onderdelen van de interventie

3.2.1 Onderdeel 1: De cyberscan

Op het moment dat een mkb'er heeft aangegeven te willen deelnemen aan het project, wordt een cyberscan door de buddy afgenomen. Dit is een gestructureerd interview dat inventariseert hoe het gesteld is met de cybersecurity van dit bedrijf. Dit meetinstrument is grotendeels samengesteld op basis van eerder onderzoek (Bekkers et al., 2020, 2021; Moneva & Leukfeldt, 2022). Het onderdeel 'medewerkers' is gebaseerd op het theoretisch raamwerk voor cyberweerbaargedrag van der Kleij en Leukfeldt (2019). Ook is er een vraag overgenomen uit de Basisscan Cyberweerbaarheid van het DTC (Hoekstra et al., 2021). Nadat de onderzoekers de cyberscan gevormd hadden, is deze nog aangevuld door een cybersecurity professional.

De cyberscan wordt afgenomen door de buddy, die de vragen voorleest en de antwoorden van de ondernemer invoert in de online cyberscan. Aan het begin van de scan controleert de buddy of de deelnemer voldoet aan de inclusiecriteria, namelijk dat de respondent 1) een ondernemer is met personeel (maximaal 250 medewerkers) of werkzaam is binnen een mkb bedrijf en 2) verantwoordelijkheid draagt voor de cybersecurity in de organisatie. Op het moment dat dit niet het geval is, wordt de scan niet bij deze persoon afgenomen en wordt gevraagd naar degene die wel verantwoordelijk is voor de cybersecurity. De scan bestaat vervolgens uit zes onderdelen, te weten: 1. De activiteiten in uw bedrijf; 2. Uw visie op cybersecurity; 3. Levering van ICT; 4. Beleid; 5. Technische maatregelen en 6. Medewerkers.

Om te beginnen brengt de cyberscan het bedrijf zelf in kaart. In Onderdeel 1, "*de activiteiten in uw bedrijf"*, wordt uitgevraagd welke activiteiten er in het bedrijf plaatsvinden die relevant zijn voor

de cybersecurity. Het gaat hier bijvoorbeeld om de apparatuur binnen het bedrijf en de manier waarop deze gebruikt wordt, zowel voor welkdoeleinden als voor privégebruik. Met deze informatie kan de buddy inschatten op welke manieren het bedrijf slachtoffer zou kunnen worden van cybercriminaliteit en welke veiligheidsmaatregelen dus prioriteit hebben.

Vervolgens brengt de cyberscan de prioritering van cybersecurity van het bedrijf in kaarten de eventuele levering van ICT en cybersecurity diensten. In onderdeel 2, "*uw visie op cybersecurity en cyberweerbaarheid"*, wordt achterhaald wat de risicoperceptie van de mkb'er is en hoeverre cybersecurity op dit moment een prioriteit is binnen het bedrijf. In onderdeel 3, *"levering van ICT",* wordt bevraagd of de mkb'er een IT-leverancier heeft en zo ja, of deze ook adequate cybersecurity levert. Daarbij wordt bij mkb'ers die aangeven dat de IT-leverancier ook cybersecurity diensten levert, doorgevraagd wat er precies wel en niet geregeld is.

Hierop volgend meet de cyberscan in welke mate er in het bedrijf reeds cybersecurity maatregelen worden genomen. In onderdeel 4, "*cybersecurity beleid"*, worden het cybersecurity beleid van het bedrijf in kaart gebracht. Het gaat hier bijvoorbeeld om wie er verantwoordelijk is voor de cybersecurity en in hoeverre er een formeel beleid is over relevante aspecten als back-ups en wachtwoorden. Onderdeel 5, "*technische maatregelen",* meet welke technische cybersecurity maatregelen gebruikt worden in het bedrijf, zoals beveiligingssoftware, het automatisch updaten hiervan, 2-factor authenticatie en het bijhouden van toegangsrechten. Ten slotte volgt onderdeel 6, *"medewerkers",* waarin de respondent wordt bevraagd over de kennis, motivatie en gelegenheid die medewerkers in de organisatie hebben over veilig online werken.

Naast dat de cyberscan binnen de interventie de basis legt voor de adviezen en implementatiedagen, fungeert het in dit rapport ook als de nulmeting voor de effectmeting van de interventie. Een aantal vragen uit de cyberscan worden daarom in meer detail besproken in hoofdstuk 4 en de volledige cyberscan is opgenomen in Bijlage 2.

3.2.2 Onderdeel 2: Het adviesrapport

De buddy schrijft het adviesrapport en stuurt dit naar de onderneming uiterlijk een week na het afnemen van de scan. Het doel van het rapport is om de mkb'er te motiveren om de cyberweerbaarheid van de organisatie te vergroten en hen te voorzien in een handelingsperspectief, bestaande uit op-maat-gemaakte adviezen om maatregelen te implementeren.

Het rapport start met risicocommunicatie, waarin het risico van cybercriminaliteit wordt geschreven, het belang van cybersecurity en de manier waarop andere ondernemers zich hiertegen beschermen. Hierbij wordt ingespeeld op twee wetenschappelijk onderbouwde factoren die bijdragen aan de motivatie van mkb'ers om maatregelen te nemen tegen ransomware, namelijk 'subjectieve norm' en 'affectieve respons'. Eerder onderzoek heeft laten zien dat hoe meer ondernemers denken

dat mensen in hun omgeving van ze verwachten dat ze maatregelen nemen (subjectieve norm), en hoe meer ondernemers zich zorgen maken over de risico's van ransomware (affectieve respons), hoe meer ze geneigd zijn zelf-beschermend gedrag ge vertonen (Bekkers et al., 2021).

Het rapport is opgedeeld in 6 onderdelen, overeenkomstig met de bovenstaand aangegeven onderdelen van de cyberscan. In elk onderdeel van het adviesrapport worden de resultaten uit de cyberscan beschreven en wordt aangegeven of er (aanvullende) maatregelen dienen te worden genomen. Ook gaat de buddy in op welke manieren de buddy hierbij zou kunnen helpen tijdens de implementatiedagen. Aan het eind van het adviesrapport volgt een korte samenvatting. Hierin beschrijft de buddy welke adviezen het belangrijkst zijn om in te voeren, (waarbij hij stoelt op de kennis en vaardigheden vanuit de training en instructies in het adviesrapport). Daarnaast wordt ook al een suggestie gedaan van welke acties de buddy zou kunnen uitvoeren tijdens de implementatiedagen.

Hoewel elk rapport op maat geschreven wordt voor een bedrijf op basis van diens cyberscan, bevat de basis al veel standaardteksten die ieder wel of niet van toepassing zijn op een specifiek bedrijf. Deze algemene teksten van het basis adviesrapport zijn opgesteld door een onderzoeker van de Haagse Hogeschool, een medewerker van de gemeente Enschede, de buddy's en de cybersecurity professional. Daarnaast is er ook nog ruimte voor extra aanvulling door de buddy. In het basis rapport staat aangegeven welke teksten verplicht zijn, optioneel zijn en op welke plekken eigen aanvulling mogelijk of nodig is. Dit wordt gedaan door de buddy, gebaseerd op de kennis die de buddy heeft opgedaan tijdens diens opleiding, de trainingen en eventueel in overleg met de cybersecurity professional.

De onderdelen van het adviesrapport zullen worden geïllustreerd met een aantal voorbeelden. In onderdeel 1 beschrijft de buddy welke specifieke aspecten en onderdelen van het bedrijf de risico's op ransomware vergroten (op basis van onderdeel 1 van de cyberscan). In onderdeel 3 van de cyberscan wordt de levering van ICT en cybersecurity diensten in kaart gebracht. Hieruit kan blijken dat de mkb'er a) geen IT-leverancier heeft, b) dat de mkb'er een leverancier heeft die geen of slechts zeer beperkt aandacht besteed aan cybersecurity, c) dat de leverancier wel aandacht aan cybersecurity maar met ruimte voor verbetering of d) dat de leverancier voldoende aandacht besteed aan cybersecurity. Voor ieder scenario zijn voor het adviesrapport standaardteksten geschreven over welke acties ondernomen kunnen worden. Op basis van onderdeel 4 van de cyberscan, gericht op beleid, oordeelt de buddy of het beleid dekkend is voor de activiteiten die binnen het bedrijf worden uitgevoerd. Voor een bedrijf dat in onderdeel 1 bijvoorbeeld aangeeft dat de persoonlijke gegevens van klanten elektronisch worden opgeslagen, dient het cybersecurity beleid te beschrijven op welke manier deze gegevens veilig worden opgeslagen. De buddy maakt een inschatting of de diverse optioneel te adviseren maatregelen belangrijk, effectief en kostenefficiënt zijn voor dit bedrijf. Op het moment dat een buddy een maatregel adviseert, wordt de bijbehorende standaard tekst opgenomen

in het adviesrapport. Tot slot begint onderdeel 6 (medewerkers) begint met een standaard tekst over de vaardigheden anticiperen, detecteren, reageren en leren. Op basis van de scan kan de buddy beoordelen hoe het met elk van de vaardigheden gesteld is bij de medewerkers. Wanneer medewerkers niet voldoende weerbaar zijn met betrekking tot een bepaalde vaardigheid, kan de buddy ook op basis van de cyberscan inschatten of dit het beste kan worden aangepakt op het gebied van het verhogen van kennis, motivatie of gelegenheid voor veilig werken. In het rapport wordt per vaardigheid een advies gegeven met betrekking tot trainingen, beleid en interne communicatie. Per vaardigheid is een standaardtekst opgesteld over welk soort training relevant kan zijn, welke afspraken in het beleid kunnen worden vastgelegd en wat er naar de medewerkers gecommuniceerd kan worden.

3.2.3 Onderdeel 3: Implementatiedagen

De implementatiedagen vinden binnen 2 tot 4 weken na het afnemen van de cyberscan plaats. De buddy's beschrijven in het adviesrapport op welke manieren zij tijdens de implementatiedagen zouden kunnen bijdragen aan het verbeteren van de cyberweerbaarheid van de organisatie. Mkb´ers kiezen vervolgens of ze gebruik willen maken van deze implementatiedagen. Indien dat het geval is, stelt de buddy zich twee dagen (of zestien uren) beschikbaar. Deze tijd wordt verdeeld in voorbereiding (externe locatie) en uitvoering (op locatie bedrijf) De buddy en de mkb'er besluiten samen welke adviezen uit het adviesrapport opgepakt worden tijdens de implementatiedagen.

Er zullen een aantal voorbeelden worden besproken van werkzaamheden van de buddy tijdens de implementatiedagen. Wanneer in onderdeel 3 van de cybersecurity scan is gebleken dat de mkb'er niet precies weet in welke mate de IT-leverancier cybersecurity maatregelen levert, kan de mkb'er de buddy vragen deze levering in kaart te brengen door bijvoorbeeld opgeleverde rapporten van de leverancier te bekijken of een interview houden met de IT-leverancier/afdeling. In het geval dat de ondernemer hulp wil op het gebied van beleid, in kaart gebracht in onderdeel 4 van de scan, kan de buddy bijvoorbeeld in gesprek gaan over wie verantwoordelijk hoort te zijn voor de cybersecurity, helpen bij het opstellen van een bedrijfscontinuïteitsplan en het opstellen of aanpassen van het cybersecurity beleidsplan. In geval dat de mkb'er de geadviseerde technische maatregelen uit onderdeel 5 wil implementeren, kan de buddy helpen met het maken van een prioriteitsstelling en bij het implementeren. In het geval dat de mkb'er de vaardigheden van de medewerkers wil verbeteren, zoals in kaart gebracht in onderdeel 6 van de scan, kan de buddy adviseren over een communicatieplan, beleidsaanpassingen en het uitrollen van trainingen. De buddy kan adviseren over passende trainingen van derden, maar ook zelf een training geven.

3.2.4 Onderdeel 4: Nameting

Het is wenselijk om de effectiviteit van de interventie in kaart te brengen. Zeven weken na het afnemen van de eerste cyberscan, wordt daarom de cyberscan opnieuw afgenomen. Deze meting dient als nameting en is voornamelijk bedoeld om de effectiviteit van de interventie en de tevredenheid hierover te meten. De volledige vragenlijst is te lezen in Bijlage 3. Deze meting draagt dus in principe niet meer bij aan het motiveren tot een gedragsverandering van de mkb'er. Omdat de nameting vergeleken dient te worden met de cyberscan, komen de vragen grotendeels hiermee overeen. We raden dan ook aan dit aan de respondenten mede te delen voorafgaand aan het afnemen van de scan, zodat zij begrijpen waarom dezelfde vragen nogmaals moeten beantwoorden.

De nameting bestaat uit vier onderdelen, te weten 1. Uw visie op cybersecurity, 2. Levering van ICT, 3. Cybersecurity beleid in uw organisatie, 4. Technische maatregelen, 5. Medewerkers en 6. Uw ervaring met dit project. Onderdeel 1 tot en met 5 in de nameting komen overeen met Onderdeel 2 tot en met 6 in de cyberscan. Hierdoor kan worden nagegaan welke van de adviezen van de buddy geïmplementeerd zijn.

In Onderdeel 6 van de nameting ("Uw ervaring met dit project") worden een aantal nieuwe vragen gesteld over het project. De respondenten kunnen in dit onderdeel aangeven hoe tevreden ze over verschillende aspecten van de interventie zijn, in hoeverre ze de interventie effectief geacht hebben en welke mogelijke verbeterpunten zij nog zien. De resultaten van dit onderdeel zijn in deze pilot vooral gebruikt om de interventie te verbeteren. Het zou echter bij toekomstige inzet van de interventie nog steeds nuttig kunnen zijn deze vragen te stellen, zodat het project kan blijven ontwikkelen.

3.3 Betrokken partijen

3.3.1 De gemeente

De interventie is ontwikkeld voor gemeenten of andere lokale overheden om de cyberweerbaarheid van het midden en klein bedrijf binnen hun regio te vergroten. De (beleids)medewerker van een gemeente die de interventie inzet, kortweg de coördinator genoemd, start met het aantrekken van buddy's (studenten die als externe stagiair worden aangesteld) en een cybersecurity professional die deze buddy's traint en begeleidt en een ruimte voor deze trainingen (veelal mogelijk in ruimte van gemeentehuis). De kosten voor de gemeente bestaat uit de (loon)kosten voor de stagiaires, het inhuren van de cybersecurity professional en het voor een aantal uren vrijstellen van een (beleids)medewerker om als coördinator de werkzaamheden van de buddy's te overzien en monitoren en het contact met de cybersecurity professional te onderhouden. Het is ook mogelijk dat verschillende gemeenten gezamenlijk de interventie uitvoeren (zoals in de pilot is gedaan, beschreven

in hoofdstuk 4), waarbij de buddy's uit verschillende gemeenten samen getraind worden, de coördinatie gecentraliseerd is en de buddy's elk in hun eigen gemeenten ingezet worden.

3.3.2 De cybersecurity professional

Voor de waarborging van de inhoudelijke kwaliteit van het project wordt door de gemeente een cybersecurity professional ingehuurd[8]. Deze professional geeft de twee trainingen voor buddy's over het schrijven van het adviesrapport en potentiële activiteiten tijdens de meeloopdagen, leest de eerste door de buddy's geschreven adviesrapporten voordat deze worden verstuurd naar de mkb'ers, is tijdens de looptijd van het project (online) aanwezig bij enkele "Q&A" bijeenkomsten waarin de buddy's met de professional kunnen sparren over inhoudelijke cybersecurity vraagstukken die zij zijn tegengekomen bij de mkb'ers in het project en is tot slot tussendoor bereikbaar voor inhoudelijke vragen van de buddy's.

3.3.3 De buddy's

De buddy is een student van een cybersecurity-gerelateerde studie[9]. Voorafgaand aan het uitvoeren van de interventie tekent de buddy een geheimhoudingsverklaring en krijgt de student een training van een cybersecurity professional en de coördinator (van de gemeente) over het afnemen van de metingen, het schrijven van een adviesrapport en het uitvoeren van de meeloopdagen, waarbij bij elk onderdeel aandacht wordt besteed aan omgaan met vertrouwelijke en gevoelige bedrijfsinformatie. Gedurende het uitvoeren van de interventie blijven de professional en coördinator beschikbaar voor vragen van de buddy's. De buddy voert het project uit als externe stagiair bij een gemeente. Deze buddy benadert dus ook uitsluitend mkb´ers die gevestigd zijn in de gemeente waar diegene stage loopt.

3.3.4 De mkb'ers

De interventie is specifiek gericht op mkb'ers, oftewel bedrijven met tussen de 1 en 250 werknemers. Het is mogelijk de mkb'ers in de gemeente op verschillende manieren te benaderen met het aanbod om deel te nemen aan de interventie. Dit kan worden gedaan door de buddy en gemeente waar deze werkzaam is, bijvoorbeeld via de mail, telefoon of door face-to-face gesprekken. Voor het werven hebben buddy's ook flyers ter beschikking waarin beknopt staat uitgelegd wat de interventie inhoudt en wat er van de mkb'er verwacht wordt. Gemeenten kunnen ook direct zelf mkb'ers benaderen, bijvoorbeeld door middel van netwerkcontacten, sociale media berichten, persberichten, flyers en

[8] Tijdens de pilot bedroeg dit in totaal 16 uur (2x training van 4 uur, 2x Q&A van 1 uur, lezen van 8 rapporten (2 per buddy) en tussendoor vragen beantwoorden per email of telefoon.

[9] Voorbeelden van cybersecurity-gerelateerde studies zijn HBO ICT, Information Security Management, Security management en Integrale Veiligheidskunde (mits er sprake is van affiniteit met en vakken over cybersecurity).

posters. Andere mogelijkheden zijn het benaderen van collectieven zoals bedrijventerreinen, PVO's (Platform Veilig Ondernemen) of belangenverenigingen en het organiseren van informatieavonden voor mkb'ers over cybersecurity waarbij zij zichzelf direct kunnen opgeven voor het 'MKB cyber buddy's' project.

4. Verloop van de pilot

In het vorige hoofdstuk is de interventie “MKB Cyber Buddy’s” beschreven. In dit hoofdstuk beschrijven we hoe de pilot van de interventie is verlopen die in de eerste helft van 2022 is uitgevoerd. Het hoofdstuk gaat in op de werving van respondenten en de corresponderende responspercentages (4.1), het verloop van de projectstappen (4.2) en de eigenschappen van de deelnemende mkb’ers (4.3). Het hoofdstuk sluit af met een uiteenzetting van de geleerde lessen tijdens de uitvoering van de pilot (4.4).

4.1 Werving en respons

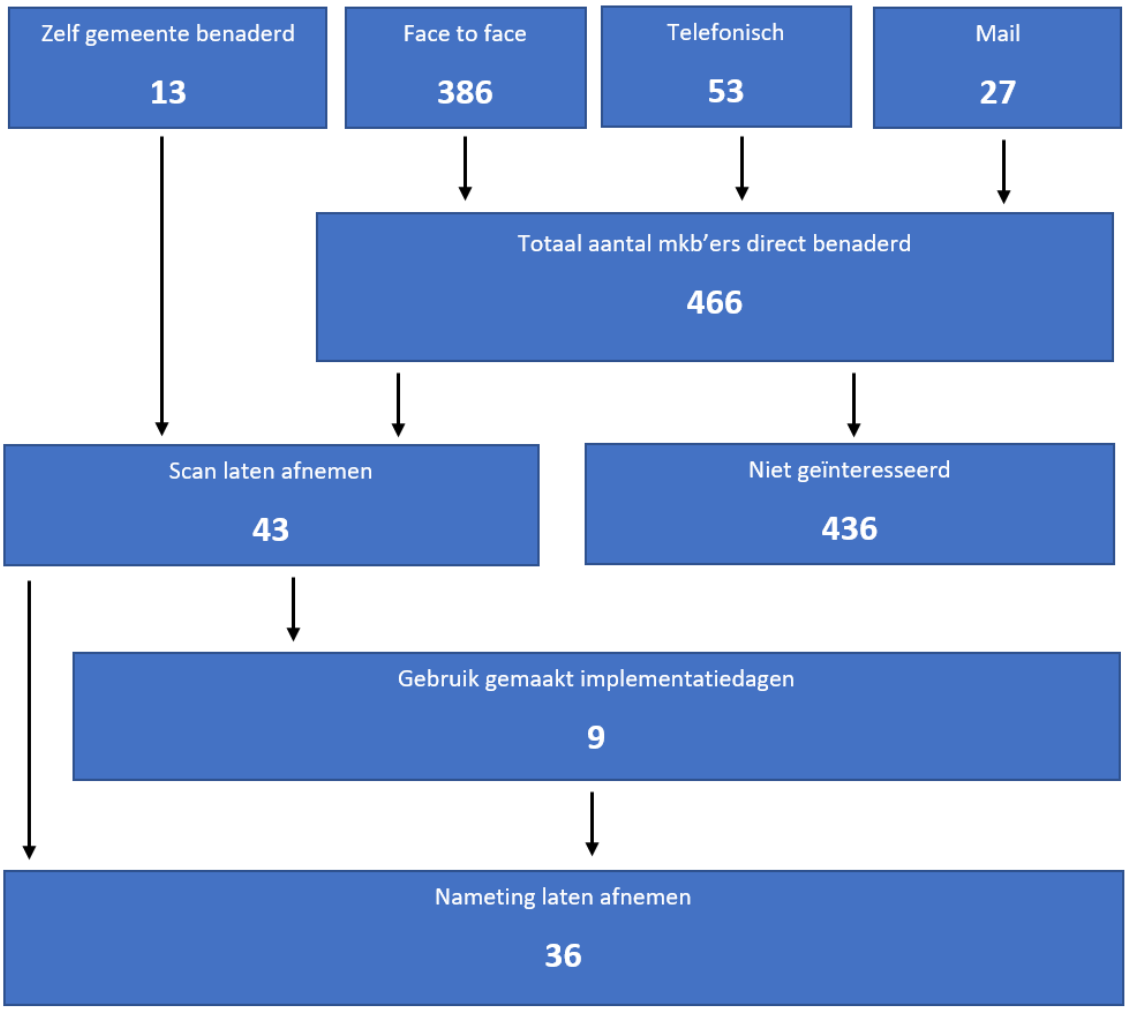
De pilot is uitgevoerd van 1 februari 2022 tot en met 15 juli 2022. Binnen deze periode hebben twee rondes van 8 weken plaatsgevonden (zie Figuur 1), waarbij in beide ronde mkb’ers geworven zijn. De eerste ronde liep van februari tot april 2022 en is uitgevoerd door vier buddy’s. De twee ronde liep van april tot juli 2022 en is uitgevoerd door drie buddy’s.

In Figuur 2 is schematisch weergegeven hoe het wervingsproces en het uitvoeren van de interventie is verlopen met betrekking tot de participatie van de respondenten. Zoals in dit figuur te zien is, zijn mkb’ers op drie verschillende manieren benaderd door de buddy’s, te weten, (1) face-to-face, (2) telefonisch en (3) per mail. In het schema is weergegeven op welke manieren voor mkb’ers *in eerste instantie* benaderd zijn. Dit betekent dus dat voor bijvoorbeeld 370 mkb’ers hun eerste contact met een buddy face-to-face plaats vond. Veel mkb’ers zijn later ook nog per mail of telefonisch benaderd, bijvoorbeeld omdat ze aan hadden gegeven geïnteresseerd te zijn, maar hun deelname nog niet hadden toegezegd tijdens het face-to-face contact moment.

In totaal zijn gedurende deze pilot 498 mkb’ers benaderd om deel te nemen aan de interventie. Hiervan hebben 43 ook uiteindelijk de scan laten afnemen. Hiervan hebben 13 mkb’ers aan het project meegedaan nadat zij zichzelf hebben gemeld bij de gemeente Utrecht met interesse om aan een project gerelateerd aan cybersecurity mee te doen. De andere 30 mkb’ers (van de 43 deelnemers) hebben meegedaan nadat zij actief zijn benaderd door een buddy. Dit betekent dat er bij mkb’ers die werden benaderd dus een respons van 6,4% en een non-respons is van 93,6%. Opvallend was dat de non-respons tussen de twee rondes in grote mate verschilde (Bijlage 4). Gedurende de eerste ronde was de non-respons namelijk 86,5%, terwijl dit tijdens ronde twee een non-respons was van 99,2%. Bijlage 4 geeft de respons van de werving per ronde weer. Het voornaamste verschil tussen de twee periodes was de tijd van het jaar, waarbij de meivakantie viel in de tweede wervingsrondes waardoor minder bezetting als reden voor het niet deelnemen aan het project werd opgegeven. Daarnaast werd in de tweede ronde relatief vaker (dan in de wervingsronde eerder in het jaar) aangegeven dat deze tijd van het jaar erg druk was voor het bedrijf en dat er geen tijd was voor het project.

Van de 43 mkb'ers die de voormeting hebben laten afnemen hebben er 9 (23,26%) gebruik gemaakt van de implementatiedagen. Mkb'ers die zichzelf hadden aangemeld maakten gemiddeld ongeveer even vaak gebruik van de implementatiedagen als de mkb'ers die zijn benaderd door buddy's. Uiteindelijk hebben 36 mkb'ers ook de nameting laten afnemen (83,7%). Redenen voor uitval waren voornamelijk dat mkb'ers nog geen tijd hadden gehad het adviesrapport op te pakken, door bijvoorbeeld een verhuizing van het bedrijf of andere prioriteiten.

Figuur 2. Pijlenschema respons MKB Cyber Buddy's



4.2 Verloop van project stappen

De stappen van de interventie zijn uitgevoerd zoals beoogd (beschreven in hoofdstuk 3). Voorafgaand aan deelname werd de respondent geïnformeerd over de deelname aan het onderzoek en over hoe de antwoorden en gegevens van de respondent en het bedrijf geanonimiseerd verwerkt zouden worden. Hierna werd de respondent gevraagd om toestemming voor deelname aan het onderzoek.

Om te verzekeren dat alle scans geanonimiseerd waren hebben de buddy's voor aan elke respondent een code toegewezen. Door deze code zowel bij de cyberscan als bij de nameting te noteren, konden de metingen geanonimiseerd aan elkaar gekoppeld worden. Op het moment dat een mkb bedrijf aangaf deel te willen nemen aan het project, werd een afspraak voor de cyberscan ingepland met degene die verantwoordelijk is voor cybersecurity of werd de scan direct afgenomen.

De buddy controleerde aan het begin van elke scan of de respondent in een mkb onderneming werkzaam was en verantwoordelijk was voor de cybersecurity.

Gedurende het afnemen van de scan las de buddy de vragen voor en noteerde hierna de antwoorden van de respondenten op de computer. Dit gebeurde door middel van een online versie van de vragenlijst via het programma Questback. De nameting is zon zeven weken na de cyberscan uitgevoerd. Op het moment van de nameting, had de respondent het adviesrapport minstens zes weken in handen en was er gelegenheid om gebruik te maken van de implementatiedagen. De nameting is volgens dezelfde procedure afgenomen als de cyberscan, door de buddy's met behulp van Questback.

4.3 Respondenten

In totaal hebben 43 bedrijven de voormeting van de cyberscan laten afnemen. Uiteindelijk hebben 36 bedrijven ook de nameting laten uitvoeren. De resultaten uit dit rapport hebben betrekking op deze 36 mkb'ers. In Tabel 2 is de beschrijvende data van de respondenten weergegeven. Meer dan de helft van de participerende organisaties heeft 1 tot 10 medewerkers (60%), een kwart heeft tussen de 11 en 50 medewerkers (25,7%) en het kleinste deel heeft tussen de 51 en 250 medewerkers (14,3%). Deelnemende bedrijven zijn overwegend gevestigd in Utrecht (68,6%). Een kleiner deel ligt in Den Helder (17,1%) en Enschede (14,3%). De meeste bedrijven zijn actief in de sector *handel en dienstverlening* (28,6%). Daarna zijn de meest vertegenwoordigde sectoren *ICT* (20,0%) en *toerisme en horeca* (17,1%). Een overige 34,4% is gelijkmatig verdeeld over vijf overige sectoren, zoals gezondheidszorg en techniek.

Tabel 2. Beschrijvende data van de respondenten van de Cyberscan (N = 36)

Eigenschappen		Respondenten	
		N	Percentage
Functie respondent	Ondernemer met personeel (max. 250) en draagt verantwoordelijkheid over de cybersecurity	22	61,1%
	Werkzaam binnen een mkb bedrijf en draagt verantwoordelijkheid over de cybersecurity	14	38.9%
Aantal medewerkers	1 – 10	21	58,3%
	11 – 50	10	27,8%
	51 – 250	5	13,9%
Gemeente	Utrecht	25	69,4%
	Den Helder	6	16,7%
	Enschede	5	13,9%
Sector	Handel en dienstverlening	10	27,8%
	ICT	7	19,4%
	Toerisme, recreatie en horeca	6	16,7%
	Gezondheidszorg en welzijn	5	13,9%
	Techniek, productie en bouw	4	11,1%
	Overig	4	11,1%

4.4 Geleerde lessen

Gedurende het uitvoeren van de pilot is gebleken dat een aantal zaken in de praktijk anders zijn gelopen dan ze vooraf (op papier) gepland waren. Hieruit zijn diverse lessen geleerd, die input leveren voor aanpassingen van de interventie voor eventuele toekomstige uitvoeringen. In deze paragraaf zal beschreven worden welke lessen gedurende de pilot geleerd zijn.

Werven

- Gedurende de pilot is gebleken dat de bereidwilligheid van mkb'ers om mee te doen aan het project heel laag is als ze "koud" worden aangesproken; zonder dat zij hiervoor over het project hadden gehoord of zelf eerder interesse hadden geuit. Mkb'ers die al eerder met de gemeente contact hadden gehad over cybersecurity (projecten) waren veel vaker bereid om mee te doen.

- Bij de eerste wervingsronde is achteraf gebleken dat de buddy's minder vaak mkb'ers face-to-face hadden aangesproken dan dat wenselijk was. Dit had deels te maken met Corona gerelateerde gedragsregels, maar mogelijk ook doordat de opdracht om vooral face-to-face te benaderen multi-interpretabel is en er vooraf geen minimaal aantal wervingsdagen op locatie is afgesproken. Hieruit blijkt dat er preciezere afspraken tussen de uitvoerders van het project en de buddy's moeten worden gemaakt, bijvoorbeeld over hoeveel bedrijven fysiek benaderd dienen te worden en hoeveel wervingsdagen op locatie er dienen plaats te vinden.
- Ook kan het vooraf afspraken maken over eventuele reiskosten naar gemeenten buiten de regio van de onderwijsinstelling van de buddy duidelijkheid scheppen over welke input er wordt verwacht vanuit de buddy's. Na de eerste wervingsronde bleek dat het aantal dagen waarop de buddy's op locatie respondenten hadden geworven lager was bij buddy's die niet gratis van het openbaar vervoer gebruik konden maken.
- In een gemeente bleek dat er in dezelfde periode een bedrijf actief was die een soortgelijke cyberscan aanbood, gesubsidieerd vanuit de gemeente. Dit was in sommige gevallen de reden dat bedrijven niet meededen aan het project. Het is daarom wenselijk dat binnen de gemeente intern afstemmen over de timing van verschillende projecten.
- Wanneer de uitvoerder van de interventie inzicht wenst in het aantal en soort bedrijven dat benaderd is voor het project, is het wenselijk om de buddy's hun wervingsverslag te laten bijhouden tijdens het werven en niet enkel achteraf te laten invullen.

Communicatie en verwachtingsmanagement met deelnemende mkb'ers

- In de eerste wervingsronde hadden een aantal gemeentes hun eigen flyers en sociale media berichten gemaakt om bedrijven zich te laten aanmelden. In sommige gemeentes waren de bedrijven die gereageerd hadden op deze flyers en berichten minder op de hoogte van wat het project inhield, dan degenen die door de buddy benaderd waren. Zij wisten bijvoorbeeld vaak niet dat er nog een rapport en meeloopdagen zouden volgen. In de tweede wervingsronde is daarom gebruik gemaakt van een standaard informatiefolder.
- Sommige mkb'ers hadden voorafgaand aan hun deelname van het project een andere verwachting van de cyberscan dan wat deze in de praktijk bleek in te houden. Verschillende respondenten hadden verwacht dat het zou gaan om bijvoorbeeld een digitale scan van de systemen of zelfs een penetratietest. Sommige respondenten waren teleurgesteld toen bleek dat de cyberscan een vragenlijst was.
- Het is efficiënt gebleken om mkb'ers voorafgaand aan de interventie duidelijk te maken wat de tijdslijn is van het project is, zodat zij zich kunnen voorbereiden op de ontvangst van het

adviesrapport, dit tijdig kunnen lezen en ook tijdig een afspraak voor de implementatiedagen kunnen inplannen.

Afnemen van de cyberscan

- Respondenten die aangaven dat de scan gelijk uitgevoerd kon worden wanneer de buddy ze face-to-face benaderde, waren sneller klaar dan degenen die hiervoor een afspraak lieten inplannen.
- Een scan uitvoeren door middel van videobellen gaat een stuk langzamer dan wanneer dit face-to-face gedaan wordt.
- In gevallen van een lange vragenmatrix in de cyberscan, bleek het vaak praktischer om deze door de respondent te laten invullen, dan om de buddy alles te laten voorlezen en invullen.

Adviesrapporten

- Het was voor de buddy's in sommige gevallen lastig om de adviesrapporten persoonlijk te maken, omdat er veel in dezelfde periode geschreven moesten worden en omdat de scans allemaal een week ervoor waren afgenomen. Hierdoor waren sommige specifieke casussen van bedrijven minder helder ten tijde van het schrijven van het rapport.

Samenwerking en communicatie tussen uitvoerders

- Het veldwerkschema (dat per week weergeeft welk projectonderdeel aan de beurt is per bedrijf) bleek in de praktijk soms lastig voor buddy's om te volgen. Dat er een veldwerk coördinator beschikbaar was voor vragen bleek niet in alle gevallen voldoende om dit op te lossen. Een training over het aanpakken van de werving (naast de training over de cyberscan en het adviesrapport) en regelmatige begeleiding is wenselijk.
- Wanneer niet volledig duidelijk is afgestemd welke verantwoordelijkheden en taken binnen het project liggen bij de verschillende actoren (b.v. uitvoerende gemeente medewerker (coördinator), andere gemeentemedewerkers, cybersecurity professional), kan dit problemen en onduidelijkheid in de samenwerking veroorzaken.

Timing van de projectonderdelen

- Mkb'ers hebben geregeld langer dan een week nodig om het adviesrapport te lezen.
- Mkb'ers willen vaak het besluit van wel of geen implementatiedagen laten afhangen van de inhoud van het adviesrapport.

- Het inplannen van de implementatiedagen bleek langer te duren dan voorheen verwacht was. In principe hadden de mkb'ers een week om het rapport te lezen en aan te geven of ze implementatiedagen wilden en wanneer deze konden plaatsvinden, maar in de praktijk duurde dit vaak langer. Daardoor werd de eerst week van implementatiedagen in het rooster van de buddy vaak nauwelijks gebruikt en werden de latere weken in het rooster drukker.
- Veel deelnemende mkb'ers gaven aan het erg druk te hebben, waardoor zij maar een beperkt aantal dagen konden aanwijzen waarop de implementatiedagen konden plaatsvinden. Dit was soms lastig te matchen met het rooster van de buddy.

Inhoud van de cyberscan

- De vragenlijst mag vaker de optie 'weet ik niet' hebben dan dat die in dit meetinstrument had. Bijvoorbeeld bij de vraag of de IT-leverancier certificaten over cybersecurity heeft.
- De tevredenheid over de implementatiedagen dient een 'niet van toepassing' optie te hebben voor mkb'ers die deze optie niet gebruikt hebben.
- De nameting kan mogelijk eenvoudiger worden vormgegeven. Nu moeten buddy's het adviesrapport erbij houden en invullen wat ze wel of niet geadviseerd hebben.
- Bedrijven kunnen nieuwe maatregelen ook uit zichzelf invoeren, in plaats van vanwege het adviesrapport. Bij de nameting kan dus ook nog een optie worden toegevoegd dat het zelf is ingevoerd en niet vanwege de interventie.

5. Methode voor de effectiviteitsmeting

Dit hoofdstuk beschrijft de manier waarop centrale concepten zijn gemeten (5.1) en de analyses hebben plaatsgevonden (5.2.)

5.1 Operationalisaties

Cybersecurity beleid

De documentatie van het cybersecurity beleid is gemeten met twee vragen. De eerste vraag is "*Heeft uw organisatie een formeel beleid met betrekking tot cybersecurity risico's (zoals over het gebruik van persoonlijke apparaten, of een back-up beleid, of een wachtwoordbeleid)?*" met als antwoordopties "*Ja*" en "*Nee*". De tweede vraag is "*Wanneer is uw beleid of zijn uw richtlijnen voor cybersecurity voor het laatst bijgewerkt of herzien om te controleren of alles up-to-date is?*".

Het management aspect van het cybersecurity beleid is gemeten met twee vragen. Als eerste is een itemlijst gepresenteerd met de vraag "*Welke van de volgende afspraken op het gebied van beheer of risicomanagement heeft u reeds ingevoerd?*". De lijst bevat 4 afspraken (Bijlage 2) waarop de respondent kan antwoorden met "*Ja*", "*Nee*" en "*Weet ik niet*". Ook kan de respondent aangeven welke overige relevante afspraken zijn gemaakt in het bedrijf.

Vervolgens is een itemlijst van potentiële 11 aspecten in een cybersecurity beleid doorgelopen, met de vraag "*Welke van de volgende aspecten vallen onder uw cybersecurity beleid? In ons beleid zijn er afspraken over...*" (Bijlage 2). Voor elk van de 11 afspraken kan de respondent antwoorden met "*Ja*", "*Nee*" en "*Weet ik niet*". De respondent kan overige relevante afspraken toevoegen.

Als laatste wordt in dit onderdeel gevraagd "*Heeft uw organisatie relevante certificaten (zoals ISO27001)?*" met de antwoordopties "*Ja*" en "*Nee*".

Technische maatregelen

Om de hoeveelheid technische maatregelen van het bedrijf te meten, is een itemlijst van 28 mogelijke maatregelen gepresenteerd met de vraag "*Welke van de volgende controlemaatregelen heeft uw bedrijf ingevoerd?*" (Bijlage 2). Voor elk van de 28 items kan de respondent antwoorden met "*Ja*", "*Nee*" en "*Weet ik niet*". De respondent kan ook overige relevante technische maatregelen toevoegen.

Medewerkers

De vaardigheden van de medewerkers zijn gemeten op het gebied van de vier vaardigheden van cyberweerbaarheid, namelijk anticiperen, detecteren, reageren en leren. Binnen elk onderdeel is ook gemeten in hoeverre de medewerkers de capaciteit, motivatie en gelegenheid tot het uitvoeren van

deze gedragingen hebben (op basis van de COM-B theorie). Dit is gedaan met 27 stellingen met de vraag "*In hoeverre bent u het eens met de volgende stellingen?*" (Bijlage 2). Per stelling kan geantwoord worden met een vijfpuntenschaal met categorieën van "*Helemaal mee oneens*" (1) tot "*Helemaal mee eens*" (5).

Anticiperen. Het aspect anticiperen is gemeten met vijf stellingen over de manieren waarop medewerkers cyberaanvallen kunnen voorkomen. Hiervan gaan twee stellingen over de capaciteit om te anticiperen, een over de gelegenheid en twee over de motivatie.

Detecteren. Het aspect detecteren is gemeten met zeven stellingen over de manieren waarop medewerkers cyberaanvallen kunnen herkennen. Hiervan gaan drie stellingen over de capaciteit, twee over de gelegenheid en twee over de motivatie.

Reageren. Het aspect reageren is gemeten met zes stellingen van de manieren waarop medewerkers kunnen reageren op cybercrime. Hiervan gaan twee stellingen over capaciteit, twee over gelegenheid en twee over motivatie.

Leren. Het aspect leren is gemeten met negen stellingen over de manieren waarop medewerkers kunnen leren van cybercriminaliteit. Hiervan gaan drie stellingen over capaciteit, drie over gelegenheid en drie over motivatie.

Risicoperceptie

De risicoperceptie van de respondent is gemeten met de vragen "*In hoeverre maakt u zich zorgen over de kans dat uw bedrijf slachtoffer wordt van cybercriminaliteit?"* en "*In hoeverre maakt u zich zorgen over de mogelijke schade die uw bedrijf oploopt door slachtofferschap van cybercriminaliteit?*". De antwoordopties voor beide vragen is een vijfpuntschaal met categorieën van "*Helemaal niet*" (1) tot "*Heel veel*" (5).

De prioriteit van cybersecurity in het bedrijf is gemeten met de vraag "*Hoe hoog of laag is voor u de prioriteit van cybersecurity van uw organisatie?*" met als antwoordopties een vierpuntschaal van "*Zeer hoog*" (1) tot "*Erg laag*" (4) en ook de optie "*Weet ik niet*". Als laatste is gevraagd in hoeverre het bedrijf bezig is kwetsbaarheden in de cyberweerbaarheid in beeld te brengen (bijlage 2).

Advies is geïmplementeerd (ja/nee)

Als eerste zijn er variabelen gemaakt waarin af te leiden was of een bepaald advies wel of niet gegeven was door de buddy (door de eerste vier antwoordopties van de nameting (die aangeven in welke mate een geadviseerde maatregel is opgepakt) per maatregel samen te voegen tot 'geadviseerd' en de laatste antwoordoptie te zien als 'niet geadviseerd'). Ook zijn variabelen aangemaakt waarmee per advies te zien was of deze ook daadwerkelijk geïmplementeerd was, door de eerste drie

antwoordopties samen te voegen tot ‘advies geïmplementeerd’, de vierde antwoordoptie te zien als ‘niet geïmplementeerd’ en de vijfde antwoordoptie (niet geadviseerd) als missing te zien.

Zowel de items over de gegeven adviezen als over de geïmplementeerde adviezen zijn vervolgens per onderdeel bij elkaar opgeteld. Zo kon voor ieder onderdeel gezien worden hoe veel adviezen er in totaal gegeven zijn en hoe veel gegeven adviezen er in totaal geïmplementeerd zijn.

Vervolgens is ook een nieuwe variabele aangemaakt waarbij het aantal geïmplementeerde adviezen gedeeld is door het aantal gegeven adviezen. Met deze variabele kon berekend worden welk percentage van de adviezen per onderdeel geïmplementeerd zijn.

5.2 Analyse

In dit rapport is beschrijvende statistiek gebruikt om in kaart te brengen in welke mate mkb’ers maatregelen voor en na de interventie hebben genomen. Ook is getoetst of de interventie tot een significant verschil bij de ondernemers geleid heeft in het aantal genomen maatregelen. Bij de onderdelen *beleid* en *technische maatregelen* is met een gepaarde t-toets getest of de mkb’ers na de interventie een significant hoger aantal maatregelen hadden dan voorafgaand aan de interventie. Deze toets kon niet uitgevoerd worden op het onderdeel *medewerkers*, omdat dit onderdeel tijdens de voormeting op een andere schaal gemeten is. Voor het onderdeel *risico* is met een gepaarde t-toets getoetst of er een significant verschil was in de antwoorden op deze stellingen voor en na de interventie.

Daarnaast is niet alleen gekeken naar de aantallen van de geïmplementeerde en gegeven adviezen, maar is ook beschreven welke adviezen het meest en minst gegeven en geïmplementeerd zijn.

6. Resultaten van de pilot

In dit hoofdstuk beschrijven we de resultaten van de pilot. Hierbij zal eerst ingegaan worden op de adviezen die buddy's gegeven hebben in de adviesrapporten en in welke mate deze vervolgens geïmplementeerd zijn door de mkb'ers (6.1). Vervolgens zal worden beschreven welke adviezen het meest en minst gegeven en geïmplementeerd zijn (6.2). Hierna gaan we in op de risicoperceptie van mkb'ers ten tijde van de voor- en nameting (6.3). Ten slotte zullen vergelijkingen worden gemaakt tussen groepen mkb'ers, bijvoorbeeld voor branche en aantal medewerkers, in het implementeren van geadviseerde maatregelen (6.4).

6.1 Gemiddeld aantal gegeven en geïmplementeerde adviezen

In Tabel 3 is weergegeven hoeveel maatregelen minimaal, maximaal en gemiddeld geadviseerd zijn en welk percentage van deze adviezen gemiddeld werd ingevoerd. Hierbij is onderscheid gemaakt tussen maatregelen die betrekking hebben op beleid, techniek en medewerkers.

Ten eerste geeft de tabel informatie over het aantal minimaal en maximaal geadviseerde maatregelen. Voor ieder onderdeel is het voorgekomen dat er geen (0) adviezen gegeven zijn. Wanneer een advies niet gegeven is, betekent dit dat de mkb'er in kwestie deze maatregel al adequaat geïmplementeerd had ten tijde van de cyberscan, of dat deze maatregel niet relevant was voor dit specifieke bedrijf. Als het aankomt op het maximaal aantal gegeven adviezen, blijkt dat het voor bijna ieder onderdeel voorgekomen is dat een mkb'er alle mogelijke adviezen uit dit onderdeel gekregen heeft. Dit is alleen niet het geval geweest bij techniek, waar het maximaal aantal gegeven adviezen 28 is, terwijl het maximaal aantal mogelijke adviezen 29 is.

Gemiddeld hebben de buddy's aan mkb'ers in totaal 35.5 maatregelen geadviseerd, verdeeld over beleids-, technische- en medewerker maatregelen. Het vaakst werden maatregelen gericht op medewerkers geadviseerd (gemiddeld 16,6 van de 27 mogelijke adviezen), gevolgd door technische maatregelen (gemiddeld 10,5 van de 29 mogelijke adviezen) en beleid (gemiddeld 8,33 van de 17 mogelijke adviezen).

Van alle gegeven adviezen, hebben de mkb'ers gemiddeld aangegeven 34,3% ingevoerd te hebben ten tijde van de nameting. Bij beleidsmaatregelen implementeren de mkb'ers gemiddeld ongeveer een derde (35,8%) van de geadviseerde maatregelen, waarbij maatregelen gericht op *management* in iets meer dan een kwart van de gevallen werd ingevoerd (28,2%) en maatregelen gericht op beleidsdocumentatie in iets hogere mate (31,9%). Ten tijde van de voormeting hadden 13 ondernemingen een formeel cybersecurity beleid en ten tijde van de nameting waren dit er 14 (niet in tabel). Ook op het gebied van maatregelen gericht op techniek is ongeveer een derde

geïmplementeerd (34,0%). Op het onderdeel medewerkers is zowel gekeken naar de 27 maatregelen in totaal, maar ook daarbinnen naar de maatregelen die aansloten bij de onderdelen anticiperen, detecteren, reageren of leren en de maatregelen die aansloten bij capaciteit, gelegenheid of motivatie. In totaal is iets minder dan een derde van de geadviseerde maatregelen gericht op medewerkers ingevoerd (29,3%). Dit gemiddelde kwam overeen bij de meeste onderdelen. Uitzonderingen hierbij zijn de vaardigheid leren (21.9%) en de COM-B factor gelegenheid (23.8%). Bij deze factoren werden gegeven maatregelen relatief minder vaak geïmplementeerd.

Tabel 3. Het gemiddeld aantal gegeven en ingevoerde adviezen per onderdeel (N = 36)

Adviezen		**Min. aantal geadviseerd**	**Max. aantal geadviseerd**	**Gem. aantal geadviseerd**	**Perc. ingevoerd**
Beleid	Management	0	4	1,72	28,2%
	Documentatie	0	12	6,61	31,9%
Techniek	Totaal	0	28	10,53	34,0%
Medewerkers	Totaal	0	27	16,64	29,3%
Vaardigheden voor cyberweerbaarheid	Anticiperen	0	5	2,67	29,7%
	Detecteren	0	7	5,03	30,3%
	Reageren	0	6	3,44	32,1%
	Leren	0	9	5,50	21,9%
COM-B	Capaciteit	0	10	6,33	32,3%
	Gelegenheid	0	8	4,78	23,8%
	Motivatie	0	9	5,53	32,4%
Alle maatregelen	Totaal	1	70	35,50	34,27%

Met een gepaarde t-toets is berekend in hoeverre de interventie geleid heeft tot een significant verschil in het aantal adviezen waarvan mkb'ers hebben aangegeven dat ze zijn ingevoerd[10]. Wanneer wordt toegespitst op beleidsmaatregelen op het gebied van management is te zien dat voorafgaand aan de interventie gemiddeld 1,44 maatregelen genomen werden (SD = 1,23). Na afloop van de interventie was dit 1,81 maatregelen (SD = 1,53). Het gaat hier om een significante toename van 25,7% ($t(35)= -2.996$; $p < 0,01$). Voor gedocumenteerde beleidsmaatregelen is gevonden dat er voorafgaand aan de eerste cyberscan gemiddeld 2,86 maatregelen waren genomen (SD = 4,18). Dit waren na afloop 4,94 maatregelen (SD = 4,15). Het gaat hier om een significante toename van 72,7% ($t(35)= -3,820$; p

[10] Dit is niet gedaan voor het aspect *Medewerkers* omdat dit vanwege het verschil in schalen bij de voor- en nameting niet mogelijk is.

< 0,001). Wat betreft technische maatregelen, namen mkb'ers voorafgaand aan de interventie gemiddeld 13,72 maatregelen (SD = 6,27). Na de interventie waren dit er 16,72 (SD = 6,72). Dit bedraagt een significante toename van 21,9% (t(35) = -4,120; p < 0,001).

Tabel 4. T-test resultaten van verschillen in gemiddeld aantal zelfbeschermende maatregelen tussen de voormeting en de nameting (N = 36)

		Voormeting		Nameting		Toename (%)	*t-waarde*	*df*
		M	*SD*	*M*	*SD*			
Beleid	Management	1,44	1,23	1,81	1,39	0,37 (25.7%)	-2,996**	35
	Documentatie	2,86	4,18	4,94	4,15	2,08 (72,7%)	-3,820***	35
Techniek	Totaal	13,72	6,27	16.72	6,72	3,00 (21,9%)	-4,120***	35

**p < 0,05; **p < 0,01 ***p<0,001*

6.2 Type adviezen dat wordt gegeven en ingevoerd

In Tabel 5 is weergegeven welke adviezen per onderdeel het vaakst en het minst vaak reeds ingevoerd waren ten tijde van de eerste cyberscan, welke adviezen geadviseerd werden en welke ook geïmplementeerd werden. Zo is bijvoorbeeld bij *Beleid – Management* te zien dat de maatregelen die de buddy's het vaakst adviseren, namelijk een continuïteitsplan en informatieveiligheid bij een specifieke functie onderbrengen, juist door de mkb'ers het minst geïmplementeerd werden. Bij *Beleid – Documentatie* was een back-upbeleid een van de meest geadviseerde maatregelen en een van de meest geïmplementeerde adviezen ten tijde van de nameting.

Bij de *Techniek* maatregelen waren de maatregelen betreffende software-updates en IT-administratierechten al overwegend vaak ingevoerd. De maatregel betreffende IT-administratierechten was dan ook een van de minst geadviseerde maatregelen door de buddy's. Opvallend is echter wel dat de mkb'ers die dit advies alsnog gekregen hebben, het in driekwart van de gevallen heeft ingevoerd.

Bij *Medewerkers* gaven respondenten aan dat de motivatie om cyberaanvallen te melden en de capaciteit om deze te herkennen al hoog was onder de medewerkers. Minder gebruikelijk was het bij de mkb'ers om het bedrijf en de medewerkers te testen. De buddy's gaven dan ook overwegend de adviezen om deze tests uit te gaan voeren. De adviezen die het vaakst werden ingevoerd, waren bij het vergroten van de capaciteit van hun medewerkers op het gebied van detecteren. De minst vaak ingevoerde adviezen betroffen beide de vaardigheid om te leren van cyberincidenten.

Tabel 5. Maatregelen die heet vaakst en minst vaak zijn ingevoerd ten tijde van de voormeting, geadviseerd en ingevoerd bij de nameting (N=36)

	Reeds ingevoerd voor voormeting *Percentages berekend over totaal van 36 bedrijven*		**Geadviseerd in interventie** *Percentages berekend over totaal van 36 bedrijven*		**Advies geïmplementeerd bij nameting** *Percentages berekend over aantal bedrijven dat advies kreeg*	
	Meest ingevoerd	*Minst ingevoerd*	Meest geadviseerd	Minst geadviseerd	Meest advies geïmplementeerd	Minst advies geïmplementeerd
Beleid – Management	Specifieke personen zijn verantwoordelijk voor cybersecurity (63,9%)	Een Information Security Management systeem (ISMS) (8,3%)	Een bedrijfscontinuïteitsplan dat cyberincidenten omvat (80,6%)	Een Information Security Management systeem (ISMS) (8,3%)	Specifieke personen zijn verantwoordelijk voor cybersecurity (35,7%)	Een bedrijfscontinuïteitplan dat cyberincidenten omvat (20,7%)
	Er zijn specifieke medewerkers wiens functie informatieveiligheid omvat (44,4%)	Een bedrijfscontinuïteitsplan dat cyberincidenten omvat (13,9%)	Er zijn specifieke medewerkers wiens functie informatieveiligheid omvat (41,7%)	Specifieke personen zijn verantwoordelijk voor cybersecurity (38,9%)	Een Information Security Management systeem (ISMS) (33,3%)	Er zijn specifieke medewerkers wiens functie informatieveiligheid omvat (27,7%)
Beleid – Documentatie	Back-up beleid (36,1%)	Omgang met Internet of Things apparatuur (13,9%)	Classificering van gegevens (72,2%)	Mobiel werken of werken op afstand (bijvoorbeeld thuiswerken) (38,9%)	Een wachtwoordbeleid dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen (44,0%)	Wat voor soort gegevens bewaard mogen worden op verwijderbare apparaten (zoals USB sticks) (22,7%)

	Een wachtwoordbeleid dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen (33,3%)	Classificering van gegevens (16,7%)	Een wachtwoordbeleid dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen (69,4%)	Omgang met Internet of Things apparatuur (online apparatuur, zoals camera's) (47,2%)	Wat personeel mag doen op de IT apparaten van uw bedrijf (43,5%)	Omgang met Internet of Things apparatuur (online apparatuur, zoals camera's) (23,5%)
Techniek	Het uitvoeren van software-updates zodra deze beschikbaar zijn (86,1%)	Aangesloten bij een Security Operatie Centrum (5,6%)	Er is een actuele lijst met software en versie nummers (72,2%)	Toegangsrechten worden goed bijgehouden en zijn bijgewerkt (11,1%)	IT-administratie rechten zijn beperkt tot specifieke gebruikers (75%)	De organisatie doet regelmatig een technische penetratie test (15%)
	IT-administratierechten zijn beperkt tot specifieke gebruikers (83,3%)	Er is een beveiligingssoftware geïnstalleerd op telefoons met bedrijfsgegevens (8,3%)	Er is beveiliging software geïnstalleerd op telefoons met bedrijfsgegevens (63,9%)	IT-administratie rechten zijn beperkt tot specifieke gebruikers (11,1%)	IT-administratie rechten worden goed bijgehouden en zijn bijgewerkt (62,5%)	Een VPN-verbinding voor op kantoor en remote werken (16,7%)

Medewerkers	Medewerkers in het bedrijf vinden het belangrijk om cyberaanvallen en -incidenten altijd direct te melden (3,92/5) [11]	Ons bedrijf test regelmatig procedures over hoe om te gaan met een cyberaanval of -incident, bijvoorbeeld in de vorm van een oefening test (1,67/5) [8]	Medewerkers regelmatig testen op hun kennis en over de ervaringen van anderen (86,1%)	Medewerkers trainen in cyberbeveiliging (38,9%)	Medewerkers leren hoe ze cyberaanvallen kunnen herkennen (45,0%)	Medewerkers de middelen bieden om te leren van cyberaanvallen- en incidenten die zich in het bedrijf hebben voorgedaan (4,8%)
	Medewerkers in ons bedrijf weten hoe ze cyberaanvallen, zoals via een phishing-email, kunnen herkennen (3,72/5) [8]	Medewerkers worden regelmatig getest op kennis en over de ervaringen van anderen (1,83/5) [8]	Medewerkers trainen in het detecteren van cyberaanvallen- en incidenten (77,8%)	Medewerkers vragen naar hun mening over het cybersecuritybeleid (47,2%)	Medewerkers leren hoe ze verdachte links op betrouwbaarheid kunnen checken (44,0%)	Geleerde lessen, bijvoorbeeld na een incident of cybercrisisoefeningto epassen in het cybersecurity-beleid (5,3%)

[11] Ten tijde van de voormeting werden respondenten gevraagd aan te geven in hoeverre zij het eens waren met deze stellingen (op een schaal van 1-5).

6.3 Risicoperceptie

Er is onderzocht of de risicoperceptie van respondenten is veranderd tussen de voor- en nameting (Tabel 6). De eerste stelling betrof de mate waarin ondernemers zich zorgen maakten over de kans dat ze slachtoffer zouden worden van cybercrime. In de voormeting gaven mkb'ers aan zich *een beetje* tot *enigszins* zorgen te maken (M = 2,67; SD = 1,014). In de nameting is deze mate van zorgen nagenoeg gelijk gebleven (M = 2,64; SD = 0,931).

Tabel 6. Risicoperceptie van mkb'ers ten tijde van de voor- en nameting (N = 36)

	Voormeting		Nameting		t-waarde	df
	M	SD	M	SD		
Zorgen slachtofferschap cybercriminaliteit	2,67	1,014	2,64	0,931	0,298 (n.s.)	35
Zorgen schade cybercriminaliteit	3,00	1,454	2,94	1,218	0,329 (n.s.)	35
Prioriteit cybersecurity	2,31	1,037	2,39	1,022	-0,649 (n.s.)	35

Bij de tweede stelling, betreffende de mate waarin mkb'ers zich zorgen maakten over de mogelijke schade die hun bedrijf zou oplopen als gevolg van cybercrime, gaven respondenten in de voormeting aan zich hier *enigszins* zorgen over te maken (M = 3,00; SD = 1,45). Gedurende de nameting was dit nagenoeg gelijk (M = 2,94; SD = 1,22). Vervolgens hebben mkb'ers aangegeven in welke mate cybersecurity een prioriteit was in hun bedrijf. Gedurende de voormeting was deze prioriteit gemiddeld *redelijk laag* (M = 2,31; SD = 1,04) en ten tijde van de nameting was deze prioriteit nagenoeg even groot (M = 2,39; SD = 1,02). Deze verandering is niet significant (t(35) = -0,649; p > 0,05). Ten tijde van de tweede cyberscan is geen significante verandering in de risicoperceptie van mkb'ers waargenomen ten opzichte van de voormeting.

6.4 Verschillen tussen groepen ondernemers in implementatie van adviezen

Vervolgens is onderzocht in welke mate deze bevindingen verschillen tussen groepen mkb'ers, op basis van een aantal verschillende kenmerken; sector, aantal medewerkers, locatie (gemeente) en of bedrijven gebruik hebben gemaakt van de implementatiedagen. Gezien het kleine totaal aantal van 35 deelnemende mkb'ers zijn subgroepen over het algemeen klein en dienen de resultaten dan ook voorzichtig te worden geïnterpreteerd.

Als eerst is hierbij gekeken naar de sector waar respondenten toe behoren (Tabel 7). Respondenten uit de sector *gezondheidszorg en welzijn* implementeerden gemiddeld vaker maatregelen op het gebied van beleidsafspraken (management; 56,3%), techniek (50,6%) en

medewerkers (43,3%). Maatregelen op het gebied van beleid- documentatie werden het vaakst geïmplementeerd in de sector *handel en dienstverlening* (58,2%). Respondenten uit de sector *toerisme, recreatie en horeca* lijken het minst vaak de diverse soorten maatregelen te hebben geïmplementeerd. De sector *ICT* implementeerde per onderdeel werd ongeveer een vijfde tot een derde van de adviezen.

Tabel 7. Gemiddeld percentage geïmplementeerde adviezen, op basis van sector (N=36)

		Gezond-heidszorg en welzijn *(N =5)*	Handel en dienst-verlening *(N = 10)*	ICT *(N = 7)*	Toerisme, recreatie en horeca *(N = 6)*	Overig *(N = 8)*
Beleid	Management	56,3%	25,0%	35,7%	20,0%	16,7%
	Documentatie	45,5%	58,2%	21,5%	6,1%	18,2%
Techniek	Totaal	50,6%	32,4%	33,1%	24,1%	33,5%
Medewerkers	Totaal	43,3%	31,2%	28,4%	18,1%	27,1%

Vervolgens is gekeken naar de mate waarin resultaten verschillen tussen kleine en grote mkb ondernemingen, waarbij categorieën in aantal medewerkers zijn vergeleken (Tabel 8). De kleinste bedrijven, van 1 tot 10 medewerkers, voerden de meeste adviezen door op het onderdeel *Beleid – Documentatie* (33,2%) en de minste op het onderdeel *Medewerkers* (23,2%). Bedrijven met 11 tot 50 medewerkers voerden gemiddeld de meeste maatregelen in op het onderdeel *Beleid – Management* (45,0%) en het minst op het onderdeel *Beleid – Documentatie* (28,5%). In grootste bedrijven van 51 tot 250 medewerkers werden meer dan de helft van de geadviseerde technische maatregelen geïmplementeerd (60,6%). Voor het onderdeel *Management – Documentatie* werden door de grote ondernemingen geen geadviseerde maatregelen overgenomen (0,0%).

Tabel 8. Gemiddeld percentage geïmplementeerde adviezen, op basis van aantal medewerkers

		1 – 10 medewerkers *(N = 21)*	11 – 50 medewerkers *(N = 10)*	51 – 250 medewerkers *(N = 5)*
Beleid	Management	24,2%	45,0%	0,0%
	Documentatie	33,2%	24,0%	40,0%
Techniek	Totaal	29,8%	28,5%	60,6%
Medewerkers	Totaal	23,2%	34,5%	44,4%

Vervolgens is onderzocht of de mate waarin geadviseerde maatregelen zijn geïmplementeerd verschilt tussen de gemeentes waarin de ondernemingen gevestigd zijn (Tabel 9). In gemeente Utrecht worden binnen alle soorten maatregelen ongeveer een kwart tot een derde van de geadviseerde maatregelen ingevoerd (36,5%). In Enschede wordt op het gebied van *Beleid – Management* (50%) en Beleid – Documentatie (45.5%) ongeveer de helft van de geadviseerde maatregelen geïmplementeerd en adviezen over *techniek* het minst (25,3%). In Den Helder werden *Beleid – Documentatie* adviezen het meest geïmplementeerd (43,8%) en *Beleid – Management* adviezen helemaal niet (0,0%).

Tabel 9. Gemiddeld percentage geïmplementeerde adviezen, op basis van gemeente

		Utrecht *(N = 25)*	Enschede *(N = 5)*	Den Helder *(N = 6)*
Beleid	Management	30,8%	50,0%	0%
	Documentatie	25,0%	45,5%	43,8%
Techniek	Totaal	35,2%	25,3%	36,5%
Medewerkers	Totaal	33,5%	31,4%	11,3%

Tot slot is onderzocht of de mate waarin geadviseerde maatregelen zijn geïmplementeerd verschilt tussen bedrijven die wel en niet gebruik hebben gemaakt van de implementatiedagen (Tabel 10). Mkb'ers die gebruik hebben gemaakt van de implementatie dagen, hebben binnen drie van de vier onderdelen meer geadviseerde maatregelen geïmplementeerd. Dit gebeurde het meest op het gebied *Beleid – Management (55.6%)* en het minst op het gebied van *Beleid – Documentatie (32.7%).* Mkb'ers die geen implementatiedagen gehad hebben, voerden aanzienlijk minder adviezen in. De enige uitzondering hierop is het onderdeel Beleid – Documentatie, waarbij ongeveer evenveel geadviseerde maatregelen werden geïmplementeerd door zowel bedrijven die wel of niet gebruik hebben gemaakt van de implementatiedagen.

Tabel 10. Gemiddeld percentage geïmplementeerde adviezen, op basis van wel of geen implementatiedagen

		Wel implementatiedagen *(N = 9)*	Geen implementatiedagen *(N = 27)*
Beleid	Management	55,6%	18,3%
	Documentatie	32,7%	31,7%
Techniek	Totaal	43,7%	31,0%
Medewerkers	Totaal	52,9%	22,0%

7. Ervaringen van betrokkenen van de pilot

Gedurende het project zijn deelnemende mkb'ers (7.1), buddy's (7.2) en gemeenten (7.3) bevraagd over hoe zij het project ervaren hebben. Deze ervaringen zullen in dit hoofdstuk besproken worden.

7.1 Evaringen van mkb'ers

Aan de mkb'ers is op twee punten tijdens het onderzoek gevraagd naar hun ervaringen met de interventie. Allereerst eindigde de nameting van de cyberscan met vragen over de ervaringen met het project. Daarnaast eindigde de nameting met de vraag of respondenten nog bereid zouden zijn om na gebeld te worden voor een kort evaluatiegesprek. In totaal is dit gesprek van gemiddeld 10 minuten met 10 respondenten gehouden. In dit hoofdstuk zullen de ervaringen van 34 deelnemende bedrijven op basis van de vragen in de nameting worden beschreven, waarbij de percentages steeds betrekking hebben op dit totaal aantal. Hiernaast zullen deze bevindingen geïllustreerd worden met quotes uit de 10 evaluatie gesprekken. Hoewel de respondenten uit zowel mannen als vrouwen bestonden, zullen voor alle respondenten mannelijke persoonlijke voornaamwoorden gebruikt worden, om hun privacy te waarborgen.

Aan het einde van de nameting zijn deelnemende mkb'ers een aantal stelling voorgelegd over de cybersecurity van hun bedrijf na afloop van de interventie (Tabel 11). Bijna twee derde van de respondenten was het eens met de stelling dat de deelnemers op basis van het adviesrapport verbeteringen hebben doorgevoerd in de cybersecurity van hun onderneming (62.9%). Gedurende de interviews is naar voren gekomen dat wanneer een mkb'er geen verbeteringen had doorgevoerd, dit ofwel betekende dat ze er tijdens het project geen tijd voor hebben gehad, ofwel betekende dat uit het adviesrapport bleek dat alles al goed geregeld was.

Vervolgens gaf de helft van de deelnemende mkb'ers aan het gevoel te hebben dat hun onderneming weerbaarder geworden. Tijdens interviews gaven mkb'ers die het niet eens waren met de stelling bijvoorbeeld aan dat uit de eerste cyberscan naar voren kwam dat het bij hen al goed geregeld was en nog weerbaarder worden niet noodzakelijk was. Mkb'ers die het wel eens waren met de stelling gaven bijvoorbeeld aan dat de interventie binnen het bedrijf meer bewustzijn heeft gecreëerd en dat ze aanpassingen hebben gemaakt die ze voorheen niet zouden maken. Een ondernemer vertelde bijvoorbeeld het volgende:

> *"Het project heeft gezorgd voor bewustwording, waardoor we nu onze onderneming hierop hebben geprofessionaliseerd. We zijn nu veel duidelijkere afspraken gaan maken over zaken die eerst zo evident leken dat we ze nooit hebben vastgelegd, zoals*

dat je niet op onbekende linkjes moeten klikken. Maar we hebben ook grotere veranderingen gemaakt, zoals dat we momenteel onze afspraken met de IT-leverancier veel duidelijker gaan maken." - Respondent B10[12]

Tabel 11. Overzicht van stellingen over ervaringen met het project van mkb'ers (schaal 1-5)

		N[13]	Helemaal/ enigszins onwaar	Niet onwaar of waar	Helemaal/ enigszins waar	M (SD)
1	Wij hebben op basis van het adviesrapport verbeteringen doorgevoerd in de cybersecurity van onze onderneming	35	12 (34,3%)	1 (2,9%)	22 (62,9%)	3,12 (1,591)
2	Ik heb het gevoel dat de cyberweerbaarheid van het bedrijf is toegenomen als gevolg van dit project	34	11 (32,4%)	6 (17,6%)	17 (50%)	3,18 (1,424)
3	Ik voel me als gevolg van dit project meer bekwaam om de verantwoordelijk over de cybersecurity te dragen dan voorheen	34	9 (26,5%)	10 (29,4%)	15 (43,5%)	3,18 (1,380)
4	Ik voel me in staat om na afloop van dit project het bedrijf verder te ontwikkelen met betrekking tot cybersecurity	34	5 (14,7%)	8 (23,5%)	21 (61,8%)	3,52 (1,278)
5	Ik heb het gevoel dat naarmate cybercrime ontwikkeld, mijn bedrijf nu in staat zal zijn om hierin mee te ontwikkelen met betrekking tot cybersecurity	34	7 (20,6%)	10 (29,4%)	17 (50,0%)	3,30 (1,212)
6	Wij gaan in onze onderneming op korte termijn (verdere) verbeteringen doorvoeren in onze cybersecurity op basis van het adviesrapport	34	8 (23,5%)	4 (11,4%)	22 (62,9%)	3,35 (1,433)

[12] Van de respondentcode verwijst de letter naar de buddy en het cijfer naar de respondent (geanonimiseerd).
[13] De N verschilt per variabelen omdat een aantal respondenten die het zodanig druk hadden dat een aantal vragen zijn overgeslagen.

Verder gaf een groot deel van de respondenten (43,5%) aan dat ze zich als gevolg van dit project beter bekwaam voelden om de verantwoordelijkheid voor de cybersecurity van het bedrijf te dragen (Tabel 11). Een merendeel van de respondenten (61,8%) voelde zich als gevolg van het project in staat om het bedrijf verder te ontwikkelen op het gebied van cybersecurity. Bovendien gaf de helft van de respondenten (50,0%) aan dat zij het gevoel hadden dat, naarmate cybercrime ontwikkelt, het bedrijf nu in staat zal zijn om hierin mee te ontwikkelen met betrekking tot cybersecurity.

De laatste stelling (Tabel 11) betrof de mate waarin mkb'ers op korte termijn nog verdere verbeteringen zouden doorvoeren. Ook hier was bijna twee-derde van de deelnemers het eens met de stelling. Deze respondenten gaven bijvoorbeeld tijdens interviews aan dat het rapport nog genoeg adviezen bevatte die zij gedurende het project nog niet hadden kunnen oppakken, maar in de toekomst wel wilden doorvoeren. Acht mkb'ers (23,5%) gaven aan dat zij niet van plan waren op korte termijn verder te gaan met het invoeren van de overgebleven adviezen uit het rapport. Deze respondenten is nader bevraagd wat hiervoor de reden is. Hierbij zijn een aantal redenen voorgelegd waarbij zij konden aangeven of deze reden voor hen wel of niet relevant was, door *ja* of *nee* te antwoorden (Tabel 12). Ook hebben zij de optie gehad hier nog andere redenen aan te dragen. Een kwart van deze respondenten gaat geen nieuwe veranderingen gaat doorvoeren omdat ze niet weten hoe ze dit zouden moeten doen. Bij de helft van de respondenten speelt mee dat ze nieuwe veranderingen niet belangrijk vinden. Ook geeft de helft van de respondenten aan dat ze vinden dat er ondertussen voldoende gedaan is, en bijna twee derde (62,5%) vindt dat de cybersecurity al goed genoeg is. Een respondent gaf een andere reden, namelijk dat er niet genoeg tijd in het bedrijf was voor cybersecurity.

Tabel 12. Redenen dat deelnemende mkb'ers op korte termijn geen verdere verbetering gaan doorvoeren (N = 8)

	Ja	Nee
Omdat we niet weten hoe	2 (25,0%)	6 (75,0%)
Omdat we het niet belangrijk vinden	4 (50,0%)	4 (50,0%)
Omdat er nu voldoende gedaan is	4 (50,0%)	4 (50,0%)
Omdat onze cybersecurity nu goed genoeg is	5 (62,5%)	3 (37,5%)
Anders, namelijk…	1 (12,5%)	7 (87,5%)

Vervolgens is de deelnemers gevraagd hoe tevreden zij waren met de verschillende onderdelen van het project (Tabel 13). Daarnaast hebben zij ook gedurende de nameting en/of

interview een toelichting op deze tevredenheid kunnen geven. Deelnemende mkb'ers waren het meest tevreden over het advies rapport en het contact met de buddy (gemiddeld 4,2, schaal 1-5). Met betrekking tot het adviesrapport gaven respondenten die tevreden waren bijvoorbeeld aan dat het in duidelijke taal geschreven was en veel inzichten bood in de kwetsbaarheden van het bedrijf. Respondenten die minder tevreden waren, gaven overwegend aan dat ze het adviesrapport te lang vonden. Zo gaf een respondent tijdens het interview het volgende aan:

> *"Ik zou liever een veel kleiner rapport krijgen, want dit was zo lang. Bij ons bedrijf stellen we per kwartaal een stuk of 12 doelen op en als we dan al 3 à 4 bereiken zijn we al tevreden. Ik zou dus liever ook te horen krijgen: 'Dit zijn de drie belangrijkste dingen voor jou om aan te pakken' dan dat ik zo'n hele lap tekst krijg."* - Respondent H8

Tabel 13. Tevredenheid van de participerende mkb'ers over onderdelen van het project (zeer ontevreden (1) – zeer tevreden (5))

	N	Min	Max	M (SD)
De eerste cyberscan	35	2	5	4,0 (0,71)
Het adviesrapport	34	3	5	4,2 (0,64)
Contact met buddy	35	3	5	4,2 (0,72)
Implementatiedagen	9	3	5	3,9 (0,78)
Project algemeen	34	2	5	3,9 (0,77)

Ook gaven een aantal respondenten van zowel de nameting als de interviews aan dat het rapport nog meer op maat gemaakt had kunnen zijn dan het tot nu toe was. Het rapport voelde voor hen heel algemeen aan, terwijl de buddy's naar hun idee wel meer informatie hadden over het bedrijf waar ze specifieker op in hadden mogen gaan.

> "*Het rapport mag meer gericht zijn op de dingen die bij ons om de vragenlijst heen besproken zijn. Nu was het een redelijk algemene rapportage die vooral gericht was op de antwoorden van de scan."* – Respondent Z9

Met betrekking tot het contact met de buddy gaven respondenten onder andere aan dat het contact professioneel en prettig was. Een respondent zei in een interview het volgende hierover:

> *"Wanneer je voor iets als dit naar een adviesbureau gaat, dan praten ze tegen je, maar de buddy praat echt met je mee. Dat vond ik heel fijn. We zijn op een heel open manier, zonder oordelen geholpen. […] Niet betuttelend of met wijzende vingertjes."* – Respondent B10

Deelnemende mkb'ers waren ook gemiddeld tevreden met de eerste cyberscan (gemiddeld 4,03). Een respondent die de cyberscan een lagere tevredenheidscore had gegeven, lichtte toe dat dit was omdat voor hem als ondernemer van een klein bedrijf, de vragenlijst relevanter leken voor grotere kantoren. Respondenten die tevreden waren met de cyberscan gaven aan dat er goede vragen gesteld werden en niks op aan te merken was. Een respondent gaf tijdens een interview aan dat de cyberscan bij hem op zichzelf al leidde tot meer bewustwording en een intentie tot gedragsverandering:

> "*Het project heeft ons echt gemotiveerd om iets te veranderen. Dit gebeurde eigenlijk al bij de vragenlijst; door constant op de vragen of we een bepaalde maatregel hadden nee te moeten antwoorden, voelde ik me een beetje stom.*" – Respondent H9

De 9 respondenten die gebruik hebben gemaakt van de implementatiedagen waren daar gemiddeld tevreden over (gemiddeld 3,9). Respondenten gaven aan dat ze het fijn vonden dat er iemand met kennis kwam meekijken in het bedrijf. Een ondernemer die gebruik had gemaakt van de implementatiedag, gaf aan in een interview aan dat de presentatie tijdens deze dag veel indruk gemaakt had.

> *"We zijn echt wakker geschud en hebben veranderingen gemaakt die we zonder dit project nooit gemaakt zouden hebben. Dit was vooral door een presentatie van de buddy. Die liet bijvoorbeeld zien dat we phishing mails niet goed controleerden en daar zijn we echt van geschrokken."* – Respondent X7

Een respondent liet weten dat hij liever gehad had dat de buddy tijdens de implementatiedag volledig zelfstandig kon werken, zodat het de ondernemer geen tijd zou kosten. Een respondent die geen gebruik had gemaakt van de implementatiedagen, liet tijdens het interview weten dat dit was omdat hij hier geen tijd voor had. Dit was onder andere omdat, ondanks het feit dat de implementatiedag door de buddy worden uitgevoerd en op *quick wins* gericht kunnen zijn, de ondernemer er alsnog een dag voor uit zou moeten trekken.

7.2 Ervaringen Buddy's

De buddy's hebben gedurende het project het meest contact gehad met de mkb'ers. Daarom zal eerst besproken worden wat de ervaringen van de buddy's waren met betrekking tot deze samenwerking. Als eerste bleek het lastiger te zijn dan verwacht om mkb'ers werven die mee wilden doen aan het project. Uit gesprekken tijdens het werven bleek bijvoorbeeld dat mkb'ers het vaak te druk hadden voor het project of cybersecurity niet als een prioriteit zagen. In een gemeente bleek – zoals eerder aangegeven –het werven ook bemoeilijkt te worden doordat er gelijktijdig door een andere organisatie (gesubsidieerde) cyberscans werden aangeboden, waar veel ondernemers al gebruik van hadden gemaakt.

De buddy's hebben zelf aangegeven dat werven over het algemeen het meest effectief was wanneer dit face-to-face gebeurde. E-mails werden in veel gevallen genegeerd en een aantal mkb'ers gaf aan dat zij in eerste instantie dachten dat de e-mails die de buddy's gestuurd hadden juist phishing-mails waren. Ook gaven de buddy's aan dat het werven effectiever bleek wanneer benadrukt werd dat het project werd aangeboden door de gemeente. Wanneer de buddy bijvoorbeeld namen van medewerkers van de gemeente kon noemen die bij de mkb'ers bekend waren, leek dit meer vertrouwen te scheppen. Als laatste was het de buddy's opgevallen dat het succes van het werven ook afhankelijk was van het moment in het jaar waarop dit gedaan werd. Werven rond de meivakantie zorgde er bijvoorbeeld voor dat veel medewerkers op vakantie waren, waardoor bedrijven het vaak drukker hadden en er geen tijd was om deel te nemen aan het project. Ook zijn er een aantal bedrijven die het drukker hadden naarmate de zomervakantie dichterbij kwam.

Bij de mkb'ers die geworven waren via mails of sociale mediaberichten, bleek later in het project vaak dat mkb'ers die toegezegd hadden mee te doen nog niet helemaal bekend waren met wat het project precies inhield. Zo kwamen zij er bijvoorbeeld pas gedurende de afname van de cyberscan achter dat er ook een adviesrapport, implementatiedagen en een nameting zouden volgen[14].

Ook hebben de buddy's vaak meegemaakt dat mkb'ers die meededen aan de cyberscan lastig te bereiken waren voor vervolgafspraken. Zo lieten buddy's de mkb'er bij het toesturen van het adviesrapport weten dat ze graag binnen een week hoorden of de mkb'er gebruik wilde maken van de implementatiedagen. Regelmatig werden deze mails niet beantwoord en moest de buddy een aantal keer nabellen, om zo zeker te weten of ze een plekje voor de implementatiedagen open moesten houden of niet. Ook voor het inplannen van de nameting gebeurde het dat de nameting ofwel op het laatste moment werd afgezegd, ofwel dat de mkb'er simpelweg niet kwam opdagen[15].

[14] Om deze reden is voor de tweede wervingsronde de flyer opgesteld, waarin alle stappen van het project extra duidelijk toegelicht werden (onderdeel van de op te vragen documenten, zie bijlage 1).

[15] Gedurende de tweede ronde van de pilot hebben de buddy's geprobeerd dit soort situaties te voorkomen door tijdens de cyberscan gelijk te laten weten wanneer ze het rapport zouden opsturen en wanneer ze hier antwoord op wilden. Vanwege

Bij de uitvoering van het project gaven een aantal buddy's aan dat het belangrijk is dat ze niet te veel mkb'ers tegelijkertijd aan het helpen zijn. Wanneer ze bijvoorbeeld in één week ruwweg 8 adviesrapporten moeten schrijven, kan dit ervoor zorgen dat deze rapporten minder gedetailleerd en persoonlijk worden. De buddy's hadden het gevoel dat ze niet genoeg tijd hadden om naar de specifieke casussen van de bedrijven te kijken, waardoor het advies minder toegespitst was dan als ze meer tijd gehad hadden. Een buddy gaf ook aan dat de rapporten waarschijnlijk persoonlijker zouden kunnen zijn wanneer ze direct na de scan geschreven werden, in tegenstelling tot wanneer er eerst 10 scans werden uitgevoerd en daarna 10 rapporten geschreven werden.

Tot slot gaven de buddy's aan dat dit project als stage zeer leerzaam en interessant voor hen geweest is. Ze lieten weten dat de diversiteit aan bedrijven die dit project meebrengt, ervoor zorgt dat ze veel kennis uit hun studie hebben kunnen toepassen in de praktijk, waardoor ze veel hebben geleerd. Ook zouden alle buddy's de stage aanraden aan medestudenten. Zo liet een buddy bijvoorbeeld weten:

> "*Ik vond het een heel leuke stage. Alles wat ik op de opleiding geleerd heb kwam hier in de praktijk terug bij de bedrijven. Door de meeloopdagen maak je echt van dichtbij mee hoe bedrijven omgaan met cybersecurity, dus bijvoorbeeld hoe ze prioriteiten stellen. Ik zou het ook aan anderen aanraden. Doordat je bij heel veel bedrijven meeloopt doe je veel verschillende dingen en krijg je onderwerpen mee uit allerlei verschillende hoeken. Daarvan leer je veel meer dan een stage die maar op één casus focust.*" - Buddy

7.3 Gemeenten

Tegen het einde van de pilot is met een medewerker van elke participerende gemeente gesproken over hun ervaringen met het project. De medewerkers waren over het algemeen positief over het project. Zo gaven zij aan dat ze de samenwerking met zowel de andere gemeentes als met de onderzoekers prettig vonden verlopen. Ook waren ze tevreden over de opzet en onderbouwing van het project. Een medewerker gaf bijvoorbeeld aan te waarderen dat het project ontworpen was vanuit wetenschappelijke inzichten.

Als minder positief aspect van het project gaven medewerkers aan dat het werven van de mkb'ers moeizamer ging dan verwacht. Medewerkers lieten weten dat ze veel verschillende manieren hebben geprobeerd om samen met hun buddy mkb'ers te werven en weten daarom ook niet zo goed

het geringe aantal respondenten dat in de tweede ronde participeerde, is het lastig te zeggen in hoeverre dit effect heeft gehad.

wat nog verbeterd zou kunnen worden. Een medewerker opperde dat het misschien beter zou zijn als het project al een paar maanden voor uitvoer aan de mkb'ers in de gemeente wordt aangekondigd, zoals dit bijvoorbeeld bij een ondernemersbijeenkomst alvast te noemen.

Een andere punt waar de gemeentemedewerkers tegenaan liepen, was dat het momenteel lastig is om voldoende studenten te vinden om de stageplaatsen te vullen. Dit is onder andere het geval voor de gemeenten die niet direct in de buurt van een Hogeschool zitten, omdat studenten dus ver zouden moeten reizen voor hun stage. Daarnaast zou de concurrentie tussen verschillende stageaanbieders momenteel groot zijn door personeelstekort. Een medewerker gaf aan dat er ook goed gekeken moet worden naar de eisen die een school stelt aan een stage, zodat vanaf het begin van de stage zeker kan zijn dat dit met elkaar aansluit. Verder gaf deze medewerker aan behoefte te hebben gehad aan beter contact met de hogescholen waar de stagiairs studeren.

Vervolgens is besproken wat, volgens de gemeentemedewerkers, de kosten en baten waren van de interventie. Is dit project de moeite die er in diende gestoken te worden waard, gezien wat het opleverde? De medewerkers gaven aan dat zij vinden dat de kosten opwegen tegen de baten. Een aantal liet weten dat het opzetten van het project in het begin wel flink wat tijd gekost heeft, maar dat dit ook logisch was aangezien het een pilot was die ontworpen moest worden. Daarnaast gaven meerdere medewerkers aan dat het project voordelig is voor gemeentes die weinig medewerkers en tijd hebben voor het dossier cybersecurity. Waar sommige grote gemeentes volledige afdeling hiervoor hebben, is dit niet bij alle gemeentes het geval. Deze medewerkers gaven aan dat het daarom prettig was dat het project in samenwerking ging met stagiaires, projectleiding, coördinatie en begeleiding vanuit de Haagse Hogeschool.

De medewerkers is ook gevraagd of zij het project aan andere gemeentes zouden aanraden of zelf nog een keer zouden uitvoeren. Hierop hebben zij allemaal positief geantwoord. Wel zouden alle medewerkers aanraden het project eerst te verbeteren aan de hand van alle lessen die gedurende de pilot zijn opgedaan.

8. Conclusie

In de huidige studie heeft een evaluatie plaatsgevonden van een interventie voor mkb'ers gericht tegen ransomware. De interventie is onderdeel van een overkoepelend project dat als doel heeft om de cyberweerbaarheid van kwetsbare groepen individuen tegen specifieke vormen van cybercriminaliteit te verhogen. De interventie heet "MKB cyber buddy's", waarbij studenten een scan afnemen bij mkb-bedrijven en op basis daarvan de deelnemende bedrijven adviseren en actief ondersteunen bij het nemen van aanvullende cybersecurity maatregelen omtrent ransomware.

We geven in dit hoofdstuk antwoord op de volgende drie onderzoeksvragen door middel van gesprekken met betrokken partijen en een voor- en nameting: (1) Hoe is het uitvoeren van de pilot van de interventie "MKB cyber buddy's project" verlopen en hoe is deze uitvoering door betrokkenen ervaren? (2) In hoeverre beïnvloedt het "MKB cyber buddy's project" de cyberweerbaarheid van deelnemende ondernemingen tegen ransomware, met betrekking tot cybersecuritybeleid, technische maatregelen en weerbaarheid van medewerkers (human factor)? (3) Welke aanpassingen kunnen gemaakt worden om de interventie te verbeteren en geschikt te maken voor andere Nederlandse gemeenten?

8.1 Hoe is het uitvoeren van de pilot van de interventie "MKB cyber buddy's project" verlopen en hoe is deze uitvoering door betrokkenen ervaren?

Het werven van respondenten bleek tijdens de pilot lastiger dan vooraf werd verwacht. Met een gemiddelde respons van 6,4% deden 30 van de 466 benaderde mkb'ers uit de drie gemeenten mee met het project. Hiernaast deden 13 mkb'ers mee nadat zij interesse bij de gemeente hadden geuit om deel te nemen aan een project over cybersecurity. In totaal maakten negen ondernemingen gebruik van de implementatiedagen en dit was minder dan werd verwacht. Van de 43 deelnemende mkb'ers lieten 36 mkb'ers (83.7%) uiteindelijk ook de nameting afnemen, waarbij uitval voornamelijk leek te worden veroorzaakt door lage prioritering van cybersecurity. De resultaten uit het rapport hebben betrekking op deze 36 ondernemingen. Deelnemende mkb'ers hadden veelal 1 tot 10 medewerkers (60%) en waren gevestigd in Utrecht (68,6%), Den Helder (17,1%) of Enschede (14,3%). De meest voorkomende sectoren waarin de deelnemers opereren zijn handel en dienstverlening (28,6%), ICT (20,0%) en toerisme en horeca (17,1%).

De ervaring van de betrokken partijen was overwegend positief. Mkb'ers gaven aan dat zij tevreden waren met de verschillende onderdelen van de interventie (gemiddeld 3,9 tot 4,2 op een schaal van 1-5). Ook gaf een groot deel van de mkb'ers aan dat zij op basis van het adviesrapport

verbeteringen hebben doorgevoerd in de cybersecurity van hun onderneming (62,9%), de interventie het bedrijf weerbaarder gemaakt had (50%), zich meer bekwaam voelen om de verantwoordelijk over de cybersecurity te dragen (43,5%), zich in staat voelt om na afloop van dit project het bedrijf verder te ontwikkelen met betrekking tot cybersecurity (61,8%) en het gevoel heeft dat naarmate cybercrime ontwikkeld, het bedrijf nu in staat zal zijn om hierin mee te ontwikkelen met betrekking tot cybersecurity (50%). Tot slot is 62,9% van plan in de onderneming op korte termijn (verdere) verbeteringen door te voeren in de cybersecurity op basis van het adviesrapport. Redenen voor deelnemers om geen verdere verbeteringen door te voeren waren omdat ze niet weten hoe (75%), omdat ze het niet belangrijk vinden (50%), omdat er nu voldoende gedaan is (50%) en omdat de cybersecurity nu goed genoeg is (37.5%). Als feedback gaven de mkb'ers vooral aan dat het adviesrapport nog meer op maat zou mogen zijn.

De buddy's van dit project waren over het algemeen blij met hun stage en gaven aan dat het een leerzaam project was dat ze aan medestudenten zouden aanraden. Als kritische noot merkten zij op dat het project soms lastig uit te voeren was wanneer het ging over de samenwerking met mkb'ers, omdat deze bijvoorbeeld andere verwachtingen en prioriteiten hadden.

De gemeentemedewerkers hebben het project als positief ervaren. Ze gaven aan dat de opzet van de pilot prettig was voor hen, omdat het niet te veel tijd kostte in verhouding met de baten. Als feedbackpunt gaven de gemeentemedewerkers voornamelijk aan dat zij graag zouden zien dat de wervingsprocedure verbeterd wordt.

8.2. In hoeverre beïnvloedt het "MKB cyber buddy's project" de cyberweerbaarheid van deelnemende ondernemingen tegen ransomware, met betrekking tot cybersecuritybeleid, technische maatregelen en weerbaarheid van medewerkers (human factor)?

Om de effecten van de interventie te meten, is gebruik gemaakt van de resultaten van de cyberscan die is afgenomen tijdens de voor- en nameting. Hierbij is gekeken naar de hoeveelheid maatregelen die geadviseerd worden, het aantal en type maatregelen dat geïmplementeerd wordt, het effect dat de interventie eventueel heeft op de visie van mkb'ers op cybersecurity en of het implementeren van geadviseerde maatregelen samenhangt met diverse kenmerken van mkb'ers.

De resultaten laten zien dat mkb'ers ongeveer een derde van de adviezen implementeren. Van de geadviseerde maatregelen, worden techniek maatregelen het meest geïmplementeerd (34%), gevolgd door maatregelen gericht op medewerkers (29%) en beleid (28% van de maatregelen gericht op cybersecurity management en 32% van de maatregelen gericht op beleidsdocumentatie). In absolute aantallen implementeren bedrijven door hun deelname aan het project gemiddeld ongeveer drie technische maatregelen, vijf maatregelen gericht op medewerkers, twee maatregelen gericht op

documentatie van cybersecuritybeleid en gemiddeld iets minder dan een halve maatregel gericht op cybersecurity management.

Binnen het theoretische model van vaardigheden voor cyberweerbaarheid (Hollnagel, 2015) worden maatregelen gericht op *leren* minder vaak geïmplementeerd (22%), gevolgd door maatregelen gericht op anticiperen, detecteren en reageren (respectievelijk 30%, 30% en 32%). Binnen het theoretische COM-B model (Michie et al., 2011) worden maatregelen gericht op gelegenheid minder vaak geïmplementeerd (24%) dan maatregelen gericht op capaciteit en motivatie (beiden 32%). Samengenomen nemen mkb'ers na afloop van de interventie significant meer maatregelen op het gebied van cybersecurity.

Vervolgens is onderzocht welke maatregelen het meest al reeds aanwezig waren bij mkb'ers voor deelname aan het project, welke adviezen het meest gegeven werden door buddy's en welke adviezen het meest geïmplementeerd werden. De volgende maatregelen werden gemiddeld het vaakst geïmplementeerd nadat deze werden geadviseerd door de buddy's, onderverdeeld naar type maatregel: specifieke personen verantwoordelijk maken voor cybersecurity en een ISM systeem (beleid management), vastleggen van wachtwoordbeleid en wat personeel mak doen op de IT apparaten van bedrijf (beleid documentatie), beperken IT rechten en bijwerken IT rechten (techniek) en medewerkers leren cyberaanvallen te herkennen en verdachte links op betrouwbaarheid checken (medewerkers). Hiernaast zijn er hierbij een aantal opvallende resultaten gevonden. Zo blijkt in sommige gevallen dat er een redelijke discrepantie bestaat tussen wat de buddy's het vaakst adviseren en wat de mkb'ers invoeren. Bijvoorbeeld wanneer het gaat om een bedrijfscontinuïteitsplan, dat vaak geadviseerd werd maar relatief weinig ingevoerd. Mogelijk hangt dit samen met het feit dat dit een van de meer omvangrijke maatregelen is om in te voeren, in termen van tijd en moeite. Ook was te zien dat de meest voorkomende beleidsmaatregel die mkb'ers al namen het back-up beleid is. Dit is noemenswaardig, omdat deze interventie voornamelijk gericht is op bescherming tegen ransomware en een back-upbeleid essentieel is in het minimaliseren van de schade van een ransomware-aanval. Verder lieten deze resultaten zien dat een advies dat niet vaak gegeven wordt, soms wel relatief vaak wordt geïmplementeerd, zoals bij het advies betreffende IT-administratierechten. Mogelijk komt dit ook doordat deze maatregel relatief beperkte tijd en moeite kost om in te voeren.

Vervolgens is onderzocht in welke mate de interventie invloed heeft gehad op de risicoperceptie van ondernemers rondom cybersecurity. De resultaten tonen aan dat de interventie gemiddeld geen verschil lijkt te hebben gemaakt in de mate waarin mkb'ers zich zorgen maken over slachtofferschap en schade van cybersecurity incidenten. Daarnaast lijkt de interventie gemiddeld ook de prioriteit die cybersecurity heeft in een bedrijf niet te veranderen. Het is niet vast te stellen of het inspelen op de 'affectieve respons' en 'subjectieve norm' in de risicocommunicatie heeft bijgedragen aan het verhogen van de motivatie van ondernemers om cybersecurity maatregelen te nemen.

Tot slot is gekeken naar de samenhang tussen de mate waarin adviezen worden geïmplementeerd en kenmerken van de deelnemende mkb'ers. Deze resultaten laten zien dat bedrijven in de sector *gezondheidszorg en welzijn* gemiddeld de meeste adviezen implementeren (43-56% van de matregelen gericht op beleid, techniek en medewerkers). Ook is te zien dat naarmate een bedrijf meer medewerkers heeft, dit bedrijf ook meer adviezen implementeert. Daarnaast kan ook verschil zitten in het soort adviezen dat geïmplementeerd wordt. Bedrijven van 11 – 50 medewerkers implementeerden bijvoorbeeld vaak (45%) maatregelen die zich richten op management van cybersecurity, terwijl deze bij bedrijven van 51 – 250 helemaal niet geïmplementeerd werden. Bedrijven uit Utrecht en Enschede lijken gemiddeld meer adviezen te implementeren dan bedrijven uit Den Helder. Ook hier is te zien dat er soms grote verschillen zijn in het type maatregelen dat geïmplementeerd wordt. Zo werden in Den Helder vooral maatregelen die zich richten op documentatie van cybersecurity beleid (44%) en techniek (37%) geïmplementeerd en veel minder vaak maatregelen gericht op medewerkers (11%) en cybersecurity management (0%). Tot slot werd gevonden dat mkb'ers die implementatiedagen hebben gehad op bijna alle onderdelen aanzienlijk meer adviezen implementeerden dan de mkb'ers die niet gebruik hebben gemaakt van deze dagen.

8.3. Welke aanpassingen kunnen gemaakt worden om de interventie te verbeteren en geschikt te maken voor andere Nederlandse gemeenten?

Gedurende de pilot zijn er verschillende lessen geleerd en verbeterpunten voor de interventie naar voren gekomen. In hoofdstuk vier zijn deze geleerde lessen beschreven. Hier zullen de verbeterpunten op hoofdlijnen worden beschreven, die betrekking hebben op de wervingsprocedure, het organiseren van het project door samenwerkende gemeenten, het afstemmen van taken en verantwoordelijkheden, het trainen van buddy's en het standaard adviesrapport. Wij adviseren de toekomstige uitvoerders voor de start van het project de volgende punten door te voeren, grotendeels met behulp van een in te huren cybersecurity expert.

Om te beginnen de verbeterpunten voor de wervingsprocedure. Tijdens de pilot is gebleken dat de non-respons hoog is wanneer mkb'ers "koud" worden gevraagd mee te doen aan het project, zonder dat zij hier vooraf over gehoord hebben of interesse hebben geuit wat betreft hulp bij cybersecurity. Licht als gemeente bedrijven in de regio dan ook al ruim voor de start van het project in. Zo kan bijvoorbeeld het project worden gepresenteerd bij ondernemings-bijeenkomsten over cybersecurity die door vele gemeenten reeds worden georganiseerd, waarbij ondernemers de optie geboden worden om zichzelf hier gelijk voor aan te melden. Wanneer het daarnaast nodig wordt geacht om bedrijven ook koud te benaderen, is het noodzakelijk dat vanuit de gemeente actief wordt bijgedragen aan het werven van deelnemende mkb'ers. De pilot heeft laten zien dat bedrijven eerder

bereid zijn deel te nemen als hen duidelijk is dat het geen studentenproject betreft, maar een project van de gemeente. Naast dat het gemeentelogo op de informatiefolder dient te worden geplaats, kan de gemeente actief groepen ondernemers benaderen via sociale media of ondernemingsverenigingen. Er zou daarnaast bij nieuwe buddy's een gemeentemedewerkers mee kunnen gaan met het werven, om hierin te begeleiden. Tot slot is het van belang dat er tijdens het werven van mkb'ers gewerkt wordt aan verwachtingsmanagement, bijvoorbeeld door gebruik te maken van de folder, zodat mkb'ers weten wat er van hen wordt verwacht en wat ze terugkrijgen voor deelname aan het project.

Een verbeterpunt voor het op grotere schaal uitrollen van het project is het centraal organiseren van het project door samenwerkende gemeenten. Zo zou er slechts één gemeentewerker een aantal uur in de week vrijgesteld hoeven worden als uitvoerder/coördinator, die de trainingen organiseert, een cybersecurity professional inhuurt, velwerkzaamheden overziet en diverse buddy's in diverse gemeenten begeleidt. Ook zouden buddy's op die manier niet aan slechts een specifieke gemeente gebonden hoeven zijn en kunnen ze over een groter gebied bedrijven helpen.

Verder wordt aangeraden dat er nog duidelijkere afspraken gemaakt worden over de verdeling van taken en verantwoordelijkheden tussen de uitvoerende gemeente medewerker(/coördinator), andere gemeentemedewerkers en cybersecurityexpert. Het hebben van een coördinator is wenselijk voor de ondersteuning van de buddy's in praktische zaken, maar welke taken en verantwoordelijkheden deze heeft zal ook deels afhangen van of de coördinator ook een stagiair is die begeleid wordt door een gemeentemedewerker, of dat deze taak volledig vervuld wordt door een gemeentemedewerker.

Een volgend verbeterpunt is het uitbreiden van de training van de buddy's. Tijdens de pilot kregen de buddy's twee trainingen van vier uur. De eerste training ging over het afnemen van de cyberscan en de tweede training over het schrijven van adviesrapport, waarbij er vooral tijd besteed is aan het invullen van de "standaard" adviezen per maatregel door de buddy's. De training zou meer tijd in beslag moeten nemen en op diverse manieren moeten worden uitgebreid. Ten eerste zou er, indien de buddy's worden geacht "koud" te werven, tijdens de training middels bijvoorbeeld een rollenspel meer tijd en aandacht moeten worden gegeven aan het werven van respondenten. Ten tweede zou de training over het schrijven van het adviesrapport meer tijd moeten worden besteed aan de unieke afwegingen die de buddy's dienen te maken per bedrijf. Er zouden in de training en het basis adviesrapport meer richtlijnen kunnen worden geboden over wanneer een advies precies wel of niet gegeven zou moeten worden. Hiernaast zou er tijdens de training geoefend kunnen worden met het schrijven van adviezen voor fictieve casussen, waarbij deel 1 van de cyberscan is ingevuld voor een aantal fictieve bedrijven. In de pilot is de keuze tussen verschillende adviezen overgelaten aan de buddy's en hebben zij dit naar eigen inzicht kunnen doen. Echter zijn in sommige gevallen zeer veel adviezen gegeven (maximum van 70 van de 73). Veel mkb'ers zullen hierbij hulp nodig hebben met

prioritering. Met behulp van een uitgebreidere training door een cybersecurityexpert zouden buddy's beter instaat worden gesteld een inschatting te maken van de relevantie van maatregelen voor specifieke bedrijven. Ook zou de buddy tijdens de cyberscan kunnen nagaan aan welk soort informatie de mkb'er behoefte heeft en tijdens de training leren hoe de buddy in deze informatiebehoefte kan voorzien, bijvoorbeeld naar welke bronnen met nadere informatie kan worden verwezen. Tegelijkertijd kan een buddy bij een bedrijf met lagere cyberweerbaarheid een deel van het rapport bondig houden, om duidelijke priortering aan te geven.

Tot slot kan de effectiviteit van de interventie eventueel worden verbeterd door een verbeterslag te maken in het standaard adviesrapport. Tijdens de pilot gaven enkele mkb'ers aan dat dit rapport te lang was en niet altijd volledig toegespitst leek op het specifieke bedrijf. Het is aan te raden dat de mkb'er ook een samenvatting van het rapport geboden wordt, zodat zij zelf, afhankelijk van hun behoeften, kunnen kiezen welk deel van het rapport ze lezen en gebruiken. Zo zou er per type maatregel een korte lijst geboden kunnen worden van de meest belangrijke 3 à 5 maatregelen die op korte termijn geïmplementeerd zouden moeten worden. Verderop in het rapport kan vervolgens de langere lijst geadviseerde maatregelen worden opgenomen, met maatregelen die over de komende maanden tot jaren geïmplementeerd zouden moeten worden. Ook zou de optie kunnen worden geboden dat de mkb'er de volledige resultaten van de cyberscan kunnen ontvangen.

8.4 Kanttekeningen bij het interpreteren van de resultaten

Bij het interpreteren van de onderzoeksresultaten van de pilot dient rekening gehouden te worden met een aantal (methodologische) beperkingen van dit onderzoek. Ten eerste betreft dit onderzoek een kleine groep van 36 mkb'ers en betreffen dit mkb'ers die open staan voor deelname aan het project. Hoewel een klein deel van de respondenten aangaf te hebben meegedaan zonder echt interesse te hebben in cybersecurity, is het aannemelijk dat een relatief groot deel van de respondenten dat heeft meegedaan aan het onderzoek al interesse hadden in of behoefte hadden aan het verbeteren van hun cybersecurity. Door deze zelfselectie zijn de resultaten van deze pilot niet generaliseerbaar zijn naar de totale populatie van het Nederlandse mkb, maar slechts naar mkb'ers die open staan voor deelname aan een cybersecurity gerelateerd project. Dit vermoeden wordt bijvoorbeeld ook bevestigd door het feit dat de sector ICT de op een na meest gerepresenteerde sector in dit onderzoek is. Het is ook belangrijk om te benoemen dat dit onderzoek geen controlegroep gehad heeft. Er is dus geen manier geweest om te controleren of een vergelijkbare groep mkb'ers over dezelfde tijdsperiode zonder deze interventie dezelfde veranderingen had doorgemaakt als de groep die wel de interventie heeft doorgemaakt. De onderzoekers verwachten echter op basis van de huidige kennis over cybersecurity gedrag van mkb'ers dat de waargenomen stijging van 34% in maatregelen in

een periode van zes weken hoger is dan gemiddeld had kunnen worden verwacht. Tot slot is zijn de resultaten van de cyberscan grotendeels gebaseerd op zelf-rapportage. De cyberscan is afgenomen tijdens een gesprek tussen de buddy en de mkb'er, wat maakt dat buddy's konden doorvragen over de manieren waarop de maatregelen zijn ingevoerd. Hoewel het niet waarschijnlijk is dat mkb'ers willens en wetens oneerlijk zouden zijn over ingevoerde maatregelen, kan er niet met zekerheid vast worden gesteld in welke mate mkb'ers die aangeven dat maatregelen zijn doorgevoerd dit ook daadwerkelijk hebben gedaan en of de maatregel volledig en op de juiste manier geïmplementeerd is.

8.5 Is de interventie "MKB cyber buddy's project" een effectieve interventie om voor Nederlandse gemeenten om de cyberweerbaarheid van mkb'ers in hun gemeente rondom ransomware te bevorderen?

Alles bij elkaar genomen kan gesteld worden dat de interventie een effectieve tool is voor Nederlandse gemeenten om de cyberweerbaarheid van een specifieke groep mkb'ers in hun gemeente te bevorderen. Deze groep mkb'ers bestaat uit mkb'ers die behoefte hebben aan of open staan voor een project om de cyberweerbaarheid van hun onderneming te toetsen en (indien nodig) verbeteren. Deze mkb'ers hebben bijvoorbeeld zelf de gemeente benaderd met interesse om deel te nemen aan een project rondom cybersecurity of stonden hiervoor open nadat zij benaderd werden voor de buddy (6.4% van alle benaderde mkb'ers). Na deelname aan het project is er sprake van een hogere mate van cyberweerbaarheid, gezien de toename van het aantal cybersecurity maatregelen dat deelnemende bedrijven lijken te nemen door hun deelname aan "MKB Cyber buddy's".

"MKB Cyber buddy's" is een geschikte interventie voor gemeenten op zoek zijn naar een effectieve tool om mkb'ers die behoefte hebben aan informatie en hulp rondom cybersecurity in deze behoefte te voorzien. Wij raden aan het project te presenteren bij ondernemings-bijeenkomsten over cybersecurity, die door vele gemeenten reeds worden georganiseerd, waarbij ondernemers de optie geboden worden om zichzelf gelijk aan te melden voor "MKB Cyber buddy's".

Literatuur

Alert Online. (2019). *Nationaal Cybersecurity Bewustzijnsonderzoek 2019* (Issue september). https://www.alertonline.nl/media/Alert-Online-Cybersecuritybewustzijnsonderzoek-2019-2.pdf

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. In *Computers and Security* (Vol. 74, pp. 144–166). Elsevier Ltd. https://doi.org/10.1016/j.cose.2018.01.001

Bekkers, L., van der Kleij, R., Schippers, N., & Leukfeldt, R. (2020). *Cyberweerbaarheidsapp MKB. Ontwikkeling van een webapplicatie om de digitale weerbaarheid van het MKB te vergroten.*

Bekkers, L., van 't Hoff-de Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, R. (2021). *Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Risicobewustzijn en preventief gedrag wat betreft ransomware en phishing. Doelgroep mkb. Deelrapport werkpakket 3.*

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*. https://doi.org/10.1016/j.tele.2021.101675

CBS. (2018). *Cybersecurity Monitor 2018*. Centraal Bureau voor de Statistiek.

CBS. (2021). *Cybersecuritymonitor 2021*. https://www.cbs.nl/nl-nl/longread/rapportages/2022/cybersecuritymonitor-2021

CBS. (2022). *Veiligheidsmonitor 2021*. Centraal Bureau voor de Statistiek.

Chainalysis. (2022). *The 2022 Crypto Crime Report*. https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Datto. (2020). *Datto's Global State of the Channel Ransomware Report*. https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30,*(2,), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. In *Internet of Things (Netherlands)* (Vol. 11). Elsevier B.V. https://doi.org/10.1016/j.iot.2020.100204

Hollnagel, E. (2015). *RAG - Resilience Analysis Grid*.

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, *8*(1). https://doi.org/10.1186/s40163-019-0097-9

Ipsos. (2018). *Cyber Security. Opvallende uitkomsten cyberonderzoek*. https://nieuws.centraalbeheer.nl/download/637007/centraalbeheer-cybersecurityonderzoekjanuari2019-819448.pdf

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

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

Leukfeldt, E. R., Kentgens, A., Prins, E., & Stol, W. (2015). *Alledaags politiewerk in een gedigitaliseerde wereld. Handreiking voor de intake van delicten met een digitale component.*

Leukfeldt, E. R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit*. WODC.

Lévesque, F. L., Chiasson, S., Somayaji, A., & Fernandez, J. M. (2018). Technological and Human Factors of Malware Attacks. *ACM Transactions on Privacy and Security*, *21*(4), 1–30. https://doi.org/10.1145/3210311

Levesque, F. L., Fernandez, J. M., & Somayaji, A. (2014). Risk prediction of malware victimization based on user behavior. *Proceedings of the 9th IEEE International Conference on Malicious and Unwanted Software, MALCON 2014*, 128–134. https://doi.org/10.1109/MALWARE.2014.6999412

Linkov, I., & Kott A. (2018). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In A. , L. I. Kott (Ed.), *Cyber Resilience of Systems and Networks*. https://doi.org/https://doi.org/10.1007/978-3-319-77492-3_1

Lopez, M. A., Lombardo, J. M., López, M., Alba, C. M., Velasco, S., Braojos, M. A., & Fuentes-García, M. (2020). Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises. *International Journal of Interactive Multimedia and Artificial Intelligence*, *6*(3), 55. https://doi.org/10.9781/ijimai.2020.08.003

Michie, S., Stralen, M. M. van, & West, R. (2011). *The behaviour change wheel: A new method for characterising and designing behaviour change interventions*. *42*(6). https://doi.org/10.1186/1748-5908-6-42

Misana-ter Huurne, E., van Houten, Y., Spithoven, R., Notté, R., & Leukfeldt, R. (2020). *Cyberweerbaarheid: risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb-ers*. https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/saxion--haagse-hogeschool---cyberweerbaarheid.-risicobewustzijn-en-zelfbeschermend-gedrag-rondom-cybercrime-onder-jongeren-en-mkb-ers.pdf

Misana-ter Huurne, E., van ’t Hoff-de Goede, S., Bekkers, L., van Houten, Y., Walther, M., Spithoven, R., & Leukfeldt, R. (2021). *Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Kwetsbare doelgroepen en bijbehorende typen cyberdelicten. Geïntegreerd deelrapport werkpakketten 1 en 2.*

Moneva, A., & Leukfeldt, E. R. (2022). Insider Threats Among Dutch SMEs: Nature and Extent of Incidents, and Cyber Security Measures. *OSF Preprints.* https://doi.org/https://doi.org/10.31219/osf.io/eqpb2

Notté, R., Slot, L., van ’t Hoff-de Goede, S., & Leukfeldt, E. R. (2019). *Cybersecurity in het mkb - Nulmeting*. Centre of Expertise Cyber Security, De Haagse Hogeschool.

Ovelgönne, M., Dumitras, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks. *ACM Transactions on Intelligent Systems and Technology*, *8*(4), 1–25. https://doi.org/10.1145/2890509

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114.

Spithoven, R. (2020). *Verbonden risico’s : maatschappelijke veiligheid in de black box society*. Boomcriminologie.

Tuttle, W. J. (2020). *Effective Strategies Small Business Leaders Use to Address Ransomware*. Doctoral dissertation, Walden University. https://scholarworks.waldenu.edu/dissertations

van der Kleij, R., & Leukfeldt, E. R. (2019). Cyber Resilient Behavior : Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In *International conference on applied human factors and ergonomics* (Issue February, pp. 16–27). Springer, Cham.

Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Cybercrime onder bedrijven*. https://www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/Cybercrime onder bedrijven definitief rapport.pdf

Wetzer, I. (2018). Cyberveilig gedrag: waarom doen we het nou niet? *Informatiebeveiliging*, *1*, Albladi, S. M., Weir, G. R. S. (2018). User char.

Zimba, A., & Chishimba, M. (2019). Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures. *International Journal of Computer Network and Information Security*, *11*(1), 26–39. https://doi.org/10.5815/ijcnis.2019.01.03

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Bijlage 1: Op te vragen documenten

Gemeentes die de interventie MKB Cyber Buddy's zelf willen uitvoeren, kunnen bij de auteurs van dit rapport een map met ondersteunende documenten opvragen. Deze map bevat de volgende documenten:

1) Een uitleg van de inhoud en het gebruik van elk document
2) De voormeting van de cyberscan
3) De nameting van de cyberscan
4) De template voor het adviesrapport
5) Een leeg bestand om het veldwerkoverzicht bij te houden
6) Een leeg bestand om een verslag van het werven bij te houden
7) Een voorbeeld van een planning voor de buddy's
8) PowerPoint slides voor de training van de buddy's
9) Een informatiefolder voor het werven

Bijlage 2: De cyberscan – voormeting

Cyberscan

voor de pilot van de

interventie 'MKB Cyber Buddy's'

van het consortium "Cyberweerbaarheid. Een gemeentelijk offensief
ter preventie van slachtofferschap van cybercrime."

Voormeting

februari 2022

dr. S. van 't Hoff-de Goede (Centre of Expertise Cyber Security, De Haagse Hogeschool)
Gemeente Den Helder
Gemeente Enschede
Gemeente Utrecht

Introtekst

Dank voor uw medewerking! U heeft zich aangemeld voor het project MKB Cyber Buddy's' van de gemeente Utrecht/Enschede/Den Helder *(1 noemen)*. In dit project neemt uw buddy - dat ben ik – een cybersecurity scan af in uw bedrijf, ontwikkelt door onderzoekers van de Haagse Hogeschool. Vervolgens schrijf ik een op maat gemaakt advies rapport en ben ik beschikbaar om u 2 dagen te helpen met het verhogen van de cyberweerbaarheid van uw organisatie. Het project eindigt met een eindinterview.
De cybersecurityscan die ik nu met u ga doornemen bestaat uit zes onderdelen, te weten 1. De activiteiten in uw bedrijf, 2. Uw visie op cybersecurity, 3. Levering van ICT, 4. Beleid, 5. Technische maatregelen en 6. Medewerkers. Aan het einde maken we afspraken over het inplannen van het eind interview en de rest van het project.
Uw gegevens worden geanonimiseerd verwerkt. Uw bedrijfsnaam en eigen naam worden niet gepubliceerd. Ik (de onderzoeker) noteer de antwoorden via een online vragenlijst.

Heeft u nog vragen voordat we kunnen beginnen?

Informed consent
Heeft u alle informatie begrepen en gaat u akkoord met deelname aan dit onderzoek?
☐ Ja

Contactgegevens

1. Naam Buddy
   [open antwoord]
2. Code bedrijf
   [open antwoord]

Selectievraag

1. Welke van de volgende uitspraken is op u van toepassing?

☐ Ik ben een ondernemer met personeel (maximaal 250 werknemers) en draag verantwoordelijkheid over de cybersecurity

☐ Ik ben werkzaam binnen een mkb bedrijf (maximaal 250 werknemers) en draag verantwoordelijkheid over de cybersecurity

☐ geen van deze uitspraken zijn van mij op toepassing → u kunt niet deelnemen aan dit onderzoek. Zou u mij kunnen doorverwijzen naar degene die verantwoordelijk is voor de cybersecurity in uw organisatie?

2. Waar vindt dit gesprek plaats?
   ☐ Fysiek
   ☐ Videobellen

3. In welke gemeente is dit bedrijf gevestigd?
   ☐ Utrecht
   ☐ Enschede
   ☐ Den Helder

Onderdeel I: de activiteiten in uw bedrijf

1. In welke sector is uw bedrijf actief?
   [open antwoord]

2. Hoeveel medewerkers heeft uw bedrijf?

3. Welke van de volgende mogelijkheden heeft of gebruikt uw bedrijf?

		Ja	*Nee*	*Weet ik niet*
1	Klanten kunnen online bestellen, reserveren, betalen voor producten of diensten, of een schenking doen			
2	Klanten kunnen online toegang krijgen tot (enkele) van uw diensten			
3	Het elektronisch opslaan van persoonlijke gegevens van uw klanten, begunstigden, gebruikers of donateurs			
4	Verwerken of beheren van persoonlijke gegevens en/of financiële gegevens en/of medische informatie van derden			
5	Ontwikkeling van software voor intern gebruik of bedienen van klanten			
	Heeft uw bedrijf…			
6	..een online bankrekening waarnaar uw klanten betalingen kunnen overmaken			
7	..een industrieel controlesysteem (ook wel ICS/SCADA/Operationele techniek, dit zijn meet- en regelsystemen voor de aansturing van industriële processen of gebouwbeheersingssystemen)			

8	..een Enterprise Resource Planning (ERP) systeem			
9	..financiële of boekhoudingssoftware			
10	..accounts of pagina's op socialmediawebsites (zoals Facebook of Twitter)			
11	..online apparatuur, zoals online camera's, machines en printers			
12	Is er nog een andere mogelijkheid die relevant lijkt in deze lijst? Ja, namelijk…… *[open antwoord]*			

4. Voeren medewerkers de onderstaande activiteiten wel eens uit tijdens werktijd?:

		Ja	*Nee*	*Weet ik niet*
1	Het gebruik van persoonlijke apparaten (zoals smartphones, tablets, eigen laptops of desktop computers) voor bedrijfsdoeleinden			
2	Het gebruik van persoonlijke accounts of pagina's op socialmediawebsites (bijvoorbeeld Facebook of Twitter) voor bedrijfsdoeleinden			
3	Het gebruik van of kopen via e-commerce services (bijvoorbeeld online goederen bestellen)			
4	Openbare wifi-netwerken gebruiken			
5	Verbinding maken met het wifi-netwerk van uw bedrijf			
6	Verbinding maken met het wifi-netwerk van een verzamelgebouw			
7	Verbinding maken met hun eigen wifi-netwerk			
8	Het gebruik van cloud-diensten			
9	Zo ja, welke? [*open antwoord]*			
10	Op afstand toegang krijgen tot een digitale werkplek			
11	Het opslaan van vertrouwelijke informatie			
12	Een andere activiteit die relevant lijkt in deze lijst, namelijk…… *[open antwoord]*			

5. Welke van de onderstaande activiteiten <u>voor privé-doeleinden</u> voeren medewerkers binnen uw bedrijf wel eens uit tijdens werktijd?

		Ja	*Nee*	*Weet ik niet*
1	Het gebruik van zakelijke apparaten voor privé-doeleinden (zoals smartphones, tablets, laptops of desktop computers)			
2	Het gebruik van bedrijfsaccounts of -pagina's op socialmediawebsites (zoals Facebook of Twitter) voor privé-doeleinden			
3	Het gebruik van een bedrijfsaccount (zoals e-mail, bankieren) om een aankoop te doen via e-commerce bedrijven voor privé-doeleinden			
4	Verbinding maken met de wifi van uw bedrijf voor privé-doeleinden			
5	Het gebruik van zakelijke cloud-diensten voor privé-doeleinden			
6	Op afstand toegang krijgen tot een digitale werkplek voor privé-doeleinden			
7	Het gebruik van vertrouwelijke bedrijfsinformatie voor privé-doeleinden			
8	Een andere activiteit die relevant lijkt in deze lijst, namelijk……			

	[open antwoord]			

Onderdeel 2: Uw visie op cybersecurity en cyberweerbaarheid

6. In hoeverre maakt u zich zorgen over…

		Helemaal niet	Een beetje	Enigszins	Nogal	Heel veel
1	*..de kans dat uw bedrijf slachtoffer wordt van cybercriminaliteit?*	□	□	□	□	□
2	*..de mogelijke schade die uw bedrijf oploopt door slachtofferschap van cybercriminaliteit?*	□	□	□	□	□

7. Hoe hoog of laag is voor u de prioriteit van cybersecurity van uw organisatie?

☐ Zeer hoog
☐ Redelijk hoog
☐ Redelijk laag
☐ Erg laag
☐ Weet ik niet

8. In hoeverre bent u bezig om kwetsbaarheden in uw cyberweerbaarheid in beeld te brengen?

☐ Daar zijn we niet mee bezig omdat we niet weten hoe of omdat we het niet belangrijk vinden en we hebben er ook geen intentie toe
☐ We zijn er nog niet mee bezig maar hebben daar wel de intentie toe
☐ We zijn bezig voorbereidingen te treffen maar hebben nog geen harde actie ondernomen
☐ Dat vinden we belangrijk en zijn ook al druk bezig
☐ We vinden het belangrijk en zijn al erg ver gevorderd, dit willen we zo houden

Onderdeel 3: levering van ICT

De volgende vragen gaan over de levering van ICT.

9. Maakt uw bedrijf gebruik van een externe IT-leverancier?
    a. Ja
    b. Nee *[→ ga naar vraag 14]*

10. Levert de externe IT-leverancier ook cybersecurity producten of diensten?
    a. Ja
    b. Nee
    c. Weet ik niet

11. Zo ja, welke diensten?
    [open antwoord]

12. Rapporteert de externe leverancier van uw ICT aan u over cybersecurity?
    a. Ja *(Ik wil u vragen, na dit gesprek, dit rapport met mij te delen)*
    b. Nee

13. Heeft u met de externe IT-leverancier afspraken gemaakt over wie verantwoordelijk is voor de cybersecurity van uw onderneming?
    a. Ja
    b. Nee

14. Heeft uw IT-leverancier relevante certificaten (zoals ISO27001) behaald?
    a. Ja
    b. Nee

Onderdeel 4. Cybersecurity beleid

De volgende vragen gaan over uw interne cybersecurity beleid.

15. Welke van de volgende afspraken op het gebied van beheer of risicomanagement heeft u ingevoerd?

		Ja	*Nee*	*Weet ik niet*
1	Specifieke personen (bestuursleden, beheerders, een bestuurder of senior manager) zijn verantwoordelijk voor cybersecurity			
2	Er zijn specifieke medewerkers wiens functie informatieveiligheid omvat *(dit is anders dan 14.1; 14.1 is een verantwoordelijkheid, 14.2 is een functie.)*			
3	Een bedrijfscontinuïteitsplan dat cyberincidenten omvat			
4	Een Information Security Management systeem (ISMS)			
5	Een andere afspraak die relevant lijkt in deze lijst, namelijk…… [open antwoord]			

16. Heeft uw organisatie een formeel beleid met betrekking tot cybersecurity risico's (zoals over het gebruik van persoonlijke apparaten, of een back-up beleid, of een wachtwoordbeleid)?
    a. Ja
    b. Nee *[ga naar vraag 19]*

17. Welke van de volgende aspecten vallen onder uw cybersecurity beleid? In ons beleid zijn er afspraken over...

		Ja	*Nee*	*Weet ik niet*
1	*Wat voor soort gegevens bewaard mogen worden op verwijderbare apparaten (zoals USB sticks)*			
2	*Mobiel werken of werken op afstand (bijvoorbeeld thuiswerken)*			
3	*Wat personeel mag doen op de IT-apparaten van uw bedrijf*			
4	*Gebruik van persoonlijke apparaten voor bedrijfsactiviteiten*			
5	*Gebruik van nieuwe digitale technologieën zoals cloud-computing*			
6	*Classificering van gegevens*			
7	*Een systeem voor documentenbeheer*			
8	*Back-up beleid*			

9	*Een wachtwoordbeleid dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen*			
10	*Omgang met Internet of Things apparatuur (online apparatuur, zoals camera's)*			
11	*Het veilig opslaan van bestanden met persoonsgegevens*			
12	Een ander aspect dat relevant lijkt in deze lijst, namelijk…… [open antwoord]			

18. Wanneer is uw beleid of zijn uw richtlijnen voor cybersecurity voor het laatst bijgewerkt of herzien om te controleren of alles up-to-date is?

☐ In de afgelopen 6 maanden
☐ 6 tot 12 maanden geleden
☐ 12 tot 24 maanden geleden
☐ 24 maanden of langer geleden
☐ het beleid/de richtlijnen zijn nog nooit bijgewerkt, ze zijn opgesteld op….. *[datum/jaar]*
☐ Weet ik niet

19. Heeft uw organisatie relevante certificaten (zoals ISO27001) behaald?
    a. Ja
    b. Nee

Onderdeel 5: Technische maatregelen

Nu wil ik het hebben over de technische controlemaatregelen van uw bedrijf.

20. Welke van de volgende controlemaatregelen heeft uw bedrijf ingevoerd?

		Ja	*Nee*	*Weet ik niet*
1	*Het uitvoeren van software-updates zodra deze beschikbaar zijn*			
2	Standaard instellingen van software en computers nakijken en aanpassen			
3	*Up-to-date software tegen malware*			
4	*Firewalls die zowel uw volledige IT-netwerk beschermen, als individuele apparaten*			
5	*Overige software om laptops te beveiligen (b.v. EDR endpoint detection & response)*			
6	*Intrusion detectie software op het netwerk*			
7	*Er is beveiligingsoftware geïnstalleerd op telefoons met bedrijfgegevens*			
8	*Er is een actuele lijst met software en versie nummers*			
9	*Het functieprofiel van de medewerker bepaalt diens toegangsrechten tot onderdelen van het bedrijfsnetwerk (bijvoorbeeld: magazijnmedewerker kan niet bij salarisadministratie)*			
10	*Toegangsrechten worden goed bijgehouden en zijn bijgewerkt* (bijvoorbeeld bij ontslag of verandering functie)			
11	*IT-administratie rechten zijn beperkt tot specifieke gebruikers*			

12	*IT-administratie rechten worden goed bijgehouden en zijn bijgewerkt*			
13	*Monitoring van gebruikersactiviteiten*			
14	*Specifieke regels voor het veilig opslaan van bestanden met persoonsgegevens*			
15	*Veiligheidsrestricties van apparaten die eigendom zijn van het bedrijf (bijvoorbeeld beperkte mogelijkheden om software op laptops te installeren)*			
16	*Toegang tot het bedrijfsnetwerk is alleen mogelijk op apparaten die eigendom zijn van het bedrijf*			
17	*Gescheiden wifi-netwerken voor personeel en gasten*			
18	*Actuele back-up van gegevens via een cloud-dienst*			
19	*Actuele back-up van gegevens via andere middelen*			
20	*Een wachtwoordkluis of manager*			
21	*Een VPN-verbinding voor op kantoor en remote werken*			
22	*Bestanden met gevoelige gegevens versleuteld opslaan en versturen (encryptie)*			
23	*Aangesloten bij een Security Operatie Centrum*			
24	*2 factor authenticatie*			
25	*Fysieke toegang tot het bedrijf is alleen gecontroleerd mogelijk*			
26	*Bedrijfslaptops kunnen op afstand geblokkeerd en opgeschoond worden*			
27	*Bedrijfstelefoons kunnen op afstand geblokkeerd en opgeschoond worden*			
28	*De organisatie doet regelmatig een technische penetratie test*			
29	Een andere afspraak die relevant lijkt in deze lijst, namelijk…… [open antwoord]			

Onderdeel 6: medewerkers

Hoe medewerkers omgaan met cyberrisico's en maatregelen is ook onderdeel van cybersecurity. We willen u nu 27 stellingen voorleggen hierover. Deze stellingen belichten het onderwerp van verschillende kanten, zodat wij een op maat gemaakt advies kunnen opstellen voor u.

21. In hoeverre bent u het eens met de volgende stellingen?

	Stellingen	**Hele-maal mee oneens**	**Redelijk mee oneens**	**Niet mee oneens/ eens**	**Redelijk mee eens**	**Hele-maal mee eens**
1	Medewerkers weten hoe we cyberincidenten op het werk kunnen voorkomen					
2	Medewerkers kennen onze belangrijkste risico's op het gebied van cybersecurity					
3	Ons bedrijf traint de medewerkers in cyberbeveiliging					
4	Medewerkers in ons bedrijf weten dat zij een belangrijke rol spelen bij het voorkomen van cyberincidenten					

5	Medewerkers in ons bedrijf vinden het belangrijk om cyberaanvallen- en incidenten te voorkomen					
6	Medewerkers in ons bedrijf weten hoe ze cyberaanvallen, zoals via een phishing-email, kunnen herkennen					
7	Medewerkers weten hoe ze verdachte links op betrouwbaarheid kunnen checken					
8	Medewerkers worden regelmatig getest op kennis en over de ervaringen van anderen.					
9	Ons bedrijf heeft duidelijke normen voor wat een cyberincident is en wat niet					
10	Ons bedrijf heeft duidelijke voorschriften over het bepalen van de veiligheid van bijlagen en hyperlinks in e-mails					
11	Medewerkers in het bedrijf vinden zichzelf bekwaam in het detecteren van cyberaanvallen- en incidenten					
12	Medewerkers in ons bedrijf zien het als hun verantwoordelijkheid om eerst de betrouwbaarheid van de afzender na te gaan, voordat zij bijlagen in e-mails openen					
13	Ons bedrijf heeft een helder stappenplan over wat te doen in het geval van een cyberaanval of -incident, zoals een ransomware aanval					
14	Medewerkers in ons bedrijf kennen dit stappenplan en hebben hiermee geoefend					
15	Ons bedrijf geeft het melden van cyberaanvallen- en incidenten een hoge prioriteit					
16	Medewerkers in ons bedrijf weten hoe zij een cyberaanval- of incident moeten melden					
17	Medewerkers in ons bedrijf vinden het belangrijk om cyberaanvallen- en incidenten altijd direct te melden					
18	Medewerkers in ons bedrijf vinden het belangrijk om collega's aan te spreken op cyberonveilig gedrag, zoals bij het niet vergrendelen van het beeldscherm bij het verlaten van de werkplek					
19	Medewerkers in ons bedrijf hebben de vaardigheden om te leren van cyberaanvallen- en incidenten					
20	Als management vragen wij onze medewerkers naar hun mening over het cybersecuritybeleid					
21	Ons bedrijf test regelmatig procedures over hoe om te gaan met een cyberaanval- of					

	incident, bijvoorbeeld in de vorm van een oefening of test					
22	Geleerde lessen, bijvoorbeeld na een incident of cybercrisisoefening, worden toegepast in het cybersecuritybeleid					
23	Geleerde lessen worden gecommuniceerd binnen de organisatie					
24	Medewerkers worden in staat gesteld om te leren van cyberaanvallen- en incidenten die zich in het bedrijf hebben voorgedaan					
25	In ons bedrijf geven wij elkaar feedback op het gebied van cyberveilig gedrag					
26	Medewerkers in ons bedrijf zijn bereid om deel te nemen aan oefeningen waar de cyberbeveiliging wordt getest					
27	Medewerkers in ons bedrijf nemen regelmatig de tijd om na te denken over wat goed gaat en wat beter kan met betrekking tot hun cyberveiligheid.					

Bijlage 3: De cyberscan – nameting

Cyberscan

voor de pilot van de

interventie 'MKB Cyber Buddy's'

van het consortium "Cyberweerbaarheid. Een gemeentelijk offensief
ter preventie van slachtofferschap van cybercrime."

Na-meting

februari 2022

dr. S. van 't Hoff-de Goede (Centre of Expertise Cyber Security, De Haagse Hogeschool)
Gemeente Den Helder
Gemeente Enschede
Gemeente Utrecht

Introtekst

Nogmaals dan voor uw medewerking aan het MKB cyberbuddy's project! Ik heb een tijd terug een cybersecurity-scan bij uw bedrijf uitgevoerd en op basis hiervan heeft u een aantal adviezen gekregen in een rapport *[en hebben we samen geprobeerd deze uit te voeren]*. We zijn nu een aantal weken verder en ik ga opnieuw een vragenlijst met u aflopen. Een aantal vragen heb ik vorige keer ook al gesteld. Deze worden nu opnieuw gesteld om te kijken of er dingen veranderd zijn. Daarnaast zullen er ook een aantal nieuwe vragen zijn.
De vragenlijst die we nu zullen doornemen bestaat uit zes onderdelen, namelijk 1. Uw visie op cybersecurity, 2. Levering van ICT 3. Beleid 4. Technische maatregelen, 5. Medewerkers en 6. Uw ervaring met dit project.
Wederom wordt alles geanonimiseerd en worden uw bedrijfsnaam en eigen naam nergens gepubliceerd. Ik noteer de antwoorden weer via een online vragenlijst.
Heeft u nog vragen voordat we kunnen beginnen?

Informed consent
Heeft u alle informatie begrepen en gaat u akkoord met deelname aan dit onderzoek?
☐ Ja

Contactgegevens

1. Naam Buddy
   [open antwoord]
2. Code bedrijf
   [open antwoord]

3. Waar vindt dit gesprek plaats?
   ☐ Fysiek
   ☐ Videobellen

Onderdeel 1: Uw visie op cybersecurity en cyberweerbaarheid

4. In hoeverre maakt u zich zorgen over…

		Helemaal niet	Een beetje	Enigszins	Nogal	Heel veel
1	*..de kans dat uw bedrijf slachtoffer wordt van cybercriminaliteit?*	□	□	□	□	□
2	*..de mogelijke schade die uw bedrijf oploopt door slachtofferschap van cybercriminaliteit?*	□	□	□	□	□

5. Hoe hoog of laag is voor u de prioriteit van cybersecurity van uw organisatie?

☐ Zeer hoog
☐ Redelijk hoog
☐ Redelijk laag
☐ Erg laag
☐ Weet ik niet

Onderdeel 2: levering van ICT

6. Heeft u sinds ons eerste gesprek een externe IT-leverancier aangenomen voor cybersecurity producten of diensten?

a. Ja
b. Nee
c. Die hadden we al

7. Zijn er sinds ons eerste gesprek veranderingen aangebracht in uw afspraken met uw externe IT-leverancier?
   a. Ja, namelijk….
   b. Nee
   c. Niet van toepassing, we hadden nog geen leverancier

Onderdeel 3: cybersecurity beleid in uw organisatie

De volgende vragen gaan over uw interne cybersecurity beleid.

8. Welke van de volgende afspraken op het gebied van beheer of risicomanagement heeft u ingevoerd op basis van het adviesrapport?

		Dit is mij geadviseerd en ik heb dit zelf ingevoerd	**Dit is mij geadviseerd en ik heb dit ingevoerd met behulp van mijn buddy**	**Dit is mij geadviseerd en we zijn begonnen met invoeren, maar zijn nog niet klaar**	**Dit is mij geadviseerd maar ik heb dit niet ingevoerd**	**Dit is mij niet geadviseerd**
1	Specifieke personen (bestuursleden, beheerders, een bestuurder of senior manager) zijn verantwoordelijk voor cybersecurity					
2	Er zijn specifieke medewerkers wiens functie informatieveiligheid omvat *(dit is anders dan 14.1; 14.1 is een verantwoordelijkheid, 14.2 is een functie.)*					
3	Een bedrijfscontinuïteitsplan dat cyberincidenten omvat					
4	Een Information Security Management systeem (ISMS)					
5	Een andere afspraak die relevant lijkt in deze lijst, namelijk…… [open antwoord]					

9. Heeft uw organisatie een formeel beleid met betrekking tot cybersecurity risico's (zoals over het gebruik van persoonlijke apparaten, of een back-up beleid, of een wachtwoordbeleid)?
    d. Ja
    e. Nee *[ga naar vraag 8]*

10. Heeft u sinds ons eerste gesprek uw cybersecurity beleid of uw richtlijnen voor cybersecurity gecontroleerd, bijgewerkt of herzien?

☐ Ja
☐ Nee

11. Welke van de volgende aspecten hebt u toegevoegd aan uw cybersecurity beleid, op basis van het adviesrapport?

		Dit is mij geadviseerd en ik heb dit zelf ingevoerd	**Dit is mij geadviseerd en ik heb dit ingevoerd met behulp van mijn buddy**	**Dit is mij geadviseerd en we zijn begonnen met invoeren, maar zijn nog niet klaar**	**Dit is mij geadviseerd maar ik heb dit niet ingevoerd**	**Dit is mij niet geadviseerd**
1	*Wat voor soort gegevens bewaard mogen worden op verwijderbare apparaten (zoals USB sticks)*					
2	*Mobiel werken of werken op afstand (bijvoorbeeld thuiswerken)*					
3	*Wat personeel mag doen op de IT-apparaten van uw bedrijf*					
4	*Gebruik van persoonlijke apparaten voor bedrijfsactiviteiten*					
5	*Gebruik van nieuwe digitale technologieën zoals cloud-computing*					
6	*Classificering van gegevens*					
7	*Een systeem voor documentenbeheer*					
8	*Back-up beleid*					
9	*Een wachtwoordbeleid dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen*					
10	*Omgang met Internet of Things apparatuur (online apparatuur, zoals camera's)*					

11	*Het veilig opslaan van bestanden met persoonsgegevens*					
12	Een ander aspect dat relevant lijkt in deze lijst, namelijk…… [open antwoord]					

Onderdeel 4: technische maatregelen

Nu wil ik het hebben over de technische maatregelen van uw bedrijf.

12. Welke van de volgende controlemaatregelen heeft uw bedrijf ingevoerd op basis van het adviesrapport?

		Dit is mij geadviseerd en ik heb dit zelf ingevoerd	**Dit is mij geadviseerd en ik heb dit ingevoerd met behulp van mijn buddy**	**Dit is mij geadviseerd en we zijn begonnen met invoeren, maar zijn nog niet klaar**	**Dit is mij geadviseerd maar ik heb dit niet ingevoerd**	**Dit is mij niet geadviseerd**
1	*Het uitvoeren van software-updates zodra deze beschikbaar zijn*					
2	Standaard instellingen van software en computers nakijken en aanpassen					
3	*Up-to-date software tegen malware*					
4	*Firewalls die zowel uw volledige IT-netwerk beschermen, als individuele apparaten*					
5	*Overige software om laptops te beveiligen (b.v. EDR endpoint detection & response)*					

6	*Intrusion detectie software op het netwerk*					
7	*Er is beveiligingsoftware geïnstalleerd op telefoons met bedrijfgegevens*					
8	*Er is een actuele lijst met software en versie nummers*					
9	*Het functieprofiel van de medewerker bepaalt diens toegangsrechten tot onderdelen van het bedrijfsnetwerk (bijvoorbeeld: magazijnmedewerker kan niet bij salarisadministratie)*					
10	*Toegangsrechten worden goed bijgehouden en zijn bijgewerkt*					
11	*IT-administratie rechten zijn beperkt tot specifieke gebruikers*					
12	*IT-administratie rechten worden goed bijgehouden en zijn bijgewerkt*					
13	*Monitoring van gebruikersactiviteiten*					
14	*Specifieke regels voor het veilig opslaan van bestanden met persoonsgegevens*					
15	*Veiligheidsrestricties van apparaten die eigendom zijn van het bedrijf (bijvoorbeeld beperkte mogelijkheden om software op laptops te installeren)*					

16	*Toegang tot het bedrijfsnetwerk is alleen mogelijk op apparaten die eigendom zijn van het bedrijf*					
17	*Gescheiden wifi-netwerken voor personeel en gasten*					
18	*Actuele back-up van gegevens via een cloud-dienst*					
19	*Actuele back-up van gegevens via andere middelen*					
20	*Een wachtwoordkluis of manager*					
21	*Een VPN-verbinding voor op kantoor en remote werken*					
22	*Bestanden met gevoelige gegevens versleuteld opslaan en versturen (encryptie)*					
23	*Aangesloten bij een Security Operatie Centrum*					
24	*2 factor authenticatie*					
25	*Fysieke toegang tot het bedrijf is alleen gecontroleerd mogelijk*					
26	*Bedrijfslaptops kunnen op afstand geblokkeerd en opgeschoond worden*					
27	*Bedrijfstelefoons kunnen op afstand geblokkeerd en opgeschoond worden*					
28	*De organisatie doet regelmatig een technische penetratie test*					
29	Een andere afspraak die					

	relevant lijkt in deze lijst, namelijk…… [open antwoord]					

13. hebben er sinds de eerste keer dat wij elkaar spraken andere veranderingen plaatsgevonden met betrekking tot de technische maatregelen van uw bedrijf?
    f. Ja, namelijk……
    g. Nee

Onderdeel 5: medewerkers

We hebben u vorige keer een lijst stellingen voorgelegd over uw medewerkers en hoe zij omgaan met cybersecurity. Op basis van die stellingen heb ik u een aantal adviezen gegeven.

14. Welke van de volgende adviezen heeft uw bedrijf opgepakt op basis van het adviesrapport?

	Advies	***Middel***	**Dit is mij geadviseerd en ik heb dit zelf ingevoerd**	**Dit is mij geadviseerd en ik heb dit ingevoerd met behulp van mijn buddy**	**Dit is mij geadviseerd en we zijn begonnen met invoeren, maar zijn nog niet klaar**	**Dit is mij geadviseerd maar ik heb dit niet ingevoerd**	**Dit is mij niet geadviseerd**
	Anticiperen						
1	Medewerkers een training geven over hoe ze cyberincidenten op het werk kunnen voorkomen	Training					
2	Medewerkers inlichten over belangrijkste risico's op het gebied van cybersecurity voor dit bedrijf	Training & communicatie					
3	Medewerkers trainen in cyberbeveiliging	Training					
4	Medewerkers in het bedrijf bewust maken van de belangrijke rol die zij spelen bij het voorkomen van cyberincidenten	Training & communicatie					
5	Medewerkers motiveren om cyberaanvallen- en incidenten te willen voorkomen	Training					
	Detecteren						

6	Medewerkers leren hoe ze cyberaanvallen kunnen herkennen	Training					
7	Medewerkers leren hoe ze verdachte links op betrouwbaarheid kunnen checken	Training					
8	Medewerkers regelmatig testen op hun kennis en over de ervaringen van anderen.	Beleid & pentesten					
9	Duidelijke normen opstellen voor wat een cyberincident is en wat niet	Beleid & communicatie					
10	Duidelijke voorschriften opstellen over het bepalen van de veiligheid van bijlagen en hyperlinks in e-mails	Beleid & communicatie					
11	Medewerkers trainen in het detecteren van cyberaanvallen- en incidenten	Training					
12	Medewerkers informeren over hun eigen verantwoordelijkheid bij het nagaan van de betrouwbaarheid van de afzender, voordat zij bijlagen in e-mails openen	Training & communicatie					
	Reageren						
13	Voor medewerkers een duidelijk stappenplan opstellen over wat ze moeten doen in het geval van een cyberaanval of -incident, zoals een ransomware aanval	Beleid					
14	Medewerkers informeren over dit stappenplan en ze hiermee laten oefenen	Communicatie & Training					
15	Binnen het bedrijf prioriteit geven aan het melden van	Beleid & Communicatie					

	cyberaanvallen- en incidenten						
16	Duidelijk richtlijnen opstellen over hoe medewerkers een cyberaanval- of incident moeten melden	Beleid					
17	Medewerkers motiveren cyberaanvallen- en incidenten direct te melden	Communicatie & Training					
18	Medewerkers inlichten over het belang van collega's aanspreken op cyberonveilig gedrag, zoals bij het niet vergrendelen van het beeldscherm bij het verlaten van de werkplek	Training					
	Leren						
19	Medewerkers laten leren van cyberaanvallen- en incidenten	Training					
20	Medewerkers vragen naar hun mening over het cybersecuritybeleid	Communicatie					
21	De procedures over hoe om te gaan met een cyberaanval- of incident testen, bijvoorbeeld in de vorm van een oefening of test	Training & pentesten					
22	Geleerde lessen, bijvoorbeeld na een incident of cybercrisisoefening, toepassen in het cybersecuritybeleid	Beleid					
23	Geleerde lessen communiceren binnen de organisatie	Communicatie					

24	Medewerkers de middelen bieden om te leren van cyberaanvallen- en incidenten die zich in het bedrijf hebben voorgedaan	Communicatie & training					
25	Binnen het bedrijf feedback faciliteren op het gebied van cyberveilig gedrag	Communicatie					
26	Met medewerkers in gesprek gaan om de bereidheid om deel te nemen aan oefeningen waar de cyberbeveiliging wordt getest te vergroten	Communicatie					
27	Binnen het bedrijf momenten (bv brainstorm sessies) inplannen om na te denken over wat goed gaat en wat beter kan met betrekking tot hun cyberveiligheid.	Communicatie					

Onderdeel 6: Uw ervaring van dit project

Als laatste wil ik u graag een aantal vragen stellen over hoe u dit project ervaren heeft. Voelt u zich vooral vrij om eerlijke en constructieve feedback te geven, want dit is zeer behulpzaam voor het verbeteren van onze interventie.

15. In hoeverre bent u het eens met de volgende stelling?

	Stellingen	Helemaal onwaar	Enigszins onwaar	Niet onwaar of waar	Enigszins waar	Helemaal waar
1	Wij hebben op basis van het adviesrapport verbeteringen doorgevoerd in de cybersecurity van onze onderneming.					

2	Wij gaan in onze onderneming op korte termijn (verdere) verbeteringen doorvoeren in onze cybersecurity op basis van het adviesrapport					
3	Ik heb het gevoel dat de cyberweerbaarheid van het bedrijf is toegenomen als gevolg van dit project					
4	Ik voel me als gevolg van dit project meer bekwaam om de verantwoordelijkheid over de cybersecurity te dragen dan voorheen					
5	Ik voel me instaat om na afloop van dit project het bedrijf verder te ontwikkelen met betrekking tot cybersecurity					
6	Ik heb het gevoel dat, naarmate cybercrime ontwikkeld, mijn bedrijf nu in staat zal zijn om hierin mee te ontwikkelen met betrekking tot cybersecurity					

16. Indien de 2e stelling met helemaal onwaar of enigszins onwaar is beantwoord:
Welk van de volgende redenen bepaalt dat u op korte termijn geen verdere verbeteringen gaat doorvoeren in uw cybersecurity op basis van het adviesrapport?

	Redenen	Ja	Nee
1	Omdat we niet weten hoe		
2	Omdat we het niet belangrijk vinden		
3	Omdat er nu voldoende gedaan is		
4	Omdat onze cybersecurity nu goed genoeg is		

5	Anders, namelijk…		

17. Op een schaal van 1 tot 5, hoe tevreden bent u over de volgende aspecten van dit project?

	Aspecten	**Zeer ontevreden**	**Ontevreden**	**Neutraal**	**Tevreden**	**Zeer tevreden**
1	De eerste cyberscan					
2	Het adviesrapport dat u ontvangen heeft naar aanleiding van de scan					
3	De 2 dagen dat uw buddy aanwezig was om de adviezen te helpen invoeren					
4	Het contact met uw buddy					
5	Het project over het algemeen					

18. Kunt u deze mate van tevredenheid kort toelichten? [open vraag]

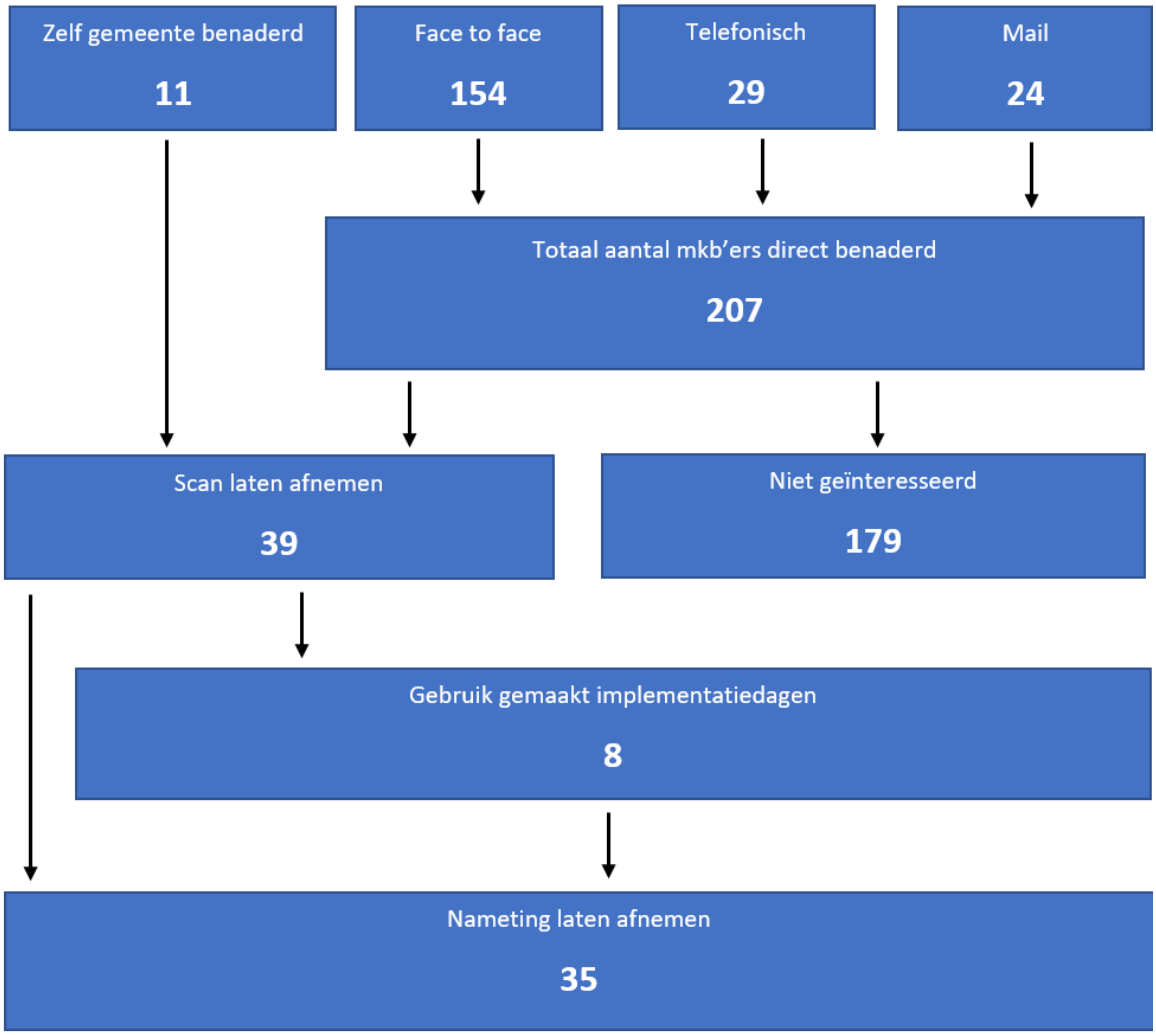
19. Denkt u dat het een goed idee is om dit project in alle Nederlandse gemeenten aan mkb'ers aan te bieden en welke aanpassingen zou u daarbij eventueel adviseren?

20. Heeft u nog opmerkingen, suggesties of andere toevoegingen over het project? [open vraag]

21. Zou u eventueel bereid zijn om voor de verdere verbetering van dit project deel te nemen aan een kort interview met onze veldwerk coördinator over uw ervaringen?
    a. Ja
    b. Nee

Bijlage 4: Schematische weergave van het wervingsproces

Wervingsronde 1



Wervingsronde 2