Van kwetsbaarheid naar weerbaarheid

Cyberweerbaarheid verhogen middels een geautomatiseerde evidence-based gedragsinterventie

2026

Isabelle Klaver
Susanne van ’t Hoff – de Goede
Rutger Leukfeldt
Kimberly Bluhm
Jurjen Jansen

Inhoudsopgave

Voorwoord

De lectoraten ‘Cybercrime en Cybersecurity’ van de Haagse Hogeschool en ‘Digitale Weerbaarheid van Mens en Organisatie’ van NHL Stenden Hogeschool zetten zich al geruime tijd in voor de digitale weerbaarheid van ondernemers, en sinds 2023 doen zij dat onder de vlag van het expertisenetwerk CyberweerbaarNL. Dit vakgebied kent grote uitdagingen, omdat de noodzaak van digitale weerbaarheid groot is maar het bereiken van ondernemers en het daadwerkelijk verhogen van digitale weerbaarheid uitdagend is gebleken.

In 2024 ontwikkelde het lectoraat ‘Cybercrime en Cybersecurity’ van de Haagse Hogeschool een interventie die geautomatiseerd op grote schaal kan worden toegepast en daarmee een unieke kans leek te bieden, ten opzichte van het huidige aanbod aan interventies. Tijdens het pilotonderzoek bleek deze interventie grote potentie te hebben. In het huidige onderzoek is deze interventie doorontwikkeld, op grote schaal ingezet en geëvalueerd.

We danken de subsidieverstrekkers Centrum voor Criminaliteitsbeheersing en Veiligheid (CCV), in het bijzonder Martijn Krijnsen, en het Ministerie van Justitie en Veiligheid voor deze mogelijkheid binnen de City Deal Lokale Weerbaarheid Cybercrime. Ook danken we ThreadStone, Platform Veilig Ondernemen (PVO) Noord-Nederland en de deelnemende brancheorganisaties en gemeenten voor hun betrokkenheid en inzet.

Isabelle Klaver
Susanne van ’t Hoff-de Goede
Rutger Leukfeldt
Kimberly Bluhm
Jurjen Jansen

Samenvatting

Achtergrond

Uit onderzoek blijkt dat het midden- en kleinbedrijf (mkb) vaak slachtoffer wordt van digitale criminaliteit, maar dat ondernemers niet altijd de benodigde cybersecuritymaatregelen nemen omdat zij bijvoorbeeld beschikken over beperkte tijd, kennis en ondersteuning. Externe dreigingen zoals malware, phishing, DDoS- en ransomwareaanvallen, maar ook interne risico's zoals zwakke wachtwoorden, onveilige configuraties en beperkte training, vergroten de kwetsbaarheid van een bedrijf. Het is daarom van groot belang dat de cyberweerbaarheid van bedrijven wordt vergroot. Cyberweerbaarheid verwijst naar het vermogen van organisaties om cyberrisico's te beheersen, aanvallen te weerstaan en snel te herstellen.

Instanties die interventies ontwikkelen of toepassen op het verhogen van deze weerbaarheid, stuiten echter op aanzienlijke uitdagingen. Ten eerste blijkt het bereiken, betrekken en actief laten deelnemen van ondernemers lastig. Hierdoor is het huidige bereik van interventies over het algemeen laag. Dit onderstreept de noodzaak voor interventies die op grote schaal kunnen worden uitgerold. Ten tweede wordt veelal gebruik gemaakt van cyberscans om digitale risico's voor ondernemers inzichtelijk te maken, maar tot op heden is nog weinig bekend over hun daadwerkelijke effectiviteit en de mate waarin ze ondernemers aanzetten tot actie om hun cyberweerbaarheid te versterken. De literatuur benadrukt daarom het belang van wetenschappelijk onderbouwde interventies met een groot bereik, duidelijke risicocommunicatie en praktische, toepasbare handvatten om veilig digitaal ondernemen binnen het mkb te bevorderen.

Onderzoeksdoel en onderzoeksvragen

Het doel van dit onderzoek is om de cyberweerbaarheid van mkb-ondernemingen te vergroten met behulp van een wetenschappelijk onderbouwde gedragsinterventie. Daarbij is gebruikgemaakt van een geautomatiseerde cybersecuritymeting die werkt op basis van open-sourcedata over digitale kwetsbaarheden. Ondernemers ontvingen vervolgens een op maat samengesteld adviesrapport met concrete stappen om hun cyberweerbaarheid te verbeteren.

Dit onderzoek sluit aan op het pilotproject *"What(s)can we do? Onderzoek naar het gebruik van een geautomatiseerde kwetsbaarhedenmeting als evidence-based gedragsinterventie"* (Van 't Hoff-de Goede et al., 2024). In die pilot is verkend in hoeverre een dergelijke meting technisch uitvoerbaar, juridisch toegestaan en effectief kan worden ingezet om de cyberweerbaarheid van ondernemers te versterken. De resultaten uit de pilot toonden aan dat er geen juridische beperkingen waren voor het meten van kwetsbaarheden aan de 'buitenkant' van de onderneming, en dat de eerste aanwijzingen duidden op een potentieel effectieve interventie. In het huidige onderzoek is deze interventie verder ontwikkeld en uitgebreid geëvalueerd.

Het project bestond uit drie fasen: fase 1 testte op kleine schaal hoe de interventie wordt ontvangen door ondernemers, in fase 2 is de interventie doorontwikkeld op basis van de inzichten uit fase 1 en in fase 3 is de interventie op grote schaal uitgevoerd om de effectiviteit te evalueren. De hoofdvragen per fase zijn:

Fase 1: *Op welke wijze kan de geautomatiseerde evidence-based gedragsinterventie voor het stimuleren van ondernemers om drie basismaatregelen voor cybersecurity te implementeren worden geoptimaliseerd*?

Fase 2: *Hoe kan de interventie, op basis van de inzichten uit de pilot en fase 1, worden doorontwikkeld?*

Fase 3: *Wat is het effect van de interventie op de cyberweerbaarheid van ondernemers?*

Methoden

In fase 1 werd de interventie getest bij 150 bedrijven, waarvan 75 ondernemers een vooraankondigingsbrief ontvingen met een mogelijkheid tot opt-out. Vervolgens gingen onderzoekers langs bij alle gemeten bedrijven met een checklist. Uiteindelijk is met 30 ondernemers een checklist ingevuld om te onderzoeken hoe de interventie werd ontvangen en welke factoren ondernemers beïnvloedden bij het openen, lezen en opvolgen van het adviesrapport. Daarnaast zijn zeven verdiepende interviews gehouden. Het hoge aantal ondernemers dat niet bereikt is in deze fase kwam door afwezigheid of beperkte beschikbaarheid van de ondernemers om de onderzoekers te woord te staan, in lijn met eerder onderzoek.

In fase 2 zijn op basis van de inzichten uit de checklists en interviews (fase 1), aanbevelingen uit het pilotonderzoek (Van 't Hoff-de Goede et al., 2024) en aanbevelingen gedaan door professionals, waaronder het toevoegen van een vooraankondiging met een opt-outmogelijkheid, de interventie verder doorontwikkeld.

In fase 3 is de interventie op grotere schaal uitgevoerd en geëvalueerd. Voor de interventie is een geautomatiseerde kwetsbaarhedenmeting uitgevoerd op basis van openbaar toegankelijke gegevens, waarbij drie gemeenten en twee brancheorganisaties de benodigde NAW-gegevens van mkb-ondernemers aanleverden. Deze ondernemers ontvingen een op maat gemaakt adviesrapport met de gevonden kwetsbaarheden, praktische aanbevelingen en een vorm van risicocommunicatie (testgroep): een coping-message of geanticipeerde spijt, of geen risicocommunicatie (controlegroep). De uiteindelijke onderzoekspopulatie bestond uit 2.646 ondernemingen, waarvan 2.056 in de testgroep en 590 in de controlegroep. Er zijn acht kwetsbaarhedenitems gemeten, zoals "*kan uw e-mail niet misbruikt worden*" en "*worden bezoekers van uw website voldoende beschermd*". Per item geldt dat een score van 0 aangeeft dat geen kwetsbaarheid is aangetroffen en een score hoger dan 0 duidt op de aanwezigheid van een kwetsbaarheid. Scores van -99 (missing values) zijn uitgesloten van de analyse. De scores op de acht items zijn per ondernemer opgeteld, wat resulteert in een totale risicopuntenscore. De meting werd tweemaal uitgevoerd: een voormeting op basis waarvan de rapportage van de ondernemer werd opgesteld en een nameting twee maanden later.

Resultaten

Uit fase 1 bleek dat de interventie over het algemeen positief werd ontvangen door ondernemers, maar er werden ook verbeterpunten genoemd. De brief en rapportage werden soms als te technisch ervaren en er was behoefte aan concretere voorbeelden van handelingsopties voor ondernemers wanneer een kwetsbaarheid werd gevonden. Daarnaast associeerden sommige ondernemers de interventie met een scam of met commerciële intenties. Ondernemers gaven aan dat de interventie

hun kennis en bewustzijn over cyberweerbaarheid had vergroot, met name ondernemers voor wie het onderwerp eerder nog geen hoge prioriteit had.

In fase 2 zijn de verbeteringen en doorontwikkelingen geïmplementeerd. De communicatie werd duidelijker en toegankelijker gemaakt (o.a. aangepaste logo's, opt-outmogelijkheid, eenvoudiger taalgebruik en verduidelijking dat het geen commercieel project is) en het handelingsperspectief werd aangescherpt met praktische vervolgstappen. Ook zijn de vormen van risicocommunicatie aangepast, van sociale norm naar een coping-message en geanticipeerde spijt, en is het onderzoeksproject verbeterd met een checklist.

In fase 3 is de effectiviteit van de interventie onderzocht. De resultaten wijzen op een effectieve interventie met een klein, maar significant effect dat bijdraagt aan de cyberweerbaarheid van ondernemers. De resultaten laten zien dat de risicopuntenscore in de testgroep in twee maanden significant daalde. Deze afname was significant groter dan de afname bij de controlegroep in dezelfde periode. Vooral de risicopunten die ondernemers zelf eenvoudig kunnen aanpakken, lieten duidelijke verbeteringen zien, het zogenaamde "laaghangende fruit" zoals de items misbruik van e-mail en onderschepping websiteverkeer. Complexere, technische risico's veranderden daarentegen nauwelijks. Het effect van de interventie verschilde per overkoepelende organisatie. Bij twee van de drie gemeenten en een van de twee brancheorganisatie was de afname in de risicopuntenscore significant groter dan de controlegroep, in de andere twee organisaties was de afname in risicopuntenscore vergelijkbaar met de controlegroep. De verschillende vormen van risicocommunicatie hadden vergelijkbare effecten, waardoor de effectiviteit van de interventie niet samen leek te hangen met de vorm van risicocommunicatie die werd toegepast. Samengevat verhoogt de interventie de cyberweerbaarheid van ondernemers met een klein, maar significant effect, waarbij het effect varieert tussen items en organisaties.

Beperkingen en vervolgstappen

Het onderzoekt kent een aantal beperkingen. Ten eerste was de respons in fase 1 relatief laag, wat de representativiteit kan beïnvloeden. Wel werden in fase 1 interessante inzichten opgedaan om de interventie te verbeteren. Ten tweede geeft de interventie slechts een gedeeltelijk beeld van de cyberweerbaarheid van ondernemers, omdat alleen openbare informatie is gebruikt. De interventie wijst ondernemers op stappen om dit deel van de cyberweerbaarheid van de onderneming te verhogen, voorzien van een concreet handelingsperspectief. Desalniettemin dragen ook kleine stappen bij aan het vergroten van de cyberweerbaarheid van het mkb. Hiernaast wijst de interventie ook op mogelijke aanvullende stappen voor het vergroten van de cyberweerbaarheid van de onderneming, door te verwijzen naar de vijf basisprincipes van het DTC en de bijhorende website (met een QR code in de rapportage). Ten derde was de grootste beperking van het onderzoek dat een groot deel van de respondenten uitgesloten moest worden van de data-analyse door een probleem in de voormeting. Hoewel we met ruim 2.600 geteste bedrijven een betrouwbaar beeld hebben opgehaald, hadden we zonder die uitsluiting meer representatieve uitspraken kunnen doen in termen van effectiviteit.

Voor de toekomst wordt aanbevolen IT-beheerders meer te betrekken, de interventie landelijk te waarborgen en deze als opstap te gebruiken voor verdere initiatieven, die bijvoorbeeld meer de diepte ingaan en/of de 'binnenkant' van de onderneming kunnen analyseren.

1. Inleiding

1.1 Achtergrond en doel onderzoek

Dit onderzoek gaat over de cyberweerbaarheid van ondernemers in het midden- en kleinbedrijf (mkb). Terwijl traditionele criminaliteit afneemt, neemt cybercriminaliteit juist toe. Vooral het mkb is kwetsbaar: jaarlijks wordt 20% van de bedrijven slachtoffer van online criminaliteit. Dit gaat vaak gepaard met grote financiële schade (CBS, 2025). Toch blijven cybersecuritymaatregelen achter, waardoor veel ondernemers onnodig risico lopen (CBS, 2024; Van 't Hoff-de Goede & Leukfeldt, 2024). Factoren zoals risicoperceptie, kennisgebrek en dagelijkse prioriteiten beïnvloeden in hoeverre ondernemers cybermaatregelen treffen (Hoffmann et al., 2024). Vooral kleinere bedrijven nemen bewust geen maatregelen of vertrouwen op standaardoplossingen zonder voldoende kennis of ondersteuning (CBS, 2024; Hoffmann et al., 2024; Hoekstra et al., 2021). Het is dan ook noodzakelijk om te werken aan cybersecurity van bedrijven om hun cyberweerbaarheid te vergroten.

Cybersecurity is een breed thema dat verschillende aspecten omvat, zoals het up-to-date houden van software, het herkennen van phishing e-mails en het veilig opslaan van belangrijke informatie. Dit verklaart waarom in verschillende interventies wordt ingezet op een brede aanpak, bijvoorbeeld door het algemene kennisniveau over cybersecurity te verhogen of door een meting aan te bieden die een lange lijst met verbeterpunten genereert op technisch, organisatorisch en menselijk vlak (Van 't Hoff-de Goede & Leukfeldt, 2024; CBS, 2024). Onderzoek toont echter aan dat interventies effectiever zijn wanneer ze zich richten op een specifieke doelgroep of op een concrete handeling (Ter Huurne & Gutteling, 2008). Bovendien ontbreekt bij veel initiatieven een evidence-based aanpak, waardoor onduidelijk blijft welke elementen daadwerkelijk werken en waarom (Bluhm et al., 2024). Hoewel het effect van cyberscans op gedragsverandering nog beperkt onderzocht is, laat kwalitatief onderzoek naar de Basisscan Cyberweerbaarheid (Hoekstra et al., 2021) zien dat het effect van deze scan in de praktijk gering kan zijn. De scan blijkt vooral geschikt voor weerbare bedrijven die hun bestaande strategie willen aanscherpen. Voor kleinere ondernemers biedt de scan minder houvast, doordat praktische ondersteuning ontbreekt (Hoekstra et al., 2021). Dit onderstreept de noodzaak van gerichte, wetenschappelijk onderbouwde interventies die ondernemers niet alleen informeren, maar ook daadwerkelijk aanzetten tot actie.

De interventie in dit onderzoek ondersteunt ondernemers bij het nemen van maatregelen om hun cyberweerbaarheid te versterken. Door hen proactief inzicht te geven in hun huidige cyberweerbaarheid op verschillende aspecten en concrete verbeteropties aan te reiken, worden zij gestimuleerd om actie te ondernemen. Dit onderzoek bouwt voort op het pilotproject '*What(s)can we do? Onderzoek naar het gebruik van een geautomatiseerde kwetsbaarhedenmeting als evidence-based gedragsinterventie*' (Van 't Hoff-de Goede et al., 2024). In dit pilotproject stond de vraag centraal: "In hoeverre is het mogelijk, toegestaan en effectief om een geautomatiseerde kwetsbaarhedenmeting uit te voeren ter bevordering van de cyberweerbaarheid van Nederlandse ondernemingen?".

Uit het pilotproject bleek dat er geen juridische bezwaren zijn voor de uitvoering van de interventie, waarbij de cyberweerbaarheid van bedrijven aan de 'buitenkant' wordt gemeten. Stakeholders zien bij de uitvoering van de interventie veel kansen voor de eigen organisaties. Zij benoemden dat de interventie als aanvulling op eigen evenementen en initiatieven kan worden gebruikt en dat de interventie op een laagdrempelige en efficiënte manier deelnemende ondernemers inzicht kan bieden om gericht hun cyberweerbaarheid te verbeteren. Hiernaast is de interventie schaalbaar, omdat deze makkelijk uit te voeren en betaalbaar is. De interventie lijkt tevens effectief te zijn vanwege de stijging in gemiddelde totaalscores binnen de testgroep vergeleken bij de controlegroep. De eerste resultaten wezen dus op een succesvolle interventie.

In de geautomatiseerde meting, die onderdeel was van de pilot, werd gebruik gemaakt van open source data over kwetsbaarheden. Het is daardoor mogelijk om op een laagdrempelige manier een beeld te krijgen van de staat van de cybersecurity van een organisatie zonder dat daarvoor het hele bedrijf moet worden doorgelicht. Tegelijkertijd kwamen de onderzoekers tot de conclusie dat de interventie verdere doorontwikkeling vereist om beter aan te sluiten bij de behoeften van ondernemers en om de eerste gevonden effecten verder te onderzoeken.

Het huidige onderzoek richt zich op het versterken van de cyberweerbaarheid van het mkb door middel van de bovengenoemde geautomatiseerde kwetsbaarhedenmeting. Het cybersecuritybedrijf ThreadStone ontwikkelde deze meting en voerde deze uit, waarbij open source-data wordt gebruikt om kwetsbaarheden in de digitale infrastructuur van bedrijven te identificeren. Het doel van dit onderzoek is om de geautomatiseerde, evidence-based gedragsinterventie te verbeteren, zodat deze ondernemers effectief stimuleert om basismaatregelen voor cybersecurity te implementeren. Deze basismaatregelen worden toegelicht in paragraaf 2.2.

1.2 Onderzoeksvragen

De interventie is verdeeld in drie fases: 1) een kleinschalige test om de interventie te kunnen optimaliseren, 2) een doorontwikkeling op basis van deze inzichten, en 3) een grootschalige uitvoering met een test- en controlegroep. Elke fase heeft zijn eigen hoofdvraag met bijbehorende subvragen.

Voor fase 1 is de hoofdvraag*: Op welke wijze kan de geautomatiseerde evidence-based gedragsinterventie voor het stimuleren van ondernemers om drie basismaatregelen voor cybersecurity te implementeren worden geoptimaliseerd?* Om deze hoofdvraag te beantwoorden, zijn de volgende deelvragen opgesteld:

1. Hoe reageren ondernemers op de vooraankondiging van de kwetsbaarhedenmeting?
2. Welke beweegredenen hebben ondernemers die een vooraankondiging hebben gekregen om al dan niet mee te doen aan de kwetsbaarhedenmeting?
3. In hoeverre bereiken de vooraankondiging en/of de rapportage de medewerkers die verantwoordelijk zijn voor cybersecurity van de geïncludeerde ondernemingen?
4. Welke beweegredenen hebben ondernemers om de envelop wel/niet te openen?
    a. In hoeverre heeft het logo op de envelop hier invloed op?

5. Welke beweegredenen hebben ondernemers om de rapportage wel/niet te lezen?
    a. In hoeverre heeft de bijgevoegde brief hierop invloed gehad?
    b. In hoeverre hebben de logo's op de brief hier invloed op?
6. Welke beweegredenen hebben ondernemers om wel/niet over te gaan tot maatregelen?
    a. In hoeverre heeft de bijgevoegde brief hierop invloed gehad?
    b. In hoeverre heeft de bijgevoegde rapportage hierop invloed gehad?
    c. In hoeverre hebben de rapportage en brief de perceptie van ondernemers op digitale veiligheid binnen hun organisaties beïnvloed?
7. Hoe beoordelen ondernemers het initiatief van de kwetsbaarhedenmeting en de communicatieproducten?
    a. In hoeverre waarderen ondernemers het dat hun onderneming (aangekondigd/onaangekondigd) een kwetsbaarhedenmeting ondergaat?
    b. Hoe beoordelen ondernemers de kwaliteit van de begeleidende brief die zij hebben ontvangen bij de rapportage?
    c. Hoe beoordelen ondernemers de kwaliteit van de rapportage van de kwetsbaarhedenmeting en de bruikbaarheid van de praktische handvatten?

Voor fase 2 is de hoofdvraag als volgt geformuleerd: *Hoe kan de interventie, op basis van de inzichten uit de pilot en fase 1, worden doorontwikkeld?* De bijhorende deelvragen zijn:

1. Welke inhoudelijke en vormmatige aanpassingen zijn doorgevoerd in de interventie?
2. Op welke wijze is het onderzoeksontwerp aangepast voor de volgende fase?
3. Welke aanbevelingen zijn (nog) niet doorgevoerd, en wat zijn de achterliggende redenen hiervoor?

Voor fase 3, de laatste fase van dit onderzoek, is de hoofdvraag: *Wat is het effect van de interventie op de cyberweerbaarheid van ondernemers?* De bijhorende deelvragen zijn:

1. In hoeverre is er een significant verschil te zien op de gemeten items tussen de voor- en nameting?
2. In hoeverre verschilt de gemeten cyberweerbaarheid tussen ondernemers(organisaties) in de voor- en nameting?
3. In hoeverre is er een effect van de verschillende vormen van risicocommunicatie op de gemeten cyberweerbaarheid?

1.3 Leeswijzer

In deze leeswijzer wordt kort toegelicht wat de lezer van dit rapport in de verschillende hoofdstukken kan verwachten. Hoofdstuk 2 bevat het literatuuronderzoek, waarin wordt ingegaan op digitale weerbaarheid en cyberrisico's in het mkb, cyberaanvallen en kwetsbaarheden bij ondernemers, bestaande initiatieven en risicocommunicatie als interventiemiddel. In hoofdstuk 3 worden de gebruikte methoden beschreven, waarbij de methoden van fase 1 en fase 3 afzonderlijk worden toegelicht. Hoofdstuk 4 presenteert de resultaten van alle drie de fases. Tot slot bevat hoofdstuk 5 de

conclusie, waarin de belangrijkste bevindingen worden samengevat, de beperkingen van het onderzoek worden besproken en aanbevelingen voor vervolgonderzoek en praktijk worden gedaan.

2. Literatuuronderzoek

Dit hoofdstuk geeft een overzicht van relevante literatuur en brengt in kaart met welke cyberrisico's ondernemers te maken hebben. Daarnaast worden bestaande cyberscans besproken, waarbij de sterke en zwakke punten worden beschreven. Tot slot wordt de risicocommunicatie toegelicht die centraal staat in de interventie, waarbij coping-message uit de Protection Motivation Theory en geanticipeerde spijt aan bod komen.

2.1 Digitale weerbaarheid en cyberrisico's in het mkb

2.1.1 Definitie, risicoperceptie ondernemers en maatregelen

Digitale weerbaarheid, in dit rapport cyberweerbaarheid genoemd, omvat het vermogen om '(relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken' (NLSC, 2022, p.9). Hausken (2020) beschrijft cyberweerbaarheid als een belangrijke factor voor het waarborgen van de operationele continuïteit van organisaties. Ondanks het belang hiervan blijken veel organisaties kwetsbaar te zijn voor cyberaanvallen, vooral wanneer basismaatregelen ontbreken (CBS, 2024; Hoekstra et al., 2021).

Uit onderzoek blijkt dat sommige mkb-ondernemers cybercrime als een belangrijk risico zien. Volgens Hoffmann et al. (2024) beschouwde 32% van de ondernemers cybercrime als een belangrijk risico, waarvan 21% het zelfs als zeer belangrijk inschatte. Dit risico werd vaak als urgent ervaren, direct na de krapte op de arbeidsmarkt. De risicoperceptie varieert echter sterk tussen sectoren en bedrijfsgroottes: ondernemers in de dienstensector en grotere bedrijven (in dit onderzoek gedefinieerd als meer dan 100 medewerkers) schatten de impact van cyberincidenten hoger in dan kleinere bedrijven en bedrijven in de industriële sector (Hoffmann et al., 2024).

Hiernaast blijkt uit onderzoek dat veel ondernemers weinig cybersecuritymaatregelen nemen. Vooral kleinere bedrijven en zzp'ers nemen minder maatregelen en kiezen vaker voor eenvoudige, minder complexe oplossingen. Zij zijn daarnaast minder geneigd om advies in te winnen over cyberrisico's. Dit wordt veelal verklaard door een gebrek aan kennis, tijd en ondersteuning. Dagelijkse operationele prioriteiten krijgen meestal voorrang boven lange termijnmaatregelen voor cyberweerbaarheid (CBS, 2024; Hoffmann et al., 2024).

Onderzoek van het CBS (2024) laat zien dat het ICT-beveiligingsniveau van bedrijven stijgt naarmate meer maatregelen worden genomen. Grotere bedrijven treffen gemiddeld vaker én complexere maatregelen dan kleinere organisaties. Basismaatregelen, zoals antivirussoftware, zijn breed ingevoerd, maar geavanceerdere maatregelen, zoals VPN's[1] en tweefactorauthenticatie[2],

[1] VPN (Virtual Private Network): een beveiligde verbinding waarmee internetverkeer wordt versleuteld en het lijkt alsof je vanaf een andere locatie verbinding maakt. Dit helpt om gegevens beter te beschermen.
[2] Tweefactorauthenticatie (2FA): een extra beveiligingsstap naast een wachtwoord, bijvoorbeeld een code via sms of een app, om in te loggen.

komen vooral bij grotere bedrijven voor. Wel is het gebruik van tweefactorauthenticatie sinds 2016 in alle bedrijfsgroottes sterk toegenomen, met de grootste groei bij kleinere bedrijven.

2.1.2 Sectorale en gedragsmatige verschillen in cyberweerbaarheid

Naast verschillen tussen bedrijfsgroottes, zijn er ook duidelijke sectorale verschillen in hoe ondernemingen omgaan met cyberrisico's. Bedrijven in de ICT-sector en gezondheidszorg scoren hoger op het gebied van cybersecurity dan bijvoorbeeld de horeca. Dit hangt deels samen met de mate van digitalisering en de gemiddelde bedrijfsgrootte binnen een sector. Grote bedrijven (in dit onderzoek gedefinieerd als organisaties met 250 of meer werkzame personen) passen vaker meerdere beveiligingsmaatregelen tegelijk toe: bijna 60% van de grootste bedrijven gebruikt alle tien onderzochte maatregelen (CBS, 2024).

Uit recent onderzoek naar de segmentatie van bedrijfsdoelgroepen blijkt dat er verschillen bestaan in de mate van veilig digitaal ondernemen en de onderliggende gedragsbepalers die dit gedrag sturen (Hof et al., 2024). Deze verschillen worden onder meer veroorzaakt door variaties in kennis, vaardigheden, waargenomen kwetsbaarheid en motivatie om beschermende maatregelen te nemen. Zo onderscheiden, op basis van hun onderzoek onder N = X bedrijven, zich vijf groepen: Voorlopers, Uitbesteders, Overmoedigen, Machtelozen en Onverschilligen, waarbij de laatste drie groepen relatief zwak scoren op veilig digitaal ondernemen. Zij vormen samen ongeveer 66% van de onderzochte groep ondernemers die eindverantwoordelijk of (mede)beslisser zijn over veilig digitaal ondernemen en vertonen verschillende patronen van gedragsbepalers die de mate van veilig digitaal ondernemen beïnvloeden. Overmoedigen onderschatten bijvoorbeeld de ernst van cyberdreigingen en hechten minder waarde aan hun digitale reputatie, terwijl Machtelozen en Onverschilligen op een breed scala aan gedragsbepalers laag scoren, waaronder kennis, vaardigheden, intentie en waargenomen controle over de situatie (Hof et al., 2024).

De bevindingen uit de literatuur onderstrepen het belang van praktijkgerichte en effectieve strategieën om het bewustzijn van cyberrisico's in het mkb te vergroten. Het bieden van duidelijke richtlijnen en de juiste risicocommunicatie is van belang, vooral omdat ondernemers vaak worstelen met het vertalen van algemene adviezen naar concrete maatregelen (CBS, 2024; Hof et al., 2024; Hoffmann et al., 2024; Hoekstra et al., 2021).

2.2 Cyberaanvallen en kwetsbaarheden onder ondernemers

2.2.1 Externe cyberdreigingen

Cyberaanvallen vormen een grote dreiging voor bedrijven en kunnen zowel financiële schade als reputatieschade veroorzaken (Arroyabe et al., 2024; ENISA, 2020). Een aantal bekende voorbeelden van externe aanvallen wordt gegeven in onderzoek van Arroyabe et al (2024). Deze worden hieronder ter illustratie toegelicht. We beogen geen totaaloverzicht te geven van externe dreigingen.

Malware, zoals virussen, trojans, ransomware en spyware, worden gemaakt om systemen te verstoren, schade aan te richten of ongeautoriseerde toegang te verkrijgen tot gevoelige gegevens. Phishing-aanvallen proberen gevoelige informatie, zoals wachtwoorden of creditcardgegevens, te bemachtigen door een nepwebsite te presenteren als een betrouwbare bron. Daarnaast zijn Denial-

of-Service- (DoS) en Distributed Denial-of-Service (DDoS)-aanvallen gericht op het overbelasten van netwerken of systemen, waardoor deze onbruikbaar worden. Een andere aanval waar bedrijven het slachtoffer van kunnen worden, is de zogenoemde Man-in-the-Middle (MITM)-aanval, waarbij cybercriminelen communicatie onderscheppen tussen twee partijen. Dit kan worden gebruikt om informatie te stelen, partijen af te luisteren of te manipuleren, bijvoorbeeld door middel van afpersing.

SQL-injectie is een kwetsbaarheid in webapplicaties waarbij onvoldoende gecontroleerde gebruikersinvoer in SQL-opdrachten wordt verwerkt. Dit kan worden misbruikt om databases te manipuleren of gevoelige gegevens te achterhalen. Als laatste is cross-site scripting (XSS) een beveiligingsfout die optreedt wanneer invoer, zoals een cookie of URL, niet goed wordt verwerkt en in de uitvoer naar de gebruiker terechtkomt. Dit biedt aanvallers de mogelijkheid om kwaadaardige codes in te voegen, wat kan leiden tot het stelen van sessiecookies, het overnemen van gebruikerssessies of het uitvoeren van ongewenste acties (Arroyabe et al., 2024; ENISA, 2020).

2.2.2 Interne cyberrisico's

Daarnaast vormen kwetsbaarheden in de systemen zelf een groot risico voor ondernemers. Zwakke wachtwoorden, onjuiste toegangsrechten (*least privilege*), en onvolledige toegangsbeveiliging kunnen ervoor zorgen dat aanvallers ongeautoriseerde toegang krijgen tot gevoelige systemen. Het niet regelmatig bijwerken van software vergroot de kans dat systemen misbruikt worden via bekende kwetsbaarheden. Kwetsbaarheden kunnen ook ontstaan door interne dreigingen, zoals kwaadwillende medewerkers (*insider threat*) of door slecht beveiligde netwerken en onveilige configuratie-instellingen. De gevolgen van cyberaanvallen kunnen ernstig zijn, vooral wanneer er geen adequate maatregelen zijn genomen om de schade te beperken of het herstel te versnellen. Het gebrek aan incidentresponsplannen kan ervoor zorgen dat een aanval langer onopgemerkt blijft en dat de reactie te laat komt, wat de schade c.q. impact vergroot.

Het gebrek aan fysieke beveiliging kan ervoor zorgen dat onbevoegden toegang krijgen tot belangrijke systemen en infrastructuur. Daarnaast verhoogt het ontbreken van goede encryptie bij het opslaan en versturen van gegevens het risico dat deze door derden worden onderschept (Arroyabe et al., 2024; ENISA, 2020).

Recent onderzoek bevestigt bovengenoemde kwetsbaarheden in de praktijk. Het Cybersecuritybeeld Nederland 2024 (CSBN, 2024) laat zien dat ransomware-aanvallen, supply-chain-aanvallen en kwetsbaarheden in veelgebruikte software de grootste dreigingen voor ondernemers zijn. In 2023 werden meer dan 170 ransomware-aanvallen geregistreerd, waarbij een groot aantal van mkb-bedrijven afkomstig zijn. Veel van deze bedrijven hadden onvoldoende basisbeveiliging getroffen, waardoor zij een makkelijk doelwit werden van deze aanvallen. Daarnaast zijn supply-chain-aanvallen steeds vaker een risico, waarbij aanvallers zich richten op toeleveranciers of softwareleveranciers. Dit kan leiden tot verstoringen verderop in de keten. De gevolgen van dergelijke aanvallen kunnen de bedrijfscontinuïteit ernstig verstoren.

Concluderend zijn de gevolgen van cyberaanvallen ernstig voor bedrijven, vooral wanneer er geen preventieve of reactieve maatregelen zijn getroffen. Het versterken van de basisbeveiliging en

het implementeren van incidentresponsplannen zijn van belang om de risico's te beheersen en de bedrijfscontinuïteit te waarborgen.

2.3 Bestaande initiatieven om cyberweerbaarheid te vergroten

Het is belangrijk om een helder beeld te geven van de bestaande interventies en hoe deze kunnen helpen om cyberweerbaarheid van het mkb te vergroten. We beperken ons daarbij, gelet op de aard van het onderzoek, tot de 'cyberscans'. In deze paragraaf kijken we zowel naar hoe ondernemers de scans ervaren, als naar hoe deze scans in de praktijk werken en wat hun belangrijkste eigenschappen zijn.

Cyberscans kunnen in algemene zin worden onderverdeeld in handmatige en geautomatiseerde scans (Van 't Hoff-de Goede et al., 2024). Handmatige cyberscans, zoals de Basisscan Cyberweerbaarheid van het DTC, betreffen veelal vragenlijsten die door de ondernemer zelf ingevuld moeten worden. Deze scans zijn tijdrovend en kunnen onnauwkeurig zijn door zelf gerapporteerde gegevens. Wanneer een professional de scan uitvoert, kan vaak een gedetailleerder en objectiever beeld van de staat van cyberweerbaarheid worden verkregen, maar dit brengt (extra) kosten met zich mee. Geautomatiseerde cyberscans, zoals een (network) vulnerability scanner, bieden snel inzicht in bekende kwetsbaarheden en kunnen continu worden uitgevoerd. Daarnaast kan ook gebruik worden gemaakt van detectietools (zoals IDS, IPS en SIEM) die malafide acties of afwijkingen signaleren en vervolgens waarschuwen of ingrijpen (NCSC, 2015).[3]

Deze scans zijn efficiënter dan handmatige scans, maar de resultaten zijn afhankelijk van de database van kwetsbaarheden die de scanner gebruikt. Ook kunnen deze scans kostbaar zijn. Er bestaan ook gratis online automatische scans, zoals het scannen van de beveiliging van een internetdomein op internet.nl. Deze bieden basisanalyses, maar missen de diepgang en professionele adviezen die een betaalde scan vaker biedt.

Een voorbeeld van een bestaande cyberscan is de Basisscan Cyberweerbaarheid, dit is een praktisch hulpmiddel waarmee ondernemers hun cyberweerbaarheid kunnen verbeteren door de vijf principes van het Digital Trust Center (DTC) toe te passen (Digital Trust Center, 2024). Het *eerste* principe draait om het in kaart brengen van risico's, waarbij organisaties hun afhankelijkheden, belangen en te beschermen gegevens identificeren. Dit helpt bij het bepalen van de relevante dreigingen en bij het ontwikkelen van strategieën voor risicobeheer. Het *tweede* principe richt zich op het bevorderen van veilig gedrag binnen de organisatie, aangezien veel cyberincidenten veroorzaakt worden door menselijke fouten. Door een veilige cultuur en bewustwording te stimuleren, kunnen medewerkers beter omgaan met digitale risico's. Het *derde* principe benadrukt het belang van het beschermen van systemen, apparaten en applicaties door veilige instellingen en tijdige dreigingsdetectie, zodat kwetsbaarheden snel worden aangepakt. Het *vierde* principe betreft het

[3] Intrusion Detection Systems (IDS) signaleren ongeautoriseerde of verdachte activiteiten binnen een netwerk of systeem en geven beheerders een waarschuwing. Intrusion Prevention Systems (IPS) identificeren niet alleen verdachte activiteiten, maar blokkeren deze ook actief om schade te voorkomen. Security Information and Event Management (SIEM)-oplossingen, verzamelen en analyseren loggegevens uit diverse bronnen om afwijkingen en mogelijke incidenten te detecteren.

beheer van toegang tot systemen en data. Het is belangrijk dat toegangsrechten zorgvuldig worden gedefinieerd en aangepast bij veranderingen in het personeel om ongeautoriseerde toegang te voorkomen. Tot slot richt het *vijfde* principe zich op het voorbereiden op incidenten. Aangezien niet alle incidenten te voorkomen zijn, is het noodzakelijk om een plan te hebben voor snelle respons en herstel. Hiermee kan de schade na een cyberaanval snel beperkt worden. Door deze principes toe te passen, kunnen ondernemers hun cyberweerbaarheid versterken (Digital Trust Center, 2024; Hoekstra et al, 2021).

De Basisscan bestaat uit 25 stellingen, 5 stellingen per basisprincipe, die verschillende onderwerpen behandelen zoals het gebruik van wachtwoordmanagers en het maken van back-ups. Na het beoordelen van de stellingen ontvangt de ondernemer een rapport met praktische aanbevelingen om de cyberweerbaarheid te verbeteren (Rijksoverheid, 2019).

Onderzoek van Hoekstra et al. (2021) toonde aan dat de scan slechts in beperkte mate gedragsverandering bij ondernemers teweegbracht. In dit onderzoek werden 18 ondernemers tweemaal geïnterviewd: het eerste interview diende als nulmeting en het tweede interview vond plaats na het invullen van de basisscan.

Bedrijven met een hoge mate van cyberweerbaarheid gebruikten de scan voornamelijk om hun sterke en zwakke punten te bevestigen en verdere stappen te bepalen. Bedrijfscontinuïteit werd door deze groep als belangrijk beschouwd, waarbij schade zoveel mogelijk moest worden voorkomen. Voor kleinere bedrijven, die vaak minder tijd en middelen hadden, bood de scan weinig toegevoegde waarde en ontbrak de praktische ondersteuning om verbeteringen door te voeren. Zoals benoemd vertrouwden zij sterk op software en hardware zoals iOS en Apple, wat juist in tegenspraak was met de adviezen van het Digital Trust Center (DTC). Het dagelijkse werk had voor deze ondernemers prioriteit. Ondernemers in deze groep vertrouwden sterk op hun netwerk, zoals vrienden en media, voor informatie over cyberweerbaarheid. Deze groep betrof voornamelijk eenmanszaken of vennootschappen. Bij jonge, innovatieve bedrijven werd de scan echter in het merendeel van de gevallen gebruikt om specifieke zwakheden in kaart te brengen, waarbij zij vooral aandacht besteedden aan certificering en ketenverantwoordelijkheid. Hoewel zij de scan nuttig vonden, misten zij dynamiek en diepgang in de resultaten. Dit gebrek aan interactie en praktische begeleiding beperkte de effectiviteit van de scan als instrument voor gedragsverandering in het mkb (Hoekstra et al., 2021).

Over de effectiviteit van cyberscans is nog beperkt informatie beschikbaar (Van ’t Hoff–de Goede et al., 2024). De beschikbare literatuur is schaars en beperkt zich vaak tot specifieke typen scans (Hoekstra et al., 2021), waardoor het moeilijk is om algemene conclusies te trekken over hun impact.

2.4 Risicocommunicatie als interventiemiddel

In het pilotonderzoek waarop deze studie voortbouwt, is risicocommunicatie ingezet om ondernemers bewust te maken van de risico’s die zij lopen en hen aan te moedigen om cybersecuritymaatregelen te treffen (Van ’t Hoff-de Goede et al., 2024). Hierbij werden methoden van geanticipeerde spijt en sociale normen toegepast om de motivatie tot het nemen van

maatregelen te verhogen. Voor het huidige onderzoek is uitgebreid literatuuronderzoek uitgevoerd om de meest effectieve benaderingen van risicocommunicatie te identificeren. Twee belangrijke benaderingen die hierbij naar voren kwamen, zijn het gebruik van een coping-message en geanticipeerde spijt. Een coping-message is gericht op het bieden van concrete handvatten voor het nemen van actie. Geanticipeerde spijt benadrukt de verwachte spijt na een cyberincident, wat ondernemers kan motiveren om preventieve maatregelen te treffen (Misana-ter Huurne et al., 2021). De volgende twee paragrafen gaan dieper in op deze vormen van risicocommunicatie.

2.4.1 Protection Motivation Theory en risicocommunicatie

De Protection Motivation Theory (PMT), ontwikkeld door Rogers (1975), veronderstelt dat mensen zichzelf (in onderhavige context: hun onderneming) beschermen als zij hiertoe gemotiveerd zijn. De mate waarin mensen gemotiveerd zijn om preventieve maatregelen te nemen, wordt beïnvloed door verschillende factoren, zoals waargenomen kwetsbaarheid, de ernst van de dreiging, de overtuiging om zelf beschermende maatregelen uit te kunnen voeren, de overtuiging dat de aanbevolen beschermende maatregelen een effectieve uitkomst zullen hebben en de veronderstelde kosten van die maatregelen (Rogers, 1975). Deze factoren worden hierna uitgebreider toegelicht. De theorie is oorspronkelijk ontwikkeld voor de gezondheidszorg, maar is sindsdien uitgebreid naar andere domeinen, waaronder die van cyberweerbaarheid (o.a. Jansen, 2018; Spithoven et al., 2022; Bekkers et al., 2023; Van 't Hoff-De Goede et al., 2025).

Het model dat uit deze theorie voortkomt, beschrijft twee cognitieve processen die bepalen of iemand gemotiveerd raakt om zich te beschermen tegen een dreiging: threat appraisal en coping appraisal. Daarnaast worden in de literatuur over risicocommunicatie twee specifieke vormen van boodschappen onderscheiden die veelvuldig zijn onderzocht binnen het cybersecuritydomein: fear appeals en coping-messages.

Threat appraisal

Het proces van de threat appraisal richt zich op hoe iemand een dreiging beoordeelt. Dit omvat de waargenomen ernst en waarschijnlijkheid van de dreiging. Afhankelijk van deze beoordeling kan dit leiden tot aangepast gedrag (maatregelen om de dreiging te verminderen) of niet-aanpassend gedrag, zoals ontkenning. Uit het onderzoek van Jones et al. (2021) blijkt dat niet-experts vaak een lage waargenomen kwetsbaarheid inschatting van zichzelf maken, omdat zij zichzelf niet als aantrekkelijke doelwitten zien, bijvoorbeeld omdat ze zichzelf niet als "grote vissen" beschouwen die hackers zouden willen aanvallen. Zoals eerder benoemd in paragraaf 2.1.2 heeft het onderzoek van het DTC (2024) inzicht gegeven in de gedragsbepalers die een rol spelen bij het nemen van maatregelen ter versterking van de cyberweerbaarheid. In dat onderzoek worden onder andere de waargenomen controle en de ervaren ernst van cyberdreigingen genoemd als relevante factoren. De ernst van de dreiging valt binnen het proces van threat appraisal. Risicocommunicatie kan in dit verband gebruikmaken van fear appeals. Een fear appeal is een boodschap die vooral de dreiging benadrukt en inspeelt op gevoelens van angst en bezorgdheid. Het doel is mensen bewust te maken van de ernst van een risico, maar een risico is dat deze strategie ook kan leiden tot vermijdingsgedrag (Lewis et al., 2007).

Coping appraisal

Het proces van coping appraisal gaat over de mate waarin iemand beoordeelt of hij of zij in staat is om met de dreiging om te gaan. Dit omvat ook de inschatting of de voorgestelde maatregelen effectief en haalbaar zijn om het risico te verminderen. Dit kan leiden tot aanpassend gedrag, mits de kosten (zowel geld als tijd/moeite) van de actie niet te hoog zijn. Deze beoordeling beïnvloedt de mate waarin mensen bereid zijn voorzorgsmaatregelen te nemen en zich aan te passen aan de dreiging (Sutton, 2001; Dodge et al., 2023; Bekkers et al., 2023; Van Bavel et al., 2018). Jones et al. (2019) benadrukken dat niet-experts vaak een lage zelfeffectiviteit ervaren doordat zij weinig kennis hebben van cybersecurity of niet weten hoe zij zichzelf effectief kunnen beschermen. Tevens vinden zij de beschikbare tegenmaatregelen soms complex, onpraktisch of ineffectief. Dit leidt ertoe dat zij de benodigde acties als te kostbaar of omslachtig inschatten, waardoor zij deze niet implementeren. Ook binnen de coping appraisal sluit het onderzoek van het DTC (2024) aan. De waargenomen controle, zoals door het DTC benoemd, valt onder dit proces. Risicocommunicatie kan hier gebruikmaken van coping-messages. Een coping-message richt zich niet op angst, maar op handelingsperspectief: het geven van duidelijke en concrete instructies die laten zien hoe iemand zich kan beschermen tegen een dreiging. Dit versterkt de zelfeffectiviteit en sluit direct aan bij het coping appraisal-proces.

Coping-messages en fear appeals in cybersecurity

Coping-messages en fear appeals zijn uitgebreid getest in het cybersecuritydomein. Van Bavel et al. (2018) onderzochten het effect van twee benaderingen om gebruikers van een website te motiveren hun cybersecurity te verbeteren: een coping-message, die hen helpt om te begrijpen hoe ze zich kunnen beschermen, en een fear appeal, die hen wijst op de risico's en gevolgen van een cyberaanval. In het experiment moesten deelnemers zo veilig mogelijk een fictieve online aankoop doen. De belangrijkste bevinding is dat deelnemers die een coping-message ontvingen, alleen of gecombineerd met een fear appeal, veiliger gedrag vertoonden dan de controlegroep. Een coping-message was effectiever dan een fear appeal alleen. Het was vooral succesvol om deelnemers te laten weten welke stappen ze konden nemen om zich online te beschermen. Een gelijksoortige uitkomst wordt ook onderschreven door Jansen en Van Schaik (2019) die een fear appeal en coping message combineerden in hun experimentele onderzoek onder N = 786 gebruikers van internetbankieren. Zij observeerden dat een bericht met sterke argumenten over het algemeen het meest effectief is om de gedragsintentie te vergroten, zoals ook benadrukt in het onderzoek van Boss et al. (2015). Overigens toonden berichten met zwakke argumenten ook in zekere mate effectiviteit ten opzichte van de controlegroep.

In onderzoek van Zhang en Borden (2019) werd een experiment uitgevoerd met een 2 (aanwezigheid van gedragsaanbevelingen: wel vs. niet) × 2 (dreiging: hoog vs. laag) × 2 (soorten berichten) tussen-proefpersonen ontwerp, om te onderzoeken hoe de combinatie van verschillende vormen van risicocommunicatie invloed heeft op de negatieve emoties (zoals angst en bezorgdheid) en gedragsintenties in de context van een cybersecuritycrisis. Dit onderzoek laat zien dat een fear appeal zonder gedragsaanbevelingen kan leiden tot gevoelens van machteloosheid en verdriet. Deze emoties werden beschouwd als niet-aanpassend en konden resulteren in vermijdingsgedrag of

ontkenning van de dreiging. Wanneer daarentegen wel concrete gedragsaanbevelingen werden gegeven, bleken fear appeals effectiever te zijn dan zonder deze aanbevelingen. Binnen het coping appraisal-proces, dat betrekking heeft op het vertrouwen in het eigen vermogen om het aanbevolen gedrag uit te voeren (zelfeffectiviteit), blijkt dat duidelijke gedragsaanbevelingen de zelfeffectiviteit versterken via twee mechanismen. Duidelijke instructies zorgen er enerzijds voor dat men beter begrijpt wat er moet gebeuren, en versterken zo het vertrouwen om de aanbevolen acties uit te voeren. Anderzijds zetten specifieke aanbevelingen aan tot actieve cognitieve verwerking, waarbij mensen verder nadenken over hoe zij zichzelf kunnen beschermen. Dit verhoogt de overtuigingskracht van de boodschap.

Wanneer de ervaren zelfeffectiviteit hoog is, zijn mensen eerder geneigd om beschermende acties te ondernemen, zelfs wanneer zij negatieve emoties zoals angst ervaren (Zhang & Borden, 2019). Shillair (2018) bevestigt dat zelfeffectiviteit een bepalende factor is voor beschermend gedrag binnen het cybersecuritydomein. Mensen die een hoge zelfeffectiviteit ervaren, zijn eerder geneigd om adequaat te reageren op dreigingen en passende beveiligingsmaatregelen te nemen. Zelfs wanneer er sprake is van negatieve emoties zoals angst, zorgt een hoge zelfeffectiviteit ervoor dat mensen deze emoties niet als verlammend ervaren, maar juist gemotiveerd raken om actie te ondernemen.

Jones et al. (2021) benadrukken dat effectieve coping-messages aan niet-experts aan drie belangrijke voorwaarden moeten voldoen. Ten eerste moeten waarschuwingen duidelijke en concrete instructies bevatten over hoe gebruikers een dreiging kunnen vermijden, zoals het verwijderen van verdachte e-mails. Dit vergroot de waargenomen effectiviteit van de boodschap. Ten tweede is het van belang dat de waarschuwingen een helder contrast bieden tussen de kosten van een aanval en de tijdsinvestering die nodig is om de aanbevolen acties uit te voeren. Dit helpt gebruikers de kosten van de tegenmaatregelen beter in te schatten, al is deze aanbeveling nog niet empirisch bevestigd. Ten derde dienen gebruikers informatie te ontvangen over het succes van hun respons op de waarschuwing, wat de zelfeffectiviteit kan versterken. Een voorbeeld hiervan is om na afloop een bericht te sturen waarin staat dat hun actie de cyberdreiging succesvol heeft tegengehouden. Echter, het verstrekken van dergelijke feedback kan ook leiden tot verstoring van de workflow en frustratie, waardoor de optimale wijze van terugkoppeling nog nader onderzocht moet worden.

De toepassing van een coping-message in risicocommunicatie naar ondernemers lijkt dus door bovenstaande onderzoeken te zijn bevestigd als een relevante invalshoek. Hoewel een groot deel van dit onderzoek is uitgevoerd in de context van burgers en consumenten, ligt het voor de hand dat dezelfde mechanismen ook relevant zijn voor ondernemers. Veel ondernemers zijn immers geen cybersecurity-experts en ervaren vergelijkbare uitdagingen bij het inschatten van dreigingen en het uitvoeren van beschermende maatregelen. Door in de begeleidende brief aan ondernemers een duidelijke coping-message toe te voegen, waarin praktische stappen die zij kunnen nemen om hun cyberweerbaarheid te vergroten kort en duidelijk worden uitgelegd, verwachten we dat zij eerder geneigd zullen zijn actie te ondernemen.

Dit sluit aan bij de bevindingen dat een coping-message doorgaans een grotere invloed heeft op gedrag en intenties dan een fear appeal.

2.4.2 Geanticipeerde spijt

Geanticipeerde spijt, oftewel het anticiperen op de negatieve emotie van spijt bij het nalaten van gewenst gedrag, heeft een bewezen invloed op het besluitvormingsproces. Mensen proberen de kans op spijt te minimaliseren door gewenst gedrag alsnog te vertonen (Lazuras et al., 2017).

Het gebruik van geanticipeerde spijt in het domein van cybersecurity is echter relatief nieuw en er is dan ook beperkt literatuur beschikbaar over de toepassing hiervan. Een van de spaarzame onderzoeken hierover is de studie van Van 't Hoff–de Goede et al. (2024). In deze pilot werd dezelfde interventie getest die in dit onderzoek centraal staat. De resultaten van Van 't Hoff-de Goede et al. (2024) lieten zien dat bedrijven die een rapportage ontvingen waarin geanticipeerde spijt was verwerkt, een grotere toename vertoonden in hun totaalscore voor cyberweerbaarheid dan de controlegroep. Echter was het effect klein en er kon geen causaal verband worden aangetoond.

In andere domeinen is meer onderzoek gedaan naar geanticipeerde spijt, waaronder in relatie tot het gebruik van condooms (Richard et al., 1996), de beslissing om wel of niet te beginnen met roken als adolescent (Conner et al., 2006), en het bieden bij veilingen (Filiz-Ozbay & Ozbay, 2007). Een relevant voorbeeld is het onderzoek van Zeelenberg (1999), waarin werd aangetoond dat consumenten sneller geneigd waren een lot te kopen voor de Postcode Loterij wanneer zij zich voorstelden hoeveel spijt zij zouden ervaren als hun postcode zou winnen terwijl zij geen lot hadden gekocht. Dit effect werd toegeschreven aan het feit dat de uitkomst van de loterij altijd bekend was, waardoor spijt niet vermeden kon worden als er geen lot was gekocht.

Daarnaast is geanticipeerde spijt ook onderzocht in de context van verkeersveiligheid. Merkelback et al. (2023) toonden aan dat bestuurders zich vaker aan de snelheidslimieten hielden wanneer ze anticipeerden op de spijt van boetes of ongelukken als ze te hard zouden rijden. Geanticipeerde spijt wordt vaak ingezet als strategie om gedragsverandering te bevorderen, zoals ook blijkt uit het gebruik van deze techniek in de COVID-19-vaccinatiecampagnes. Door mensen zich de negatieve emoties voor te stellen die ze zouden ervaren als ze geen vaccinatie zouden nemen, kan de motivatie voor vaccinatie worden verhoogd (RIVM Corona Gedragsunit, 2021).

In de context van cyberweerbaarheid kan deze benadering gebruikt worden om ondernemers te motiveren tot het nemen van preventieve maatregelen door hen bewust te maken van de spijt die ze zouden ervaren als ze geen actie ondernemen.

Hoewel het effect van geanticipeerde spijt in het cybersecuritydomein volgens Van 't Hoff–de Goede et al. (2024) klein was en er geen direct causaal verband kon worden aangetoond, vormt dit geen reden om de inzet van deze strategie te vermijden. Immers, in andere domeinen, zoals gezondheid, verkeersveiligheid en consumentengedrag, is geanticipeerde spijt bewezen effectief in het stimuleren van gedragsverandering (zoals hierboven besproken). Daarom is het waardevol om deze benadering ook in het kader van cyberweerbaarheid verder te onderzoeken en toe te passen.

3. Onderzoeksmethoden

In dit hoofdstuk worden de methoden van dit onderzoek besproken, die uit twee delen bestaan. Het eerste deel behandelt de methoden die zijn gebruikt om de onderzoeksvraag te beantwoorden over hoe de kwetsbaarhedenmeting door de ondernemers wordt ontvangen. Het tweede deel richt zich op de kwetsbaarhedenmeting zelf, waarbij de gebruikte items, de operationalisatie en de dataset worden toegelicht. De interventie is in een eerdere studie van Van 't Hoff-de Goede et al. (2024) juridisch getoetst. Voor onderhavig onderzoek hebben we de gehele onderzoeksopzet succesvol laten toetsen door de Ethische Adviescommissie van NHL Stenden Hogeschool.

3.1 Methoden fase 1: ervaringen van ondernemers

Eerst wordt ingegaan op de methoden die zijn toegepast in fase 1 van het onderzoek. Deze fase richtte zich, zoals eerder genoemd, op de wijze waarop ondernemers de interventie hebben ervaren. Dit is onderzocht door middel van fieldtrips en interviews.

3.1.1 Dataselectie

In fase 1 staat het verdiepend testen van de geautomatiseerde evidence-based gedragsinterventie – bestaande uit een kwetsbaarhedenmeting en communicatieproducten – centraal. In deze fase zijn de ervaringen van ondernemers met de interventie onderzocht binnen een kleine steekproef. We hadden hiervoor een bedrijventerrein aanpak gehanteerd. Een branchegerichte aanpak is verkend, maar kwam uiteindelijk niet van de grond. Belemmeringen lagen onder andere in de terughoudendheid van de brancheverenigingen bij het benaderen van leden.

Als eerste stap stond het selecteren van een geschikt bedrijventerrein centraal, wat in overleg met PVO Noord-Nederland heeft plaatsgevonden. Op dit bedrijventerrein – gelokaliseerd in Noord-Nederland – waren bedrijven actief vanuit verschillende branches. We hebben ervoor gekozen om lokale netwerkpartners te informeren over onze plannen. Allereerst hebben we contact gezocht met de betreffende terreinmanager. Hij juichte het initiatief toe. Dit geldt ook voor de betreffende gemeentemedewerkers die we hierover informeerden (afdelingen Openbare Orde en Veiligheid en Economische Zaken), die belast zijn met het thema cyberweerbaarheid van organisaties in hun werkgebied. Ook private samenwerkingspartners zijn op de hoogte gesteld dat we activiteiten zouden ontplooien op het betreffende bedrijventerrein.

Via open source databronnen hebben we uiteindelijk 150 bedrijven op dat bedrijventerrein geselecteerd, en hebben we de benodigde gegevens van de bedrijven gezocht en gevonden. Op het bedrijventerrein waren meer dan 150 bedrijven actief. Om deze reden hebben we gekeken naar het type bedrijven dat actief is. We hebben ervoor gekozen om grote ketens uit te sluiten van deelname, omdat deze hun cybersecuritymaatregelen over het algemeen beter voor elkaar hebben en/of landelijk zijn belegd. We noteerden het webadres van de onderneming, dat nodig was voor het afnemen van de kwetsbaarhedenmeting, alsook de NAW-gegevens, om ze per post te kunnen bereiken. We legden deze vast in een beveiligd Excel-bestand.

Vervolgens kenden we de 150 bedrijven willekeurig toe aan twee groepen van 75. De ene groep kreeg een vooraankondigingsbrief met informatie over de achtergrond en het verloop van het onderzoek (zie bijlage I), alsook de kans om zich uit te schrijven (opt-out) en de andere groep kreeg geen brief.[4] We wilden testen in hoeverre deze variatie invloed heeft op de effectiviteit van de interventie. De brieven zijn op vrijdag 29 mei 2024 verstuurd. De ondernemers kregen een week de tijd om zich eventueel uit te schrijven. Vier ondernemers hebben daarvan gebruik gemaakt. Een voorbeeld van een reactie van een geselecteerde ondernemer was: “Wij willen niet meewerken aan het onderzoek; zijn een 2-manszaak.” Ook ontvingen we enkele mails waarin vragen werden gesteld over de authenticiteit van de brief en

het onderzoek. In een geval werd aangegeven dat men dacht dat het om een SPAM-actie ging. Via mail of telefoon is contact opgenomen om de betreffende ondernemers of medewerkers meer duidelijkheid te verschaffen.

Op basis van de afmeldingen kon het databestand met webadressen definitief worden gemaakt (*N* = 146) en op veilige wijze worden gedeeld met ThreadStone, het bedrijf dat de kwetsbaarhedenmeting heeft ontwikkeld en uitvoerde. Deze meting controleert de online beschikbare informatie van de onderneming op veiligheidsrisico’s. Met deze meting wordt vastgesteld of er kwetsbaarheden in de website en e-mailserver zitten. Voorbeelden van mogelijkheden zijn het uitvoeren van een check op kwetsbaarheden op domeinnaamniveau waardoor inzicht ontstaat in of er sprake is van versleuteling van het verkeer tussen website en bezoekers, of er poorten ‘open’ staan op de server van de website die mogelijk misbruikt kunnen worden en of communicatie via de browser niet gemanipuleerd kan worden. Medio juni waren de metingen voltooid en ontvingen we op veilige wijze de individuele rapportages. In deze op maat gemaakte rapportages zijn de resultaten van de kwetsbaarhedenmeting opgenomen en zijn, waar mogelijk en relevant, concrete handvatten aangereikt waar verbetering mogelijk is. Hiermee kunnen ondernemers de gevonden kwetsbaarheden oplossen, al dan niet samen met de IT-leverancier, en kunnen ze de cybersecurity van hun onderneming naar een hoger niveau tillen. Het handelingsperspectief is gericht op het verbeteren van drie basisprincipes van veilig digitaal ondernemen. De rapportages, met begeleidende brief (zie bijlage II), zijn per post verstuurd op vrijdag 28 juni.

3.1.2 Checklist

Op donderdag 11 juli (12.30 – 16.30 uur) en op dinsdag 16 juli (11.00 – 15.00 uur) 2024, zo’n twee weken na het versturen van de rapportages (zie par. 3.1), zijn onderzoekers met een checklist naar het bedrijventerrein gegaan met als doel om enkele ervaringen van ondernemers vast te leggen. De checklist bestond uit een aantal algemene vragen over hoe zij de interventie hebben ervaren (zie bijlage V). Het bedrijventerrein is door de onderzoekers opgedeeld in acht zones met in totaal 146 bedrijven, om zodoende de taken eenvoudig te verdelen onder de onderzoekers. In totaal hebben we

[4] De ondernemers die geen vooraankondigingsbrief kregen, zijn naderhand geïnformeerd over het (doel van het) onderzoek via de begeleidende brief die is meegestuurd met de rapportage van de kwetsbaarhedenmeting.

bij 140 bedrijven een poging gedaan om de checklist in te vullen. In 30 gevallen waren we succesvol (netto respons van 20,5%). Hieronder volgt een beschrijving van de bevindingen per dag.

Op 11 juli hebben we in totaal bij 86 bedrijven een poging gedaan om een checklist af te nemen. Bij 24 bedrijven hebben we een checklist kunnen afnemen[5], met twee konden we direct een interview afnemen en met tien mochten we contact opnemen om later een interview in te plannen (zie par. 3.1.3). Bij drie bedrijven werden we verzocht via de mail contact op te nemen, omdat ze de brief met de rapportage naar hun weten niet hadden ontvangen of nog niet hadden gelezen. Bij 31 bedrijven hadden we geen succes. Dit had verschillende redenen. De meeste ondernemers gaven aan daar geen tijd voor of behoefte aan te hebben. In een aantal van deze gevallen gaf men wel aan de rapportage te hebben doorgestuurd naar de directie of het management. Soms kwam het voor dat een bedrijf kenbaar dicht was (door vakantie of door een verbouwing) en in enkele gevallen was het betreffende bedrijf verhuisd naar een andere locatie. Ook was een reden om niet mee te werken dat de rapportage naar eigen zeggen niet is ontvangen of anderszins onbekend is. In de resterende 28 gevallen hebben we genoteerd om op 16 juli nog een poging te ondernemen. In die gevallen werden we wel te woord gestaan, maar was de juiste persoon om verschillende redenen niet aanwezig om onze vragen te beantwoorden. In sommige gevallen was het pand dicht/onbemand. Ook kwam het voor dat er geen bel aanwezig was, en zagen we ook geen beweging om anderszins de aandacht te trekken. Ook in die gevallen hebben we een notitie gemaakt om een nieuwe poging te ondernemen.

Op 16 juli hebben we een tweede ronde gemaakt. In totaal hebben we bij 68 bedrijven een poging gedaan om de checklist af te nemen. Dit betreffen 51 bedrijven die in ronde 1 niet zijn benaderd en 17 bedrijven waarbij we een tweede poging deden. Van de nieuw benaderde bedrijven konden we in 11 gevallen een checklist afnemen. In geen van deze gevallen stond men open om benaderd te worden voor een interview. Bij 39 bedrijven hadden we geen succes. De redenen hiervoor zijn overeenkomstig ronde 1. Van één bedrijf kregen we de contactgegevens van de juiste persoon om te benaderen. Van de 17 bedrijven waar we opnieuw langs gingen was de succesratio laag. Dit leverde één ingevulde checklist op en één uitnodiging om de juiste persoon een e-mail te sturen. Uiteindelijk is het er, vanwege tijdsbeperkingen, bij zes bedrijven niet van gekomen om de checklist in te vullen.

De ervaringen met de ondernemers was over het algemeen prettig. Gezegd moet worden dat voor sommige bedrijven het hoogseizoen is en daarom geen tijd was om de onderzoekers te woord te staan. Met personen die kritisch tegenover de interventie stonden kon goed worden geconverseerd en uiteindelijk gaven de meesten aan het belang ervan in te zien, ook al geldt dat dan meer voor 'de buurman' dan voor hunzelf. In beide ronden gaven verschillende ondernemers na het invullen van de checklist aan alles wel gezegd te hebben wat ze willen zeggen en voelden niet de behoefte om daar dieper op in te gaan tijdens een interview.

Tijdens beide ronden gaven meerdere mensen iets terug over de onbekendheid met de brief. Het vaakst kregen we terug dat meerdere personen verantwoordelijk zijn voor de front-office en het in ontvangst nemen van de post, en in roulatie wordt gewerkt, waardoor het wellicht bij andere personen binnen die bedrijven wel bekend was geweest.

[5] Eén ingevulde checklist telt voor twee individuele bedrijven die in hetzelfde (gedeelde) pand zitten. Eén en dezelfde persoon is verantwoordelijk voor IT-gerelateerde zaken.

Ook hoorden we dat dergelijke post direct bij de eigenaar wordt gebracht, waardoor de inhoud van onze vraag niet bekend voorkwam bij degene die we vroegen. In enkele gevallen werd de moeite gedaan om een rondje langs collega's te maken of rond te bellen om te kijken of anderen wel kennis hadden genomen van de brief en/of rapportage.

Tevens hoorden we terug dat wanneer een onderwerp niet aanspreekt, men het ook heel snel kan vergeten. In een geval waar een autogarage werd binnengelopen gaf een mevrouw aan dat de onderzoeker geluk had haar te treffen. "Als ik er niet was en je mijn man had getroffen, dan had hij vast gezegd dat hij geen brief heeft ontvangen." Alles wat 'niet relevant' is, wordt meteen aan de kant geschoven. Een eigenaar van een restaurant gaf op zijn beurt aan dat hij niet bekend is met de brief en rapportage, "maar misschien mijn vrouw wel". Hij gaf naar eigen zeggen aan 'op leeftijd' te zijn, en houdt zaken rondom de website zelf niet bij.

De op papier ingevulde checklists zijn verwerkt in SPSS versie 28. Ook zijn de analyses uitgevoerd middels dit programma.

3.1.3 Interviews

Naast de checklists zijn interviews met ondernemers afgenomen. Hiermee werd in kaart gebracht hoe de interventie bij ondernemers is ontvangen en welke beweegredenen zij hebben om de rapportage (i) wel of niet te openen en (ii) wel of niet te lezen, en (iii) of ze wel of niet overgaan tot het nemen van maatregelen. Hiervoor ontwikkelden we een interviewprotocol (zie bijlage VII). De deelnemers zijn geworven tijdens de fieldtrips. Twee ondernemers wilden ten tijde van de eerste fieldtrip direct meewerken aan een interview. Verspreid over beide fieldtrips kregen we van 13 ondernemers de toezegging om op een later moment een interview te plannen of kregen de onderzoekers de betreffende contactgegevens van een collega die ze mochten benaderen voor een interview. Met al deze ondernemers/medewerkers is via de mail of telefoon, afhankelijk van de contactgegevens die we kregen, contact gezocht. Uiteindelijk is met 7 ondernemers of andere medewerkers die verantwoordelijk zijn voor de cybersecurity een interview afgenomen. De eerste twee interviews zijn afgenomen op 11 juni. De overige interviews tussen 20 september en 22 oktober 2024. De lengte van de interviews lag tussen 7 en 32 minuten. Zes interviews hebben op locatie bij de ondernemer plaatsgevonden. Eén interview is via Microsoft Teams uitgevoerd.

Deelname aan de interviews was vrijwillig, anoniem en conform de geldende normen van (toegepast) wetenschappelijk onderzoek. Voorafgaand aan het interview hebben de respondenten informatie ontvangen over het doel van het onderzoek en hoe de informatie uit het interview zal worden verwerkt. Daarnaast is aan de respondenten toestemming gevraagd om het gesprek voor uitwerkingsdoeleinden op te nemen. Voordat het interview werd gestart, tekenden respondenten een *informed consentformulier* (bijlage VI). Hierin wordt uitleg gegeven over het onderzoek, de procedures en rechten aangaande deelname. De interviews zijn naderhand uitgewerkt in gespreksverslagen die, indien gewenst, ter controle aan de geïnterviewden zijn nagestuurd. Daarna zijn de opnames verwijderd. De gespreksverslagen zijn aan de hand van vooraf opgestelde thema's geanalyseerd, namelijk de thema's van de deelvragen. Per deelvraag is de relevante informatie uit het gespreksverslag gehaald. Indien noodzakelijk, zijn deze bevindingen gecombineerd met de bevindingen die uit de checklists zijn voortgekomen.

3.2 Methoden fase 3: effectevaluatie

De gebruikte methoden voor fase 3 zijn in deze paragrafen beschreven. Met deze methoden is onderzocht of de interventie effect heeft gehad op de cyberweerbaarheid van ondernemers.

3.2.1 De geautomatiseerde kwetsbaarhedenmeting

Om ondernemers inzicht te geven in hun cyberweerbaarheid, is in dit onderzoek een geautomatiseerde meting ingezet die potentiële kwetsbaarheden in hun digitale infrastructuur weergeeft. Deze meting maakt uitsluitend gebruik van openbaar beschikbare informatie en is eerder gebruikt in het onderzoek van Van 't Hoff–de Goede et al (2024). De geautomatiseerde kwetsbaarhedenmeting is ontwikkeld door ThreadStone, een cybersecurityorganisatie die zich richt op digitale risicobeheersing. Bij de implementatie van deze technologie is zorgvuldig rekening gehouden met juridische en ethische aspecten. Een uitgebreide juridische toetsing is gedaan door Van 't Hoff-de Goede et al. (2024). Hiermee is bevestigd dat de gehanteerde werkwijze past binnen geldende wet- en regelgeving.

De unieke insteek van de geautomatiseerde kwetsbaarhedenmeting is dat in plaats van dat bedrijven zelf het initiatief dienen te nemen voor een meting, zoals bij bestaande scans vaak het geval is, deze meting wordt uitgevoerd in opdracht van overkoepelende organisaties, zoals gemeenten of brancheverenigingen. Dit maakt het mogelijk om in één keer een bredere groep ondernemers te bereiken, wat kan bijdragen aan een collectieve versterking van de cyberweerbaarheid binnen een sector of regio.

Ondernemers ontvingen een op maat gemaakt rapport met een overzicht van de kwetsbaarheden die zijn aangetroffen en concrete aanbevelingen om hun cyberweerbaarheid te verbeteren. Door bedrijven op een toegankelijke manier inzicht te geven in hun digitale risico's en hen direct bruikbare handvatten te bieden voor verbetering, helpt deze aanpak om de cyberweerbaarheid van het Nederlandse bedrijfsleven te versterken.

Een belangrijk voordeel van deze aanpak is dat de metingen desgewenst periodiek herhaald kunnen worden om zo continu te monitoren hoe bedrijven ervoor staan op het gebied van cyberweerbaarheid. Dit biedt niet alleen inzicht in de effectiviteit van genomen maatregelen, maar maakt het ook mogelijk om ontwikkelingen over tijd te volgen. Zowel bedrijven zelf als beleidsmakers en onderzoekers kunnen hier waardevolle lessen uit trekken en zo werken aan structurele verbetering.

3.2.2 Operationalisatie

De gemeten kwetsbaarheden zijn geoperationaliseerd door ThreadStone. In Tabel 1 worden de metingen weergegeven die in de rapportage worden gebruikt, met bij elk een korte toelichting.

Tabel 1. *Operationalisatie kwetsbaarheden*

	Meting	**Voorbeeld resultaat**	**Toelichting**
1	Verspreidt uw website geen malware?	Uw website komt op blacklist(s) voor en lijkt kwalijke software (malware) te verspreiden.	Bezoekers van uw website ontvangen mogelijk kwalijke software (malware) op hun systemen. Deze kwalijke software kan bij deze bezoekers zorgen voor (veel) overlast, zoals inbraak of platleggen van hun systemen. Ook kan het voorkomen dat bezoekers uw website niet meer kunnen benaderen.
2	Verspreidt uw website geen spam?	Uw website komt op blacklist(s) voor en lijkt spam te verspreiden.	U kunt worden aangesproken op het verspreiden van spam waardoor uw website kan worden afgesloten. Daarnaast komen uw e-mails waarschijnlijk niet aan bij de geadresseerden.
3	Verspreidt uw mailserver geen spam?	Uw mailserver komt op blacklist(s) voor en lijkt spam te verspreiden.	U kunt worden aangesproken op het verspreiden van spam waardoor uw mailserver kan worden afgesloten. Daarnaast komen uw e-mails waarschijnlijk niet aan bij de geadresseerden.
4	Zijn gevoelige gegevens van uw medewerkers niet openbaar?	Gevoelige gegevens van medewerkers van uw organisatie, waaronder wellicht ook gebruikersnamen en wachtwoorden, zijn openbaar.	Kwaadwillenden kunnen mogelijk inbreken in (cloud-gebaseerde) systemen die uw organisatie gebruikt
5	Kan uw e-mail niet misbruikt worden?	E-mailprotocollen zijn niet juist ingesteld.	Onbevoegden kunnen eenvoudig namens (medewerkers van) uw organisatie e-mails versturen, of uw e-mails komen niet aan.
6	Kan het verkeer met uw website niet worden onderschept?	Communicatie met uw website is niet (juist) versleuteld, waardoor verkeer mogelijk kan worden onderschept.	Onbevoegden kunnen communicatie van bezoekers van uw website onderscheppen. Uw website kan lager in de zoekresultaten van Google presteren dan mogelijk is.
7	Zijn er geen ongebruikelijke aanvalspaden	Er staan ongebruikelijke digitale deuren open. Hier kunnen kwaadwillenden	Kwaadwillenden kunnen zwakke plekken in uw website vinden. Hierdoor

	op uw website mogelijk?	mogelijk een opening vinden die ze kunnen gebruiken om in te breken.	kunnen zij gegevens stelen, aanpassen of uw website verstoren.
8	Worden bezoekers van uw website voldoende beschermd?	Securityprotocollen worden niet juist afgedwongen op de browser van de bezoeker.	Onbevoegden kunnen communicatie met uw website (met mogelijk gevoelige gegevens van bezoekers) onderscheppen en mogelijk manipuleren.
9	Is informatie over de configuratie van uw website afgeschermd?	Uw website geeft informatie vrij over de instellingen. Hackers kunnen deze informatie gebruiken om uw website aan te vallen.	Doordat eenvoudig achterhaald kan worden welke software uw website gebruikt, is het makkelijker voor een kwaadwillende om te controleren of uw website kwetsbaar is. Hierdoor kunnen eenvoudiger openingen in uw website worden gevonden waardoor deze kan worden gehackt (stelen of manipuleren van data of verstoren van de werking).
10	Kan websiteverkeer naar uw website niet gemanipuleerd worden?	Het is mogelijk om websiteverkeer naar uw website te manipuleren, waardoor u niet kunt garanderen dat uw bezoekers úw website bezoeken maar zij dat wel denken (en dus worden doorgesluisd naar een kwalijke website).	Kwaadwillenden kunnen wachtwoorden of andere vertrouwelijke informatie onderscheppen van bezoekers van uw website
11	Is uw website, mailserver en nameserver gereed voor nieuwe standaarden?	Uw server is niet voorbereid voor de nieuwe internetstandaarden.	In de toekomst zal steeds meer en meer verkeer verlopen via de nieuwe IPv6 standaarden. Het is daarom verstandig om hier ook voorbereid op te zijn.

Zoals in bovenstaande tabel is te zien, zijn er 11 items waarop het domein van een ondernemer wordt gemeten. Tabel 2 toont het overzicht van de mogelijke scores aan. Het elfde item, "*Is uw website, mailserver en nameserver gereed voor nieuwe standaarden*?", wordt niet meegenomen in de uiteindelijke eindscore van het cyberweerbaarheidsniveau. Dit komt doordat deze nieuwe standaarden nog niet overal in gebruik zijn en het niet om een daadwerkelijk cyberrisico gaat.

De items zijn zodanig opgesteld dat een score van nul aangeeft dat er geen kwetsbaarheid is aangetroffen in de digitale infrastructuur. Een score hoger dan nul duidt erop dat er in zekere mate een kwetsbaarheid is vastgesteld. Wanneer een score van -99 wordt toegekend, betekent dit dat het niet mogelijk was om te bepalen of de kwetsbaarheid aanwezig is en is dit dus een missing-value.

Tabel 2. *Operationalisatie scoreverdeling*

Controlepunt	**Score**
Verspreidt uw website geen malware?	0: De website komt niet voor op malware verspreidende lijsten; 1: Het IP van de website komt voor op malware lijsten; 3: De website komt voor op malware lijsten; Invalid: De test kon niet worden uitgevoerd
Verspreidt uw website geen spam?	0: De website komt niet voor op spamlijsten; 1: De website komt voor op ≤ 2 spam lijsten; 2: De website komt voor op ≤ 5 spam lijsten; 3: De website komt voor op ≤ 200 spam lijsten
Verspreidt uw mailserver geen spam?	0: De mailserver komt niet voor op spamlijsten; 1: De mailserver komt voor op ≤ 2 spam lijsten; 2: De website komt voor op ≤ 5 spam lijsten; 3: De website komt voor op ≤ 200 spam lijsten; Invalid: De server heeft geen MX-record
Zijn gevoelige gegevens van uw medewerkers niet openbaar?	0: Er zijn geen e-mailadressen van medewerkers gevonden die voorkomen op lijsten met gehackte e-mailadressen; 0,25: Er zijn ≤ 2 gehackte e-mailadressen gevonden; 0,5: Er zijn ≤ 10 gehackte e-mailadressen gevonden; 0,75: Er zijn ≤ 200 gehackte e-mailadressen gevonden; 1: Er zijn > 200 gehackte e-mailadressen gevonden Invalid: De test kon niet worden uitgevoerd
Kan uw e-mail niet misbruikt worden?	0: SPF, DMARC en DKIM zijn allemaal goed ingesteld; 1: Één van de waarden is niet goed ingesteld; 2: Twee van de waarden zijn niet goed ingesteld Invalid: De test kon niet worden uitgevoerd
Kan het verkeer met uw website niet worden onderschept?	0: SSL correct ingericht, score A of A+; 1: SSL Score B; 2: SSL Score C; 3: SSL Score D of lager; Invalid: De test kon niet worden uitgevoerd
Zijn er geen ongebruikelijke aanvalspaden op uw website mogelijk?	0: Alleen de veilige poorten staan open ['80','443', '22', '2222', '993', '995', '465']; 0,25: Één extra poort buiten de veilige poorten is open; 0,5: Twee extra poorten buiten de veilige poorten zijn open; 0,75: Drie extra poorten buiten de veilige poorten zijn open; 1: Vier of meer extra poorten buiten de veilige poorten zijn open Invalid: De test kon niet worden uitgevoerd
Worden bezoekers van uw website voldoende beschermd?	0: Alle security headers zijn goed geïmplementeerd op de website voor zowel HTTP als HTTPS; 0,5: 1 ontbrekende header; 1: 2 ontbrekende headers; 1,5: 3 ontbrekende headers; 2: 4 of meer ontbrekende headers Invalid: Het was niet mogelijk om de headers van de website te lezen

Is informatie over de configuratie van uw website afgeschermd?	0: Er wordt geen informatie vrijgegeven over welke achterliggende software wordt gebruikt op de website (zowel op HTTP als op HTTPS); 0,5: 1 configuratieheader ontbreekt (bijvoorbeeld op HTTPS maar niet op HTTP); 1: 4 configuratieheaders ontbreken; Invalid: Het was niet mogelijk om de headers van de website te lezen
Kan websiteverkeer naar uw website niet gemanipuleerd worden?	0: DNSSec aanwezig; 2: Geen DNSSec aanwezig; Invalid: De test kon niet worden uitgevoerd
Is uw website, mailserver en nameserver gereed voor nieuwe standaarden?	Deze controle maakt geen deel uit van de score. Een negatief resultaat op deze controle heeft dus geen impact op de score.

3.2.3 Adviesrapportage en handelingsperspectief

De rapportage die ondernemers ontvangen, begint met een gepersonaliseerde brief waarin wordt uitgelegd door wie de rapportage is opgesteld en waarom de ondernemer deze ontvangt. Er wordt benadrukt dat het project geen commercieel karakter heeft, maar is bedoeld om ondernemers te ondersteunen bij het verbeteren van hun cyberweerbaarheid. In de brief wordt ook toegelicht hoe de rapportage kan bijdragen aan het versterken van de cyberweerbaarheid van de organisatie en wat de vervolgstappen zijn. Verder wordt uitgelegd dat de meting uitsluitend gebruik maakt van openbaar beschikbare bronnen (Bijlage II).

Hierna volgt in de adviesrapportage (zie Bijlage III) een overzichtelijke tabel waarin de belangrijkste bevindingen uit de meting worden gepresenteerd. Hierin worden aandachtspunten genoemd, samen met de mogelijke gevolgen. Zo wordt bijvoorbeeld het aandachtspunt *"Gevoelige gegevens van medewerkers van uw organisatie, waaronder wellicht ook gebruikersnamen en wachtwoorden, zijn openbaar"* genoemd, met als mogelijk gevolg: *"Kwaadwillenden kunnen mogelijk inbreken in (cloud-gebaseerde) systemen die uw organisatie gebruikt."*.

Vervolgens wordt een overzicht gegeven van alle controles die tijdens de meting zijn uitgevoerd. Bij elke controle wordt aangegeven of er sprake is van een goede score, een aandachtspunt, of dat een beoordeling niet mogelijk was. De rapportage verduidelijkt dat een goede score niet betekent dat alles volledig veilig is, omdat de meting een momentopname betreft en een globaal karakter heeft. Bij iedere controle wordt een toelichting gegeven, samen met een concreet advies. Een voorbeeld hiervan is de controle *"Kan website verkeer naar uw website niet gemanipuleerd worden?"*, met als toelichting: *"We hebben gecontroleerd of bezoekers die uw domeinnaam bezoeken, ook echt op uw website terechtkomen en niet worden omgeleid naar een nepwebsite. In uw geval blijkt de instelling hiervoor niet goed of afwezig te zijn; uw website blijkt geen DNSSEC (extra beveiliging voor domeinnamen) te ondersteunen."* Het bijbehorende advies luidt: *"Zorg ervoor dat DNSSEC wordt ingesteld op uw domein. Dit laat u doen door de hoster of beheerder van uw domein."*

De rapportage eindigt met een overkoepelend handelingsperspectief waarmee ondernemers gericht stappen kunnen zetten om hun cyberweerbaarheid te verbeteren (zie paragraaf 4.2.1.1 en Bijlage V).

3.2.4 Risicocommunicatie

In de huidige studie is een experimenteel design toegevoegd door gebruik te maken van verschillende vormen van risicocommunicatie. Alle ondernemers zijn gerandomiseerd toegewezen aan een van drie groepen. De eerste groep ontving de risicocommunicatie genaamd coping-message (zie paragraaf 2.4.1). De tweede groep ondernemers ontving een vorm van risicocommunicatie die zich richt op geanticipeerde spijt (zie paragraaf 2.4.2). De derde groep ondernemers ontvingen geen aanvullende risicocommunicatie. Zij ontvingen, net als de andere twee groepen, achtergrondinformatie over het risico van cybercriminaliteit en het belang van cyberweerbaarheid voor ondernemers. De risicocommunicatie is beschreven in paragraaf 4.2.1.1.

3.2.5 Dataverzameling en respons

Het uitgangspunt van dit onderzoek was om een hoog aantal ondernemers te bereiken. Voor het verzamelen van de nodige NAW-gegevens van ondernemers hebben wij ondersteuning gevraagd bij diverse brancheorganisaties en gemeenten. Deze samenwerking is op verschillende manieren tot stand gekomen, waaronder het geven van meerdere pitches tijdens relevante congressen om onze aanpak en doelen toe te lichten.

Als resultaat van deze pitches en relevante connecties hebben twee brancheverenigingen (Br1 en Br2) en drie gemeenten (Ge1, Ge2, en Ge3) aangegeven om deel te nemen aan het onderzoek. Tabel 3 toont het aantal respondenten per organisatie. De brancheverenigingen en gemeenten zijn in dit rapport geanonimiseerd.

De ondernemers vanuit de gemeenten zijn geselecteerd door de gemeenten zelf, door het opvragen van NAW gegevens en de URL van de onderneming uit de registers van de Kamer van Koophandel (KvK) voor alle ondernemers (Ge1 en Ge2) in de desbetreffende gemeente of een bedrijventerrein (Ge3). De gemeenten hebben vervolgens ondernemers verwijderd indien gegevens onvolledig waren, dubbel waren (meerdere ondernemingen met dezelfde URL), of aan de KvK hebben aangegeven geen post te willen ontvangen. Ge3 heeft hiernaast bedrijven met meer dan 250 medewerkers verwijderd, omdat grotere bedrijven doorgaans een interne IT-afdeling of externe IT-dienstverlener hebben en andere initiatieven van de gemeente zich op deze groep hebben gericht. Tot slot hebben de onderzoekers ondernemers verwijderd uit de datasets van de gemeenten, indien dezelfde ondernemers voorkwamen in de dataset van een van de brancheverenigingen die meededen aan het huidige onderzoek (in totaal 14 ondernemers). Bij Ge1 zijn ongeveer 300 adressen uit de initiële steekproef verwijderd, wat resulteerde in een uiteindelijke aanvankelijke steekproef van 1036. Bij Ge2 resulteerde dit in een reductie van ongeveer 200 bedrijven, waardoor er 964 bedrijven overbleven. Voor Ge3 resulteerde de selectie in een set van 2148 unieke adressen. Om een gelijke steekproefgrootte te hanteren, werd hieruit willekeurig een steekproef van 1000 adressen getrokken.

Voor Br1 bestond de initiële steekproef uit 4.373 leden. Binnen deze groep hadden 163 ondernemingen geen website, en bij 416 ondernemingen ging het om dubbele URL's (meerdere

ondernemers met dezelfde URL, bijvoorbeeld franchisenemers). Hierdoor bleef een steekproef van 3794 ondernemingen over. Voor Br2 is het totale aantal leden als initiële steekproef gehanteerd, wat neerkomt op 1880 ondernemingen. Van deze groep hadden 42 ondernemingen geen beschikbaar adres, en bij 320 ondernemingen betrof het dubbele adressen, franchisenemers of andere vormen van herhaling. Na deze opschoning bleef een steekproef van 1.518 ondernemingen over.

Tabel 3 biedt een volledig overzicht van het aantal verzonden vooraankondigingen en rapportages per organisatie, evenals de redenen voor afmeldingen van ondernemers en uitsluitingen door de onderzoekers. De tabel laat zien hoeveel ondernemers in eerste instantie zijn aangemeld door de betreffende organisaties en hoeveel daarvan uiteindelijk een rapportage hebben ontvangen. In totaal werden door vijf verschillende organisaties 8.307 rapportages aangeleverd, waarvan organisatie Br1 het grootste aandeel leverde met 3.794 rapportages (46%), gevolgd door Br2 met 1.518 rapportages (18%). De gemeenten, Ge1, Ge2 en Ge3, droegen elk ongeveer 12% bij aan het totaal, respectievelijk 1.036, 964 en 995 rapportages.

Gemeenten hadden, percentueel gezien, enigszins meer afmeldingen door ondernemers. Dit komt mogelijk doordat in de brieven van de gemeenten expliciet een opt-out werd vermeld.

De redenen voor afmeldingen varieerden, maar enkele motieven kwamen herhaaldelijk naar voren. Een veelvoorkomende reden was de onzekerheid onder ondernemers over de legitimiteit van het onderzoek. Sommige ondernemers gaven aan dat ze bang waren dat het initiatief mogelijk een vorm van phishing of een commerciële scan betrof, waardoor zij besloten niet deel te nemen. Daarnaast was er weerstand tegen het gehanteerde opt-out-principe; verschillende ondernemers gaven aan dat zij het onwenselijk vonden om zonder expliciete toestemming in het onderzoek te worden opgenomen. Tevens werd de termijn waarbinnen afmelding mogelijk was door enkele respondenten als te kort ervaren. Een andere reden die regelmatig werd genoemd, was dat ondernemers al eigen maatregelen hadden getroffen op het gebied van cyberweerbaarheid. Vanuit die optiek achtten zij deelname aan de kwetsbaarhedenmeting overbodig, omdat zij ervan overtuigd waren reeds voldoende inzicht te hebben in hun cyberrisico's.

Daarnaast werden 138 rapportages afgemeld omdat de post retour was gekomen. Het merendeel van deze retourzendingen was afkomstig van Br1, waarvan 84 rapportages (61%) retour werden ontvangen. De andere organisaties rapporteerden relatief minder retours, variërend tussen 6% en 13%.

In veertien gevallen bleek dat rapportages dubbel voorkwamen bij de brancheverenigingen, waarbij dit fenomeen vooral bij de organisaties Ge1, Ge2 en Ge3 optrad. Organisaties Br1 en Br2 kenden geen dubbele rapportages.

Naast afmeldingen en dubbelen zijn er technische beperkingen die de verzending hebben beïnvloed. In totaal zijn 474 domeinen als niet-bestaand geïdentificeerd, wat betekent dat de URL niet kon worden bereikt. Daarnaast waren er veertien gevallen waarin het opgegeven domein ongeldig bleek. Deze hebben er eveneens bijgedragen aan een daling van het aantal daadwerkelijk verzonden rapportages.

Uiteindelijk werden 7.612 rapportages daadwerkelijk verzonden, wat neerkomt op 91% van het totale startaantal. Hierbij vertoonde Br2 de hoogste verzendingsgraad van 98%, gevolgd door br1 met 93%. De drie gemeenten verstuurden iets minder, met percentages variërend van 82% tot 92%.

Tabel 3. *Aantal respondenten vooraankondiging en rapportages*

	Ge1	*Ge2*	*Ge3*	*Br1*	*Br2*	Totaal
Start aantal (aangeleverd door organisatie)	1.036	964	995	3794	1.518	8.307
Dubbel met brancheverenging	5	3	6	0	0	14
Verwijderd vanwege non-existing of geen valide domeinnaam	58	141	123	155	11	488
Totaal aantal verzonden vooraankondigingen	973	820	866	3.639	1.507	7.805
Afgemeld door ondernemer	5	18	19	8	3	53
Afgemeld omdat post retour	17	8	18	84	11	138
Initiële populatie onderzoeksgroep (percentages t.o.v. start aantal)	951 (92%)	794 (82%)	829 (83%)	3.546 (93%)	1.492 (98%)	7.612 (91%)

Naast de hierboven genoemde afmeldingen zijn er ook andere reacties van ondernemers ontvangen. Verschillende ondernemers reageerden positief, maar de aangeleverde KvK-gegevens bleken verouderd, waardoor het geregistreerde domein niet meer correct was. In totaal hebben 21 ondernemers verzocht om een aanpassing van het domein, waarna de kwetsbaarhedenmeting is uitgevoerd op het nieuw aangeleverde domein. Naast deze verzoeken werden ook e-mails ontvangen van ondernemers die geen specifieke vraag hadden, maar enkel wilden laten weten dat ze enthousiast waren over het initiatief en met de resultaten aan de slag gingen. Zo gaf een ondernemer uit *Ge2* aan:

> *"Uw conclusies heb ik laten toetsen door onze CISO. Op basis van aanvullende metingen concluderen wij dat we geen hoge risico's lopen en dat één risico al onder de aandacht was. Dank voor uw proactiviteit, het is onder controle."*

Een andere ondernemer uit *Ge3* liet weten:

> *"Wat geweldig dat u onze webpagina's heeft doorgelicht. Heel hartelijk bedankt! Ik heb uw bevindingen doorgespeeld aan de Information Security van [naam], van wiens website wij onderdeel zijn. Zij gaan ermee aan de slag. "*

Voor elke organisatie is een gelijk aantal respondenten willekeurig verdeeld over drie groepen. De eerste groep kreeg de coping-message (totaal 32.9%), de tweede groep ontving een boodschap gericht op geanticipeerde spijt (totaal 33.7%) en de derde groep ontving geen risicocommunicatie (totaal 33.4%). Deze verdeling is weergegeven in Tabel 4.

Tabel 4. *Verdeling Respondenten Organisaties a.d.h.v. Risicocommunicatie*

Organisatie	**Risicocommunicatie**	**Aantal**	**Percentage**
Ge1	Coping	285	3.7 %
Ge1	Geanticipeerde spijt	319	4.14 %
Ge1	Geen risicocommunicatie	322	4.18 %
Ge2	Coping	285	3.7 %
Ge2	Geanticipeerde spijt	287	3.73 %
Ge2	Geen risicocommunicatie	279	3.62 %
Ge3	Coping	271	3.52 %
Ge3	Geanticipeerde spijt	259	3.36 %
Ge3	Geen risicocommunicatie	269	3.49 %
Br1	Coping	1.197	15.55 %
Br1	Geanticipeerde spijt	1.210	15.72 %
Br1	Geen risicocommunicatie	1.211	15.73 %
Br2	Coping	483	6.28 %
Br2	Geanticipeerde spijt	512	6.65 %
Br2	Geen risicocommunicatie	508	6.6 %
Totaal		7.697	100 %

Tot slot is er een controlegroep bestaande uit 2.672 bedrijven die geen rapportage hebben ontvangen. Zij hebben geen interventie ondergaan, waardoor deze groep dient als vergelijkingsbasis om het effect van de interventie op de experimentele groep te kunnen beoordelen.

3.2.6 Definitieve onderzoekspopulatie

Vanwege een probleem met de meting van de items '*Verspreidt uw website geen spam?*' en '*Verspreidt uw mailserver geen spam?*', waarbij sommige ondernemers een onjuiste score hebben ontvangen, is besloten deze ondernemers uit de dataset te verwijderen. In Bijlage VIII is uitgesplitst hoe de scores van ondernemers met een foutieve score verschilden op de betreffende items en in hun totale score tussen de aangepaste en oorspronkelijke voormeting, inclusief het aantal respondenten (N). Omdat dit technisch probleem de effectiviteit van de interventie kon beïnvloeden, zijn alleen de ondernemers waarbij de meting correcte resultaten heeft weergegeven behouden. Daarnaast zijn alle ondernemers die op één (of meerdere) items een missing-value hadden verwijderd. Dit resulteert in een definitieve onderzoekspopulatie van 2.646 ondernemingen (Tabel 6).

Tabel 6. *Verdeling Respondenten Definitieve Onderzoekspopulatie*

		N
Testgroep	*Totaal testgroep*	2.056
	Br1	550
	Br2	959
	Ge1	139
	Ge2	131
	Ge3	277
Controlegroep	*Totale controlegroep*	590
Risicocommunicatie	*Geen risicocommunicatie*	669
	Coping	596
	Geanticipeerde spijt	791
Totale onderzoekspopulatie	*Testgroep + controlegroep*	2.646

3.2.7 Dataverwerking

Gelet op de gevoeligheid van de data is ervoor gekozen om de gegevensuitwisseling via een beveiligde omgeving te laten plaatsvinden. Dit waarborgde de privacy van de betrokken ondernemers en voorkwam dat vertrouwelijke informatie via onbeveiligde kanalen, zoals e-mail, moest worden gedeeld. Er is gebruik gemaakt van Surf Research Drive van de Haagse Hogeschool, dit is een digitale opslagomgeving waar onderzoekers hun onderzoeksdata veilig kunnen opslaan, archiveren en delen. Dit helpt om data goed te beheren en ervoor te zorgen dat informatie toegankelijk blijft. Door gebruik te maken van de Research Drive wordt de kwaliteit en betrouwbaarheid van het onderzoek gewaarborgd, wat belangrijk is voor transparantie en controleerbaarheid binnen het wetenschappelijk proces.

3.2.8 Statistische analysemethoden

Om de effecten van de kwetsbaarhedenmeting in kaart te brengen, zijn de gegevens in SPSS (versie 28) geanalyseerd met behulp van *t*-toetsen. Voor zowel de organisaties als de verschillende vormen van risicocommunicatie werd voor de test- en controlegroep het gemiddelde van de voormeting en de nameting berekend. Vervolgens zijn de verschillen tussen voor- en nameting getest met *t*-toetsen om te bepalen of deze veranderingen significant waren. Deze analyses zijn uitgevoerd voor alle variabelen, waardoor inzicht wordt verkregen in de effecten van de meting per organisatie, per vorm van risicocommunicatie, en in vergelijking met de controlegroep die geen rapportage heeft ontvangen.

3.2.9 Beperkingen

De gebruikte methoden in fase 1 en 3 hebben enkele beperkingen. Deze beperkingen en hoe hiermee is omgegaan in het onderzoek zijn hier toegelicht.

Beperkingen fase 1

De volgende beperkingen hebben betrekking op fase 1, waarin de eerste inzichten zijn verzameld over de effectiviteit en perceptie van de geautomatiseerde evidence-based gedragsinterventie onder ondernemers. Een beperking die in deze fase naar voren kwam heeft betrekking op de respons. De respons op de fieldtrips en interviews was relatief laag. Slechts een klein deel van de aanvankelijk beoogde bedrijven heeft de checklist ingevuld, en uiteindelijk werden slechts enkele interviews afgenomen. Dit kan invloed hebben op de representativiteit van de bevindingen. Het tijdstip van dataverzameling, in de zomerperiode, kan hier een rol hebben gespeeld, aangezien sommige bedrijven gesloten waren of met een beperkte bezetting werkten. Om de lage respons tijdens de eerste fase te verbeteren, hebben we besloten dezelfde bedrijven tijdens een tweede bezoek opnieuw te benaderen, in de hoop dat er dan iemand aanwezig zou zijn. Deze aanpak heeft geleid tot een lichte verhoging van de respons. Het was niet mogelijk om de dataverzameling naar een later tijdstip te verschuiven, omdat dit aanzienlijke vertraging in het project zou veroorzaken.

Beperkingen fase 3

De gebruikte methoden in fase 3 hebben ook enkele beperkingen. De belangrijkste beperking is dat de rapportage die ondernemers ontvangen geen volledig beeld geeft van de werkelijke cyberweerbaarheid van hun onderneming. Omdat alleen openbaar toegankelijke bronnen worden geanalyseerd, blijft een groot deel van de digitale beveiliging buiten beschouwing. Hierdoor kan het voorkomen dat een ondernemer een rapport ontvangt waarin alle gecontroleerde aspecten positief scoren, wat ten onrechte de indruk kan wekken dat er geen verdere actie nodig is. In werkelijkheid kunnen er kwetsbaarheden bestaan in niet-openbaar toegankelijke systemen die niet in het onderzoek zijn meegenomen. Om dit te ondervangen, wordt in de begeleidende brief van de rapportage benadrukt: "*Let op: onze controle op openbare kwetsbaarheden is een goede eerste stap, maar geen volledige beveiligingscontrole van uw website en e-mailserver. Op de laatste pagina van het rapport vindt u verdere stappen om de cyberweerbaarheid van uw onderneming te vergroten*." Hiernaast bevat, zoals eerder benoemd, de laatste pagina van het rapport een handelingsperspectief met praktische adviezen en verwijzingen naar het Digital Trust Center (DTC), waar ondernemers aanvullende informatie en concrete vervolgstappen kunnen vinden. Een laatste beperking van het onderzoek is dat een deel van de data verloren is gegaan doordat sommige ondernemers een onjuiste score hebben ontvangen. Hierdoor kon de interventie niet op de beoogde schaal worden uitgevoerd. Desondanks is de uiteindelijke onderzoekspopulatie voldoende omvangrijk om betekenisvolle analyses uit te voeren en conclusies te trekken.

4. Resultaten

De resultaten worden, net als bij de methoden, in fasen gepresenteerd. Waar de methoden uit twee fasen bestonden, is bij de resultaten een extra fase toegevoegd. Fase 1 richtte zich op hoe ondernemers de rapportage ontvingen, fase 2 behandelt de doorontwikkelingen op basis van deze inzichten, en fase 3 onderzoekt of de kwetsbaarhedenmeting daadwerkelijk effect heeft.

4.1 Resultaten fase 1: Optimalisatie van de gedragsinterventie

4.1.1 Reactie ondernemers op ontvangen van rapportage

In dit hoofdstuk zijn de resultaten van het onderzoek per deelvraag beschreven. Hierbij richten we ons op de volgende onderdelen: de reactie van ondernemers op de vooraankondiging (par. 4.1.2), de beweegredenen voor deelname (par. 4.1.3), het bereik van de brief en rapportage (par. 4.1.4), de beweegredenen voor het openen van de envelop (par. 4.1.5), de beweegredenen voor het lezen van de rapportage (par. 4.1.6), de beweegredenen om over te gaan tot maatregelen (par. 4.1.7) en de beoordeling van de interventie (par. 4.1.8).

4.1.2 Reactie ondernemers op vooraankondiging

In deze paragraaf zijn de resultaten behorend bij de eerste deelvraag '*Hoe reageren ondernemers op de vooraankondiging van de kwetsbaarhedenmeting?*' beschreven.

Zoals in de onderzoeksopzet (par. 3.1) is beschreven, heeft de helft van de geselecteerde ondernemers (*N* = 75) een vooraankondigingsbrief (bijlage I) ontvangen. In deze brief werd benoemd dat de digitale infrastructuur van de website werd geanalyseerd, wat de reden en het belang van de kwetsbaarhedenmeting is, en dat de ondernemer, indien gewenst, zich van deelname kon uitsluiten.

Tijdens de fieldtrips is bij twaalf ondernemers een vragenlijst afgenomen die een aankondigingsbrief hebben ontvangen. Hiervan gaf één ondernemer aan niet op de hoogte te zijn van de ontvangen brief. De elf ondernemers die de aankondigingsbrief hebben ontvangen, hebben deze ook geopend en gelezen. Zes ondernemers geven aan positief te zijn over de brief. De andere vijf ondernemers hebben een neutrale mening over de brief. De ondernemers die de aankondigingsbrief als positief beoordelen, geven aan dat de workflow met een vooraankondiging positief is *(N* = 2), de brief duidelijk is (*N* = 1) en aandacht voor het thema van belang is (*N* = 1).

Naast de positieve oordelen benoemen bevraagde ondernemers een aantal negatieve punten. Eén van de respondenten benoemt dat het als minder prettig wordt ervaren dat als een ondernemer niet aan de kwetsbaarhedenmeting wil deelnemen, hij zelf actie moet ondernemen (*N* = 1). Ook wordt door één geënquêteerde ondernemer benoemd dat hij het karakter van de brief dwingend vond. Al leek dit wel een positief effect te hebben voor deelname.

> *"Workflow is slim. De brief komt wel nogal dwingend over. Als jullie hadden gevraagd of we mee wilden doen, hadden we waarschijnlijk geen actie ondernomen"*

Het dwingende karakter kwam ook naar voren in een mail die we ontvingen naar aanleiding van de aankondigingsbrief. In een paar andere mails die we ontvingen werden vragen gesteld over de authenticiteit van de brief.

> *"In de brief wordt vermeld dat er zonder tegenbericht een scan zal worden uitgevoerd, wat ons enigszins verbaast. [...] Daarnaast valt het dwingende karakter van de brief op. De brief is gedateerd op 29 mei en vereist een reactie vóór 7 juni. Deze signalen doen vermoeden dat er iets niet in de haak is, en we beginnen te twijfelen aan de authenticiteit van deze brief."*

4.1.3 Beweegredenen voor deelname na vooraankondiging

In deze paragraaf zijn de resultaten beschreven om de tweede deelvraag '*Welke beweegredenen hebben ondernemers die een vooraankondiging hebben gekregen om al dan niet mee te doen aan de kwetsbaarhedenmeting?*' te beantwoorden.

Van de 75 ondernemers die een vooraankondiging hebben ontvangen, hebben twee ondernemers zich via e-mail afgemeld. Hiervoor hebben zij verschillende redenen gegeven. Eén van de ondernemers gaf aan dat zij de werkwijze in dit initiatief ongepast vinden. De andere respondent benoemt dat zij een tweemanzaak zijn, waardoor zij niet aan het initiatief willen deelnemen.

Aan ondernemers met vooraankondiging is tijdens de fieldtrips gevraagd of zij hebben overwogen om hun onderneming voor de kwetsbaarhedenmeting af te melden. Drie respondenten geven aan dit te hebben overwogen, vijf respondenten geven aan dit niet te hebben overwogen en de overige drie ondernemers hebben geen expliciete mening hierover. Aan de drie respondenten die afmelding overwogen is vervolgens gevraagd naar de reden om zich niet af te melden voor de kwetsbaarhedenmeting. Hiervoor geven zij verschillende redenen, namelijk omdat ze zijn overgestapt naar een nieuwe dienstverlener (N = 1), door het dwingende karakter van de brief (N = 1) en omdat de mogelijkheid voor afmelding er simpelweg was (N = 1). De respondenten die het afmelden niet hebben overwogen, geven als reden voor deelname aan dat zij het belangrijk vinden om mee te werken (N = 1), het een belangrijk onderwerp vinden (N = 1) of omdat ze nieuwsgierig zijn (N = 1).

Twee van de zeven geïnterviewden hebben een vooraankondiging ontvangen. Eén geïnterviewde geeft aan dat het initiatief intern is besproken en dat zij toen hebben besloten om zich niet voor de interventie af te melden. De geïnterviewde benoemt daarnaast dat ze voor een extra controle van de website openstaan, omdat zij ICT een belangrijk onderwerp vinden en zich daarom niet hebben afgemeld. Ten slotte benoemt de geïnterviewde dat zij binnenkort een interne scan laten uitvoeren, onder andere gericht op Microsoft 365. Hierdoor krijgt het thema cyberweerbaarheid al aandacht en vinden ze de huidige kwetsbaarhedenmeting passend. De andere geïnterviewde geeft aan dat zij veelvuldig met (kwetsbare) data werken en een extra controle daarom waarderen.

4.1.4 Bereik van vooraankondiging en rapportage

In deze paragraaf zijn de resultaten behorend bij de derde deelvraag '*In hoeverre bereiken de vooraankondiging en/of de rapportage de medewerkers die verantwoordelijk zijn voor cybersecurity van de geïncludeerde ondernemingen?*' beschreven.

Zoals in par. 3.1 is beschreven, zijn 150 ondernemers op een bedrijventerrein voor de kwetsbaarhedenmeting geselecteerd. Hiervan hebben 75 ondernemers een vooraankondiging ontvangen. Tijdens de fieldtrips hebben twaalf ondernemers die een vooraankondiging hebben ontvangen de enquête ingevuld. Hiervan geven elf ondernemers aan dat ze de brief hebben ontvangen en één ondernemer geeft aan hier niet van op de hoogte te zijn. De overige achttien ondernemers die de enquête hebben ingevuld, hebben geen vooraankondiging ontvangen.

Daarnaast is aan de ondernemers gevraagd of zij het poststuk (brief + rapportage) hebben ontvangen. Hierbij geven 28 van de 30 respondenten aan dit te hebben ontvangen.

Twee respondenten benoemen dat ze niet op de hoogte zijn van het poststuk. In het verlengde hiervan is aan de respondenten gevraagd of het poststuk bij de juiste persoon terecht is gekomen. Hierbij gaat het om de werknemer die verantwoordelijk is voor de cybersecurity in de onderneming. 24 respondenten geven aan dat het poststuk bij de verantwoordelijke voor cybersecurity terecht is gekomen, twee respondenten geven aan dat het poststuk niet bij de juiste persoon terecht is gekomen en twee respondenten wisten dit niet.

4.1.5 Beweegredenen voor wel/niet openen envelop

In deze paragraaf zijn de resultaten behorend bij de vierde deelvraag *'Welke beweegredenen hebben ondernemers om de envelop wel/niet te openen*?' beschreven. Hierbij worden de resultaten voor de subvraag '*In hoeverre heeft het logo op de envelop hier invloed op?'* tevens gepresenteerd.

In zowel de enquête als in de interviews is aan ondernemers gevraagd waarom zij het poststuk wel/niet hebben geopend. De respondenten van de enquête geven als voornaamste reden om het poststuk wel te openen dat zij nieuwsgierig waren (*N* = 5) of dat zij alle poststukken openen (*N* = 4). Andere redenen die de respondenten noemen, zijn dat NHL Stenden een bekende partij is voor de desbetreffende ondernemer (*N* = 2) en omdat de aankondigingsbrieven zijn geopend (*N* = 2).

Een aantal respondenten benoemen ook redenen waarom ze het poststuk (nog) niet hebben geopend. Hierbij geven twee respondenten aan dat ze door de vakantie het poststuk nog niet hebben geopend en één respondent benoemt dat ze hun ICT centraal hebben geregeld, waardoor ze niet aan initiatieven deelnemen.

In de interviews is tevens aan ondernemers naar de beweegredenen voor het openen van de brief gevraagd. Hierbij geven zes geïnterviewden aan dat zij altijd alle post lezen en om deze reden de envelop hebben geopend. Eén geïnterviewde benoemt dat zij een vooraankondiging hebben ontvangen, waardoor zij ook de tweede brief hebben geopend.

Invloed logo's

Uit de resultaten komt naar voren dat het voor de respondenten niet uitmaakt welk logo er op de envelop staat, omdat zij veelal alle post openen. Uit één van de interviews komt aanvullend naar voren dat als de interventie in andere delen van Nederland wordt uitgevoerd, een logo op de envelop dient te staan die past bij de regio.

4.1.6 Beweegredenen voor wel/niet lezen rapportage

In deze paragraaf zijn de resultaten behorend bij de vijfde deelvraag '*Welke beweegredenen hebben ondernemers om de rapportage wel/niet te lezen?*' beschreven. Daarnaast worden de resultaten voor de subvragen '*In hoeverre heeft de bijgevoegde brief hierop invloed gehad?*' en '*In hoeverre hebben de logo's hierop invloed gehad?*' gepresenteerd.

Aan respondenten van de enquête is gevraagd of zij zelf of de verantwoordelijke voor cybersecurity de rapportage heeft gelezen. Hierbij gaven vijftien respondenten aan de rapportage te hebben gelezen, twee respondenten gaven aan de rapportage niet te hebben gelezen en in zes gevallen is dit anders verlopen. Vervolgens is aan respondenten gevraagd waarom ze de rapportage wel/niet hebben gelezen. Interesse en nieuwsgierigheid worden als voornaamste reden genoemd (*N* = 4) om de rapportage te lezen. Daarnaast gaf één respondent aan dat er geen specifieke reden was om de rapportage te openen (N = 1). De respondenten die aangaven de rapportage niet te hebben gelezen, geven vakantie (*N* = 1) of het nog moeten doorsturen naar de juiste afdeling (*N* = 1) als reden. In de gevallen dat het anders is verlopen, benoemt één van de respondenten dat de rapportage gedeeltelijk is gelezen, omdat het onderwerp ook deels eerder is uitgelegd.

Invloed brief

De geïnterviewden geven aan dat zij de brief en rapportage veelal als één stuk ervaren, waarbij het lezen van de brief niet per definitie invloed heeft op het al dan niet lezen van de bijgevoegde rapportage. Daarnaast wordt nieuwsgierigheid door in de brief te benoemen dat (mogelijk) kwetsbaarheden zijn gevonden als reden genoemd.

Invloed logo's

Ook is aan respondenten gevraagd naar hun mening over de logo's op de envelop en brief. Hierbij komt naar voren dat zeven ondernemers positief zijn over de logo's, zestien ondernemers geven aan een neutrale mening te hebben, één ondernemer is negatief over de logo's en zes ondernemers hebben geen antwoord gegeven op de vraag.

Respondenten die aangaven een positieve mening te hebben over de logo's op de brief, benoemen dat het hierdoor duidelijk is wie de brief heeft verstuurd (*N* = 2) en dat deze logo's een vertrouwd gevoel geven (*N* = 1). Respondenten die een neutrale mening over de logo's hebben, geven aan dat ze geen sterke mening hebben of hier niet expliciet naar hebben gekeken (*N* = 3) en dat het NHL Stenden logo opviel (*N* = 2). Bij deze laatste twee respondenten benoemt één van hen dat de onderneming eerder met de hogeschool heeft samengewerkt. De andere respondent geeft aan dat de hogeschool bij hen bekend is en het hierdoor als legitiem is ervaren. Ook werd door respondenten benoemd dat ze niet expliciet naar de logo's hebben gekeken, dat het logo van PVO opviel en dat het logo bovenaan het meest opvalt. Ten slotte heeft één respondent een toelichting gegeven op een negatieve mening, namelijk dat er te veel logo's op de voorkant van de brief staan.

De geïnterviewden bevestigen bovenstaande bevindingen. Alle geïnterviewden geven aan dat (het logo van) de afzender geen verschil zou maken, al benoemen twee van hen dat het logo van NHL Stenden opviel en vertrouwen heeft opgewekt. Eén van hen benoemt dat hij bekend is met deze partij

en positieve ervaringen heeft gehad. Ook geeft deze geïnterviewde aan het handig te vinden dat de logo's van alle betrokken partijen onderaan de brief zijn opgenomen.

4.1.7 Beweegredenen voor wel/niet overgaan tot maatregelen

In deze paragraaf zijn de resultaten behorend bij de zesde deelvraag '*Welke beweegredenen hebben ondernemers om wel/niet over te gaan tot maatregelen?'* beschreven. Tevens worden de resultaten van de drie subvragen gepresenteerd: '*In hoeverre heeft de bijgevoegde brief hierop invloed gehad?', 'In hoeverre heeft de bijgevoegde rapportage hierop invloed gehad?'* en '*In hoeverre hebben de rapportage en de brief de perceptie van ondernemers op digitale veiligheid binnen hun organisatie beïnvloed?*'.

Overgaan tot maatregelen

Wanneer respondenten bij de voorgaande vragen in de enquête hebben aangegeven de brief en rapportage te hebben gelezen, is hen vervolgens gevraagd of zij, op basis van de adviezen in de rapportage, van plan zijn om vervolgstappen te zetten. Vijf respondenten hebben aangegeven reeds stappen te hebben ondernomen. Al deze respondenten geven aan contact met de systeembeheerder of externe ICT'er te hebben opgenomen.

Een deel van de respondenten (*N* = 11) heeft de intentie om stappen te gaan ondernemen, al heeft dit op moment van afname nog niet plaatsgevonden. In alle gevallen is de intentie om contact op te nemen met de systeembeheerder of externe ICT'er. Zes respondenten hebben geen stappen ondernomen en zijn ook niet van plan om dat te doen. Redenen die hiervoor worden genoemd, zijn dat de uitkomsten niet als dringend of verontrustend worden ervaren (*N* = 2), dat de ondernemer alles heeft uitbesteedt en de website enkel gebruikt om informatie te versturen (*N* = 1), of dat door het hoogseizoen nog geen actie is ondernomen (*N* = 1). Zeven respondenten geven aan dat dit nog niet duidelijk is. Redenen die worden genoemd, zijn dat het afhankelijk is wat de ICT-beheerder zegt (*N* = 4) en dat het bedrijf zich nog in de rapportage moet verdiepen (*N* = 1).

Alle geïnterviewden geven aan al maatregelen te hebben doorgevoerd of de intentie hebben om dit te doen. Eén geïnterviewde geeft bijvoorbeeld aan dat de informatie aan de IT-partijen is doorgestuurd en dat zij reeds een terugkoppeling hebben ontvangen. In deze terugkoppeling stond vermeld dat de IT-partijen geen reden zagen om actie te ondernemen, omdat er volgens hen geen risico aanwezig is. Een andere geïnterviewde geeft aan dat bepaalde bevindingen uit de rapportage naar de externe ICT partij zijn doorgegeven en dat zij reeds wijzigingen hebben doorgevoerd. Daarnaast heeft deze respondent diverse e-mailadressen op 'Have I been powned' gecontroleerd. De geïnterviewde benoemt in het verlengde hiervan dat zij als organisatie van plan zijn om deze controle op domeinnaamniveau te laten controleren, maar dat zij dit intern, financieel, moeten verantwoorden. Ten slotte benoemt respondent 7 dat zij het thema bij de werknemers onder de aandacht hebben gebracht, bijvoorbeeld op het gebied van veilige wachtwoorden.

Invloed brief en rapportage op het overgaan tot maatregelen

Uit de interviews komt naar voren dat de brief en rapportage bij vijf van zeven ondernemers invloed hebben gehad op het overgaan tot maatregelen. Eén geïnterviewde geeft aan dat zij door de brief en

rapportage noodzaak voelen om stappen te nemen. Twee andere geïnterviewden geven daarentegen aan dat zij reeds met het thema bezig zijn, waardoor zij door de brief en rapportage niet direct de noodzaak voelen. Een geïnterviewde benoemt bijvoorbeeld dat de brief en rapportage niet per definitie invloed hebben gehad op het overgaan tot maatregelen, omdat zij alles hebben besteed. Diegene geeft wel aan dat de brief en rapportage naar de externe ICT'er zijn verstuurd, zodat zij, indien gewenst, de bevindingen kunnen doorvoeren. Op het moment van onderhavig onderzoek heeft de geïnterviewde nog geen reactie van de partij ontvangen. Een andere geïnterviewde geeft aan dat zij als bedrijf in de veronderstelling waren dat de onderdelen die in de rapportage naar voren zijn gekomen, werden meegenomen door de websitebouwer en dat dit onderdeel was van het takenpakket van de websitebouwer. De rapportage heeft hen laten inzien dat zij hier zelf ook een verantwoordelijkheid in hebben.

Invloed brief en rapportage op perceptie cyberweerbaarheid

Uit de interviews komt naar voren dat de respondenten verdeeld zijn over de invloed van de brief en rapportage op hun perceptie op cyberweerbaarheid. Twee respondenten geven aan dat middels deze interventie meer bewustwording voor het thema is gecreëerd en zij serieuzer met het thema aan de slag willen gaan. Hierbij maakt de respondent de kanttekening dat ze niet direct in de actiestand zijn gegaan, maar wel van plan zijn om actie te gaan ondernemen. Een andere respondent geeft aan dat de interventie niet per definitie invloed heeft op de perceptie, omdat zij vanuit de bedrijfsvereniging eerder soortgelijke testen hebben laten uitvoeren. In deze testen is bijvoorbeeld gekeken naar de beveiliging van het wifi-netwerk. Daarnaast geeft de respondent aan dat alles omtrent de digitale beveiliging is uitbesteed om de veiligheid te waarborgen en zij hierdoor zich minder met het thema bezighouden. Desalniettemin, is het volgens de respondent positief om af en toe het thema onder de aandacht te brengen. Twee respondenten benoemen dat cyberweerbaarheid prioriteit heeft en dat de rapportage hier geen verandering in heeft gebracht. Zij zijn namelijk in de veronderstelling dat ze al diverse maatregelen treffen en digitaal veilig werken.

4.1.8 Beoordeling interventie door ondernemers

In deze paragraaf zijn de resultaten behorend bij de zevende deelvraag '*Hoe beoordelen ondernemers het initiatief van de kwetsbaarhedenmeting en de communicatieproducten*?' beschreven.

Aan het einde van de enquête is aan ondernemers gevraagd in hoeverre zij dit initiatief waarderen en of zij verbeterpunten hebben. Een groot deel van de ondernemers geeft aan het initiatief als positief te ervaren (*N* = 20). Hierbij benoemen zij dat zij van de uitkomsten kunnen leren, inzicht in de risico's krijgen, dat tijd om naar een partij toe te stappen een belemmering kan zijn, dat het een ongevraagde prikkel is om actie te ondernemen en dat de werkwijze als prima wordt ervaren. Daarnaast benoemen een aantal ondernemers twijfels te hebben over het initiatief, bijvoorbeeld dat het mogelijk als scam kan worden ervaren en dat de commerciële partij hier ook een bepaald belang bij kan hebben.

De verbeterpunten die uit de enquêtes naar voren zijn gekomen, hebben voornamelijk betrekking op dat een aankondigingsbrief is gewenst *(N* = 4), al benoemt één respondent ook dat

ondernemers naar aanleiding van de aankondiging hun beveiliging kunnen aanpassen waardoor niet de juiste situatie wordt weergegeven. Een ander verbeterpunt is dat de rapportage vooral gericht is op een ICT'er/ICT-afdeling, waardoor het voor reguliere werknemers als moeilijk leesbaar wordt ervaren. Om de leesbaarheid te verhogen, zouden concrete voorbeelden kunnen helpen. Ten slotte wordt de betrokkenheid van een commerciële partij als mogelijke belemmering genoemd. Het bijbehorende verdienmodel wordt door een aantal respondenten als discutabel ervaren.

In de interviews is tevens aan de ondernemers gevraagd hoe zij de interventie en communicatieproducten beoordelen, en of zij mogelijk verbeterpunten voor de interventie hebben. Uit de interviews komen veelal dezelfde punten naar voren als bij de enquête, namelijk dat de geïnterviewden de interventie positief waarderen en in de veronderstelling zijn dat de interventie ook elders kan worden uitgevoerd.

Beoordeling communicatieproducten

Zes respondenten geven over het algemeen een positief oordeel over de brief, zowel qua vormgeving als inhoud. Twee van de respondenten benoemen dat de brief korter en bondiger kan, waardoor eerder de belangrijkste boodschap wordt gegeven. Als voorbeeld benoemt één van hen dat de belangrijkste punten middels bullet points bovenaan de brief kunnen staan en dat daaronder een verdieping wordt gegeven. Eén respondent geeft aan kritisch te zijn op de brief. Deze respondent geeft aan dat de brief duidelijk is, maar dat de toon als belerend is ervaren.

> "*Het werd heel streng neergezet, alsof je eigenlijk slecht bent. Eigenlijk had er wel iets mogen staan om het persoonlijk toe te lichten. Dus hoe groot de risico's zijn, persoonlijk toe te lichten in plaats van alleen maar te constateren. Wat ik ook mis, is hoe kunnen we het voorkomen en is het wel te voorkomen?*" (R.6)

Vervolgens is in de interviews gevraagd naar de mening van de ondernemers over de bijgeleverde rapportage. De geïnterviewden geven aan de rapportage en de bijgeleverde adviezen als bruikbaar te ervaren. Eén van hen noemt expliciet dat er geen informatie ontbreekt. Desalniettemin, geven twee geïnterviewden aan dat de informatie in de rapportage als te technisch en moeilijk leesbaar kan worden ervaren. Dit geldt volgens hen vooral voor kleine ondernemers die geen ICT'er in dienst hebben. Hierbij geeft één van de geïnterviewden als verbeterpunt om concrete voorbeelden te gebruiken.

> *"De 'what's in it for me' is belangrijk. Als een ondernemer dit krijgt en die heeft er geen verstand van, snapt ie het niet. Mijn collega, die deze brief uit de brievenbus heeft gepakt, die opende de envelop en checkte de brief en die dacht 'laat maar, dit is mij te moeilijk' en die legde 'm dus weg."* (R.3)

Beoordeling interventie

In de interviews zijn een aantal onderdelen van de interventie nader toegelicht, namelijk de vooraankondiging en de aanpak in de interventie. Wat betreft de vooraankondiging van de interventie

zijn de respondenten verdeeld. Drie van hen benoemen dat dit niet noodzakelijk is. Eén van hen legt uit dat wanneer een vooraankondiging wordt verzonden, een ondernemer rekening kan houden met de uitvoering van de interventie en mogelijk verbeteringen kan uitvoeren. Als kanttekening geeft de respondent aan dat grote bedrijven hier mogelijk anders tegenaan kijken dan kleine bedrijven. Desalniettemin, geeft deze respondent aan geen problemen te hebben met de aanpak zonder een vooraankondiging. De andere respondenten geven aan dat een vooraankondiging gewenst is. Eén geïnterviewde geeft als voorbeeld dat de branche- of bedrijfsvereniging hierin kan worden betrokken. Deze respondent geeft aan dat zij in de eerste instantie verbaasd waren toen zij de brief en rapportage ontvingen. Daarnaast geeft de respondent aan dat zij eerst in de veronderstelling waren dat de interventie mogelijk nep zou kunnen zijn, al wekte het logo van NHL Stenden Hogeschool op de envelop vertrouwen. Desalniettemin, geeft de respondent aan dat oplichters ook dit logo kunnen gebruiken. Een andere geïnterviewde geeft aan dat een aankondiging gewenst is, omdat een rapportage zonder aankondiging mogelijk onverwachts voor de ondernemers kan aankomen en dat zij mogelijk het gevoel krijgen dat anderen zich met de organisatie bemoeien. Deze respondent geeft wel de mogelijkheid dat een vooraankondiging (indirect) door media-aandacht kan worden gegenereerd. Als er in de media veel aandacht is voor het thema en vanuit de zender, zoals een overheid, wordt gezegd dat er meer controle op plaats gaat vinden, zou dat ook als vooraankondiging kunnen gelden. De respondent maakt hierbij de vergelijking met bepaalde wetgeving waar organisaties zich aan dienen te houden en waarop controles worden uitgevoerd.

Wat betreft de aanpak zijn de respondenten over het algemeen positief over de interventie en benoemen dat dit een handig hulpmiddel is om kennis over het thema bij ondernemers te verbeteren; voornamelijk bij ondernemers bij wie het thema minder hoog op de agenda staat. De respondenten benoemen verschillende onderdelen waarin zij verbetering mogelijk zien. Eén geïnterviewde benoemt dat het betrekken van een commerciële partij mogelijk discutabel is. De respondent geeft als verbeterpunt het mogelijk betrekken van studenten in plaats van de commerciële partij. Studenten van een bepaalde opleiding zouden ook een dergelijke meting als schoolopdracht kunnen ontwikkelen en afnemen. Drie andere respondenten geven aan dat in de aanpak rekening moet worden gehouden met kleinere bedrijven op een bedrijventerrein en dat zij tijdens hun eigen werkzaamheden zien dat deze groep achterblijft. Beide zijn in de veronderstelling dat deze manier van informatie aanreiken kan werken bij kleine bedrijven, maar dat er ook kleine bedrijven zijn die weinig tot niks aan cybersecurity doen. Eén van hen noemt expliciet dat zij een daling zien in het aantal bedrijven dat een cybersecurityverzekering afsluit. Bij deze ondernemers kan de inhoud van de rapportage mogelijk te complex zijn, al vinden de respondenten dit initiatief wel passend voor deze groep en werkt dit mogelijk voor hen beter dan (landelijke) overheidscampagnes.

> “Er zitten hier ook kleinere bedrijfjes die niks hebben. Ik zie dat in de praktijk ook bij onze klanten. Dan kom ik ergens en hebben ze een Windows 7 computer. Daar maak ik dan wel een opmerking over. Maar ja, als je nog nooit bent gehackt of nog nooit een virus hebt gehad, zie je daar de meerwaarde niet van in. Cybersecurity kost vrij veel geld. Ik snap dat kleinere bedrijfjes dat niet doen. Dan vind ik zo'n initiatief wel mooi.” (R.5)

Ten slotte benoemt respondent 3 dat in de selectie van bedrijven voor het initiatief meer kan worden gekeken naar de branche waarop het initiatief wordt uitgevoerd. Hierbij kan volgens de respondent onderscheid worden gemaakt tussen bedrijven waarvoor het initiatief wel/niet relevant kan zijn. De respondent is in de veronderstelling dat dit initiatief voornamelijk voor kleine ondernemingen of eenmanszaken relevant kan zijn, omdat die hier wellicht niet alle kennis voor hebben en/of een IT-partner hebben.

4.2 Resultaten fase 2: Doorontwikkelingen interventie

Op basis van de bevindingen van de pilot (Van 't Hoff-De Goede et al., 2024) en fase 1 van het huidige onderzoek (paragraaf 4.1) zijn diverse aspecten geïdentificeerd waarbij verdere doorontwikkeling van de interventie wenselijk was om de effectiviteit van de interventie te vergroten. In dit hoofdstuk worden de aanbevelingen uiteengezet die zijn doorgevoerd (zie paragraaf 4.2.1).

4.2.1 Aanbevelingen die zijn doorontwikkeld

In deze paragraaf worden de aanbevelingen die zijn doorontwikkeld besproken. Deze aanbevelingen zijn deels voortgekomen uit de pilot en deels uit fase 1 van dit onderzoek. Daarnaast zijn er tijdens een bijeenkomst door professionals verschillende aanbevelingen gedaan. In paragraaf 4.2.1.1 worden de doorontwikkelingen met betrekking tot de interventie behandeld en in paragraaf 4.2.1.2 komen de doorontwikkelingen van het onderzoeksproject aan bod.

4.2.1.1 Doorontwikkelingen interventie

De volgende doorontwikkelingen hebben betrekking met aspecten die de daadwerkelijke interventie betreffen. Hierbij ligt de nadruk op praktische toepassingen die gericht zijn op het versterken van de effectiviteit van de aanpak.

Verandering logo's

De logo's op de begeleidende brief die naar de ondernemers is verstuurd, werden aangepast om de samenwerking met de nieuwe partners correct weer te geven. Het gaat hier om NHL Stenden Hogeschool, de Haagse Hogeschool en ThreadStone. Daarnaast zijn logo's toegevoegd van de organisatie waartoe de ondernemer behoort. Dit betreft ofwel een van de twee brancheorganisaties of een van de drie deelnemende gemeenten. Het toevoegen van logo's is bedoeld om ervoor te zorgen dat ondernemers de organisaties herkennen, wat de legitimiteit van de interventie vergroot.

Toevoegen van een vooraankondiging met opt-out

In de pilot is naar voren gekomen dat meerdere respondenten bezwaar maakten tegen het ongevraagde karakter van de kwetsbaarhedenmeting en de verwerking van persoonsgegevens. In de bijgevoegde brief werd al uitgelegd dat er geen juridische bezwaren zijn tegen de werkwijze. Daarnaast is het huidige onderzoek beoordeeld door een ethische commissie. We verduidelijken dit nu verder door middel van eenvoudiger taalgebruik. Een nadere toelichting op het taalgebruik vindt u onder het kopje 'Aanpassen taalgebruik' verderop in deze paragraaf.

Door verschillende professionals werd, tijdens het congres van CyberweerbaarNL en Centrum voor Criminaliteitspreventie en Veiligheid op 19 september in Apeldoorn, voorgesteld om ondernemers vooraf te informeren over de kwetsbaarhedenmeting en hen een opt-out mogelijkheid te bieden. Deze aanpak zou het ongevraagde karakter van de meting verminderen en ondernemers de keuze geven om al dan niet deel te nemen. Om deze reden is besloten om het gebruik van een vooraankondiging met opt-out te onderzoeken. In fase 1 van ons onderzoek hebben we de helft van

de ondernemers voorafgaand aan de kwetsbaarhedenmeting een vooraankondiging gestuurd, waarbij zij de mogelijkheid kregen om zich af te melden (opt-out).

Uit het onderzoek in fase 1 bleek dat de meeste ondernemers die de vooraankondiging hebben ontvangen, de brief geopend en gelezen hadden, en oordeelden hier grotendeels neutraal tot positief over. De vooraankondiging bereikte in de meeste gevallen de juiste persoon binnen de organisatie, namelijk degene die verantwoordelijk is voor cybersecurity.

In de effectmeting (fase 3) is daarom besloten alle ondernemers voorafgaand aan de meting een vooraankondiging te sturen (Bijlage I). In deze brief werd uitgelegd wanneer de meting zou gaan plaatsvinden, door wie deze wordt uitgevoerd, waarom dit gebeurt en wat de vervolgstappen zijn. In de communicatie richting de ondernemers vanuit de gemeenten werd expliciet vermeld dat ondernemers vijf werkdagen de tijd hadden om zich af te melden. Bij de brancheverenigingen werd alleen aangegeven dat ondernemers bij vragen per e-mail contact konden opnemen, zonder expliciet de mogelijkheid tot afmelding te benoemen. In deze brief hebben de vijf deelnemende organisaties bovendien hun eigen motivatie kunnen toevoegen op de daarvoor aangegeven plek in Bijlage I. De motivatie van alle gemeenten was: *'Gemeente X ondersteunt ondernemers bij het vergroten van hun cyberweerbaarheid*.' De brancheverenigingen formuleerden hun motivatie als volgt: de ene vereniging gaf aan deel te nemen *'om de cyberweerbaarheid binnen de branche te vergroten*,' terwijl de andere aangaf deel te nemen *'om haar leden ook preventief te ondersteunen bij veilig ondernemen*.'

Toevoegen van contactgegevens

Tijdens de pilot gaf een aantal ondernemers aan dat het ontbreken van contactgegevens in de communicatie een knelpunt vormde. Om dit op te lossen, worden nu duidelijke contactgegevens opgenomen in de brief, waarbij ondernemers contact kunnen opnemen via het genoemde e-mailadres. Hiermee werd communicatie met ondernemers mogelijk gemaakt en werd de drempel verlaagd voor het sturen van vragen of opmerkingen door ondernemers.

Doorontwikkeling risicocommunicatie

Een andere doorontwikkeling van de interventie betreft de risicocommunicatie. Uit de pilot bleek dat ondernemers die de risicocommunicatie geanticipeerde spijt ontvingen het hoogste percentage verbetering in hun cyberweerbaarheid vertoonden. In het huidige onderzoek is opnieuw een literatuuronderzoek uitgevoerd om te onderzoeken of er andere studies zijn die aanvullende factoren voor effectieve risicocommunicatie identificeerden, welke aansluiten bij de behoeften van ondernemers.

Uit dit literatuuronderzoek blijkt dat de Protection Motivation Theory (PMT) nuttig kan zijn voor een risicocommunicatie (zie paragraaf 2.4). Dit model onderzoekt het cognitieve proces dat mensen aanzet tot actie wanneer zij geconfronteerd worden met een dreiging. Diverse studies laten zien dat een coping-message effectief kan om mensen aan te moedigen tot actie en zo hun cyberweerbaarheid te vergroten. Daarom wordt een coping-message ingezet in de risicocommunicatie van de interventie. De eerste groep ontving de risicocommunicatie coping-message waarin ondernemers worden aangespoord om maatregelen te nemen tegen

cybercriminaliteit. De gebruikte boodschap luidt: *"Maak uw bedrijf weerbaar tegen cybercriminaliteit. Dit rapport laat zien waar uw bedrijf kwetsbaar is voor online aanvallen. Bespreek deze punten met uw IT-leverancier om eenvoudige maatregelen te nemen en uw bedrijf te beschermen tegen online gevaren."*

De tweede groep ondernemers ontving een vorm van risicocommunicatie die zich richt op geanticipeerde spijt. Hierbij is de volgende boodschap gebruikt: *"Voorkomen is goedkoper dan genezen! Werk nu aan uw cyberweerbaarheid om latere kosten te voorkomen."* Deze benadering is eerder gebruikt in het onderzoek van Van 't Hoff-de Goede et al. (2024), waarin ondernemers die deze vorm van risicocommunicatie ontvingen, een significante stijging in hun cyberweerbaarheid lieten zien in vergelijking met de controlegroep die geen rapportage heeft ontvangen.

De derde groep ondernemers ontvingen geen aanvullende risicocommunicatie. Zij ontvingen, net als de andere twee groepen, achtergrondinformatie over het risico van cybercriminaliteit en het belang van cyberweerbaarheid voor ondernemers.

Verduidelijking van de niet-commerciële doelstellingen in brief

Uit zowel de pilot als fase 1 kwam naar voren dat een aantal respondenten de interventie associeerde met een commerciële ondertoon. Om dit misverstand weg te nemen, is in fase 3 expliciet gecommuniceerd dat de interventie geen commerciële doeleinden heeft, maar gericht is op het vergroten van de cyberweerbaarheid van ondernemingen en dat het onderzoek enkel educatieve doeleinden betreft. In de bijgevoegde brief die naast de rapportage naar ondernemers wordt verstuurd, wordt om deze reden de volgende vraag toegevoegd: *"Is dit reclame of een commercieel project?",* waarna vervolgens wordt uitgelegd dat dit niet het geval is.

Aanpassen taalgebruik

In fase 1 werd duidelijk dat de brief en de rapportage voor sommige ondernemers te technisch en daardoor lastig te begrijpen was. Daarnaast is het taalniveau in acht genomen. Alle teksten zijn nu opgesteld op taalniveau B1, zoals aanbevolen door de Rijksoverheid. Dit taalniveau staat voor eenvoudig Nederlands en is toegankelijk voor de meeste mensen in Nederland. Ingewikkelde termen worden hierbij zoveel mogelijk vermeden. Daarnaast is het aantal woorden in de vooraankondiging, de bijgevoegde brief, de rapportage en het handelingsperspectief waar mogelijk verminderd.

Doorontwikkeling handelingsperspectief

Het handelingsperspectief werd aangepast van scenario's naar stappen. In de pilot werden in het handelingsperspectief twee scenario's beschreven: één voor ondernemers zonder IT-leverancier en één voor ondernemers met een IT-leverancier. Dit wordt nu veranderd naar twee stappen. Stap 1 richt zich op het aanpakken van gevonden kwetsbaarheden. Dit perspectief houdt rekening met twee scenario's: ondernemers met en zonder een IT-leverancier. Voor ondernemers zonder IT-leverancier die overwegen een IT-leverancier in de arm te nemen wordt verwezen naar een website van het Digital Trust Center (DTC), waar adviezen staan beschreven voor het zoeken naar een IT-leverancier. Voor ondernemers met een IT-leverancier wordt verwezen naar een andere website van het DTC, waar wordt beschreven hoe zij het gesprek kunnen aangaan met hun leverancier over de gevonden

kwetsbaarheden. In stap 2 worden ondernemers erop gewezen dat cybersecurity breder is dan de gemeten kwetsbaarheden in het rapport, en worden zij voor meer informatie over de vijf basisprincipes van cybersecurity verwezen naar een derde website van het DTC. Het handelingsperspectief is te zien in Bijlage IV.

4.2.1.2 Doorontwikkelingen onderzoeksproject

De volgende doorontwikkelingen hebben betrekking op aspecten die het onderzoeksproject zelf beïnvloeden. Hierbij ligt de nadruk op methodologische verbeteringen die gericht zijn op het vergroten van de betrouwbaarheid en validiteit van de onderzoeksresultaten.

Inzicht ontvangst van brieven en rapportage door ondernemers

Tijdens de pilot konden er geen uitspraken gedaan worden over het bereik van de interventie. Het was onduidelijk of de verbetering van de cyberweerbaarheid kwam door de rapportage, of dat dit kwam door toeval. Om inzicht te krijgen in de mate waarin ondernemers daadwerkelijk de rapportages openen en lezen, werd een checklist ontwikkeld die kan meten hoe ondernemers omgaan met de ontvangen informatie. Vervolgens zijn onderzoekers met deze checklist langs ondernemers gegaan, zoals uitgebreid besproken in de methoden (paragraaf 3.1). Dit moet bijdragen aan een beter begrip van het bereik en de impact van de rapportages. De gebruikte checklist is toegevoegd in Bijlage V. Hiernaast zijn ook interviews gehouden voor een verdiepend inzicht, dit is gedaan aan de hand van een interview, te vinden in bijlage VII.

Verbeteren representatie van gemeten bedrijven

In de pilot was het niet mogelijk om vast te stellen of de gemeten bedrijven representatief waren voor het volledige spectrum van Nederlandse ondernemingen, omdat er geen informatie beschikbaar was over hun demografische kenmerken. Dit gebrek aan data maakt het lastig om de resultaten te generaliseren. In de pilot werd aangegeven dat het voor verdere doorontwikkeling belangrijk is om te zorgen voor een bredere dataverzameling. In het huidige onderzoek worden twee branches geïncludeerd, waardoor er informatie beschikbaar is over de sector van de steekproef. Deze bevindingen kunnen worden vergeleken met die vanuit de drie gemeenten, waarbij geen selectie op branche heeft plaatsgevonden. Ook is er een steekproef geïncludeerd die groter en daarmee representatiever is dan in de pilot. Dit zorgt ervoor dat de steekproef in het huidige onderzoek een betere afspiegeling vormt van Nederlandse bedrijven.

4.3 Resultaten fase 3: Effectiviteit van de kwetsbaarhedenmeting

In deze paragraaf worden de resultaten van fase 3 besproken. Hierbij wordt gekeken naar het effect van de interventie op de cyberweerbaarheid van ondernemers. Er wordt onderscheid gemaakt tussen de testgroep en de controlegroep die geen rapportage heeft ontvangen, de verschillende organisaties en de gebruikte risicocommunicatie.

4.3.1 Beschrijvende statistiek voormeting

Om inzicht te krijgen in de cyberweerbaarheid van de ondernemers wordt in deze paragraaf de beschrijvende statistiek van de voormeting besproken. In Tabel 6 worden onder andere beschrijvende statistieken van de eerste meting weergegeven (kolommen “voor”). Voor elke variabele zijn de minimum- en maximumwaarden opgenomen. Voor de losse items geldt dat een lage score wijst op een lage kwetsbaarheid en dus een lager risico, terwijl een hoge score duidt op een grotere kwetsbaarheid en dus een groter risico. Er is een nieuwe variabele totaalscore aangemaakt, namelijk alle risicopunten bij elkaar opgeteld (met uitzondering van de items ‘*Verspreidt uw website geen spam?*’ en ‘*Verspreidt uw mailserver geen spam?*’ zoals benoemd in paragraaf 3.2.6). Een hoger totaal aantal risicopuntenscore betekent dus een hogere kwetsbaarheid. Een visualisatie van de resultaten van de voormeting is opgenomen in Figuur 1.

Totale onderzoeksgroep/testgroep/controlegroep

Zoals te zien is in Tabel 6 bestaat de totale onderzoeksgroep uit 2.646 respondenten. De totale risicopuntenscore varieert van minimaal 0 tot maximaal 12,25. Gemiddeld behaalden de respondenten in de voormeting een 6,39 risicopuntenscore. De testgroep scoorde bij de voormeting gemiddeld lager, met een 6,16 risicopuntenscore, terwijl de controlegroep die geen rapportage heeft ontvangen een hogere gemiddelde risicoscore had van 7,20. Deze verschillen zijn ook zichtbaar op itemniveau, op vrijwel alle afzonderlijke items scoort de controlegroep lager dan de testgroep, met uitzondering van de items *‘gevoelige gegevens medewerkers openbaar’*, *‘informatie configuratie website afgeschermd’* en *‘manipulatie websiteverkeer mogelijk’,* waar de verschillen nihil zijn.

Organisaties

De organisaties verschillen onderling in hun risicopuntenscore. Opvallend is dat ondernemers van organisatie Br2 aanzienlijk lager scoren dan de overige organisaties, met een gemiddelde van een 4,63 risicopuntenscore. De andere organisaties scoren tussen de 6,63 (Ge3) en 8,13 (Ge2). Dit verschil is ook zichtbaar op itemniveau. Vooral bij de items *‘kan e-mail misbruikt worden’*, *‘onderschepping websiteverkeer*, *‘ongebruikelijke aanvalspaden op website’* en *‘manipulatie websiteverkeer mogelijk’* scoort organisatie Br2 duidelijk lager dan de rest. De overige organisaties liggen bij de meeste items dicht bij elkaar. De grootste onderlinge verschillen zijn te zien bij de items *‘onderschepping websiteverkeer*, waarbij de laagste score een 0,30 (Br2) en de hoogste score een 1,66 (Ge2) is, en *‘manipulatie websiteverkeer mogelijk’* waarbij de laagste score een 0,90 (Br2) en de hoogste score een 1.69 (Br1) is.

Risicocommunicatie

Bij de vergelijking van risicopuntenscores ten tijde van de voormeting tussen de verschillende vormen van risicocommunicatie valt op dat de groep met geanticipeerde spijt de laagste gemiddelde risicoscore heeft in de voormeting (5,87), terwijl de coping-groep de hoogste score behaalt (6,62). De groep zonder risicocommunicatie scoort daar tussenin met een gemiddelde van 6,09. De verschillen tussen de groepen zijn echter relatief klein. Dit patroon is ook zichtbaar op itemniveau. De grootste verschillen tussen de vormen van risicocommunicatie komen naar voren bij twee items. Bij het item *'kan e-mail misbruikt worden'* scoorden zowel de groep zonder risicocommunicatie als de groep met geanticipeerde spijt 1,10, terwijl de groep met de coping-message 1,26 scoorde. Bij het item '*onderschepping websiteverkeer'* waren de scores 0,63 (geanticipeerde spijt), 0,73 (geen risicocommunicatie) en 0,88 (coping-message).

4.3.2 Beschrijvende statistiek nameting

In deze paragraaf worden de beschrijvende statistieken van de nameting besproken. Deze resultaten zijn weergegeven in Tabel 6 en Figuur 1.

Totale onderzoeksgroep/testgroep/controlegroep

In de nameting zijn vergelijkbare verschillen gevonden tussen de controlegroep die geen rapportage heeft ontvangen en de testgroep als bij de voormeting. Over alle respondenten genomen is de gemiddelde score 6,20. De testgroep scoort opnieuw lager (5,90), terwijl de controlegroep hoger scoort (7,12). Dit patroon is ook zichtbaar op itemniveau waarbij de controlegroep consequent hogere risicopunten behaalt dan de testgroep, met nogmaals uitzondering van de items *'gevoelige gegevens medewerkers openbaar'*, *'informatie configuratie website afgeschermd'* en *'manipulatie websiteverkeer mogelijk'*.

Organisaties

Ook tussen de organisaties blijven de onderlinge verschillen vergelijkbaar met die uit de voormeting. Br2 behaalt opnieuw een lagere gemiddelde score (4,50) dan de overige organisaties, waarvan de scores variëren tussen 6,34 (Ge3) en 7,94 (Ge2). Dit patroon is eveneens zichtbaar op itemniveau, Br2 scoort aanzienlijk lager op de items *'kan e-mail misbruikt worden'*, *'onderschepping websiteverkeer'*, *'ongebruikelijke aanvalspaden op website'* en *'manipulatie websiteverkeer mogelijk'*. De grootste onderlinge verschillen worden, net als bij de voormeting, gevonden bij de items *'onderschepping websiteverkeer'* en *'manipulatie websiteverkeer mogelijk'*.

Risicocommunicatie

Tot slot zijn ook bij de verschillende vormen van risicocommunicatie vergelijkbare patronen zichtbaar als bij de voormeting. De risicocommunicatie *geanticipeerde spijt* laat opnieuw de laagste risicopuntenscore zien (5,68), terwijl *coping* het hoogste scoort (6,35). De groep die geen risicocommunicatie ontving, bevindt zich daartussen met een gemiddelde score van 5,88. De verschillen tussen de groepen zijn echter relatief klein. Dit patroon is eveneens zichtbaar op

itemniveau, waarbij de grootste verschillen tussen de vormen van risicocommunicatie worden gevonden bij de items *'kan e-mail misbruikt worden'* en *'onderschepping websiteverkeer'*.

4.3.3 Verschil voor- en nameting

In deze paragraaf worden de verschillen tussen de voor- en nameting van de interventie besproken. Net als in de voorgaande paragrafen wordt gekeken naar de verschillen tussen de testgroep en controlegroep die geen rapportage heeft ontvangen, tussen de verschillende organisaties en tussen de vormen van risicocommunicatie. De resultaten zijn weergegeven in Tabel 6 en Figuur 1.

Totale onderzoeksgroep/testgroep/controlegroep

Zoals te zien is in Tabel 6, laat de totale populatie een verschil zien van -0,19 in de risicopuntenscore. Dit betekent dat de deelnemers in de nameting gemiddeld 0,19 risicopunten minder behaalden dan in de voormeting. Dit verschil is statistisch significant. De testgroep laat een grotere afname zien, met een verschil van -0,22, wat eveneens significant is. De controlegroep die geen rapportage heeft ontvangen, heeft een kleinere afname van -0,08, maar ook dit verschil is significant. Op itemniveau zijn deze significante verschillen grotendeels terug te zien. Voor de testgroep zijn de verschillen tussen voor- en nameting op vrijwel alle items significant, met uitzondering van *'verspreidt website malware'* en *'gevoelige gegevens medewerkers openbaar'*. Bij de controlegroep zijn de verschillen alleen significant op de items '*kan e-mail misbruikt worden'* en '*ongebruikelijke aanvalspaden op website*'. De grootste afname in risicopunten is zichtbaar bij de testgroep op de items *'kan e-mail misbruikt worden'* en *'onderschepping websiteverkeer'*, beide met een verschil van -0,06. De items *'verspreidt website malware'* en *'gevoelige gegevens medewerkers openbaar'* lijken niet door de interventie te zijn beïnvloed.

Organisaties

Bij de verschillende organisaties is het grootste verschil in de risicopuntenscore te zien bij organisatie Br1, met een verschilscore van -0,34. Alle organisaties laten een significant verschil zien tussen de voor- en nameting. Het kleinste verschil wordt gevonden bij Br2 (-0,13), wat zou kunnen worden verklaard doordat dit de organisatie is die in de voormeting al de laagste risicoscore behaalde. De overige organisaties, namelijk de gemeenten, variëren in hun verschilscore van -0,19 (Ge2) tot -0,29 (Ge3). Op itemniveau is te zien dat de grootste verschillen voorkomen bij de items *'kan e-mail misbruikt worden'* en *'onderschepping websiteverkeer'*, al verschilt dit per organisatie. Bij het eerste benoemde item is het verschil vooral groot bij Br1 en Ge1, beide met een verschil van -0,11, terwijl bij Ge2 geen significant verschil is gevonden. Bij *'onderschepping websiteverkeer'* zijn de grootste verschillen zichtbaar bij Br1, Ge2 en Ge3, terwijl Br2 en Ge1 hier geen significant verschil laten zien. Bij het item *'manipulatie websiteverkeer mogelijk'* is alleen bij de brancheorganisaties een significant verschil gevonden, niet bij de gemeenten. Voor *'voldoende bescherming bezoekers website'* geldt dat Ge3 en beide brancheorganisaties een significant verschil laten zien, terwijl Ge1 en Ge2 dat niet doen. Voor de overige items zijn de verschillen verwaarloosbaar.

Risicocommunicatie

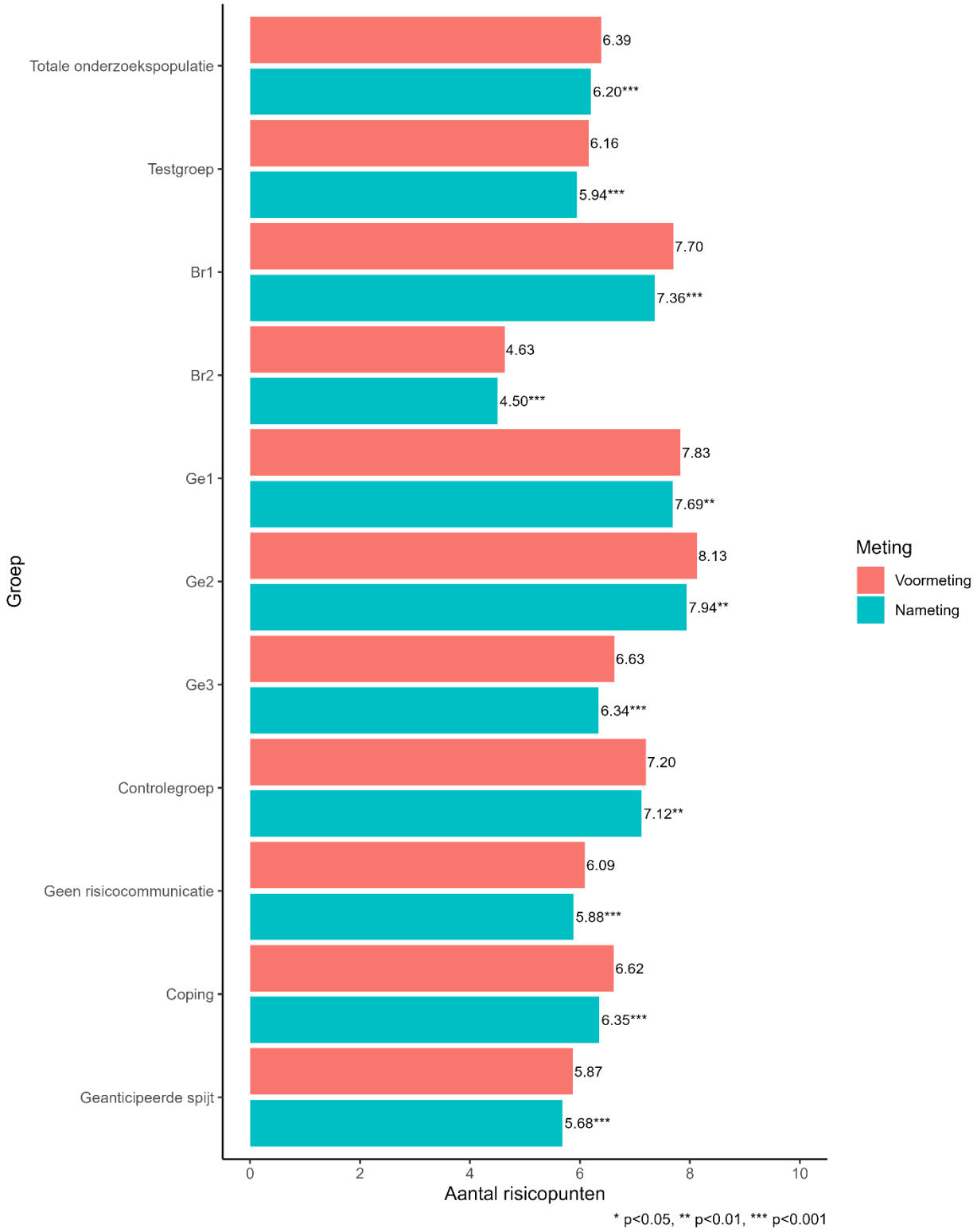
Bij de verschillende vormen van gebruikte risicocommunicatie binnen deze interventie laat de coping-message het grootste verschil zien, met een verschilscore van -0,27. De risicocommunicatie geanticipeerde spijt heeft een iets kleiner verschil dan de groep die geen risicocommunicatie ontving, namelijk -0,19 ten opzichte van -0,21. Alle gevonden verschillen tussen de voor- en nametingen zijn statistisch significant. Wanneer wordt gekeken naar de afzonderlijke items, zijn vergelijkbare bevindingen zichtbaar als in de voorgaande paragrafen. Zo zijn bij de items '*verspreidt website malware'* en *'gevoelige gegevens medewerkers openbaar'* geen of slechts kleine significante verschillen gevonden. Bij '*voldoende bescherming bezoekers website'* en '*informatie configuratie website afgeschermd'* waren de verschillen wel significant, maar klein. De meest interessante bevindingen doen zich voor bij de items '*kan e-mail misbruikt worden*', '*onderschepping websiteverkeer'*, '*voldoende bescherming bezoekers website'* en '*manipulatie websiteverkeer mogelijk'*. Vooral bij '*onderschepping websiteverkeer'* en '*manipulatie van websiteverkeer'* zijn de verschillen opvallend, omdat beide uitsluitend een significant verschil laten zien bij de respondenten die een risicocommunicatie ontvingen. De groep die geen risicocommunicatie ontving, liet geen significant verschil zien. Bij '*onderschepping websiteverkeer'* had de coping-message een verschilscore van -0,08 en geanticipeerde spijt een verschilscore van -0,05. Voor '*manipulatie websiteverkeer'* lagen de scores dicht bij elkaar: -0,03 voor coping en -0,04 voor geanticipeerde spijt. Bij '*kan e-mail misbruikt worden*' en '*voldoende bescherming bezoekers website'* zijn voor de twee vormen van risicocommunicatie en de groep die geen risicocommunicatie ontving kleine significante verschillen gevonden.

Tabel 6. *Beschrijving van gevonden risicopunten (per kwetsbaarheid en totaal) voor testgroep en controlegroep, in de voor- en nameting, met vergelijking tussen organisaties en risicocommunicatie*

			Totaal risicopuntenscore			**Verspreidt website malware**			**Gevoelige gegevens medewerkers openbaar**			**Kan e-mail misbruikt worden**			**Onderschepping websiteverkeer**			**Ongebruikelijke aanvalspaden op website**			**Voldoende bescherming bezoekers website**			**Informatie configuratie website afgeschermd**			**Manipulatie websiteverkeer mogelijk**		
Groep		*N*	*Voor*	*Na*	*Verschil*	*Voor*	*Na*	*Verschil*	*Voor*	*Na*	*Verschil*	*Voor*	*Na*	*Verschil*	*Voor*	*Na*	*Verschil*	*Voor*	*Na*	*Verschil*	*Voor*	*Na*	*Verschil*	*Voor*	*Na*	*Verschil*	*Voor*	*Na*	*Verschil*
Minimaal - maximaal			0-12.25			0-3			0-1			0-2			0-3			0-1			0-2			0-1			0-2		
Totale onderzoekspopulatie (testgroep en controlegroep)		2646	6.39	6.20	-0.19***	0.21	0.21	0	0.10	0.10	0	1.18	1.13	-0.05***	0.91	0.86	-0.05***	0.56	0.54	-0.02***	1.64	1.61	-0.03***	0.57	0.56	-0.01***	1.22	1.19	-0.03***
Testgroep	*Totaal*	2056	6.16	5.94	-0.22***	0.20	0.20	0	0.11	0.12	0.01	1.15	1.09	-0.06***	0.74	0.68	-0.06***	0.54	0.53	-0.01***	1.61	1.56	-0.05***	0.58	0.56	-0.02***	1.24	1.21	-0.03***
	Br1	550	7.70	7.36	-0.34***	0.25	02.25	0	0.10	0.10	0	1.57	1.46	-0.11***	1.04	0.94	-0.10***	0.71	0.70	-0.01	1.74	1.67	-0.07***	0.59	0.58	-0.01**	1.69	1.65	0-.04*
	Br2	959	4.63	4.50	-0.13***	0.15	0.15	0	0.12	0.12	0	0.77	0.74	-0.03**	0.30	0.29	-0.01	0.40	0.39	-0.01**	1.44	1.40	-0.04***	0.55	0.53	-0.02***	0.90	0.88	-0.02**
	Ge1	139	7.83	7.69	-0.24**	0.24	0.24	0	0.12	0.13	0.01	1.58	1.47	-0.11**	1.28	1.23	-0.05	0.64	0.63	-0.01	1.76	1.74	-0.02	0.62	0.61	0	1.60	1.55	-0.05
	Ge2	131	8.13	7.94	-0.19**	0.22	0.23	0.01	0.09	0.09	0	1.54	1.53	-0.01	1.66	1.54	-0.12**	0.68	0.66	-0.02	1.85	1.84	-0.01	0.60	0.59	0	1.48	1.47	-0.01
	Ge3	277	6.63	6.34	-0.29***	0.24	0.24	0	0.13	0.14	0.01**	1.21	1.16	-0.05**	0.95	0.86	-0,09**	0.57	0.55	-0.02	1.74	1.66	-0.08***	0.60	0.58	-0.02*	1.20	1.16	-0.04
Controlegroep		590	7.20	7.12	-0.08**	0.25	0.25	0	0.04	0.04	0	1.28	1.26	-0.02*	1.51	1.49	-0.02	0.61	0.60	-0.01***	1.7	1.77	0	0.57	0.57	0	1.16	1.14	-0.02
Risicocommunicatie	*Geen risicocommunicatie*	669	6.09	5.88	-0.21***	0.19	0.19	0	0.11	0.11	0	1.10	1.04	-0.06***	0.73	0.70	-0.03	0.55	0.53	-0.02***	1.60	1.54	-0.06***	0.57	0.50	0.02***	1.24	1.22	-0.02
	Coping	596	6.62	6.35	-0.27***	0.23	0.24	0.01	0.11	0.12	0.01*	1.26	1.18	-0.08***	0.88	0.80	-0.08***	0.58	0.57	-0.01	1.68	1.62	-0.06***	0.59	0.57	-0.02***	1.29	1.26	-0.03**
	Geanticipeerde spijt	791	5.87	5.68	-0.19***	0.19	0.19	0	0.12	0.12	0	1.10	1.06	-0.04**	0.63	0.58	-0.05***	0.50	0.49	-0.01**	1.57	1.54	-0.03***	0.57	0.56	-0.01*	1.19	1.15	-0.04***

*p<0.05, **p<0.01, ***p<0.001

Figuur 1. *Visualisering van gevonden risicopunten (per kwetsbaarheid en totaal) voor testgroep en controlegroep, in de voor- en nameting, met vergelijking tussen organisaties en risicocommunicatie*



Vervolgens hebben we gekeken in hoeverre het effect van de interventie verschilde tussen de diverse groepen. Tabel 7 toont aan dat het verschil tussen de testgroep en de controlegroep die geen rapportage heeft ontvangen significant is. Dit betekent dat de testgroep een significant grotere verbetering laat zien dan de controlegroep. Daarnaast is onderzocht of de organisaties en de vormen van risicocommunicatie significant verschillen van de controlegroep. Tabel 7 laat zien dat dit het geval is voor de organisaties Br1, Ge1 en Ge3. Dit betekent dat deze drie groepen een grotere toename in cyberweerbaarheid (oftewel sterkere afname in risicopuntenscore) dan de controlegroep. Ook scoren geen risicocommunicatie, de coping-message en geanticipeerde spijt significant beter dan de controlegroep, waarbij het sterkste significantieniveau is gevonden bij de coping-message.

Tussen de organisaties onderling is een significant verschil gevonden tussen de brancheorganisaties Br1 en Br2. Daarnaast zijn er significante verschillen tussen Br1 en Ge2 en tussen Br2 en Ge3. De overige combinaties tussen de organisaties laten geen significante verschillen zien.

Wat betreft de risicocommunicatie zijn alleen significante verschillen gevonden ten opzichte van de controlegroep die geen rapportage heeft ontvangen en niet tussen de verschillende vormen van risicocommunicatie onderling. Dit betekent dat het effect van de interventie niet verschilde tussen de verschillende vormen van risicocommunicatie.

Tabel 7. *Kruistabel met vergelijking van het effect van de interventie tussen de testgroep en controlegroep, de organisaties en de verschillende vormen van risicocommunicatie*

	Testgroep	**Controlegroep**	**Br1**	**Br2**	**Ge1**	**Ge2**	**Ge3**	**Geen risico-communicatie**	**Coping**	**Geanticipeerde spijt**
Testgroep	X	***	X	X	X	X	X	X	X	X
Controlegroep	***	X	***	NS	*	NS	***	**	***	**
Br1	X	***	X	***	NS	*	NS	X	X	X
Br2	X	NS	***	X	NS	NS	*	X	X	X
Ge1	X	*	NS	NS	X	NS	NS	X	X	X
Ge2	X	NS	*	NS	NS	X	NS	X	X	X
Ge3	X	***	NS	*	NS	NS	X	X	X	X
Geen risicocommunciatie	X	**	X	X	X	X	X	X	NS	NS
Coping	X	***	X	X	X	X	X	NS	X	NS
Geanticipeerde spijt	X	**	X	X	X	X	X	NS	NS	X

****<p.001 <**0.01 *<0.05*

NS = Niet significant

5. Conclusie en discussie

5.1 Conclusie

Het bovenliggende doel van het huidige onderzoek is het versterken van de cyberweerbaarheid van mkb-ondernemingen door middel van een wetenschappelijk onderbouwde gedragsinterventie. In dit onderzoek is gebruikgemaakt van een geautomatiseerde cybersecurity meting gebaseerd op open-sourcedata over kwetsbaarheden. Ondernemers ontvingen een op-maat gemaakt adviesrapport met een concreet handelingsperspectief.

Dit onderzoek bouwt voort op het pilotproject *"What(s)can we do? Onderzoek naar het gebruik van een geautomatiseerde kwetsbaarhedenmeting als evidence-based gedragsinterventie"* (Van 't Hoff-de Goede et al., 2024). In dit pilotproject is onderzocht in hoeverre een geautomatiseerde kwetsbaarhedenmeting mogelijk, juridisch toegestaan en effectief ingezet kan worden ter versterking van de cyberweerbaarheid van ondernemers. De bevindingen lieten zien dat er geen juridische belemmeringen waren en dat de eerste resultaten wezen op een veelbelovende en potentieel effectieve interventie.

In het huidige onderzoek is de interventie van Van 't-Hoff-de Goede et al. (2024) doorontwikkeld en geëvalueerd. Het onderzoek bestond uit drie fasen. In fase 1 is de interventie op kleine schaal inhoudelijk getest om de ervaringen en beoordelingen van ondernemers te onderzoeken. In fase 2 is de interventie doorontwikkeld, onder meer op basis van de inzichten uit fase 1. In fase 3 is de interventie grootschalig geïmplementeerd en geëvalueerd, met als doel de impact van de interventie op de cyberweerbaarheid van ondernemingen te toetsen.

In de volgende paragrafen worden de conclusies van deze drie fasen besproken, evenals de belangrijkste beperkingen en aanbevelingen.

5.1.1 Conclusie fase 1

De centrale onderzoeksvraag in fase 1 luidde: *"Op welke wijze kan de geautomatiseerde, evidence-based gedragsinterventie ter stimulering van ondernemers om drie basismaatregelen voor cybersecurity te implementeren, worden geoptimaliseerd?"* In deze fase is de interventie getest bij 150 bedrijven op een bedrijventerrein in Noord-Nederland, geselecteerd in overleg met PVO Noord-Nederland. De deelnemende bedrijven waren afkomstig uit diverse branches. Grote ketens zijn uitgesloten, aangezien deze doorgaans beschikken over geavanceerdere cybersecuritymaatregelen of landelijk georganiseerde beveiligingsprocessen. Van de 150 bedrijven ontvingen 75 ondernemers een vooraankondigingsbrief, waarin de meting werd toegelicht en een mogelijkheid tot opt-out werd geboden. Vier ondernemers maakten gebruik van deze opt-out. Vervolgens is de meting uitgevoerd op alle overige bedrijven en ontvingen zij een adviesrapport met handelingsperspectief. Vervolgens bezochten onderzoekers alle bedrijven en gebruikten daarbij een checklist met algemene vragen over de ervaringen met de interventie. Bij 140 bedrijven is geprobeerd de checklist af te nemen, dit lukte uiteindelijk bij 30 bedrijven. Het invullen van de checklist was niet mogelijk wanneer ondernemers geen tijd of behoefte hadden, wanneer het bedrijf gesloten was (bijvoorbeeld door vakantie of verbouwing), wanneer het rapport volgens de ondernemer niet bekend was, of wanneer de juiste contactpersoon niet aanwezig was. Daarnaast zijn bij een deel van de bedrijven korte interviews afgenomen om te

onderzoeken hoe de interventie is ontvangen, welke beweegredenen ondernemers hadden om de rapportage (i) wel of niet te openen, (ii) wel of niet te lezen en (iii) wel of niet over te gaan tot het nemen van maatregelen. De interviewdeelnemers zijn geworven tijdens de bedrijfsbezoeken. In totaal zijn zeven interviews afgenomen.

Het doel van fase 1 was om inzicht te krijgen in de reacties van ondernemers op de vooraankondiging, de redenen voor deelname, het bereik van de brief en rapportage, de beweegredenen voor het openen en lezen van het rapport, de overwegingen om al dan niet maatregelen te nemen, en de algemene beoordeling van de interventie.

Uit de ingevulde checklists en de afgenomen interviews kwamen verschillende inzichten naar voren. Ten eerste bleek dat de meeste ondernemers de vooraankondiging ontvingen, openden en lazen. Belangrijke drijfveren hiervoor waren nieuwsgierigheid en de erkenning dat cybersecurity een relevant thema is. Over het algemeen werd de vooraankondiging neutraal tot positief beoordeeld. Een enkeling ervaarde de brief als dwingend. Het poststuk bereikte bovendien meestal de juiste contactpersoon binnen de organisatie. Hoewel de gebruikte logo's voor de meeste ondernemers weinig invloed hadden, werd het logo van NHL Stenden Hogeschool in sommige gevallen als betrouwbaar ervaren, vanwege de regionale bekendheid van de instelling.

De rapportage werd doorgaans geopend uit interesse en nieuwsgierigheid. Tegelijkertijd bleek dat de technische inhoud voor vooral kleinere ondernemers soms lastig te begrijpen was. Een deel van de ondernemers ondernam direct actie naar aanleiding van de rapportage, terwijl anderen aangaven de intentie te hebben om op een later moment maatregelen te treffen. Ook was er een groep ondernemers die geen maatregelen nam, veelal vanwege een lage ervaren urgentie of omdat cybersecurity zou zijn uitbesteed aan een externe partij. Over het algemeen gaven ondernemers wel aan dat zij voornemens hadden om contact op te nemen met hun systeembeheerder of ICT-dienstverlener.

De begeleidende brief bij de rapportage droeg in sommige gevallen bij aan een gevoel van urgentie, terwijl andere ondernemers aangaven dat cybersecurity al aandacht had binnen het bedrijf, waardoor de brief weinig extra invloed had. De percepties van de invloed van de brief en de rapportage op hun bewustzijn van cyberweerbaarheid waren verdeeld: sommige ondernemers ervaarden een toename in bewustwording, terwijl anderen aangaven zelf weinig noodzaak te voelen omdat alle digitale veiligheidszaken zouden zijn uitbesteed.

De interventie werd over het algemeen positief beoordeeld. Tegelijkertijd kwamen enkele aandachtspunten naar voren. Ondernemers gaven aan behoefte te hebben aan betere leesbaarheid, concretere voorbeelden en een betere toegankelijkheid voor kleinere bedrijven. Daarnaast leefde bij sommige ondernemers de indruk dat de interventie mogelijk kon worden gezien als een vorm van oplichting of dat een commerciële partij hierbij belang zou kunnen hebben. Ook werd aangegeven dat een voorafgaande aankondigingsbrief wenselijk zou zijn om de legitimiteit van de interventie te versterken.

Een belangrijke conclusie uit deze fase is dat de interventie een waardevol instrument blijkt om de kennis en bewustwording rondom cybersecurity bij ondernemers te vergroten, vooral bij ondernemers voor wie het thema nog geen hoge prioriteit heeft. Ook werden mogelijke verbeteringen aangemerkt.

5.1.2 Conclusie fase 2

In fase 2 is de interventie op verschillende manieren aangepast en doorontwikkeld op basis van zowel de inzichten uit fase 1, de eerdere pilot en aanbevelingen van professionals. Deze worden hieronder puntsgewijs toegelicht. De centrale vraag in deze fase luidde: *"Hoe kan de interventie, op basis van de inzichten uit de pilot en fase 1, verder worden doorontwikkeld?"* De doorontwikkelingen zijn verdeeld in (1) aanpassingen aan de interventie en (2) aanpassingen aan het onderzoeksproject.

De manieren waarop de interventie is doorontwikkeld worden kort uiteengezet:

- **Logo's aangepast voor herkenbaarheid en legitimiteit.**
  De logo's zijn aangepast vanwege de samenwerking met nieuwe partners. Zo zijn de logo's van NHL Stenden Hogeschool, De Haagse Hogeschool en ThreadStone weergegeven. Daarnaast is ook het logo van de gemeente/brancheorganisatie waartoe de ondernemer behoort opgenomen.
- **Voorafgaande brief met opt-out toegevoegd om het ongevraagde karakter tegen te gaan.**
  Op basis van de aanbevelingen van verschillende professionals is besloten een vooraankondiging met opt-outmogelijkheid toe te voegen aan de interventie. Deze aanbeveling is in fase 1 getest om te beoordelen hoe ondernemers hierop reageerden, met een overwegend neutraal tot positief resultaat. In de vooraankondiging werd duidelijk uitgelegd wanneer de meting zou plaatsvinden, door wie deze werd uitgevoerd, waarom deze plaatsvond en welke vervolgstappen mogelijk waren. Ondernemers die tot een gemeente behoorden, kregen expliciet de opt-outmogelijkheid vermeld, terwijl ondernemers die tot een brancheverenigingbehoorden niet expliciet een opt-out werd aangeboden maar contactgegevens werden geboden om bij vragen een e-mail te sturen.
- **Contactgegevens toegevoegd om communicatie te vergemakkelijken.**
  Er is een apart e-mailadres aangemaakt waar ondernemers met vragen terecht konden, om de communicatie te vergemakkelijken.
- **Risicocommunicatie verbeterd met coping-message en geanticipeerde spijt**.
  De risicocommunicatie met geanticipeerde spijt is toegepast, omdat uit de pilot bleek dat de groep die deze vorm van communicatie ontving de grootste verbetering in digitale veiligheid liet zien. De geanticipeerde spijt-communicatie luidde: "*Voorkomen is goedkoper dan genezen! Werk nu aan uw cyberweerbaarheid om latere kosten te voorkomen*." Daarnaast is een nieuwe vorm van risicocommunicatie toegevoegd, namelijk een coping-message gebaseerd op de Protection Motivation Theory. Uit de literatuur bleek dat dit effectief kan zijn om mensen te motiveren maatregelen te nemen. De inhoud van de coping-message luidde: "*Maak uw bedrijf weerbaar tegen cybercriminaliteit. Dit rapport laat zien waar uw bedrijf kwetsbaar is voor online aanvallen. Bespreek deze punten met uw IT-leverancier om eenvoudige maatregelen te nemen en uw bedrijf te beschermen tegen online gevaren*." Een derde groep ondernemers ontving geen risicocommunicatie, zodat de effecten van beide vormen van risicocommunicatie vergeleken konden worden.
- **Duidelijker vermeld dat het geen commercieel project is.**

In fase 1 gaven enkele ondernemers aan dat zij de interventie associeerden met een commerciële ondertoon. In de begeleidende brief wordt nu expliciet vermeld dat de meting geen commercieel doel heeft en kosteloos wordt aangeboden.

- **Taalgebruik vereenvoudigd naar B1-niveau**.
  In fase 1 kwam naar voren dat het taalgebruik van de interventie soms te technisch was. Daarom zijn de brieven en de rapportage aangepast naar B1-niveau, zoals aanbevolen door de Rijksoverheid, om de begrijpelijkheid voor ondernemers te vergroten.
- **Doorontwikkeling handelingsperspectief.**
  Het handelingsperspectief is aangepast van scenario's naar twee stappen. Stap 1 richt zich op het aanpakken van de gevonden kwetsbaarheden en maakt onderscheid tussen ondernemers met en zonder IT-leverancier. Ondernemers zonder leverancier worden verwezen naar de adviezen van het Digital Trust Center (DTC) voor het vinden van een geschikte partij, terwijl ondernemers met een leverancier worden doorverwezen naar de DTC-richtlijnen om het gesprek met hun leverancier over kwetsbaarheden te voeren. Stap 2 benadrukt dat cybersecurity verder reikt dan de aspecten die in de rapportage zijn gemeten, en verwijst ondernemers naar de DTC-website met informatie over de vijf basisprincipes van cybersecurity.

Voor het onderzoeksproject zijn de volgende doorontwikkelingen gedaan:

- **Checklist ontwikkeld om ontvangst en gebruik van rapportages te meten.**
  In de pilot ontbrak informatie over het daadwerkelijke ontvangst en bereik van de brief en de rapportage. In fase 1 is dit inzicht verkregen door gebruik te maken van een checklist, die tijdens bezoeken aan de ondernemers is doorlopen. Daarnaast zijn er verdiepende interviews afgenomen om inzicht te krijgen in de mening van ondernemers over de interventie.
- **Kwaliteit steekproef verhoogd.**
  In de pilot ontbrak informatie over de demografische kenmerken van de bedrijven, waardoor representativiteit niet kon worden vastgesteld. Het huidige onderzoek bevat branchegegevens die kunnen worden vergeleken met gemeenten. Daarnaast is de steekproef groter, waardoor de resultaten een betere afspiegeling vormen van Nederlandse ondernemingen.

5.1.3 Conclusie fase 3

De hoofdvraag van fase 3 luidde: *"Wat is het effect van de interventie op de cyberweerbaarheid van ondernemers?"* De geautomatiseerde kwetsbaarhedenmeting is uitgevoerd in opdracht van drie gemeenten en twee brancheorganisaties. De ondernemers ontvingen een vooraankondiging en vervolgens een op maat gemaakte rapportage, bestaande uit een begeleidende brief en een adviesrapport. Het rapport geeft een overzicht van de gevonden kwetsbaarheden en biedt praktische adviezen om deze aan te pakken, evenals een handelingsperspectief om de cyberweerbaarheid structureel te versterken.

Voor de interventie werden elf items gemeten. De gemeten items waren: *verspreidt uw website geen malware, verspreidt uw website geen spam, verspreidt uw mailserver geen spam, zijn gevoelige gegevens van uw medewerkers niet openbaar, kan uw e-mail niet misbruikt worden, kan het verkeer met uw website niet worden onderschept, zijn er geen ongebruikelijke*

aanvalspaden op uw website mogelijk, worden bezoekers van uw website voldoende beschermd, is informatie over de configuratie van uw website afgeschermd, kan websiteverkeer naar uw website niet gemanipuleerd worden, en is uw website, mailserver en nameserver gereed voor nieuwe standaarden.

Van deze elf items zijn acht meegenomen in de analyses. De items *verspreidt uw website geen spam*, *verspreidt uw mailserver geen spam* en *is uw website, mailserver en nameserver gereed voor nieuwe standaarden* zijn uitgesloten. De eerste twee van deze items werden uitgesloten vanwege problemen met foutieve scores (paragraaf 5.2), en het derde item vanwege nieuwe standaarden die nog niet breed zijn toegepast. Voor elk van de acht items werd vastgesteld in welke mate er een risico is gevonden en werden risicopunten toegekend. Het totaal van deze risicopunten is de "risicopuntenscore".

De rapportage bevat een tabel met de belangrijkste aandachtspunten, mogelijke gevolgen van de gevonden cybersecurityrisico's en een toelichting met concreet advies per punt. In de begeleidende brief ontvingen sommige ondernemers risicocommunicatie in de vorm van geanticipeerde spijt, anderen een coping-message en een derde groep kreeg geen risicocommunicatie.

De analyses toonden aan dat de risicoscores bij de nameting over het algemeen waren gedaald vergeleken bij de voormeting, waarbij de daling in de testgroep significant groter was dan in de controlegroep die geen rapportage had ontvangen. Het betreft een kleine maar significante daling van gemiddeld 0,22 risicopunten in de testgroep, vergeleken bij 0,08 risicopunten in de controlegroep. Alle organisaties lieten een significante verbetering in risicopuntenscore zien tussen de voor- en nameting. Het grootste effect werd gevonden bij Br1, terwijl Br2 de kleinste afname liet zien, wat samenhangt met de reeds lage scores bij de voormeting van deze groep. De gemeenten lieten middelgrote afnames zien, waarbij Ge3 de grootste verbetering liet zien en Ge2 de kleinste. De organisaties Br1, Ge1 en Ge3 lieten een significant grotere afname in risicopuntenscore zien dan de controlegroep die geen rapportage had ontvangen.

De interventie leek verder met name effect te hebben op specifieke items die direct door gedrag beïnvloed kunnen worden, het zogenaamde 'laaghangend fruit'. Risicopunten zoals "*kan e-mail misbruikt worden*" en "*onderschepping websiteverkeer*" lieten na de interventie duidelijke verbeteringen zien. Dit is verklaarbaar doordat ondernemers voor deze risico's zelf relatief eenvoudig maatregelen kunnen nemen, zoals het instellen van sterke wachtwoorden, het gebruik van twee-factor-authenticatie of het aanpassen van e-mailinstellingen. Andere risicopunten, zoals "*verspreiding van malware via de website*" of "o*penbaar staan van gevoelige gegevens*", lieten nauwelijks verandering zien. Deze risico's zijn vaak structureel of technisch van aard en kunnen niet eenvoudig door gedragsverandering worden verminderd.

Bij de verschillende vormen van risicocommunicatie, zowel bij coping-message als geanticipeerde spijt, werd een afname in risicoscores waargenomen, waarbij de coping-message de grootste effecten liet zien. De verschillen tussen de verschillende vormen van risicocommunicatie waren echter niet significant. De effectiviteit van de interventie lijkt daarmee niet samen te hangen met de toegepaste risicocommunicatie.

Concluderend kan gezegd worden dat de interventie de cyberweerbaarheid van ondernemers in kleine mate maar wel significant verhoogt. De effectgrootte varieert tussen items en organisaties. Voor de praktijk betekent dit dat dit onderzoeksproject een interventie heeft opgeleverd die laagdrempelig op grote schaal kan worden ingezet en opzichzelfstaand een kleine significante verbetering in cyberweerbaarheid bewerkstelligt. De interventie is daarmee een

zinvolle eerste stap waarmee een groot aantal ondernemers kan worden bereikt zonder dat zij zich actief hoeven aan te melden voor de interventie. De interventie ziet echter toe op een klein deel van de cyberweerbaarheid van ondernemingen en volstaat niet om een substantieel cyberweerbaarheidsniveau te bereiken. Bovendien is het van belang te benadrukken dat een kleine verbetering niet mag leiden tot schijnveiligheid bij ondernemers; voortdurende aandacht en aanvullende maatregelen blijven noodzakelijk om digitale risico's effectief te beheersen. Beleidsmakers en brancheorganisaties zouden daarom moeten inzetten op een combinatie van herhaling en aanvullende, verdiepende interventies om het effect te versterken (zie paragraaf 5.3).

Wetenschappelijk gezien bevestigt dit onderzoek dat cyberweerbaarheid beïnvloedbaar is, wat theoretische modellen over gedragsverandering en risicoperceptie ondersteunt. Tegelijkertijd vraagt de beperkte effectgrootte om vervolgonderzoek naar welke elementen van de interventie het meest bijdragen en hoe deze kunnen worden geoptimaliseerd. De toevoeging van risicocommunicatie heeft in dit onderzoek geen significante bijdrage geleverd aan de effectiviteit van de interventie. Vervolgonderzoek is nodig naar een mogelijk effect van andere vormen van risicocommunicatie.

5.2 Beperkingen

Het onderzoek kent enkele beperkingen. In fase 1 was de respons laag, wat de representativiteit kan beïnvloeden. Het tijdstip van dataverzameling, vlak voor de zomerperiode, kan hierbij van invloed zijn geweest, omdat sommige bedrijven gesloten waren of met een beperkte bezetting werkten. De respons is uiteindelijk licht verhoogd omdat is besloten dezelfde bedrijven een tweede keer te bezoeken. Ondanks deze beperkingen heeft fase 1 belangrijke aanknopingspunten opgeleverd voor de doorontwikkeling van de interventie.

Daarnaast brengen de gebruikte onderzoeksmethoden enkele beperkingen met zich mee. De meting biedt slechts een gedeeltelijk beeld van de cyberweerbaarheid van ondernemingen, omdat uitsluitend gebruik is gemaakt van openbaar beschikbare informatie. Hierdoor kan het voorkomen dat een ondernemer een rapport ontvangt waarin alle gecontroleerde onderdelen goed scoren, wat onterecht de indruk kan wekken dat verdere actie niet noodzakelijk is. Om dit risico te beperken, is in de begeleidende brief expliciet vermeld dat de controle op openbare kwetsbaarheden een waardevolle eerste stap is, maar geen volledige beveiligingscontrole van de website, e-mailserver of cybersecurity van de onderneming vormt. Op de laatste pagina van het rapport is bovendien een handelingsperspectief opgenomen, met praktische adviezen en verwijzingen. Hier kunnen ondernemers aanvullende informatie en concrete vervolgstappen vinden om hun cyberweerbaarheid verder te verbeteren. Het gebruik van één meetmoment maakt het echter lastig om inzicht te krijgen in het proces van implementatie en de redenen waarom bepaalde maatregelen wel of niet zijn uitgevoerd. Externe factoren, zoals drukke periodes of economische omstandigheden, kunnen eveneens de uitkomst beïnvloeden, los van de kwaliteit van de aangedragen oplossingen. Ondanks deze beperkingen levert de meting een bruikbaar startpunt op om ondernemers bewust te maken van digitale risico's en hen te stimuleren tot vervolgstappen.

Een belangrijke beperking van dit onderzoek tot slot is dat een deel van de ondernemers moet worden uitgesloten van de effectmeting vanwege foutieve scores op twee van de tien items.

Deze items hadden betrekking op de vraag of de website of mailserver van de respondent spam verspreidde. Ten onrechte kreeg een substantieel deel van de ondernemers risicopunten toegekend op deze twee items. Omdat dit de effectiviteit van de interventie binnen deze groep heeft kunnen beïnvloeden, zijn alle ondernemers die een onjuiste score hadden ontvangen uit de dataset verwijderd. Ondanks deze beperking bleef de uiteindelijke onderzoekspopulatie voldoende groot om betrouwbare analyses uit te voeren en conclusies te formuleren.

5.3 Aanbevelingen

Op basis van het huidige onderzoek worden enkele aanbevelingen gedaan voor de verdere doorontwikkeling en implementatie van de interventie.

Betrokkenheid van IT-beheerders en onderwijs

Uit fase 1 van het onderzoek bleek dat veel ondernemers de rapportage van de kwetsbaarhedenmeting doorgaven aan hun IT-beheerders, omdat zij de verantwoordelijkheid voor cybersecurity zouden hebben uitbesteed. Dit roept de vraag op in hoeverre de effectiviteit van de interventie afhankelijk is van de betrokkenheid van deze IT-beheerders. Voor de verdere ontwikkeling van de interventie is het wenselijk om de rol van IT-beheerders beter te begrijpen en IT-beheerders te includeren in de interventie. Toekomstig onderzoek kan zich richten op hoe IT-beheerders de adviezen uit de rapportage interpreteren en welke factoren hun besluitvorming beïnvloeden om al dan niet actie te ondernemen. Samenwerking met brancheorganisaties binnen de IT-sector kan helpen om de betrokkenheid van IT-beheerders te vergroten en de effectiviteit van de interventie te waarborgen.

Hiernaast zouden studenten van een ICT of soortgelijke opleiding kunnen worden ingezet bij het helpen van ondernemers bij het werken aan hun cyberweerbaarheid en het navolgen van de adviezen in de rapportage. Ook zouden deze studenten de cyberweerbaarheid van de onderneming aanvullend kunnen analyseren (zie ook hieronder). Zo kan worden gedacht aan het koppelen van studenten en ondernemers in een buddy-project (zie bijvoorbeeld Van ’t Hoff-De Goede et al., 2022).

De borging van de interventie

Het is belangrijk dat de interventie wordt geborgd. Hiervoor is de betrokkenheid nodig van een organisatie die in staat is om de interventie landelijk uit te rollen. Dit wordt momenteel al verkend door het CCV, het ministerie van Justitie en Veiligheid en PVO. In deze borging zou bovendien samenwerking kunnen worden aangegaan met brancheorganisaties en gemeenten, of andere overkoepelende partijen. Ook is het denkbaar dat de meting wordt opgenomen in integrale controles en projecten die zich veelal richten op veiligheid, maar nog niet altijd op cyberweerbaarheid.

Wanneer deze landelijke implementatie wordt gerealiseerd, kan de interventie ook gekoppeld worden aan andere interventies. Er kan bijvoorbeeld in de rapportage verwezen worden naar andere landelijke en lokale projecten. Het volgende punt over doorontwikkeling gaat verder in op deze mogelijke projecten waar naar verwezen kan worden.

Opstap naar verdere initiatieven

Deze interventie richt zich op een klein deel van de cybersecurity van ondernemers, omdat alleen de openbare informatie van de digitale infrastructuur van ondernemers wordt gemeten. De interventie biedt opzichzelfstaand al een klein effect, maar kan hier bovenop ondernemers aanmoedigen om verder te gaan met het verbeteren van hun cybersecurity. Hiertoe zou in de communicatie kunnen worden verwezen naar andere projecten, die tegen lage kosten voor aanmelding beschikbaar kan worden gesteld. Een eerste voorbeeld is om ondernemers aan te moedigen om naast de 'buitenkant' van de onderneming ook de 'binnenkant' van de onderneming te (laten) analyseren, bij voorkeur over langere tijd om inzicht te krijgen in real-time dreigingen en weerbaarheid. Dit kan worden bewerkstelligd door aanvullende interventies, bijvoorbeeld met de inzet van studenten. Een dergelijke aanpak is overigens wel intensiever en minder schaalbaar. Daarnaast kan gewezen worden op actuele lokale projecten of projecten uit de "cybersnackbox" van het CCV om ondernemers op een laagdrempelige manier aan te spreken.

Deze initiatieven kunnen ervoor zorgen dat de toename van cyberweerbaarheid niet stopt na de geautomatiseerde cyberweerbaarheidsinterventie, maar dat deze interventie als opzet dient voor een bredere benadering van cyberweerbaarheid, waardoor ondernemers een dieper inzicht krijgen in hun cybersecurity en gestimuleerd worden om vervolgstappen te nemen.

Literatuurlijst

Arends, J., Derksen, E., & Morren, M. (2025). Online veiligheid en criminaliteit 2024. In *CBS*. Centraal Bureau voor Statistiek.

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & De Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Bekkers, L., Van 't Hoff-De Goede, S., Huurne, E. M., Van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, *127*, 103099. https://doi.org/10.1016/j.cose.2023.103099

Bluhm, K., Andriessen, M., Wal, M. van der, Berkenpas, M., Boer, D. de, Leukfeldt, R., Spithoven, R. & Jansen, J. (2024). *Een eerste blik op het verloop en de werking van cyberweerbaarheidsprojecten in Nederland: Procesevaluaties van CCV City Deal projecten*. NHL Stenden Hogeschool.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly, 39(4), 837–864.

Centraal Bureau voor Statistiek. (2024). Cybersecurity Monitor 2023. In *CBS*.

Conner, M., Conner, M., Sandberg, T., McMillan, B., & Higgins, A. (2006). Role of anticipated regret, intentions and intention stability in adolescent smoking initiation. *British journal of health psychology, 11*(1), 85-101

Cybersecuritybeeld Nederland 2024 voor ondernemers. (2024, 28 oktober). Digital Trust Center (Min. Van EZ). Geraadpleegd op 16 januari 2025, van https://www.digitaltrustcenter.nl/nieuws/cybersecuritybeeld-nederland-2024-voor-ondernemers#:~:text=Voornaamste%20dreigingen%20voor%20ondernemers%20in%202024&text=Hierbij%20dreigen%20criminelen%20steeds%20vaker,criminelen%20hun%20slag%20konden%20slaan.

Digital Trust Center (DTC). (z.d.). De 5 basisprincipes van veilig digitaal ondernemen. Digital Trust Center. https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

Digital Trust Center (DTC). (z.d.). Doe de Basisscan Cyberweerbaarheid. Digital Trust Center. https://www.digitaltrustcenter.nl/tools/doe-de-basisscan-cyberweerbaarheid

Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, *22*(4), 849–868. https://doi.org/10.1111/1745-9133.12641

ENISA (2020). *Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected*. *European Union Agency For Cybersecurity*. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends.

Filiz-Ozbay, E., & Ozbay, E. Y. (2007). Auctions with anticipated regret: Theory and experiment. *American Economic Review, 97*(4), 1407-1418.

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet Of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Hoekstra, M., De Vries, S., Berkenpas, M., & Jansen, J. (2021). *De werking van de basisscan Cyberweerbaarheid: Een kwalitatief onderzoek naar het gedrag van ondernemers*.

Hof, T., Van Der Kleij, R., & Mergler, S. (2024). Veilig digitaal ondernemen: Inzicht in motivaties en barrières door doelgroepsegmentatie. In *Digitaal Trust Center*. TNO Publiek.

Hoffmann, P., de Leede, J., & Van Staveren, M. T. (2024). *Nationale Monitor Risicomanagement MKB*. https://www.averoachmea.nl/kennis/risicomanagement/rapport-nationale-monitor-risicomanagement-mkb-2024

Huurne, E.F.J. ter, & Gutteling, J.M. (2008). Information needs and risk perception as predictors of risk information seeking. *Journal of Risk Research, 11*(7), 847-862.

Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience*. Open Universiteit

Jansen, J. & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human - Computer Studies, 123*, 40-55.

Jones, K. S., Lodinger, N. R., Widlus, B. P., Namin, A. S., & Hewett, R. (2021). Do Warning Message Design Recommendations Address Why Non-Experts Do Not Protect Themselves from Cybersecurity Threats? A Review. *International Journal Of Human-Computer Interaction*, *37*(18), 1709–1719. https://doi.org/10.1080/10447318.2021.1908691

Lazuras, L., Barkoukis, V., Mallia, L., Lucidi, F., & Brand, R. (2017). More than a feeling: The role of anticipated regret in predicting doping intentions in adolescent athletes. *Psychology of Sport and Exercise, 30,* 196-204

Leukfeldt, E.R. (2021). *Van theorie naar praktijk: De geleerde lessen van 4 jaar onderzoek naar cybersecurity in het mkb*. De Haagse Hogeschool.

Lewis, I., Watson, B., Tay, R., & White, K. M. (2007). The role of fear appeals in improving driver safety: A review of the effectiveness of fear-arousing (threat) appeals in road safety advertising.*International Journal of Behavioral Consultation and Therapy, 3*(2), 203–222. https://doi.org/10.1037/h0100799

Matthijsse, S. R., Van 'T Hoff-De Goede, M. S., & Leukfeldt, E. R. (2023). Your files have been encrypted: a crime script analysis of ransomware attacks. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09496-z

Matthijsse, S., Loggen, J., Leukfeldt, E., & van 't Hoff-de Goede, S. (2024). De waarde van crime script analyse voor nieuwe vormen van criminaliteit: Geleerde lessen uit de ontwikkeling van drie (cyber)crime scripts. In *Crime scripting: Theorie en praktijk* (pp. 161–184). Boom.

Nationaal Cyber Security Centrum (NCSC). (2015). *Handreiking voor implementatie van detectie-oplossingen: Praktische informatie voor een succesvolle implementatie*.

Nederlandse cybersecuritystrategie (NLCS) & Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2022). *Nederlandse Cybersecuritystrategie 2022-2028: Ambities en acties voor een digitaal veilige samenleving*.

Merkelbach, I., Tendron, MSc., Goossens, MSc., & Behavioural Insight Group Rotterdam. (2023). Gedragsonderzoek 30 km/u in Rotterdam. In Gemeente Rotterdam, *Eindrapport*. Behavioural Insight Group Rotterdam.

Notté, R.J., L. Slot, S. van 't Hoff-de Goede & E.R. Leukfeldt (2019). *Cybersecurity in het mkb: Nulmeting*. De Haagse Hogeschool.

Richard, R., Van der Pligt, J., & De Vries, N. (1996). Anticipated regret and time perspective: Changing sexual risk-taking behavior. *Journal of Behavioral Decision Making, 9*(3), 185-199

RIVM Corona Gedragsunit. (2021). *Verkenning Factoren van invloed op deelname aan COVID-19 vaccinatie*.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal Of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Shillair, R. J. (2018). *Mind the gap: Perceived self- efficacy, domain knowledge and their effects on responses to a cybersecurity compliance message* [proefschrift].

Spithoven, R., Leukfeldt, R., Misana-ter Huurne, E., van 't Hoff – de Goede, S., van Houten, Y., Bekkers, L., Foppen, E., & te Bos, J. (2022). *Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime*. Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion; Lectoraat Cybercrime & Cybersecurity, De Haagse Hogeschool; Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR).

Sutton, S. (2001). Health Behavior: Psychosocial theories. In *Elsevier eBooks* (pp. 6499–6506). https://doi.org/10.1016/b0-08-043076-7/03872-9

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2018). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal Of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Van 't Hoff-de Goede, S., Brasker, E., Bekkers, L., & Leukfeldt, R. (2022). *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?* D*eelrapport werkpakket 4 - mkb*. Centre of Expertise Cyber Security, de Haagse Hogeschool/Regieorgaan SIA.

Van 't Hoff-de Goede, M.S., & Leukfeldt, E. R. (2025). Slachtofferschap van cybercriminaliteit. In *Basisboek cybercriminaliteit*.

Van 't Hoff-de Goede, M.S., Leukfeldt, E. R., De Weijer, V., & Kleij, V. D. (2025). Does protection motivation predict self-protective online behaviour? Comparing self-reported and actual online behaviour using a population-based survey experiment. *Computers in Human Behavior Reports*, *18*, 100649. https://doi.org/10.1016/j.chbr.2025.100649

Van 't Hoff-de Goede, M.S., Wal, M. van der, & Leukfeldt, R. (2024). *What (s)can we do? Onderzoek naar het gebruik van een geautomatiseerde kwetsbaarhedenmeting als evidence based gedragsinterventie*. De Haagse Hogeschool.

Zeelenberg, M. (1999). Anticipated regret, expected feedback and behavioral decision making. *Journal of behavioral decision making, 12*(2), 93-106.

Zhang, X. A., & Borden, J. (2019). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal Of Risk Research*, *23*(10), 1336–1352. https://doi.org/10.1080/13669877.2019.1646315

Bijlage I: Vooraankondigingsbrief

Aan de directeur/eigenaar van
[bedrijfsnaam]
[adres]
[postcode] [plaats]

Datum: Contactgegevens:

Onderwerp: Aankondiging kwetsbaarhedenmeting van [URL]

Beste ondernemer,

Met deze brief willen wij u informeren over de kwetsbaarhedenmeting die wij gaan uitvoeren om cybersecurity risico's op te sporen in uw website en e-mailserver van [URL]. Deze meting zoekt naar kwetsbaarheden in openbaar toegankelijke onderdelen; er wordt niet ingebroken in uw systemen. De meetresultaten worden naar u verzonden en zijn niet openbaar. De resultaten worden vervolgens anoniem gemaakt en daarna gebruikt voor wetenschappelijk onderzoek.

Wie voeren de meting uit?
De kwetsbaarhedenmeting wordt uitgevoerd in opdracht van [Gemeente/Brancheverenigingen], De Haagse Hogeschool en NHL Stenden Hogeschool door Threadstone. [Gemeente/Brancheverenigingen], neemt deel aan dit project, omdat [hier geeft elke organisatie zijn eigen motivatie]. Heeft u vragen of wilt u uw onderneming afmelden voor de kwetsbaarhedenmeting? Stuur dan een e-mail naar [e-mailadres]. U heeft hiervoor vijf werkdagen na ontvangst van deze brief de tijd, daarna zal de meting worden uitgevoerd [deze versie is gebruikt voor gemeente, voor brancheverenigingen werd een opt-out niet expliciet benoemd]

Waarom wordt de meting uitgevoerd?
De kwetsbaarhedenmeting wordt uitgevoerd bij een groot aantal ondernemers in [Gemeente/Brancheverenigingen]. Zo willen wij ondernemingen weerbaarder maken tegen cybercriminaliteit. Jaarlijks wordt één op de vijf ondernemingen slachtoffer van cybercriminaliteit, waarbij zij schade ondervinden. Voorbeelden hiervan zijn het stilliggen van de bedrijfsvoering door ransomware of financiële schade door online fraude. De rapportage die u binnenkort ontvangt kan u helpen uw onderneming beter te beschermen.

Mogen wij ongevraagd een meting uitvoeren?
De meting richt zich uitsluitend op het openbaar toegankelijke deel van uw digitale omgeving; de website en e-mailserver van uw bedrijf. Ons doel is uitsluitend de digitale veiligheid van uw onderneming te vergroten. Daarom is het voor ons mogelijk om deze meting uit te voeren zonder dat u zich hier vooraf voor heeft aangemeld.

Wat is het vervolg?
U ontvangt binnenkort een overzichtelijk rapport met de resultaten van de kwetsbaarhedenmeting. Hierin worden ook praktische aanbevelingen gedaan om kwetsbaarheden aan te pakken. Deze stappen kunt u zelf of samen met uw IT-leverancier uitvoeren (indien van toepassing). Zo kunt u de cybersecurity van uw onderneming verbeteren.

Bijlage II: Begeleidende brief rapportage kwetsbaarhedenmeting

Aan de directeur/eigenaar van
[bedrijfsnaam]
[adres]
[postcode] [plaats]

[Risicocommunicatie]

Datum: Contactgegevens:

Onderwerp: resultaten van kwetsbaarhedenmeting van [URL]

Beste ondernemer,

U heeft onlangs een brief ontvangen waarin stond dat we een kwetsbaarhedenmeting zouden uitvoeren om cybersecurity risico's op te sporen in uw website en e-mailserver van [URL]. Deze meting is nu uitgevoerd. We hebben gekeken naar kwetsbaarheden in openbaar toegankelijke onderdelen; er is niet ingebroken in uw systemen. In het bijgevoegde rapport staan de resultaten en uitleg over welke stappen u kunt nemen om de cyberweerbaarheid van uw organisatie te verbeteren.

Wie voeren de meting uit?
De kwetsbaarhedenmeting is uitgevoerd in opdracht van [Gemeente/Brancheverenigingen], De Haagse Hogeschool en NHL Stenden Hogeschool door Threadstone.
[Gemeente/Brancheverenigingen] neemt deel aan dit project, omdat [Gemeente/Brancheverenigingen] ondernemers ondersteunt bij het vergroten van hun cyberweerbaarheid. Heeft u vragen? Stuur dan een e-mail naar weerbaarheidsmeting@hhs.nl.

Waarom ontvangt u deze rapportage?
De kwetsbaarhedenmeting is uitgevoerd bij een groot aantal ondernemers in [Gemeente/Brancheverenigingen] ontvangen een rapport. Zo willen wij ondernemingen weerbaarder maken tegen cybercriminaliteit. Jaarlijks wordt één op de vijf ondernemingen slachtoffer van cybercriminaliteit, waarbij zij schade ondervinden. Voorbeelden hiervan zijn het stilliggen van de bedrijfsvoering door ransomware of financiële schade door online fraude. Het bijgevoegde rapport kan u helpen uw onderneming beter te beschermen.

Hoe kan dit rapport u helpen?
In dit rapport staan de resultaten van de kwetsbaarhedenmeting en op maat gemaakt advies, met duidelijke stappen om deze kwetsbaarheden op te lossen. Met het advies in dit rapport kunt u samen met uw eigen IT leveancier(s) de nodige stappen zetten om uw cybersecurity te verbeteren.

Is dit reclame of een commercieel project?
Nee, dit project heeft geen commercieel doel. De betrokken organisaties zetten zich in voor het verbeteren van de digitale weerbaarheid van bedrijven. De meting en adviezen worden kosteloos aangeboden en zijn alleen bedoeld om ondernemers te helpen hun digitale veiligheid te verbeteren.

Wat is het vervolg?
In het bijgevoegde rapport leest u welke digitale kwetsbaarheden we hebben gevonden en we geven praktische adviezen om uw digitale weerbaarheid te verbeteren. Volg de aanbevelingen in het rapport en werk hierbij samen met uw IT-leverancier(s). Let op: onze controle op openbare kwetsbaarheden is een goede eerste stap, maar geen volledige beveiligingscontrole van uw website en e-mailserver. Op de laatste pagina van het rapport vindt u verdere stappen voor het vergroten van de cyberweerbaarheid van uw onderneming.

Hoogachtend,
Team weerbaarheidsmeting van de Haagse Hogeschool, Hogeschool NHL Stenden, Threadstone en [Gemeente/Brancheverenigingen]

DE HAAGSE HOGESCHOOL

NHL STENDEN hogeschool

ThreadStone CYBER SECURITY

[Logo Gemeente/Branche-vereniging]

Bijlage III: Voorbeeld rapportage

Uw Cyber Kracht Meting

Opgesteld voor

Meting uitgevoerd op domeinnaam …

Deze meting is uitgevoerd op …

DE HAAGSE HOGESCHOOL

NHL STENDEN hogeschool

Hoe digitaal veilig is uw organisatie?

Eén op de vijf ondernemers is slachtoffer van cybercriminelen. Maar hoe kwetsbaar is uw organisatie? Om hierachter te komen heeft de Haagse Hogeschool een `Cyber Kracht Meting` laten uitvoeren. De uitkomst voor uw organisatie vindt u in dit rapport. Deze uitkomst delen we uiteraard niet met anderen.

Rapport

Dit rapport geeft inzicht in welke zaken al goed zijn geregeld en wat aandachtspunten zijn voor uw organisatie op het gebied van digitale veiligheid. Wij adviseren u deze punten door te nemen met uw verantwoordelijke IT`er zodat hij/zij deze kan bekijken en zo mogelijk kan oplossen.

Deze rapportage is tot stand gekomen op basis van uitvraag van openbare bronnen op het internet, gekoppeld aan uw domeinnaam. Er zijn dus **geen** ethische hackers ingeschakeld die geprobeerd hebben om digitaal bij uw bedrijf binnen te komen. Er is alleen op basis van een domeinnaam van een afstand gekeken of er ramen of deuren open staan waar cybercriminelen kans zien om binnen te komen.

In het rapport geven we een algemeen beeld van welke risico`s er worden gelopen. Een aantal controles is voor iedere organisatie relevant, bijvoorbeeld de controle op veilige e-mail. Andere controles, bijvoorbeeld van de website, zijn niet voor elke organisatie even relevant. Om daar een goed, compleet beeld over te vormen, kan een cybersecurity expert u helpen met het in kaart brengen van uw risico`s en u adviseren over de juiste maatregelen op het gebied van beleid, bewustzijn van medewerkers en techniek.

Deze gratis meting is bedoeld om u inzicht te geven; u kunt de meting zien als een eerste, laagdrempelige aanzet waarmee u direct uw informatiebeveiliging en digitale weerbaarheid kunt geven.

Hieronder staan de belangrijkste bevindingen uit de meting.

	Aandachtspunten	Mogelijk gevolg
!	Gevoelige gegevens van medewerkers van uw organisatie, waaronder wellicht ook gebruikersnamen en wachtwoorden, zijn openbaar.	*Kwaadwillenden kunnen mogelijk inbreken in (cloud-gebaseerde) systemen die uw organisatie gebruikt.*
!	Er staan ongebruikelijke digitale deuren open. Hier kunnen kwaadwillenden mogelijk een opening vinden die ze kunnen gebruiken om in te breken.	*Kwaadwillenden kunnen zwakke plekken in uw website vinden. Hierdoor kunnen zij gegevens stelen, aanpassen of uw website verstoren.*
!	Securityprotocollen worden niet juist afgedwongen op de browser van de bezoeker.	*Onbevoegden kunnen communicatie met uw website (met mogelijk gevoelige gegevens van bezoekers) onderscheppen en mogelijk manipuleren.*

!	Uw website geeft informatie vrij over de instellingen. Hackers kunnen deze informatie gebruiken om uw website aan te vallen.	*Doordat eenvoudig achterhaald kan worden welke software uw website gebruikt, is het makkelijker voor een kwaadwillende om te controleren of uw website kwetsbaar is. Hierdoor kunnen eenvoudiger openingen in uw website worden gevonden waardoor deze kan worden gehackt (stelen of manipuleren van data of verstoren van de werking).*

!	Het is mogelijk om websiteverkeer naar uw website te manipuleren, waardoor u niet kunt garanderen dat uw bezoekers úw website bezoeken maar zij dat wel denken (en dus worden doorgesluisd naar een kwalijke website).	*Kwaadwillenden kunnen wachtwoorden of andere vertrouwelijke informatie onderscheppen van bezoekers van uw website.*
!	Uw server is niet voorbereid voor de nieuwe internetstandaarden.	*In de toekomst zal steeds meer verkeer lopen via de nieuwe IPv6 standaarden. Het is daarom verstandig om hier ook voorbereid op te zijn.*

Controles die zijn uitgevoerd

Al onze uitgevoerde controles zijn gebaseerd op openbare bronnen die we op het internet konden raadplegen. Hieronder leest u welke controles dit zijn. Een goed of slecht resultaat betekent niet automatisch dat uw informatiebeveiliging ook goed of slecht is.

Controle	Resultaat
Verspreidt uw website geen malware?	✓
Verspreidt uw website geen spam?	✓
Verspreidt uw mailserver geen spam?	✓
Zijn gevoelige gegevens van uw medewerkers niet openbaar?	!
Kan uw e-mail niet misbruikt worden?	✓
Kan het verkeer met uw website niet worden onderschept?	✓
Zijn er geen ongebruikelijke aanvalspaden op uw website mogelijk?	!
Worden bezoekers van uw website voldoende beschermd?	!
Is informatie over de configuratie van uw website afgeschermd?	!
Kan websiteverkeer naar uw website niet gemanipuleerd worden?	!
Is uw website, mailserver en nameserver gereed voor nieuwe internetstandaarden?	!

✓ :goede score *) ? :niet kunnen bepalen ! :aandachtspunt, zie eerste pagina

*) Een goede score is mooi, maar let op: deze meting is globaal én een momentopname.

DE HAAGSE HOGESCHOOL

NHL STENDEN hogeschool

Onderbouwing

Op deze pagina vindt u de onderbouwing van de resultaten. Deze onderbouwing kunt u doornemen met de verantwoordelijke IT'er, zodat hij/zij de geconstateerde aandachtspunten nader kan bekijken en zo mogelijk wegnemen.

Controle	Onderbouwing	Advies
Verspreidt uw website geen malware?	Websites die kwalijke software, zoals malware en virussen, verspreiden, worden op zogenaamde 'blacklists' bijgehouden. We hebben gekeken of uw website voorkomt op zogenaamde 'blacklists'. Uw website komt niet voor op deze blacklists, prima!	Geen verdere actie nodig.
Verspreidt uw website geen spam?	Websites die spam (ongewenste e-mail) versturen, worden bijgehouden op zogenaamde 'blacklists'. We hebben gekeken of uw website voorkomt op deze 'blacklists'. Uw website komt niet voor op deze blacklists, prima!	Geen verdere actie nodig.
Verspreidt uw mailserver geen spam?	Mailservers waarvan bekend is dat ze spam (ongewenste e-mail) versturen, worden bijgehouden op zogenaamde 'blacklists'. We hebben gecontroleerd of uw mailserver op deze blacklists voorkomt. Uw mailserver komt niet voor op deze lijsten, prima!	Geen verdere actie nodig.
Zijn gevoelige gegevens van uw medewerkers niet openbaar?	We hebben gekeken of er e-mailadressen van uw website zijn die voorkomen in bestanden die door hackers zijn gestolen. Dat zijn bestanden met bijvoorbeeld wachtwoorden. We zien dat er e-mailadressen van uw domeinnaam staan in bestanden die door hackers zijn gestolen.	De controle die we hebben uitgevoerd is beperkt. Kijk op www.haveibeenpwned.com voor meer informatie. Laat elke medewerker zijn of haar e-mailadres(sen) controleren. Benadruk dat zij voor elke applicatie een ander wachtwoord moeten gebruiken. Zéker voor de websites die op Haveibeenpwned.com worden getoond.
Kan uw e-mail niet misbruikt worden?	We hebben de instellingen van uw mailserver gecontroleerd. Als de instellingen niet goed zijn, kunnen anderen misschien nep-mails sturen alsof ze van uw bedrijf komen. Goed nieuws: uw mailserver is goed ingesteld en kan niet misbruikt worden!	Geen verdere actie nodig.
Kan het verkeer met uw website niet worden onderschept?	We hebben gekeken of het verkeer tussen uw website en uw bezoekers versleuteld is. Een bezoeker ziet dit aan een groen slotje links in de browser (zogenaamd "https"). De SSL certificaten van uw website zijn prima ingericht!	Geen verdere actie nodig.

! Zijn er geen ongebruikelijke aanvalspaden op uw website mogelijk?	We hebben gekeken welke 'deuren' (poorten) op uw website open staan. Hoe meer deuren er open zijn, hoe makkelijker het is voor anderen om in te breken. Wij zien dat de volgende poort(en) op uw website "open" staan: pop3_starttls:110, imap_starttls:143, ftp:21, https:443, smtps:465, smtp_starttls:587, http:80, https:8443, imaps:993, pop3s:995.	In principe zijn voor het bezoeken van uw website alleen poort 80 en 443 nodig. Laat controleren waarom de andere porten open staan en laat nakijken of dit echt nodig is. Dit doet u bij de hostingpartij van uw website.
! Worden bezoekers van uw website voldoende beschermd?	We hebben gecontroleerd of het verkeer tussen uw website en bezoekers veilig is en niet zomaar kan worden aangepast. In uw geval zien we dat de volgende headers voor http en/of https niet juist zijn ingesteld: X-Frame-Options, X-Content-Type-Options, Content-Security-Policy, Referrer-Policy.	Laat de hiernaast aangegeven headers van uw website nakijken. Dit laat u doen door de ontwikkelaar van uw website.
! Is informatie over de configuratie van uw website afgeschermd?	We hebben gekeken of we kunnen zien welke software uw website gebruikt. Als anderen dit weten, kunnen ze gerichte aanvallen uitvoeren. We zien dat uw website gebruik maakt van nginx, PleskLin.	Zorg ervoor dat de informatie over de software(versies) die uw website gebruikt wordt afgeschermd. Dit laat u doen door de ontwikkelaar van uw website.
! Kan website verkeer naar uw website niet gemanipuleerd worden?	We hebben gecontroleerd of bezoekers die uw domeinnaam bezoeken, ook echt op uw website terechtkomen en niet worden omgeleid naar een nep website. In uw geval blijkt de instelling hiervoor niet goed of afwezig te zijn; uw website blijkt geen DNSSec (extra beveiliging voor domeinnamen) te ondersteunen.	Zorg ervoor dat DNSSec wordt ingesteld op uw domein. Dit laat u doen door de hoster of beheerder van uw domein.
! Is uw website, mailserver en nameserver gereed voor nieuwe internetstandaarden?	We hebben gecontroleerd of uw website en servers (mailserver en nameserver) voldoen aan de nieuwste internetprotocollen (IPv6). Het blijkt dat uw website en EMAIL geen IPv6 ondersteunt. Dit is niet direct een beveiligingsprobleem, maar kan in de toekomst wel leiden tot (veiligheids) problemen.	IPv6 is de nieuwe standaard voor internetverkeer. Vraag de beheerder van uw website en EMAIL om dit te ondersteunen. Met IPv6 wordt beveiliging in de toekomst makkelijker. Ook zal internetverkeer sneller worden geregeld.

Bijlage IV: Handelingsperspectief

Welke stappen kunt u nu het beste nemen?

Stap 1: Werk aan gevonden kwetsbaarheden

Scenario 1: U heeft een IT leverancier

Wanneer u een IT-leverancier heeft, adviseren wij u om de gevonden kwetsbaarheden in uw cybersecurity en de maatregelen in deze rapportage met hen te bespreken. In dit gesprek kunt u de volledigheid van de IT-dienstverlening en verantwoordelijkheden bespreken. Wilt u tips voor dit gesprek? Bezoek de website van het Digital Trust Center (DTC) voor constructieve adviezen. Het DTC is een onafhankelijke overheidsorganisatie die ondernemers adviseert op het gebied van cybersecurity. In de bijgevoegde folder vindt u een overzicht met informatie en antwoorden op veelgestelde vragen. Meer informatie is beschikbaar op de DTC-website; scan de QR-code met uw smartphone om direct naar de webpagina te gaan of ga naar https://digitaltrustcenter.nl/afspraken

Scenario 2: U heeft geen IT leverancier

Wellicht overweegt u om een IT leverancier in de arm te nemen? Veel van deze aanbieders bieden goedkope pakketten met cybersecurity aan die uw bedrijf beter bestand maken tegen cyberaanvallen. Op de website van het van het Digital Trust Center (DTC) kunt u direct tips lezen over het kiezen van een IT leverancier. Het DTC is een onafhankelijke overheidsorganisatie dat ondernemers voorligt en adviseert op het gebied van cybersecurity. Scan de QR-code om naar de betreffende webpagina van het DTC te gaan of ga naar https://digitaltrustcenter.nl/praatplaat

Stap 2: Werk aan bredere cybersecurity binnen uw organisatie

U kunt beginnen met het in acht nemen van de vijf basisprincipes van cyberweerbaarheid. De basisprincipes zijn om uw cybersecurity regelmatig te controleren en eenvoudige beveiligingsmaatregelen te implementeren. Veel digitale incidenten ontstaan door een gebrek aan deze maatregelen. Met deze principes ontwikkelt u een sterke cyberbeveiligingsstrategie die aansluit bij uw organisatie. Scan de QR-code om meer informatie te vinden over deze basisprincipes of ga naar https://digitaltrustcenter.nl/5princi

Bijlage V : Checklist

Checklist vooraankondiging

		Poging 1	Poging 2
A.	Vertegenwoordiger CS onderneming aanwezig?	O Ja O Nee	O Ja O Nee
B.	Rol vertegenwoordiger:		
C.	Heeft u onze brief ontvangen waarin wij hebben aangekondigd dat wij een cybersecuritymeting zouden gaan uitvoeren? (Envelop maat A3, met logo van NHLS, erin zat een brief)	O Ja O Nee O Weet niet	
	Heeft u de brief geopend?	O Ja O Nee	
D.	Heeft u deze brief gelezen?	O Ja O Nee	

Deel 1: Vooraankondiging

Wat vond u van deze brief?

O Positief O Neutraal O Negatief

Eventuele toelichting (bijv. Welke onderdelen waren positief/negatief):

Heeft u overwogen uw bedrijf af te melden voor de kwetsbaarhedenscan? Waarom wel/niet?

Deel 2: Rapportage

Ongeveer een week geleden hebben wij u de rapportage van de kwetsbaarhedenmeting gestuurd.

		Ja	Nee	Anders
1.	Heeft u het poststuk ontvangen? (Envelop maat A3, met logo van NHLS, erin zat een brief)			
2.	Is het poststuk bij de juiste persoon in uw bedrijf aangekomen die verantwoordelijk is voor CS?			
3.	Heeft u/diegene het poststuk geopend?			

*Notitie. Indien persoon waarmee wordt gesproken deze niet heeft ontvangen/gezien, vragen of degene gesproken kan worden die daar wel kennis over heeft, of toestemming vragen opnieuw langs te komen tijdens vervolgbezoek bedrijventerrein.

Waarom wel/niet geopend?

In de envelop zat een brief en een rapportage. Wat is uw mening over de logo's die op de brief stonden (NHLS, HHs, PVO, ThreadStone)?

O Positief O Neutraal O Negatief

Indien positief, waarom? Indien negatief, wat had u graag anders gezien?

		Ja	Nee	Anders
4.	Heeft u/uw collega die verantwoordelijk is voor CS de rapportage in het poststuk gelezen?			

Waarom wel/niet gelezen?

	*Indien gelezen:	Ja	Nee	Anders
5.	Bent u van plan om stappen te zetten op basis van de adviezen in de aangeleverde rapportage?			
6.	Heeft u al stappen gezet op basis van de aangeleverde rapportage?			

Toelichting (bijv. waarom wel/geen actie):

In hoeverre waardeert u dit initiatief? Heeft u nog concrete suggesties/tips?

	*Alleen vragen indien men de rapportage heeft ontvangen, geopend en gelezen.	Ja	Nee	Anders
7.	Zouden wij een interview met u mogen plannen om (dieper) op bovenstaande vragen in te gaan?			

Beschikbare data + contactgegevens (eventuele reden non-response):

Checklist zonder vooraankondiging

		Poging 1	Poging 2
A.	Vertegenwoordiger CS onderneming aanwezig?	O Ja O Nee	O Ja O Nee
B.	Rol vertegenwoordiger:		

Deel 2: Rapportage

Ongeveer een week geleden hebben wij u een rapportage van de kwetsbaarheden meting gestuurd.

		Ja	Nee	Anders
1.	Heeft u het poststuk ontvangen? (Envelop maat A3, met logo van NHLS, erin zat een brief)			
2.	Is het poststuk bij de persoon in uw bedrijf aangekomen die verantwoordelijk is voor CS?			
3.	Heeft u/diegene het poststuk geopend?			

*Notitie. Indien persoon waarmee wordt gesproken deze niet heeft ontvangen/gezien, vragen of degene gesproken kan worden die daar wel kennis over heeft, of toestemming vragen opnieuw langs te komen tijdens vervolgbezoek bedrijventerrein.

Waarom wel/niet geopend?

In de envelop zat een brief en een rapportage. Wat is uw mening over de logo's die op de brief stonden (NHLS, HHs, PVO, ThreadStone)?

O Positief O Neutraal O Negatief

Indien positief, waarom? Indien negatief, wat had u graag anders gezien?

		Ja	Nee	Anders
4.	Heeft u/uw collega die verantwoordelijk is voor CS de rapportage in het poststuk gelezen?			

Waarom wel/niet gelezen?

	*Indien gelezen:	Ja	Nee	Anders
5.	Bent u van plan om stappen te zetten op basis van de adviezen in de aangeleverde rapportage?			
6.	Heeft u al stappen gezet op basis van de aangeleverde rapportage?			

Toelichting (bijv. waarom wel/geen actie)

In hoeverre waardeert u dit initiatief? Heeft u nog concrete suggesties/tips?

	*Alleen vragen indien men de rapportage heeft ontvangen, geopend en gelezen.	Ja	Nee	Anders
7.	Zouden wij een interview met u mogen plannen om (dieper) op bovenstaande vragen in te gaan?			

Beschikbare data + contactgegevens (eventuele reden non-response):

Bijlage VI: Informed consent

In opdracht van NHL Stenden Hogeschool, De Haagse Hogeschool en PVO Noord-Nederland is de digitale infrastructuur van een selectie ondernemingen op het bedrijventerrein De Hemrik in Leeuwarden door cybersecuritybedrijf ThreadStone gescand. Zo hebben wij vastgesteld of er kwetsbaarheden in uw openbaar bereikbare digitale infrastructuur zitten. Om te bepalen hoe ondernemers deze interventie ervaren, worden interviews met de gescande ondernemers afgenomen. Dit interview zal ongeveer 20 -30 minuten duren.

Uw deelname is vrijwillig en u kunt het interview te allen tijde stoppen, of u kunt weigeren dat uw gegevens worden gebruikt voor het onderzoek. Voorgenoemde kan zonder opgave van reden. Uw gegevens zullen in dat geval worden vernietigd. Het stopzetten van deelname heeft op geen enkele manier nadelige gevolgen voor u.

Uw privacy is en blijft te allen tijde beschermd. Er wordt zorgvuldig omgegaan met persoonsgegevens en de onderzoekers dragen zorg dat deze niet direct herleidbaar zijn. De informatie die u in een interview geeft, wordt enkel voor de hierboven genoemde doeleinden gebruikt. Alle gegevens worden vertrouwelijk behandeld en opgeslagen.

Als u besluit om uw deelname aan het onderzoek te stoppen of bij eventuele vragen, kunt u contact opnemen met de onderzoeksleider:
Jurjen Jansen
E. [e-mailadres]

Toestemmingsverklaring

○ Ik heb bovenstaande informatie gelezen en begrepen. Al mijn vragen voorafgaand aan het interview zijn beantwoord en ik ben vrijwillig akkoord gegaan met deelname aan dit onderzoek.

Handtekening respondent	Handtekening onderzoeker
Datum	Datum

Bijlage VII: Interviewprotocol

Inleiding. Allereerst bedankt dat u wilt meewerken aan dit interview. Mijn naam is … en ik ben werkzaam als onderzoeker aan … Hogeschool. Samen met NHL Stenden Hogeschool/de Haagse Hogeschool voeren wij onderzoek uit naar de digitale weerbaarheid van ondernemers in Nederland, waaronder op het bedrijventerrein waar uw onderneming is gevestigd. Dit doen we in opdracht van het Centrum voor Criminaliteitspreventie en Veiligheid en met ondersteuning van PVO Noord-Nederland.
Doel interview. Het doel van ons onderzoek is het ontwikkelen en evalueren van een interventie die ondernemers kan ondersteunen om de digitale weerbaarheid van hun onderneming te vergroten. Daarmee proberen we slachtofferschap van online criminaliteit zoveel mogelijk te voorkomen. Specifiek in dit interview willen we focussen op hoe kwetsbaarhedenmeting – de brief en de rapportage die we aan u verstuurd hebben op dd. 28/06/2024 – door u is ervaren, in hoeverre u naar aanleiding van deze brief actie onderneemt of dat van plan bent te doen t.a.v. de digitale weerbaarheid van uw onderneming, en op welke wijze wij deze interventie mogelijk kunnen verbeteren. Het interview zal maximaal een half uur in beslag nemen.
Belangrijke informatie vooraf.

- Alle input wordt anoniem verwerkt in een eindrapport. De resultaten zullen niet naar u herleidbaar zijn.
- U mag uw deelname aan het interview op elk moment stoppen, zonder opgave reden.
- We willen het interview graag opnemen ter bevordering van de uitwerking ervan. Gaat u daarmee akkoord? De opname wordt vernietigd na uitwerking.
- Hebt u nog vragen over het onderzoek?
- ‘Informed consent’-formulier (digitaal) laten tekenen.
- Indien akkoord: *start opname*

Dan wil ik graag beginnen met het interview.

1. Kunt u iets vertellen over uw onderneming/de organisatie waarvoor uw werkt, in welke branche deze actief is en welke rol u hebt in de organisatie?
2. Op welke wijze hebt u de digitale veiligheid van uw onderneming/de organisatie waarvoor uw werkt geregeld? (Zelf, specifieke afdeling, werknemer met affiniteit, uitbesteedt, etc.)
3. Heeft u in de afgelopen vijf jaar te maken gehad met incidenten door toedoen van digitalisering? (Uitval, verstoring, digitale criminaliteit [poging/slachtofferschap], etc.)

Indien vooraankondiging:
Ik wil nu graag een aantal vragen stellen over de brief die wij u voorafgaande aan de kwetsbaarhedenmeting hebben gestuurd.

1. In hoeverre hebt u deze brief ontvangen en gelezen? (Indien niet ontvangen/gelezen, door naar deel 2)
2. Wat vindt u van de vooraankondiging middels de brief?
3. Wat vindt u van de toon van brief?
4. Wat vindt u van de manier van communiceren in brief?
5. Heeft u op andere wijze acties ondernomen naar aanleiding van de aankondigingsbrief?

6. Vindt u dat we de vooraankondiging moeten blijven sturen naar ondernemers in de toekomst (of alleen de brief met de rapportage)?
7. Wat is voor u de belangrijkste reden om mee te doen aan de kwetsbaarhedenmeting? Notitie interviewer. Evt. anders verwoorden: waarom heeft u zich niet uitgeschreven van deelname? (Bijv. specifieke aanleiding, interesse, baat het niet dan schaadt het niet, etc.)

Deel 2

8. Wat vindt u van het initiatief waarbij uw bedrijfswebsite (notitie interviewer: huidige aanpak benoemen) aangekondigd/onaangekondigd wordt gescand?
   a. Waarom vindt u dat?
9. Wat zou u ervan vinden wanneer dit (notitie interviewer: tegenovergestelde aanpak) aangekondigd/onaangekondigd zou gebeuren? Waarom?

<u>Envelop en brief</u>

Dan wil ik u nu wat vragen stellen over de tweede envelop die u van ons heeft gekregen, waar de rapportage in zat.

10. Hebt u de envelop en brief zelf gezien en gelezen? (Notitie interviewer; indien nodig vragen overslaan en doorgaan met vraag 12)
    a. Wat is uw algemene indruk van de envelop die u heeft ontvangen?
    b. Waarom heeft u de envelop wel/niet geopend?
    c. Wat vindt u van het logo op de envelop? Maakt dit verschil om de envelop wel of niet te openen?
    d. Zijn er nog andere redenen waarom u de envelop wel/niet heeft geopend?
11. Wat is uw algemene indruk van de brief die u hebt ontvangen?
    a. Wat vindt u van de vormgeving van de brief?
    b. Wat vindt u van de logo's die erop staan?
    c. Wat vindt u van de schrijfstijl van de brief?
    d. Wat sprak u aan in de brief?
    e. Wat sprak u minder/niet aan in de brief?
    f. Indien niet direct aan bod gekomen; Wat vond u van:
       - De toon/stijl van de brief?
       - De bevindingen over de veiligheid van uw website?
       - De aanbevelingen om de veiligheid van uw website te verbeteren? (Duidelijk, praktisch uitvoerbaar, etc.)
       - Hoe zou u de brief in z'n geheel beoordelen? (kwaliteit)
12. Hebt u aanbevelingen/tips om de brief duidelijker/aansprekender/etc. te maken?
    a. Mist u specifieke informatie?
13. In hoeverre motiveerde de brief u om de bijgevoegde rapportage te lezen?
14. Is de (inhoud van de) brief bij de juiste persoon terecht gekomen?
    a. Wie is deze werknemer/Welke functie heeft deze werknemer?

<u>Rapportage</u>

15. Hebt u de rapportage met de uitkomsten van de kwetsbaarhedenmeting zelf gelezen? (notitie interviewer; indien nodig vragen overslaan en doorgaan met vraag 17)

    a. Wat is de algemene indruk van de rapportage die u hebt ontvangen? (Kwaliteit)
    b. In hoeverre voldoet de rapportage aan uw verwachtingen over de digitale veiligheid binnen uw onderneming?
    c. Wat vindt u van de adviezen in de rapportage?
    d. In hoeverre zijn de adviezen bruikbaar?
    e. In hoeverre zijn de adviezen (praktisch) uitvoerbaar?
16. Hebt u aanbevelingen/tips om de rapportage duidelijker/aansprekender/etc te maken?
    a. Mist u specifieke informatie?
17. In hoeverre heeft de rapportage invloed op uw perceptie op digitale veiligheid binnen uw organisatie?
    a. Indien niet direct benoemd; In hoeverre heeft de brief invloed gehad op uw:
        - Bewustzijn over digitale veiligheid van uw onderneming/de organisatie waarvoor uw werkt?
        - Houding t.a.v. …
        - Urgentiebesef t.a.v. …
        - …
18. Hebt u naar aanleiding van de brief/rapportage actie(s) ondernomen, of bent u van plan om dit te doen?
    a. In hoeverre heeft de brief hierop invloed gehad?
    b. In hoeverre heeft de rapportage hierop invloed gehad?
    c. Zo ja, kunt u aangeven welke acties? Wat is daarvoor de belangrijkste motivatie? Was deze brief de aanleiding of een extra duwtje in de rug? Wilt u nog meer doen? Wat hebt u nodig om dit te kunnen realiseren?
    d. Zo nee, kunt u aangeven waarom niet? Wat is daarvoor de belangrijkste motivatie? Wat zou moeten veranderen om toch over te gaan tot actie? Wat hebt u nodig om dit te kunnen realiseren?
    e. Indien wordt aangegeven dat alles op orde is/de IT-(beveiliging) is uitbesteedt, doorvragen

19. Vindt u dat wij de kwestbaarhedenmeting op deze manier moeten aanbieden aan meer ondernemers? Heeft u nog suggesties voor verbetering?
20. Is er volgens u een onderwerp niet aan de orde gekomen die u graag nog zou willen delen?

Respondent bedanken en opname eindigen.

Bijlage VIII : Beschrijvende resultaten originele en aangepaste voormeting

Groep			*N*	*Threadstone-score*		*Totaal risicopunten*		*Verspreidt uw website geen spam?*		*Verspreidt uw mailserver geen spam?*	
				OV	AV	OV	AV	OV	AV	OV	AV
Alle organisaties (testgroep en controlegroep)		Juiste score	2807	3.21	3.21	9.27	7.53	1.62	0.73	1.65	0.71
		Te lage score	6325	1.68	4.47	9.41	5.83	2.94	1.09	2.95	1.04
Testgroep	*Totaal*	Juiste score	2199	3.28	3.28	9.16	7.43	1.56	0.71	1.60	0.69
		Te lage score	5033	1.59	4.43	9.54	5.88	2.93	1.09	2.95	1.03
	Br1	Juiste score	571	1.07	1.07	13.37	9.97	2.87	1.22	2.89	1.10
		Te lage score	2806	1.61	4.43	9.49	5.88	2.89	1.09	2.91	1.02
	Br2	Juiste score	1019	5.35	5.25	5.36	5.13	0.40	0.29	0.45	0.33
		Te lage score	411	1.62	4.56	9.52	5.80	3.00	1.13	3.00	1.04
	Ge1	Juiste score	154	1.10	1.10	13.49	10.00	2.95	1.19	2.94	1.12
		Te lage score	749	1.53	4.38	9.73	5.91	3.00	1.11	3.00	1.06
	Ge2	Juiste score	143	1.00	1.00	13.87	10.34	3.00	1.19	2.95	1.15
		Te lage score	606	1.55	4.39	9.66	5.92	2.98	1.08	2.99	1.05
	Ge3	Juiste score	319	2.97	2.97	9.72	7.80	1.67	0.70	1.71	0.71
		Te lage score	461	1.64	4.45	9.60	5.81	2.99	1.06	2.98	1.03
Controlegroep		Juiste score	608	3.01	3.01	9.58	7.81	1.78	0.79	1.83	0.78
		Te lage score	1292	1.05	4.59	9.02	5.68	2.95	1.09	2.95	1.05
Risicocommunicatie	*Geen risicocommunicatie*	Juiste score	715	3.30	3.30	9.13	7.40	1.57	0.72	1.62	0.72
		Te lage score	1698	1.60	4.40	9.54	5.90	2.90	1.09	2.94	1.03
	Coping	Juiste score	639	2.80	2.80	10.07	7.99	1.84	0.81	1.86	0.76
		Te lage score	1763	1.57	4.42	9.59	5.89	2.96	1.09	2.95	1.04
	Geanticipeerde spijt	Juiste score	846	3.63	3.63	8.50	7.03	1.35	0.63	1.37	0.61
		Te lage score	1572	1.61	4.47	9.51	5.85	2.94	1.10	2.95	1.03