What (s)can we do?
Onderzoek naar het gebruik van een geautomatiseerde kwetsbaarhedenmeting als evidence based gedragsinterventie

M.S. van ’t Hoff-de Goede
M.L. van der Wal
E.R. Leukfeldt

Centre of Expertise Cyber Security, De Haagse Hogeschool

2024

DE HAAGSE HOGESCHOOL

Inhoudsopgave

Samenvatting 3

1. Inleiding 8
   1.1. Aanleiding 8
   1.2. Doelstelling 9
   1.3. Onderzoeksvragen 9
   1.4. Leeswijzer 10
2. Theorie en eerder onderzoek 11
   2.1. Cyberweerbaarheid 11
   2.2. Cyberscans 12
   2.3. Risicocommunicatie 14
3. De geautomatiseerde kwetsbaarhedenmeting 16
   3.1. Wat is de geautomatiseerde kwetsbaarhedenmeting? 16
   3.2. Onderdelen kwetsbaarhedenmeting 16
   3.3. Adviesrapportage, handelingsperspectief en risicocommunicatie 19
   3.4. Beperkingen 19
4. Methoden 20
   4.1. Steekproef 20
   4.2. Definiëring onderdelen meting 22
   4.3. Dataverwerking van de resultaten van de metingen 23
   4.4. Statistische analyse methoden 23
5. Resultaten 24
   5.1. Juridische risicobeoordeling 24
   5.2. Interviews met stakeholders 25
      5.2.1. Eerste reacties en algemeen beeld 25
      5.2.2. Communicatie van de resultaten naar de deelnemers 26
      5.2.3. Kansen voor de eigen organisatie 27
      5.2.4. Knelpunten van de interventie 27
   5.3. Resultaten kwetsbaarhedenmeting 29
      5.3.1. Vergelijking voor- en nameting per bedrijventerrein 29
      5.3.2. Vergelijking deelnemende bedrijventerreinen met controlegroep 34
6. Conclusie en discussie 36
   6.1. Beantwoording onderzoeksvragen 36
   6.2. Beperkingen 39
   6.3. Aanbevelingen 40

Literatuur 41
Bijlage I – Juridische risicobeoordeling 45
Bijlage II – Interviewprotocol 49

Samenvatting

Achtergrond en eerder onderzoek

Een groeiende groep ondernemers is zich bewust van de mogelijke risico's die de digitalisering van het bedrijfsleven met zich meebrengt, en neemt in toenemende mate maatregelen om hun cyberweerbaarheid te verbeteren en het risico op slachtofferschap van cybercriminaliteit zo laag mogelijk te houden. Toch loopt een te groot deel van de ondernemers achter in het nemen van beschermende maatregelen, resulterend in een hoger risico op slachtofferschap van cybercriminaliteit. Het is daarom van groot belang dat er empirisch onderbouwde (*evidence-based*) interventies worden ontwikkeld en ingezet om de cyberweerbaarheid van Nederlandse ondernemingen te vergroten.

Om ondernemers bij te staan in het verbeteren van hun cyberweerbaarheid, ontwikkelden veel instanties hulpmiddelen, waaronder cyberscans. Cyberscans helpen de ondernemer inzicht te verkrijgen in de huidige stand van zaken omtrent hun cyberweerbaarheid. Deze cyberscans worden zowel off- als online aangeboden, al dan niet kosteloos, door zowel private- als overheidsorganisaties. Er bestaan handmatige cyberscans waarbij de ondernemer zelf of samen met een cybersecurityprofessional een (online) vragenlijst invult en geautomatiseerde cyberscans waarbij de infrastructuur van een onderneming gecontroleerd wordt op kwetsbaarheden. De scans lopen zijn zeer uiteenlopend in de mate waarin de cyberweerbaarheid volledig en betrouwbaar in kaart wordt gebracht. Er is tot op heden zeer beperkt onderzoek gedaan naar de effectiviteit van dergelijke initiatieven. Het is dan ook de vraag in welke mate deze initiatieven werkelijk bijdragen aan de verhoging van de cyberweerbaarheid van Nederlandse ondernemingen.

Onderzoeksdoel en onderzoeksvragen

Het doel van dit onderzoek is het toetsen van een interventie gericht op het vergroten van de cyberweerbaarheid van ondernemingen. De interventie bestaat uit een geautomatiseerde kwetsbaarhedenmeting resulterend in een door ondernemingen te ontvangen (op maat gemaakte) rapportage van gevonden kwetsbaarheden, waarin risicocommunicatie en een handelingsperspectief is opgenomen. Het betreft een interventie waar ondernemers zich niet voor hoeven aan te melden, maar die uitgevoerd kan worden in opdracht van bijvoorbeeld een overheidsorganisatie voor een groep ondernemingen, zoals gehele bedrijventerreinen of sectoren.

De volgende onderzoeksvraag staat centraal in dit rapport: "*In hoeverre is het mogelijk, toegestaan en effectief om een geautomatiseerde kwetsbaarhedenmeting uit te voeren ter bevordering van de cyberweerbaarheid van Nederlandse ondernemingen?"* De volgende deelvragen worden beantwoord in dit rapport:

1. Is het juridisch toegestaan om een geautomatiseerde kwetsbaarhedenmeting uit te voeren bij ondernemingen, zonder dat zij hier vooraf toestemming voor hebben gegeven?
2. Welke kansen en knelpunten zien betrokkenen bij het uitvoeren van een geautomatiseerde kwetsbaarhedenmeting bij Nederlandse ondernemingen?

3. In welke mate verandert de cyberweerbaarheid van ondernemingen na het ontvangen van de geautomatiseerde kwetsbaarhedenmeting en in hoeverre is dit vergelijkbaar tussen de verschillende bedrijventerreinen en de controlegroep?

Interventiebeschrijving

De interventie bestaat allereerst uit een geautomatiseerde kwetsbaarhedenmeting, waarbij in de openbaar toegankelijke digitale infrastructuur van ondernemingen wordt gemeten of er sprake is van kwetsbaarheden. Elke onderneming start in de geautomatiseerde kwetsbaarhedenmeting met een "totaalscore cyberweerbaarheid" van tien en krijgt vervolgens minpunten voor elke gevonden kwetsbaarheid. De totaalscore kan daartoe uiteenlopen (van één tot tien), waarbij één de laagst haalbare score is en tien de hoogst haalbare score. De kwetsbaarhedenmeting heeft tien onderdelen waarmee de volgende kwetsbaarheden in kaart worden gebracht: Verspreidt de website malware? Verspreidt de website spam? Verspreidt de mailserver spam? Zijn gevoelige gegevens van medewerkers openbaar? Kan e-mail misbruikt worden? Zijn de website, mailserver en nameserver gereed voor nieuwe standaarden?[1] Kan het websiteverkeer worden onderschept? Zijn er ongebruikelijke aanvalspaden op de website mogelijk? Worden bezoekers van de website voldoende beschermd? Is informatie over de configuratie van de website afgeschermd? Kan websiteverkeer naar de website gemanipuleerd worden?

Op basis van deze meting worden adviesrapportages opgesteld voor elke onderneming. In deze adviesrapportages staan de gevonden kwetsbaarheden omschreven. De adviesrapportage omvat tevens een handelingsperspectief zodat ondernemers weten hoe kwetsbaarheden kunnen worden verholpen. Ook is informatie opgenomen over de basisprincipes van veilig digitaal ondernemen en worden ondernemers verwezen naar webpagina's met advies over het voeren van een gesprek met de eigen IT leverancier omtrent het verbeteren van de cyberweerbaarheid van de onderneming. Wanneer de ondernemer geen IT leverancier heeft, wordt deze doorverwezen naar een webpagina waarop tips worden gegeven over het contracteren van een IT leverancier en welke afspraken hierbij kunnen worden gemaakt.

Aan de adviesrapportages is een begeleidende brief met risicocommunicatie toegevoegd. Goede risicocommunicatie kan ondernemers aansporen cybersecuritymaatregelen te treffen. Onderzoek naar het beïnvloeden van gedrag heeft laten zien dat de invloed van "geanticipeerde spijt" en "sociale norm" belangrijke voorspellende factoren zijn voor menselijk gedrag. Daarom is de risicocommunicatie in deze interventie op deze twee factoren toegespitst. Geanticipeerde spijt betreft het overwegen van spijt voorafgaand aan een gedraging; wanneer individuen verwachten spijt te krijgen wanneer zij gewenst gedrag niet vertonen, zullen zij eerder geneigd zijn het gewenste gedrag alsnog te vertonen. Daarnaast kunnen de sociale normen van vrienden, collega's en concurrenten van invloed zijn op de normen en het gedrag van ondernemers; wanneer ondernemers merken dat ondernemers om hen heen verwachten dat zij cybersecuritymaatregelen treffen, lijken meer ondernemers cybersecuritymaatregelen te treffen. In dit onderzoek is gebruik gemaakt van twee types risicocommunicatie om inzicht te verschaffen in de mate waarop de verschillende vormen van risicocommunicatie het nemen van cybersecuritymaatregelen beïnvloeden. De brief die ondernemers ontvangen bevat één van de drie mogelijke varianten op

[1] Item 6, 'Is uw website gereed voor de nieuwe internetstandaarden (IPv6)?' is niet in de totaalscore meegenomen omdat dit nog geen echte kwetsbaarheid is, dit item is puur informatief van aard voor de ondernemer.

risicocommunicatie, namelijk: 1) geen risicocommunicatie, waarbij alleen de inhoudelijke brief is toegevoegd, 2) geanticipeerde spijt als risicocommunicatie waar bovenaan de brief het citaat *"Voorkomen is goedkoper dan genezen! Werk nu aan de cyberweerbaarheid van uw bedrijf om latere kosten te voorkomen.*" is toegevoegd, en 3) sociale normen als risicocommunicatie met als bijbehorend citaat "*Ondernemers in uw regio werken hard aan hun cybersecurity, met dit rapport kunt u dit ook doen!*"

Onderzoeksmethoden

Allereerst is door een juridische partij een juridische risicobeoordeling uitgevoerd om de legitimiteit van de interventie vast te kunnen stellen.

Vervolgens zijn interviews met betrokkenen afgenomen, zijnde medewerkers van tien verschillende organisaties die zich bezighouden met de cyberweerbaarheid van ondernemingen. Zo is gesproken met medewerkers van gemeenten, overheidsorganisaties en politie om inzichten te verkrijgen in de verwachtte werkbaarheid en bruikbaarheid van de interventie en de kansen en knelpunten die zij met betrekking tot de interventie voorzien.

Tot slot is de geautomatiseerde kwetsbaarhedenmeting uitgevoerd bij 1.967 ondernemingen verdeeld over vier verschillende bedrijventerreinen. Drie van deze bedrijventerreinen zijn onderdeel van de interventiegroep, waarbij de ondernemers een adviesrapportage met de resultaten van de kwetsbaarhedenmeting, het handelingsperspectief en een variant van risicocommunicatie hebben ontvangen. Het vierde bedrijventerrein dient als controlegroep. Ondernemers in de controlegroep hebben noch een adviesrapportage noch een variant van risicocommunicatie ontvangen. De controlegroep weerspiegelt de gemiddelde verandering in cyberweerbaarheid zonder interventie. De kwetsbaarhedenmeting is twee keer uitgevoerd, in een zogenoemde voor- en nameting, waardoor de cyberweerbaarheid voor en na het ontvangen van de adviesrapportage in kaart is gebracht.

Resultaten

Deelvraag 1: Is het juridisch toegestaan om een geautomatiseerde kwetsbaarhedenmeting uit te voeren bij ondernemingen, zonder dat zij hier vooraf toestemming voor hebben gegeven?

In een juridische risicobeoordeling is vastgesteld dat de kwetsbaarhedenmeting mag worden uitgevoerd, omdat het hierbij het rechtmatig opvragen van informatie en de rechtmatige verwerking van deze informatie betreft. Als wettelijke grondslag voor de verzameling en verwerking wordt het gerechtvaardigd belang aangemerkt. Een kanttekening is dat de kwetsbaarhedenmeting alleen kwetsbaarheden mag vaststellen en dat de digitale infrastructuur van de ondernemingen niet verder mag worden binnengetreden (middels eventuele gevonden kwetsbaarheden) voor verdere metingen.

Deelvraag 2: Welke kansen en knelpunten zien betrokkenen bij het uitvoeren van een geautomatiseerde kwetsbaarhedenmeting bij Nederlandse ondernemingen?

Op basis van de gehouden interviews met betrokkenen kan worden geconstateerd dat betrokkenen binnen tien organisaties de meerwaarde van deze interventie inzien en dat de respondenten kansen zien

omtrent het gebruik van de interventie in combinatie met eigen initiatieven. De respondenten benadrukken dat de communicatie van de resultaten naar de deelnemers op een gepersonaliseerde en heldere manier dient plaats te vinden en dat duidelijk dient te zijn wat de ondernemer met deze informatie kan doen (handelingsperspectief). Door de laagdrempeligheid en schaalbaarheid van de interventie zien de respondenten kansen in de toepassing hiervan op een grote groep ondernemers. Tevens hebben de respondenten knelpunten aangekaart met betrekking tot het motiveren van de ondernemers en over de mogelijke juridische struikelblokken bij de uitvoering van de interventie. Alvorens betrokkenen al dan niet overgaan tot het verder uitrollen van de kwetsbaarhedenmeting, is de in dit rapport opgenomen juridische risicobeoordeling en pilot daarom wenselijk.

Deelvraag 3: In welke mate verandert de cyberweerbaarheid van ondernemingen na het ontvangen van de geautomatiseerde kwetsbaarhedenmeting en in hoeverre is dit vergelijkbaar tussen de verschillende bedrijventerreinen en de controlegroep?

In alle bedrijventerreinen, inclusief de controlegroep, werd een significante stijging in de gemiddelde ”totaalscore cyberweerbaarheid” waargenomen. De groep bedrijven die een adviesrapportage en de risicocommunicatievariant *geanticipeerde spijt* heeft ontvangen, toont de sterkste stijging in totaalscore. Hierna toont het bedrijventerrein dat alleen een adviesrapportage heeft ontvangen de sterkste stijging, gevolgd door de controlegroep en als laatste de groep ondernemingen die een adviesrapportage met risicocommunicatievariant *sociale norm* heeft ontvangen.

Bij een van de bedrijventerreinen uit de interventiegroep was sprake van een grotere toename van de cyberweerbaarheid dan bij de controlegroep. Het bedrijventerrein met risicocommunicatievariant *geanticipeerde spijt* liet, vergeleken met de controlegroep, een significant sterkere toename in totaalscore de voor- en nameting zien. Dit kan erop duiden dat *geanticipeerde spijt* als risicocommunicatie een effect heeft gehad op het treffen van cybersecuritymaatregelen. De bedrijventerreinen met alleen een adviesrapport of een adviesrapport in combinatie met risicocommunicatievariant *sociale norm* laten in vergelijking met de controlegroep een vergelijkbare verandering in hun totaalscore zien.

Onderzoeksbeperkingen en vervolgstappen

De interventie lijkt een positief effect te hebben gehad op de cyberweerbaarheid van de interventiegroep, maar hierbij dienen enkele kanttekeningen te worden geplaatst. Op basis van dit onderzoek kan niet worden vastgesteld welke ondernemers al dan niet daadwerkelijk kennis hebben genomen van de adviesrapportage, wat hun eventuele beweegredenen waren om de adviezen in de rapportage (niet) te volgen en of de ondernemers daadwerkelijk naar aanleiding van de adviesrapportage en/of risicocommunicatie stappen hebben ondernomen om hun cyberweerbaarheid te verbeteren. Ook is onduidelijk welke rol de risicocommunicatie gespeeld heeft in de effectiviteit van de interventie. Bovendien was het in dit onderzoek niet mogelijk rekening te houden met mogelijk relevante externe factoren die de bereidheid en mogelijkheid om kwetsbaarheden tegen te gaan kunnen beïnvloeden, zoals het aantal medewerkers, de branche en de omzet van de onderneming. Tot slot beslaat de kwetsbaarhedenmeting maar een klein deel van de cybersecurity van een onderneming en is niet met zekerheid vast te stellen of de onderzoekspopulatie representatief is voor Nederlandse ondernemingen.

Vervolgonderzoek naar de mate waarin ondernemers daadwerkelijk kennis nemen van de adviesrapportage en hun beweegredenen om naar aanleiding van de adviesrapportage al dan niet hun cyberweerbaarheid te verbeteren, is belangrijk om conclusies te kunnen trekken over het daadwerkelijke effect van de interventie. Specifieke aanknopingspunten voor vervolgonderzoek omvatten onder andere de rol die de adviesrapportage en risicocommunicatie hebben gespeeld in de overweging van ondernemers om aan hun cyberweerbaarheid te werken. Verder dient de interventie onder een grotere interventiegroep te worden getest. Ook dienen externe factoren die buiten beschouwing van het huidige onderzoek zijn gebleven, zoals als de branche, bedrijfsgrootte en omzet, in vervolgonderzoek waar mogelijk te worden geïncludeerd.

1. Inleiding

1.1. Aanleiding

Cybercriminaliteit is een veelvoorkomend probleem geworden voor Nederlandse inwoners en de op hoog tempo digitaliserende ondernemingen (CBS, 2022). Zo had in 2022 ruim 77 procent van alle Nederlandse bedrijven een bedrijfswebsite en ondernam bijna 71 procent van de ondernemingen digitaliseringsinitiatieven (CBS, 2023). Waar de digitalisering zorgt voor vooruitgang in het Nederlandse bedrijfsleven, krijgen cybercriminelen tegelijkertijd steeds meer mogelijkheden tot het plegen van cybercriminaliteit. Inmiddels heeft één op de vijf ondernemingen in Nederland te maken gehad met een vorm van cybercriminaliteit (Notté et al., 2019). Het stijgende aantal ondernemers dat slachtoffer wordt van cybercriminaliteit maakt dat het verbeteren van de cyberweerbaarheid hoog op de onderzoeksagenda behoort te staan (Hoekstra et al., 2021).

De ontwikkeling van cybersecurity bij ondernemingen lijkt echter niet op hetzelfde tempo mee te groeien als het slachtofferschap van cybercriminaliteit (Rijksoverheid, 2021; NCTV, 2021). Ondernemers in het midden- en kleinbedrijf (mkb) zijn zich vaak bewust van de mogelijke risico's die de digitale wereld met zich meebrengt en een groeiende groep ondernemers neemt cybersecuritymaatregelen om hun onderneming, personeel en klanten tegen deze risico's te kunnen beschermen (Misana-ter Huurne et al., 2020). Toch lopen nog veel ondernemers achter met het nemen van beschermende maatregelen, zoals het maken van back-ups en het updaten van software, waardoor deze ondernemingen een relatief hoger risico lopen om slachtoffer te worden van cybercriminaliteit (Munnichs et al., 2017; Veenstra et al., 2015). Het is daarom van belang onderzoek uit te voeren naar de cyberweerbaarheid van ondernemingen in het mkb en naar welke factoren de cyberweerbaarheid kunnen bevorderen.

Een manier om inzicht te verkrijgen in de huidige stand van zaken omtrent de cyberweerbaarheid van een onderneming, is via een cyberscan. Overheidsinstanties en commerciële organisaties bieden veelvuldig cyberscans aan, onder andere door middel van het invullen van vragenlijsten, uitgebreide *vulnerability scanning*[2] of een snelle, automatische scan op een gratis website. Ondanks dat deze cyberscans op grote schaal worden aangeboden, vindt weinig tot geen onderzoek plaats naar de effecten van deze scans. Bovendien worden met het aanbieden van cyberscans alleen ondernemers bereikt die geïnteresseerd zijn in, of actief zijn op het gebied van cybersecurity. Om deze redenen is het project "Evidence based cybersecurity gedragsinterventie" gericht op drie basisprincipes van digitaal veilig ondernemen" opgezet.

In dit project hebben onderzoekers van De Haagse Hogeschool een interventie ontwikkeld waarbij door middel van een geautomatiseerde kwetsbaarhedenmeting bij ondernemingen naar zwakke plekken in de digitale infrastructuur wordt gezocht. Voor de meting wordt gebruik gemaakt van *open source*[3] data. De resultaten van deze meting geven de ondernemer inzicht in een deel van hun cyberweerbaarheid. Het is een goede eerste stap naar de verbetering van cyberweerbaarheid bij ondernemers in het mkb.

De kwetsbaarhedenmeting is op drie bedrijventerreinen uitgevoerd, alsook op een controlegroep op een vierde terrein. In totaal zijn twee metingen uitgevoerd, beginnende met een voormeting waarbij

[2] Kwetsbaarhedenmeting. Het scannen van een digitale infrastructuur op zwakke plekken.
[3] Data die in beginsel vrij toegankelijk is voor elke internetgebruiker.

de toen geldende stand van zaken omtrent de cyberweerbaarheid van de ondernemingen werd vastgesteld. Na de voormeting is de adviesrapportages in combinatie met risicocommunicatie en handelingsperspectief verzonden naar de ondernemers. Zeven weken na verzending van de resultaten van de meting is er een nameting uitgevoerd om eventuele verschillen in cyberweerbaarheid te kunnen meten.

In dit rapport zijn de resultaten van de interventie beschreven. Aan de hand van statistische analyses zijn de effecten van de interventie gemeten en is getracht een antwoord te geven op het vraagstuk van hoe ondernemers kunnen worden aangespoord om hun cyberweerbaarheid te verbeteren.

Onderzoekers van De Haagse Hogeschool werkten in dit project samen met cybersecuritybedrijf Threadstone en professionals van het Platform Veilig Ondernemen (PVO) Den Haag. Threadstone heeft de kwetsbaarhedenmeting ontwikkeld en uitgevoerd.

1.2. Doelstelling

Dit onderzoek heeft tot doel een interventie te toetsen die zich richt op het vergroten van de cyberweerbaarheid van ondernemers door middel van een geautomatiseerde kwetsbaarhedenmeting. Tevens wordt getracht inzichten te verschaffen in de manier waarop en in welke mate verschillende vormen van risicocommunicatie de keuze beïnvloeden om cybersecuritymaatregelen te treffen. Het doel van dit rapport is drieledig. Allereerst wordt de interventie zelf beschreven. Hierop volgend worden de resultaten van de effectmeting van de interventie besproken. Als laatste worden aanbevelingen gedaan voor de doorontwikkeling en toepassing van de interventie.

1.3. Onderzoeksvragen

De volgende onderzoeksvraag staat centraal in dit rapport:

> *In hoeverre is het mogelijk, toegestaan en effectief om een geautomatiseerde kwetsbaarhedenmeting uit te voeren ter bevordering van de cyberweerbaarheid van Nederlandse ondernemingen?*

Om tot een antwoord op de hoofdvraag te kunnen komen, worden de volgende deelvragen behandeld:

1. Is het juridisch toegestaan om een geautomatiseerde kwetsbaarhedenmeting uit te voeren bij ondernemingen, zonder dat zij hier vooraf toestemming voor hebben gegeven?
2. Welke kansen en knelpunten zien betrokkenen in het uitvoeren van een geautomatiseerde kwetsbaarhedenmeting bij Nederlandse ondernemingen?
3. In welke mate verandert de cyberweerbaarheid van ondernemingen na het ontvangen van de geautomatiseerde kwetsbaarhedenmeting en in hoeverre is dit vergelijkbaar tussen de verschillende bedrijventerreinen en de controlegroep?

1.4. Leeswijzer

In hoofdstuk 2 is een overzicht gegeven van de bestaande literatuur over cyberweerbaarheid en cyberscans en wordt de theoretische grondslag van de interventie besproken. In Hoofdstuk 3 wordt de interventie zelf in algemene zin beschreven. Hoofdstuk 4 bevat een omschrijving van de gebruikte onderzoeksmethoden. De resultaten worden in hoofdstuk 5 beschreven en in hoofdstuk 6 zijn de bijbehorende conclusies en een discussie opgenomen.

2. Theorie en eerder onderzoek

In dit hoofdstuk wordt een beschrijving gegeven van de relevante theorie en bestaand onderzoek. Inzichten uit de theorie en eerder onderzoek ondersteunen de interventie die is uitgelicht in dit onderzoek. In dit hoofdstuk staat beschreven wat kan worden verstaan onder cyberweerbaarheid (2.1.), verschillende vormen van cyberscans zijn en waar mogelijk hun effectiviteit (2.2.) en ten slotte is er een theoretische onderbouwing opgenomen voor het gebruik van de verschillende vormen van risicocommunicatie, zijnde geanticipeerde spijt en sociale norm (2.3.).

2.1. Cyberweerbaarheid

Deze paragraaf zal ingaan op de in dit rapport gehanteerde definitie van cyberweerbaarheid (2.1.1.) en de basisprincipes van cybersecurity waarmee in dit onderzoek is gewerkt (2.1.2.).

2.1.1. Definities

Ondanks dat veel ondernemers zich bewust zijn van de risico's van cybercriminaliteit, blijft een grote groep ondernemers toch achter met het nemen van beschermende maatregelen om hun cyberweerbaarheid te verhogen (CBS, 2022; Munnichs et al., 2017; Veenstra et al., 2015). Cyberweerbaarheid is "het vermogen van een organisatie om cyberincidenten te kunnen weerstaan, hierop te kunnen reageren en ervan te kunnen herstellen om de operationele continuïteit van de organisatie te kunnen waarborgen" (Hausken, 2020). Cyberweerbaarheid heeft betrekking op het nemen van cybersecurity maatregelen en het vertonen van zelfbeschermend gedrag met betrekking tot cybercriminaliteit (Misana-ter Huurne et al., 2021a; Van der Kleij & Leukfeldt, 2019). Ook de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) ziet cyberweerbaarheid niet alleen als het treffen van cybersecuritymaatregelen om relevante risico's in te perken, maar voegt hieraan toe dat cyberweerbaar zijn ook te maken heeft met hoe er op cyberincidenten wordt gereageerd (NCTV, 2022).

2.1.2. Basisprincipes van cybersecurity

Verschillende instanties hebben hulpmiddelen ontwikkeld om ondernemers te ondersteunen in het verbeteren van hun cyberweerbaarheid. Eén van deze ondersteunende instanties is het Digital Trust Center (DTC). Het DTC is door het Ministerie van Economische Zaken en Klimaat in het leven geroepen om ondernemers in Nederland bij te staan met advies en hulpmiddelen om veilig digitaal te kunnen ondernemen. Zij hebben vijf basisprincipes van veilig digitaal ondernemen ontwikkeld om ondernemers te helpen de basis van cybersecurity op orde te brengen en hiermee hun cyberweerbaarheid te vergroten. Deze principes staan hieronder verder uitgelegd (DTC, z.d.):

- Inventariseer kwetsbaarheden binnen de onderneming: het is van belang te inventariseren waar de zwakke plekken binnen de digitale infrastructuur van een onderneming zich bevinden. Dit omvat bijvoorbeeld het identificeren van de belangrijkste systemen en wat er gebeurt als deze niet meer werken. Door inzicht te verkrijgen in de relevante risico's binnen de organisatie kunnen gerichte maatregelen worden genomen om de cyberweerbaarheid te vergroten.

- Kies veilige instellingen: wanneer nieuwe en bestaande software moet worden gebruikt, is het van belang dat de instellingen worden gecontroleerd voordat de software wordt gebruikt. Soms staan er functies onnodig automatisch aan of staan bepaalde instellingen niet goed afgesteld op de behoeften van de gebruiker. Ook het aanmaken van sterke wachtwoorden, multi-factor authenticatie (MFA) en het gebruik van firewalls valt hieronder. Deze maatregelen kunnen er voor zorgen dat de digitale infrastructuur van de onderneming beter is beveiligd.
- Voer updates regelmatig uit: het is van belang alle apparaten binnen de organisatie die zijn verbonden met een netwerk regelmatig te updaten. Updates zorgen ervoor dat niet alleen de software blijft werken, maar ook dat beveiligingsupdates worden uitgevoerd om het risico op slachtofferschap van cybercriminaliteit zo laag mogelijk te houden.
- Beperk de toegang tot systemen: om een onderneming zo veilig mogelijk te houden, is het van belang dat alleen de medewerkers die toegang tot bepaalde systemen of ruimtes nodig hebben deze daadwerkelijk krijgen. Dit kan per medewerker of afdeling worden gedefinieerd waardoor niet onnodig toegang wordt verschaft aan medewerkers die dit niet nodig hebben.
- Voorkom virussen en andere malware: virussen en andere malware kunnen er voor zorgen dat bepaalde systemen binnen een organisatie niet of nauwelijks meer kunnen worden gebruikt. De bedrijfsvoering kan ernstig worden verstoord en kan voor hoge financiële- en reputatieschade zorgen. Virussen kunnen worden voorkomen door het gebruik van een antivirusprogramma, medewerkers te stimuleren zich online veilig te gedragen en de installatie van software te beperken tot vertrouwde programma's.

Deze vijf basisprincipes van veilig digitaal ondernemen kunnen er gezamenlijk voor zorgen dat de digitale veiligheid van ondernemers op een laagdrempelige manier kan worden gewaarborgd.

2.2. Cyberscans

Cyberscans helpen de ondernemer inzicht te verkrijgen in de cyberweerbaarheid van hun onderneming. Er is een grote hoeveelheid en verscheidenheid aan organisaties en websites die on- en offline cyberscans aanbieden. In deze paragraaf zullen de twee meest aangeboden varianten worden besproken: handmatige cyberscans en geautomatiseerde cyberscans. Waar mogelijk zal de effectiviteit van deze scans worden besproken.

De eerste variant die zal worden beschreven is de handmatige cyberscan. Er is een grote verscheidenheid aan dergelijke cyberscans beschikbaar om de digitale infrastructuur van een onderneming te kunnen testen op kwetsbaarheden. Zo worden cyberscans bijvoorbeeld in de vorm van vragenlijsten online aangeboden door overheidsorganen als het DTC met hun Basisscan Cyberweerbaarheid (DTC, z.d.), maar ook door particuliere verzekeringsmaatschappijen als de Cyberscan van Interpolis en de Allianz Cyber Risicoscan. Dergelijke vragenlijsten kunnen online door de ondernemer worden ingevuld zodat aan de hand van verschillende stellingen en vragen een beeld wordt verkregen van het huidige niveau van hun cyberweerbaarheid. In deze 'handmatige' cyberscans moet echter veel tijd en werk worden gestoken door de ondernemer om een compleet beeld van de cybersecurity van een onderneming te vergaren (Wang et al., 2019). Een ander belangrijk nadeel is dat de scans volledig of deels

zijn gebaseerd op zelf-gerapporteerde antwoorden van de onderzochte onderneming. Het beeld dat uit een dergelijke scan naar voren komt kan daarom afwijken van de daadwerkelijke cyberweerbaarheid van een organisatie (Van ’t Hoff-de Goede et al., 2019).

Voor een meer compleet en objectiever beeld kunnen handmatige cyberscans ook door een cybersecurityprofessional worden uitgevoerd. Hierbij gaat de professional langs bij een ondernemer om gezamenlijk de cyberscan door te lopen. Grote financiële dienstverleners als Nationale Nederlanden, maar ook particuliere cybersecuritybedrijven bieden cyberscans door cyberprofessionals aan. Eerder zijn ook pilot-onderzoeken gedaan voor overheidsprojecten als MKB Cyber Buddy’s, waar cybersecuritystudenten een cyberscan hebben uitgevoerd bij ondernemingen (Van ’t Hoff-de Goede et al., 2022). De ondernemer moet hiervoor zelf inzicht verschaffen in de huidige stand van zaken omtrent hun cybersecurity. Een voordeel van uitvoering van deze handmatige scans door een professional is dat er snel een uitgebreider beeld kan worden verkregen van de cybersecurity binnen een organisatie dan wanneer de ondernemer de cyberscan zelf afneemt. De professional kan in de beoordeling (de *assessment*) ook de bedrijfsvoering verwerken en kan hierop een op maat gemaakt cyberweerbaarheidsplan opstellen voor de ondernemer. Ook heeft de cybersecurityprofessional vaak meer kennis over cyberweerbaarheid dan de ondernemer zelf, waardoor kwetsbaarheden die anders over het hoofd worden gezien wél worden aangekaart. Een nadeel van dit proces is dat deze scans duurder zijn omdat de uren van de professional ook in rekening worden gebracht.

Voor een completer beeld van mogelijke risico’s binnen de digitale infrastructuur van een onderneming, kan de ondernemer een geautomatiseerde cyberscan uit laten voeren. Een bekende uitvoering hiervan is de (*network) vulnerability scanner,* meestal in de vorm van software die de digitale infrastructuur scant op kwetsbaarheden (Werlinger et al., 2021; Holm et al., 2011). Bekende uitgevers hiervan zijn bijvoorbeeld Nessus en Acunetix. Bij gebruik van dergelijke digitale cyberscans wordt de digitale infrastructuur van een onderneming automatisch gescand en worden de resultaten hiervan vergeleken met de kwetsbaarheden die op dit moment bekend zijn, zoals opgenomen in een kwetsbaarhedendatabase. Vaak ontvangt de ondernemer na de scan een rapportage waarin de gevonden kwetsbaarheden op risiconiveau zijn ingedeeld. Hiermee is het mogelijk om, in vergelijking met de handmatige scans, zowel snel en efficiënt de zwakke plekken in de infrastructuur van het netwerk aan te tonen (Holm et al., 2011), als het continu scannen van de digitale infrastructuur op nieuwe kwetsbaarheden (Rennhard et al., 2019). Deze geautomatiseerde scans worden vaak door particuliere cybersecurityondernemingen aangeboden en kunnen, zeker in combinatie met advies naar aanleiding van de resultaten, erg duur zijn. Tevens zijn digitale kwetsbaarhedenscanners niet altijd volledig of up-to-date met de nieuwste kwetsbaarheden, waardoor er van meerdere scanners tegelijkertijd gebruik zou moeten worden gemaakt voor volledig uitsluitsel.

Hoewel geautomatiseerde cyberscans door particuliere cybersecurityondernemingen vaak erg duur kunnen zijn, bestaan er ook gratis online automatische scans. Zo kan de beveiliging van een internetdomein en e-mailadressen bijvoorbeeld oppervlakkig worden gescand op internet.nl. Hierbij wordt onder andere gekeken welke beveiligingscertificaten worden ondersteund en of HTTPS[4] correct staat ingesteld. Ook de website haveibeenpwnd.com voert een geautomatiseerde variant van de cyberscan uit. Op basis van een ingevuld e-mail adres wordt automatisch gecontroleerd of dit e-mail

[4] Dit protocol versleutelt de communicatie tussen een website en een bezoeker.

adres, in het geval van een gebruikersaccount vaak in combinatie met het bijbehorende wachtwoord, bij een datalek betrokken is geweest en deze gegevens dus op het internet zijn te achterhalen. Deze varianten op de gratis geautomatiseerde cyberscan zijn twee veel gebruikte voorbeelden, maar online zijn er meer van dit soort scans te vinden. Een voordeel van deze cyberscans is dat het gratis en zeer snel is, maar deze varianten op de cyberscan belichten maar een zeer klein deel van de cybersecurity en bieden geen uitgebreid, professioneel advies over het verhelpen van de gevonden kwetsbaarheden.

Binnen de wetenschap is nog weinig onderzoek gedaan naar de daadwerkelijke effecten van cyberscans. Veel van de evaluaties van cyberscans betreffen één specifieke scan of scanvariant, waardoor het niet mogelijk is om algemene conclusies te trekken over de werkbaarheid en effectiviteit van de cyberscans. Hierdoor is er een grote behoefte aan empirisch onderbouwde cyberscans, waarbij de effectiviteit van de cyberscans wordt gemeten. Effectieve cyberscans kunnen ondernemers namelijk aansporen om maatregelen te treffen om hun cyberweerbaarheid te verbeteren.

2.3. Risicocommunicatie

In combinatie met een cyberscan kan goede risicocommunicatie ondernemers aansporen om cybersecuritymaatregelen te treffen (Misana-ter Huurne et al., 2021b). Dergelijke risicocommunicatie kan voor individuen en organisaties van belang zijn om te weten welke risico's zij lopen, gemotiveerd te worden om stappen te nemen en geïnformeerde beslissingen te nemen ten aanzien van mogelijke risico's (Bongers et al., 2021; Nurse et al., 2011). Voor een goede risicocommunicatie is een duidelijke boodschap nodig waarin de ernst van het risico staat beschreven (Frewer, 2004). Deze paragraaf belicht twee factoren die binnen de risicocommunicatie kunnen worden ingezet om de motivatie om cybersecuritymaatregelen te treffen te vergroten, namelijk *geanticipeerde spijt* (2.3.1.) en sociale norm (2.3.2.).

2.3.1. Geanticipeerde spijt

Het nemen van beslissingen wordt deels beïnvloed door de kans op spijt na het vertonen van gedrag (Carfora et al., 2017; Lazuras et al., 2017; Verkijika, 2019). Spijt is een negatieve emotie en komt voor wanneer een situatie voordeliger had kunnen uitpakken als andere keuzes waren gemaakt (Gilovich & Medvec, 1995; Sandberg & Conner, 2008; Schwarz et al., 2014). Het voorafgaand aan een besluit overwegen van spijt staat bekend als *geanticipeerde spijt*: "een verwachte negatieve, affectieve respons op ongewenste uitkomsten" (Lazuras et al., 2017). Anticiperen op spijt kan het gedrag van een individu beïnvloeden, waarbij het individu tracht de kans op spijt te minimaliseren (Abraham & Sheeran, 2003; Janis & Mann, 1977; Loomes & Sugden, 1982; Shih & Schau, 2011; Zeelenberg, 1999). Met andere woorden, wanneer mensen verwachten spijt te krijgen wanneer zij gewenst gedrag nalaten, zullen zij eerder geneigd zijn dit gewenste gedrag alsnog te vertonen. Wanneer binnen interventies gericht op gedragsverandering gebruik wordt gemaakt van geanticipeerde spijt, kan hiermee de kans op het beoogde gedrag worden verhoogd (Bongers et al., 2021).

Een groot deel van de huidige literatuur omtrent geanticipeerde spijt heeft betrekking op interventies buiten cybersecurity, zoals het gebruik van condooms (Richard et al., 1996), wel of niet beginnen met roken als adolescent (Conner et al., 2006) en bieden bij veilingen (Filiz-Ozbay & Ozbay,

2007). Ook het Postcode Loterij-voorbeeld van Zeelenberg (1999) laat zien dat wanneer een individu de mogelijkheid op spijt anticipeert, deze sneller geneigd is een Postcode Loterij-lot te kopen. Deze conclusie wordt toegeschreven aan het feit dat het individu de uitkomst van de Postcode Loterij altijd te weten komt, waardoor spijt niet kan worden voorkomen wanneer er geen lot is gekocht (Zeelenberg, 1999).

De invloed van spijt en geanticipeerde spijt op gedrag is binnen de cybersecurity nog weinig belicht (Renaud et al., 2022). Eerder werk laat wel zien dat geanticipeerde spijt een positieve invloed heeft op de intentie van medewerkers van organisaties om cyberveilig gedrag te vertonen (Sommestad et al., 2015). Hierop voortbouwend is waargenomen dat geanticipeerde spijt een positieve invloed heeft op zelf-gerapporteerd veilig gedrag bij het gebruik van smartphones (Verkijika, 2018). Hoewel al enkele onderzoeken zijn uitgevoerd om de invloed van geanticipeerde spijt op veilig cybergedrag te kunnen duiden, is het van belang deze kennis uit te breiden door op dit gebied meer onderzoek te verrichten.

2.3.2. Sociale norm

Ook onze sociale omgeving heeft grote invloed op ons gedrag (Geber et al., 2021). De normen van vrienden, collega's en concurrenten kunnen van invloed zijn op de normen en het gedrag van ondernemers (Das et al., 2015; Das, 2016). Individuen observeren hun vakgenoten of leeftijdsgenoten en daarbij ook het gedrag wat binnen deze groepen wordt vertoond. Het eigen gedrag wordt hierop gebaseerd zodat dit overeenkomt met de gehanteerde sociale norm binnen de desbetreffende groep (Cialdini et al., 1990; Geber et al., 2021). Sociale normen kunnen derhalve cyberveilig gedrag beïnvloeden (Das et al., 2014; Das, 2016; Rader et al., 2012). Ondernemers kunnen bijvoorbeeld te horen krijgen dat hun concurrenten cybersecuritymaatregelen hebben getroffen, waardoor zij zelf ook sneller geneigd zijn extra stappen te zetten om hun eigen cybersecurity op een hoger niveau te tillen (Bongers et al., 2021; Das, 2016; Misana-ter Huurne et al., 2020).

Sociale norm is eerder toegepast in onderzoek naar gedrag in verschillende domeinen zoals belastingontduiking (Kahan, 2019), recycling (Schultz, 1999) en milieubewust gedrag (De Groot et al., 2021). Ook in cybersecurityonderzoek werd de sociale norm onderzocht. Het observeren van gedragingen in de nabije omgeving van een individu kan ervoor zorgen dat cybersecuritymaatregelen die voorheen niet genomen werden alsnog worden genomen (Li et al., 2019; Pfleeger & Caputo, 2012). Zo kan bijvoorbeeld het instellen van een beveiligingscode voor een telefoon in de hand worden gewerkt doordat dit door een individu als de norm wordt gezien binnen de eigen sociale kringen (Das, 2016). Later is onder 1.020 ondernemers onderzoek gedaan middels een vragenlijst, waaruit bleek dat de invloed van de sociale omgeving een belangrijke voorspeller van gedrag is naast diverse andere factoren als zelfeffectiviteit en affectieve respons (Misana ter Huurne et al., 2021b). Kortom: wanneer ondernemers het gevoel hebben dat andere ondernemers om hen heen verwachten dat zij zichzelf beschermen tegen cybercriminaliteit, lijken meer ondernemers zelfbeschermende maatregelen te treffen.

3. De geautomatiseerde kwetsbaarhedenmeting

In dit hoofdstuk staat beschreven wat de geautomatiseerde kwetsbaarhedenmeting is (3.1.) en uit welke onderdelen de meting bestaat (3.2.). Verder worden het adviesrapport, de risicocommunicatie en het handelingsperspectief besproken (3.3.). Het hoofdstuk wordt afgesloten met enkele beperkingen van de interventie (3.4.).

3.1. Wat is de geautomatiseerde kwetsbaarhedenmeting?

In de huidige paragraaf gaan we in op de kwetsbaarhedenmeting die in dit onderzoek getoetst is. Deze kwetsbaarhedenmeting onderscheidt zich van de hiervoor beschreven cyberscans omdat deze kwetsbaarhedenmeting niet op initiatief van de ondernemer, maar op initiatief van een overkoepelende organisatie, zoals een gemeente of brancheorganisatie, wordt uitgevoerd voor een grote groep ondernemingen tegelijkertijd. De geautomatiseerde kwetsbaarhedenmeting controleert de openbaar-bereikbare digitale infrastructuur van ondernemingen op kwetsbaarheden in de cyberweerbaarheid, op basis van de domeinnaam van de bedrijfswebsite. De resultaten van deze meting worden in een op maat gemaakte adviesrapportage met risicocommunicatie en handelingsperspectief opgenomen, waarna deze worden verstrekt aan de ondernemers. Met behulp van de rapportage kunnen ondernemers stappen nemen om hun cyberweerbaarheid te vergroten. De geautomatiseerde kwetsbaarhedenmeting maakt het mogelijk om na een bepaalde periode de cyberweerbaarheid van alle bedrijven opnieuw te meten, waarna beide metingen met elkaar worden vergeleken. Door meer dan één keer te meten wordt een temporeel beeld gecreëerd van de cyberweerbaarheid van de ondernemingen.

De geautomatiseerde kwetsbaarhedenmeting is door cybersecurityorganisatie Threadstone ontwikkeld om op een efficiënte manier mogelijke kwetsbaarheden in de digitale infrastructuur van ondernemingen in kaart te kunnen brengen. De geautomatiseerde kwetsbaarhedenmeting maakt gebruik van openbaar toegankelijke informatie over de digitale infrastructuur van ondernemingen. De rechtmatigheid van deze werkwijze is getoetst middels een juridische risicobeoordeling. De risicobeoordeling is aangevraagd om de mogelijke juridische risico's omtrent het uitvoeren van de geautomatiseerde kwetsbaarhedenmeting in kaart te brengen. De resultaten van de juridische risicobeoordeling komen later aan bod. De volledige beoordeling is in Bijlage I opgenomen.

3.2. Onderdelen van de kwetsbaarhedenmeting

De geautomatiseerde kwetsbaarhedenmeting controleert de openbaar bereikbare digitale infrastructuur van ondernemers op de volgende mogelijke kwetsbaarheden (Tabel 1):

Tabel 1: Definiëring controles kwetsbaarheden

#	Controle	Toelichting
1	Verspreidt de website malware?	Er wordt gecontroleerd of de website voorkomt op zwarte lijsten voor malware, zogenaamde *malware blacklists*. Op deze blacklists worden websites bijgehouden

		waarvan bekend is dat ze malware (malafide software, virussen etc.) verspreiden.
2	Verspreidt de website spam?	Er wordt gecontroleerd of de website voorkomt op zwarte lijsten voor spam, zogenaamde *spam blacklists*. Op deze blacklists worden websites bijgehouden waarvan bekend is dat ze spam (ongewenste e-mail) verspreiden.
3	Verspreidt de mailserver spam?	Er wordt gecontroleerd of de mailserver voorkomt op spam blacklists. Op deze blacklists worden mailservers bijgehouden waarvan bekend is dat ze spam (ongewenste e-mail) wordt verspreiden.
4	Zijn gevoelige gegevens van medewerkers openbaar?	Er wordt gecontroleerd of e-mailadressen die bij het domein horen, betrokken zijn bij datalekken middels vergelijking met gelekte lijsten.
5	Kan e-mail misbruikt worden?	De instellingen van de mailserver worden gecontroleerd. Als de mailserver niet correct is ingesteld, kan dit betekenen dat criminelen uit naam van de organisatie e-mails kunnen versturen.
6	Zijn de website, mailserver en nameserver gereed voor nieuwe standaarden? *De resultaten van dit item zijn illustratief voor de ondernemer en zijn niet meegenomen in de berekening van de totaalscore.*	Er wordt gecontroleerd of de website, mailserver en nameserver de nieuwste internetprotocollen ondersteunen (IPv6).
7	Kan het websiteverkeer worden onderschept?	Er wordt gecontroleerd of het verkeer tussen de website en de bezoekers versleuteld is. Een bezoeker ziet dit aan een groen slotje links in de browser (https).
8	Zijn er ongebruikelijke aanvalspaden mogelijk?	Er wordt gecontroleerd welke poorten er op de server van de website “open” staan. Hoe meer poorten er open staan, hoe meer aanvalspaden een crimineel heeft om op de website in te breken.
9	Worden bezoekers van de website voldoende beschermd?	Er wordt gecontroleerd of communicatie op de browser van de websitebezoeker niet kan worden gemanipuleerd. Dit wordt gedaan door na te gaan of securityprotocollen op de juiste wijze worden afgedwongen op de browser van bezoekers van de website.
10	Is de informatie over de configuratie van de website voldoende beschermd?	Er wordt gecontroleerd of kan worden herleid welke software(versies) door de website wordt gebruikt. Een crimineel kan met deze kennis gerichte aanvallen uitvoeren.
11	Kan websiteverkeer naar de website gemanipuleerd worden?	Er wordt gecontroleerd of bezoekers die naar de domeinnaam gaan ook altijd op de desbetreffende website terechtkomen (en niet worden omgeleid naar een nep-website van een crimineel).

3.3. Adviesrapportage, handelingsperspectief en risicocommunicatie

De resultaten van de geautomatiseerde kwetsbaarhedenmeting worden na afloop van de meting in een adviesrapportage opgenomen. Hierbij wordt een korte toelichting per kwetsbaarheid gegeven en een beschrijving van de maatregelen die nodig zijn om de kwetsbaarheid te verhelpen. Deze adviesrapportage wordt voor elke onderneming op maat opgesteld, waardoor alle ondernemingen een uniek rapport krijgen. Het komt voor dat er meer dan één bedrijf onder hetzelfde domein valt; in dat geval ontvangt de ondernemer een rapportage voor het desbetreffende domein, waarbij de rapportage is gericht aan meerdere bedrijven. De resultaten zijn dus wel van één unieke domeinnaam.

De adviesrapportage eindigt met een handelingsperspectief waarin ondernemers worden opgeroepen met hun cyberweerbaarheid aan de slag te gaan. Het handelingsperspectief is zo ontworpen dat de ondernemers worden aangespoord met hun IT leverancier in gesprek te gaan over eventueel gevonden kwetsbaarheden. Wanneer de ondernemer (nog) geen IT leverancier heeft, wordt deze aangespoord de mogelijkheden tot het in de hand nemen van een IT leverancier te verkennen. Om hierbij te helpen bevat het handelingsperspectief QR-codes die naar relevante webpagina's van het DTC leiden om de ondernemer van algemene informatie te kunnen voorzien. De webpagina's bieden informatie over het maken van afspraken met een nieuwe IT leverancier[5] of het gesprek voeren over cybersecurity met de al aangestelde IT leverancier[6].

De adviesrapportage wordt vergezeld door een begeleidende brief. Er zijn drie varianten op de begeleidende brief: twee varianten met een vorm van risicocommunicatie en één variant zonder risicocommunicatie. De risicocommunicatie is als een citaat aan de begeleidende brief toegevoegd. Zoals eerder beschreven zijn deze verschillende vormen van risicocommunicatie: geanticipeerde spijt (zie ook 2.3.1.1.) en sociale norm (zie ook 2.3.1.2.). Wanneer een individu vooraf mogelijke spijt anticipeert door het al dan niet vertonen van een gedraging, heet dit geanticipeerde spijt. Voor geanticipeerde spijt is het citaat *"Voorkomen is goedkoper dan genezen! Werk nu aan de cyberweerbaarheid van uw bedrijf om latere kosten te voorkomen.*" gebruikt. De sociale norm speelt in op de omgeving van een individu of organisatie en de gedragingen die in deze omgeving als norm worden gezien. Deze sociale norm beïnvloedt het gedrag van anderen in dezelfde sociale omgeving. Voor sociale norm is het bijbehorende citaat in de begeleidende brief "*Ondernemers in uw regio werken hard aan hun cybersecurity, met dit rapport kunt u dit ook doen!*"

3.4. Beperkingen

De geautomatiseerde kwetsbaarhedenmeting en bijbehorende rapportage kennen enkele beperkingen waarmee in dit onderzoek rekening moet worden gehouden. Ten eerste wordt maar een beperkte hoeveelheid kwetsbaarheden gemeten. Alleen openbare bronnen worden bekeken, waardoor een groot deel van de cybersecurity van de ondernemingen onbelicht blijft. Dit betekent dat maar een klein deel van alle mogelijke cybersecuritykwetsbaarheden gemeten wordt in de interventie. Het betreft als het ware het topje van de ijsberg en hoewel het ondernemers aanspoort de belangrijke eerste stappen

[5] https://www.digitaltrustcenter.nl/informatie-advies/afspraken-maken-met-een-it-leverancier
[6] https://www.digitaltrustcenter.nl/gesprek-met-it-dienstverlener

richting cyberweerbaarheid te zetten, is het cybersecurityproces niet afgerond wanneer zij de gevonden kwetsbaarheden hebben verholpen. De bijgevoegde informatiefolder van het DTC wijst ondernemers op de beginstappen die kunnen worden genomen ter verbetering van de cyberweerbaarheid van de onderneming. Hiermee kunnen ondernemers zich verder bewapenen tegen cybercriminelen dan wanneer zij alleen de opgestuurde adviesrapportage gebruiken.

Een tweede beperking ligt in het feit dat niet alle onderdelen van de meting een resultaat opleveren. Per bedrijf kan het voorkomen dat één of meer van de gemeten onderdelen van de infrastructuur geen resultaat oplevert. Dit kan komen doordat bepaalde onderdelen niet in elke infrastructuur terug te vinden zijn, waardoor de test niet kan worden uitgevoerd. In de resultaten staat deze uitkomst aangegeven als “onbekend”.

Een derde beperking is dat hoewel dit project juist de ondernemers bereikt die zich niet hebben opgegeven voor hulp met betrekking tot hun cybersecurity, er beperkt zicht is op het bereik dat het project heeft. Zo is het niet bekend in hoeverre ondernemers de rapportage openen, lezen en waarderen, mede doordat deze met de post wordt verzonden. Ook is niet bekend in hoeverre ondernemers van plan zijn op de lange termijn met de resultaten aan de slag te gaan, alleen welke ondernemers dit na bepaalde tijd ook daadwerkelijk doen. Hoewel terwijl het project tot doel heeft ondernemers aan te zetten om extensievere maatregelen ter vergroting van cyberweerbaarheid te treffen dan voorheen, kan alleen gemeten worden in hoeverre de kwetsbaarheden die onderdeel zijn van de kwetsbaarhedenmeting veranderen door de tijd heen.

4. Methoden

In dit hoofdstuk worden de gebruikte onderzoeksmethoden besproken. Allereerst zal worden ingegaan op de steekproef (4.1.), vervolgens wordt de definiëring van de items van de kwetsbaarhedenmeting besproken (4.2.), waarna in zal worden gegaan op de dataverwerking (4.3.). Ten slotte worden de verschillende statistische analysemethoden beschreven (4.4.).

4.1. Steekproef

Voor de uitvoering van dit onderzoek is gebruik gemaakt van twee verschillende steekproeven. Ter beantwoording van deelvraag 2 (de kansen en knelpunten die betrokkenen zien bij het uitvoeren van een geautomatiseerde kwetsbaarhedenmeting) zijn interviews gehouden met professionals in het werkveld van digitale veiligheid van ondernemers (4.1.1.). Ter beantwoording van deelvraag 3 (de mate waarin de cyberweerbaarheid van ondernemingen verandert na het ontvangen van de geautomatiseerde kwetsbaarhedenmeting en in hoeverre is dit vergelijkbaar tussen de verschillende groepen) is een steekproef van ondernemingen samengesteld (4.1.2.).

4.1.1. Expertinterviews

Eén van de doelen van dit onderzoek was te onderzoeken welke knelpunten betrokkenen zien bij de kwetsbaarhedenmeting. Teneinde dit in kaart te brengen zijn interviews gehouden met betrokkenen. De onderzoekers hebben experts benaderd werkzaam bij overheidsorganisaties die in enige vorm werkzaamheden uitvoeren om de (digitale) veiligheid van ondernemers te verbeteren. De respondenten zijn via het eigen netwerk van de onderzoekers benaderd, waarna gebruik is gemaakt van de sneeuwbalmethode om verdere respondenten te werven. In totaal zijn dertien professionals van tien verschillende overheidsorganisaties geïnterviewd. De interviews duurden minimaal 28 minuten en maximaal één uur en zes minuten met een gemiddelde van ongeveer 49 minuten (tabel 2).

Tabel 2: respondentenoverzicht voor interviews met betrokkenen

Organisatie	Respondent	Lengte interview	Soort organisatie
A	A1 & A2	01:06:22	Overheidsorganisatie
B	B1 & B2	00:50:50	Overheidsorganisatie
C	C1	00:56:24	Gemeente
D	D1	00:28:24	Overheidsorganisatie
E	E1	01:04:41	Politie eenheid
F	F1	00:36:42	Overheidsorganisatie
G	G1	00:37:20	Gemeente
H	H1	00:57:05	Gemeente
I	I1	00:47:36	Gemeente
J	J1 & J2	00:49:13	Overheidsorganisatie

In deze semigestructureerde interviews zijn de experts bevraagd naar hun meningen en ideeën met betrekking tot de interventie. Tijdens de interviews zijn onder andere de bruikbaarheid van de interventie voor de eigen organisatie en waar zij deze eventueel willen of kunnen toepassen besproken met de respondenten. Tevens is gesproken over de meest geschikte manier waarop de resultaten van de interventie naar de deelnemers kan worden gecommuniceerd. Ook zijn hier mogelijke struikelblokken en complicaties met betrekking tot de uitvoering van de interventie besproken. De exacte onderwerpen staan opgenomen in het interviewprotocol (bijlage II).

4.1.2. Geautomatiseerde kwetsbaarhedenmeting

De steekproef van de geautomatiseerde kwetsbaarhedenmeting omvatte ondernemingen in de regio Den Haag op drie bedrijventerreinen: hier aangeduid als Bedrijventerrein 1, Bedrijventerrein 2 en Bedrijventerrein 3. Er is gekozen voor geografische afbakening van de betrokken ondernemingen in de regio, omdat deze afbakening resulteert in een duidelijk begrensde groep met een grote verscheidenheid aan branches. De drie verschillende bedrijventerreinen zijn geselecteerd op basis van de geografische ligging en het aantal bedrijven dat zich op deze terreinen bevindt. Vervolgens is via verschillende databases gezocht naar een overzicht van de bedrijven gevestigd op de die bedrijventerreinen en bijbehorende domeinnamen van deze bedrijven. Allereerst is via de Kamer van Koophandel (KvK) op postcode en straatnaam gezocht naar alle ingeschreven bedrijven. Hierna is via Company.info gezocht naar de overige kenmerken die niet via de KvK konden worden opgehaald. De ontbrekende domeinnamen zijn handmatig opgezocht via Google.

Hiernaast is een bedrijventerrein in Utrecht (Bedrijventerrein 4) geselecteerd om als controlegroep te fungeren in dit onderzoek. De controlegroep was ten tijde van het onderzoek al onderdeel van de database van Threadstone. De domeinnamen uit de controlegroep zijn onderworpen aan dezelfde geautomatiseerde kwetsbaarhedenmeting als die van de interventiegroep, maar deze bedrijven hebben geen rapportage ontvangen. Deze groep wordt geacht de gemiddelde verandering in cybersecurity zonder interventie weer te geven. Dit maakt het mogelijk voor de onderzoekers om veranderingen in cyberweerbaarheid van de bedrijven in de interventiegroep te vergelijken met eventuele verandering in cyberweerbaarheid van de niet-deelnemende bedrijven, zijnde de bedrijven in de controlegroep.

In totaal waren op de drie bedrijventerreinen in de interventiegroep 3.076 bedrijven gevestigd ten tijde van het samenstellen van de lijst met deelnemende bedrijven. Verdere vaststelling of bedrijven al dan niet een eigen domeinnaam hebben, resulteerde in een steekproef van 1.644 bedrijven (53,44% van alle bedrijven aanwezig op de terreinen). Na verder onderzoek is gebleken dat enkele bedrijven dezelfde domeinnaam hadden. Na samenvoeging van deze bedrijven onder de gezamenlijke domeinnaam, resulteerde dit in 1.460 domeinnamen voor het onderzoek in de interventiegroep. Tijdens het uitvoeren van de voormeting is gebleken dat enkele domeinnamen niet (langer) bestonden. Het uiteindelijk gemeten aantal domeinen in de interventiegroep is N=1391 (45,2% van alle bedrijven aanwezig op de terreinen). Het aantal gemeten domeinen in de controlegroep is N=576, waardoor het totaal aantal gemeten domeinen in het onderzoek N=1967 betreft (tabel 3).

Tabel 3: Verdeling gemeten domeinnamen per bedrijventerrein

Terrein en risicocommunicatie	N	%
Bedrijventerrein 1 – Geen risicocommunicatie	514	26,13%
Bedrijventerrein 2 – Geanticipeerde spijt	376	11,12%
Bedrijventerrein 3 – Sociale norm	501	25,47%
Bedrijventerrein 4 – Controlegroep	576	29,28%
Totaal	1.967	100%

4.2. Definiëring van de onderdelen van de meting

De interventie is gebaseerd op drie van de vijf principes van veilig digitaal ondernemen van het DTC (z.d.). Binnen dit onderzoek ligt de nadruk op de volgende drie principes: (1) het inventariseren van kwetsbaarheden, (2) het uitvoeren van updates en (3) het voorkomen van malware.
Het cyberweerbaarheidsniveau van de domeinnamen van de ondernemingen is aan de hand van tien items vastgesteld. Dit betreft dus tien van de elf items waarop de domeinnamen worden gecontroleerd (tabel 1). Controle zes ("Is uw website, mailserver en nameserver gereed voor nieuwe standaarden?") wordt niet meegenomen in de eindscore van de kwetsbaarhedenmeting en is puur illustratief voor de ondernemer. Ten tijde van de kwetsbaarhedenmeting betrof dit namelijk nog geen 'echte' kwetsbaarheid, omdat de nieuwe standaarden nog niet overal in gebruik zijn. Aan deze controle is dan ook geen score toegekend en deze wordt niet meegenomen in de analyses.

Onderstaande tabel (tabel 4) bevat een overzicht van de gebruikte items inclusief de verschillende mogelijke scores. Alle items zijn zo gedefinieerd dat een score van nul inhoudt dat een kwetsbaarheid niet is gevonden in de digitale infrastructuur. Elke waarde hoger dan nul betekent dat de kwetsbaarheid in enige mate is vastgesteld tijdens de kwetsbaarhedenmeting. Een score van -99 houdt in dat het niet mogelijk was om de desbetreffende kwetsbaarheid al dan niet vast te stellen voor de onderneming (missend gegeven, *missing*).

Tabel 4: Definiëring items (hoe hoger de score, hoe meer kwetsbaarheid op dit item is gedetecteerd)

Item	Scoreschaal
Verspreidt de website malware?	0, 1, 3, -99
Verspreidt de website spam?	0, 1, 2, 3
Verspreidt de mailserver spam?	0, 1, 2, 3, -99
Zijn gevoelige gegevens van medewerkers openbaar?	0, 0.25, 0.5, 0.75, 1, -99
Kan e-mail misbruikt worden?	0, 1, 2, -99
Kan het websiteverkeer worden onderschept?	0, 1, 2, 3, -99
Zijn er ongebruikelijke aanvalspaden op de website mogelijk?	0, 0.25, 0.5, 0.75, 1, -99
Worden bezoekers van de website voldoende beschermd?	0, 0.5, 1, 1.5, 2, -99
Is informatie over de configuratie van de website voldoende afgeschermd?	0, 0.5, 1, -99
Kan websiteverkeer naar de website gemanipuleerd worden?	0, 2, -99

Op basis van deze tien items wordt vervolgens voor elke onderneming een ”totaalscore cyberweerbaarheid” berekend. Elke onderneming start in de geautomatiseerde kwetsbaarhedenmeting met een totaalscore van tien en krijgt vervolgens minpunten voor elke gevonden kwetsbaarheid. Item *totaalscore cyberweerbaarheid* kan uiteenlopen van één tot tien, waarbij één de laagst haalbare score is en tien de hoogst haalbare score.

4.3. Dataverwerking van de resultaten van de metingen

De resultaten van zowel de voor- als de nameting zijn via een beveiligde omgeving in Excel format met de onderzoekers gedeeld. Aan elk item is een aparte datakolom toegewezen waarin de betreffende scores van de onderneming staan opgenomen. De data is geanonimiseerd voordat de statistische analyses zijn uitgevoerd. Hierdoor kunnen de resultaten van de metingen niet worden herleid naar specifieke ondernemingen. Om de statistische analyses uit te kunnen voeren, is de dataset ingeladen in statistisch analyseprogramma SPSS. De originele dataset staat op een beveiligde omgeving opgeslagen en alleen de onderzoekers hebben toegang tot de desbetreffende omgeving.

4.4. Statistische analysemethoden

De beschrijvende resultaten van de voor- en nameting zijn geanalyseerd met behulp van frequentie- en kruistabellen, met als doel de behaalde itemscores in kaart te brengen. Verder zijn er vergelijkende analyses in de vorm van (on)gepaarde t-toetsen uitgevoerd om vergelijking van de gemiddelde itemscores van de voor- en nameting per bedrijventerrein mogelijk te maken. Ook zijn voor alle items de verschilscores van de interventiegroep vergeleken met die van de controlegroep om de effectiviteit van de verschillende varianten van risicocommunicatie te kunnen bepalen.

5. Resultaten

In dit hoofdstuk staan de resultaten van het onderzoek beschreven. Allereerst worden de resultaten van de juridische risicobeoordeling beschreven (5.1.), gevolgd door de interviews met stakeholders (5.2.) en tot slot zijn de resultaten van de pilot van de kwetsbaarheden meting beschreven (5.3.).

5.1. Juridische risicobeoordeling

In deze paragraaf staan de resultaten van de juridische risicobeoordeling besproken om deelvraag 1: “Is het juridisch toegestaan om een geautomatiseerde kwetsbaarhedenmeting uit te voeren bij ondernemingen, zonder dat zij hier vooraf toestemming voor hebben gegeven?” te beantwoorden.

Voorafgaand aan de uitvoering van de geautomatiseerde kwetsbaarhedenmeting is een juridische risicobeoordeling uitgevoerd door ICTRecht (bijlage I), om te kunnen duiden of de informatieverzameling en het gebruik hiervan rechtmatig is. Hoewel voor de informatieverzameling gebruik is gemaakt van openbaar bereikbare informatiebronnen, kan dit gebruik in theorie leiden tot (privacyrechtelijke) bezwaren omtrent de verzameling en verwerking van informatie. Verder was voorzien dat zelfs computervredebreuk een rol zou kunnen spelen, gezien de onaangekondigde aard van de informatieverzameling. Hierom is het van belang van tevoren de wettigheid van de interventie vast te stellen.

Met betrekking tot de rechtmatigheid van de informatieverzameling is er in de juridische risicobeoordeling gekeken naar de bron van de gebruikte informatie en of deze informatie publiekelijk is gepubliceerd. De juridische risicobeoordeling beziet dat de geautomatiseerde kwetsbaarhedenmeting gebruik maakt van openbare bronnen om eventuele kwetsbaarheden in de digitale infrastructuur van een onderneming aan het licht te kunnen brengen. In geval van het vaststellen of de betreffende website of mailserver spam of malware verspreidt, zijn in de kwetsbaarhedenmeting zogenaamde *blacklists* gecontroleerd op de aanwezigheid van de domeinnaam. Aangezien *blacklists* gemaakt zijn met als doel dergelijke controles mogelijk te maken, is het onwaarschijnlijk dat deze controles als onrechtmatig kunnen worden beschouwd.

Tevens wordt gebruik gemaakt van publieke *DNS-records* om vast te kunnen stellen of de e-mail vatbaar is voor misbruik door een derde partij, of het domein compatibel is met de nieuwe IPv6 standaarden en of het verkeer naar de website vatbaar is voor manipulatie. Doordat de *DNS-records* publiek zijn, is de opvraag van deze informatie rechtmatig.

Voor de controle op het hanteren van de nieuwste SSL/TLS standaarden, het afdwingen van de juiste securityprotocollen bij de gebruiker en het achterhalen van de software(versie) gebruikt door de website, wordt in de kwetsbaarhedenmeting te allen tijde gebruik gemaakt van informatie die door de website zelf openbaar ter beschikking wordt gesteld. Het opvragen en gebruiken van deze informatie is dus volledig rechtmatig en resulteert niet in juridische struikelblokken.

Meer zorg moet worden betracht bij het achterhalen of e-mailadressen van medewerkers betrokken zijn geweest bij een datalek. Voor deze controle wordt namelijk gebruik gemaakt van de zogenaamde *password dumps*, openbare online bestanden die gegevens als e-mailadressen,

gebruikersnamen en wachtwoorden bevatten. Doordat deze dumps veel persoonlijke gegevens staan bevatten, is het van belang de verwerking tot een minimum te beperken. De verwachte impact op de betrokkenen is echter klein doordat er alleen wordt vastgesteld of het betreffende domein voorkomt in de *password dump* en vanwege het feit dat de gegevens hoe dan ook in de *password dump* voorkomen. De kwetsbaarhedenmeting beperkt zich tot het vaststellen van aanwezigheid van een gegeven in de *password dump* waardoor er verder niets met de gegevens gebeurt. Ook is deze controle een noodzakelijk onderdeel om tot een volledige kwetsbaarhedenmeting te komen. Deze controle is dan ook gestoeld op het gerechtvaardigd belang als juridische grondslag.

Met betrekking tot het mogelijke knelpunt van computervredebreuk is de *portscan* van belang waarbij wordt gecontroleerd of er onnodig poorten open staan waardoor een crimineel ongeautoriseerd de digitale infrastructuur van de onderneming kan betreden. De Hoge Raad heeft in een arrest bepaald dat het enkel uitvoeren van een portscan niet kan worden aangemerkt als binnendringing in de zin van computervredebreuk[7].

Concluderend kan de opvraag en verwerking van alle informatie worden gestoeld op het gerechtvaardigd belang als wettelijke grondslag. Het gaat bij nagenoeg elke controle om informatie die rechtmatig is gepubliceerd of waarbij de informatie wordt gebruikt met als doeleinde betreffende kwetsbaarheden aan het licht te brengen. Alleen de controle op de aanwezigheid van gegevens in *password dumps* behoeft de kanttekening dat het hierbij gaat om persoonsgevoelige informatie, waardoor er op basis van de AVG een wettelijke grondslag moet zijn. Ook hier is het gerechtvaardigd belang voldoende als wettelijke grondslag. Met betrekking tot computervredebreuk is het van belang dat het bij de vaststelling van kwetsbaarheden blijft en dat de gevonden kwetsbaarheden niet worden gebruikt om verdere metingen in de infrastructuur uit te voeren.

5.2. Interviews met betrokkenen

In deze paragraaf worden de relevante resultaten van de stakeholder interviews besproken om een antwoord te formuleren op deelvraag 2: “Welke kansen en knelpunten zien stakeholders bij het uitvoeren van een geautomatiseerde kwetsbaarhedenmeting bij Nederlandse ondernemingen?”. Allereerst staan de eerste algemene reacties van de respondenten met betrekking tot de interventie beschreven (5.2.1.). Hierna is de communicatie van de adviesrapportage naar de deelnemers besproken (5.2.2.). Verder is ingegaan op de potentie van deze interventie voor de eigen organisatie en werkzaamheden van de respondenten (5.2.3.). De paragraaf eindigt met eventuele knelpunten die door de respondenten zijn benoemd (5.2.4.).

5.2.1. Eerste reacties en algemeen beeld

De eerste reacties van respondenten van acht van de tien organisaties bleken positief; zij waren direct enthousiast over de geautomatiseerde kwetsbaarhedenmeting en zien veel kansen voor de implementatie van de interventie. Respondent A1 stelde noemde het initiatief “*Super vet!*”. Een collega, respondent A2, voegde daar aan toe dat dit initiatief leuk is voor de lokale ondernemers. Respondent C1 heeft een positief beeld van de interventie en denkt dat het bijgevoegde handelingsperspectief en de

[7] Hoge Raad 8 januari 2019, ECLI:NL:HR:2019:560.

focus op de drie DTC punten een goede methode is, omdat daar snelle winst behaald kan worden. De focus op gedragsverandering was voor respondent D1 een enthousiasmerend kenmerk doordat dit volgens eigen zeggen nog weinig wordt toegepast. Dezelfde respondent stelde tevens dat de mogelijkheid op het landelijk uitrollen van de interventie grote maatschappelijke relevantie kan hebben. Het confronterende en kosteloze karakter van de interventie was voor respondent E1 een positief punt. De behoefte vanuit de ondernemer aan hulp bij cyberweerbaarheid zorgde ervoor dat respondent F1 de interventie ziet als een waardevol en belangrijk initiatief. Respondent G1 ziet de waarde van de interventie in en denkt dat het aannemen van een proactieve houding positief kan uitpakken voor de ondernemer. Respondent H1 denkt dat de scan kan helpen met het verbeteren van de cyberweerbaarheid van een onderneming. Ten slotte stelt respondent I1 dat deze scan een "*waanzinnig goed plan*" (Respondent I1, p.3) is en dat het ongevraagde karakter van de interventie een positief punt is.

Buiten bovengenoemde positieve reacties lieten respondenten van twee organisaties meer terughoudendheid zien in hun reacties, door direct meerdere vragen te stellen en enkele bedenkingen te benoemen. Respondent B1 vroeg zich bijvoorbeeld af of de rapportage niet te technisch zou zijn voor de ondernemer om te begrijpen, en of er geen prioritering van de te treffen maatregelen in de adviesrapportage dient te worden opgenomen. Respondent J1 stelt in het interview dat de scan zeer beperkt is doordat er maar een klein deel van de cybersecurity van een onderneming wordt gescand. Bovengenoemde respondenten zagen echter wel de meerwaarde van deze interventie in voor het verbeteren van de cyberweerbaarheid van ondernemingen.

Al met al hebben de respondenten een positief beeld van de interventie, waarbij een verscheidenheid aan redenen wordt aangehaald. Zij lijken enthousiast over het initiatief en willen graag betrokken blijven bij het proces. Enkele respondenten lieten meer terughoudendheid zien, maar stelden dat ook zij erg enthousiast zijn over het project.

5.2.2. Communicatie van de resultaten naar de deelnemers

In deze deelparagraaf wordt besproken hoe respondenten denken dat de communicatie van de resultaten en het handelingsperspectief zo effectief mogelijk kan worden vormgegeven.

Respondenten van drie van de tien organisaties spraken zich uit over de manier waarop de ondernemers worden aangespoord om de in de adviesrapportage benoemde maatregelen daadwerkelijk te implementeren. Respondent E1 stelde dat confrontatie soms de beste leerschool is, maar dat je de resultaten wel duidelijk en persoonlijk moet overbrengen. Volgens respondent H1 moeten de resultaten zo concreet mogelijk aan de deelnemers worden gecommuniceerd en er moet de communicatie duidelijk laten zien wat de deelnemers met de resultaten kunnen doen. Respondent G1 haakt hier op in door te stellen dat ondernemers niet het gevoel moeten krijgen dat hierin iets wordt opgelegd door bijvoorbeeld een gemeente of een andere overheidsinstantie.

Tot slot gaf respondent A2 aan dat het nuttig zou zijn wanneer de ondernemers niet alleen een rapportage van de voor-, maar ook van de nameting ontvangen. Ook respondent B2 vroeg zich af of de resultaten van de nameting naar de ondernemer zouden worden gecommuniceerd. Op die manier kan de ondernemer zelf nagaan of de maatregelen genomen naar aanleiding van het adviesrapport effectief zijn gebleken:

> "*Voornamelijk voor de ondernemer, die wil eigenlijk gewoon, die wordt gescand en die krijgt iets en die wil hopelijk dingen gaan veranderen en nou ja daarom zou ik het dus vet vinden als hij dan zo'n rapportage terug zou krijgen om dan te laten zien van je hebt het geprobeerd maar je bent er nog niet helemaal, of je moet nog dit en dit doen*."(Respondent A2, p.6).

Samenvattend kan worden gesteld dat de respondenten vinden dat de resultaten op een zo concreet mogelijke manier moeten worden gecommuniceerd naar de deelnemers van het onderzoek. Ook zou het volgens enkele respondenten nuttig zijn om de resultaten van de nameting ook aan de deelnemers te verstrekken, in plaats van alleen de eerste scan.

5.2.3. Kansen voor de eigen organisatie

In deze deelparagraaf wordt besproken hoe respondenten de interventie in relatie tot hun eigen organisaties en werkzaamheden zien en of zij baat hebben bij de interventie en haar resultaten.

Alle respondenten hebben aangegeven dat zij de resultaten van de interventie graag willen gebruiken voor eigen initiatieven en evenementen binnen hun organisaties. Zij denken dat de resultaten als voorbeelden kunnen worden gebruikt om hun eigen cyberweerbaarheidsevenementen kracht bij te zetten. Ook willen zij andere bruikbare informatie graag gebruiken bij het opzetten en uitvoeren van voorlichtingen en/of evenementen.

> "*Dus per definitie is dit voor ons een interventie om weer een paar slachtoffers te kunnen voorkomen*." (Respondent E1, p.11).

Het verkrijgen van inzichten in de huidige stand van zaken omtrent cyberweerbaarheid bij ondernemers (respondent G1) en de resultaten gebruiken om cyberweerbaarheid op de agenda te krijgen bij ondernemingen (respondent J1) werden verder aangehaald als potentieel relevant voor hun organisaties.

Al met al zijn de respondenten van mening dat de interventie en de resultaten van het project hen kunnen helpen met het opzetten, uitvoeren en ondersteunen van eigen initiatieven. Ook het verkrijgen van meer informatie over het cyberweerbaarheidsniveau bij ondernemers bleek voor een respondent een behulpzaam aspect van het project.

5.2.4. Knelpunten van de interventie

In deze deelparagraaf staan verschillende knelpunten centraal, zoals benoemd door de betrokkenen, met betrekking tot het uitvoeren van de interventie. Er zal worden besproken welke obstakels de respondenten verwachten tijdens en na de scan tegen te komen.

Het door de respondenten meest genoemde knelpunt is het aanzetten van ondernemers om hun cyberweerbaarheid te vergroten. Respondenten van vijf van de tien organisaties hebben aangegeven dat dit in het verleden moeilijk is gebleken en hebben hun zorgen uitgesproken over de betrokkenheid van de ondernemers bij de interventie. Respondent B1 liet weten dat de ervaring leert dat ondernemers lastig in beweging zijn te krijgen. Respondent D1 stelde dat bij elk project het meekrijgen van de ondernemers wel een knelpunt is. Respondenten F1 en I1 zijn het hiermee eens, waarbij respondent F1 toevoegt dat ondernemers vaak wel weten dat cyberweerbaarheid van belang is, maar dat zij handvatten behoeven

om hiermee aan de slag te gaan. Het fenomeen cyberweerbaarheid wordt volgens respondent B2 door veel ondernemers als te abstract gezien, door te benoemen dat bij door hen uitgevoerde projecten bleek dat ondernemers daardoor geen tijd en/of geld willen of kunnen investeren in hun cybersecurity. Respondent G1 beaamt dit en noemt dit de "*unwillingness natuurlijk van de partijen zelf*." (Respondent G1, p.6).

Verder benoemden respondenten van drie van de tien organisaties dat deze kwetsbaarhedenmeting in juridisch lastig vaarwater zou kunnen geraken, voornamelijk omtrent het verkrijgen van informatie zonder dat hiervoor toestemming is verleend. Respondent A2 benoemde dat er normaliter een vrijwaring zou moeten worden ondertekend voor het uitvoeren van een kwetsbaarhedenmeting. Respondent G1 sloot hierbij aan en vroeg zich af of zonder toestemming een kwetsbaarhedenmeting mag worden uitgevoerd. Respondent C1 vroeg zich specifiek af of dit AVG-technisch zomaar mocht. Na uitleg over de juridische risicobeoordeling werden deze twijfels echter snel weggenomen bij de respondenten.

Ten slotte gaan respondenten van twee organisaties in op het feit dat de scan wordt uitgevoerd door een commerciële partij. Respondenten A2 en C1 vragen zich beiden af wat hiervoor de insteek is, of er duidelijke afspraken zijn gemaakt en of ondernemers worden geadviseerd producten af te nemen bij deze partij. Respondenten geven aan dat het van belang is dat er geen commerciële acquisitie wordt ondernomen in de interventie indien overheidsorganisaties de opdracht geven voor de interventie.

Resumerend kan worden gesteld dat de respondenten vooral knelpunten zien in het motiveren van ondernemers om daadwerkelijke stappen te nemen aan de hand van de ontvangen adviesrapportage. Ook op juridisch vlak en omtrent het eventueel toevoegen van commerciële acquisitie bij de rapportage zagen enkele respondenten mogelijke obstakels die dienen te worden weggenomen alvorens hun organisaties in de toekomst zelf opdracht zouden geven tot het uitrollen van de interventie.[8]

[8] De huidige rapportage gaat in op de genoemde knelpunten, onder andere door de interventie te beschrijven (waarbij duidelijk wordt dat er geen acquisitie plaatsvindt) en door middels een juridische toetsing.

5.3. Resultaten kwetsbaarhedenmeting

In deze paragraaf zullen de resultaten van de statistische analyses worden beschreven. Allereerst worden de voor- en nameting per bedrijventerrein vergeleken (5.3.1.), waarna de vergelijking met de controlegroep is beschreven (5.3.2.).

5.3.1. Vergelijking voor- en nameting per bedrijventerrein

Om na te gaan in welke mate de cyberweerbaarheid van ondernemingen verandert na ontvangst van de geautomatiseerde kwetsbaarhedenmeting en te controleren in hoeverre dit vergelijkbaar is tussen de verschillende bedrijventerreinen en de controlegroep (deelvraag 3) zijn de scores van de voor- en nameting van verschillende items berekend en vergeleken. Tabel 5 geeft de controles weer die in de kwetsbaarhedenmeting zijn uitgevoerd en in de adviesrapportage staan opgenomen (zie ook paragraaf 4.2.).

Tabel 5: Controles van de kwetsbaarhedenmeting

Nr.	Item
1	*Verspreidt de website malware?*
2	*Verspreidt de website spam?*
3	*Verspreidt de mailserver spam?*
4	*Zijn gevoelige gegevens van medewerkers openbaar?*
5	*Kan e-mail misbruikt worden?*
6	*Kan het websiteverkeer worden onderschept?*
7	*Zijn er ongebruikelijke aanvalspaden op de website mogelijk?*
8	*Worden de bezoekers van de website voldoende beschermd?*
9	*Is informatie over de configuratie van de website voldoende afgeschermd?*
10	*Kan internetverkeer naar de website gemanipuleerd worden?*

Beschrijving totaalscores deelnemende bedrijven en controlegroep

Ten tijde van de voormeting had de volledige interventiegroep (bedrijventerreinen 1, 2 & 3) een gemiddelde “Totaalscore Cyberweerbaarheid” van 4,62 op een schaal van één tot tien. Na het versturen van de adviesrapportages had de interventiegroep een gemiddelde “Totaalscore Cyberweerbaarheid” van 4,82, zijnde een significante stijging (p=<0,001).

De controlegroep (bedrijventerrein 4), de groep die geen adviesrapporten heeft ontvangen, had ten tijde van de voormeting een gemiddelde “Totaalscore Cyberweerbaarheid” van 4,85. Bij de nameting toonde deze groep een gemiddelde totaalscore van 5,01. Ook bij de controlegroep is sprake van een significante stijging van de totaalscore (p=<0,001).

Vergelijking kwetsbaarhedenscores per bedrijventerrein

Vervolgens is gekeken naar de gevonden kwetsbaarheden per bedrijventerrein ten tijde van de voor- en nameting. Een positieve waarde van de verschilscore voor item “Totaalscore Cyberweerbaarheid” houdt in dat er een verbetering van de totale score heeft plaatsgevonden. Een negatieve waarde van de

verschilscore van de specifieke onderdelen van de kwetsbaarhedenmeting houdt in dat er een vermindering in kwetsbaarheden voor het betreffende item heeft plaatsgevonden.

De bedrijventerreinen hebben verschillende combinaties van de adviesrapportage en risicocommunicatie ontvangen (zie ook paragraaf 3.3). Bedrijventerrein 1 heeft een rapportage ontvangen, maar geen risicocommunicatie. Bedrijventerrein 2 heeft een rapportage ontvangen en heeft de risicocommunicatievariant geanticipeerde spijt ontvangen met het citaat ”Voorkomen is goedkoper dan genezen! Werk nu aan de cyberweerbaarheid van uw bedrijf om latere kosten te voorkomen”. Bedrijventerrein 3 heeft een adviesrapportage ontvangen met de risicocommunicatievariant sociale norm, met het citaat ”Ondernemers in uw regio werken hard aan hun cybersecurity, met dit rapport kunt u dit ook doen!“. Bedrijventerrein 4 fungeert als controlegroep en heeft noch een adviesrapportage, noch een vorm van risicocommunicatie ontvangen.

Tabel 6: Vergelijking tussen voormeting en nameting per bedrijventerrein.

Item	B1 Geen risico-communicatie	B2 Geanticipeerde spijt	B3 Sociale norm	B4 Controlegroep
Totaalscore cyberweerbaarheid	0,195***	0,370***	0,074*	0,155***
Verspreidt de website malware?	-0,004	0,003	0,006	-0,000
Verspreidt de website spam?	-0,020	-0,183***	-0,018	-0,034*
Verspreidt de mailserver spam?	-0,060**	-0,193***	-0,054***	-0,069***
Zijn gevoelige gegevens van medewerkers openbaar?	0,001	-0,003	0,001	0,0004
Kan e-mail misbruikt worden?	-0,018	-0,019	0,002	-0,026*
Kan het websiteverkeer worden onderschept?	-0,031	-0,011	0,006	-0,008
Zijn er ongebruikelijke aanvalspaden op de website mogelijk?	-0,006	-0,045***	-0,004	-0,006
Worden bezoekers van de website voldoende beschermd?	-0,055**	-0,045**	-0,042***	-0,016
Is informatie over de configuratie van de website voldoende afgeschermd?	-0,007	0,002	-0,007	0,011
Kan websiteverkeer naar de website gemanipuleerd worden?	-0,004	0,027	-0,016	-0,021*

P: ≤0,05, ≤0,01**, <0,001****

De resultaten van de uitgevoerde t-toetsen (tabel 6 en figuur 1) laten zien dat de gemiddelde “totaalscore cyberweerbaarheid” van bedrijventerrein 1 significant met 0,195 (p=<0,001) is gestegen van 4,84 naar 5,03 op een schaal van 1 tot en met 10. Specifiek is er een significante daling waargenomen in gevonden kwetsbaarheden op de volgende onderdelen van de kwetsbaarhedenmeting: ”Verspreidt de mailserver spam?“ en ”Worden bezoekers van de website voldoende beschermd?” (figuur 1). Deze dalingen duiden op een significante vermindering van het risico op misbruik van deze onderdelen van de digitale infrastructuur.

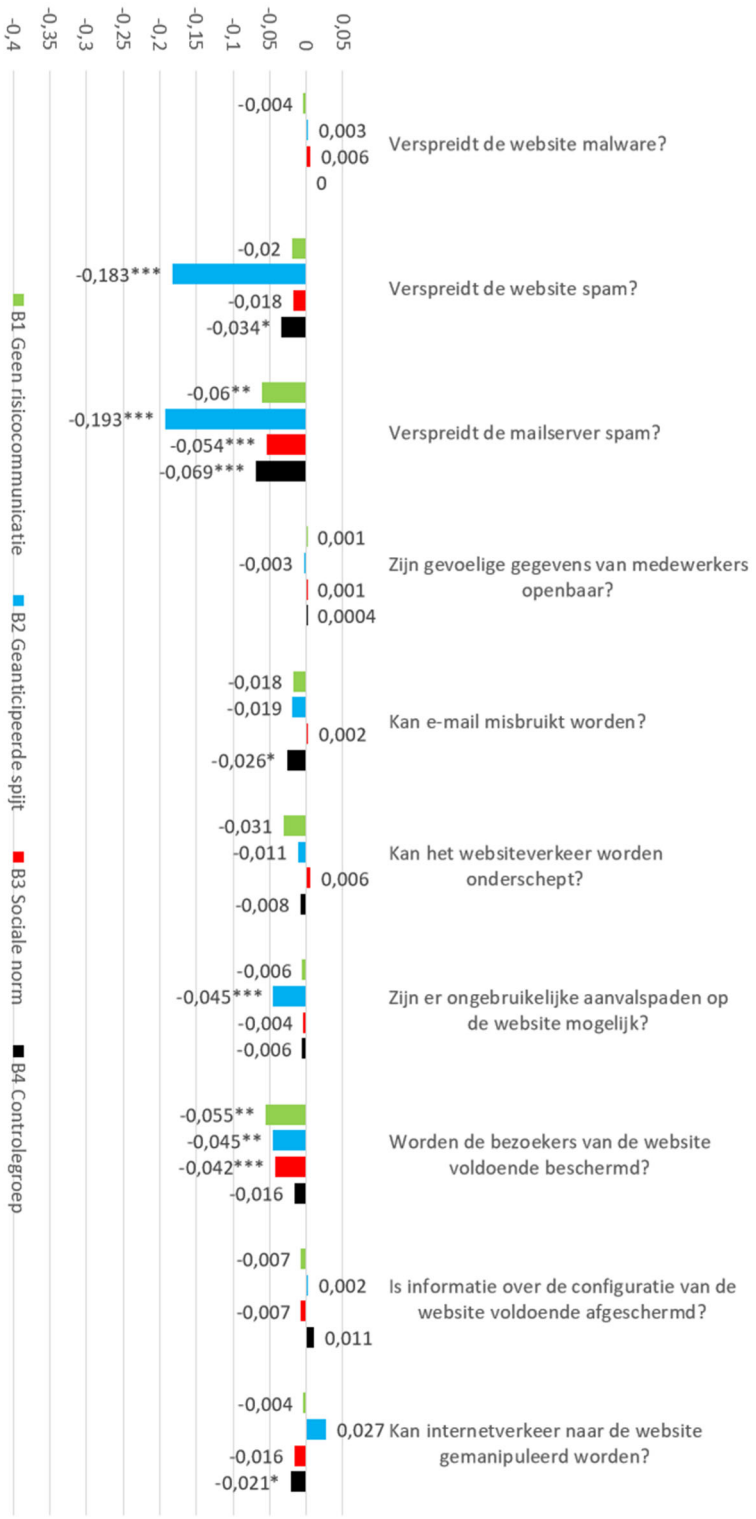
De gemiddelde “totaalscore cyberweerbaarheid” van bedrijventerrein 2 is significant gestegen met 0,370 (p=<0,001) van 4,19 naar 4,56 (tabel 6). Er is een significante daling waargenomen in het aantal

gevonden kwetsbaarheden van de volgende onderdelen van de kwetsbaarhedenmeting: ”Verspreidt de website spam?”, ”Verspreidt de mailserver spam?”, ”Zijn er ongebruikelijke aanvalspaden op de website mogelijk?“ en ”Worden bezoekers van de website voldoende beschermd?“ (figuur 1).

Ook de gemiddelde “totaalscore cyberweerbaarheid” van bedrijventerrein 3 is significant gestegen, met 0,074 (p=≤0,050) van 4,71 naar 4,78 op een schaal van 1 tot en met 10 (tabel 6). De waargenomen gemiddelde daling in gevonden kwetsbaarheden op de kwestbaarhedenmeting onderdelen ”Verspreidt de mailserver spam?” en ”Worden bezoekers van de website voldoende beschermd?“ is significant (figuur 1).

De gemiddelde “totaalscore cyberweerbaarheid” van de controlegroep is ook significant gestegen, met 0,155 (p=<0,001) van 4,85 naar 5,01 (tabel 6). Er is een significante daling waargenomen in het aantal gevonden kwetsbaarheden van de volgende onderdelen van de kwetsbaarhedenmeting: ”Verspreidt de website spam?”, “Verspreidt de mailserver spam?”, “Kan e-mail misbruikt worden?” en “Kan websiteverkeer naar de website gemanipuleerd worden?” (figuur 1).

Figuur 1. Gemiddelde verandering in gevonden kwetsbaarheden tussen de voor- en nameting per bedrijventerrein



Percentage vooruitgang

Naast het vergelijken van de scores op voor- en nameting is ook gekeken naar het percentage bedrijven dat tussen deze metingen vooruitgegaan is op de verschillende onderdelen van de kwetsbaarhedenscan. Hierbij behandelen we de bedrijven nogmaals per bedrijventerrein, en dus per risicocommunicatievariant.

Gemiddeld zijn bij 10,1% van alle bedrijven die een rapportage hebben ontvangen minder kwetsbaarheden gevonden ten tijde van de nameting, vergeleken met de voormeting. Bij de bedrijven in de controlegroep was dit percentage 8,3% (niet in tabel). Op bedrijventerrein 1 zijn er minder kwetsbaarheden gevonden bij alle onderdelen van de kwetsbaarhedenmeting, met uitzondering van onderdeel ”Zijn gevoelige gegevens van medewerkers openbaar?”. Ook is de “totaalscore cyberweerbaarheid” van deze interventiegroep onder 9,5% van de ondernemingen omhooggegaan (tabel 7). Op bedrijventerreinen 2 en 3 werd er onder respectievelijk 11,2% en 10% van de bedrijven een verbetering in de “totaalscore cyberweerbaarheid” gevonden. Op alle onderdelen van de kwetsbaarhedenmeting werden minder kwetsbaarheden gevonden bij een percentage van de bedrijven op deze bedrijventerreinen (tabel 7). Ten slotte werd binnen bedrijventerrein 4 (controlegroep) gevonden dat 8,3% van de ondernemingen een hun “totaalscore cyberweerbaarheid” hebben verhoogd. Voor bijna alle onderdelen van de kwetsbaarhedenmeting is er bij een percentage van deze bedrijven een vermindering in gevonden kwetsbaarheden gevonden, met uitzondering van ”Zijn gevoelige gegevens van medewerkers openbaar?“ (tabel 7).

Tabel 7: Percentage bedrijven dat vooruitgang heeft geboekt per item, uitgesplitst naar bedrijventerrein/risicocommunicatievariant.

Item	B1 Geen risico-communicatie	B2 Geanticipeerde spijt	B3 Sociale norm	B4 Controle groep
Totaalscore cyberweerbaarheid	9,5%	11,2%	10%	8,3%
Verspreidt de website malware?	1,4%	2,1%	0,8%	1%
Verspreidt de website spam?	5,3%	22%	4,9%	7%
Verspreidt de mailserver spam?	10,1%	23,2%	7,2%	12,4%
Zijn gevoelige gegevens van medewerkers openbaar?	0%	0,5%	0,4%	0%
Kan e-mail misbruikt worden?	2,5%	4,8%	1,8%	2,4%
Kan het websiteverkeer worden onderschept?	3,1%	2,9%	1,7%	2,2%
Zijn er ongebruikelijke aanvalspaden op de website mogelijk?	2,5%	6,6%	1,6%	1,4%
Worden bezoekers van de website voldoende beschermd?	6,4%	5,8%	4,2%	1,3%
Is informatie over de configuratie van de website voldoende afgeschermd?	4,3%	4,8%	3,6%	2,7%
Kan websiteverkeer naar de website gemanipuleerd worden?	1,8%	1,3%	1,8%	1%

5.3.2. Vergelijking deelnemende bedrijventerreinen met controlegroep

Vervolgens worden de gemiddelde verschilscores van de bedrijventerreinen die onderdeel zijn van de interventiegroep vergeleken met de controlegroep. Hierbij is de vraag of de verandering in getroffen maatregelen tussen de voor- en nameting significant groter is onder de bedrijventerreinen die een adviesrapportage hebben ontvangen dan onder de bedrijven die geen rapportage hebben ontvangen (de controlegroep). De resultaten van de vergelijkende analyses worden per bedrijventerrein beschreven.

Tabel 8: Vergelijking bedrijventerreinen (B1-B3) met controlegroep (B4)

Item	Gemiddelde verandering in score B1vsB4	Gemiddelde verandering in score B2vsB4	Gemiddelde verandering in score B3vsB4	Gemiddelde verandering in score B1-3vsB4
Totaalscore cyberweerbaarheid	0,040	0,215**	-0,081	0,044
Verspreidt de website malware?	-0,004	0,003	0,006	0,001
Verspreidt de website spam?	0,015	-0,149***	0,016	-0,029
Verspreidt de mailserver spam?	0,010	-0,123***	0,015	-0,025
Zijn gevoelige gegevens van medewerkers openbaar?	0,001	-0,003	0,001	-0,00043
Kan e-mail misbruikt worden?	0,009	0,007	0,028	0,015
Kan het websiteverkeer worden onderschept?	-0,023	-0,003	0,014	-0,004
Zijn er ongebruikelijke aanvalspaden op de website mogelijk?	-0,00019	-0,040*	0,001	-0,010
Worden bezoekers van de website voldoende beschermd?	-0,039*	-0,030	-0,027	-0,032*
Is informatie over de configuratie van de website voldoende afgeschermd?	-0,019	-0,010	-0,018	-0,016
Kan websiteverkeer naar de website gemanipuleerd worden?	0,017	0,047*	0,005	0,021

P: ≤0,05, ≤0,01**, <0,001****

Wanneer de verschilscores van bedrijventerrein 1 en de controlegroep worden vergeleken, blijkt dat de verandering tussen voor- en nameting voor bedrijventerrein 1 significant groter is dan de verandering waargenomen voor de controlegroep voor het kwetsbaarhedenmeting onderdeel ”Worden bezoekers van de website voldoende beschermd?” (tabel 8). In bedrijventerrein 1 was er dus tijdens de onderzoeksperiode sprake van een grotere afname in kwetsbaarheden op dit onderdeel dan in de controlegroep in dezelfde periode. Voor de overige onderdelen werd een vergelijkbare verandering binnen de controlegroep en bedrijventerrein 1 gevonden. Ook de gemiddelde toename in de totaalscore in bedrijventerrein 1 is vergelijkbaar (niet significant groter of kleiner) dan de gemiddelde toename in de totaalscore in de controlegroep.

Uit de vergelijking tussen bedrijventerrein 2 en de controlegroep is gebleken dat de toename in de “totaalscore cyberweerbaarheid” significant groter was tussen de voor- en nameting in bedrijventerrein 2 dan in de controlegroep. Specifiek laten de kwetsbaarheden meting onderdelen ”Verspreidt de website spam?”, ”Verspreidt de mailserver spam?”, ”Zijn er ongebruikelijke aanvalspaden op de website mogelijk?“ en “Kan websiteverkeer naar de website gemanipuleerd worden?“ een significant grotere verandering zien tussen de voor- en nameting in bedrijventerrein 2 in vergelijking met de controlegroep.

De vergelijking tussen bedrijventerrein 3 en de controlegroep laat zien dat voor alle onderdelen van de kwetsbaarhedenmeting de verandering, tussen de voor- en nameting, bij bedrijven uit bedrijventerrein 3 vergelijkbaar is met bedrijven uit de controlegroep. De verandering op de verschillende onderdelen van de kwetsbaarhedenmeting en de totaalscore in bedrijventerrein 3 is dus niet significant groter of kleiner dan de veranderingen in de controlegroep.

Ten slotte is de volledige interventiegroep (bedrijventerrein 1, bedrijventerrein 2 & bedrijventerrein 3) met de controlegroep vergeleken, waaruit bleek dat er alleen voor onderdeel ”Worden bezoekers van de website voldoende beschermd?“ sprake is van een significante grotere daling in het aantal gevonden kwetsbaarden in de interventiegroep dan de controlegroep.

6. Conclusie en discussie

In dit hoofdstuk worden de onderzoeksvragen beantwoord (6.1.), enkele beperkingen van het onderzoek beschreven (6.2.) en worden aanbevelingen voor vervolgonderzoek gedaan (6.3.).

6.1. Beantwoording onderzoeksvragen

In dit onderzoek stond de volgende onderzoeksvraag centraal:

"In hoeverre is het mogelijk, toegestaan en effectief om een geautomatiseerde kwetsbaarhedenmeting uit te voeren ter bevordering van de cyberweerbaarheid van Nederlandse ondernemingen?"

Ter beantwoording van deze hoofdvraag zijn drie deelvragen opgesteld. Vervolgens is er een juridische risicobeoordeling van de kwetsbaarhedenmeting uitgevoerd en zijn interviews afgenomen met betrokkenen. Tot slot is de geautomatiseerde kwetsbaarhedenmeting uitgevoerd op drie Nederlandse bedrijventerreinen. We zullen in deze conclusie de deelvragen en hoofdvraag beantwoorden.

Deelvraag 1: Is het juridisch toegestaan om een geautomatiseerde kwetsbaarhedenmeting uit te voeren bij ondernemingen, zonder dat zij hier vooraf toestemming voor hebben gegeven?

Er is een juridische risicobeoordeling uitgevoerd om de rechtmatigheid van de geautomatiseerde kwetsbaarhedenmeting te toetsen, waarbij er voor elk onderdeel van de kwetsbaarhedenmeting door een juridische partij is getoetst of deze in overeenstemming is met de wetgeving. De volledige juridische risicobeoordeling is opgenomen als bijlage I.

Samenvattend is door de jurist vastgesteld dat de geautomatiseerde kwetsbaarhedenmeting rechtmatige opvraag van informatie en rechtmatig gebruik van de opgevraagde gegevens betreft. Waar het het scannen van password dumps betreft, is voor de verwerking van deze persoonsgegevens een wettelijke grondslag noodzakelijk. In de juridische risicobeoordeling is aangegeven dat het gerechtvaardigd belang voldoende grondslag biedt om de betreffende persoonsgegevens te verwerken en wordt gesteld dat er juridisch geen problematiek wordt voorzien op dit gebied. Een kanttekening is dat de kwetsbaarhedenmeting alleen kwetsbaarheden mag vaststellen en dat de digitale infrastructuur van de ondernemingen niet verder mag worden binnengetreden (middels eventuele gevonden kwetsbaarheden) voor verdere metingen.

Deelvraag 2: Welke kansen en knelpunten zien betrokkenen bij het uitvoeren van een geautomatiseerde kwetsbaarhedenmeting bij Nederlandse ondernemingen?

Interviews met betrokkenen, werkzaam in organisaties die zich bezighouden met de cyberweerbaarheid van Nederlandse ondernemingen, laten zien dat er een grote behoefte bestaat aan een werkende, empirisch onderbouwde (evidence-based) gedragsinterventie om ondernemingen te helpen in het

vergroten van hun cyberweerbaarheid. Respondenten hebben verschillende kansen en knelpunten benoemd met betrekking tot de interventie die centraal staat in het huidige onderzoek.

Respondenten reageerden overwegend zeer enthousiast op de interventie en zien in de uitvoering ervan kansen liggen voor het helpen van ondernemers. Zij verwachten dat middels de interventie op een laagdrempelige manier een op maat gemaakt handelingsperspectief kan worden geven voor het verbeteren van hun cyberweerbaarheid. Enthousiasme werd geuit over het feit dat de ondernemer zich niet hoeft aan te melden voor het afnemen van de kwetsbaarhedenmeting, de kosten van de interventie relatief laag zijn en de interventie schaalbaar is. Respondenten van twee organisaties reageerden meer terughoudend vanwege voorziene knelpunten, maar zien de meerwaarde van de interventie voor ondernemers wel in.

De juiste manier van resultaten uit de kwetsbaarhedenmeting communiceren naar de ondernemers is volgens de respondenten van groot belang voor de effectiviteit van de interventie. De respondenten stellen dat persoonlijke en heldere communicatie ervoor kan zorgen dat ondernemers sneller geneigd zijn daadwerkelijk stappen te ondernemen na het ontvangen van de adviesrapportage. Duidelijk aangeven welke maatregelen de ondernemer kan treffen en hoe deze moeten worden geïmplementeerd (een handelingsperspectief) is van groot belang om ervoor te zorgen dat de interventie laagdrempelig blijft.

De meeste betrokkenen zien kansen voor de interventie binnen hun eigen organisatie naast reeds bestaande eigen evenementen en initiatieven. Zij stellen dat de interventie een goede eerste stap kan zijn om ondernemers aan te sporen gericht te werken aan de cyberweerbaarheid van hun organisatie. Vervolgens zien de respondenten kansen om middels de interventie ondernemers te wijzen op bijvoorbeeld aankomende evenementen en ervoor zorgen dat meer ondernemers gebruik maken van de al bestaande initiatieven.

De respondenten zien echter ook verschillende mogelijke knelpunten met betrekking tot de uitvoering van de interventie. Zo geven diverse respondenten aan hun bedenkingen te hebben wanneer het gaat om het tot handelen aanzetten van de ondernemers. Respondenten benoemen dat zij zelf grote moeite hebben met het aansporen van ondernemers tot het treffen van cybersecuritymaatregelen. Ook een mogelijke commerciële ondertoon bleek een punt van zorg voor enkele respondenten. Daarnaast zien de respondenten bovendien mogelijke knelpunten op het juridische vlak, waarbij de verwerking van persoonsgegevens en het ongevraagde karakter van de interventie centraal stonden. De respondenten stellen dat op dit vlak voorzichtigheid geboden is en merken op dat ondernemers mogelijk negatief kunnen reageren op het uitvoeren van de kwetsbaarhedenmeting zonder hun toestemming en zonder op de hoogte te zijn gebracht van de kwetsbaarhedenmeting. Alvorens betrokkenen al dan niet overgaan tot het verder uitrollen van de kwetsbaarhedenmeting, is de in dit rapport opgenomen juridische risicobeoordeling en pilot daarom wenselijk.

> *Deelvraag 3: In welke mate verandert de cyberweerbaarheid van ondernemingen na het ontvangen van de geautomatiseerde kwetsbaarhedenmeting en in hoeverre is dit vergelijkbaar tussen de verschillende bedrijventerreinen en de controlegroep?*

In alle bedrijventerreinen, inclusief de controlegroep, werden gemiddeld minder kwetsbaarheden waargenomen ten tijde van de nameting, in vergelijking met de voormeting die zeven weken eerder

plaatsvond. Bij een van de bedrijventerreinen uit de interventiegroep was sprake van een significant grotere toename in cyberweerbaarheid vergeleken met de controlegroep. Namelijk, bij bedrijven in het bedrijventerrein dat een adviesrapportage met geanticipeerde spijt als risicocommunicatievariant heeft ontvangen ("Voorkomen is goedkoper dan genezen! Werk nu aan de cyberweerbaarheid van uw bedrijf om latere kosten te voorkomen."), werd gemiddeld een significant grotere stijging in de "totaalscore cyberweerbaarheid" gevonden dan in de controlegroep. In dit bedrijventerrein steeg de gemiddelde totaalscore van 4,19 naar 4,56 op een schaal van een tot tien, een significante stijging. Bij zo'n 11,2% van de ondernemingen in dit bedrijventerrein is de "totaalscore cyberweerbaarheid" toegenomen in de onderzoeksperiode. Binnen deze groep is specifiek een daling waargenomen in het aantal gevonden kwetsbaarheden van de volgende onderdelen van de kwetsbaarhedenmeting: "Verspreidt de website spam?", "Verspreidt de mailserver spam?", "Zijn er ongebruikelijke aanvalspaden op de website mogelijk?" en "Worden de bezoekers van de website voldoende beschermd?".

Ook bedrijven in het bedrijventerrein die een adviesrapportage hebben ontvangen zonder risicocommunicatie (bedrijventerrein 1) laten gemiddeld een significante stijging in "totaalscore cyberweerbaarheid" zien, van 4,84 naar 5,03. Deze stijging is echter vergelijkbaar met de stijging die de controlegroep in dezelfde periode liet zien. Onder 9,5% van de ondernemingen in dit bedrijventerrein is de "totaalscore cyberweerbaarheid" toegenomen in de onderzoeksperiode. Op de volgende onderdelen van de kwetsbaarhedenmeting zijn in dit bedrijventerrein gemiddeld significant minder kwetsbaarheden gevonden tijdens de nameting, vergeleken met de voormeting: "Verspreidt de mailserver spam?" en "Worden de bezoekers van de website voldoende beschermd?".

Ten slotte bleek dat ondernemingen die een adviesrapportage en de risicocommunicatievariant sociale norm hebben ontvangen (bedrijventerrein 3), gemiddeld de minst sterke stijging in "totaalscore cyberweerbaarheid" lieten zien, van 4,71 naar 4,78. Deze toename tussen de voor- en nameting was significant maar vergelijkbaar bij de stijging die plaatsvond bij de controlegroep in dezelfde periode. Bij zo'n 10% van de ondernemingen is de "totaalscore cyberweerbaarheid" toegenomen in de onderzoeksperiode. Binnen deze groep is specifiek een daling waargenomen in het aantal gevonden kwetsbaarheden van de volgende onderdelen van de kwetsbaarhedenmeting: "Verspreidt de mailserver spam?" en "Worden bezoekers van de website voldoende beschermd?".

Ook onder bedrijven in de controlegroep is de gemiddelde "totaalscore cyberweerbaarheid" significant toegenomen tijdens de onderzoeksperiode, van 4,85 naar 5,01. De controlegroep heeft noch een adviesrapportage, noch een vorm van risicocommunicatie ontvangen, waardoor deze groep fungeert als een ijkpunt voor de gemiddelde verandering van cybersecurity onder Nederlandse ondernemingen in de onderzoeksperiode. Binnen de controlegroep is bij zo'n 8,3% van de ondernemingen de "totaalscore cyberweerbaarheid" toegenomen tijdens de onderzoeksperiode. Op de volgende onderdelen van de kwetsbaarhedenmeting zijn in dit bedrijventerrein gemiddeld significant minder kwetsbaarheden gevonden tijdens de nameting, vergeleken met de voormeting: "Verspreidt de website spam?", "Verspreidt de mailserver spam?", "Kan het websiteverkeer naar de website gemanipuleerd worden?" en "Kan e-mail worden misbruikt?".

Wanneer de deelnemende bedrijventerreinen worden vergeleken met de controlegroep blijkt uit de resultaten dat bedrijventerrein 2 met risicocommunicatievariant geanticipeerde spijt de enige groep is die een significant sterkere toename van de totaalscore laat zien tussen de voor- en nameting dan de controlegroep. Dit kan erop duiden dat geanticipeerde spijt als risicocommunicatie een positieve invloed

heeft op het treffen van cybersecuritymaatregelen ten opzichte van de controlegroep. De bedrijventerreinen die geen risicocommunicatie of sociale norm als risicocommunicatie hebben ontvangen bij hun adviesrapportage laten een vergelijkbare afname zien in gevonden kwetsbaarheden als de controlegroep. Er is meer onderzoek nodig om deze verschillen te duiden.

Concluderend kan de onderzoeksvraag: “In hoeverre is het mogelijk, toegestaan en effectief om een geautomatiseerde kwetsbaarhedenmeting uit te voeren ter bevordering van de cyberweerbaarheid van Nederlandse ondernemingen?” als volgt worden beantwoord. Er zijn in de juridische risicobeoordeling geen juridische bezwaren gevonden tegen de uitvoering van de interventie. Betrokkenen zien bij de uitvoering van de interventie veel kansen voor de eigen organisaties. Er is benoemd 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 kan bijstaan hun cyberweerbaarheid te verbeteren. Hiernaast is de interventie schaalbaar omdat deze makkelijk uit te voeren en betaalbaar is. Bij de uitvoering van de interventie is waargenomen dat een van de varianten van de kwetsbaarhedenmeting een grotere stijging in cyberweerbaarheid heeft bewerkstelligd dan de controlegroep. Namelijk, binnen het bedrijventerrein die de risicocommunicatievariant geanticipeerde spijt heeft ontvangen, werd ten tijde van de nameting (vergeleken met de voormeting) een significant grotere afname waargenomen in gevonden kwetsbaarheden dan binnen de controlegroep. Deze resultaten wijzen op een succesvolle pilot van een laagdrempelige, schaalbare interventie.

6.2. Beperkingen

De interventie heeft een vernieuwend karakter, maar kent ook enkele beperkingen. Zo hebben de onderzoekers na het versturen van de rapportages geen zicht meer gehad op welke ondernemers de rapportages wel of niet hebben gelezen. Het is denkbaar dat een deel van de ondernemers de adviesrapportages niet heeft gelezen en een ander deel de rapportages wel heeft gelezen, maar vervolgens geen stappen heeft ondernomen om de gevonden kwetsbaarheden te verhelpen. Meer duidelijkheid over het aantal ondernemers die kennis hebben genomen van de adviesrapportage zou inzicht verschaffen in de effectiviteit van de interventie.

Doordat bedrijventerrein 2 de grootste significante stijging heeft vertoond bij de nameting ten opzichte van de voormeting, lijkt geanticipeerde spijt als risicocommunicatie de meest effectieve manier om ondernemers aan te sporen om cybersecuritymaatregelen te treffen. Het is hierbij de vraag of de risicocommunicatie dit positieve effect heeft veroorzaakt, of dat dit is veroorzaakt door externe, nog niet onderzochte factoren. Een kanttekening die bovendien moet worden gemaakt, is dat deze interventiegroep ten tijde van de voormeting een enigszins lagere gemiddelde totaalscore had dan de andere twee deelnemende bedrijventerreinen. De huidige onderzoek kan worden beschouwd als pilot van de interventie en de gebruikte risicocommunicatie. Er is vervolgonderzoek nodig om vast te stellen op welke manier risicocommunicatie bijdraagt aan de effectiviteit van de interventie.

Hoewel er geen duidelijke redenen zijn om aan te nemen dat de deelnemende bedrijventerreinen afwijken van andere Nederlandse bedrijventerreinen, is niet met zekerheid vast te stellen dat de onderzoekspopulatie representatief is voor Nederlandse ondernemingen. Demografische kenmerken van

de ondernemingen zoals het aantal medewerkers, de branche en de omzet waren in dit onderzoek niet bekend. Hoewel aangenomen wordt dat de spreiding op deze kenmerken vergelijkbaar is in de vier bedrijventerreinen, is het mogelijk dat er enige afwijkingen zijn tussen de bedrijventerreinen op een of meerdere niet geobserveerde kenmerken. Vervolgonderzoek zou kunnen uitsluitsel kunnen bieden in hoeverre de kwetsbaarhedenmeting effectief is voor onder andere specifieke branches en diverse bedrijfsgroottes.

Tot slot moet met betrekking tot de conclusies de kanttekening worden gemaakt dat deze kwetsbaarhedenmeting een zeer klein deel van de cybersecurity van ondernemingen omvat. Hierdoor kunnen geen overkoepelende conclusies worden gemaakt over de algehele cybersecurity van de deelnemende ondernemingen.

6.3. Aanbevelingen

Verder vervolgonderzoek naar de effectiviteit van de kwetsbaarhedenmeting is zeer aan te bevelen. Zo is het onduidelijk in welke mate de gebruikte risicocommunicatie de effectiviteit van de interventie heeft beïnvloed.

Vervolgonderzoek kan bovendien dieper ingaan op de stappen die ondernemers al dan niet nemen na het ontvangen van de adviesrapportage. Inzicht in deze en andere vraagstukken zou kunnen worden verkregen door het bevragen van deelnemende ondernemers naar hun ervaringen met de interventie en hun beweegredenen voor het al dan niet ondernemen van actie ter verbetering van de cybersecurity naar aanleiding van de adviesrapportage en/of risicocommunicatie.

In het huidige onderzoek is het onduidelijk gebleven in hoeveel ondernemingen de medewerker die verantwoordelijk is voor de cybersecurity van de onderneming kennis heeft genomen van de adviesrapportage. In vervolgonderzoek zou hier inzicht in kunnen worden verschaft door te toetsen in welke mate de adviesrapportage wordt gelezen, bijvoorbeeld door het achteraf bevragen van respondenten of door het opnemen van een QR code die gescand dient te worden, waarbij geregistreerd kan worden hoe vaak de QR code door een uniek IP adres wordt geopend.

Verder dient de interventie onder een grotere interventiegroep te worden getest waarbij meer bekend is over de kenmerken van de betrokken ondernemingen. Toekomstig onderzoek dient bijvoorbeeld zoveel mogelijk rekening te houden met andere verklarende factoren voor het treffen van maatregelen op basis van de adviesrapportage, zoals de branche, het aantal medewerkers en het volwassenheidsniveau van de cyberweerbaarheid van de organisatie. Op deze manier kunnen externe factoren namelijk worden meegenomen in de analyses en wordt een meer compleet beeld van de effectiviteit van de interventie gecreëerd.

Vervolgonderzoek naar de gemiddelde stijging van cyberweerbaarheid van ondernemingen in Nederland en welke factoren hieraan bijdragen kan duidelijkheid scheppen naar de daadwerkelijke invloed van de interventie. Bovendien kan dergelijk onderzoek aanknopingspunten bieden voor het verdere ontwikkeling van de risicocommunicatie en het handelingsperspectief die deel uitmaken van de interventie.

Literatuur

Abraham, C., & Sheeran, P. (2003). Acting on intentions: The role of anticipated regret. *British Journal of social psychology, 42*(4), 495-511.

Bongers, K.C.A., Leukfeldt, E.R., Kleij van der, R., Ancher, M., & Bekkers, L. (2021). *Human Factors in Cybersecurity in mkb; Rapportage pilots Ontvankelijkheid bij Ondernemers*. Inspire to Act i.s.m. Haagse Hogeschool.

Carfora, V., Caso, D., & Conner, M. (2017). Randomised controlled trial of a text messaging intervention for reducing processed meat consumption: The mediating roles of anticipated regret and intention. *Appetite*, *117*, 152-160.

CBS. (2022). *ICT-gebruik bij bedrijven 2021*. Centraal Bureau voor de Statistiek.

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

CBS. (2023). *Toepassing van internetstrandaarden voor website van bedrijven.* Centraal Bureau voor de Statistiek.

Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of personality and social psychology*, *58*(6), 1015.

Coles-Kemp, L., Ashenden, D., & O'Hara, K. (2018). Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen. *Politics and Governance*, *6*(2), 41-48.

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.

Das, S. (2016). Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity. *it-Information Technology*, *58*(5), 237-245.

Das, S., Kim, T. H. J., Dabbish, L. A., & Hong, J. I. (2014). The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)* (pp. 143-157).

Das, S., Kramer, A. D., Dabbish, L. A., & Hong, J. I. (2015, February). The role of social influence in security feature adoption. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing* (pp. 1416-1426).

De Groot, J. I., Bondy, K., & Schuitema, G. (2021). Listen to others or yourself? The role of personal norms on the effectiveness of social norm interventions to change pro-environmental behavior. *Journal of Environmental Psychology*, *78*, 101688.

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

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

Frewer, L. (2004). The public and effective risk communication. *Toxicology letters*, *149*(1-3), 391-397.

Geber, S., Baumann, E., Czerwinski, F., & Klimmt, C. (2021). The effects of social norms among peer groups on risk behavior: A multilevel approach to differentiate perceived and collective norms. *Communication Research*, *48*(3), 319-345.

Gilovich, T., & Medvec, V. H. (1995). The experience of regret: What when and why. *Psychological Bulletin, 102*, 379–395.

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, 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*. NHL Stenden.

Holm, H., Sommestad, T., Almroth, J., & Persson, M. (2011). A quantitative evaluation of vulnerability scanning. *Information Management & Computer Security*, *19*(4), 231-247.

ICTRecht. (2022). *Memorandum ThreadRisk. Beoordeling van juridische risico's bij geautomatiseerde beveiligingscontroles voor websites.* [Memorandum].

Janis, I.L., & Mann, L. (1977). *Decision-making: A psychological analysis of conflict, choice and commitment.* New York: Free Press.

Kahan, D. M. (2019). Social influence, social meaning, and deterrence. In *Criminal Law* (pp. 429-476). Routledge.

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.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity 53 behavior. *International Journal of Information Management, 45*, 13–24.

Loomes, G., & Sugden, R. (1982). Regret theory: An alternative theory of rational choice under uncertainty. *Economic Journal, 92*, 805–824.

Misana-ter Huurne, E., van Houten, Y., Spithoven, R., Notté, R., & Leukfeldt, E. R. (2020). *Cyberweerbaarheid: risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb-ers*. Saxion Hogeschool/de Haagse Hogeschool.

Misana-ter Huurne, E., van 't Hoff-de Goede, S., Bekkers, L., van Houten, Y., Walther, M., Spithoven, R., & Leukfeldt, E. R. (2021a). *Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Deelrapport werkpakket 1-2.* Hogeschool Saxion /de Haagse Hogeschool.

Misana-ter Huurne, E., Bekkers, L., Van 't Hoff-de Goede, S., Van Houten, Y., Hansen, S., Foppen, E., Ebrahem, S., Spithoven, R. & Leukfeldt, R. (2021b). *Cyberweerbaarheid - een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Risicobewustzijn, preventief gedrag en de verklaring daarvoor.* D*eelrapport werkpakket 3.* Hogeschool Saxion /de Haagse Hogeschool.

Munnichs, G. M., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: over cyberdreigingen en versterking van weerbaarheid*. Rathenau Instituut.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), (2021, juni). *Cybersecuritybeeld Nederland 2021*. Ministerie van Justitie en Veiligheid.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), (2022, juli). *Cybersecuritybeeld Nederland 2022*. Ministerie van Justitie en Veiligheid.

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

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011, September). Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)* (pp. 60-68). IEEE.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597–611.

Rader, E., Wash, R., & Brooks, B. (2012, July). Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (pp. 1-17).

Renaud, K., Searle, R., & Dupuis, M. (2022, October). Cybersecurity regrets: I've had a few.... je ne regrette. In *Proceedings of the 2022 New Security Paradigms Workshop* (pp. 1-20).

Rennhard, M., Esposito, D., Ruf, L., & Wagner, A. (2019). Improving the effectiveness of web application vulnerability scanning. *International Journal on Advances in Internet Technology*, *12*(1/2), 12-27.

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.

Rijksoverheid (2021). *Adviesrapport Integrale aanpak cyberweerbaarheid.* Geraadpleegd van https://www.rijksoverheid.nl/documenten/rapporten/2021/04/06/tk-bijlage-csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

Sandberg, T., & Conner, M. (2008). Anticipated regret as an additional predictor in the theory of planned behaviour: A meta-analysis. *British journal of social psychology*, *47*(4), 589-606.

Schultz, P. W. (1999). Changing behavior with normative feedback interventions: A field experiment on curbside recycling. *Basic and applied social psychology*, *21*(1), 25-36.

Schwarz, G.M., Wong, K.F.E., & Kwong, J.Y. (2014). The role of regret in institutional persistence and change. *Journal of Change Management, 14*(3), 309-333.

Shih, E., & Schau, H. J. (2011). To justify or not to justify: The role of anticipated regret on consumers' decisions to upgrade technological innovations. *Journal of Retailing, 87*(2), 242–251.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security, 23*(2), 200-217.

Van 't Hoff-de Goede, S., van der Kleij, R., van de Weijer, S., & Leukfeldt, R. (2019). Hoe veilig gedragen wij ons online? *Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*. Den Haag: WODC, Centre of Expertise Cybersecurity, de Haagse Hogeschool, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.

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

Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Online criminaliteit onder bedrijven: Een onderzoek naar slachtofferschap van online criminaliteit onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland.* NHL Hogeschool/Politieacademie/Open Universiteit.

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security, 77*, 860–870.

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286-296.

Wang, B., Liu, L., Li, F., Zhang, J., Chen, T., & Zou, Z. (2019, December). Research on web application security vulnerability scanning technology. In *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* (Vol. 1, 1524-1528). IEEE.

Werlinger, R., Muldner, K., Hawkey, K. and Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security, 18*(1), 26-42.

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

Bijlage I – Juridische risicobeoordeling

Beoordeling van juridische risico's bij geautomatiseerde beveiligingscontroles voor websites

1| Inleiding

Het CCV, de Haagse Hogeschool en ThreadStone hebben ICTRecht benaderd met het verzoek een risicobeoordeling uit te voeren ten aanzien van ThreadRisk, een dienst van ThreadStone die op geautomatiseerde wijze de beveiligingsrisico's van websites in kaart brengt.

Bij het in kaart brengen van verschillende risico's die mogelijk spelen ten aanzien van een bepaalde website wordt de website zelf beoordeeld en raadpleegt ThreadRisk openbare bronnen om een beeld van de informatiebeveiliging te vormen. Zo kan er bijvoorbeeld worden gecontroleerd of er gevoelige gegevens van medewerkers online staan, de e-mailserver op een blacklist staat, het websiteverkeer versleuteld plaatsvindt en of de softwareversies van websites zijn afgeschermd.

Hoewel er zoals gezegd gebruik wordt gemaakt van openbare bronnen, betekent openbaarheid nog niet altijd dat de informatieverzameling en het gebruik ook *rechtmatig* zijn. Zo kunnen er privacyrechtelijke bezwaren bestaan bij het verwerken van de betreffende gegevens, kunnen er op de gegevens auteurs- of databankrechten rusten en kunnen er – meer in algemene zin – schadeclaims ontstaan op grond van onrechtmatige daad wanneer derde partijen overlast ondervinden aan de informatieverzameling. Tot slot moet er aandacht worden besteed aan het feit dat veel veiligheidsonderzoeken waar geen toestemming voor is verkregen door de onderzochte partij op bepaalde punten kunnen grenzen aan computervredebreuk.

In dit memo wordt ingegaan op de eventuele aanwezigheid van de hiervoor beschreven juridische problematiek ten aanzien van elk van de onderzoeken ('controles') die via ThreadRisk worden uitgevoerd.

2 | Juridische risico's bij controles

Via ThreadRisk worden de volgende controles uitgevoerd. Hieronder wordt per controle ingegaan op de aanwezigheid van juridische problematiek zoals benoemd in de inleiding.

Controle
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?
Is uw website gereed voor nieuwe standaarden?
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?

Controle 1, controle 2 en controle 3 | Malware en spam

Om na te gaan of de website en/of de relevante server mogelijk in worden gezet om malware en/of spam te verspreiden wordt er gebruik gemaakt van gepubliceerde blacklists. Deze blacklists zijn bedoeld en gepubliceerd om dergelijke controles mogelijk te maken. Hoewel ThreadStone niet heeft aangegeven welke blacklists zij precies raadpleegt, is het daarom onwaarschijnlijk dat het raadplegen en gebruiken ervan onrechtmatig is of problemen oplevert in het kader van de problematiek die is beschreven in hoofdstuk 1.

Controle 4 | Openbaarheid gevoelige gegevens

Om te controleren of gevoelige gegevens geassocieerd met e-mailadressen die bij de domeinnaam van de website horen eventueel openbaar toegankelijk zijn, maakt ThreadRisk gebruik van zogenaamde 'password dumps' en andere openbare lekken van logingegevens.

Bij deze toepassing van ThreadRisk wordt – ten aanzien van afnemers van ThreadRisk – slechts het domein van de betreffende e-mailadressen verwerkt, om te zien of er mogelijk adressen met het relevante websitedomein voorkomen in de password dumps en lekken.

Algemene verordening gegevensbescherming

Wat echter niet moet worden vergeten is dat de password dumps en lekken óók persoonsgegevens bevatten – niet alleen de persoonsgegevens van medewerkers van de afnemer (bij een match), maar ook die van derde partijen waar ThreadRisk op wordt ingezet (al dan niet met medeweten van die partijen) en de andere slachtoffers die in de password dump staan opgenomen.

Het verwerken van lijsten met e-mailadressen en wachtwoorden is een verwerking van persoonsgegevens in de zin van de Algemene verordening gegevensbescherming ("AVG"). ThreadStone moet dus een grondslag hebben voor de verwerking van deze persoonsgegevens via ThreadRisk. Voor verwerking van de persoonsgegevens van medewerkers van afnemers van ThreadRisk die hun eigen website scannen zou de grondslag 'uitvoering van de overeenkomst' kunnen worden gebruikt.[9] Immers is verwerking van deze gegevens – in het geval van een match met een gegeven uit een password dump – nodig om de ThreadRisk dienst te kunnen leveren.

Voor de overige gegevens die in de password dump staan opgenomen is de grondslag het gerechtvaardigd belang.[10] Er is sprake van een gerechtvaardigd belang als de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen. De relevante belangen betreffen zowel ThreadStone's eigen belang om de dienstverlening aan te kunnen bieden als ook het belang van haar klanten om gelekte wachtwoorden op te sporen en zo hun (online) veiligheid te verbeteren. Dit belang dient afgewogen te worden tegen het belang van de overige betrokkenen. De overige betrokkenen zijn in dit geval de rest van de mensen wiens persoonsgegevens in de password dumps staan. De mensen in deze lijsten kunnen in principe in twee categorieën ingedeeld worden: werknemers van het bedrijf dat gecheckt wordt en anderen (mensen die er niets mee te maken hebben).

[9] Artikel 6(1)(b) Algemene verordening gegevensbescherming.
[10] Artikel 6(1)(f) Algemene verordening gegevensbescherming.

Het is goed te beargumenteren dat de belangenafweging in het voordeel van ThreadStone uitvalt. Voor de overige betrokkenen is de impact van de verwerking klein. Het doorzoeken is voor ThreadStone vereist om de gegevens van klanten te vinden, maar ThreadStone doet verder niets met die gegevens. Het risico dat de betrokkenen lopen komt doordat hun gegevens gelekt zijn (en dus op die lijsten terecht zijn gekomen) en niet de verwerking van ThreadStone. Of de verwerking door ThreadStone nu wel of niet uitgevoerd wordt, verandert niets aan de situatie van de betrokkenen.

Mocht het zo zijn dat ThreadRisk wordt ingezet om de website van een derde te beoordelen (dus *niet* de website van de directe afnemer van ThreadRisk) dan gaat de eerdergenoemde grondslag 'uitvoering van de overeenkomst' niet op. Er bestaat dan immers (in de meeste gevallen) geen overeenkomst tussen de eigenaar van de website en ThreadStone. Dit betekent dat gegevens van personen met een emailadres bij het betreffende domein sowieso niet op grond van de uitvoering van de overeenkomst kunnen worden verwerkt. Dit is ook altijd het geval wanneer het betreffende domein ook e-mailadressen bevat van mensen die geen werknemersrelatie (of een andersoortige overeenkomst waar de betreffende verwerking uit kan volgen) hebben met de eigenaar van de website – zelfs wanneer die websitehouder een directe afnemer is van ThreadRisk.

Gezien het bovenstaande beveelt ICTRecht aan om de verwerking in beide gevallen – dus zowel de eventuele e-mailadressen binnen het domein waar een match mee is in de password dumps als de overige betrokkenen – te stoelen op de grondslag van het gerechtvaardigd belang.

Controle 5 | Vatbaarheid e-mail voor misbruik

De voor deze controle relevante DMARC-, SPF-, DKIM-instellingen worden opgehaald uit de publieke DNS records. Het ophalen en gebruiken van deze informatie om ThreadRisk te leveren is rechtmatig en levert geen problemen op in het licht van de problematiek die is beschreven in hoofdstuk 1.

Controle 6 | Compatibiliteit nieuwe standaarden

Om na te gaan of de website IPv6 ondersteunt wordt er – net als bij controle 5 – gebruik gemaakt van informatie opgenomen in publieke DNS records, waardoor ook controle 6 als rechtmatig te beschouwen is en geen problemen oplevert vanuit de perspectieven genoemd in hoofdstuk 1.

Controle 7 | Vatbaarheid verkeer voor onderschepping

Om te controleren of de website de nieuwste SSL/TLS standaarden hanteert wordt er een simpele geautomatiseerde check uitgevoerd. Deze informatie is te allen tijde inzichtelijk voor alle bezoekers van de website en in dat kader ook gericht op deze precieze informatievoorziening. Opvraag en gebruik van deze informatie is dus volledig rechtmatig en levert geen juridische problematiek op.

Controle 8 | Ongebruikelijke aanvalspaden

Via ThreadRisk worden er geautomatiseerde 'port scans' uitgevoerd om na te gaan of er onnodig poorten open staan die door kwaadwillende derden kunnen worden gebruikt om een aanval op de website te verwezenlijken. De Hoge Raad heeft bepaald dat enkel het uitvoeren van een port scan geen

'binnendringing' is in de zin van computervredebreuk.[11] ThreadStone mag dit dus doen om ThreadRisk te kunnen leveren. Het moet dan uiteraard wel bij port scans blijven.

Controle 9 | Bescherming bezoekers

Om na te gaan of de website, naast de nieuwste versleutelingsstandaarden te hanteren, tevens de juiste securityprotocollen afdwingt bij bezoekers, wordt net zoals bij controle 7 gebruik gemaakt van informatie die de website altijd publiceert op het moment dat men deze aanspreekt, wat betekent dat het ophalen en gebruiken van deze informatie in het kader van ThreadRisk als rechtmatig kan worden beschouwd.

Controle 10 | Afscherming configuratie

Net zoals in het geval van controle 7 en controle 9, wordt er in het geval van controle 10 gekeken naar informatie die de website te allen tijde publiceert, om te kijken of het mogelijk is voor (kwaadwillende) bezoekers van de website om te achterhalen welke softwareversies er worden gebruikt door de website. Waarmee deze bezoekers op gerichte wijze op zoek zouden kunnen gaan naar kwetsbaarheden die zij kunnen exploiteren om de website binnen te dringen. Omdat het hier weer informatie betreft die te allen tijde publiek is en bedoeld is voor dit specifieke type informatievoorziening, is gebruik van deze informatie ook als rechtmatig te beschouwen. Hier geldt hetzelfde als bij controle 8: het moet natuurlijk wel blijven bij het *aftasten* van kwetsbaarheden. Deze mogen niet daadwerkelijk gebruikt worden.

Controle 11 | Vatbaarheid verkeer voor manipulatie

Om te controleren of er sprake kan zijn van omleiding van websiteverkeer door kwaadwillende derden naar een ander adres, wordt gebruik gemaakt van publieke DNS-records om na te gaan of er sprake is van een AAA-record of een DNSsecrecord. Opvraag en gebruik van deze informatie is dus, net als bij de controles 5 en 6 rechtmatig en levert geen juridische problemen op zoals beschreven in hoofdstuk 1.

3 | Conclusie

In het kader van de in hoofdstuk 1 beschreven juridische invalshoeken is er bij de verschillende controles sprake van rechtmatige opvraag en rechtmatig gebruik van de betreffende gegevens. Immers gaat het in bijna alle gevallen om informatie die rechtmatig is gepubliceerd en soms zelfs expliciet bedoeld is voor de doeleinden die ThreadStone ermee voor ogen heeft.

In het geval van het nalopen van password dumps behoeft dit nog wel een kanttekening. Hierbij is er namelijk sprake van de verwerking van persoonsgegevens. Op basis van de AVG moet daar een wettelijke grondslag voor zijn. Hoewel er in die context meerdere mogelijkheden zijn, raadt ICTRecht aan om de verwerking van *alle* persoonsgegevens in het kader van de password dumps te stoelen op de grondslag van het gerechtvaardigd belang.

Allicht ten overvloede: het is uiteraard – bij nagenoeg alle beschreven controles – van groot belang dat het bij het *aftasten* van beveiligingsrisico's blijft. Het onderzoek mag niet verder gaan dan dat.

[11] Hoge Raad 8 januari 2019, ECLI:NL:HR:2019:560.

Bijlage II – Interviewprotocol

Algemene inleiding

- Dank voor uw deelname aan dit interview/gesprek.
- Mijn naam is … en ik ben onderzoeker aan het Centre of Expertise Cyber Security van de Haagse Hogeschool.
- Zoals u misschien weet zijn wij bezig met een nieuwe interventie gericht op het verhogen van cyberweerbaarheid van ondernemers.
- Doel van interview:
    - Beeld krijgen van wat er bij externe partijen van dit project wordt verwacht en waar behoeftes liggen
    - Wat dit project zou kunnen betekenen voor uw organisatie
    - Welke knelpunten u ziet in dit project
- Interview zal ongeveer een uur duren.
- Het interview wordt anoniem verwerkt en in de rapportage zullen de resultaten niet herleidbaar zijn naar u.
- We willen het interview graag opnemen ter bevordering van de uitwerking ervan. Gaat u daarmee akkoord? *start opname*

Dan wil ik graag beginnen met het interview.

1. Wat is uw beroep en binnen welke organisatie bent u werkzaam?

Projectbeschrijving

- Ons project is gericht op het verhogen van de cyberweerbaarheid van ondernemingen
- Naast onze onderzoeksgroep zijn een aantal partijen betrokken bij het project: Platvorm Veilig Ondernemen (PVO) Den Haag, een aantal Zuid Hollandse gemeenten en Threadstone *(heeft de scan ontwikkeld)*
- In dit project gaan wij een door ons ontwikkelde interventie testen
- Deze interventie bestaat uit een geautomatiseerde kwetsbaarheidsscan en een aanvullend op maat gemaakt adviesrapport.
- Het gaat om een geautomatiseerde meting waarbij gebruik gemaakt wordt van open source data over kwetsbaarheden.
- Een uitvoerende partij kan dus kiezen voor deze interventie, een regio of doelgroep bepalen en de hele groep laten scannen. Deze geautomatiseerde scan scant bijvoorbeeld alle ondernemingen in een bepaald bedrijventerrein, zonder dat de ondernemingen hiervan op de hoogte zijn.
- De uitvoerder van de interventie voert alle domeinnamen in van de geselecteerde bedrijven. De geautomatiseerde kwetsbaarhedenmeting controleert op zwakke plekken met betrekking tot de website en de mailserver.
- De scan en het rapport gaan in op 3 van de 5 basisprincipes van veilig digitaal ondernemen van DTC: inventariseren van kwetsbaarheden, updates uitvoeren en malware voorkomen.

- Op basis van de scans ontvangen de ondernemers een individueel rapport met een handelingsperspectief waarmee zij de weerbaarheid van de onderneming kunnen verhogen.
- Hierna volgt nog een geautomatiseerde nameting om de interventie te toetsen, deze resultaten maken inzichtelijk of de cyberweerbaarheid daadwerkelijk is verhoogd.
- *Indien respondent vraagt naar voorbeelden: De scan brengt bijvoorbeeld in kaart 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.*

Algemene projectvragen

[indien respondent bij dit onderdeel vooral ingaat op knelpunten, geef dan aan dat je daar in het volgende deel van het interview graag bij stil wil staan en stuur terug naar de vraag]

2. Wat is, na de gegeven introductie, uw algemene/eerste indruk van dit project?
3. Hoe denkt u dat een automatische kwetsbaarhedenmeting iets zou kunnen betekenen voor uw partij/bedrijf?
4. Wat verwacht u/uw organisatie uit dit project te kunnen halen?
5. a. Welke andere behoeften zou uw organisatie hebben ten aanzien van dit project?
   b. Welke aanvullende informatie zou u graag verkrijgen vanuit een automatische kwetsbaarhedenmeting?
6. Op basis van de eerder gegeven informatie, verwacht u dat u of uw organisatie mee zou willen doen aan dit project?

Knelpunten/moeilijkheden

7. Welke (eventuele) knelpunten verwacht u bij de uitvoering van dit project? Wanneer deze er zijn, waar zitten deze volgens u?
8. Hoe denkt u dat het project juridisch gezien in elkaar steekt?

Eerdere soortgelijke projecten

9. Heeft u ervaring met eerdere projecten over soortgelijke onderwerpen of onderzoeksmethoden?
10. *Aanvulling nadat vorige vraag beantwoord is:* Eventueel nog soortgelijke projecten met bijvoorbeeld ondermijning als onderwerp i.p.v. cyberweerbaarheid?

Bereiken deelnemers

11. Wat is denkt u de beste route is om zo veel mogelijk ondernemers en bedrijven te kunnen scannen en adviseren? Via welke partijen zouden wij deze interventie moeten uitvoeren?
12. Denkt u dat het een goede route zou zijn via
    a. De Kamer van Koophandel?
    b. de gemeente?
    c. Iets anders?

13. In dit project willen we ook graag de scans tussen ondernemers vergelijken. Bijvoorbeeld per branche of per regio. Daarvoor hebben we dit soort gegevens nodig. Heeft u een suggestie over hoe wij snel aan data over bedrijven kunnen komen?
    a. Denk aan achtergrondkenmerken van de onderneming zoals postcode, aantal medewerkers, in welke branche zitten de bedrijven etc.
14. Welke kenmerken vinden jullie interessant om nog mee te vergelijken?

Tot slot

15. Wanneer is dit project volgens u een succes? Wanneer juist niet?
16. Zijn er bepaalde wensen vanuit uw organisatie die u graag terugziet in dit project?