**Inzicht in motivaties en barrières door doelgroepsegmentatie**

# Veilig digitaal ondernemen

**TNO Publiek ⟩ TNO 2024 R10701**

**April 2024**

**Defence, Safety & Security**
www.tno.nl
+31 88 866 15 00
info@tno.nl

TNO 2024 R10701 – April 2024

# Veilig digitaal ondernemen

## Inzicht in motivaties en barrières door doelgroepsegmentatie



| | |
|---|---|
| Auteurs | Tineke Hof, Rick van der Kleij, Silke Mergler |
| Rubricering rapport | TNO Publiek |
| Titel | TNO Publiek |
| Rapporttekst | TNO Publiek |
| Bijlagen | TNO Publiek |
| Aantal pagina's | 72 (excl. voor- en achterblad) |
| Aantal bijlagen | 6 |
| Opdrachtgever | Digital Trust Center |

# Samenvatting

**Probleemstelling en onderzoeksvraag**
Wanneer bedrijven slachtoffer worden van een cyberincident, krijgen ze te maken met financiële gevolgen, dataverlies en mogelijke schade aan hun reputatie. Het goede nieuws is echter dat veel incidenten kunnen worden voorkomen of een verminderde impact kunnen hebben wanneer beschermende maatregelen worden genomen. Deze maatregelen kunnen eenvoudige acties omvatten, zoals het regelmatig updaten van software, het maken van back-ups of het implementeren van multifactorauthenticatie. In dit onderzoek noemen we dit 'veilig digitaal ondernemen'.

Ondanks dat deze acties eenvoudig lijken en er veel partijen zijn die advies geven over de implementatie ervan, voeren bedrijven ze niet altijd uit. Dit komt door verschillende barrières die hen ervan weerhouden actie te ondernemen om hun digitale weerbaarheid te verbeteren. Sommige ondernemers geloven bijvoorbeeld niet dat cyberdreigingen een risico voor hen vormen, terwijl anderen de mogelijke impact van deze incidenten onderschatten of niet weten welke stappen ze kunnen nemen om zich ertegen te beschermen.

Een deel van de doelgroeporganisaties van het Digital Trust Center (DTC), het niet-vitale bedrijfsleven, neemt nog onvoldoende beschermende maatregelen tegen cyberdreigingen. Het DTC heeft TNO gevraagd om te onderzoeken hoe de actiebereidheid onder de doelgroeporganisaties van het DTC vergroot kan worden. Het doel van het onderzoek is om inzicht te geven in de motivaties en barrières die verschillende bedrijven ervaren bij veilig digitaal ondernemen. Op basis van dit inzicht kan het DTC deze doelgroeporganisaties gericht ondersteunen met producten en diensten om daadwerkelijke gedragsverandering te realiseren, met als gevolg een verhoogde cyberweerbaarheid. Om deze hoofdvraag te beantwoorden, zijn de volgende drie deelvragen geformuleerd:
1. Op welke doelgroeporganisaties zou het DTC zich moeten richten?
2. Waarom nemen deze bedrijven niet de noodzakelijke maatregelen om zichzelf beter te beschermen?
3. Hoe kan het DTC hierop reageren?

**Aanpak van het onderzoek**
Via psychografische segmentatie hebben we onderzocht welke groepen bedrijven onvoldoende beschermende maatregelen nemen. Traditionele segmentatie op basis van bedrijfseconomische of geografische kenmerken (bijvoorbeeld omzet, bedrijfstak, vestigingsplaats) schiet tekort in het begrijpen van de redenen achter het gedrag van ondernemers. Psychografische segmentering verdeelt bedrijven op basis van motviates en barrières, wat inzicht geeft in waarom ondernemers (on)voldoende veilig digitaal ondernemen.

Om de doelgroeporganisaties van het DTC te segmenteren hebben we medio 2023 een vragenlijstonderzoek uitgevoerd onder een steekproef van de volwassen Nederlandse beroepsbevolking. Het onderzoek richtte zich op veilig digitaal ondernemen en bevroeg 795 ondernemers die eindverantwoordelijk of (mede)beslisser zijn voor veilig digitaal ondernemen binnnen hun bedrijf. De variable veilig digitaal ondernemen werd gemeten aan de hand van 11 stellingen over gedragingen op dit gebied, gebaseerd op de Basisscan Cyberweerbaarheid van het DTC[1].

[1] https://www.digitaltrustcenter.nl/tools/doe-de-basisscan-cyberweerbaarheid

Op de verzamelde data zijn meerdere analyses uitgevoerd. Met een regressieanalyse hebben we de relaties tussen veilig digitaal ondernemen en mogelijke motivaties en barrières onderzocht. De uitkomsten van deze analyse laten zien welke variabelen van invloed zijn op veilig digitaal ondernemen. Er is vervolgens een latente klassenanlyse uitgevoerd om de doelgroeporganisaties te kunnen verdelen in groepen. Binnen een groep lijken de bedrijven op elkaar, terwijl bedrijven in de verschillende groepen van elkaar verschillen op basis van de gemeten kenmerken. De bevindingen uit deze analyses zijn gebruikt om stapsgewijs interventie-ideeen te bepalen met als doel verschillende groepen bedrijven te kunnen bereiken en tot actie te bewegen. Ook is er een voorspellingsmodel ontwikkeld waarmee kan worden bepaald tot welk segment een bedrijf waarschijnlijk behoort.

**Resultaten**
De doelgroeporganisaties zijn op te delen in vijf doelgroepen. Deze groepen verschillen van elkaar wat betreft de mate van veilig digitaal ondernemen en onderliggende gedragsbepalers.

**Voorlopers (22%)**
Bedrijven binnen deze groep laten een patroon zien van het nemen van alle vereiste beschermende maatregelen. Ze zijn in staat om deze maatregelen te nemen, hebben de hulpbronnen om dat te doen en zijn zeer gemotiveerd. Bedrijven in deze groep kunnen worden aangemoedigd om nog vaker een wachtwoordmanager te gebruiken om hun wachtwoorden te beheren. Daarnaast kunnen deze bedrijven een belangrijke rol spelen bij het ondersteunen van andere bedrijven, bijvoorbeeld door hun kennis door te delen via het online platform van de DTC community.

**Uitbesteders (12%)**
Ook bedrijven in deze groep scoren hoog op veilig digitaal ondernemen, maar niet zo hoog als Voorlopers. Ze zijn qua gedragsbepalers vergelijkbaar met Voorlopers, maar zijn van mening dat het nemen van beschermende maatregelen niet de verantwoordelijkheid is van hun eigen organisatie, en besteden hun cybersecurity in grote mate uit aan externe IT-serviceproviders (72%). Het DTC kan bedrijven in deze groep helpen met producten en diensten die hen ondersteunen bij het uitbesteden van IT-diensten, zoals sjablonen voor service level overeenkomsten en richtlijnen voor gesprekken met IT-dienstverleners. Ook kunnen bedrijven in deze groep worden aangemoedigd om nog vaker een wachtwoordmanager te gebruiken om hun wachtwoorden te beheren.

**Overmoedigen (30%)**
Overmoedigen vertonen een patroon van het nemen van beschermende maatregelen, maar in mindere mate dan Voorlopers en Uitbesteders. Ze onderschatten de gevolgen van een cyberbeveiligingsincident. Deze organisaties geven niet veel om hoe hun organisatie bekend staat bij hun klanten en relaties wat betreft de mate van cyberveiligheid in hun bedrijfsvoering en denken dat de kans om slachtoffer te worden klein is. Bedrijven in deze groep kunnen worden aangemoedigd om hun response op een cyberincident uit te werken. Ook kan het DTC het gebruik van een wachtwoordmanager stimuleren.

**Machtelozen (18%)**
Machtelozen nemen onvoldoende beschermende maatregelen. Ze hebben weinig kennis, vaardigheden en hulpbronnen om zichzelf te beschermen. Ze onderschatten de gevolgen van een cyberbeveiligingsincident echter niet, en denken dat de kans om slachtoffer te worden aanwezig is. Voor bedrijven in deze groep kan het DTC benadrukken dat het invoeren van tweefactorauthenticatie

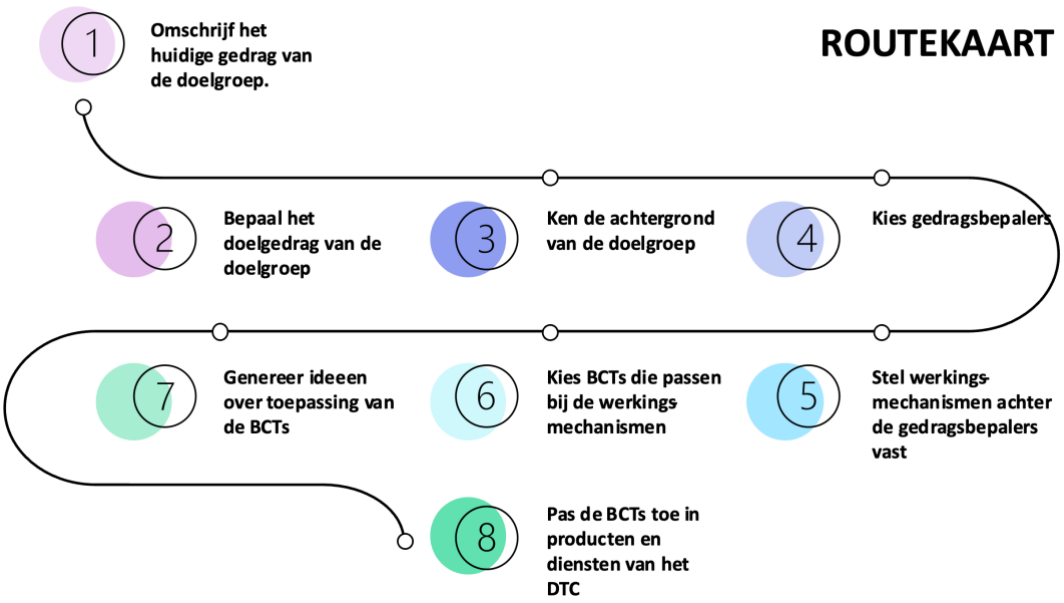
om accounts te beschermen van grote waarde is. Daarnaast is het belangrijk om regelmatige updates van software en systemen aan te moedigen.

**Onverschilligen (18%)**

Onverschilligen nemen onvoldoende beschermende maatregelen. Tegelijkertijd zijn ze niet overtuigd dat het nemen van aanbevolen maatregelen daadwerkelijk de dreiging zal verminderen, ze zijn niet gemotiveerd om hun organisatie te beschermen en denken dat de kans om slachtoffer te worden klein is. Het DTC kan bedrijven in deze groep ondersteunen bij het identificeren van kwetsbaarheden in hun systemen. Ook is het van belang om hen aan te moedigen om hun response op een cyberincident uit te werken. Bovendien is het nodig om het gebruik van zowel tweefactorauthenticatie als een wachtwoordmanager te stimuleren.

Deze segmentering biedt het DTC inzicht in de behoeften en uitdagingen van de verschillende groepen op het gebied van veilig digitaal ondernemen. Met deze kennis kan het DTC de groepen gerichter ondersteunen bij het nemen van beschermingsmaatregelen.

Op het gebied van het treffen van maatregelen voor veilig digitaal ondernemen zijn er drie doelgroepen die achterblijven. Deze groepen worden aangeduid als de Overmoedigen, Machtelozen en Onverschilligen. Samen vormen zij 66% van de bedrijven. Het is van belang dat het DTC hen gericht aanmoedigt om specifieke cyberbeschermingsmaatregelen te treffen. Bedrijven in deze groepen hebben te maken met verschillende factoren die hen belemmeren om daadwerkelijk maatregelen te nemen. Het DTC kan via een reeks stappen tot interventies komen die aansluiten bij de behoeften van elke specifieke doelgroep. Voor de doelgroepen Overmoedigen, Machtelozen en Onverschilligen zijn specifieke routekaarten ontwikkeld. De algemene stappen zijn weergegeven in de onderstaande routekaart[2].




**Figuur S.1:** Routekaart om te komen tot interventies.

[2] In de routekaart wordt de afkorting BCTs gebruikt. Dit staat voor 'Behavior Change Techniques', ofwel gedragsveranderingstechnieken. BCTs zijn systematische procedures die zijn opgenomen als een actief onderdeel van een interventie om gedrag te veranderen.

**Aanbevelingen**
Uit dit onderzoek zijn twee strategische aanbevelingen voortgekomen. Deze aanbevelingen geven het DTC richting bij het vergroten van de actiebereidheid van de doelgroeporganisaties en het bewerkstelligen van daadwerkelijke gedragsverandering.

1. Uitwerking, implementatie en evaluatie van stimulerende maatregelen voor een algemeen weerbaardere doelgroep, zodat doelgroeporganisaties daadwerkelijk stappen ondernemen om hun situatie te verbeteren. Het huidige onderzoek heeft aangetoond welke specifieke motivaties en barrières er zijn voor bepaalde doelgroepen. Ook zijn er voorbeelden gegeven van interventies die bedrijven in deze doelgroepen kunnen motiveren om stappen te zetten om hun eigen cyberweerbaarheid te vergroten óf anderen te helpen bij het nemen van maatregelen (bijvoorbeeld door 'voorlopers' te ondersteunen bij het helpen van 'achterblijvers'). Deze aanbeveling richt zich op het uitwerken, implementeren en evalueren van specifieke stimulerende maatregelen die zijn afgestemd op de verschillende factoren die het gedrag van ondernemers beinvloeden en die bepalend zijn voor hun beslissing om al dan niet actie te ondernemen. Een uitdaging hierbij is om ook die ondernemers te bereiken die van nature geen reden zien om actie te ondernemen, ongeacht de kwaliteit en beschikbaarheid van hulpbronnen. Deze groep neemt soms weloverwogen het risico op een cyberincident voor lief.

2. Zorg ervoor dat geschikte producten en diensten beschikbaar zijn via passende, bekende en toegankelijke kanalen. Deze aanbeveling richt zich op het bereiken van specifieke doelgroepen, inclusief de moeilijk bereikbare. Deze doelgroepen hebben uiteenlopende behoeften, varierend van uitleg over basismaatregelen tot meetinstrumenten om weerbaarheidsniveaus in kaart te brengen en ondersteuning bij risicoanalyses. Het DTC kan gebruik maken van de verkorte vragenlijst die in dit onderzoek is ontwikkeld om bedrijven door te verwijzen naar naar passende producten en diensten. Bovendien blijkt uit dit onderzoek dat bedrijven in de verschillende groepen verschillende communicatiekanalen gebruiken om zichzelf te informeren over veilig digitaal ondernemen. Dit benadrukt het belang van maatwerk bij het leveren van producten en diensten. Deze producten en diensten moeten bovendien makkelijk toegankelijk zijn waarbij verspreiding, ook in de toekomst, plaatsvindt via een centraal loket.

# Inhoudsopgave

# 1 Inleiding

## 1.1 Aanleiding van het onderzoek

Het Cyber Security Beeld Nederland (CSBN) 2021 kopt “cyberaanvallen tasten zenuwstelsel maatschappij aan” en stelt dat cyberweerbaarheid in onze maatschappij nog onvoldoende is, waarbij een groot verschil in mate van weerbaarheid geconstateerd wordt tussen organisaties (NCTV, 2021). Ook recente versies van het CSBN bevestigen dit beeld. Het CSBN uit 2023 stelt bijvoorbeeld: “Er gaapt een kloof tussen organisaties die de cyberveiligheid op orde hebben en organisaties die dat niet hebben” (NCTV, 2023). Het CSBN uit 2023 constateert daarbij dat ondanks hun beste bedoelingen deze ‘achterblijvers’ niet altijd actie ondernemen.

Organisaties die niet onder de doelgroep van het Nationaal Cyber Security Centrum (NCSC) vallen (vitale aanbieders en Rijksoverheid), kunnen sinds 2018 terecht bij het Digital Trust Center (DTC) voor ondersteuning. De missie van het DTC is om deze bedrijven (ruim twee miljoen) weerbaarder te maken tegen toenemende cyberdreigingen[3], alles van zzp'ers tot en met het grootbedrijf. Het DTC bedient deze bedrijven met praktische kennis, instrumenten, dreigingsinformatie [4] en mogelijkheden om samenwerkingsverbanden aan te gaan.

De producten van het DTC dragen naar verwachting bij aan het vergroten van het cybersecuritybewustzijn in het bedrijfsleven[5]. Dit is belangrijk, maar bewustzijn alleen is niet voldoende. Het gaat erom dat op basis van de producten en diensten die het DTC verstrekt ook actie wordt ondernomen om de weerbaarheid tegen cyberdreigingen te vergroten. Bedrijven moeten in actie komen en concrete maatregelen treffen. Het is nog grotendeels onduidelijk hoe de stap van bewustzijn via handelingsbereidheid naar daadwerkelijke veranderingen bij bedrijven kan worden gestimuleerd. Bedrijven verschillen daarbij in drijfveren om wel of niet te acteren op basis van de door het DTC aangeleverde (kennis)producten. Een advies dat het ene bedrijf aanzet tot het nemen van maatregelen kan onvoldoende aansluiten bij de behoeften en prioriteiten van een ander bedrijf, waardoor die geen actie onderneemt.

Het DTC heeft nog onvoldoende zicht op de impact van de producten en diensten die zij op dit moment beschikbaar stelt in relatie tot de diversiteit binnen doelgroep. Eerder onderzoek laat zien dat een belangrijk instrument van het DTC, de basisscan, leidt tot concrete gedragsverandering, maar onder slechts een deel van de doelgroep (Hoekstra, De Vries, Berkenpas & Jansen, 2021). Het DTC heeft daarom behoefte aan advies om haar producten en diensten gerichter en met meer impact in te zetten. Wetenschappelijke inzichten over methoden om te komen tot gedragsverandering kunnen in deze behoefte voorzien.

Het DTC heeft TNO gevraagd om het volgende te onderzoeken: hoe kan de actiebereidheid onder de doelgroeporganisaties van het DTC – het niet-vitale bedrijfsleven – vergroot worden om hun online beveiliging te verbeteren en daardoor daadwerkelijke gedragsverandering te realiseren met meer cyberweerbaarheid tot gevolg.

[3] https://www.security.nl/posting/673451/Ministerie+gaat+volgend+jaar+dreigingsinformatie+met+bedrijfsleven+delen
[4] https://www.digitaltrustcenter.nl/community
[5] https://www.digitaltrustcenter.nl/nieuws/cbs-publiceert-ict-kenmerken-van-dtc-bedrijven

Om deze hoofdvraag te beantwoorden zijn de volgende drie deelvragen geformuleerd: op *wie* (welke bedrijven) zou het DTC zich moeten richten; *waarom* nemen deze bedrijven niet de noodzakelijke maatregelen om zichzelf beter te beschermen en *hoe* kan het DTC reageren?

Voordat we beschrijven hoe we de onderzoeksvragen hebben beantwoord, definiëren we nu eerst als de achtergrond van het onderzoek de belangrijkste begrippen en modellen die we in het onderzoek hanteren.

## 1.2 Achtergrond en definities

In dit onderzoek is 'veilig digitaal ondernemen' centraal gesteld. Het ministerie van Economische Zaken en Klimaat (EZK) heeft het Digital Trust Center (DTC) opgericht om ondernemers hierbij te helpen. Hiertoe adviseert het DTC om 5 basisprincipes op te volgen: (1) Inventariseer kwetsbaarheden; (2) Kies veilige instellingen; (3) Voer updates uit; (4) Beperk toegang; (5) Voorkom virussen en andere malware.[6] Ondernemers die de vijf basisprincipes van veilig digitaal ondernemen opvolgen, vergroten hun *digitale weerbaarheid* tegen ernstige cyberincidenten. Veilig digitaal ondernemen is in deze studie gedefinieerd als: gedragingen van ondernemers in overeenstemming met de vijf basisprincipes van veilig digitaal ondernemen om de digitale weerbaarheid van de onderneming te bevorderen.

Digitale weerbaarheid is een verzamelnaam voor allerlei verschillende middelen en manieren om cybercriminaliteit tegen te gaan en de cybersecurity te verhogen (Hoekstra e.a., 2021), met als uiteindelijk doel het waarborgen van de bedrijfscontinuïteit (Björk, Henkel, Stirna & Zdravkovic, 2015; Dupont, Shearing, Bernier & Leukfeldt, 2023). In de literatuur worden vier vaardigheden gekoppeld aan de weerbaarheid van een organisatie (Van der Kleij & Leukfeldt, 2019). Het gaat daarbij om (1) anticiperen, (2) monitoren, (3) reageren en (4) leren. Dit houdt in dat men weerbaar is wanneer men weet (a) wat te verwachten, (b) waarop te letten, (c) wat te doen en (d) wat er is gebeurd (als het toch misgaat). Samenvattend kan worden geconcludeerd dat het binnen deze context in preventieve zin gaat om tegenstand te bieden tegen bekende en onbekende digitale dreigingen en in repressieve zin om snel en doeltreffend te kunnen herstellen als gevolg van een cyberincident. Dit laatste wordt veelal aangeduid met de term 'veerkracht'. Dit perspectief roept ook een meer holistische benadering op, waarbij beveiliging niet kan worden teruggebracht tot de som van alle technische tools die binnen een organisatie zijn ingezet, maar voortkomt uit de constante interacties van mensen, hardware, software en processen verweven in een dicht netwerk van interne en externe verbindingen (Dupont e.a., 2023).

De ondernemer speelt een belangrijke rol bij veilig digitaal ondernemen.[7] Hij of zij moet tenslotte besluiten om de vijf basisprincipes op te volgen. Om het gedrag van de ondernemer te beïnvloeden (en te verklaren) kan gebruik worden gemaakt van gedragsmodellen. In dit onderzoek is gebruik gemaakt van het *Behavioral change wheel* (Michie, Van Stralen & West, 2011). Dit model is gebaseerd op het idee dat gedrag wordt aangedreven door kennis, gelegenheid en motivatie. Dit model voorspelt dat veilig digitaal ondernemen afhangt van de kennis die de ondernemer bezit over risico's en manieren om zichzelf te beschermen, de gelegenheid die de ondernemer daartoe heeft en de mate waarin de ondernemer gemotiveerd is om dat ook daadwerkelijk te doen. Het model doet ook aanbevelingen over hoe gedrag is te beïnvloeden. Eerste toepassingen van dit gedragsmodel op cybersecurity zijn veelbelovend (zie bv. Van der Kleij, Van 't Hoff - De Goede, Van de Weijer & Leukfeldt, 2020; Van der Kleij, Wijn & Hof, 2020). Zo laten Van der Kleij, Hof en Wijn (2020) zien dat het model veilig digitaal werken verklaart van medewerkers in de financiële sector. Van der Kleij, Van

[6] https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

[7] Daar waar we ondernemer schrijven, bedoelen we ook anderen binnen het bedrijf met een verantwoordelijkheid voor digitale weerbaarheid.

't Hoff - De Goede, Van de Weijer & Leukfeldt (2020) laten zien dat het model tevens gebruikt kan worden om het online gedrag van burgers te verklaren.  De reden dat dit model is gebruikt in dit onderzoek, is vanwege de verwachting dat dit gedragsmodel een goed kader biedt voor het opstellen van een advies over stimuleringsmaatregelen voor het beïnvloeden van de handelingsbereidheid voor veilig digitaal ondernemen en het vergroten van de digitale weerbaarheid van de doelgroep van het DTC.

Gedragsmodellen zijn belangrijk om te begrijpen hoe gedrag beïnvloed kan worden. Maar net zo belangrijk is om te snappen welk type interventie aansluit bij welk type organisatie. Bijvoorbeeld als het gaat om de manier van overbrengen van informatie rondom een specifiek advies is het essentieel om de boodschap te laten aansluiten bij de ontvanger. Een recente studie uitgevoerd door het Britse Behavioural Insights Team in samenwerking met het NCSC UK laat zien dat via simpele boodschappen bedrijven kunnen worden aangezet tot het nemen van actie en dat het uitmaakt op welke manier deze boodschap wordt gebracht.[8] Een goed begrip van de verschillende typen doelgroeporganisaties en hun behoeften voor ondersteuning vanuit de overheid is hiervoor belangrijk.

Hiertoe is besloten om de doelgroep te segmenteren. Segmentatie is de praktijk waarbij een populatie in benaderbare groepen wordt verdeeld volgens bepaalde eigenschappen. In dit geval gebeurt dat om meer gepersonaliseerde interventies te kunnen creëren. Deze eigenschappen kunnen bijvoorbeeld demografische of bedrijfseconomische kenmerken zijn, zoals omvang, sector of regio. Zo'n demografisch kenmerk kan wel een gemeenschappelijk kenmerk van bedrijven (bijv. bedrijfsgrootte) zijn, maar het is niet per se een veroorzaker van het 'niet handelen'. En het kenmerk bedrijfsgrootte biedt ook niet een voor de hand liggend aanknopingspunt voor een bepaalde manier van interveniëren of communiceren. Onderliggende barrières en drijfveren worden dan over het hoofd gezien. In dit onderzoek is ervoor gekozen om te segmenteren op basis van psychografische kenmerken. Psychografische segmentatie verdeelt organisaties in groepen op basis van onderliggende motivaties en voorkeuren – de factoren die van invloed zijn op (on)veilig digitaal ondernemen. Daarbij helpt het om te bepalen hoe te reageren.

[8] "What would happen if your website was attacked?" | The Behavioural Insights Team (bi.team)

# 2 Aanpak van het onderzoek

In het onderzoek is gebruik gemaakt van verschillende dataverzamelingsmethoden. Zo zijn groepsinterviews (kwalitatief onderzoek) en enquêtes (kwantitatief onderzoek) met elkaar gecombineerd. Dit vergroot de geldigheid van het onderzoek. De verschillende methoden worden hieronder besproken.

## 2.1 Groepsinterviews

Als verkenning op het onderwerp veilig digitaal ondernemen en om een eerste segmentering te toetsen is gesproken met 20 ondernemers. De gesprekken vonden plaats eind 2022 in twee semigestructureerde groepsinterviews . De ondernemers die wij spraken kwamen uit verschillende sectoren en waren werkzaam bij bedrijven met verschillende groottes, inclusief zzp'ers. De sessies duurden ongeveer twee uur en werden via Microsoft Teams gehouden. Ondernemers zijn geworven door de onderzoekers via twee verschillende panels: de online DTC-community en het ondernemerspanel Ondernemersdenkenmee.nl, beiden van EZK. Ondernemers kregen een cadeaubon als dank voor hun deelname (zie ook Bijlage B).

## 2.2 Vragenlijstonderzoek

Om een antwoord te vinden op de deelvragen is medio 2023 een vragenlijstonderzoek uitgevoerd onder een steekproef van de Nederlandse beroepsbevolking. Deelnemers werden, in samenwerking met de onderzoekers, geworven door het panelbureau Motivaction. Het panel is ISO-gecertificeerd en bestaat uit meer dan 70.000 actieve deelnemers die zowel online als offline zijn geworven. Het panel vormt een goede afspiegeling van de Nederlandse bevolking op het gebied van kenmerken zoals opleiding, leeftijd, geslacht, regio en etniciteit.

Aan de vragenlijst hebben in totaal 795 ondernemers deelgenomen die eindverantwoordelijk zijn of (mede)beslisser voor veilig digitaal ondernemen binnen hun bedrijf, waaronder zzp'ers, mkb'ers en grootbedrijven tot 400 medewerkers.

De vragenlijst is door TNO gemaakt en is opgedeeld in vijf verschillende onderdelen: een deel om te bepalen of respondenten tot de doelgroep behoren, een aantal achtergrondvragen, een deel over veilig digitaal ondernemen, een deel over mogelijke gedragsbepalers en enkele vragen over het gebruik van informatiebronnen en gewenste ondersteuning door de overheid. De gehele vragenlijst bestond uit 47 vragen (zie Bijlage D).

De verschillende variabelen die met de vragenlijst zijn gemeten, worden hieronder in meer detail toegelicht.

### 2.2.1 Veilig digitaal ondernemen

Deze variabele werd gemeten door 11 stellingen over verschillende gedragingen met betrekking tot veilig digitaal ondernemen. De gedragsthema's en onderliggende specifieke gedragingen zijn

gebaseerd op de Basisscan Cyberweerbaarheid van het DTC[9], resulterend in 11 gedragingen verdeeld over de vijf basisprincipes[10] voor veilig digitaal ondernemen (zie ook par. 1.2).

Voor een overzicht van alle stellingen zie de vragenlijst in Bijlage D. Een voorbeeld is: “Mijn organisatie maakt regelmatig een back-up (reservekopie) van alle belangrijke informatie”.

Antwoordmogelijkheden voor respondenten waren: Zeer oneens; Oneens; Enigszins oneens; Niet eens, niet oneens; Enigszins eens; Mee eens; Zeer eens (7-punt Likert-type schaal) of Niet van toepassing. De hoogste score (7) wordt toegekend aan de veiligste antwoordoptie. De variabele veilig digitaal ondernemen is het gemiddelde van deze 11 scores. Als maat voor de betrouwbaarheid van deze meting voor veilig digitaal ondernemen is gekeken naar de Cronbach’s α (alfa) van de scores op de 11 stellingen. Een ondergrens voor deze maat is 0,70. De alfa voor deze meting is 0,89 waarmee is vastgesteld dat de meting bruikbaar is.

### 2.2.2 Gedragsbepalers

Mede gebaseerd op de resultaten van de groepsinterviews met ondernemers, hebben we aanvankelijk zes mogelijke obstakels gedefinieerd geformuleerd voor veilig digitaal ondernemen, namelijk:

- Zichzelf niet als potentieel slachtoffer zien;
- Onderschatten van de gevolgen van onveilig digitaal ondernemen;
- Niet weten hoe te beginnen met veilig digitaal ondernemen;
- Niet belangrijk vinden van veilig digitaal ondernemen;
- Veilig digitaal ondernemen niet hun verantwoordelijkheid vinden;
- De middelen niet hebben om veilig digitaal te ondernemen.

Voor het opstellen van de vragenlijst hebben we in de wetenschappelijke literatuur naar constructen gezocht voor elk van de verklaringen die ons in staat stellen om de benodigde gegevens te verzamelen.

In Tabel **2.1** staan per verklaring genoemd: relevante onderliggende psychologische constructen, details m.b.t. vragenlijstitems en bronvermelding.

[9] Doe de Basisscan Cyberweerbaarheid | Digital Trust Center (Min. van EZK)
[10] De 5 basisprincipes van veilig digitaal ondernemen | Digital Trust Center (Min. van EZK)

**Tabel 2.1:** Overzicht van gedragsbepalers.

| Verklaring | Psychologische constructen | Details (aantal items, Cronbach's α, voorbeelditem) | Bron |
|---|---|---|---|
| Zien zichzelf niet als potentieel slachtoffer | Waargenomen kwetsbaarheid *(perceived vulnerability)*; Slachtofferschap | Waargenomen kwetsbaarheid: 1 item.<br>"Hoe waarschijnlijk is het volgens jou dat jouw organisatie in de komende 12 maanden slachtoffer wordt van een cyberincident?"<br><br>Slachtofferschap: 1 item.<br>"Heeft bij jouw organisatie in de afgelopen 12 maanden een cyberincident plaatsgevonden?" | Weinstein (1987); Witte (1996) |
| Onderschatten de gevolgen van (on)veilig digitaal ondernemen | Response effectiviteit (*response efficacy*); Waargenomen ernst (*perceived severity*) | Response effectiviteit: 3 items, Cronbach's α = .860.<br>"Veilig digitaal ondernemen vermindert de kans om slachtoffer te worden van een cyberincident"<br><br>Waargenomen ernst: 3 items, Cronbach's α = .878.<br>"Ik vind dat cyberincidenten een ernstig probleem zijn voor mijn organisatie" | Witte (1996); Herath & Rao (2009); Champion & Skinner (2008); Dodel & Mesch (2017) |
| Weten niet hoe te beginnen met veilig digitaal ondernemen | Kennis; Vaardigheden | Kennis: 2 items, Cronbach's α = .898.<br>"Ik weet hoe ik veilig digitaal kan ondernemen"<br><br>Vaardigheden: 2 items, Cronbach's α = .744.<br>"Ik ben getraind om veilig digitaal te kunnen ondernemen" | Huijg e.a. (2014); Amemori e.a. (2011) |
| Vinden veilig digitaal ondernemen niet belangrijk | Protectie Motivatie Intentie (PMI); Reputatie (*reputation*); Prioriteit (*priority*); Bereidwilligheid | Protectie motivatie intentie: 2 items, Cronbach's α = .746.<br>"Wij zijn bereid er alles aan te doen om de organisatie te beschermen tegen cyberincidenten"<br><br>Reputatie: 2 items, Cronbach's α = .771.<br>"Wij willen een voorbeeld zijn voor andere organisaties op het gebied van veilig digitaal ondernemen"<br><br>Prioriteit: 3 items, Cronbach's α = .883.<br>"Andere onderwerpen op de agenda hebben een hogere prioriteit dan veilig digitaal ondernemen"<br><br>Bereidwilligheid: 2 items, Cronbach's α = .859.<br>"Onze organisatie is voornemens in de komende 12 maanden maatregelen te nemen om de digitale veiligheid te vergroten" | Herath & Rao (2009); Ajzen (1991); Huijg e.a. (2014) |
| Vinden veilig digitaal ondernemen niet hun verantwoordelijkheid | Verantwoordelijkheid; Controle (*locus of control*) | Verantwoordelijkheid: 1 item,<br>"Veilig digitaal ondernemen is de verantwoordelijkheid van mijn organisatie (vs. van anderen)"<br><br>Controle: 1 item,<br>"Veilig digitaal ondernemen ligt binnen de controle van mijn organisatie (vs. buiten de controle)" | Weinstein (1987); Workman e.a. (2008) |

| Verklaring | Psychologische constructen | Details (aantal items, Cronbach's α, voorbeelditem) | Bron |
|---|---|---|---|
| Hebben niet de middelen om veilig digitaal te ondernemen | Hulpbronnen (*resources*) | Hulpbronnen: 3 items, Cronbach's α = .739. "Om veilig digitaal te ondernemen heeft mijn organisatie de beschikking over voldoende financiële middelen" | Van der Kleij e.a. (2021); Huijg e.a. (2014) |

### 2.2.3 Controlevariabelen

In dit onderzoek is gewerkt met controlevariabelen. Dit zijn variabelen die niet per se bijdragen aan het beantwoorden van de hoofdvraag, maar waarvoor wordt gecontroleerd in bepaalde analyses, omdat ze de uitkomsten kunnen beïnvloeden. Om expliciet rekening te houden met mogelijke effecten van bedrijfsgrootte, economische sector, het ondersteund worden door een externe IT-dienstverlener en mate van digitalisering van bedrijven, hebben we voor deze variabelen statistisch gecontroleerd in de regressieanalyse door de data voor de controlevariabelen te modelleren samen met de data voor de onafhankelijke en afhankelijke variabelen. Op die manier zijn de effecten van de controlevariabelen geïsoleerd.

## 2.3 Analyses

Er zijn in dit onderzoek drie soorten analyses uitgevoerd op de data die is verzameld met de vragenlijst.

Ten eerste is een multivariate regressieanalyse gedaan om te onderzoeken welke factoren (gedragsbepalers) samenhangen met veilig digitaal ondernemen (afhankelijke variabele). Hiermee zijn de zes mogelijke obstakels getoetst voor veilig digitaal ondernemen (zie par 2.2.2). Hiermee kan de deelvraag worden beantwoord over *waarom* deze bedrijven niet de noodzakelijke maatregelen nemen om zichzelf beter te beschermen.

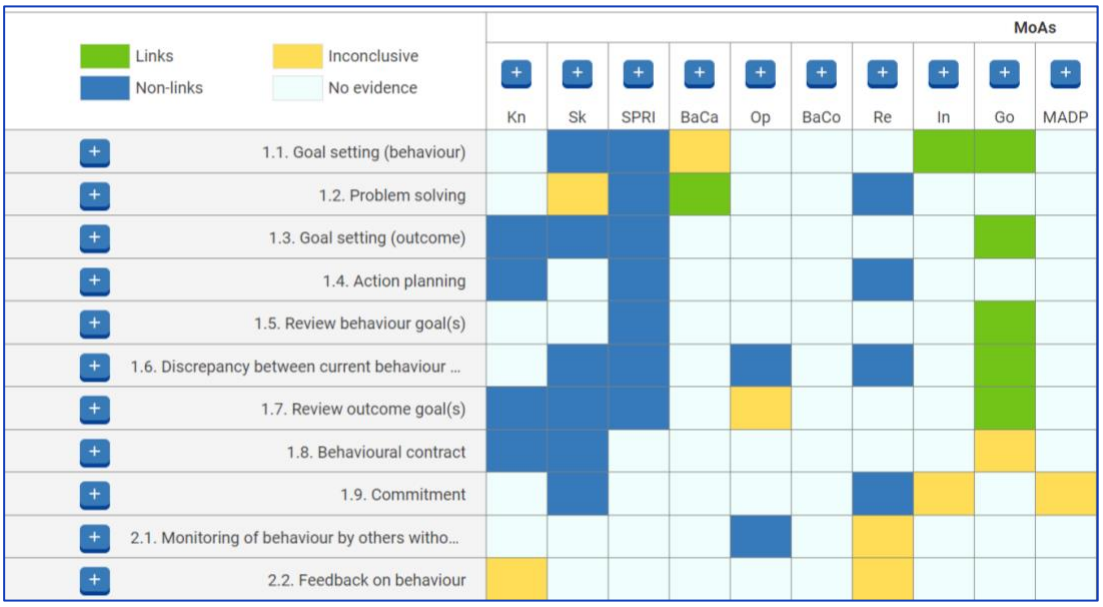
Ten tweede is een latente klassenanalyse uitgevoerd om de deelvraag te beantwoorden: op *wie* (welke bedrijven) zou het DTC zich moeten richten? Met een latente klassenanalyse kunnen in een populatie subgroepen (segmenten) worden geïdentificeerd van gelijksoortige eenheden op basis van hun kenmerken op een aantal van tevoren te bepalen variabelen. Er is gebruikt gemaakt van 14 variabelen: Veilig digitaal ondernemen, Kennis, Vaardigheden, Prioriteit, Waargenomen ernst, Hulpbronnen, Protectie Motivatie Intentie, Reputatie, Bereidwilligheid, Response-effectiviteit, Verantwoordelijkheid, Controle, Waargenomen kwetsbaarheid en Slachtofferschap (zie ook Tabel **2.1**.). Er zijn drie analyses uitgevoerd waarmee een 4-clusteroplossing, een 5-clusteroplossing, en een 6-clusteroplossing zijn gevormd. Een korte toelichting op de uitkomst van deze analyse staat in Bijlage F.

Ten derde is een voorspellingsmodel ontwikkeld. Hierbij is gebruik gemaakt van de software Latent Gold. Met dit model kunnen in de toekomst eenvoudig bedrijven worden gesegmenteerd. Vragenlijstitems met de grootste bijdrage aan het identificeren van de groepen zijn gebruikt voor het maken van een korte vragenlijst, ofwel het voorspellingsmodel. Daarbij is gekeken of er voldoende dekking is over de verschillende gedragsbepalers (gedrag, kennis, vaardigheid, etc.). Er is gestart door het panelbureau met een selectie van 17 items, vervolgens 12 en tenslotte 10. Bij het percentage voorspelling met het 10-item model kwam 1 segment uit vlak onder het stopcriterium van 80%. Het gemiddeld voorspellingspercentage van dit model is 83%. Door het panelbureau is verklaard dat een 10-item model met een gemiddeld voorspellingspercentage van 83% een zeer acceptabel resultaat is.

## 2.4 Identificeren van interventies

Om de derde deelvraag te beantwoorden; *hoe* kan het DTC reageren, is een stapsgewijs proces voor het identificeren van interventies gevolgd (zie Michie, Atkins & West, 2014). Per segment zijn telkens een of twee relevante gedragsbepalers gekozen. De keuze voor gedragsbepalers is gebaseerd op de resultaten van de verschillende analyses. Eerst is gekeken welke gedragsbepalers volgens de latente klasse analyse het meest kenmerkend zijn voor elk segment. Vervolgens is gekeken naar de resultaten van de regressieanalyse of deze gedragsbepalers ook daadwerkelijk van invloed zijn (statistisch significant) op veilig digitaal ondernemen.

Voor elk van de gekozen gedragsbepaler is een selectie bepaald van gedragsveranderingstechnieken (*Behavior Change Techniques*, ofwel BCTs)[11]. Een BCT is een systematische procedure die is opgenomen als een actief onderdeel van een interventie om gedrag te veranderen (Michie & Johnston, 2013). Een BCT is daarmee de kleinste component van een gedragsinterventie en kan alleen of in combinatie met andere BCTs worden gebruikt. BCTs specificeren dus de minimale inhoud van wat moet worden geleverd. Een BCT specificeert niet de wijze van uitvoering of levering. Het is mogelijk dat een bepaalde BCT op veel verschillende manieren wordt afgeleverd. Feedback kan bijvoorbeeld per brief of persoonlijk worden gegeven, aan groepen of aan een individu, eenmalig of frequent, door een persoon of via een automatisch elektronisch bericht. Voor het selecteren van BCTs hebben we gebruik gemaakt van de *Theory and techniques tool*[12]. Deze tool geeft voor een groot aantal gedragsbepalers een overzicht van effectieve BCTs (zie Figuur **2.1**).




**Figuur 2.1:** Deel van de *Theory and Techniques Tool* (humanbehaviourchange.org). Op de X-as (boven) staan gedragsbepalers. Op de Y-as (links) staan 93 verschillende BCTs. In de cellen is weergegeven welk bewijs er is voor effectiviteit van de BCT bij een gegeven gedragsbepaler.

Gedragsveranderingsinterventies omvatten een of meer BCTs. Voor een volledige specificatie van een gedragsveranderingsinterventie moeten zowel de actieve inhoud, dat wil zeggen de BCTs, als de wijze van uitvoering worden beschreven.

[11] Voor een overzicht van BCTs, zie bijvoorbeeld: https://www.bcts.23.co.uk/
[12] https://theoryandtechniquetool.humanbehaviourchange.org/tool

In een derde stap hebben de onderzoekers op basis van geselecteerde BCTs een aantal gedragsveranderingsinterventies bepaald voor elk van de kenmerkende gedragsbepalers per segment. Stel dat een belangrijke gedragsbepaler kennis is. Het ontbreekt de bedrijven in een segment aan de noodzakelijke kennis om veilig digitaal te werken. Een mogelijke BCT is het geven van instructie. In dit geval zou een BCT kunnen bestaan uit het stapsgewijs instructie geven over hoe gedrag in relatie tot veilig digitaal ondernemen moet worden uitgevoerd. Een specifieke gedragsveranderingsinterventie zou in dit geval kunnen zijn om deze instructie in een maandelijkse online workshopsetting voor ondernemers te laten verzorgen door het DTC.

In een vierde stap hebben de onderzoekers voor de segmenten Overmoedigen, Machtelozen en Onverschilligen, de gedragsbepalers, gedragsveranderingstechnieken en gedragsveranderingsinterventies procesmatig gevisualiseerd op zogenaamde routekaarten (zie Bijlage A). De routekaart biedt een leidraad voor hoe het proces voor het bepalen van aanvullende gedragsveranderingsinterventies doorlopen kan worden van keuze voor gedragsbepaler tot toepassing in producten en/of diensten.

In de vijfde stap hebben de onderzoekers samen met het DTC en het Behavioural Insights Team van het ministerie van Economische Zaken onderzocht of de geselecteerde BCTs terugkomen in de producten en diensten van het DTC. We hebben besproken welke bestaande producten en diensten geschikt zijn voor de segmenten die in dit onderzoek geïdentificeerd zijn. Daarnaast hebben we nagedacht over eventuele nieuwe producten en diensten op basis van de door ons geïdentificeerde BCTs. De bevindingen uit deze vijfde stap zijn verwerkt in de sectie ‘Interventies identificeren’.

# 3 Resultaten

## 3.1 Achtergrondkenmerken van de bedrijven

Tabel 3.1 geeft de grootte weer van de bedrijven waar de respondenten van het vragenlijstonderzoek werkzaam zijn. Hieruit blijkt dat 41% van de respondenten werkt als zzp'er. De minste respondenten zijn werkzaam bij een bedrijf met 250-400 werknemers.

**Tabel 3.1:** Aantal personen in dienst.

| Bedrijfsgrootte | Percentage | Aantal |
|---|---|---|
| Geen personeel (zzp'er) | 41 | 326 |
| 2-9 werknemers | 18 | 143 |
| 10-49 werknemers | 18 | 144 |
| 50-249 werknemers | 20 | 157 |
| 250-400 werknemers | 3 | 25 |
| Totaal | 100 | 795 |

Tabel 3.2 laat zien uit welke sectoren de bedrijven afkomstig zijn. Hieruit blijkt dat 19% van de bedrijven uit de sector zakelijke dienstverlening komt. De minste bedrijven zijn werkzaam in de sectoren Landbouw/ bosbouw/ visserij en delfstoffenwinning en overheid.

**Tabel 3.2:** Verdeling van de bedrijven over sectoren.

| Sector | Percentage | Aantal |
|---|---|---|
| Landbouw/ bosbouw/ visserij en delfstoffenwinning | 2,5 | 20 |
| Industrie en energie | 3,9 | 31 |
| Bouwnijverheid | 4,8 | 38 |
| Handel/ vervoer en horeca | 13,6 | 108 |
| Informatie en communicatie | 12,1 | 96 |
| Financiële dienstverlening | 9,6 | 76 |
| Verhuur en handel van onroerend goed | 3,5 | 28 |
| Zakelijke dienstverlening | 18,5 | 147 |
| Overheid | 2,5 | 20 |
| Onderwijs | 5,8 | 46 |
| Gezondheids- en welzijnszorg | 8,8 | 70 |
| Cultuur/ soort en recreatie | 5,3 | 42 |
| Overige branches/ diensten | 9,2 | 73 |
| Totaal | 100 | 795 |

In Tabel **3.3** is de mate van zelf-gerapporteerde digitalisering van de bedrijven weergegeven. Hieruit blijkt dat 14,5 % van alle bedrijven niet of nauwelijks is gedigitaliseerd. Het merendeel van bedrijven heeft dus een bepaalde mate van digitalisering en is daarmee (potentieel) kwetsbaar voor digitale incidenten of aanvallen.

**Tabel 3.3:** Mate van digitalisering van de bedrijven.

| Mate van digitalisering | Percentage | Aantal |
|---|---|---|
| Niet gedigitaliseerd | 14 | 115 |
| Gemiddeld gedigitaliseerd | 3 | 297 |
| Wel gedigitaliseerd | 46 | 368 |
| Weet niet/ geen mening | 2 | 15 |
| Totaal | 100 | 795 |

In de tabellen hieronder wordt elke kolom getoetst ten opzichte van alle andere kolommen samen. Hierbij wordt rekening gehouden met de verschillende groottes van de groepen. Kleurmarkkeringen geven aan of er significante verschillen zijn tussen kolommen. Wanneer een groep significant hoger scoort op een vraag, wordt dit aangegeven met een GROENE markering. Wanneer een groep significant lager scoort op een vraag, wordt dit aangegeven met een ORANJE markering. Onderstaande tabel laat zien dat bij 11% van alle bedrijven een cyberincident heeft plaatsgevonden. Interessant is dat 6% aangeeft het niet te weten. Het werkelijke percentage zou dus hoger kunnen zijn. Interessant is verder dat het percentage lager is onder zzp'ers. Slechts 5% van de zzp'ers geeft aan een cyberincident te hebben meegemaakt in het afgelopen jaar. Het verschil met bedrijven met andere bedrijfsgroottes is significant.

**Tabel 3.4:** Percentage van bedrijven waarbij een cyberincident in het afgelopen jaar heeft plaatsgevonden afgezet tegen de bedrijfsgrootte.

| | Ik werk als zelfstandige zonder personeel (zzp'er) | 2-9 werknemers | 10-49 werknemers | 50-249 werknemers | 250-400 werknemers | Allen (n = 795) |
|---|---|---|---|---|---|---|
| Ja | 5% | 10% | 17% | 20% | 24% | 11% |
| Nee | 91% | 85% | 75% | 75% | 56% | 83% |
| Weet ik niet | 4% | 5% | 8% | 5% | 20% | 6% |

GROEN = Groep scoort significant hoger dan alle andere groepen samen (in de kolommen).
ORANJE = Groep scoort significant lager dan alle andere groepen samen (in de kolommen).

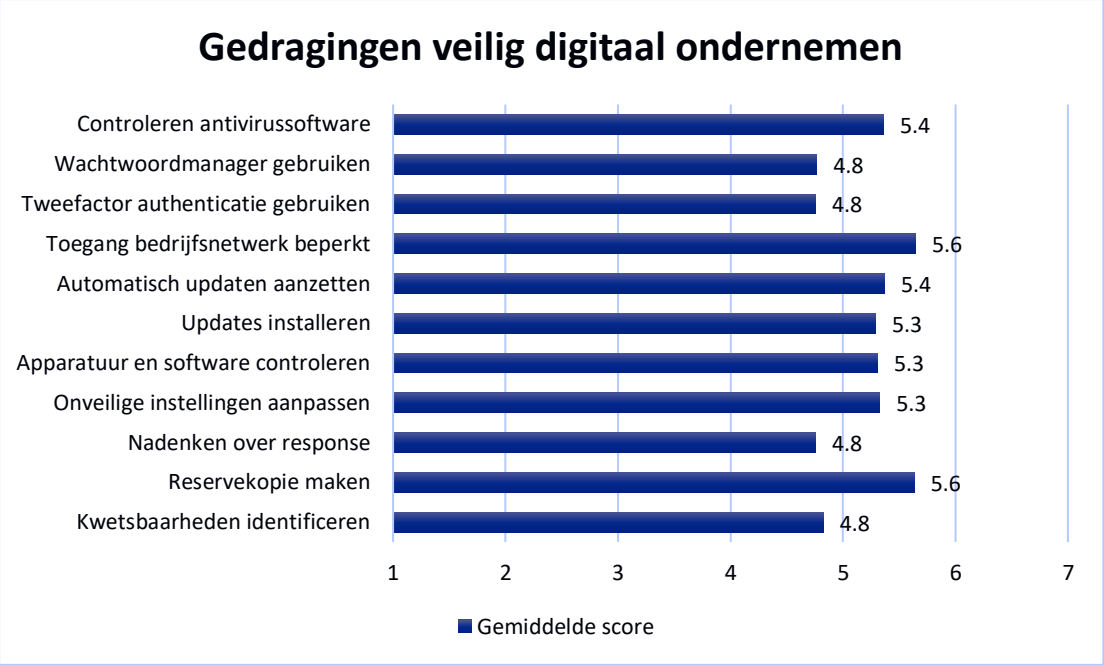
**Tabel 3.5:** Mate van digitalisering t.o.v. bedrijfsgrootte.

| | Zzp'er | 2-9 werknemers | 10-49 werknemers | 50-249 werknemers | 250-400 werknemers | Allen (n = 795) |
|---|---|---|---|---|---|---|
| Niet gedigitaliseerd | 24% | 11% | 10% | 3% | 8% | 14% |
| Gemiddeld gedigitaliseerd | 35% | 37% | 40% | 41% | 24% | 37% |
| Wel gedigitaliseerd | 37% | 51% | 48% | 55% | 68% | 46% |
| Weet niet/ geen mening | 4% | 1% | 1% | 0% | 0% | 2% |

GROEN = Groep scoort significant hoger dan alle andere groepen samen (in de kolommen).
ORANJE = Groep scoort significant lager dan alle andere groepen samen (in de kolommen).

## 3.2 Gedragingen van de bedrijven

Uit Figuur 3.1 blijkt dat bedrijven het hoogst scoren op het maken van reservekopieën en het beperken van de toegang tot hun bedrijfsnetwerk. Bedrijven scoren het laagst op het gebruiken van een wachtwoordmanager en tweefactorauthenticatie, identificeren van kwetsbaarheden en nadenken over hoe ze moeten reageren op een incident.




**Figuur 3.1:** Gemiddelde score per gedraging.

## 3.3 Factoren die van invloed zijn op veilig digitaal ondernemen

De resultaten van de multivariate regressieanalyse zijn weergegeven in Tabel 3.6.

**Tabel 3.6:** Resultaten van multivariate regressieanalyse voor veilig digitaal ondernemen. NB. De groen gedrukte coëfficiënten zijn statistisch significant (p < .05).

| | B | SE | t | Sig. |
|---|---|---|---|---|
| (Constant) | 0,934 | 0,263 | 3,549 | 0,000 |
| **Kennis** | 0,221 | 0,036 | 6,089 | 0,000 |
| **Vaardigheid** | 0,139 | 0,035 | 4,006 | 0,000 |
| Prioriteit | 0,044 | 0,031 | 1,394 | 0,164 |
| Waargenomen ernst | 0,036 | 0,022 | 1,644 | 0,101 |
| **Hulpbronnen** | 0,131 | 0,028 | 4,646 | 0,000 |
| **Protectie motivatie intentie** | 0,149 | 0,033 | 4,459 | 0,000 |
| Reputatie | 0,052 | 0,027 | 1,908 | 0,057 |
| Bereidwilligheid | 0,034 | 0,024 | 1,420 | 0,156 |
| **Response-effectiviteit** | 0,081 | 0,029 | 2,783 | 0,006 |
| Onder eigen controle | 0,003 | 0,020 | 0,132 | 0,895 |
| Eigen verantwoordelijkheid | 0,024 | 0,017 | 1,394 | 0,164 |
| Waargenomen kwetsbaarheid | -0,040 | 0,021 | -1,890 | 0,059 |
| Slachtofferschap (vs. Nee + Weet niet) | 0,071 | 0,083 | 0,853 | 0,394 |
| **Zzp (vs. Nee)** | -0,137 | 0,056 | 2,440 | 0,015 |
| Industrie en energie (vs. Landbouw) | -0,021 | 0,192 | -0,110 | 0,913 |
| Bouwnijverheid (vs. Landbouw) | -0,164 | 0,185 | -0,890 | 0,374 |
| Handel/ vervoer en horeca (vs. Landbouw) | -0,190 | 0,163 | -1,166 | 0,244 |
| Informatie en communicatie (vs. Landbouw) | -0,110 | 0,166 | -0,662 | 0,508 |
| Financiële dienstverlening (vs. Landbouw) | -0,032 | 0,169 | -0,189 | 0,851 |
| Verhuur en handel van onroerend goed (vs. Landbouw) | -0,131 | 0,197 | -0,664 | 0,507 |
| Zakelijke dienstverlening (vs. Landbouw) | -0,197 | 0,159 | -1,237 | 0,216 |
| Overheid (vs. Landbouw) | -0,076 | 0,215 | -0,353 | 0,724 |
| Onderwijs (vs. Landbouw) | 0,036 | 0,179 | 0,199 | 0,842 |
| Gezondheids-en welzijnszorg (vs. Landbouw) | -0,014 | 0,169 | -0,080 | 0,936 |
| Cultuur/ sport en recreatie (vs. Landbouw) | -0,097 | 0,184 | -0,524 | 0,600 |
| Overige branches/diensten (vs. Landbouw) | -0,130 | 0,169 | -0,768 | 0,443 |
| **Uitbesteden (vs. Ja)** | -0,121 | 0,052 | -2,325 | 0,020 |
| Digitalisering | 0,076 | 0,027 | 2,877 | 0,004 |

Noten:
$R^2$ (determinatiecoëfficiënt) = 64%, p < .001. N = 795. B = Ongestandaardiseerde regressiecoëfficiënt;
SE = standaard meetfout;
t = toetswaarde t-toets;
sig. = significantiewaarde.
NB. Om te kunnen bepalen of sector een relevante voorspeller is van veilig digitaal ondernemen is telkens als referentie de sector Landbouw/ bosbouw/ visserij en delfstoffenwinning genomen.

Uit de multivariate regressieanalyse blijkt dat alle variabelen tezamen 64% van de variantie in veilig digitaal ondernemen verklaren. Dit wil zeggen dat het model in 64% van de gevallen de mate van veilig digitaal ondernemen succesvol kan voorspellen. Dit suggereert dat de variabelen die zijn opgenomen in het model een relevante rol spelen bij het voorspellen van veilig digitaal ondernemen.

Uit het model blijkt dat het beschikken over kennis, vaardigheden en hulpbronnen een goede voorspeller is voor de mate van veilig digitaal ondernemen. Ook het hebben van de intentie om het bedrijf te beschermen tegen cyberincidenten en het kunnen inschatten van de gevolgen van (on)veilig digitaal ondernemen is van invloed op de mate van veilig digitaal ondernemen. Dit zijn vijf belangrijke gedragsbepalers die te beïnvloeden zijn met stimuleringsmaatregelen. Ook blijkt dat de bedrijfsgrootte, het uitbesteden van IT-diensten en mate van digitalisering van bedrijven van invloed zijn op veilig digitaal ondernemen. Zzp'ers nemen over het algemeen minder cyberveiligheidsmaatregelen dan niet-zzp'ers. Bedrijven die ondersteuning krijgen van een externe IT-dienstverlener zijn beter in staat om veilig digitaal te ondernemen. En bedrijven die aangeven een hoge mate van digitalisering te hebben, scoren hoger op het gebied van veilig digitaal ondernemen. De mate van digitalisering en het uitbesteden van IT-diensten kunnen worden beïnvloed door stimuleringsmaatregelen. Ondernemers kunnen bijvoorbeeld worden aangemoedigd om meer te investeren in digitalisering of ze kunnen hulp krijgen bij het uitbesteden van IT-diensten.

## 3.4 Groeperen van bedrijven op basis van kenmerken

Er is een latente klassenanalyse uitgevoerd om groepen bedrijven te kunnen vormen. Met deze methode zijn er groepen gemaakt waarbij bedrijven in een groep op elkaar lijken op basis van de gemeten kenmerken en waarbij de bedrijven in de verschillende groepen van elkaar verschillen. De uitkomsten van deze analyse helpen bij het ontwikkelen van gerichte interventies om groepen bedrijven te bereiken en tot actie te bewegen.

Er zijn vijf groepen te onderscheiden. Deze groepen verschillen van elkaar wat betreft de mate van veilig digitaal ondernemen en onderliggende gedragsbepalers, bijvoorbeeld kennis, waargenomen kwetsbaarheid en belang dat bedrijven hechten aan veilig digitaal ondernemen. Deze vijf groepen zijn binnen dit onderzoek voorzien van herkenbare en werkbare labels[13]:

- Voorlopers

Bedrijven binnen deze groep laten een patroon zien van het nemen van alle vereiste beschermende maatregelen. Ze zijn in staat om deze maatregelen te nemen, hebben de hulpbronnen om dat te doen en zijn zeer gemotiveerd.

- Uitbesteders

Ook bedrijven in deze groep scoren hoog op veilig digitaal ondernemen, maar niet zo hoog als Voorlopers. Ze zijn vergelijkbaar met Voorlopers, maar zijn van mening dat het nemen van beschermende maatregelen niet de verantwoordelijkheid is van hun eigen organisatie, en besteden hun cybersecurity in grote mate uit aan externe IT-serviceproviders (72%).

[13] Dit zijn voorlopige labels. Het is aan het DTC om definitieve labels te bepalen voor de groepen.

Overmoedigen

Overmoedigen vertonen een patroon van het nemen van beschermende maatregelen, maar in mindere mate dan Voorlopers en Uitbesteders. Ze onderschatten de gevolgen van een cyberbeveiligingsincident. Deze organisaties geven niet veel om hoe hun organisatie bekend staat bij hun klanten en relaties wat betreft de mate van cyberveiligheid in hun bedrijfsvoering en denken dat de kans om slachtoffer te worden klein is.

Machtelozen

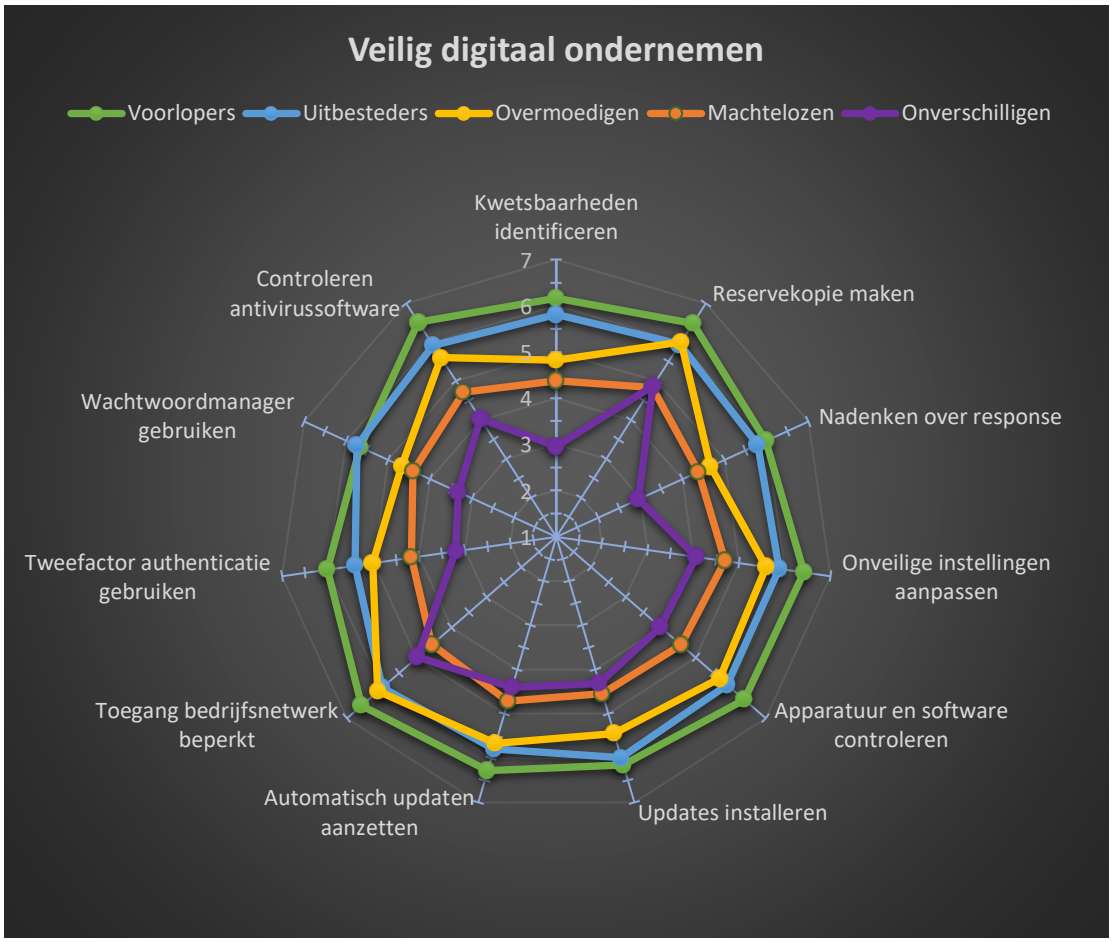
Machtelozen nemen onvoldoende beschermende maatregelen. Ze hebben weinig kennis, vaardigheden en hulpbronnen om zichzelf te beschermen. Ze onderschatten de gevolgen van een cyberbeveiligingsincident echter niet, en denken dat de kans om slachtoffer te worden aanwezig is.

Onverschilligen

Onverschilligen nemen onvoldoende beschermende maatregelen. Tegelijkertijd zijn ze niet overtuigd dat het nemen van aanbevolen maatregelen daadwerkelijk de dreiging zal verminderen, ze zijn niet gemotiveerd om hun organisatie te beschermen en denken dat de kans om slachtoffer te worden klein is.

De verdeling van de onderzochte bedrijven over de verschillende groepen laat zien dat de groep Overmoedigen het grootst is met 30%. Daarna volgen Voorlopers (22%), Machtelozen (18%), Onverschilligen (18%) en Uitbesteders (12%).

Figuur **3.2** laat zien in welke mate de verschillende groepen veilig digitaal ondernemen. Hoe hoger de score op een factor, hoe vaker of beter een bedrijf in die groep die gedraging uitvoert.




**Figuur 3.2:** Mate van veilig digitaal ondernemen per groep.

Tabel **3.7** laat zien hoe de verschillende groepen scoren op de verschillende gedragsbepalers.

**Tabel 3.7:** Score per groep op de factoren. Prioriteit is gemeten op een schaal van 1 t/m 5, de andere variabelen op een schaal van 1 t/m 7. De factor Slachtofferschap in de afgelopen 12 maanden is gemeten als ja/nee en ontbreekt daarom in deze figuur. GROEN = Groep scoort significant hoger dan alle andere groepen samen. ORANJE = Groep scoort significant lager dan alle andere groepen samen.

| | Voorlopers | Uitbesteders | Overmoedigen | Machtelozen | Onverschilligen |
|---|---|---|---|---|---|
| Kennis | 6,1 | 5,7 | 5,4 | 4,3 | 3,8 |
| Vaardigheden | 5,9 | 5,6 | 4,9 | 4,3 | 3,1 |
| Prioriteit | 3,4 | 2,4 | 2,8 | 2,9 | 2,3 |
| Waargenomen ernst | 3,7 | 5,5 | 3,1 | 4,2 | 2,5 |
| Hulpbronnen | 5,9 | 5,8 | 4,8 | 4,3 | 3,5 |
| Protectie Motivatie Intentie | 6,2 | 5,9 | 4,9 | 4,5 | 3,7 |
| Reputatie | 5,9 | 5,9 | 4,1 | 4,3 | 2,8 |
| Bereidwilligheid | 5,4 | 5,9 | 4,4 | 4,6 | 3,5 |
| Response effectiviteit | 6,3 | 5,7 | 5,5 | 4,4 | 4,8 |
| Verantwoordelijkheid | 6,3 | 4,0 | 5,7 | 4,2 | 4,5 |

| | Voorlopers | Uitbesteders | Overmoedigen | Machtelozen | Onverschilligen |
|---|---|---|---|---|---|
| Controle | 6,2 | 5,3 | 5,4 | 4,5 | 4,1 |
| Waargenomen kwetsbaarheid | 3,2 | 5,5 | 3,1 | 4,2 | 2,8 |

In de secties 3.4.1 t/m 3.4.5 wordt per groep bedrijven een beschrijving gegeven van de mate van veilig digitaal ondernemen en de onderliggende gedragsbepalers. Er wordt beschreven of een groep relatief gezien hoger of lager scoort op de onderliggende gedragsbepalers ten opzichte van de gemiddelde scores van alle andere groepen samen. In de tabellen onder de beschrijving staan de gemiddelde scores per gedragsbepaler vermeld. Na de beschrijvingen van de vijf verschillende groepen volgen tabellen en beschrijvingen die per achtergrondkenmerk/controlevariabele weergeven hoe de score hierop is verdeeld over elk van de vijf groepen.

## 3.4.1 Voorlopers

**Gedrag**

Deze bedrijven zijn voorlopers in veilig digitaal ondernemen. Ze hebben een gemiddelde score van 6,2 uit 7 op 11 gedragingen die belangrijk zijn voor digitale veiligheid. Dit is de hoogste score van alle groepen.

**Gedragsbepalers**

De bedrijven in de groep Voorlopers scoren ten opzichte van de gemiddelde scores van de bedrijven in alle andere groepen hoog op:

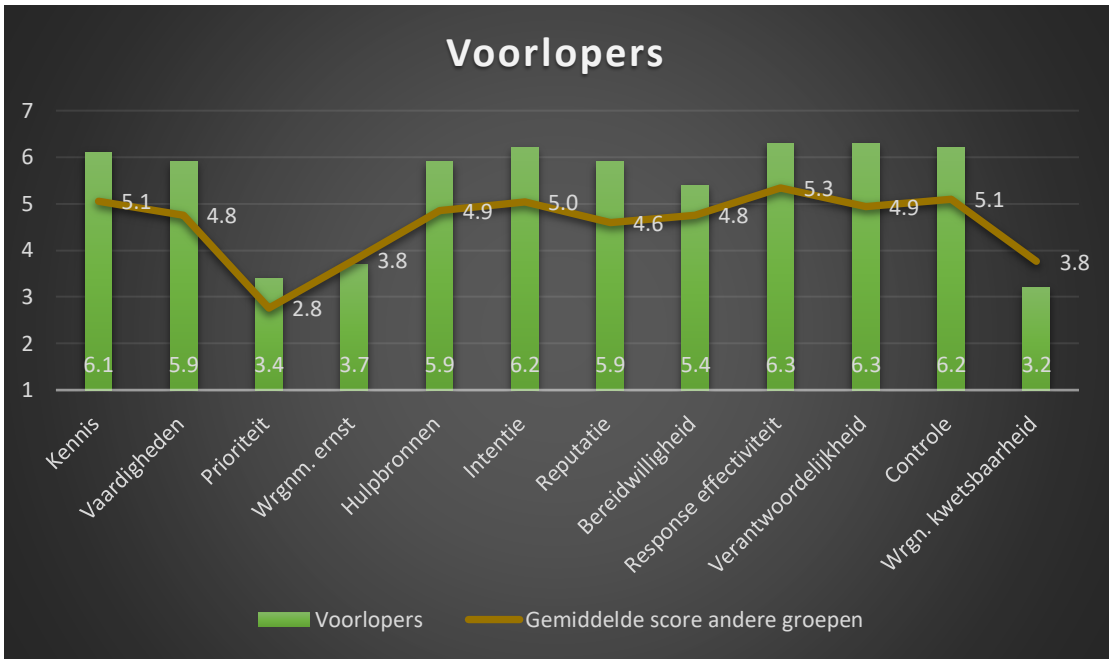
- Kennis;
- Vaardigheden;
- Prioriteit;
- Hulpbronnen;
- Intentie;
- Reputatie;
- Bereidwilligheid;
- Response-effectiviteit;
- Verantwoordelijkheid;

- Controle.

Ten opzichte van de gemiddelde scores van de bedrijven in alle andere groepen samen scoren zij relatief laag op:

- Waargenomen kwetsbaarheid.

De gemiddelde score op Waargenomen ernst is vergelijkbaar met de gemiddelde score van de bedrijven in alle andere groepen samen.




**Figuur 3.3:** Gemiddelde scores op gedragsbepalers voor bedrijven in de groep Voorlopers (balken) en gemiddelde scores van de andere groepen (lijn).

## 3.4.2 Uitbesteders

**Gedrag**

Deze bedrijven scoren, samen met de Voorlopers, hoog op veilig digitaal ondernemen. Ze hebben een gemiddelde score van 5,8 uit 7 op 11 gedragingen die van belang zijn voor digitale veiligheid.

**Gedragsbepalers**

De bedrijven in de groep Uitbesteders scoren ten opzichte van de gemiddelde scores van de bedrijven in alle andere groepen hoog op:

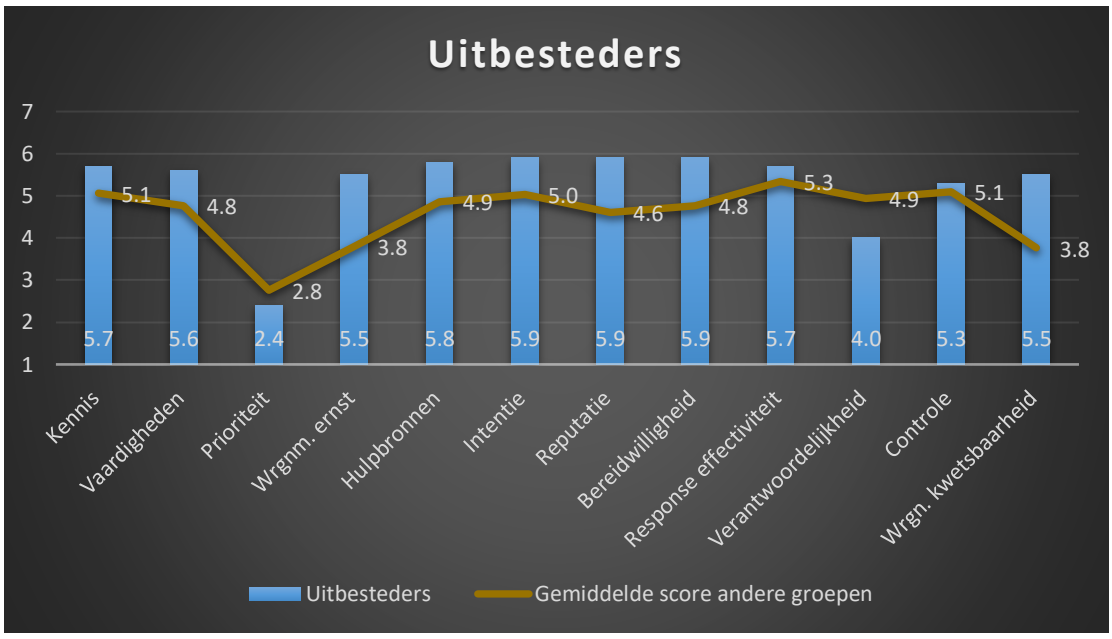
- Kennis;
- Vaardigheden;

- Waargenomen ernst;
- Hulpbronnen;
- Intentie;
- Reputatie;
- Bereidwilligheid;
- Response-effectiviteit;
- Waargenomen kwetsbaarheid.

Ten opzichte van de van de gemiddelde scores van de bedrijven in alle andere groepen samen scoren zij relatief laag op:

- Prioriteit;
- Verantwoordelijkheid.

De gemiddelde score op Controle is vergelijkbaar met de gemiddelde score van de bedrijven in alle andere groepen samen.



**Figuur 3.4:** Gemiddelde scores op factoren voor bedrijven in de groep Uitbesteders (balken) en gemiddelde scores van de andere groepen (lijn).

### 3.4.3 Overmoedigen

**Gedrag**

Deze bedrijven scoren redelijk hoog op veilig digitaal ondernemen. Ze hebben een gemiddelde score van 5,4 uit 7 op 11 gedragingen die belangrijk zijn voor digitale veiligheid.

**Gedragsbepalers**

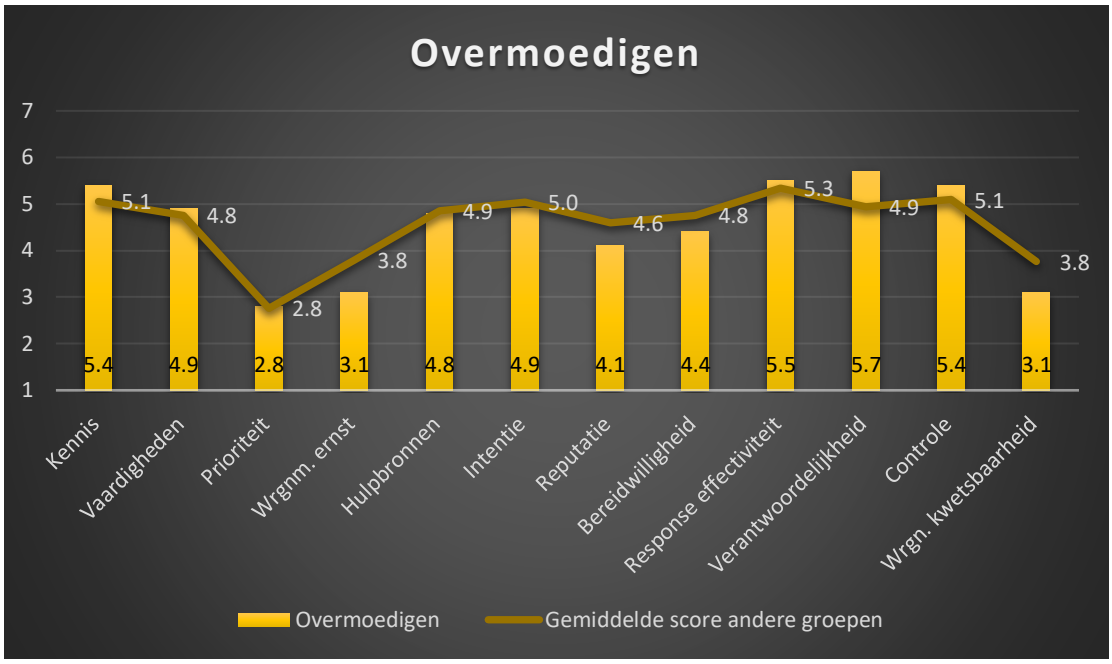
De bedrijven in de groep Overmoedigen scoren ten opzichte van de gemiddelde scores van de bedrijven in alle andere groepen samen relatief hoog op:

- Kennis;
- Vaardigheden;
- Response-effectiviteit;
- Verantwoordelijkheid;
- Controle.

Ten opzichte van de van de gemiddelde scores van de bedrijven in alle andere groepen samen scoren zij relatief laag op:

- Waargenomen ernst;
- Reputatie;
- Bereidwilligheid;
- Waargenomen kwetsbaarheid.

De gemiddelde scores op Prioriteit, Hulpbronnen en Intentie zijn vergelijkbaar met de gemiddelde scores van de bedrijven in alle andere groepen samen.




**Figuur 3.5:** Gemiddelde scores op factoren voor bedrijven in de groep Overmoedigen (balken) en gemiddelde scores van de andere groepen (lijn).

### 3.4.4 Machtelozen

**Gedrag**

Deze bedrijven scoren redelijk op veilig digitaal ondernemen. Ze hebben een gemiddelde score van 4,6 uit 7 op 11 gedragingen die belangrijk zijn voor digitale veiligheid.

**Factoren**

De bedrijven in de groep Machtelozen scoren ten opzichte van de gemiddelde scores van de bedrijven in alle andere groepen samen relatief hoog op:

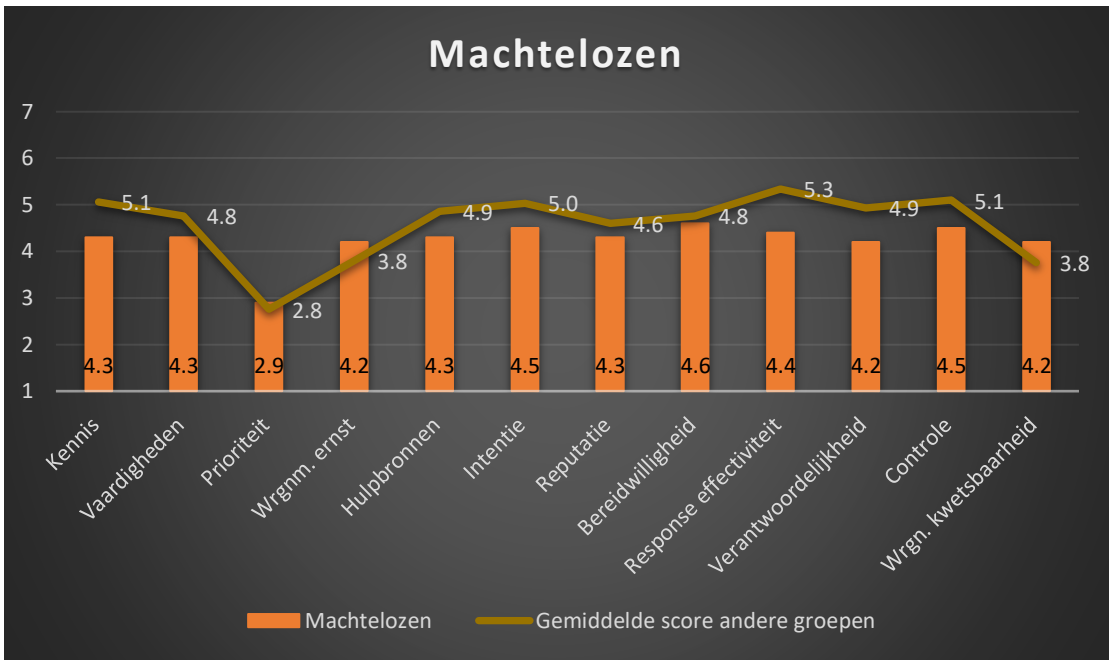
- Waargenomen ernst;
- Waargenomen kwetsbaarheid.

Ten opzichte van de van de gemiddelde scores van de bedrijven in alle andere groepen samen scoren zij relatief laag op:

- Kennis;
- Vaardigheden;
- Hulpbronnen;
- Intentie;

- Reputatie;
- Bereidwilligheid;
- Response-effectiviteit;
- Verantwoordelijkheid;
- Controle.

De gemiddelde score op Prioriteit is vergelijkbaar met de gemiddelde scores van de bedrijven in alle andere groepen samen.




**Figuur 3.6:** Gemiddelde scores op factoren voor bedrijven in de groep Machtelozen (balken) en gemiddelde scores van de andere groepen (lijn).

## 3.4.5 Onverschilligen

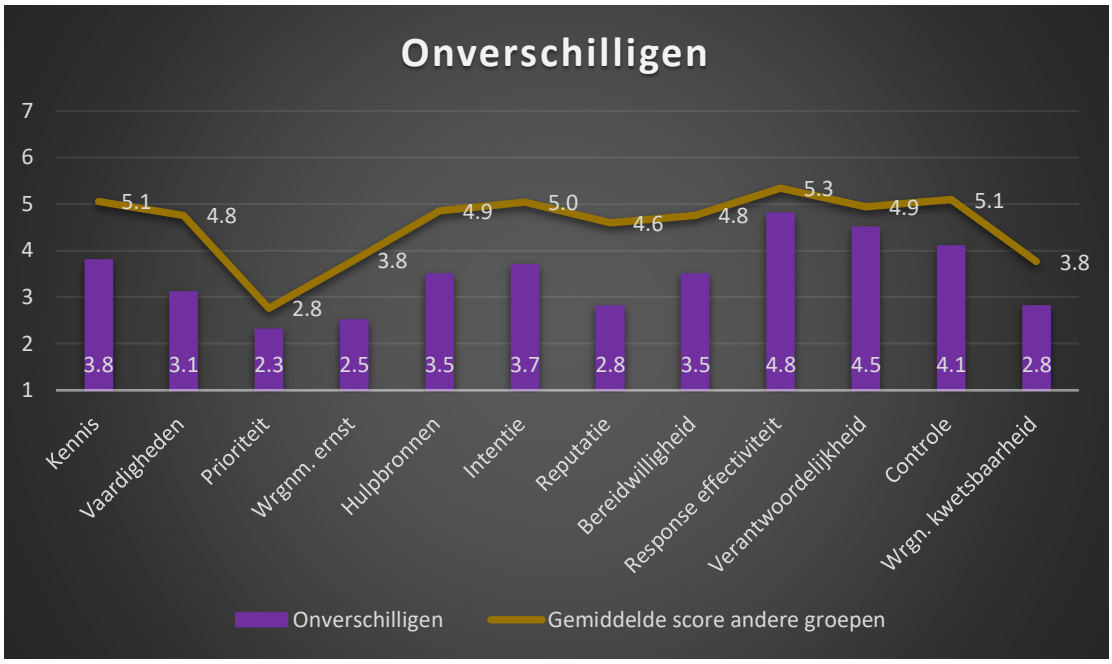
**Gedrag**

Deze bedrijven scoren matig op veilig digitaal ondernemen. Ze hebben een gemiddelde score van 3,9 uit 7 op 11 gedragingen die belangrijk zijn voor digitale veiligheid.

**Factoren**

Ten opzichte van de van de gemiddelde scores van de bedrijven in alle andere groepen samen scoren zij relatief laag op alle factoren:

- Kennis;
- Vaardigheden;
- Prioriteit;
- Waargenomen ernst;
- Hulpbronnen;
- Intentie;
- Reputatie;
- Bereidwilligheid;
- Response-effectiviteit;
- Verantwoordelijkheid;
- Controle;
- Waargenomen kwetsbaarheid.




**Figuur 3.7:** Gemiddelde scores op factoren voor bedrijven in de groep Onverschilligen (balken) en gemiddelde scores van de andere groepen (lijn).

## 3.5 Achtergrondvariabelen per groep

Onderstaande tabellen geven per groep de percentages weer voor de mate van digitalisering, sectoren, mate van ondersteuning door externe IT-dienstverlener, bedrijfsgrootte en slachtofferschap in de afgelopen 12 maanden. Deze variabelen zijn concreet en meetbaar en kunnen behulpzaam zijn bij het bereiken van groepen die het DTC kan ondersteunen met op de groep afgestemde producten en diensten.

### 3.5.1 Mate van digitalisering

Bij de variabele over de mate van digitalisering komt naar voren dat bedrijven die hoog scoren op mate van digitalisering vaker behoren tot de groepen Voorlopers en Uitbesteders. Bedrijven die laag scoren op mate van digitalisering behoren vaker tot de groep Onverschilligen.

**Tabel 3.8:** Mate van digitalisering per groep.

| | Voorlopers | Uitbesteders | Overmoedigen | Machtelozen | Onverschilligen | Allen (n=795) |
|---|---|---|---|---|---|---|
| Niet gedigitaliseerd | 3% | 8% | 14% | 12% | 37% | 14% |
| Gemiddeld gedigitaliseerd | 31% | 24% | 39% | 54% | 35% | 37% |
| Wel gedigitaliseerd | 65% | 67% | 47% | 30% | 24% | 46% |
| Weet niet/ geen mening | 1% | 1% | 1% | 4% | 4% | 2% |
| Gemiddeldetoets | 2,6 | 2,6 | 2,3 | 2,2 | 1,9 | 2,3 |
| Standaarddeviatie | 0,55 | 0,63 | 0,71 | 0,64 | 0,79 | 0,72 |

GROEN = Groep scoort significant hoger dan alle andere groepen samen (in de kolommen).
ORANJE = Groep scoort significant lager dan alle andere groepen samen (in de kolommen).

### 3.5.2 Sectoren

Als wordt gekeken naar de sectoren waaruit ten minste 10% van de bedrijven afkomstig is, blijkt dat bedrijven uit de sectoren Handel/Vervoer en horeca en Zakelijke dienstverlening gelijkmatig verdeeld zijn over de groepen. Bedrijven uit de sector Informatie en communicatie behoren vaker tot de groep Voorlopers en minder vaak tot de groep Machtelozen. Bedrijven uit de sector Financiële dienstverlening behoren vaker tot de groepen Machtelozen en Uitbesteders, en minder vaak tot de groep Onverschilligen.

**Tabel 3.9:** Sectoren per groep.

| | Voorlopers | Uitbesteders | Overmoedigen | Machtelozen | Onverschilligen | Allen (n=795) |
|---|---|---|---|---|---|---|
| Landbouw/ bosbouw/ visserij en delfstoffenwinning | 3% | 2% | 2% | 6% | 1% | 3% |
| Industrie en energie | 4% | 7% | 3% | 4% | 2% | 4% |
| Bouwnijverheid | 2% | 7% | 5% | 6% | 6% | 5% |
| Handel/ vervoer en horeca | 11% | 10% | 16% | 16% | 11% | 14% |
| Informatie en communicatie | 20% | 10% | 12% | 7% | 9% | 12% |
| Financiële dienstverlening | 10% | 15% | 7% | 16% | 4% | 10% |
| Verhuur en handel van onroerend goed | 2% | 9% | 2% | 4% | 4% | 4% |
| Zakelijke dienstverlening | 22% | 21% | 17% | 15% | 18% | 18% |
| Overheid | 5% | 7% | 1% | 2% | 0% | 3% |
| Onderwijs | 2% | 3% | 8% | 6% | 8% | 6% |
| Gezondheids- en welzijnszorg | 7% | 8% | 10% | 9% | 9% | 9% |
| Cultuur/ sport en recreatie | 2% | 1% | 7% | 1% | 13% | 5% |
| Overige branches/diensten | 9% | 2% | 10% | 8% | 14% | 9% |

GROEN = Groep scoort significant hoger dan alle andere groepen samen (in de kolommen).
ORANJE = Groep scoort significant lager dan alle andere groepen samen (in de kolommen).

### 3.5.3 Ondersteuning door externe IT-dienstverlener

Als wordt gefocust op de mate waarin bedrijven zich laten ondersteunen door een externe IT-dienstverlener dan blijkt dat de bedrijven die ondersteuning van een IT-dienstverlener krijgen vaker voorkomen in de groep Uitbesteders. Bedrijven die zich niet laten ondersteunen door een externe IT-dienstverlener komen vaker voor in de groep Onverschilligen.

**Tabel 3.10:** Wel of geen ondersteuning van een externe IT-dienstverlener per groep.

| Item | Voorlopers | Uitbesteders | Overmoedigen | Machtelozen | Onverschilligen | Allen (n=795) |
|---|---|---|---|---|---|---|
| Ja, ik krijg wel ondersteuning van een externe IT-leverancier of dienstverlener | 60% | 72% | 53% | 57% | 32% | 54% |
| Nee, ik krijg geen ondersteuning van een externe IT-leverancier of dienstverlener | 40% | 28% | 47% | 43% | 68% | 46% |

GROEN = Groep scoort significant hoger dan alle andere groepen samen (in de kolommen).
ORANJE = Groep scoort significant lager dan alle andere groepen samen (in de kolommen).

### 3.5.4 Bedrijfsgrootte

Zzp'ers komen vaker voor in de groepen Overmoedigen en Onverschilligen. Voor de andere bedrijven is het beeld minder duidelijk. Bedrijven met 2-9 werknemers behoren minder vaak tot de groep Uitbesteders. Bedrijven met 10-49 werknemers komen vaker voor in de groepen Voorlopers, Uitbesteders, maar ook in de groep Machtelozen. Bedrijven met 50-249 werknemers komen vaker voor in de groepen Voorlopers en Uitbesteders. Bedrijven met 250-400 werknemers daarentegen komen vaker voor in zowel Uitbesteders als Machtelozen.

**Tabel 3.11:** Aantal personen in dienst per groep.

| | Voorlopers | Uitbesteders | Overmoedigen | Machtelozen | Onverschilligen | Allen (n=795) |
|---|---|---|---|---|---|---|
| Geen personeel (zzp'er) | 30% | 8% | 53% | 26% | 71% | 41% |
| 2-9 werknemers | 18% | 8% | 21% | 18% | 19% | 18% |
| 10-49 werknemers | 24% | 27% | 12% | 26% | 8% | 18% |
| 50-249 werknemers | 27% | 48% | 12% | 23% | 2% | 20% |
| 250-400 werknemers | 2% | 10% | 1% | 7% | 0% | 3% |

GROEN = Groep scoort significant hoger dan alle andere groepen samen (in de kolommen).
ORANJE = Groep scoort significant lager dan alle andere groepen samen (in de kolommen).

### 3.5.5 Slachtofferschap in de afgelopen 12 maanden

Uit de verdeling van incidenten blijken verschillende beelden. In totaal geeft 11% van alle bedrijven aan een slachtoffer te zijn geweest van een cyberincident in de afgelopen 12 maanden. Daarbij kan worden opgemerkt dat verder niet is doorgevraagd naar de aard van het incident. Het is dus onduidelijk of dit een ernstig incident betrof of dat dit relatief licht was. Wat verder opvalt is dat 6% niet weet of zij een cyberincident hebben meegemaakt. Een voorwaarde voor cyberweerbaarheid is dat je in staat bent om incidenten te detecteren. Als dit vermogen ontbreekt is adequate reactie niet mogelijk. Verder valt op dat van alle bedrijven die een incident hebben doorgemaakt 49% in de groep

Uitbesteders zit. Bedrijven die geen slachtoffer zijn geweest van een cyberincident behoren vooral tot de groep Voorlopers, maar ook tot de Overmoedigen.

**Tabel 3.12:** Slachtofferschap in de afgelopen 12 maanden per cluster.

| | Voorlopers | Uitbesteders | Overmoedigen | Machtelozen | Onverschilligen | Allen (n=795) |
|---|---|---|---|---|---|---|
| Ja | 5% | 49% | 3% | 16% | 6% | 11% |
| Nee | 94% | 40% | 96% | 68% | 88% | 83% |
| Weet ik niet | 1% | 11% | 1% | 16% | 6% | 6% |

GROEN = Groep scoort significant hoger dan alle andere groepen samen (in de kolommen).
ORANJE = Groep scoort significant lager dan alle andere groepen samen (in de kolommen).

## 3.6 Voorspellen in welke groep een bedrijf valt

Bedrijven in een groep lijken op elkaar wat betreft mate van veilig digitaal ondernemen en de onderliggende gedragsbepalers. De groepen verschillen onderling van elkaar. Hoe kan snel worden bepaald tot welke groep een bedrijf hoort, zonder dat het bedrijf de volledige vragenlijst invult? Hiervoor is een voorspellingsmodel gemaakt. Het DTC kan de verkorte vragenlijst en syntax (zie Bijlage E) gebruiken om een applicatie te bouwen waarmee bedrijven die de DTC-website bezoeken (achter de schermen) tot een groep kunnen worden toebedeeld. Vervolgens kunnen zij gericht naar passende interventies worden doorverwezen.

Het resultaat is een vragenlijst van 10 items en een algoritme waarmee een bedrijf met een nauwkeurigheid van meer dan 83% kan worden gecategoriseerd in een van de vijf groepen. De 10 items zijn beschreven in Tabel **3.13**.

**Tabel 3.13:** Voorspellingsmodel op basis van 10 items (83%).

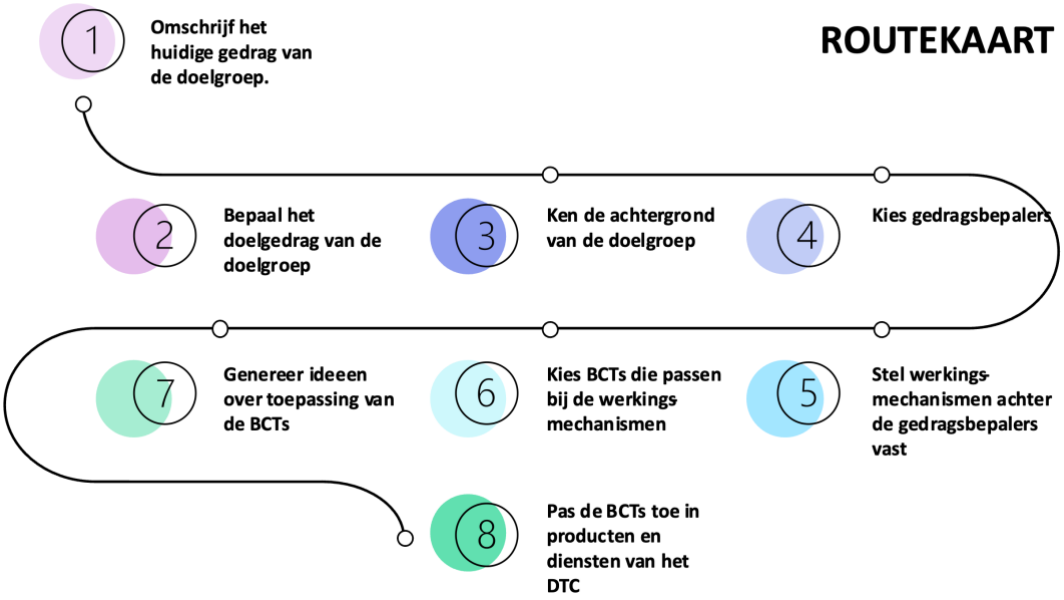
| Variabele | Item |
|---|---|
| Gedrag | Mijn bedrijf/organisatie controleert periodiek of de apparatuur en software binnen de organisatie up-to-date is. |
| Kennis | Ik weet hoe ik veilig digitaal kan ondernemen. |
| Vaardigheid | Ik ben getraind om veilig digitaal te kunnen ondernemen. |
| Waargenomen ernst | Ik vind dat het voortbestaan van mijn organisatie wordt bedreigd door cyberincidenten. |
| Intentie | Wij zijn bereid er alles aan te doen om de organisatie te beschermen tegen cyberincidenten. |
| Reputatie | Wij willen een voorbeeld zijn voor andere organisaties op het gebied van veilig digitaal ondernemen. |
| Verantwoordelijkheid | In hoeverre ben je het eens dat veilig digitaal ondernemen (...) 1= is de verantwoordelijkheid van anderen? 7= is de verantwoordelijkheid van mijn organisatie. |
| Response-effectiviteit 1 | Veilig digitaal ondernemen helpt onze organisatie om meer weerbaar te zijn tegen cyberrisico's die de bedrijfsvoering kunnen verstoren. |
| Response-effectiviteit 2 | Veilig digitaal ondernemen is een effectieve manier om cyberincidenten te voorkomen. |
| Waargenomen kwetsbaarheid | Hoe waarschijnlijk is het volgens jou dat jouw organisatie in de komende 12 maanden slachtoffer wordt van een cyberincident? |

## 3.7 Identificeren van interventies: wat past bij welke groep?

De segmentering biedt het DTC inzicht in de behoeften en uitdagingen van de verschillende groepen op het gebied van veilig digitaal ondernemen. Met deze kennis kan het DTC de groepen gerichter ondersteunen bij het nemen van beschermingsmaatregelen.

Op het gebied van het treffen van maatregelen voor veilig digitaal ondernemen zijn er drie doelgroepen die achterblijven. Deze groepen worden aangeduid als de Overmoedigen, Machtelozen en Onverschilligen. Samen vormen zij 66% van de bedrijven. Het is van belang dat het DTC hen gericht aanmoedigt om specifieke cyberbeschermingsmaatregelen te treffen. Bedrijven in deze groepen hebben te maken met verschillende factoren die hen belemmeren om daadwerkelijk maatregelen te nemen. Het DTC kan via een reeks stappen tot interventies komen die aansluiten bij de behoeften van elke specifieke doelgroep. Voor de doelgroepen Overmoedigen, Machtelozen en Onverschilligen zijn specifieke routekaarten ontwikkeld. De algemene stappen zijn weergegeven in de onderstaande routekaart[14] in Figuur **3.8**.

[14] In de routekaart wordt de afkorting BCTs gebruikt. Dit staat voor 'Behavior Change Techniques', ofwel gedragsveranderingstechnieken. BCTs zijn systematische procedures die zijn opgenomen als een actief onderdeel van een interventie om gedrag te veranderen.




**Figuur 3.8:** Routekaart om te komen tot interventies.

Van elke groep wordt eerst een korte omschrijving gegeven en vervolgens worden er ideeën voor interventies geschetst. De gevolgde stappen staan beschreven in hoofdstuk 2 Aanpak van het onderzoek.

### 3.7.1 Interventies voor Voorlopers

De bedrijven in deze groep zijn voorlopers op het gebied van veilig digitaal ondernemen. Ze hebben al belangrijke maatregelen genomen om hun digitale weerbaarheid te verbeteren. Het doel voor deze bedrijven is om hun huidige aanpak voort te zetten. Deze bedrijven kunnen daarnaast een waardevolle rol spelen bij het bereiken en motiveren van andere bedrijven. Dit kan op de volgende manieren:

**Kennisuitwisseling stimuleren:** We raden aan dat de groep van voorlopers wordt aangemoedigd om hun kennis door te delen binnen hun eigen keten en netwerk. Het principe van 'voorloper helpt volger' is hier toepasselijk. DTC zou inspirerende voorbeelden kunnen presenteren aan de voorlopers over diverse manieren waarop ze hun kennis kunnen verspreiden. Dit zou een effectieve strategie kunnen zijn om kennisuitwisseling te bevorderen.

**DTC-website promoten:** We adviseren dat voorlopers een actieve rol spelen in het verspreiden en promoten van de DTC-website onder hun kleinere leveranciers of klanten. Dit is in hun belang, omdat het hun keten veiliger maakt. Daarom zouden voorlopers promotiemateriaal en informatiepakketten van het DTC kunnen ontvangen om te delen met hun netwerk en keten. Het DTC zou strategieën kunnen overwegen om deze informatiepakketten bij de voorlopers te krijgen en om de achterblijvers in contact te brengen met de voorlopers. Dit contact kan plaatsvinden op natuurlijke momenten, bijvoorbeeld via IT-dienstverleners die DTC-pakketten delen met hun klanten. Het behouden en versterken van een positieve reputatie is essentieel voor IT-dienstverleners; een veilige sector in het algemeen is gunstig. Dit zou ook in de communicatie moeten worden opgenomen.

**Communicatiestrategieën herijken:** We adviseren het DTC om de communicatiestrategieën met de voorlopers te heroverwegen. Het DTC zou kunnen nagaan hoe effectief de gangbare informatiebronnen en -kanalen zijn (bijv. nieuwsbrieven, webinars). Het is ook belangrijk om te

onderzoeken hoe deze kanalen kunnen worden verbeterd of aangevuld om een effectievere communicatie met de voorlopers te waarborgen, bijvoorbeeld via de DTC Community. Het doel is om ervoor te zorgen dat de voorlopers volledig geïnformeerd en betrokken zijn bij het proces. Dit zal bijdragen aan het succes van hun initiatieven op het gebied van digitale veiligheid.

### 3.7.2 Interventies voor Uitbesteders

Deze groep bestaat voornamelijk uit grotere bedrijven (10-49 werknemers en groter) die veelal ondersteund worden door een externe IT-dienstverlener. De bedrijven in de groep Uitbesteders scoren hoog op veilig digitaal ondernemen. Van de 11 gedragingen uit de Basisscan Cyberweerbaarheid scoren zij het laagst op Gebruiken van tweefactor-authenticatie.

Uit Figuur **3.4** blijkt dat bedrijven in de groep Uitbesteders relatief laag scoren op de gedragsbepalers Eigen verantwoordelijkheid en Prioriteit. Vanwege de grote afhankelijkheid van externe IT-dienstverleners is het cruciaal dat deze bedrijven een gelijkwaardige gesprekspartner zijn of worden voor externe partijen. Dit kan op de volgende manieren:

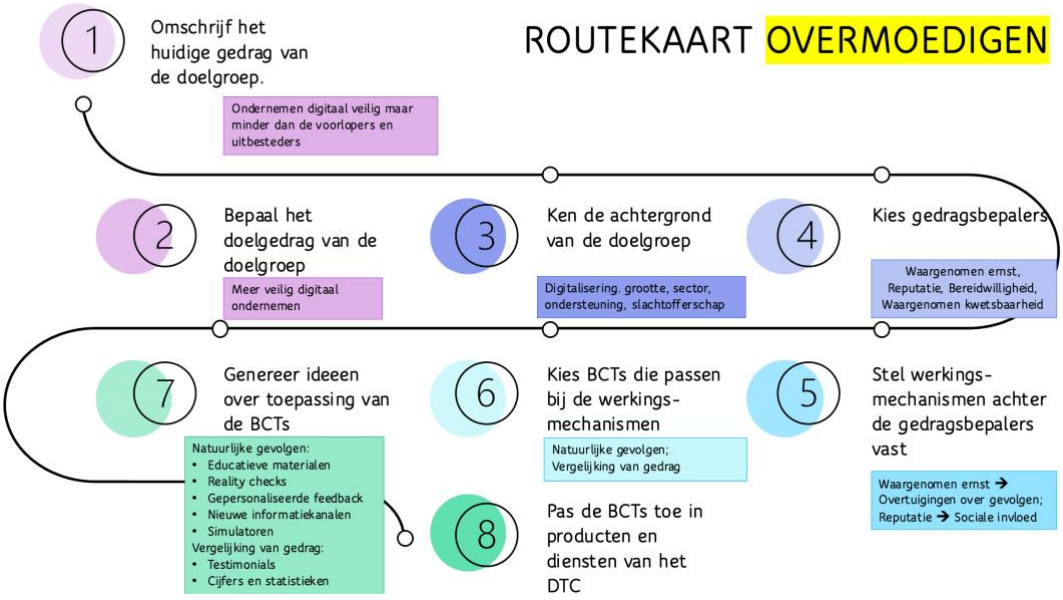
**Zelfredzaamheid vergroten**: Bedrijven kunnen worden gestimuleerd om op cursus te gaan, zodat zij de juiste vragen kunnen stellen en minder afhankelijk worden. Ook kunnen deze bedrijven worden aangemoedigd om mensen (parttime) in dienst nemen die zelf de check kunnen doen op de kwaliteit en betrouwbaarheid van de dienstverlening.

***Conversational agent* ontwikkelen**: Een ander idee is om een *conversational agent* (een AI-powered chatbot) te ontwikkelen die de bedrijven kan helpen bij het voeren van gesprekken met de externe IT-dienstverleners. Deze *chatbot* zou bijvoorbeeld tips kunnen geven, vragen kunnen suggereren of waarschuwen voor valkuilen. Dit kan de ondernemers meer vertrouwen en inzicht geven in het uitbestedingsproces.

***Second opinion* aanbieden**: Uitbesteders hebben wel behoefte aan een soort second opinion of risicoanalyse, maar dat is een dienst die niet iedereen kan betalen. Het DTC kan hierbij helpen door goede voorbeelden van uitbesteders als rolmodellen zichtbaar en benaderbaar te maken voor andere uitbesteders die behoefte hebben aan een second opinion.

**Netwerk vergroten**: Uitbesteders zouden ook de informatie van het DTC (bijv. stappenplan) kunnen doordelen met hun kleinere toeleveranciers of klanten, om zo hun keten veiliger te maken. Hiervoor zou ook de DTC-community gebruikt kunnen worden, waar ondernemers elkaar om advies kunnen vragen over het inschakelen van bepaalde partijen of aanschaffen van bepaalde software.

### 3.7.3 Interventies voor Overmoedigen




**Figuur 3.9:** Uitkomsten van de stappen om te komen tot interventies voor de doelgroep Overmoedigen.

*Huidig gedrag, doelgedrag en achtergrond van Overmoedigen*
De groep Overmoedigen bestaat veelal uit zzp'ers die positief scoren op veilig digitaal ondernemen. Op de 11 gedragingen uit de Basisscan Cyberweerbaarheid scoren zij echter lager dan de Voorlopers en Uitbesteders en het laagst op Nadenken over de response bij een cyberincident en Gebruiken van een wachtwoordmanager.

Figuur **3.5** laat zien dat bedrijven in de groep Overmoedigen relatief laag scoren op de gedragsbepalers Waargenomen ernst, Reputatie, Bereidwilligheid en Waargenomen kwetsbaarheid.

*Gedragsbepalers, werkingsmechanismen, BCT's, interventie-ideeën voor Overmoedigen*
Hier geven we een aantal interventie-ideeën die passen bij de gedragsbepalers Waargenomen ernst en Reputatie.

De gedragsbepaler **Waargenomen ernst** is gerelateerd aan het werkingsmechanisme Overtuigingen over gevolgen. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorie Natuurlijke gevolgen:

- Geef informatie over (emotionele-, sociale- en omgevings) gevolgen van het gedrag;
- Vestig de aandacht op de gevolgen van het wel of niet uitvoeren van gedrag;
- Geanticipeerde spijt.

Deze BCTs kan het DTC gebruiken bij:

- **Educatieve materialen verstrekken:** Verstrek informatie via afbeeldingen, grafieken en tekst over (emotionele-, sociale- en omgevings) gevolgen van onveilig digitaal ondernemen. Bijvoorbeeld via Informatie & Advies, Toolkits en Campagnes.
- **Persoonlijke verhalen laten delen:** Laat vergelijkbare ondernemers vertellen over de ernstige gevolgen van onveilig digitaal ondernemen voor hunzelf, hun onderneming en hun naaste omgeving. Bijvoorbeeld via Ondernemersverhalen en Netwerkbijeenkomsten.
- **Gepersonaliseerde feedback geven**: Simuleer een schijnaanval en laat de ondernemer ervaren in hoeverre de ondernemer veilig digitaal onderneemt. Leg hierbij de nadruk op Nadenken over de response bij een cyberincident en Gebruiken van een wachtwoordmanager. Bijvoorbeeld via de Basisscan, de Cyberveilig Check en de Security Check Procesautomatisering.
- **Reality checks aanbieden**: Bied een *reality check* aan waarmee ondernemers te zien krijgen hoe ze er echt voorstaan. Dit kan bijvoorbeeld door ongevraagd kleine, eenvoudige checks te doen, zoals de internet.nl-check. Deze check geeft een score en advies over de digitale veiligheid van de ondernemer. De Cyberveilig Check voor zzp en mkb is een nieuwe interventie die hierbij aansluit, want hierna kunnen ze gelijk door met het aanvragen van subsidie voor het verbeteren van de digitale veiligheid.
- **Nieuwe informatiekanalen aanboren:** Een mogelijkheid is om via andere partijen informatie over gevolgen te verstrekken, zoals accountants, de KvK, IT-dienstverleners en leveranciers van producten (bv. Google).
- **Simulator ontwikkelen:** Een ander idee is om een simulator te ontwikkelen die bedrijven laat zien en ervaren wat er kan gebeuren als ze hun digitale veiligheid niet op orde hebben. Dit kan bijvoorbeeld door een scenario te schetsen waarin ze gehackt worden of een boete krijgen. Dit zou de ondernemers meer bewust kunnen maken van de risico's en de gevolgen. Dit kan ook worden ontwikkeld om risico's voor slachtoffers in kaart te brengen: bijv. hoe de gegevens van een gesimuleerd familielid zijn gelekt en worden gebruikt voor bankhelpdeskfraude.

De gedragsbepaler **Reputatie** is gerelateerd aan het werkingsmechanisme Sociale invloed. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorie Vergelijking van gedrag:

- Sociale vergelijking;
- Informatie over de goedkeuring van anderen.

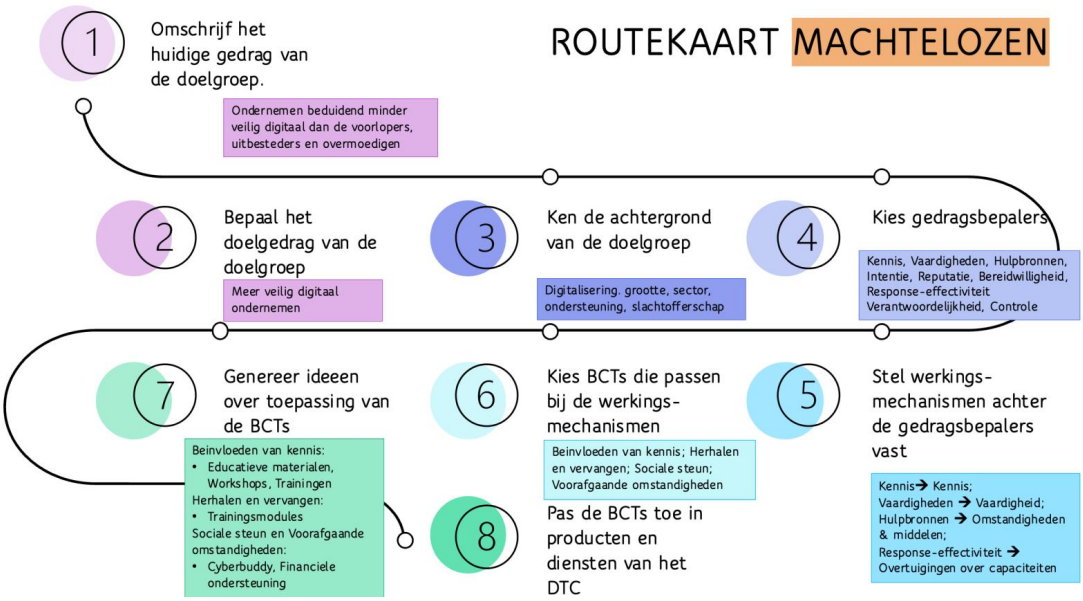
Deze BCTs kan het DTC gebruiken bij:

- **Testimonials laten delen**: Informeer deze groep over hoe andere bedrijven in hun netwerk en keten denken over (on)veilig digitaal ondernemen. Laat andere bedrijven uitspreken dat zij het

belangrijk vinden dat het bedrijf waar zij zaken mee doen veilig digitaal onderneemt. Bijvoorbeeld via Ondernemersverhalen, de DTC-community en Campagnes.

**Cijfers en statistieken verstrekken:** Laat zien wat de norm is; hoe 'scoren' vergelijkbare bedrijven op veilig digitaal ondernemen? Bijvoorbeeld via Weekupdates, Onderzoeken en Data en Netwerkbijeenkomsten.

### 3.7.4 Interventies voor Machtelozen




**Figuur 3.10:** Uitkomsten van de stappen om te komen tot interventies voor de doelgroep Machtelozen.

*Huidig gedrag, doelgedrag en achtergrond van Machtelozen*
Deze groep bestaat veelal uit bedrijven die redelijk scoren op veilig digitaal ondernemen. Op de 11 gedragingen uit de Basisscan Cyberweerbaarheid scoren zij echter aanmerkelijk lager dan de Voorlopers, Uitbesteders en Overmoedigen en het laagst op Tweefactorauthenticatie en Updates installeren.

Figuur **3.6** laat zien dat bedrijven in de groep Machtelozen relatief laag scoren op de gedragsbepalers Kennis, Vaardigheden, Hulpbronnen, Intentie, Reputatie, Bereidwilligheid, Response-effectiviteit, Verantwoordelijkheid en Controle.

*Gedragsbepalers, werkingsmechanismen, BCT's, interventie-ideeën voor Machtelozen*
Hier geven we een aantal interventie-ideeën die passen bij de gedragsbepalers Kennis, Vaardigheden, Hulpbronnen en Response-effectiviteit.

De gedragsbepaler **Kennis** is gerelateerd aan het werkingsmechanisme Kennis. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorie Beïnvloeden van kennis:

Geef instructies over hoe het gedrag uit te voeren is.

Deze BCT kan het DTC gebruiken bij:

- **Educatieve materialen verstrekken:** Verstrek informatie via afbeeldingen, video's, infographics en tekst, bijvoorbeeld over het aanvragen van subsidie. Leg ook uit welk gedrag hoort bij veilig digitaal ondernemen en laat zien welke kleine stappen zij kunnen zetten om een start te maken.
- **Workshops aanbieden**: Bied workshops aan waarin ondernemers in kleine groepen van elkaar kunnen leren, vragen stellen, best practices uitwisselen, ervaringen bespreken en elkaar ondersteunen bij veilig digitaal ondernemen.

De gedragsbepaler **Vaardigheden** is gerelateerd aan het werkingsmechanisme Vaardigheid. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorieën Beïnvloeden van kennis en Herhalen en vervangen:

- Geef instructies over hoe het gedrag uit te voeren is;
- Graduele taken;
- Oefenen/ herhalen/ inslijpen van gedrag.

Deze BCT kan het DTC gebruiken bij:

- **Trainingsmodules aanbieden**: Bied trainingsmodules aan waarin ondernemers stapsgewijs eerst leren en daarna de opgedane kennis toepassen in specifieke opdrachten.

De gedragsbepaler **Hulpbronnen** is gerelateerd aan het werkingsmechanisme Omstandigheden & middelen. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorieën Sociale steun en Voorafgaande omstandigheden:

- Organiseer praktische ondersteuning en hulp;
- Herstructureer de omstandigheden.

Deze BCT kan het DTC gebruiken bij:

- **Cyberbuddy-koppels vormen**: Laat een vergelijkbare ondernemer ondersteunen en aanmoedigen: de cyberbuddy kan ter plekke instructies geven en demonstreren hoe bepaald gedrag i.r.t. veilig digitaal ondernemen of bijvoorbeeld het aanvragen van een subsidie uitgevoerd moeten worden. De cyberbuddy kan daarnaast beschikbaar zijn als back-up/vraagbaak.
- **Financiële ondersteuning aanbieden:** Maak het aanvragen van subsidie voor maatregelen, opleiding en training gemakkelijk.

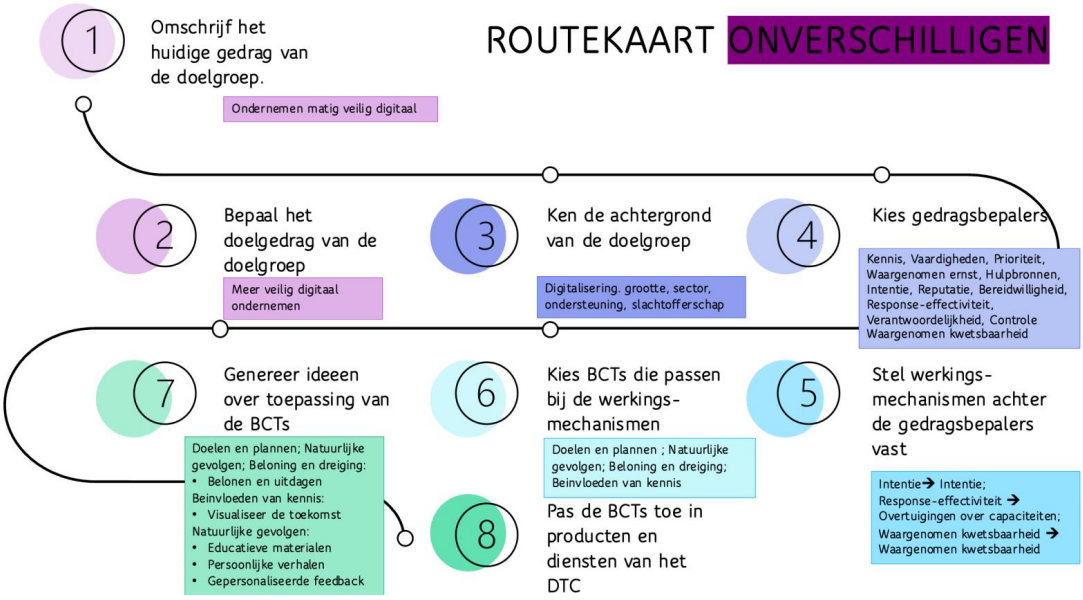
De gedragsbepaler **Response-effectiviteit** is gerelateerd aan het werkingsmechanisme Overtuigingen over capaciteiten. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorie Beinvloeden van kennis:

- Geef instructies over hoe het gedrag uit te voeren is.

Deze BCT kan het DTC gebruiken bij:

- **Trainingen aanbieden:** Maak het volgen van training en bijscholing mogelijk: awareness, gedrag aanleren en inslijpen, praktijkoefeningen, simulaties.

## 3.7.5 Interventies voor Onverschilligen




**Figuur 3.11:** Uitkomsten van de stappen om te komen tot interventies voor de doelgroep Onverschilligen.

*Huidig gedrag, doelgedrag en achtergrond van Onverschilligen*
Deze groep bestaat veelal uit zzp'ers die in lagere mate gedigitaliseerd zijn en weinig cyberincidenten hebben meegemaakt. Op de 11 gedragingen uit de Basisscan Cyberweerbaarheid scoren zij aanmerkelijk lager dan de Voorlopers, Uitbesteders, Overmoedigen en Machtelozen en het laagst op Tweefactorauthenticatie, Wachtwoordmanager gebruiken, Nadenken over response bij een cyberincident en Kwetsbaarheden identificeren.

Figuur **3.7** laat zien dat bedrijven in de groep Onverschilligen relatief laag scoren op alle gedragsbepalers: Kennis, Vaardigheden, Prioriteit, Waargenomen ernst, Hulpbronnen, Intentie, Reputatie, Bereidwilligheid, Response-effectiviteit, Verantwoordelijkheid, Controle en Waargenomen kwetsbaarheid.

*Gedragsbepalers, werkingsmechanismen, BCT's, interventie-ideeën voor Onverschilligen.*

Hier geven we een aantal interventie-ideeën die passen bij de gedragsbepalers Intentie, Response-effectiviteit en Waargenomen kwetsbaarheid.

De gedragsbepaler **Intentie** is gerelateerd aan het werkingsmechanisme Intentie. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorieën Doelen en plannen, Natuurlijke gevolgen, Beloning en dreiging:

- Doelen stellen (gedrag);
- Geef informatie over (emotionele-, sociale- en omgevings) gevolgen van het gedrag;
- Beloning in vooruitzicht stellen.

Deze BCTs kan het DTC gebruiken bij:

- **Beloningen en uitdagingen bieden**: Stel bedrijven een beloning (korting, kans op een prijs) in het vooruitzicht als zijn de Basisscan Cyberweerbaarheid voltooien.

De gedragsbepaler **Response-effectiviteit** is gerelateerd aan het werkingsmechanisme Overtuigingen over capaciteiten. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorie Beinvloeden van kennis:

- Geef instructies over hoe het gedrag uit te voeren is.

Deze BCTs kan DTC gebruiken bij:

- **Toekomst visualiseren**: Daag ondernemers uit zich voor te stellen hoe ze zich zouden voelen als zij slachtoffer zouden worden van een cyberincident als gevolg van onveilig digitaal ondernemen.

De gedragsbepaler **Waargenomen kwetsbaarheid** is gerelateerd aan het werkingsmechanisme Waargenomen kwetsbaarheid. Dit werkingsmechanisme is verbonden met gedragsveranderingstechnieken uit de categorie Natuurlijke gevolgen:

- Geef informatie over (emotionele-, sociale- en omgevings) gevolgen van het gedrag;
- Vestig de aandacht op de gevolgen van het wel of niet uitvoeren van gedrag.

Deze BCTs kan DTC gebruiken bij:

- **Educatieve materialen verstrekken:** Verstrek informatie via afbeeldingen, grafieken en tekst over (emotionele-, sociale- en omgevings) gevolgen van onveilig digitaal ondernemen. Bijvoorbeeld via Informatie & Advies, Toolkits en Campagnes.

- **Persoonlijke verhalen laten delen:** Laat vergelijkbare ondernemers vertellen over de ernstige gevolgen van onveilig digitaal ondernemen voor hunzelf, hun onderneming en hun naaste omgeving. Bijvoorbeeld via Ondernemersverhalen en Netwerkbijeenkomsten.
- **Gepersonaliseerde feedback geven**: Simuleer een schijnaanval en laat de ondernemer ervaren in hoeverre hij/zij veilig digitaal onderneemt. Leg hierbij de nadruk op Kwetsbaarheden identificeren, Tweefactorauthenticatie, Nadenken over de response bij een cyberincident en Gebruiken van een wachtwoordmanager. Bijvoorbeeld via Basisscan, Cyberveilig Check en Procesautomatisering Check.

# 4 Conclusie

Het Digital Trust Center (DTC) wil inzicht verkrijgen in hoe het veilig digitaal ondernemen bij verschillende doelgroeporganisaties kan bevorderen. Een deel van de doelgroeporganisaties neemt nog onvoldoende beschermende maatregelen tegen cyberdreigingen. Het DTC wil deze doelgroeporganisaties gericht kunnen ondersteunen met producten en diensten.

TNO heeft onderzocht hoe doelgroeporganisaties die momenteel onvoldoende veilig digitaal ondernemen, gestimuleerd kunnen worden tot het nemen van beschermende maatregelen die hun cyberweerbaarheid vergroten. Om deze hoofdvraag te beantwoorden, zijn de volgende drie deelonderzoeksvragen beantwoord:

1. Op welke doelgroeporganisaties zou het DTC zich moeten richten?
   - Welke specifieke doelgroepen zijn er te onderscheiden?
   - Wat zijn specifieke gedragingen die aangemoedigd kunnen worden bij deze doelgroepen?

2. Waarom nemen deze bedrijven niet de noodzakelijke maatregelen om zichzelf beter te beschermen?
   - Wat zijn de belemmeringen of drempels die deze organisaties ervan weerhouden om maatregelen te treffen?
   - Welke gedragsbepalers spelen hierbij een rol, zoals kennis, prioriteiten en waargenomen kwetsbaarheid?

3. Hoe kan het DTC hierop reageren?
   - Wat zijn de stappen om te komen tot interventies voor de (drie) doelgroepen die achterblijven op het gebied van veilig digitaal ondernemen?
   - Welke interventies zou het DTC kunnen inzetten om deze doelgroepen te ondersteunen?

Hieronder geven we de belangrijkste resultaten weer en sluiten we af met enkele aanbevelingen.

## 4.1 Doelgroepen

De doelgroeporganisaties zijn opgedeeld in vijf doelgroepen.

Voorlopers

Bedrijven binnen deze groep laten een patroon zien van het nemen van alle vereiste beschermende maatregelen. Ze zijn in staat om deze maatregelen te nemen, hebben de hulpbronnen om dat te doen en zijn zeer gemotiveerd.

Uitbesteders

Ook bedrijven in deze groep scoren hoog op veilig digitaal ondernemen, maar niet zo hoog als Voorlopers. Ze zijn vergelijkbaar met Voorlopers, maar zijn van mening dat het nemen van beschermende maatregelen niet de verantwoordelijkheid is van hun eigen organisatie, en besteden hun cybersecurity in grote mate uit aan externe IT-serviceproviders (72%).

Overmoedigen

Overmoedigen vertonen een patroon van het nemen van beschermende maatregelen, maar in mindere mate dan Voorlopers en Uitbesteders. Ze onderschatten de gevolgen van een cyberbeveiligingsincident. Deze organisaties geven niet veel om hoe hun organisatie bekend staat bij hun klanten en relaties wat betreft de mate van cyberveiligheid in hun bedrijfsvoering en denken dat de kans om slachtoffer te worden klein is.

Machtelozen

Machtelozen nemen onvoldoende beschermende maatregelen. Ze hebben weinig kennis, vaardigheden en hulpbronnen om zichzelf te beschermen. Ze onderschatten de gevolgen van een cyberbeveiligingsincident echter niet, en denken dat de kans om slachtoffer te worden aanwezig is.

Onverschilligen

Onverschilligen nemen onvoldoende beschermende maatregelen. Tegelijkertijd zijn ze niet overtuigd dat het nemen van aanbevolen maatregelen daadwerkelijk de dreiging zal verminderen, ze zijn niet gemotiveerd om hun organisatie te beschermen en denken dat de kans om slachtoffer te worden klein is.

Deze groepen verschillen van elkaar wat betreft de mate van veilig digitaal ondernemen en onderliggende gedragsbepalers, bijvoorbeeld kennis, waargenomen kwetsbaarheid en belang dat bedrijven hechten aan veilig digitaal ondernemen. Deze segmentering biedt het DTC inzicht in de behoeften en uitdagingen van de verschillende doelgroepen op het gebied van veilig digitaal ondernemen. Met deze kennis kan het DTC de doelgroepen gerichter ondersteunen bij het nemen van beschermingsmaatregelen.

Als het DTC bedrijven die momenteel achterblijven op het gebied van veilig digitaal ondernemen wil stimuleren, dan zijn de Overmoedigen, Machtelozen en Onverschilligen de groepen waarop het DTC zich zou moeten richten. Samen vormen zij 66% van de bedrijven.

Voor deze drie doelgroepen zijn specifieke gedragingen relevant om te stimuleren.

Overmoedigen

- Moedig bedrijven in deze groep aan om hun response op een cyberincident uit te werken.
- Stimuleer het gebruik van een wachtwoordmanager om wachtwoorden veilig te beheren.

Machtelozen

- Benadruk het belang van tweefactorauthenticatie om accounts te beschermen.
- Moedig regelmatige updates van software en systemen aan.

Onverschilligen

- Ondersteun bedrijven in deze groep bij het identificeren van kwetsbaarheden in hun systemen.
- Moedig hen aan om hun response op een cyberincident uit te werken.
- Stimuleer het gebruik van zowel tweefactorauthenticatie als een wachtwoordmanager.

Ook de groep Uitbesteders kan worden geholpen door het DTC. Denk bijvoorbeeld aan producten en diensten die hen ondersteunen bij het uitbesteden van IT-diensten, zoals sjablonen voor service level overeenkomsten en richtlijnen voor gesprekken met IT-dienstverleners. Ook kunnen bedrijven in de groep Uitbesteders worden aangemoedigd om een wachtwoordmanager te gebruiken om hun wachtwoorden te beheren. Dit is ook het gedrag dat bij bedrijven in de groep Voorlopers gestimuleerd kan worden. Daarnaast kunnen deze bedrijven een belangrijke rol spelen bij het ondersteunen van andere bedrijven, bijvoorbeeld door hun kennis door te delen via het online platform van de DTC community.

## 4.2 Gedragsbepalers

Er zijn acht factoren die van invloed zijn op de mate waarin de doelgroeporganisaties veilig digitaal ondernemen. Het ontbreken van kennis, vaardigheden en hulpbronnen vormt een belangrijke belemmering voor veilig digitaal ondernemen. Bedrijven weten bijvoorbeeld niet hoe of waar te beginnen of waar ze de kennis kunnen vinden om hen op weg te helpen. Er zijn ook bedrijven die geen financiële ruimte hebben voor de aanschaf van cybersecuritymiddelen of waarbij steun vanuit de sociale omgeving of het hogere management ontbreekt om te investeren. Ook een ontbrekende intentie om het bedrijf te beschermen en een onderschatting van de gevolgen zijn negatief van invloed op veilig digitaal ondernemen. Daarnaast scoren bedrijven die geen personeel hebben, of die niet ondersteund worden door een externe IT-dienstverlener, of die in lage mate gedigitaliseerd zijn lager op het gebied van veilig digitaal ondernemen.

Bij de doelgroepen die achterblijven in veilig digitaal ondernemen spelen verschillende gedragsbepalers een belangrijke rol.

Bedrijven in de groep Overmoedigen scoren relatief laag op vier gedragsbepalers:

- Waargenomen ernst: ze onderschatten de ernst van cyberincidenten.
- Reputatie: ze hechten weinig waarde aan hun digitale reputatie.
- Bereidwilligheid: ze zijn minder geneigd om actie te ondernemen.
- Waargenomen kwetsbaarheid: ze zien hun bedrijf als minder kwetsbaar.

Bedrijven in de groep Machtelozen scoren relatief laag op een breed scala aan gedragsbepalers: Kennis, Vaardigheden, Hulpbronnen, Intentie, Reputatie, Bereidwilligheid, Response-effectiviteit, Verantwoordelijkheid en Controle.

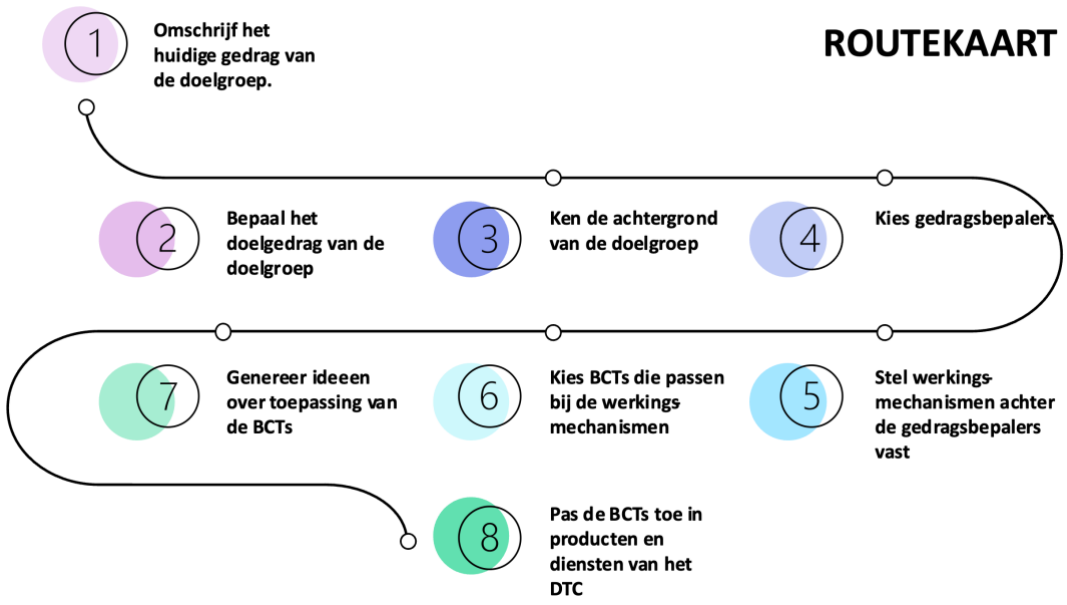
En bedrijven in de groep Onverschilligen scoren relatief laag op *alle* gedragsbepalers: Kennis, Vaardigheden, Prioriteit, Waargenomen ernst, Hulpbronnen, Intentie, Reputatie, Bereidwilligheid, Response-effectiviteit, Verantwoordelijkheid, Controle en Waargenomen kwetsbaarheid.

Op basis van deze gedragsbepalers kan het DTC gerichte interventies toepassen om deze groepen te ondersteunen.

## 4.3 Interventies

De bedrijven in de groep Voorlopers hebben al belangrijke maatregelen genomen om hun digitale weerbaarheid te verbeteren. Het doel voor deze bedrijven is om hun huidige aanpak voort te zetten. Deze bedrijven kunnen daarnaast een waardevolle rol spelen bij het bereiken en motiveren van andere bedrijven. Bedrijven in de groep Uitbesteders zijn in sterke mate afhankelijk van hun externe IT-dienstverleners. Voor deze bedrijven is het cruciaal dat zij een gelijkwaardige gesprekspartner zijn of worden voor externe partijen.

Op het gebied van het treffen van maatregelen voor veilig digitaal ondernemen zijn er drie doelgroepen die achterblijven. Deze groepen worden aangeduid als de Overmoedigen, Machtelozen en Onverschilligen. Voor bedrijven in deze doelgroepen is het van belang dat het DTC hen gericht aanmoedigt om specifieke cyberbeschermingsmaatregelen te treffen. Bedrijven in deze groepen ondervinden verschillende factoren die hen belemmeren om daadwerkelijk maatregelen te nemen. Het DTC kan via een reeks stappen tot interventies komen die aansluiten bij de behoeften van elke specifieke doelgroep. De stappen zijn weergegeven in de onderstaande generieke routekaart, in Figuur **4.1**.




**Figuur 4.1:** Routekaart om te komen tot interventies.

Voor de doelgroepen Overmoedigen, Machtelozen en Onverschilligen zijn specifieke routekaarten opgesteld. De uitkomsten van de gevolgde stappen voor elk van deze drie doelgroepen zijn weergegeven in Figuur **3.9**, Figuur **3.10** en Figuur **3.11** van dit rapport (zie ook Bijlage A).

## 4.4 Aanbevelingen

Uit dit onderzoek zijn twee strategische aanbevelingen voortgekomen. Deze aanbevelingen geven het DTC richting bij het vergroten van de actiebereidheid van de doelgroeporganisaties en het bewerkstelligen van daadwerkelijke gedragsverandering.

Deze aanbevelingen zijn in overeenstemming met een conceptadvies over de cyberweerbaarheid van het Nederlandse midden- en kleinbedrijf aan de ministers van Justitie en Veiligheid en Economische Zaken en Klimaat door de Cyber Security Raad[15] en een recente studie door Deloitte naar de cyberweerbaarheidskloof[16]. Het uitgangspunt hierbij is om het de gehele doelgroep te bereiken – dus niet enkel op zoek te gaan naar achterblijvers die in potentie het grootste risico lopen – en de aanpak te baseren op de daadwerkelijke behoeften van deze ondernemers en de gedragsbepalers die aan het handelen ten grondslag liggen. Deze aanbevelingen zijn:

1. Uitwerking, implementatie en evaluatie van stimulerende maatregelen voor een algemeen weerbaardere doelgroep, zodat doelgroeporganisaties daadwerkelijk stappen ondernemen om hun situatie te verbeteren. Het huidige onderzoek heeft aangetoond welke specifieke motivaties en barrières er zijn voor bepaalde doelgroepen. Ook zijn er voorbeelden gegeven van interventies die bedrijven in deze doelgroepen kunnen motiveren om stappen te zetten om hun eigen cyberweerbaarheid te vergroten óf anderen te helpen bij het nemen van maatregelen (bijvoorbeeld door ‘voorlopers’ te ondersteunen bij het helpen van ‘achterblijvers’). Deze aanbeveling richt zich op het uitwerken, implementeren en evalueren van specifieke stimulerende maatregelen die zijn afgestemd op de verschillende factoren die het gedrag van ondernemers beinvloeden en die bepalend zijn voor hun beslissing om al dan niet actie te ondernemen. Een uitdaging hierbij is om ook die ondernemers te bereiken die van nature geen reden zien om actie te ondernemen, ongeacht de kwaliteit en beschikbaarheid van hulpbronnen. Deze groep neemt soms weloverwogen het risico op een cyberincident voor lief.

2. Zorg ervoor dat geschikte producten en diensten beschikbaar zijn via passende, bekende en toegankelijke kanalen. Deze aanbeveling richt zich op het bereiken van specifieke doelgroepen, inclusief de moeilijk bereikbare. Deze doelgroepen hebben uiteenlopende behoeften, varierend van uitleg over basismaatregelen tot meetinstrumenten om weerbaarheidsniveaus in kaart te brengen en ondersteuning bij risicoanalyses. Het DTC kan gebruik maken van de verkorte vragenlijst die in dit onderzoek is ontwikkeld om bedrijven door te verwijzen naar naar passende producten en diensten. Bovendien blijkt uit dit onderzoek dat bedrijven in de verschillende groepen verschillende communicatiekanalen gebruiken om zichzelf te informeren over veilig digitaal ondernemen. Dit benadrukt het belang van maatwerk bij het leveren van producten en diensten. Deze producten en diensten moeten bovendien makkelijk toegankelijk zijn waarbij verspreiding, ook in de toekomst, plaatsvindt via een centraal loket.

[15] CSR, 2024. Concept. ‘Verkleinen van de cyberweerbaarheidskloof’. Advies over de cyberweerbaarheid van het Nederlandse midden- en kleinbedrijf. CSR-advies 2024, nr. 2.
[16] Deloitte, 2024. Cyberweerbaarheidskloof. Onderzoek naar de mogelijkheden om bedrijven binnen het mkb te helpen bij het bereiken van een optimaal cyberweerbaarheidsniveau. 02 februari 2024, conceptversie.

# Referenties


Amemori, M., Michie, S., Korhonen, T., Murtomaa, H. & Kinnunen, T. H. (2011). Assessing implementation difficulties in tobacco use prevention and cessation counselling among dental providers. *Implementation Science*, *6*, 1-10.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50* (2), 179–211.

Björk, F., Henkel, M., Stirna, J. & Zdravkovic, J. (2015). Cyber resilience – fundamentals for a definition. In: Rocha, A., Correia, A.M., Costanzo, S., Reis, L.P. (Eds.), *New Contributions in Information Systems and Technologies.* London: Springer, 311-316.

Champion, V. L. & Skinner, C. S. (2008). The health belief model. *Health behavior and health education: Theory, research, and practice*, 4, 45-65.

Dodel, M. & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, 68, 359-367.

Dupont, B., Shearing, C., Bernier, M. & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security*, *132*, 103372.

Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. (2006). *Multivariate data Analysis.* New Jersey: Prentice Hall.

Hair, J. F., Ringle, C. M. & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19* (2), 139-152.

Herath, T. & Rao, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*, 106-125.

Hoekstra, M., De Vries, S., Berkenpas M. & Jansen, J. (2021). *De werking van de basisscan cyberweerbaarheid*. Thorbecke academie, NHL Stenden.

Huijg, J. M., Gebhardt, W. A., Dusseldorp, E., Verheijden, M. W., van der Zouwe, N., Middelkoop, B. J. & Crone, M. R. (2014). Measuring determinants of implementation behavior: psychometric properties of a questionnaire based on the theoretical domains framework. *Implementation Science*, *9*(1), 1-15.

Jamanota. R. (2023). *Multicollineariteit – Wat is het en hoe bereken of bewijs je het?* Scriptium. https://www.scriptium.nl/multicollineariteit/

Michie, S., Atkins, L. & West, R. (2014). The behaviour change wheel. A guide to designing interventions. 1st ed. Great Britain: Silverback Publishing.

Michie, S., Van Stralen, M.M. & West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science*, *6* (1), 1-12.

Michie, S. & Johnston, M. (2013). Behavior Change Techniques. In: *Gellman, M.D., Turner, J.R.* (eds) Encyclopedia of Behavioral Medicine. Springer, New York, NY.

Van der Kleij, R., Wijn, R. & Hof, T. (2020). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. *Computers & Security, Vol. 97.* 101938.

Van der Kleij, R., Van 't Hoff - De Goede, S., Van de Weijer, S. & Leukfeldt, R. (2020). Ons cybergedrag is veel onveiliger dan we zelf denken. Implicaties voor effectief beïnvloedingsbeleid door de overheid. *Justitiële Verkenningen, 46* (2), 113-128.

Van der Kleij, R. & Leukfeldt, R. (2019). Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In: *Ahram T., Karwowski W.*

(eds.), Advances in Human Factors in Cybersecurity. AHFE 2019. Advances in Intelligent Systems and Computing, vol 960. Springer, Cham.

Van der Kleij, R., Van 't Hoff-De Goede, S., Van de Weijer, S. & Leukfeldt, R. (2021). How Safely Do We Behave Online? An Explanatory Study into the Cybersecurity Behaviors of Dutch Citizens. In*: Zallio M., Raymundo Ibañez C., Hernandez J.H.* (eds) Advances in Human Factors in Robots, Unmanned Systems and Cybersecurity. AHFE 2021. Lecture Notes in Networks and Systems, vol 268. Springer, Cham.

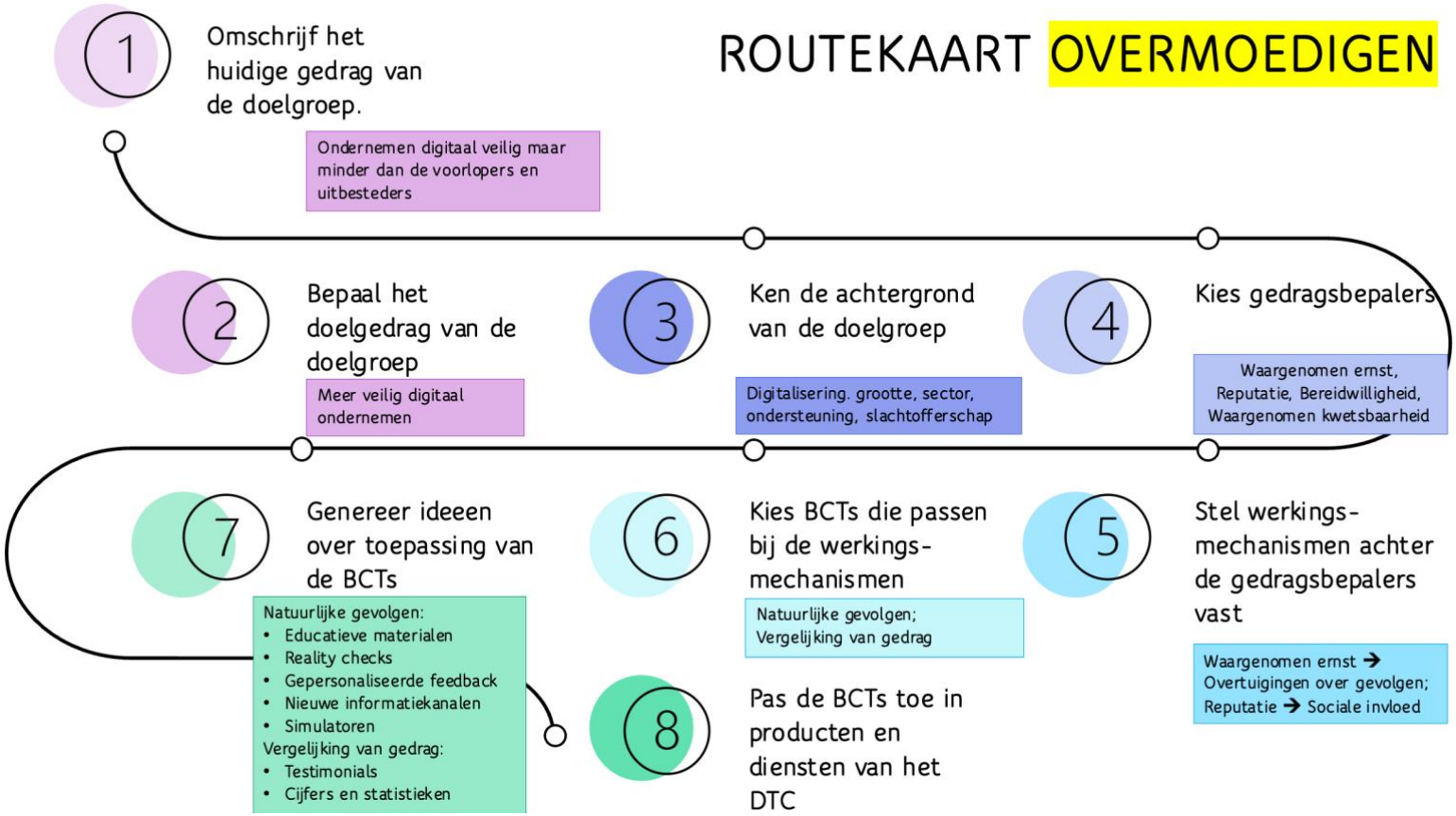
Witte, K. (1996) Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale, *Journal of Health Communication, 1*(4), 317-342.

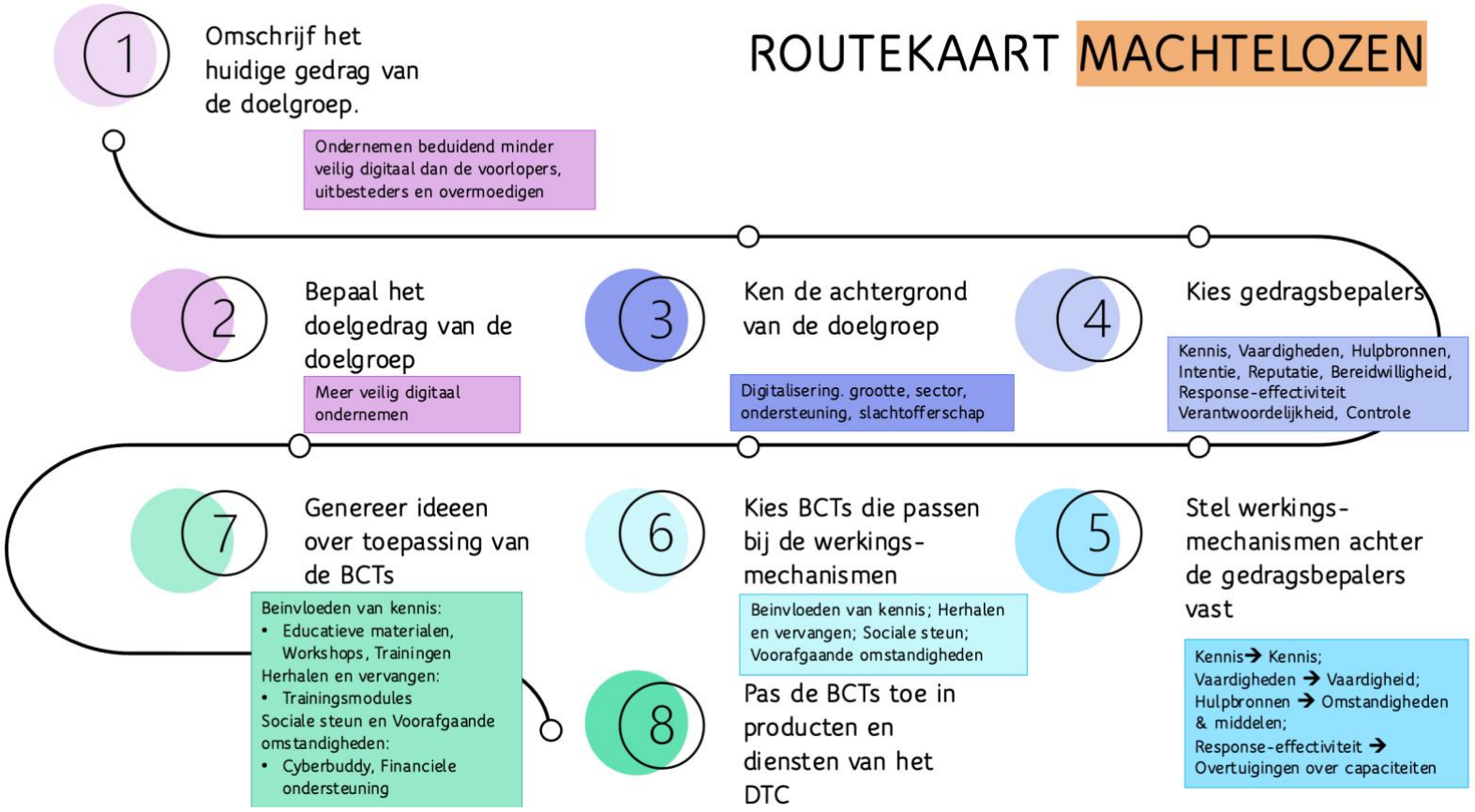
Workman, M., Bommer, W. H. & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816

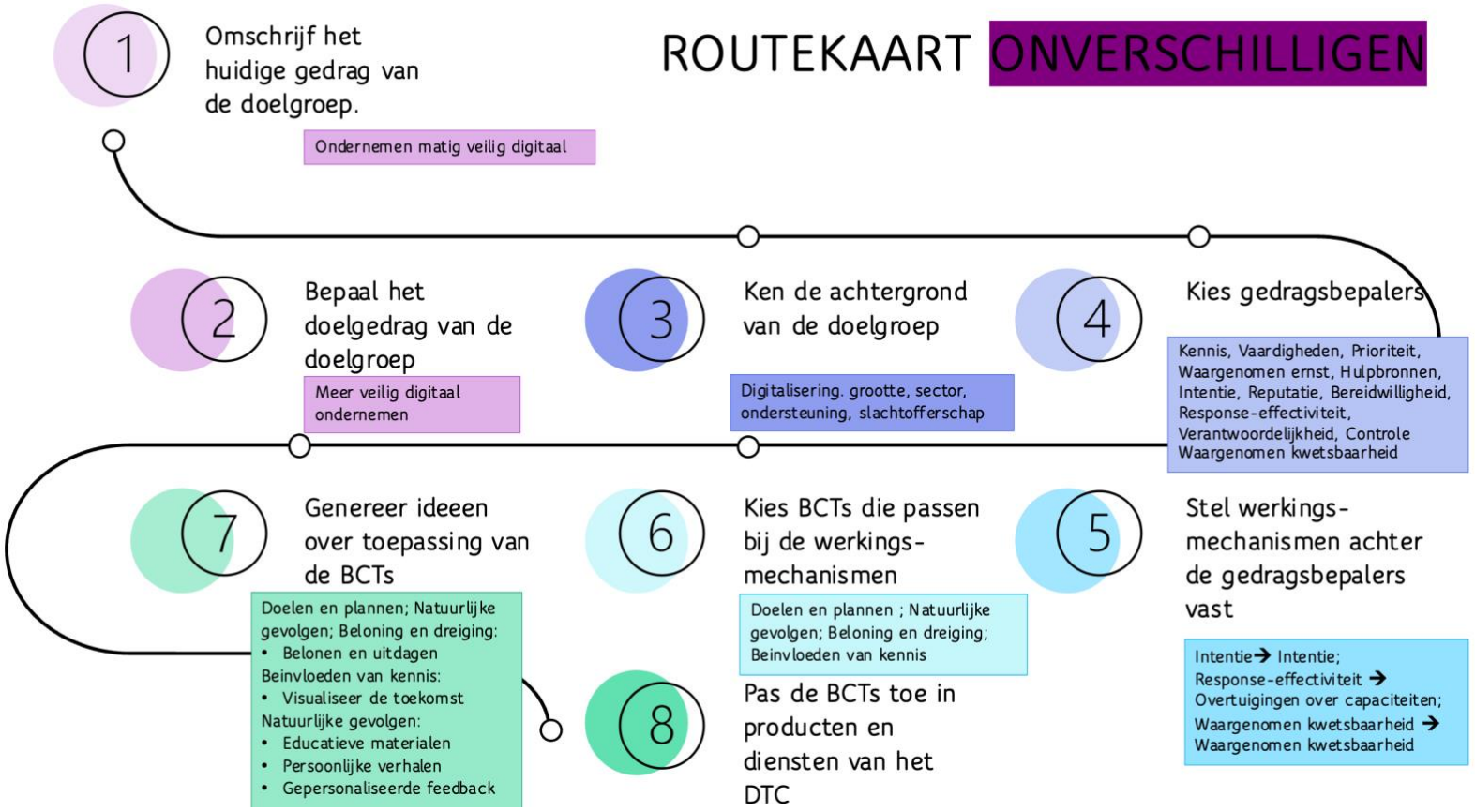
Weinstein, N. D. (1987). Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample. *Journal of Behavioral Medicine, 10*(5), 481-500.

Bijlage A

# Routekaarten


ROUTEKAART OVERMOEDIGEN
1
Omschrijf het huidige gedrag van de doelgroep.
Ondernemen digitaal veilig maar minder dan de voorlopers en uitbesteders
2
Bepaal het doelgedrag van de doelgroep
Meer veilig digitaal ondernemen
3
Ken de achtergrond van de doelgroep
Digitalisering. grootte, sector, ondersteuning, slachtofferschap
4
Kies gedragsbepalers
Waargenomen ernst, Reputatie, Bereidwilligheid, Waargenomen kwetsbaarheid
5
Stel werkings-mechanismen achter de gedragsbepalers vast
Waargenomen ernst → Overtuigingen over gevolgen; Reputatie → Sociale invloed
6
Kies BCTs die passen bij de werkings-mechanismen
Natuurlijke gevolgen; Vergelijking van gedrag
7
Genereer ideeen over toepassing van de BCTs
Natuurlijke gevolgen:
• Educatieve materialen
• Reality checks
• Gepersonaliseerde feedback
• Nieuwe informatiekanalen
• Simulatoren
Vergelijking van gedrag:
• Testimonials
• Cijfers en statistieken
8
Pas de BCTs toe in producten en diensten van het DTC


ROUTEKAART MACHTELOZEN
1
Omschrijf het huidige gedrag van de doelgroep.
Ondernemen beduidend minder veilig digitaal dan de voorlopers, uitbesteders en overmoedigen
2
Bepaal het doelgedrag van de doelgroep
Meer veilig digitaal ondernemen
3
Ken de achtergrond van de doelgroep
Digitalisering. grootte, sector, ondersteuning, slachtofferschap
4
Kies gedragsbepalers
Kennis, Vaardigheden, Hulpbronnen, Intentie, Reputatie, Bereidwilligheid, Response-effectiviteit Verantwoordelijkheid, Controle
5
Stel werkings-mechanismen achter de gedragsbepalers vast
Kennis➔ Kennis;
Vaardigheden ➔ Vaardigheid;
Hulpbronnen ➔ Omstandigheden & middelen;
Response-effectiviteit ➔ Overtuigingen over capaciteiten
6
Kies BCTs die passen bij de werkings-mechanismen
Beinvloeden van kennis; Herhalen en vervangen; Sociale steun; Voorafgaande omstandigheden
7
Genereer ideeen over toepassing van de BCTs
Beinvloeden van kennis:
• Educatieve materialen, Workshops, Trainingen
Herhalen en vervangen:
• Trainingsmodules
Sociale steun en Voorafgaande omstandigheden:
• Cyberbuddy, Financiele ondersteuning
8
Pas de BCTs toe in producten en diensten van het DTC


ROUTEKAART ONVERSCHILLIGEN
1
Omschrijf het huidige gedrag van de doelgroep.
Ondernemen matig veilig digitaal
2
Bepaal het doelgedrag van de doelgroep
Meer veilig digitaal ondernemen
3
Ken de achtergrond van de doelgroep
Digitalisering. grootte, sector, ondersteuning, slachtofferschap
4
Kies gedragsbepalers
Kennis, Vaardigheden, Prioriteit, Waargenomen ernst, Hulpbronnen, Intentie, Reputatie, Bereidwilligheid, Response-effectiviteit, Verantwoordelijkheid, Controle Waargenomen kwetsbaarheid
5
Stel werkings-mechanismen achter de gedragsbepalers vast
Intentie→ Intentie;
Response-effectiviteit → Overtuigingen over capaciteiten;
Waargenomen kwetsbaarheid → Waargenomen kwetsbaarheid
6
Kies BCTs die passen bij de werkings-mechanismen
Doelen en plannen ; Natuurlijke gevolgen; Beloning en dreiging; Beinvloeden van kennis
7
Genereer ideeen over toepassing van de BCTs
Doelen en plannen; Natuurlijke gevolgen; Beloning en dreiging:
• Belonen en uitdagen
Beinvloeden van kennis:
• Visualiseer de toekomst
Natuurlijke gevolgen:
• Educatieve materialen
• Persoonlijke verhalen
• Gepersonaliseerde feedback
8
Pas de BCTs toe in producten en diensten van het DTC

# Bijlage B
# Groepsgesprekken met ondernemers

**Aanleiding**
Op basis van achtergrondliteratuur en interne werksessies is een eerste segmentering gemaakt. Het slidedeck (Doelgroepsegmenten en persona's) met deze eerste segmentering, de bevindingen uit de groepsgesprekken, de aangepaste segmentering en de persona's is gedeeld met het DTC. Meer informatie over de persona's is te vinden in Bijlage C.


We hebben deze eerste segmentering in zes doelgroepen getoetst met ondernemers.

**Methode**
De eerste opzet van de doelgroepen is getoetst met ondernemers aan de hand van de volgende vragen:

- Herken jij jezelf in een van deze doelgroepen?
- Welke beschrijving past bij jou?
- Ontbreken bij deze groepen redenen, motieven of barrières die jullie eerder hebben genoemd? Zo ja, welke precies? En bij welke groep horen die?

**Resultaten**

In totaal hebben 3 sessies met ondernemers plaatsgevonden, waarvan 1 individueel gesprek en 2 groepssessies.

Hieruit kwamen samengevat de volgende punten naar voren:

- Over het algemeen herkenden de deelnemers de verschillende segmenten en konden ze zichzelf plaatsen. De meeste ondernemers plaatsten zichzelf in groep ‘b’. Dit werd mede veroorzaakt door de volgende motivatie:
  - Met betrekking tot groep ‘a’ werd aangegeven dat deze groep wellicht niet bestond: 100% cybersecure en –weerbaar is niet realistisch en beperkt meetbaar.

- Er waren niet te veel groepen, maar 1 deelnemer gaf aan dat er een groep ontbrak:
  - De groep die wel bezig was, maar ook wist dat de digitale weerbaarheid nog niet op orde was.

Dit heeft geleid tot aanpassing van de doelgroepen zoals hieronder zichtbaar op de volgende slide.

# Bijlage C
# Persona’s

## Aanleiding

Segmenten verwijzen naar verschillende groepen ondernemers die van elkaar verschillen op basis van diverse factoren zoals bekwaamheid, kennis en motivatie. Deze verschillen kunnen aanzienlijk zijn en hebben invloed op de manier waarop zij reageren op bepaalde producten of diensten.

Persona’s zijn een effectief hulpmiddel bij het (her)ontwerpen van toepassingen, in dit geval producten en diensten op de website van het Digital Trust Centre. Persona’s helpen ontwerpers om een beter begrip te krijgen van de (toekomstige) gebruikers van hun producten of diensten. Persona’s zijn fictieve karakters die een specifieke doelgroep representeren. Ze zijn ontworpen om de kenmerken, behoeften, motieven en bekwaamheden van elke doelgroep te belichten.

Het gebruik van persona’s kan helpen om een toepassing te creëren die aantrekkelijk is voor verschillende doelgroepen en hen aanzet tot actie. Door de gebruikers te verlevendigen, kunnen ontwerpers een product of dienst ontwerpen die echt aansluit bij de behoeften en verwachtingen van de eindgebruiker. Dit resulteert in een meer gepersonaliseerde en effectieve gebruikerservaring. Persona’s zijn archetypen die de essentiële kenmerken en motivaties van een doelgroep naar voren brengen, waardoor ontwerpers een dieper inzicht krijgen in de gebruikers die zij bedienen.

## Methode

Op basis van literatuur, de groepsgesprekken met ondernemers en de inhoudelijke gesprekken met de DTC-projectbegeleiders hebben we informatie en voorlopige inzichten met betrekking tot de zes segmenten verzameld. Vervolgens hebben we in een interne brainstormsessie onze ideeën en inzichten over de kenmerken van de segmenten, hun behoeften en hun uitdagingen met elkaar gedeeld. De gemeenschappelijke kenmerken en patronen die per segment naar voren kwamen tijdens deze werksessie vormden vervolgens de basis voor de verdere uitwerking van de persona’s. We hebben elke persona een naam gegeven en voorzien van een korte schets van hun onderneming/bedrijf, hun visie op en ervaring met cyberweerbaarheid en een kenmerkende quote.

## Resultaten

**Persona 1**
Persona 1 is een representant van de Voorlopers. Deze ondernemers hebben hun digitale weerbaarheid (relatief) goed op orde.

**Anne, eigenaar van een kledingmerk**
Anne begon jaren geleden met een idee voor een kledinglijn en heeft ondertussen al redelijk wat mensen in dienst. Anne heeft het fundament van digitale weerbaarheid van het bedrijf op orde. Door een hack bij een collega-ondernemer werd zichtbaar wat de gevolgen zouden kunnen zijn voor Annes bedrijf. Ondertussen heeft Anne veel stappen ondernomen, bijv. op het gebied van certificering. Het bedrijf is en blijft relatief cyberweerbaar. Dit weet Anne door de regelmatige pen-testen die worden uitgevoerd door een externe dienstverlener.

*“Digitale weerbaarheid is nodig en ik doe mijn best om het zo goed mogelijk op orde te hebben. Liever nu investeren dan straks alles verliezen.”*

**Persona 2**
Persona 2 is een representant van de Overmoedigen. Deze ondernemers denken dat hun digitale weerbaarheid op orde is, maar dat is eigenlijk niet zo.

**Beau, eigenaar van een middelgroot ICT-bedrijf**
Beau is goed op de hoogte van alle ontwikkelingen op het gebied van cybersecurity en vindt het erg belangrijk dat het bedrijf digitaal weerbaar is. Vorig jaar heeft het ICT-bedrijf geïnvesteerd in de nieuwste software en er is een IT-consultant in dienst. Alles is op orde, of toch niet? Want heeft Beau wel de juiste opdracht gegeven aan de IT-consultant? En weten de medewerkers tijdens een incident eigenlijk wel wat ze moeten doen?

*“Ik denk dat ik goed bezig met het onderhouden van alle systemen en het implementeren van maatregelen”.*

**Persona 3**
Persona 3 is een representant van de Lerenden.
Deze ondernemers vinden digitale weerbaarheid belangrijk, maar weten niet hoe digitale weerbaarheid goed ingericht kan worden. Hun digitale weerbaarheid is (nog) niet op orde, want ze weten niet waar te beginnen of hoe te vervolgen.

**Charlie, verzorgt huiswerkbegeleiding aan scholen en bij gezinnen thuis**
Charlie maakt gebruik van digitale middelen bij het begeleiden van leerlingen bij hun huiswerk, zoals online bijeenkomsten, informatievideo’s en planningssystemen. Charlie is zich ervan bewust dat dit op een cyberveilige manier dient te gebeuren en heeft gezocht naar tools en advies om hierbij te helpen. Overrompeld door alle te maken keuzen heeft Charlie besloten om op een later moment wel weer aandacht te besteden aan de digitale weerbaarheid van het bedrijf.

*“Wat een overweldigend aanbod! Maar wat is nou goed en wat heb ik echt nodig om digitaal weerbaar te zijn? Ik weet niet waar ik moet beginnen…”*

**Persona 4**
Persona 4 is een representant van de Penningmeesters. Deze ondernemers vinden digitale weerbaarheid belangrijk, maar hebben geen financiële middelen om hun digitale weerbaarheid (in een keer) goed in te richten.

**Dezi, werkt bij een familiebedrijf in kaas in deeltijd als IT-expert**
Dezi is binnen het familiebedrijf verantwoordelijk, naast overige werkzaamheden, voor het inrichten en beheren van alle IT- en OT-systemen die nodig zijn voor de geautomatiseerde processen in het kaaspakhuis. Zo is onlangs nieuwe software ter ondersteuning van het logistieke proces in gebruik genomen. Dezi is zich ervan bewust dat digitale weerbaarheid belangrijk is en zou graag aanvullende maatregelen willen treffen. Dezi ondervindt echter weerstand binnen het bedrijf, want veiligheid is duur en levert niet direct iets op en kan derhalve geen toegang krijgen tot de middelen die nodig zijn om de digitale weerbaarheid echt goed in te richten.

*“Ik wil wel investeren in digitale weerbaarheid, maar ik krijg het niet voor elkaar om er voldoende financiële middelen voor vrij te maken.”*

**Persona 5**

Persona 5 is een representant van de Argelozen. Deze ondernemers vinden digitale weerbaarheid niet belangrijk, omdat ze risico's en consequenties onderschatten en/of zichzelf niet als doelwit zien.

**Elian, heeft een eigen kapperszaak**
Elian werkt hard en probeert elke dag vol te zitten met afspraken. Om het klantenbestand te behouden en uit te breiden maakt Elian reclame voor de kapperszaak via Instagram en maakt gebruik van een online bookingstool. Met digitale weerbaarheid is Elian niet bezig: "Iedereen gebruikt toch internet?"

*"Welk risico loop ik nou? Ik denk niet dat er bij mij iets van waarde te halen valt."*

**Persona 6**
Persona 6 is een representant van de Critici. Deze ondernemers doen uit principe niets aan digitale weerbaarheid, omdat zij digitale weerbaarheid onnodig complex of duur vinden,
of omdat zij het niet hun verantwoordelijkheid vinden.

**Fabien, eigenaar van een hoveniersbedrijf**
Fabien heeft al jaren het bedrijf. Fabien ziet vaak berichten voorbij komen over cyberweerbaarheid en de nieuwste tools. Deze verwijdert hij elke keer, want het is toch niet relevant. Het irriteert Fabien dat er steeds meer regels komen en hij veel spam krijgt over cybersecurity, wat hij beschouwt als geldklopperij. Volgens Fabien is de cybercrimineel verantwoordelijk voor zijn misdrijven, niet het slachtoffer. Volgens Fabien moet de overheid beter zijn best doen om criminelen aan te pakken en niet de ondernemers lastig te vallen met regeltjes en op kosten te jagen.

*"Cyberweerbaar zijn is onzin en duur."*

# Bijlage D
# Vragenlijst

Leeswijzer:

**Dikgedrukte teksten** zijn de namen van de hoofdstukken, respondenten krijgen dit niet te zien.

Teksten in *groen en cursief* geven aan hoe de antwoordcategorieën worden voorgelegd. Wanneer de antwoorden gerandomiseerd zijn, staan de 'anders, nl' en 'weet niet' categorie of 'geen van deze' altijd onderaan de lijst.

## Selectievragen

S1. Hoeveel personen zijn er bij benadering in dienst bij de organisatie/het bedrijf waar je werkt?

*Zijn er meerdere vestigingen van de organisatie waar je werkzaam bent, dan gaat het om de totale organisatie, dus alle vestigingen bij elkaar.*

*Single respons, niet randomiseren.*

- Ik werk als zelfstandige zonder personeel (zzp'er)
- 2-9 werknemers
- 10-49 werknemers
- 50-249 werknemers
- 250-400 werknemers
- Meer dan 400 werknemers
- Ik ben niet (meer) werkzaam

Indien werkzaam en maximaal 400 werknemers:

S2. Ben je binnen jouw organisatie (mede)beslisser voor veilig digitaal ondernemen *<mouseover: Veilig digitaal ondernemen houdt in dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging>* en krijg je op dit gebied ondersteuning van een externe IT-leverancier of dienstverlener?

*Single respons, niet randomiseren.*

- Ja, ik ben (mede)beslisser en ik krijg ondersteuning van een externe IT-leverancier of dienstverlener
- Ja, ik ben (mede)beslisser en ik krijg geen ondersteuning van een externe IT-leverancier of dienstverlener
- Nee, ik ben geen (mede)beslisser > einde vragenlijst
- Weet niet/geen mening > einde vragenlijst

- Niet van toepassing > einde vragenlijst

## Overige achtergrondvragen (branche en mate van digitalisering)

Q1. In welke branche werk je?

*Single respons, niet randomiseren.*

- Landbouw, bosbouw, visserij en delfstoffenwinning
- Industrie en energie
- Bouwnijverheid
- Handel, vervoer en horeca
- Informatie en communicatie
- Financiële dienstverlening
- Verhuur en handel van onroerend goed
- Zakelijke dienstverlening
- Overheid
- Onderwijs
- Gezondheids-en welzijnszorg
- Cultuur, sport en recreatie
- Overige branches/diensten

Q2. In welke mate is de bedrijfsvoering van jouw organisatie gedigitaliseerd?

- Niet gedigitaliseerd
- Nauwelijks gedigitaliseerd
- Gemiddeld gedigitaliseerd
- Veel gedigitaliseerd
- (Bijna) volledig gedigitaliseerd
- Weet niet/ geen mening

## Veilig digitaal ondernemen

Q3-7. In hoeverre ben je het eens of oneens met de volgende stellingen over veilig digitaal ondernemen binnen jouw organisatie? Onder veilig digitaal ondernemen verstaan we in de vragenlijst dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging.

Als er staat ‘mijn bedrijf/organisatie’ kun je ook lezen: ‘onze externe IT-leverancier of dienstverlener’.

*Randomiseren.*

> Mijn bedrijf/organisatie inventariseert regelmatig wat de kwetsbaarheden zijn van ICT-onderdelen

> Mijn bedrijf/organisatie maakt regelmatig een back-up (reservekopie) van alle belangrijke informatie

> In mijn bedrijf/organisatie denken we regelmatig na over wat te doen in het geval van een cyberincident *<mouseover: Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken>*

> Als sprake is van onveilige standaardinstellingen op (netwerk)apparatuur of software past bedrijf/organisatie deze direct aan

> Mijn bedrijf/organisatie controleert periodiek of de apparatuur en software binnen de organisatie up-to-date is

> Als er een update beschikbaar is voor de zakelijke mobiele telefoon of voor de apps die in gebruik zijn, installeert bedrijf/organisatie die direct

> Mijn bedrijf/organisatie zorgt ervoor dat op apparatuur en software binnen de organisatie automatisch updaten is aangezet

> Mijn bedrijf/organisatie zorgt ervoor dat medewerkers alleen toegang hebben tot de informatie die zij nodig hebben voor hun werkzaamheden

> Mijn bedrijf/organisatie zorgt ervoor dat het bedrijfsnetwerk alleen toegankelijk is voor medewerkers

> Mijn bedrijf/organisatie zorgt ervoor dat als een medewerker uit dienst gaat direct de toegang tot het pand, bedrijfsapparatuur en software worden afgesloten

> Mijn bedrijf/organisatie zorgt ervoor dat medewerkers niet alleen een gebruikersnaam en wachtwoord gebruiken om in te loggen op bedrijfssystemen, maar ook een extra beveiliging via bijvoorbeeld een code op een telefoon (tweefactor-authenticatie)

> Mijn bedrijf/organisatie zorgt ervoor dat medewerkers gebruik maken van een wachtwoordmanager *<mouseover: Een wachtwoordmanager is een digitale kluis die al je inloggegevens veilig voor je bewaart. Om deze kluis te openen maak je gebruik van één hoofdwachtwoord of een makkelijk te onthouden wachtwoordzin>* voor het veilig bewaren van inloggegevens

> Mijn bedrijf/organisatie controleert periodiek of op alle bedrijfsapparatuur antivirussoftware aanwezig is

> Mijn bedrijf/organisatie zorgt ervoor dat medewerkers alleen software van het internet kunnen downloaden en installeren wanneer daar specifieke toestemming voor is verstrekt

- Zeer oneens
- Oneens
- Enigszins oneens
- Niet eens, niet oneens
- Enigszins eens
- Mee eens
- Zeer eens
- Weet niet/geen mening

## Kennis en vaardigheden

Q8. In hoeverre ben je het eens of oneens met de volgende stellingen over jouw kennis en vaardigheden op het gebied van veilig digitaal ondernemen *<mouseover: Veilig digitaal ondernemen*

*houdt in dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging>*?

*Randomiseren.*

> Ik weet wat nodig is om veilig digitaal te ondernemen

> Ik weet hoe ik veilig digitaal kan ondernemen

> Ik heb de vaardigheden om veilig digitaal te kunnen ondernemen

> Ik ben getraind om veilig digitaal te kunnen ondernemen

- Zeer oneens
- Oneens
- Enigszins oneens
- Niet eens, niet oneens
- Enigszins eens
- Mee eens
- Zeer eens

## Prioriteit

Q9. Veilig digitaal ondernemen *<mouseover: Veilig digitaal ondernemen houdt in dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging>* is een onderwerp dat hoger of lager kan staan op de agenda van organisaties. Hoe vaak doen zich de volgende situaties voor binnen jouw organisatie?

**Andere onderwerpen op de agenda…**

*Randomiseren.*

> … hebben een hogere prioriteit dan veilig digitaal ondernemen

> … zijn meer urgent dan veilig digitaal ondernemen

> … zijn dringender dan veilig digitaal ondernemen

- Nooit
- Zelden
- Soms
- Vaak
- Altijd

## Waargenomen ernst

Q10. In hoeverre ben je het eens of oneens met de volgende stellingen over de ernst van cyberincidenten *<mouseover: Gebeurtenissen of acties waarbij de beveiliging van hardware, software, informatie, een proces of jouw organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken>*?

*Randomiseren.*

> Ik vind dat cyberincidenten een ernstig probleem zijn voor mijn organisatie

> Ik vind dat de productiviteit van mijn organisatie wordt bedreigd door cyberincidenten

> Ik vind dat het voortbestaan van mijn organisatie wordt bedreigd door cyberincidenten

- Zeer oneens
- Oneens
- Enigszins oneens
- Niet eens, niet oneens
- Enigszins eens
- Mee eens
- Zeer eens

## Hulpbronnen (resources)

Q11. In hoeverre ben je het eens of oneens met de volgende stellingen over de ondersteuning bij veilig digitaal ondernemen *<mouseover: Veilig digitaal ondernemen houdt in dat dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging>* binnen jouw organisatie?

**Om veilig digitaal te ondernemen ….**

*Randomiseren.*

> ….is voldoende tijd beschikbaar binnen mijn organisatie

> … heeft mijn organisatie de beschikking over voldoende financiële middelen

> … kan mijn organisatie rekenen op een team van professionals dat helpt

> … kan mijn organisatie rekenen op de medewerkers om te helpen

- Zeer oneens
- Oneens
- Enigszins oneens
- Niet eens, niet oneens
- Enigszins eens
- Mee eens
- Zeer eens

## Protectiemotivatie-intentie en Reputatie

Q12. In hoeverre ben je het eens of oneens met de volgende stellingen over de motivatie voor veilig digitaal ondernemen *<mouseover: Veilig digitaal ondernemen houdt in dat dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging>* binnen jouw organisatie?

*Randomiseren.*

> Wij willen graag de cyberweerbaarheid van de organisatie op orde brengen

> Wij zijn bereid er alles aan te doen om de organisatie te beschermen tegen cyberincidenten

> Wij willen dat onze organisatie bij onze klanten of relaties bekend staat om hoe wij veilig digitaal ondernemen

> Wij willen een voorbeeld zijn voor andere organisaties op het gebied van veilig digitaal ondernemen

- Zeer oneens
- Oneens
- Enigszins oneens
- Niet eens, niet oneens
- Enigszins eens
- Mee eens
- Zeer eens

## Onder eigen controle & Eigen verantwoordelijkheid (locus of control)

Q13. Kun je hieronder aanvinken in hoeverre je het meer eens bent met het linker uiteinde of met het rechter uiteinde van de stelling.

*Hoe meer je naar rechts antwoordt, hoe meer je het eens bent met het rechter uiteinde, hoe meer naar links je antwoordt, hoe meer je het eens bent met het linker uiteinde.*

Veilig digitaal ondernemen *<mouseover: Veilig digitaal ondernemen houdt in dat dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging>*...

*Randomiseren.*

*Slider met 7 punten en ankers op de uiterste waarden.*

> … ligt buiten de controle van mijn organisatie o o o o o o o … ligt binnen de controle van mijn organisatie

> … is de verantwoordelijkheid van mijn organisatie o o o o o o o … is de verantwoordelijkheid van anderen

## Bereidwilligheid

Q14. In hoeverre ben je het eens of oneens met de volgende stellingen over de intentie om veiliger digitaal te ondernemen *<mouseover: Veilig digitaal ondernemen houdt in dat dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging>* binnen jouw organisatie?

*Randomiseren.*

> Onze organisatie is van plan in de komende 12 maanden veiliger digitaal te gaan ondernemen

> Onze organisatie is voornemens in de komende 12 maanden maatregelen te nemen om de digitale veiligheid te vergroten

- Zeer oneens
- Oneens
- Enigszins oneens
- Niet eens, niet oneens
- Enigszins eens

- Mee eens
- Zeer eens
- Weet niet/geen mening

## Response-effectiviteit

Q15. In hoeverre ben je het eens of oneens met de volgende stellingen over het nut van veilig digitaal ondernemen *<mouseover: Veilig digitaal ondernemen houdt in dat dat ondernemers zich weren tegen digitale dreigingen en voldoende investeren in beveiliging>* voor jouw organisatie?

*Randomiseren.*

> Veilig digitaal ondernemen helpt onze organisatie om meer weerbaar te zijn tegen cyberrisico's die de bedrijfsvoering kunnen verstoren

> Veilig digitaal ondernemen is een effectieve manier om cyberincidenten te voorkomen

> Veilig digitaal ondernemen vermindert de kans om slachtoffer te worden van een cyberincident

- Zeer oneens
- Oneens
- Enigszins oneens
- Niet eens, niet oneens
- Enigszins eens
- Mee eens
- Zeer eens

## Waargenomen kwetsbaarheid

Q16. Hoe waarschijnlijk is het volgens jou dat jouw organisatie in de komende 12 maanden slachtoffer wordt van een cyberincident *<mouseover: Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken>*?

- Heel onwaarschijnlijk
- Onwaarschijnlijk
- Enigszins onwaarschijnlijk
- Niet waarschijnlijk, niet onwaarschijnlijk
- Enigszins waarschijnlijk
- Waarschijnlijk
- Heel waarschijnlijk

## Slachtofferschap

Q17. Heeft bij jouw organisatie in de afgelopen 12 maanden een cyberincident *<mouseover: Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken>* plaatsgevonden?

- Ja
- Nee
- Weet ik niet

## Overige vragen

Q18. Welke bronnen zijn voor jou het belangrijkst om je te informeren over veilig digitaal ondernemen?

Meerdere antwoorden mogelijk.

*Multiple response.*

*Randomiseren, behalve laatste 2.*

- ICT-beheerder binnen mijn organisatie
- Onze externe IT-leverancier of dienstverlener
- De bank
- Digital Trust Center (DTC)
- Nationaal Cyber Security Centrum (NCSC)
- Centrum voor Criminaliteitspreventie en Veiligheid (CCV)
- Platform Veilig Ondernemen (PVO)
- Kamer van Koophandel (KvK)
- MKB Nederland
- Brancheorganisaties
- Lokale ondernemersvereniging
- Medeondernemers
- Gemeente
- Familie of vrienden
- Zoekmachine op internet (zoals Google)
- Anders, namelijk ….
- Weet niet

Q19. Hoe zou de overheid jouw organisatie kunnen ondersteunen met veilig digitaal ondernemen?

Geef aan wat je belangrijkste wensen of behoeften zijn.

- *5 open tekstvakken.*
- Wij hebben geen behoefte aan ondersteuning door de overheid

## Einde

Je bent aan het einde gekomen van de vragenlijst. Als je nog wat wilt aanpassen, kan je nu nog terug gaan naar de voorgaande vragen.

# Bijlage E
# Syntax voorspellingsmodel

**SPSS-syntax voor 10 items.**

```
DO IF MISSING(iQ3_BP3_1).
COMPUTE #iQ3_BP3_1_lg=0.
COMPUTE #iQ3_BP3_1_lg_m=1.
ELSE.
COMPUTE #iQ3_BP3_1_lg=iQ3_BP3_1.
COMPUTE #iQ3_BP3_1_lg_m=0.
END IF.
DO IF MISSING(iQ8_A2).
COMPUTE #iQ8_A2_lg=0.
COMPUTE #iQ8_A2_lg_m=1.
ELSE.
COMPUTE #iQ8_A2_lg=iQ8_A2.
COMPUTE #iQ8_A2_lg_m=0.
END IF.
DO IF MISSING(iQ8_B2).
COMPUTE #iQ8_B2_lg=0.
COMPUTE #iQ8_B2_lg_m=1.
ELSE.
COMPUTE #iQ8_B2_lg=iQ8_B2.
COMPUTE #iQ8_B2_lg_m=0.
END IF.
DO IF MISSING(iQ10_3).
COMPUTE #iQ10_3_lg=0.
COMPUTE #iQ10_3_lg_m=1.
ELSE.
COMPUTE #iQ10_3_lg=iQ10_3.
COMPUTE #iQ10_3_lg_m=0.
END IF.
DO IF MISSING(iQ12_A2).
COMPUTE #iQ12_A2_lg=0.
COMPUTE #iQ12_A2_lg_m=1.
ELSE.
COMPUTE #iQ12_A2_lg=iQ12_A2.
COMPUTE #iQ12_A2_lg_m=0.
END IF.
DO IF MISSING(iQ12_B2).
COMPUTE #iQ12_B2_lg=0.
COMPUTE #iQ12_B2_lg_m=1.
ELSE.
COMPUTE #iQ12_B2_lg=iQ12_B2.
COMPUTE #iQ12_B2_lg_m=0.
END IF.
DO IF MISSING(iQ13_2R).
```

```
COMPUTE #iQ13_2R_lg=0.
COMPUTE #iQ13_2R_lg_m=1.
ELSE.
COMPUTE #iQ13_2R_lg=iQ13_2R.
COMPUTE #iQ13_2R_lg_m=0.
END IF.
DO IF MISSING(iQ15_1).
COMPUTE #iQ15_1_lg=0.
COMPUTE #iQ15_1_lg_m=1.
ELSE.
COMPUTE #iQ15_1_lg=iQ15_1.
COMPUTE #iQ15_1_lg_m=0.
END IF.
DO IF MISSING(iQ15_2).
COMPUTE #iQ15_2_lg=0.
COMPUTE #iQ15_2_lg_m=1.
ELSE.
COMPUTE #iQ15_2_lg=iQ15_2.
COMPUTE #iQ15_2_lg_m=0.
END IF.
DO IF MISSING(iQ16).
COMPUTE #iQ16_lg=0.
COMPUTE #iQ16_lg_m=1.
ELSE.
COMPUTE #iQ16_lg=iQ16.
COMPUTE #iQ16_lg_m=0.
END IF.
* Compute classification logits.
COMPUTE Cluster_lg_1=(0)
+(0)*#iQ3_BP3_1_lg
+(0)*#iQ8_A2_lg
+(0)*#iQ8_B2_lg
+(0)*#iQ10_3_lg
+(0)*#iQ12_A2_lg
+(0)*#iQ12_B2_lg
+(0)*#iQ13_2R_lg
+(0)*#iQ15_1_lg
+(0)*#iQ15_2_lg
+(0)*#iQ16_lg
+(0)*#iQ3_BP3_1_lg_m
+(0)*#iQ8_A2_lg_m
+(0)*#iQ8_B2_lg_m
+(0)*#iQ10_3_lg_m
+(0)*#iQ12_A2_lg_m
+(0)*#iQ12_B2_lg_m
+(0)*#iQ13_2R_lg_m
+(0)*#iQ15_1_lg_m
+(0)*#iQ15_2_lg_m
+(0)*#iQ16_lg_m.
COMPUTE Cluster_lg_2=(-57.090559)
+(1.1599731)*#iQ3_BP3_1_lg
+(1.3488498)*#iQ8_A2_lg
```

```
+(0.94924184)*#iQ8_B2_lg
+(0.26975906)*#iQ10_3_lg
+(2.2524608)*#iQ12_A2_lg
+(1.4038307)*#iQ12_B2_lg
+(0.4250671)*#iQ13_2R_lg
+(1.1135756)*#iQ15_1_lg
+(1.2402669)*#iQ15_2_lg
+(0.093326415)*#iQ16_lg
+(7.0541479)*#iQ3_BP3_1_lg_m
+(7.791566)*#iQ8_A2_lg_m
+(4.8926999)*#iQ8_B2_lg_m
+(0.825986)*#iQ10_3_lg_m
+(12.838629)*#iQ12_A2_lg_m
+(6.5892137)*#iQ12_B2_lg_m
+(2.6018108)*#iQ13_2R_lg_m
+(6.5777883)*#iQ15_1_lg_m
+(7.3113828)*#iQ15_2_lg_m
+(0.29635705)*#iQ16_lg_m.
COMPUTE Cluster_lg_3=(21.327359)
+(-0.87425218)*#iQ3_BP3_1_lg
+(-1.2395642)*#iQ8_A2_lg
+(-0.22412313)*#iQ8_B2_lg
+(0.62363575)*#iQ10_3_lg
+(-0.49540106)*#iQ12_A2_lg
+(0.38911929)*#iQ12_B2_lg
+(-0.95219449)*#iQ13_2R_lg
+(-1.0645249)*#iQ15_1_lg
+(-0.88219107)*#iQ15_2_lg
+(0.74357894)*#iQ16_lg
+(-4.5499305)*#iQ3_BP3_1_lg_m
+(-6.0987024)*#iQ8_A2_lg_m
+(-0.97567881)*#iQ8_B2_lg_m
+(2.1415157)*#iQ10_3_lg_m
+(-2.3194692)*#iQ12_A2_lg_m
+(1.5454817)*#iQ12_B2_lg_m
+(-4.7096481)*#iQ13_2R_lg_m
+(-5.2560616)*#iQ15_1_lg_m
+(-4.3671519)*#iQ15_2_lg_m
+(2.718579)*#iQ16_lg_m.
COMPUTE Cluster_lg_4=(36.128207)
+(-1.1721577)*#iQ3_BP3_1_lg
+(-1.6822596)*#iQ8_A2_lg
+(-1.2220468)*#iQ8_B2_lg
+(-0.28109449)*#iQ10_3_lg
+(-1.0944138)*#iQ12_A2_lg
+(-0.72334638)*#iQ12_B2_lg
+(-0.49685685)*#iQ13_2R_lg
+(-0.96474405)*#iQ15_1_lg
+(-0.57073788)*#iQ15_2_lg
+(-0.18535891)*#iQ16_lg
+(-5.8265545)*#iQ3_BP3_1_lg_m
+(-7.9153942)*#iQ8_A2_lg_m
```

```
+(-4.2933735)*#iQ8_B2_lg_m
+(-0.71886554)*#iQ10_3_lg_m
+(-4.714645)*#iQ12_A2_lg_m
+(-2.2063465)*#iQ12_B2_lg_m
+(-2.6937177)*#iQ13_2R_lg_m
+(-4.8213602)*#iQ15_1_lg_m
+(-2.9330606)*#iQ15_2_lg_m
+(-0.54859656)*#iQ16_lg_m.
COMPUTE Cluster_lg_5=(-36.85454)
+(0.26504129)*#iQ3_BP3_1_lg
+(0.68267795)*#iQ8_A2_lg
+(0.89497217)*#iQ8_B2_lg
+(1.3605193)*#iQ10_3_lg
+(1.3903561)*#iQ12_A2_lg
+(1.6634097)*#iQ12_B2_lg
+(-1.6895876)*#iQ13_2R_lg
+(0.15173567)*#iQ15_1_lg
+(0.46097987)*#iQ15_2_lg
+(1.881612)*#iQ16_lg
+(1.5372548)*#iQ3_BP3_1_lg_m
+(3.8218015)*#iQ8_A2_lg_m
+(4.5858945)*#iQ8_B2_lg_m
+(5.681822)*#iQ10_3_lg_m
+(7.5708926)*#iQ12_A2_lg_m
+(8.0832568)*#iQ12_B2_lg_m
+(-7.1033861)*#iQ13_2R_lg_m
+(0.84287684)*#iQ15_1_lg_m
+(2.5919066)*#iQ15_2_lg_m
+(8.2722967)*#iQ16_lg_m.
* Compute odds from logits.
COMPUTE #max_lg=Cluster_lg_1.
DO IF Cluster_lg_2>#max_lg.
COMPUTE #max_lg=Cluster_lg_2.
END IF.
DO IF Cluster_lg_3>#max_lg.
COMPUTE #max_lg=Cluster_lg_3.
END IF.
DO IF Cluster_lg_4>#max_lg.
COMPUTE #max_lg=Cluster_lg_4.
END IF.
DO IF Cluster_lg_5>#max_lg.
COMPUTE #max_lg=Cluster_lg_5.
END IF.
COMPUTE Cluster_lg_1=exp(Cluster_lg_1-#max_lg).
COMPUTE Cluster_lg_2=exp(Cluster_lg_2-#max_lg).
COMPUTE Cluster_lg_3=exp(Cluster_lg_3-#max_lg).
COMPUTE Cluster_lg_4=exp(Cluster_lg_4-#max_lg).
COMPUTE Cluster_lg_5=exp(Cluster_lg_5-#max_lg).
* Compute modal class and probabilities from odds.
COMPUTE #max_lg=Cluster_lg_1.
COMPUTE Cluster_lg_modal=1.
DO IF Cluster_lg_2>#max_lg.
```

```
COMPUTE #max_lg=Cluster_lg_2.
COMPUTE Cluster_lg_modal=2.
END IF.
DO IF Cluster_lg_3>#max_lg.
COMPUTE #max_lg=Cluster_lg_3.
COMPUTE Cluster_lg_modal=3.
END IF.
DO IF Cluster_lg_4>#max_lg.
COMPUTE #max_lg=Cluster_lg_4.
COMPUTE Cluster_lg_modal=4.
END IF.
DO IF Cluster_lg_5>#max_lg.
COMPUTE #max_lg=Cluster_lg_5.
COMPUTE Cluster_lg_modal=5.
END IF.
COMPUTE #sum_lg=Cluster_lg_1+Cluster_lg_2+Cluster_lg_3+Cluster_lg_4+Cluster_lg_5.
COMPUTE Cluster_lg_1=Cluster_lg_1/#sum_lg.
COMPUTE Cluster_lg_2=Cluster_lg_2/#sum_lg.
COMPUTE Cluster_lg_3=Cluster_lg_3/#sum_lg.
COMPUTE Cluster_lg_4=Cluster_lg_4/#sum_lg.
COMPUTE Cluster_lg_5=Cluster_lg_5/#sum_lg.
EXECUTE.
```

In Tabel E.1 staat beschreven de kans op een juiste indeling in segment op basis van het voorspellingsmodel voor bedrijven in elk van de clusters.

**Tabel E.1:** Kans (in procenten) op correcte voorspelling per segment.

| | | **Voorspeld model (basis 10 items)** | | | | | Totaal |
|---|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | **5** | |
| | Overmoedigen | 197 | 15 | 17 | 11 | 3 | 243 |
| | | 81,1% | 6,2% | 7,0% | 4,5% | 1,2% | 100,0% |
| | Voorlopers | 20 | 152 | 0 | 0 | 6 | 178 |
| | | 11,2% | 85,4% | 0,0% | 0,0% | 3,4% | 100,0% |
| | Machtelozen | 11 | 0 | 121 | 4 | 5 | 141 |
| | | 7,8% | 0,0% | 85,8% | 2,8% | 3,5% | 100,0% |
| | Argelozen | 16 | 0 | 13 | 112 | 0 | 141 |
| | | 11,3% | 0,0% | 9,2% | 79,4% | 0,0% | 100,0% |
| | Uitbesteders | 3 | 4 | 4 | 0 | 81 | 92 |
| | | 3,3% | 4,3% | 4,3% | 0,0% | 88,0% | 100,0% |
| **Totaal** | | **247** | **171** | **155** | **127** | **95** | 795 |
| | | **31,1%** | **21,5%** | **19,5%** | **16,0%** | **11,9%** | 100,0% |

## Bijlage F

# Latente klassenanalyse

Op basis van de groepsgesprekken met ondernemers en interne werksessies zijn aanvankelijk 6 hypothetische segmenten en persona's gevormd (zie Bijlagen B en C). De latente klassenanalyse leverde 3 mogelijke segmentatiemodellen op: met 4 segmenten, met 5 segmenten, en met 6 segmenten. Het model met 4 segmenten was nog niet volledig. Dit betekent dat er meer differentiatie mogelijk was. Ook van de 5-segmenten naar de 6-segmenten oplossing levert meer onderscheidingsvermogen op. Maar daarna niet meer: het onderscheiden van 7 segmenten levert niets extra's meer op. Op basis van inhoudelijke en praktische afwegingen met betrekking tot herkenbare en hanteerbare segmenten is gekozen voor het segmentatiemodel met 5 segmenten. Het model met 5 segmenten leverde zinnige en duidelijk onderscheidbare segmenten op. Het onderscheid dat wij dachten te kunnen vinden tussen de veronderstelde segmenten lerenden en de penningmeesters bleek niet aanwezig. De groepen met relatief weinig kennis en vaardigheden zijn ook degenen met relatief weinig resources.

**Defence, Safety & Security**

Kampweg 55
3769 DE  Soesterberg
www.tno.nl

TNO innovation for life