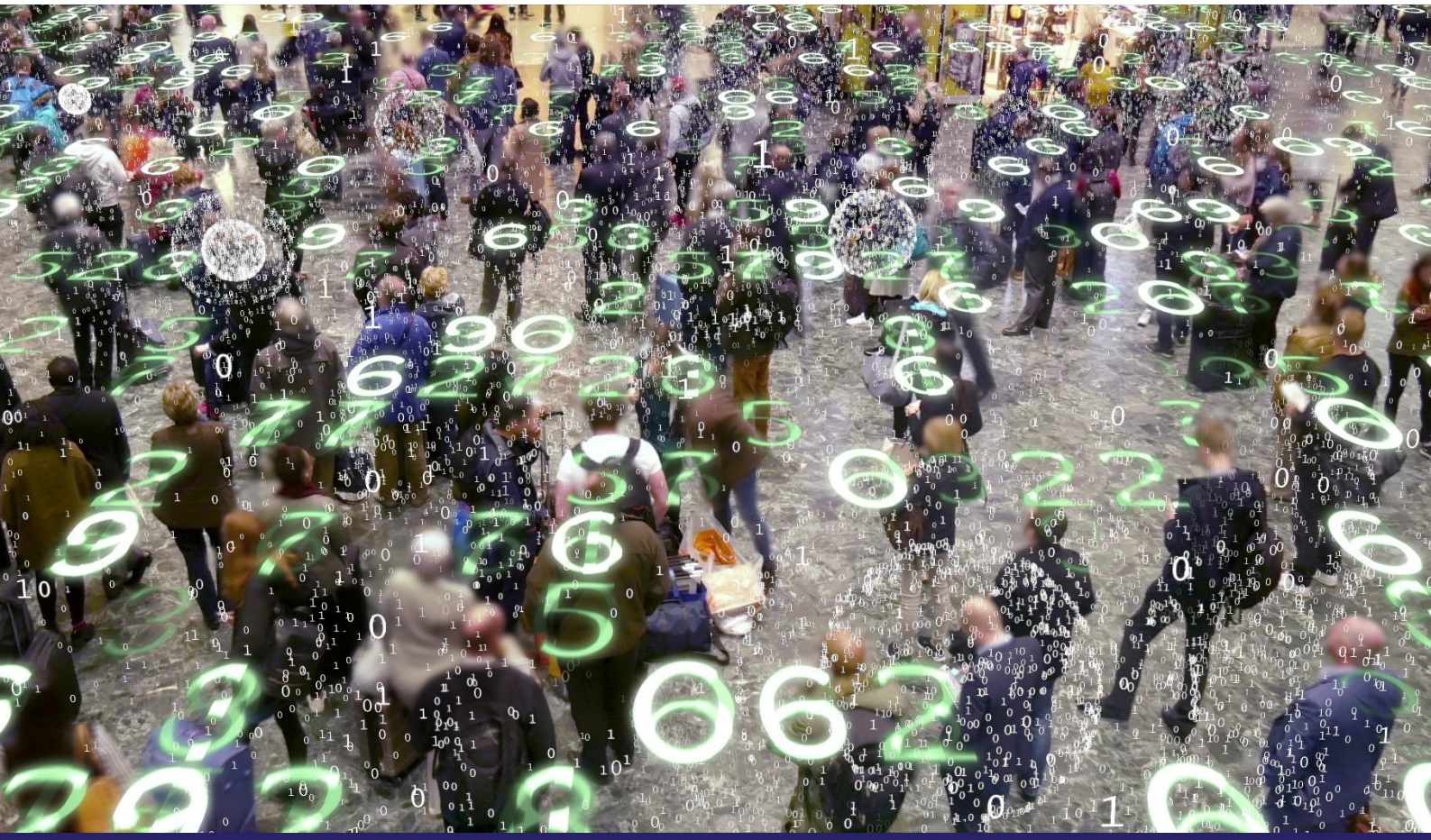
De werking van de Basisscan Cyberweerbaarheid

Een kwalitatief onderzoek naar het gedrag van ondernemers

Auteurs: dr. Maarten Hoekstra, mr. Sipke de Vries, Maike Berkenpas BA, dr. Jurjen Jansen
Onderzoeksgroep Cybersafety



THORBECKE ACADEMIE
NHL STENDEN

Voorwoord

Met veel genoegen leggen wij deze rapportage aan u voor. De onderzoeksgroep Cybersafety van NHL Stenden Hogeschool meent met dit onderzoek een goed inzicht te hebben verkregen in de mate waarin en de wijze waarop de Basisscan Cyberweerbaarheid van het DTC leidt tot gedragsverandering bij ondernemers.

Dank gaat uit naar de bedrijfseigenaren en ICT-beheerders die, vaak nadat wij zij persoonlijk benaderd hadden, hun vertrouwen aan ons schonken. Zij gaven ons het inzicht in hun bedrijfsvoering, zowel in de harde als in de zachte aspecten, waardoor wij het DTC kunnen voorzien van waardevolle informatie over de werking van de basisscan. Bij de totstandkoming van dit onderzoek bleek, meer dan gebruikelijk, het vinden van voldoende respondenten van uiteenlopende aard, omvang en spreiding, een flinke uitdaging. Wij denken ten eerste dat door de coronacrisis veel ondernemers in een overlevingsstand stonden waardoor deelname niet tot de prioriteiten behoorde. Ten tweede vermoeden we dat ondernemers terughoudend zijn geweest in het aanmelden via koppelingen in mails en berichten via sociale media. Wellicht is dat een goed teken!

Door open gesprekken op regelmatige basis met onze opdrachtgever zijn we steeds in staat gebleken om constructieve keuzes te maken over de dilemma's die zich tijdens het onderzoek aandienden. Hiervoor danken wij Jeroen Kasbergen dan ook graag persoonlijk.

Namens de onderzoeksgroep Cybersafety
Dr. Maarten Hoekstra
Projectleider

Leeuwarden, 21 september 2021

Samenvatting

De onderzoeksgroep Cybersafety van NHL Stenden Hogeschool in Leeuwarden, heeft in opdracht van het Digital Trust Center (DTC), in kaart gebracht in hoeverre de Basisscan Cyberweerbaarheid leidt tot gedragsverandering bij ondernemers. In totaal zijn achttien ondernemers, variërend qua omvang, bedrijfstak en geografische ligging, betrokken bij het onderzoek. Respondenten zijn daartoe tweemaal geïnterviewd. Het eerste interview was een zogenoemde nulmeting waarin de uitgangssituatie in kaart werd gebracht. Dit betrof ten eerste de mate waarin men aan de vijf door het DTC onderscheiden basisprincipes, zoals het uitvoeren van software-updates en het reguleren van toegang tot systemen, invulling gaf en ten tweede de achterliggende factoren zoals houdingaspecten en omgevingsinvloeden die daaraan ten grondslag liggen. Het tweede interview werd gehouden nadat de respondent de basisscan had ingevuld en stond in het teken van gedragsverandering en de mogelijke wijzigingen in achterliggende factoren.

Door deze tweetrapsbenadering werd duidelijk dat de basisscan in enige mate leidt tot concrete gedragsverandering van de doelgroep. Uit dit onderzoek blijkt echter dat het goed is te beseffen dat 'de ondernemer' eigenlijk niet bestaat. Er kunnen grofweg drie 'typen' ondernemers worden onderscheiden waardoor beter inzicht ontstaat in de werking van de basisscan. De eerste groep, die de cyberweerbaarheid over het algemeen al goed op orde heeft, ziet de scan als een geschikt middel om zich aan te spiegelen. Het bevestigt vaak hun eigen beeld van de sterkten en zwakten van hun cyberweerbaarheid en zien in de uitkomsten van de basisscan een aanleiding om 'door te pakken'. De tweede groep, veelal kleine ondernemingen, ervaart weinig steun vanuit de overheid. Ondernemers in deze groep laten zich leiden door berichten uit de (sociale) media en vertrouwen in hoge mate op soft- en hardware zoals iOS en Apple. Zij zijn weliswaar alert, maar over het algemeen te druk met dagelijkse werkzaamheden om zich continu met cyberweerbaarheid bezig te houden. Zij ervaren dan ook relatief weinig baat bij de basisscan. De derde groep betreft 'jonge' ondernemers die zelf ook veelal internetdiensten aanbieden. Zij zijn niet alleen kritisch op hun eigen bedrijf maar ook ten opzichte van branchegenoten, leveranciers en overheid leggen zij de lat hoog. Ketenverantwoordelijkheid en certificering zijn belangrijke drijfveren. Ook zij zien de basisscan als een interessant hulpmiddel, maar missen daarin een zekere dynamiek en diepgang.

Wij geven het DTC ten eerste in overweging om meer in te zetten op interactie met de ondernemers. Respondenten geven namelijk aan dat het niet alleen de basisscan is, die aanzet tot gedragsverandering maar vooral ook het gesprek met een deskundige. Ten tweede valt te overwegen om een onderscheid te maken tussen verschillende typen bedrijven. Sommige bedrijven zijn immers vooral geïnteresseerd in de kosten in tijd en geld die een bepaalde maatregel met zich meebrengt, terwijl andere bedrijven juist het overzicht en het globale karakter waarderen. Ten derde geven we mee dat

daadwerkelijke gedragsverandering om een langdurig commitment van zowel de respondent als het DTC vraagt. In die zin valt te overwegen om langdurig te monitoren en juist gedragsverandering in sociale netwerken centraal te stellen en minder uit te gaan van de technisch-inhoudelijke aspecten van cyberweerbaarheid zoals die centraal staan in de huidige basisscan.

Inhoudsopgave

THORBECKE
ACADEMIE

NHL STENDEN

1. Inleiding

1.1 Aanleiding

Vandaag de dag vinden inbreuken op netwerken en computersystemen steeds vaker plaats. Cybercriminelen gaan daarbij ook telkens geraffineerder te werk, terwijl ondernemers in het algemeen en het midden- en kleinbedrijf (hierna: mkb'ers) in het bijzonder niet per definitie de urgentie voelen om in te zetten op cyberweerbaarheid. Mede door toedoen van het coronavirus doen de meeste ondernemers vrijwel alles digitaal. Het belang voor een veilige digitale omgeving wint daarmee aan urgentie.

Dat incidenten binnen de cyberwereld onze maatschappij fors kunnen raken, blijkt uit een aantal recente voorbeelden. Zo ontdekte de gemeente Lochem in 2019 dat haar ICT-systeem gehackt was. Er zijn geen aanwijzingen dat deze hackers daadwerkelijk bij de persoonsgegevens van de Lochemse inwoners zijn gekomen. Wel was de insteek van de hackers duidelijk. Zij wilden data versleutelen om dit in ruil voor losgeld weer vrij te geven. De gemeente is volgens experts door het oog van de naald gekropen. Eveneens in juni van dat jaar werd bij KPN een softwarefout opgemerkt. Door deze fout was het alarmnummer 112 voor burgers onbereikbaar. In december 2019 vond door middel van 'phishing' een serie digitale aanvallen op de Universiteit van Maastricht plaats. Pas nadat de universiteit twee ton 'losgeld' betaalde werden de systemen weer vrijgegeven en waren ze weer bereikbaar voor studenten en personeel.

We zien dat dit soort aanvallen in de afgelopen twee jaar steeds vaker voorkomen en lijken bovendien steeds agressiever te worden[1]. In de afgelopen twee jaar kwamen onder andere nieuwsberichten voorbij over de hack op de gemeente Hof van Twente[2], de zogenoemde 'kaashack'[3] en de aanval op de Mandemakers Groep[4]. In de Nederlands context wijzen brancheorganisaties en verzekeringsmaatschappijen[5] dan ook op de toenemende aantallen aanvallen op mkb-bedrijven. Nederland is overigens niet het enige land dat met deze dreiging te maken heeft, maar komt wereldwijd voor. Recente internationale incidenten betreffen bijvoorbeeld de cyberaanval op de Colonial

---

[1] KRO-NCRV (2021). *Cybersecurity-bedrijven waarschuwen voor agressievere ransomware-aanvallen in Nederland*. Verkregen via: https://pointer.kro-ncrv.nl/cybersecurity-bedrijven-waarschuwen-voor-agressievere-ransomware-aanvallen-in-nederland#gs.5c1oj5

[2] NOS (2020). *Gemeente Hof van Twente platgelegd door hacker*. Verkregen via https://nos.nl/artikel/2359142-gemeente-hof-van-twente-platgelegd-door-hacker.html

[3] NOS (2021) *Oproep-na-kaas-hack-bestempel-voedselvoorziening-als-vitale-infrastructuur*. Verkregen via https://nos.nl/artikel/2376492-oproep-na-kaas-hack-bestempel-voedselvoorziening-als-vitale-infrastructuur

[4] NOS (2021) *Mandemakers-groep-getroffen-door-cyberaanval-hackers-eisen-losgeld*. Verkregen via https://nos.nl/artikel/2387348-mandemakers-groep-getroffen-door-cyberaanval-hackers-eisen-losgeld.

[5] Verbond van Verzekeraars (2021) *Risicoklasseindeling-vergroot-cyberweerbaarheid-mkb*. Verkregen via https://www.verzekeraars.nl/publicaties/actueel/nieuwe-risicoklasseindeling-vergroot-cyberweerbaarheid-mkb

oliepijpleiding in de Verenigde Staten[6] en de wereldwijde problemen die zich voordeden naar aanleiding van de aanval op softwareleverancier Kaseya[7].

In bovenstaande voorbeelden gaat het om relatief grote incidenten. Digitale dreigingen zijn er echter op allerlei niveaus. Denk bijvoorbeeld ook aan phishing, malware en BEC-fraude ('business e-mail compromise', zoals valse factuurfraude en ceo-fraude). Omdat mkb'ers steeds afhankelijker worden van digitale middelen, is het van belang dat zij weerbaar zijn tegen dergelijke dreigingen. Een van de partijen in Nederland die zich bezighoudt om het mkb digitaal weerbaar(der) te maken is het Digital Trust Center (hierna: DTC).

Dit onderzoek is uitgevoerd in opdracht van het DTC. Het doel van onderzoek is de mate waarin de zogeheten Basisscan Cyberweerbaarheid van het DTC hieraan bijdraagt op kwalitatieve wijze te evalueren. Het DTC en de basisscan worden nader toegelicht in paragraaf 1.2. Daarna volgen de werkwijze van de basisscan (paragraaf 1.3) en de relevantie van dit onderzoek (paragraaf 1.4). In paragraaf 1.5 volgen de doelstelling, vraagstelling en methodologie die aan deze studie ten grondslag liggen.

1.2 Cyberweerbaarheid en het DTC

Ondernemers zijn in toenemende mate afhankelijk van digitale toepassingen en middelen. Ze gebruiken deze voor verschillende doeleinden, zoals het verkopen van goederen, het verzamelen en opslaan van gegevens, het communiceren met klanten en het overmaken van geld. Hoewel grotere organisaties zich steeds beter wapenen tegen digitale dreigingen, lijken zelfstandigen zonder personeel (hierna: zzp'ers) en mkb'ers achter te blijven. Omdat deze bedrijven steeds vaker doelwit zijn van cyberaanvallen (o.a. Leiden, Appelman, Ham, & Ferwerda, 2014; Jansen, Veenstra, Zuurveen, & Stol, 2016; Vasileiou & Furnell, 2019), wordt het weerbaar(der) maken van deze doelgroepen cruciaal geacht; ook gelet op de belangrijke positie die het mkb inneemt in de Nederlandse economie. We weten op basis van onderzoek van Notté en Slot (2017) dat een op de vijf mkb'ers in een jaar tijd slachtoffer was van uiteenlopende vormen van cybercrime.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV, 2021) geeft aan dat digitale weerbaarheid in essentie gaat over het vermogen om digitale risico's in een voldoende mate te beheersen. Dat is ook gelijk waar de crux ligt: de digitale weerbaarheid is (nog) niet overal op orde, waardoor ondernemers kwetsbaar zijn voor incidenten (o.a. Notté & Slot, 2017; Furnell & Vasileiou, 2019; Stol, 2015). De NCTV (2021)

---

[6] Bloomberg (2021). *Hackers-breached-colonial-pipeline-using-compromised-password*. Verkregen via https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[7] The Guardian (2021). *Kaseya-ransomware-hackers-attack*. Verkregen via https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-hackers-attack

ziet dat slachtofferschap vooral voorkomt wanneer organisaties onvoldoende basismaatregelen hebben getroffen om incidenten te voorkomen.

Cyberweerbaarheid ofwel digitale weerbaarheid is een verzamelnaam voor allerlei verschillende middelen en manieren om cybercriminaliteit tegen te gaan en de cybersecurity te verhogen (zie o.a. Rothrock, 2018). In de literatuur worden vier vaardigheden gekoppeld aan weerbaarheid (o.a. Hollnagel, 2015; Matzenberger, 2013; 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 (indien 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 soms ook wel aangeduid met de term 'veerkracht'.

Hoewel digitale weerbaarheid gaat om het managen van risico's in de breedste zin van het woord (Jansen, 2018), beperkt dit onderzoek zich tot preventie van digitale risico's, omdat de basisscan daarop gericht is. Vermeld dient te worden dat preventie niet (alleen) gaat om het voorkomen van incidenten, maar ook om het inperken van de mogelijk impact ervan. Er wordt in dit onderzoek vooral gekeken naar de gedragsmatige aspecten van digitale weerbaarheid. Immers, onveilig onlinegedrag kan leiden tot een verhoogde kans op slachtofferschap (Jansen, 2018). Anders gesteld, veilig onlinegedrag is een belangrijke voorwaarde voor veilig digitaal ondernemen.

Om het hoofd te kunnen bieden aan cybercriminaliteit is in 2018 het DTC opgericht[8]. Het DTC maakt onderdeel uit van het ministerie van Economische Zaken en Klimaat. De oprichting gebeurde onder meer naar aanleiding van een motie van twee Kamerleden en op advies van de Cyber Security Raad. Het advies van deze Raad was om een centrum op te richten voor bedrijven uit de niet-vitale sectoren, zodat ook zij over cyberweerbaarheid geadviseerd en geïnformeerd zouden kunnen worden door een Rijksinstelling. De vitale sectoren werden namelijk al ondersteund door het Nationaal Cyber Security Centrum (NCSC). De missie van het DTC is om 1,8 miljoen Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberbedreigingen. Dat doet het DTC bijvoorbeeld door samenwerkingsverbanden (cyberweerbaarheidsnetwerken) te stimuleren: bedrijven die groepen ondernemers helpen met veilig digitaal ondernemen. Het DTC zet in op een zogeheten *Digital Trust Community*, een gesloten omgeving waar bedrijven relevante informatie kunnen delen en uitwisselen. Het DTC biedt, op een laagdrempelige manier, kennis, informatie en advies aan ondernemers aan.

[8] De informatie uit deze alinea is ontleend aan de website van het Digital Trust Center: https://www.digitaltrustcenter.nl/over-het-digital-trust-center

Daarnaast biedt het DTC de Basisscan Cyberweerbaarheid aan. Deze scan is een hulpmiddel voor ondernemers om te inventariseren hoe de onderneming scoort op het gebied van veilig digitaal ondernemen. Wanneer een ondernemer de scan doorloopt, komt hij[9], aan de hand van 25 stellingen, te weten waar de onderneming in digitaal opzicht staat. Het doel van de basisscan is om de ondernemer verder te helpen bij het op orde kan krijgen van de basisbeginselen van cyberweerbaarheid. De ondernemer krijgt na het invullen van de basisscan vervolgens een rapportage met adviezen over stappen die hij zelf kan zetten om de digitale weerbaarheid van de onderneming naar een hoger niveau te tillen. De scan en de daaruit voortvloeiende adviezen zijn gebaseerd op vijf, door het DTC opgestelde, basisprincipes van digitale weerbaarheid: inventariseer kwetsbaarheden, kies veilige instellingen, voer updates uit, beperk toegang en voorkom virussen en andere malware. Deze principes worden in de volgende paragraaf nader toegelicht.

1.3 Opzet en gebruik van de basisscan

Om een duidelijker beeld te geven hoe de basisscan functioneert, worden de vijf basisprincipes hieronder beschreven[10].

Basisprincipe 1: inventariseer kwetsbaarheden

Bij het basisprincipe 'inventariseer kwetsbaarheden' bepaalt de ondernemer hoe groot de kans is dat een dreiging optreedt en wat de eventuele impact van die dreiging is. Hierbij wordt gekeken naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Dit zijn drie belangrijke beveiligingseigenschappen van digitale 'assets' (Hartel & Herman, 2012). Beschikbaarheid kijkt naar of informatie wel of niet beschikbaar en toegankelijk is. Integriteit verwijst naar de juistheid, actualiteit en volledigheid van informatie. Vertrouwelijkheid kijkt naar de gevolgen als informatie eventueel naar buiten lekt. Door de kwetsbaarheden te inventariseren kan de weerbaarheid van ondernemers groter worden. Bovendien, als een incident zich voordoet, kunnen de hoofd- en bijzaken beter worden onderscheiden waardoor het incident eerder kan worden opgelost.

Basisprincipe 2: kies veilige instellingen

Bij het basisprincipe 'veilige instellingen' worden ondernemers gestimuleerd om verder te kijken dan de standaardinstellingen die leveranciers voor hun apparatuur en software kiezen. Door slechts standaardinstellingen te gebruiken, is de kans op cyberdreigingen groter dan als de instellingen door de ondernemer worden aangepast. Denk bijvoorbeeld aan standaard wachtwoorden op routers. Het DTC adviseert om de

[9] Deze rapportage hanteert omwille van de leesbaarheid consequent de 'Hij-vorm' terwijl evengoed de 'Zij-vorm' van toepassing is.

[10] Deze paragraaf is gebaseerd op de website van het Digital Trust Center: https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

instellingen te controleren en ze aan te passen voordat ze worden aangesloten op het internet. Hieronder valt ook het uitzetten van functies en diensten die niet nodig zijn maar wel aanstaan. Daarnaast adviseert het DTC het gebruik van sterke, veilige en uiteenlopende wachtwoorden en extra beveiliging voor gevoelige zaken als bankzaken met behulp van een tweestapsverificatie. Tweestapsverificatie houdt in dat wordt ingelogd met veelal een code (zoals een wachtwoord) en een tweede, aanvullende stap. Deze tweede stap is vaak een tijdelijke sleutel die wordt verstuurd via sms of mail, of wordt gegenereerd met een token. Tot slot raadt het DTC aan om gebruik te maken van firewalls. Met firewalls kan worden gecontroleerd en beheerd welke verbindingen er zijn tussen het eigen netwerk en andere netwerken.

Basisprincipe 3: voer updates uit

Het derde basisprincipe van de basisscan is het 'uitvoeren van updates'. Het DTC raadt aan om altijd de meest recente beveiligingsupdates te installeren. Up-to-date software is van belang voor alle apparaten die met het internet verbonden zijn. Vaak zijn de updates beschikbaar omdat de producenten van de apparatuur en software deze aan de eindgebruikers aanbieden. Dit basisprincipe wordt genoemd omdat gedateerde software gemakkelijker toegankelijk is voor cybercriminelen. Door systemen up-to-date te houden, hebben ondernemers bijvoorbeeld minder kans om slachtoffer te worden van virussen of via bekende lekken die door derden worden misbruikt.

Basisprincipe 4: beperk toegang

Het vierde basisprincipe is 'toegang beperken'. Ondernemers moeten regelen dat personen binnen of buiten de onderneming alleen toegang hebben tot systemen als deze passen bij de werkzaamheden en de tijdsduur waarbinnen de werkzaamheden plaatsvinden. Uitgebreidere autorisaties moeten alleen verstrekt worden als deze echt nodig zijn. Door dit op deze manier vorm te geven, voorkomen ondernemers dat personen binnen en/of buiten hun bedrijf toegang hebben tot gegevens die zij niet nodig hebben. In deze context wordt gesproken over 'netwerksegmentatie'[11] en 'least-privilege'[12].

Basisprincipe 5: voorkom virussen en andere malware

Het laatste principe van de basisscan is het bevorderen van de beveiliging tegen 'virussen en andere malware'. De ondernemer moeten zich bijvoorbeeld bewust zijn van de risico's die gepaard gaan met het gebruik van usb-sticks. Daarnaast wordt een

[11] Netwerksegmentatie houdt in dat een netwerk in meerdere zones of groepen wordt verdeeld. Hiermee kan worden voorkomen dat een virus of aanvaller zich eenvoudig in het gehele netwerk kan verspreiden (NCSC.nl, z.d.).

[12] Least privilege kan vrij worden vertaald als het toebedelen van minimale rechten. Dit geldt zowel voor accounts als voor fysieke ruimten. Dit principe gaat ervan uit dat mensen alleen toegang tot data en systemen krijgen die nodig zijn voor het uitvoeren van hun taak. Hiermee kan worden voorkomen dat een indringer beperkte activiteiten kan uitvoeren (NCSC.nl, z.d.).

betaalde virusscanner geadviseerd. Ook wordt gewezen op het bewust downloaden van applicaties, zodat de ondernemer op de hoogte is van wat hij installeert.

1.4 Relevantie onderzoek en vraagstelling

Dit onderzoek is gericht op de doorwerking van de basisscan in termen van gedragsverandering. Een eventuele verandering in gedrag wordt inzichtelijk gemaakt door de mate waarin de vijf basisprincipes (beter) worden nageleefd. De focus van dit onderzoek ligt op de stimulerende en beperkende factoren ten aanzien van de vijf basisprincipes. Als hoofdvraag is geformuleerd: *In hoeverre leidt de 'Basisscan Cyberweerbaarheid' tot gedragsverandering bij ondernemers?*

Om de hoofdvraag te kunnen beantwoorden zijn onderstaande deelvragen geformuleerd:

1. Hoe kan gedragsverandering inzichtelijk worden gemaakt?
2. Welke factoren liggen aan gedrag en gedragsverandering ten grondslag?
3. In welke gedragsfase bevinden ondernemers zich voor en na het maken van de basisscan?
4. Welke factoren zijn in de praktijk bepalend voor mogelijke gedragsverandering?
5. Welke aanbevelingen kunnen worden gedaan om de effectiviteit (in termen van gedragsverandering) van de basisscan te vergroten?

De eerste twee deelvragen zijn theoretisch van aard terwijl de deelvragen 3, 4 en 5 een empirisch karakter hebben. Het DTC wil graag 1,8 miljoen bedrijven verder helpen bij hun digitale weerbaarheid; de basisscan is daarvoor een belangrijk instrument. Dit onderzoek kan daarom ook getypeerd worden als een bijzonder type beleidsevaluatie.

1.5 Methoden en respons

Het onderzoek kenmerkt zich op hoofdlijnen door twee methoden die gezamenlijk tot een oordeel leiden over de mate waarin de basisscan leidt tot gedragsverandering bij ondernemers, te weten een literatuuronderzoek en interviews. Beide methoden worden kort toegelicht.

Voor dit kwalitatieve onderzoek is een beknopte literatuurstudie verricht, om te bepalen welke gedragsfasen onderscheiden kunnen worden en welke mogelijke factoren verklarend zijn (Deelvragen 1 en 2). In dit onderzoek wordt een vijftal fasen van gedragsverandering gebruikt om inzichtelijk te maken of en in hoeverre ondernemers hun gedrag hebben aangepast. (Ontleend aan Prochaska & Diclemente, 1993; Rijksoverheid, 2011). De wetenschappelijke literatuur kent meerdere modellen (o.a. Bandura & McClelland, 1977; Deci & Ryan, 1985) die gebruikt kunnen worden om gedragsverandering te onderzoeken. De combinatie van het ASE-model (zie o.a. De Vries, Mudde, Dijkstra, & Willemsen, 1998) en het COM-B model (o.a. Hendriks, Kremers, Wierix & Jansen, 2017) biedt dit onderzoek de nodige handvatten. Deze modellen zijn namelijk eerder gebruikt voor onderzoeken waarbij de rijksoverheid gedragsverandering

onderzocht (De Ridder & Lechner, 2004). Uit de combinatie van modellen zijn op hoofdlijnen drie factoren gedistilleerd die in dit onderzoek zijn toegepast. Dit zijn: houding, omgeving en (zelf)effectiviteit. Voor een nadere toelichting wordt verwezen naar hoofdstuk 2.

In totaal zijn achttien ondernemers tweemaal (online via beeldbellen) geïnterviewd om de werking van de basisscan goed in beeld te brengen. Deelname aan de (gestructureerde) interviews was vrijwillig en op anonieme basis. Het eerste interview betrof een nulmeting om te bepalen in welke fase de onderneming zich op dat moment bevond. Deze interviews zijn afgenomen tussen december 2020 en juni 2021. De interviews duurden gemiddeld zestig minuten. De interviews zijn vastgelegd volgens protocol en vervolgens uitgewerkt in verslagvorm.

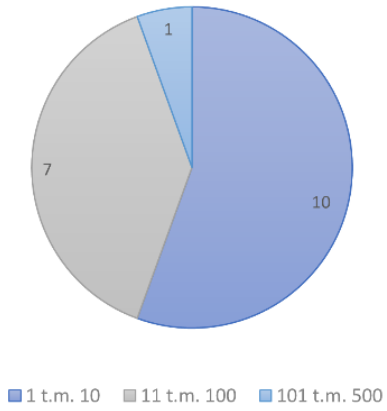
Na de nulmeting werd gevraagd aan de ondernemers of zij de basisscan wilden invullen. Nadat ondernemers de basisscan maakten, werd middels een tweede interview onderzocht of zij hun gedrag aanpasten en dus nieuwe maatregelen troffen. Deze interviewronde vond plaats tussen januari 2021 en juni 2021. Deze interviews duurden gemiddeld dertig minuten. De tijd die tussen het eerste en het tweede interview zat, betrof gemiddeld drie weken. De wijze van afname, uitwerking en verwerking is identiek aan de procedures van de eerste interviews. De verslagen van de interviews zijn ter verificatie aan de respondent voorgelegd.

Zowel het eerste als het tweede interview zijn ontworpen aan de hand van de belangrijkste elementen uit de theorie (zie hoofdstuk 2) en middels een peerreview (tweemaal door sr. Onderzoeker van de onderzoeksgroep Cybersafety) getest en aangepast (vergroten gebruiksvriendelijkheid voor respondent) om de praktische bruikbaarheid te waarborgen. Voor beide interviews werd een interviewprotocol aangehouden, zie bijlagen I en II.

In totaal zijn dus achttien respondenten betrokken in het onderzoek. Deze zijn via drie verschillende kanalen benaderd:

1. Een (herhaald) LinkedIn-bericht vanuit de onderzoeksgroep Cybersafety van NHL Stenden Hogeschool. De respons (vier aanmeldingen) hierop was beperkt. Daarom is in overleg met de opdrachtgever overgegaan op de volgende stap.
2. Een elektronische mailing (ook herhaald) naar een groep van 2.500 potentiële respondenten (met herleidbare contactgegevens afkomstig uit een bestand van 8.000 willekeurig door de Kamer van Koophandel geselecteerde adressen). Slechts één bedrijf meldde zich daadwerkelijk aan via deze weg. In deze fase werd een verwerkersoverkomst tussen opdrachtgever en opdrachtnemer opgesteld. Vanwege de geringe respons werd, wederom in overleg met de opdrachtgever gekozen voor de volgende stap, te weten:
3. Directe benadering van het netwerk door medewerkers van de onderzoeksgroep Cybersafety. Deze stap, die tevens een herijking van het streefaantal inhield, bleek het meest succesvol en leverde dertien nieuwe respondenten op.

Met deze getrapte benadering is een divers palet aan bedrijven in het onderzoek betrokken. Zowel bedrijven die al vergevorderd zijn op het gebied van cyberweerbaarheid, als bedrijven die zich nog in het beginstadium bevinden, maken deel uit van dit onderzoek. Het merendeel (al spreken we hier van geringe aantallen) van de respondenten (n = 10) kan als kleinbedrijf (≤ 10 medewerkers) worden omschreven terwijl een minderheid (n = 8) behoort tot de middelgrote ondernemingen (11-500 medewerkers), zie figuur 1.1. Eén specifiek bedrijf springt er qua omvang uit met een bedrijfsomvang van ongeveer vijfhonderd medewerkers. De andere middelgrote bedrijven hadden niet meer dan honderd medewerkers in dienst. De wijze van werving van respondenten kan worden omschreven als een combinatie van een quotumbenadering (afgesproken aantal zoals overeengekomen met de opdrachtgever) en een 'convenience-benadering'. Dat laatste betreft het gegeven dat een deel van de respondenten uit het beschikbare netwerk van de onderzoekers komt. Daarnaast is een beperkt aantal respondenten geworven via de initiële mailingen hetgeen een meer 'random karakter' heeft. Gefocust wordt op dieperliggende factoren voor een goed begrip van de werking van de basisscan. Het verhaal ofwel narratief (zie o.a. Sools, 2011) van deze ondernemers staat centraal.



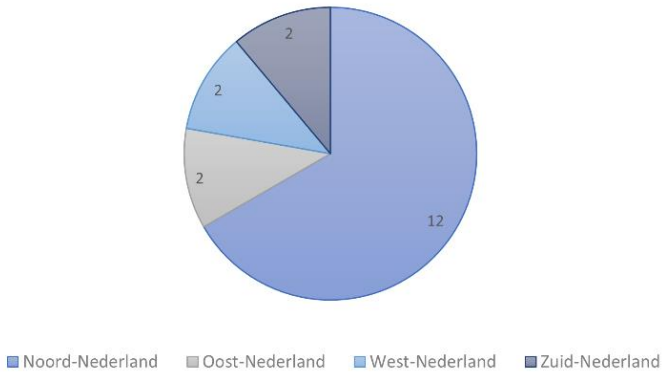
Figuur 1.1: Bedrijfsgrootte

We zien dat de respons een brede spreiding heeft over type werkzaamheden, zie tabel 1.1. De indeling naar type werkzaamheden betreft de belangrijkste bedrijfsactiviteit zoals de respondent die zelf heeft aangegeven. Daarbij hebben de onderzoekers de vertaling gemaakt naar de standaardindeling van het Centraal Bureau voor de Statistiek (CBS).

Respondent	Type werkzaamheden	Indeling CBS
A	Machinebouw	Landbouw, bosbouw en visserij
B	Softwareontwikkelaar	Informatie en communicatie
C	Automatische industrialisering	Informatie en communicatie
D	Installatietechniek	Bouwnijverheid
E	Groothandel landbouwmaterialen	Zakelijke dienstverlening
F	Aardappelteelt	Landbouw, bosbouw en visserij
G	Onderzoek	Zakelijke dienstverlening
H	Reclame	Informatie en communicatie
I	Projectadvies	Zakelijke dienstverlening
J	Webdevelopment	Informatie en communicatie
K	Watersport	Cultuur en recreatie
L	Marketing	Informatie en communicatie
M	Interieurbouw	Bouwnijverheid
N	Technische groothandel	Zakelijke dienstverlening
O	Sportlessen	Cultuur en recreatie
P	Inrichting bedrijven	Bouwnijverheid
Q	Arbeidsveiligheid	Zakelijke dienstverlening
R	Bewindvoering	Zakelijke dienstverlening

Tabel 1.1: Werkzaamheden en indeling CBS van Respondenten

Twaalf respondenten zijn afkomstig uit Noord-Nederland, zie figuur 1.2. De andere drie gebiedsdelen van het land zijn vertegenwoordigd met elk twee bedrijven.



Figuur 1.2 Respons naar geografische verspreiding

1.6 Leeswijzer

In het volgende hoofdstuk (hoofdstuk 2) staat het theoretisch raamwerk voor dit onderzoek centraal. Daarin wordt vooral ingegaan op de modellen (ASE en COM-B) die gebruikt worden om gedragsverandering te verklaren en om gedragsfasen te kunnen onderscheiden. Hoofdstuk 2 sluit af met een schematische weergave van de belangrijkste elementen van de theorie. Dit conceptuele model vormt de basis voor het

onderzoeksontwerp, de interviews en de rapportage. Hoofdstuk 3 geeft de resultaten van het empirische onderzoek weer. Ten eerste wordt een overzicht gegeven van 'scores' van de respondenten ten aanzien van hun 'gedrag' en de waardering die zij hebben voor de basisscan. Vervolgens wordt per bedrijf ingegaan op de factoren die het gedrag en de gedragsverandering bepalen. Deze achttien 'gevalsstudies' vormen het empirische hart van dit onderzoek omdat daarmee duidelijk wordt gemaakt in hoeverre en op welke wijze de basisscan van invloed is geweest op het al dan niet veranderen van gedrag. Hoofdstuk 4 behandelt de conclusies ten aanzien van de werking de basisscan, enkele beperkingen van dit onderzoek, een drietal concrete aanbevelingen voor het DTC en een beknopte slotbeschouwing. Dit slothoofdstuk laat zien dat bedrijven zich in uiteenlopende stadia van bewustwording bevinden en welke inzichten dat biedt ten aanzien van de effectiviteit van de basisscan in termen van gedragsverandering.

2. Fasen van gedrag en achterliggende factoren

2.1 Inleiding

De kern van het onderzoek betreft gedragsverandering bij ondernemers op het gebied van cyberweerbaarheid ten gevolge van het uitvoeren van de basisscan. De basisscan gaat in op een vijftal basisprincipes van veilig digitaal ondernemen en laat zien waar ondernemers alert op moeten zijn (zie paragraaf 1.3). De bedoeling van de scan is dat de ondernemer zich bewust wordt van de digitale kwetsbaarheden van zijn bedrijf en op basis daarvan de nodige maatregelen neemt om deze op te heffen of te verminderen. De vraagstukken die in dit hoofdstuk beantwoord worden zijn hoe gedragsverandering vanuit theoretisch perspectief inzichtelijk gemaakt kan worden (paragraaf 2.2) en welke factoren aan gedrag ten grondslag liggen (paragraaf 2.3). Paragraaf 2.4 belicht het conceptuele model, voortvloeiend uit de gemaakte keuzen voor het onderzoek.

2.2 Fasen van gedrag

In dit onderzoek wordt een vijftal fasen van gedragsverandering gebruikt om inzichtelijk te maken of en in hoeverre ondernemers hun gedrag hebben aangepast. Ontleend aan Prochaska en Diclemente (1993) en Rijksoverheid (2011) is voor vijf fasen gekozen vanwege de in de praktijk bewezen waarde en herkenbaarheid.

1. *Pre-contemplatiefase*; de fase waarin men niet de intentie heeft om gedrag te veranderen. Grofweg vallen hier twee typen ondernemers onder. 1) De onwetenden: de mensen die zich niet bewust zijn van een bepaalde gedraging of die niet hebben nagedacht over de voordelen van in dit geval een betere cyberweerbaarheid; men weet gewoon niet beter. 2) De onwillenden: mensen die van de materie op de hoogte zijn, maar hun gedrag niet willen veranderen. Dit kan door demoralisering komen; eerdere pogingen hebben niet gebracht wat men gehoopt had, of doordat men het simpelweg niet nodig acht om het gedrag te veranderen.

2. *Contemplatiefase*; de fase waarin men gedragsverandering overweegt, maar nog niet tot concrete actie overgaat. De intentie om het gedrag te veranderen is er, maar er zit nog een verschil tussen de bestaande en de gewenste situatie. De voor- en nadelen van de actie(s) worden in deze fase overwogen. In dit geval zou een afweging kunnen zijn of het de moeite waard is om de cyberweerbaarheid te vergroten.

3. *Preparatiefase*; de fase waarin men voorbereidingen treft maar nog niet tot concrete actie overgaat. Vaak zijn in deze fase al veranderingen waarneembaar. Men heeft bijvoorbeeld al informatie opgevraagd over verbeteringen in de cyberweerbaarheid, maar komt er nog niet aan toe.

4. *Actiefase*; de fase waarin men daadwerkelijk aan de slag gaat met de aspecten die uit bepaalde inzichten voortkomen. Bij dergelijke ondernemers vindt een concrete gedragsverandering plaats.

5. *Behoudfase*; de fase waarin men de inspanning beloond ziet en de goede elementen graag wil behouden. Een ondernemer ziet duidelijk de voordelen van zijn eigen handelen in omdat dit leidt tot een adequaat niveau van cyberweerbaarheid.

De vraag, die in de volgende paragraaf aan de orde komt, is welke factoren mogelijk het gedrag en de gedragsfase bepalen.

2.3 Factoren van gedragsverandering

De wetenschappelijke literatuur kent talrijke modellen (o.a. Bandura & McClelland, 1977; Deci & Ryan, 1985) die gebruikt kunnen worden om gedragsverandering te onderzoeken. De combinatie van het ASE-model (zie o.a. De Vries, Mudde, Dijkstra, & Willemsen, 1998) en het COM-B model (o.a. Hendriks, Kremers, Wierix, & Jansen, 2017) biedt dit onderzoek de nodige handvatten. Deze modellen zijn namelijk eerder gebruikt voor onderzoeken waarbij de rijksoverheid gedragsverandering onderzocht en evalueerde rook- en bewegingsbeleid (De Ridder & Lechner, 2004). Uit de combinatie van modellen zijn op hoofdlijnen drie factoren gedistilleerd die in dit onderzoek zijn toegepast, namelijk: houding, omgeving en (zelf)effectiviteit. Houding betreft de afweging van voor- en nadelen, baten en kosten voor de ondernemer om het gedrag te (willen) veranderen. Bij omgeving gaat het om stimulansen en belemmeringen door factoren en actoren uit de omgeving voor gedragsverandering. Zelfeffectiviteit heeft betrekking op de inschatting van eigen vaardigheden. In de volgende sub-paragrafen wordt een toelichting gegeven over het ASE-model en het COM-B model. De wijze waarop deze worden toegepast in het onderzoek is weergegeven in het tweedelige conceptuele model in paragraaf 2.4.

2.3.1 Het ASE-model

Het ASE-model is een acroniem voor Attitude, Sociale invloed & Eigen effectiviteitsmodel en vormt een fundament van dit onderzoek.[13] Deze drie factoren beïnvloeden de intentie om over te gaan tot bepaald gedrag. Intentie wordt volgens dit model gezien als een belangrijke voorspeller voor daadwerkelijk gedrag. Het ASE-model is gebaseerd op de Theory of Planned Behavior (Ajzen, 1991) en de Social Learning Theory (Bandura, 1986). Met behulp van dit model kan gedrag worden verklaard en geanalyseerd. Ook kunnen antwoorden worden gevonden op hoe gedrag beïnvloed kan worden. Het ASE-model kijkt naar verschillende oorzaken voor gedragsverandering. Enerzijds is dat de zelfeffectiviteit van de ondernemer. Anderzijds worden ook externe factoren onderzocht, zoals bijvoorbeeld de invloed van overheidscampagnes op het onderwerp.

[13] In dit onderzoek spreken we over 'zelfeffectiviteit' in plaats van 'eigen effectiviteit' vanwege de aansluiting bij het taalgebruik van de doelgroep.

Attitude

Bij attitude wordt gekeken naar de positieve of negatieve gevoelens ten opzichte van een bepaalde gedraging (Fishbein & Ajzen, 1975). Daarbij geldt hoe positiever de houding hoe waarschijnlijker dat men overgaat tot bepaald gedrag. In deze context betreft attitude de houding van de bedrijfseigenaar of de directie in termen van afweging van de voor- en nadelen van gedragsverandering (Rijksoverheid, 2011). De voor- en nadelen worden gevormd door de verschillende opvattingen die heersen over een bepaalde gedraging (Rotmans, 2005). Een voordeel van gedragsverandering in dit onderzoek is dat ondernemers doorkrijgen dat zij beter beschermd kunnen zijn tegen bijvoorbeeld 'DDoS-aanvallen'.[14] Of dat ze een beter imago krijgen als de cyberweerbaarheid op een hoger niveau staat. Nadelen voor het veranderen van de aanpak rondom cyberweerbaarheid kunnen zijn dat dit de ondernemer (meer) tijd en geld kost. Of dat het te ingewikkeld is. De ondernemer weegt deze factoren tegen elkaar af en bepaalt zo waar hij staat.

Sociale invloed

Soms zijn andere mensen bepalend voor het gedrag van de ondernemer. In dit onderzoek kunnen dit bijvoorbeeld collega-ondernemers zijn, die belangrijk of een voorbeeld zijn voor de respondent. Hierbij geldt dat wanneer de sociale omgeving verwacht dat men het doelgedrag uitoefent en/of dat gedrag zelf uitoefent, men eerder geneigd is om dat ook te doen (Fishbein & Ajzen, 2010). Ook gedragsveranderingscampagnes spelen een rol in de sociale omgeving. Dit blijkt bijvoorbeeld uit een onderzoek uitgevoerd naar onlinepesten, waarbij de conclusie is dat mensen vooral moeten worden gewezen om zelf in actie te komen wanneer zij pesten zien (Lee & Wu, 2018). De sociale omgeving bepaalt voor een groot deel hoe men ergens tegen aan kijkt. Sociale invloed kan worden opgesplitst in drie onderdelen (De Ridder & Lechner, 2004):

1. De sociale norm: ofwel het oordeel dat anderen over het gedrag van de ondernemer hebben;
2. De directe sociale steun: de mate waarin het gedrag van de ondernemer, op het gebied van cyberweerbaarheid, door anderen wordt gestimuleerd;
3. Model-leren: de mate waarin de omgeving van de ondernemer inzet op cyberweerbaarheid, zodat dit als voorbeeldgedrag voor de ondernemer kan zijn.

Zelfeffectiviteit

Het derde onderdeel is zelfeffectiviteit. Dit betreft de eigen inschatting van vaardigheden of het vermogen om een bepaalde doelgedraging uit te voeren. Hierbij geldt dat personen die menen bepaalde gedragingen te kunnen uitvoeren, eerder

[14] Een *distributed denial-of-service*-aanval of DDoS-aanval is een opzettelijke aanval waarbij enorme hoeveelheden data worden verzonden om de toegang van de beoogde gebruikers tot systemen, netwerken of diensten te blokkeren (Van der Hulst & Neve, 2008).

geneigd zijn om dat te doen dan personen die minder vertrouwen in zichzelf hebben (Bandura, 1977). In deze context wordt onderzocht in welke mate men zichzelf in staat acht invloed uit te oefenen op cyberweerbaarheid. In de sociaal-cognitieve wetenschap wordt zelfeffectiviteit ook wel het belangrijkste mechanisme genoemd dat invloed heeft op het gedrag van iemand (Lee & Wu, 2018; Rotmans, 2005). Ook in studies naar informatiebeveiligingsgedrag komt zelfeffectiviteit naar voren als een van de factoren die sterk samenhangt met gedragsintentie (zie Jansen, 2018).

Barrières en vaardigheden

De barrières en vaardigheden refereren aan de (on)mogelijkheden die de ondernemer heeft om zijn voornemen om te zetten in daadwerkelijk gedrag. Hierbij gaan barrières over externe (on)mogelijkheden, zoals regelgeving, en vaardigheden over gedragsmogelijkheden, zoals lerend vermogen. Het model bevat ten slotte nog een feedback-loop, wat het een dynamisch model maakt (Rotmans, 2005). Als de ondernemer in kwestie in de tweede meting ander gedrag vertoont dan in de eerste meting, veranderen de concepten uit het model. Zodoende kan het ASE-model van toepassing zijn op zowel de eerste als de tweede meting.

2.3.2 Het COM-B model

Zoals uitgelegd in de vorige sectie is gedragsintentie een belangrijke uitkomstvariabele van het ASE-model. Hoewel het verband tussen intentie en feitelijk gedrag sterk, consistent en theoretisch gefundeerd is (Anderson & Agarwal, 2010), is er vaak enige discrepantie tussen wat mensen aangeven te gaan doen en wat mensen daadwerkelijk doen (Workman, Bommer, & Straub, 2008). Dit wordt ook wel de *intention-behaviour gap* genoemd. Dit geldt ook voor cybergedrag (Crossler, Johnston, Lowry, e.a., 2013; Jansen, 2018). Met behulp van het tweede model dat een centrale plek inneemt in het onderzoek, het COM-B model, nemen we een aantal aanvullende factoren in ogenschouw. Het COM-B model is, net als het ASE-model, bedoeld om gedrag te analyseren.

Het COM-B model staat voor: Capability, Opportunity, Motivation en Behaviour. In dit model is gedrag (behaviour) het resultaat van de samenhang tussen capaciteit, gelegenheid en motivatie, en de onderlinge interactie tussen deze componenten (Michie, Van Stralen, & West, 2011). Op die manier wordt gedrag verklaard vanuit meerdere invalshoeken. Er ontstaat zo een breder beeld van het gedrag van iemand en als vervolg kunnen passende acties worden ondernomen om het gedrag van diegene te veranderen of te faciliteren. Samengevat kunnen de drie componenten als volgt worden omschreven:

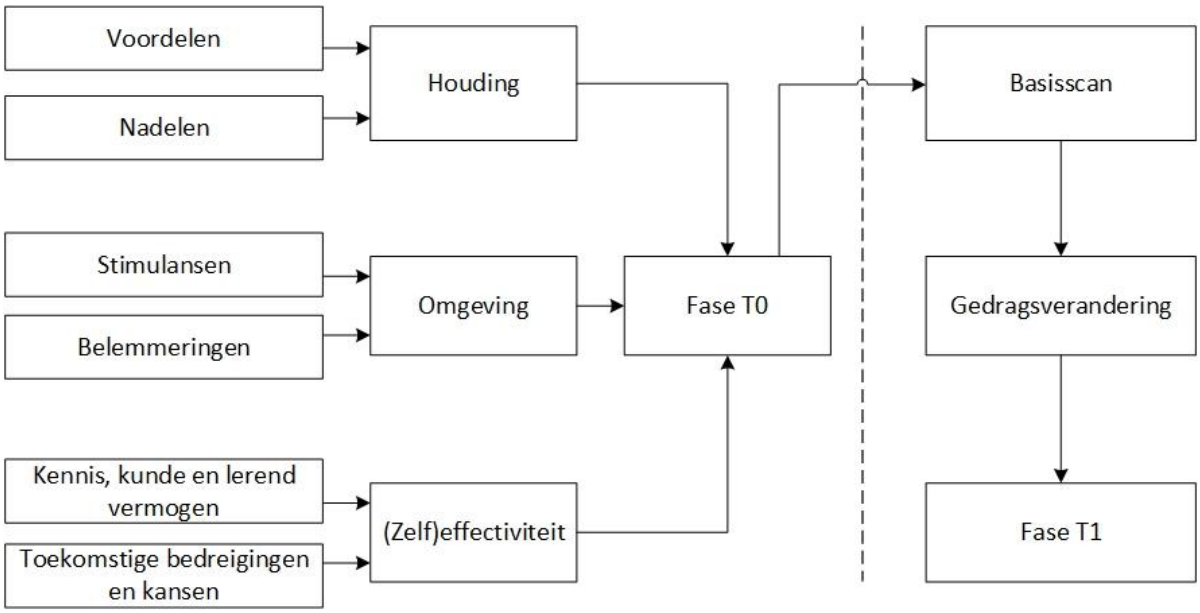
- Capaciteit (capability). Dat wil zeggen of ondernemers over de combinatie van kennis, kunde en lerend vermogen beschikken om over te gaan tot bepaald gedrag. Denk bijvoorbeeld aan kennis om phishing mails te herkennen en de kunde om die te melden.

- Gelegenheid (opportunity): Waaronder wordt verstaan de mogelijkheden die de omgeving of organisatie biedt om specifiek gedrag te vertonen of daarin juist belemmerd. Denk bijvoorbeeld aan iemand die een phishing poging wil melden bij zijn organisatie, terwijl de organisatie daarvoor geen dienst heeft ingericht.
- Motivatie (motivation). Hieronder valt psychologische processen van individuele werknemers ten aanzien van specifiek gedrag. Denk bijvoorbeeld aan iemand die het nut en de noodzaak niet inziet van het melden van phishing berichten.

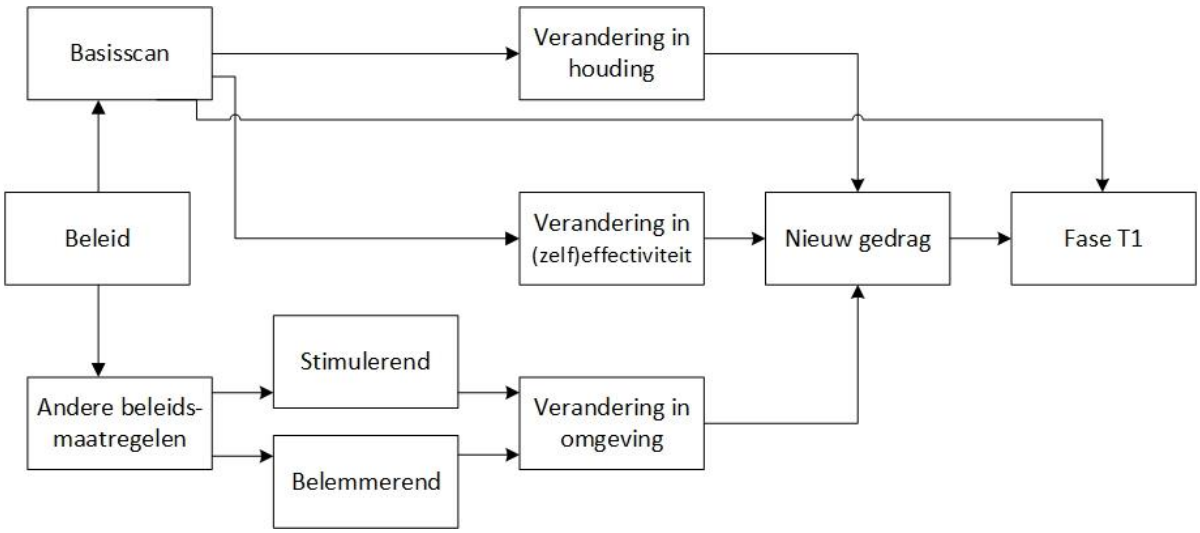
Het COM-B model verklaart gedrag maar beoogt ook te helpen bij het kiezen en ontwerpen van concrete interventies om gedrag te veranderen. Hiervoor hebben onderzoekers het zogenoemde 'behaviour change wheel' geïntroduceerd (Michie, Van Stralen, & West, 2011). Het gaat voor dit onderzoek te ver om daar dieper op in te gaan, maar biedt wel potentie, ook voor veilig onlinegedrag en informatiebeveiliging (zie bijv. 't Hoff-de Goede, Van der Kleij, Weijer, & Leukfeldt, 2019; Van der Kleij, Wijn, & Hof, 2020).

2.4 Conceptueel model

Op basis van hiervoor genoemde informatie hebben we een conceptueel model ontwikkeld met daarin de belangrijkste theoretische elementen. Het conceptueel model bestaat uit twee delen. Het eerste deel heeft betrekking op de nulmeting, zie figuur 2.1. Het eerst deel laat grofweg zien dat de factoren houding, omgeving en (zelf)effectiviteit van de ondernemer bepalend zijn voor gedragsfase. Het tweede deel van het model heeft betrekking op de (mogelijke) gedragsverandering als gevolg van het uitvoeren van de basisscan, zie figuur 2.2. Dit deel toont of, en zo ja op welke wijze, dezelfde factoren beïnvloed zijn na het maken van de basisscan en op welke wijze daardoor nieuw gedrag wordt bewerkstelligd.



Figuur 2.1: Conceptueel model fase T0



Figuur 2.2: Conceptueel model fase T1

De elementen uit de beide delen van het conceptueel model vormen de leidraad voor de ordening en interpretatie van de onderzoeksresultaten, zie het volgende hoofdstuk.

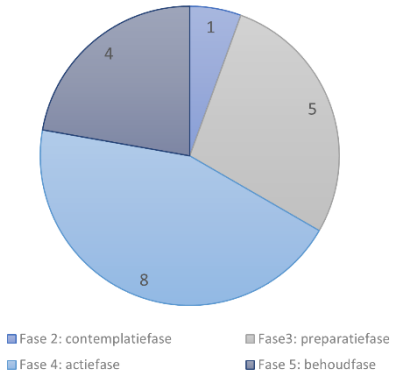
3. Resultaten

3.1 Inleiding

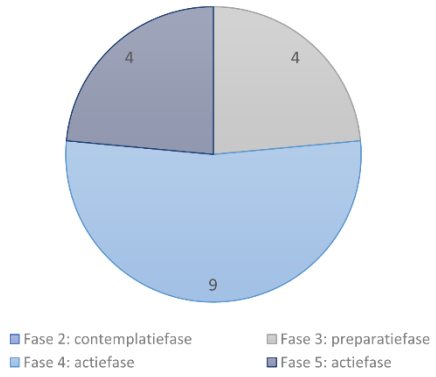
Dit hoofdstuk gaat in op de vraag in hoeverre de basisscan ondernemers aanzet tot gedragsverandering op het gebied van cyberweerbaarheid. Daartoe wordt eerst een overzicht gegeven van de belangrijkste bevindingen ten aanzien van de gedragsfasen en de waardering van ondernemers ten aanzien van de basisscan (paragraaf 3.2). Vervolgens gaat paragraaf 3.3 per bedrijf uitgebreid in op dagelijkse overwegingen om al dan niet de bedrijfsvoering aan te scherpen als het gaat om cyberweerbaarheid. Dit hoofdstuk behandelt daarmee onderzoeksvragen 3, 4 en 5 in samenhang.

3.2 Overzicht van de data

We zien dat de deelnemende bedrijven zich, op basis van zelfinzicht, betrekkelijk hoog inschatten, zie figuur 3.1. De meerderheid bevindt zich in de fasen 4 (n = 8) dan wel 5 (n = 5). Dat wil zeggen dat de respondent vindt dat hij de zaken al goed op orde heeft, al benoemen de meeste bedrijven ook de nodige verbetermogelijkheden. Na het maken van de basisscan, en het tweede interview, geven de bedrijven overwegend aan zich in dezelfde fase te bevinden (figuur 3.2). Een enkeling vond zichzelf aanvankelijk te laag ingeschat, terwijl enkele anderen hun eigen bedrijf in tweede instantie juist wat kritischer bekeken. De eerste indruk is dus dat de basisscan niet direct leidt tot een verandering van gedragsfase.



Figuur 3.1: Verdeling bedrijven over gedragsfasen voor basisscan

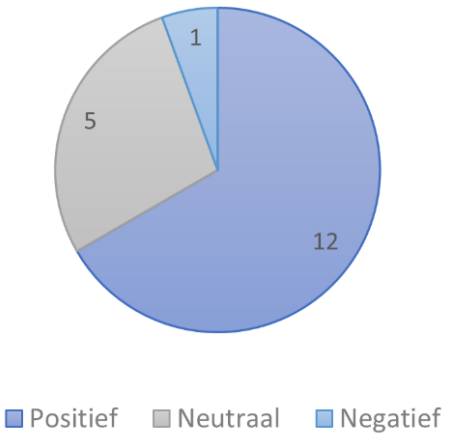


Figuur 3.2: Verdeling bedrijven over faseveranderingen na basisscan[15]

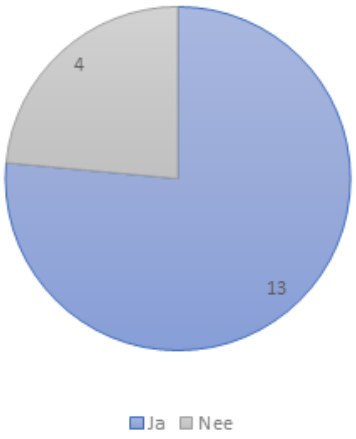
Het beperkte aantal 'faseveranderingen' wil echter niet zeggen dat de basisscan niet gewaardeerd wordt (figuur 3.3). Een ruime meerderheid ziet zeker toegevoegde waarde. Men geeft aan dat het instrument de ondernemer een spiegel voorhoudt. De

[15] Bij sommige figuren is sprake van zeventien in plaats van achttien respondenten omdat deze respondent, vanwege methodologische bezwaren (vraagstelling basisscan) geen medewerking verleende aan het invullen van de basisscan.

respondenten die 'neutraal' scoren zijn van mening dat de scan behulpzaam is, maar zijn overwegend kritisch over het algemene karakter. Eén respondent laat zich expliciet negatief uit over de basisscan, voor uitleg zie paragraaf 3.3, respondent G. De meerderheid van de bedrijven zien als gevolg van de basisscan duidelijk de meerwaarde in van het inzetten op cyberweerbaarheid (figuur 3.4). Het drukt hen nogmaals op de feiten en draagt bij aan een hernieuwd urgentiebesef. Er zijn echter ook bedrijven (een minderheid) die geen meerwaarde zien om in te zetten op cyberweerbaarheid. Voor de overweging daarvoor wordt verwezen naar de volgende paragraaf waarin de ondernemers hierover hun mening uiten.

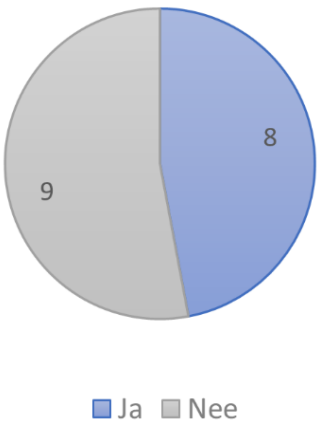


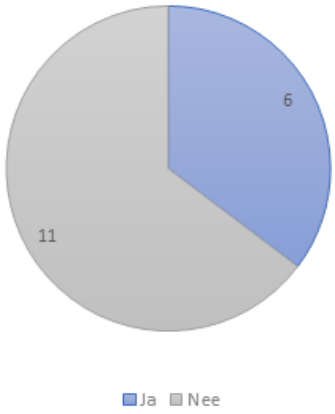
Figuur 3.3: Waardering van ondernemers voor de basisscan



Figuur 3.4: Inzien van meerwaarde inzet cyberweerbaarheid

Respondenten geven overwegend aan (zie figuur 3.5) dat zij niet of in beperkte mate bewuster zijn geworden van de zwakheden in hun organisatie als gevolg van de basisscan. Over het algemeen zijn de respondenten zeer betrokken bij hun bedrijf en hadden zij zich ook al verdiept in de materie. Voor een grote minderheid is de basisscan in dit opzicht echter wel waardevol gebleken. Respondenten geven verder in meerderheid aan dat de basisscan hen geen nieuwe inzichten heeft opgeleverd wat betreft toekomstige bedreigingen (figuur 3.6). Zij ervaren de scan als te statisch. Het betreft echt een momentopname.

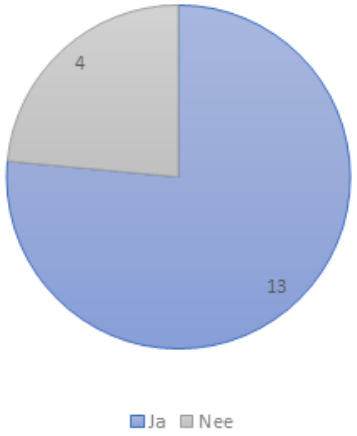


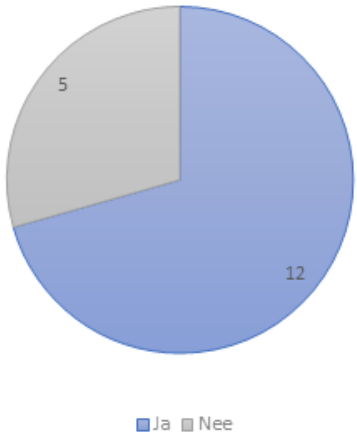


Figuur 3.5: Beter bewustzijn zwakheden

Figuur 3.6: Beter bewustzijn toekomstige bedreigingen

De respondenten laten in meerderheid (zie figuur 3.7) weten dat zij zich, na het uitvoeren van de basisscan, beter bewustzijn van de inspanning die zij nog moeten verrichten. Het drukt hen nogmaals met de neus op de feiten. Respondenten geven vervolgens aan kritisch te zijn (figuur 3.8) over van de mate waarin de basisscan hen aanvullend handelingsperspectief biedt. De inzichten zijn vooral bevestigend voor de huidige situatie, maar niet zozeer vernieuwend.

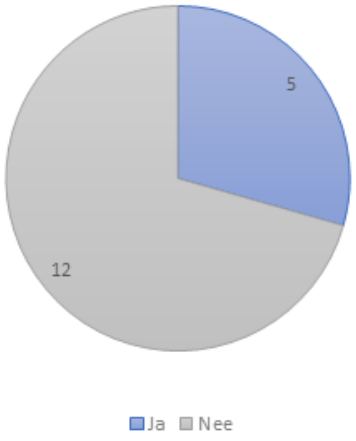


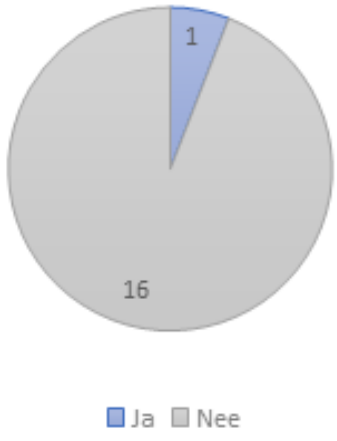


Figuur 3.7: Beter bewustzijn inspanningen

Figuur 3.8: Vergroten handelingsperspectief

De respondenten geven aan dat de basisscan hen niet of nauwelijks nieuwe inzichten oplevert als het gaat om de benodigde kennis, de kosten en de tijdsbesteding om de bedrijfsvoering verder te professionaliseren. Deze inzichten zijn gevisualiseerd in de figuren 3.9 en 3.10.



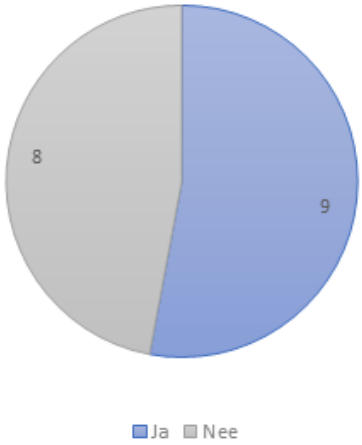


Figuur 3.9: Vergroten inzicht kennis en kunde

Figuur 3.10: Vergroten inzicht kosten en tijdsbesteding

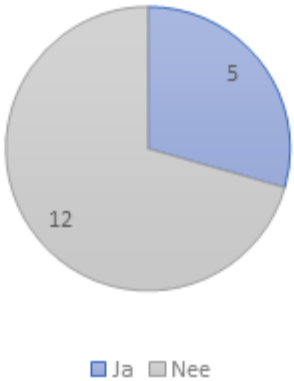
Vervolgens zien we in figuur 3.11 dat iets meer dan de helft van de bedrijven daadwerkelijk tot actie overgaat naar aanleiding van de basisscan. Dergelijke acties zijn op ieder gedragsniveau waar te nemen. De acties variëren van de (versnelde) aanschaf

van nieuwe servers tot een gesprek met de directie over de prioriteiten. De gedragsverandering is onder andere terug te voeren op het gegeven dat de meerderheid van de bedrijven als gevolg van de basisscan duidelijk meerwaarde zien in het inzetten op cyberweerbaarheid.



Figuur 3.11: Gedragsverandering naar aanleiding van de basisscan

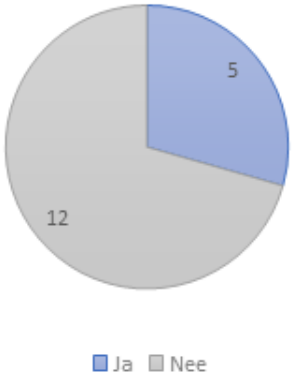
Nu we zicht hebben op de waardering van de basisscan ten aanzien van 'interne' drijfveren, presenteren we enkele resultaten ten aanzien van belemmeringen of stimulansen vanuit de 'buitenwereld'. Allereerst laat figuur 3.12 zien dat ondernemers nauwelijks meer stimulans ervaren van de overheid bij het op orde brengen van de cyberweerbaarheid. Doordat de overheid op veel andere terreinen rondom de bedrijfsvoering wel nadrukkelijk aanwezig is (denk aan: controles, belastingen, wetgeving), wordt de overheid juist als afstandelijk ervaren rond het thema digitale weerbaarheid. Ondernemers die 'ja' scoren op dit item geven vooral aan dat zij de basisscan waarderen en dat meewegen in hun oordeel.



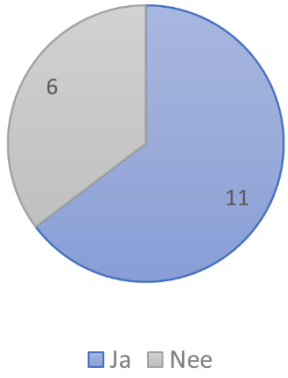
Figuur 3.12: Stimulans door de overheid

Van branchenoten (en overigens ook van zakenpartners) ervaart men op het eerste gezicht weinig stimulansen, zie figuur 3.13. Uit de interviews zal blijken (zie paragraaf 3.3) dat een aantal ondernemers zich wel laat leiden door ketenverantwoordelijkheid en 'peer pressure'. In figuur 3.14 is te zien dat ondernemers zich in iets ruimere mate gestimuleerd voelen door kennisinstellingen, zie. Een meerderheid laat weten beter op de hoogte te

zijn van onderzoeken en publicaties al moet hierbij worden opgemerkt dat niet zozeer concrete voorbeelden worden genoemd, maar vooral dit onderzoek positief gewaardeerd wordt.



Figuur 3.13: Stimulans door branchegenoten



Figuur 3.14: Stimulans door kennisinstellingen

Tussentijdse conclusie

Een beschouwing van de figuren en de toelichtingen leert dat de ondernemers de basisscan waarderen omdat deze hen een spiegel voorhoudt en ook in enige mate aanzet tot concrete actie. Dat betreft dan met name aspecten die zij over het algemeen eerder zelf al onderkend hadden. Het geeft hen net dat zetje dat nodig is om daadwerkelijk de handschoen op te pakken. Dat er nauwelijks sprake is van een verandering van fase heeft, wat betreft de basisscan, te maken met het beperkte inzicht dat de basisscan oplevert ten aanzien van kosten en tijdsbesteding.

Het lijkt erop dat men de 'quickwins' nu implementeert maar voor toekomstige bedreigingen en diepgaandere maatregelen onvoldoende houvast vindt bij de basisscan. De volgende paragraaf laat zien over welke overwegingen en dilemma's de ondernemers concreet spreken.

3.3 Gedragsverandering bij achttien ondernemers

Deze paragraaf vormt de kwalitatieve onderbouwing van de in de vorige paragraaf geschetste beelden. Gekozen is, vanwege het kwalitatieve karakter van het onderzoek om de ondernemer, en de wijze waarop hij de basisscan heeft ervaren, centraal te stellen. De resultaten worden dus per ondernemer gepresenteerd waarmee de uniciteit van de ervaringen recht wordt gedaan en dieper inzicht wordt verkregen in de effectiviteit van de basisscan. Alle bevindingen, verkregen door de interviews met de respondenten, worden gepresenteerd op overeenkomstige wijze, te weten:

A. Een, vanwege het waarborgen van de anonimiteit, zeer beknopte schets van het bedrijf;
B. De uitgangssituatie. Dit betreft de wijze waarop het bedrijf invulling geeft aan de basisprincipes en de achterliggende factoren;
C. De situatie na de basisscan op de onder B geschetste factoren;

D. Een oordeel van de respondent over de mate waarin de basisscan leidt tot gedragsverandering.

Bedrijf A: Zorgen om thuiswerkers

Schets van bedrijf A

Bedrijf A is werkzaam als toeleverancier van machines voor de veeteelt. Het bedrijf telt vijfhonderd werknemers en is gevestigd in Zuid-Nederland. Respondent A is Chief Information Security Officer (CISO) en is daarmee verantwoordelijk voor de digitale weerbaarheid van het bedrijf. Ook ICT en privacyaspecten horen tot zijn taakgebied. Het eerste interview is gehouden op 1 april en het tweede interview op 15 april 2021. De respondent benoemt als eerste associaties met cyberweerbaarheid: "De organisatie beschermen tegen datalekken en inbreuken." Daarbij gaan zijn gedachten in beginsel uit naar de 'buitenkant'. Ook cybersecurity van 'binnenuit' verdient de aandacht, zoals het meenemen van data door medewerkers. "Data moeten binnen het bedrijf blijven, dat is de kern." Het bedrijf heeft de ambitie om het in digitaal opzicht beter te doen dan de 'buurman' waarbij de respondent aangeeft dat het een utopie is om te veronderstellen dat 100% veiligheid haalbaar is.

Uitgangssituatie

Vijf basisprincipes

Wat betreft het in kaart brengen van 'kwetsbaarheden' geeft de respondent aan dit belangrijk te vinden en ook regelmatig een scan uit te voeren. De kwetsbaarheden worden beoordeeld op het risicogehalte en mogelijke tegenmaatregelen. Als knelpunt wordt aangegeven dat hiervoor lang niet altijd voldoende tijd beschikbaar is. Ten aanzien van de 'instellingen' geeft de respondent ook aan het belang te onderkennen en er druk mee bezig te zijn. Toch ziet men dat er nog wel stappen gemaakt kunnen worden ten aanzien van de automatische meldingen en de officepakketten. Ook het belang van 'updates' wordt ruimschoots onderkend. Men ziet nog te nemen stappen in het creëren van overzicht van de applicaties en het bijhouden van updates op een centrale plek. Eigenlijk wil men dat iedereen met dezelfde versies werkt. Qua cyberveiligheid en logistiek wordt het dan gemakkelijker om klachten te verwerken, zo is de gedachte. Ten aanzien van 'toegangsrestricties' onderkent bedrijf A eveneens het belang. Als werknemers het netwerk van buiten benaderen moeten zij multifactorverificatie toepassen via de mobiele telefoon. In het bedrijf zelf wordt tweefactorverificatie gebruikt. "Dat zijn goede stappen, maar winst valt te behalen bij toeleveranciers die deze werkwijze nog niet altijd hebben." Bedrijf A onderkent tenslotte het belang om 'virussen en malware' buiten de deur te houden. Op elke pc draait een antiviruspakket en er is een firewall bij de kantoorpanden geïnstalleerd. Het internetverkeer wordt bovendien via een centraal punt gemonitord. Door de recente pandemie is dit moeilijker geworden, maar omdat het wel belangrijk wordt gevonden, wordt hier relatief veel aandacht aan besteed.

Factoren houding en (zelf)effectiviteit

Respondent A geeft aan dat het van groot belang is om te weten hoe het bedrijf er qua cyberweerbaarheid voor staat: dat er inzicht is in de kwetsbaarheden van apparatuur, software en menselijke aspecten. En vooral dat bekend is waar indringers de grootste kans hebben om schade aan te richten. "Belangrijk is om up-to-date te blijven. Systemen verouderen snel terwijl nieuwe bedreigingen zich razendsnel ontwikkelen. Dit betekent een enorme werklast voor de ICT-afdelingen." Nog belangrijker voor de respondent is het om een afweging te kunnen maken op basis van analyses over de impact en de kosten van tegenmaatregelen: "Je zal keuzes moeten maken over wat je wel en wat je niet oppakt." Daarnaast vragen cloud-toepassingen om een andere benaderingswijze en de inzet van specifieke kennis en kunde. Het is zaak dat het bedrijf zich hiervan bewust blijft.

Omgevingsfactoren

Respondent A geeft in eerste instantie aan dat het bedrijf niet sterk vanuit de omgeving worden gestimuleerd. Alleen vanuit de naleving van de AVG[16] wordt wel een sterk sturende werking ervaren. Vanuit technisch oogpunt lukt het vaak wel om passende maatregelen treffen, maar het menselijke aspect wordt soms wel als lastig ervaren. Zo dient ook de HRM-afdeling (Human Resource Management) goed betrokken te zijn. Medewerkers met meervoudige functies binnen het bedrijf vormen ook een uitdaging omdat zij vaak van dubbele voorzieningen gebruik moeten maken.

Op basis van het eerste interview wordt geconcludeerd dat Bedrijf A zich bevindt in fase 4: de actiefase. Men is zich zeer bewust van het belang van cyberweerbaarheid en men onderneemt ook al in ruime mate actie.

Situatie na de basisscan

Vijf basisprincipes

Respondent A geeft aan dat de scores van de basisscan niet als een verrassing kwamen. Men ziet aan de ene kant een bevestiging van de ingezette acties, maar aan de andere kant scherpt het toch ook weer het bewustzijn aan. De resultaten uit de scan worden besproken met de directie omdat men een bevestiging van de noodzaak ziet. Ook wil men budget en capaciteit vrijmaken. Daar doet zich direct een uitdaging voor: "Hoe kom je in deze tijd aan voldoende mankracht? En nog praktischer. Hoe krijg je alle pc's vanuit andere locaties weer binnen voor updates en onderhoud?" Ten aanzien van de vijf basisprincipes is Bedrijf A gestart met een inventarisatie van apparatuur, is men zich bewuster geworden van de niet-kritische systemen en neemt men zich voor daar ook meer aandacht aan te besteden. Met betrekking tot 'updates' was de urgentie bekend,

[16] AVG staat voor Algemene Verordening Gegevensbescherming, de Nederlandse naam voor de Europese General Data Protection Act (GDPR). In deze Europese wetgeving zijn voor de lidstaten, waaronder Nederland, de belangrijkste regels voor de omgang met persoonsgegevens vastgelegd.

dit blijft een issue. Vooral pc's van thuiswerkers blijven een zwakke plek. Ten aanzien van 'toegangsrestricties' groeit het besef dat externe partijen een probleem zouden kunnen zijn: "Daar heb je maar in beperkt mate grip op." Er zijn nog geen concrete nieuwe acties ondernomen op het gebied van 'virussen en malware', maar overwogen wordt om meer in te zetten op monitoring om afwijkende data-uitwisseling vroegtijdig te kunnen waarnemen en te lokaliseren.

Factoren houding en (zelf)effectiviteit

Respondent A geeft zich aan zich, naar aanleiding van de basisscan, meer bewust te zijn van de concrete bedreigingen in het heden en de toegevoegde waarde van inzetten op digitale weerbaarheid. Daarnaast heeft hij beter inzicht in de sterkten en zwakten van de organisatie en de concrete inspanningen die de organisatie nog moet verrichten. Daarentegen heeft de basisscan geen of weinig inzicht gegeven in het kostenniveau van noodzakelijke maatregelen en de tijdsbesteding. Ook eventuele toekomstige bedreigingen en de kennis en kunde die men nu nodig heeft, zijn op hetzelfde niveau gebleven.

Omgevingsfactoren

De basisscan heeft ertoe bijgedragen dat Respondent A meer zicht heeft op de invloed van de omgeving. Hierbij valt te denken aan informatie van het NCSC, branchegenoten en het delen van leermomenten en het deelnemen aan bijvoorbeeld webinars. Van kennisinstellingen hoort men betrekkelijk weinig. Respondent A verwacht dat vanuit ontwikkelingen zoals certificeren (ISO-normering[17]) een sterk sturende werking zal uitgaan.

Oordeel over de basisscan

Ten aanzien van de basisscan concludeert Respondent A dat het instrument geholpen heeft om de aandacht vast te houden en om enkele zaken enigszins aan te scherpen. Tot een verandering in gedragsfase heeft dat (nog) niet geleid. Daarvoor is de scan wellicht wat te algemeen op dit moment. Dieper inzicht in investeringskosten zou een mooie aanvulling kunnen zijn, aldus Respondent A.

Bedrijf B: Genieten van Cyberweerbaarheid

Schets van bedrijf B

Bedrijf B heeft vijfenzestig medewerkers in dienst en is gevestigd in Noord-Nederland. Het bedrijf is gespecialiseerd in automatisering van bedrijfsprocessen. Respondent B is kwaliteitsmanager en houdt zich onder andere bezig met de certificering van de organisatie, in dit geval ISO-9001[18]. Het eerste interview met Bedrijf B is gehouden op 4

[17] ISO-normen zijn normen op het gebied van standaardisatie.
[18] ISO-9001 is de norm voor kwaliteitsmanagement. Als een bedrijf hieraan voldoet laat het zien zich aan de internationale eisen van kwaliteitsmanagement te voldoen.

december 2020, het tweede interview op 22 januari 2021. Respondent B geeft aan dat cyberweerbaarheid een zeer belangrijk onderdeel is van de bedrijfsvoering. Het type werkzaamheid dat dit bedrijf levert is gericht op automatisering en ICT, met klanten die de hoogste digitale veiligheidsniveaus eisen. De reden voor Bedrijf B om mee te doen aan dit onderzoek is omdat het bedrijf wil controleren of ze alle aspecten hebben meegenomen.

Uitgangspositie

Vijf basisprincipes

Bedrijf B heeft een eigen gespecialiseerde ICT-afdeling en voldoet aan de ISO-normering. Respondent B geeft aan dat op het gebied van 'kwetsbaarheden' het bedrijf zelf onderzoekt welke kwetsbaarheden er zijn. Dit doen zij bijvoorbeeld door op elkaars computers in te breken om te kijken waar de kwetsbaarheden liggen. Daarnaast wordt iedere week een scan uitgevoerd, waarbij alle apparaten van Bedrijf B worden doorgelicht. Op het gebied van 'instellingen' heeft Bedrijf B beleid waarbij alle wijzigingen moeten worden goedgekeurd door de ICT-afdeling. "Die goedkeuringsprocedure is soms wat vervelend voor de werknemers, maar het zorgt wel voor een uniforme, digitaal veilige, omgeving." 'Updates' gaan op eenzelfde manier: de centrale ICT-afdeling scant de beoogde updates en voert deze voor het hele bedrijf uit. Daardoor zijn de werknemers met de meeste ICT-kennis degenen die de updates goedkeuren en uitvoeren. Op die manier probeert Bedrijf B het risico te minimaliseren. Wat betreft 'toegangsrestricties' gebruikt Bedrijf B tweefactorverificatie: werknemers loggen in met een eenmalige code, gekoppeld aan een veilig eigen wachtwoord. Respondent B geeft aan dat zij met de toegang tot de werktelefoons nog enkele stappen zouden kunnen zetten. Deze werktelefoons zouden een mogelijke dreiging kunnen worden, vanwege mogelijk ongeautoriseerd gebruik. Tot slot doet Bedrijf B er alles aan om 'virussen en malware' te voorkomen. Hiervoor heeft Bedrijf B een betaalde versie van diverse virusscanners geïnstalleerd. De ICT-afdeling voert wekelijks een scan uit op alle apparaten van de organisatie.

Factoren houding en (zelf)effectiviteit

Bedrijf B onderkent de belangen van de basisprincipes en streeft naar perfectie als het gaat om digitale weerbaarheid. Doordat de corebusiness van het bedrijf automatisering is, de klanten het hoogste niveau eisen en het bedrijf er zelf veel tijd aan wil besteden is de inschatting van respondent B dat het bedrijf digitale weerbaarheid goed geregeld heeft. Respondent B geeft aan dat een paar jaar geleden de aandacht voor digitale weerbaarheid minder (goed) was. Nadat veranderingen in het management hadden plaatsgevonden, veranderde deze houding. Het nieuwe management zag nadrukkelijker het belang in van digitale weerbaarheid. Dit leidde tot investeringen, zowel in kwantitatief als in kwalitatief opzicht. Hierbij worden nu kosten noch moeite bespaard. Volgens respondent B is de houding van het management bepalend voor de mate waarin de organisatie aandacht besteedt aan digitale weerbaarheid. Respondent B acht zijn bedrijf kortom zeer in staat om de ontwikkelingen op het gebied van digitale weerbaarheid te blijven volgen en waar mogelijk een stap voor te blijven.

Omgevingsfactoren

Bedrijf B zit in een netwerk van ICT-organisaties. In dit netwerk worden onderlinge hackpogingen ondernomen om te testen of de digitale weerbaarheid op orde is. Respondent B geeft aan dat een omgeving waar men (evenveel) aandacht heeft voor digitale weerbaarheid net zo bepalend is als de houding van het management: "Bedrijven moeten elkaar helpen en van elkaar leren, dat maakt het ook leuk." Bedrijf B onderkent verder de grote invloed van de ISO-normering. "Wij bevinden ons in een omgeving waar digitale weerbaarheid bovenmatig gestimuleerd wordt."

Op basis van het eerste interview wordt geconcludeerd dat bedrijf B zich in fase 5 bevindt: de behoudfase. Bedrijf B ziet de dat inspanningen worden beloond en wil dit zo houden. Tegelijkertijd benoemt Respondent B dat de ontwikkelingen nooit stoppen en dat er altijd nog stappen gezet kunnen worden, maar dat er alles aan wordt gedaan om bij te blijven.

Situatie na de basisscan

Vijf basisprincipes

Respondent B heeft op 16 december 2020 de basisscan gemaakt. Daaruit kwam, zoals Respondent B al verwacht had, de maximale score. Volgens Respondent B is het enige waar nog meer op gelet moet, met het oog op de certificering, het aspect documentatie. De resultaten van de basisscan zijn besproken binnen de ICT-afdeling. Hij geeft aan dat men nog geen aanvullende acties op de vijf basisprincipes heeft ondernomen. Bij iedere vraag of er veranderingen zijn doorgevoerd bij een basisprincipe geeft hij aan dat dit al op orde was. Respondent B zegt: "De dagelijkse ontwikkelingen bij digitale weerbaarheid blijven, maar we konden geen concrete acties uit de basisscan halen."

Factoren houding en (zelf)effectiviteit

Er hebben volgens Respondent B geen veranderingen plaatsgevonden ten opzichte van het eerste interview. De basisscan heeft voor hem niet geleid tot nieuwe inzichten of kennis. Ook qua inzicht in kosten en tijdsinvesteringen ziet Respondent B geen veranderingen. Hij geeft aan dat hij dit ook niet verwacht had.

Omgevingsfactoren

De basisscan heeft niet direct geleid tot andere inzichten vanuit de omgeving voor respondent B. De geïnterviewde geeft aan dat hij dit ook niet echt verwacht had, doordat het bedrijf al in een inspirerende omgeving zit. Respondent B geeft daarnaast aan het erg goed vinden dat onderzoeken als deze gehouden worden. Hij verwacht dat bedrijven daardoor bewuster kunnen worden van de mogelijke gevaren maar ook de kansen om te investeren.

Oordeel over basisscan

Respondent B ziet de resultaten van de basisscan vooral als een bevestiging van de eigen inzichten. Het bedrijf was al vrij zeker van de mate van digitale weerbaarheid en ziet de bevestiging in de uitkomsten. Hij geeft in het tweede interview aan dat de basisscan een goed instrument kan zijn voor bedrijven die minder aandacht besteden aan digitale weerbaarheid. Dat type bedrijven heeft volgens respondent B concrete voorbeelden van voorvallen nodig om de urgentie te voelen.

Bedrijf C: Cyberweerbaarheid als prioriteit

Schets van Bedrijf C

Bedrijf C is gespecialiseerd in industriële automatisering. Het bedrijf is gevestigd in Noord-Nederland en heeft vijftien medewerkers in dienst. Respondent C is manager Research & Development. Het eerste interview is gehouden op 9 december 2020 en het tweede interview op 28 januari 2021. De associaties met cyberweerbaarheid van respondent C zijn: "Dat je weet wat de gevaren zijn en welke risico's er kleven aan een organisatie die digitale werkzaamheden uitvoert." Respondent C benoemt dat het bedrijf al ruim twintig jaar bezig is met de informatie-uitwisseling op afstand en dat het bedrijf ISO-27001[19] gecertificeerd is. Hij schat daarom in dat het bedrijf de digitale weerbaarheid goed op orde heeft maar nog verder zou kunnen werken aan de bewustwording onder medewerkers.

Uitgangspositie

Vijf basisprincipes

Een van de belangrijkste aspecten van het in kaart brengen van 'kwetsbaarheden' is volgens Respondent C dat je weet wat wanneer gebeurt. Bedrijf C heeft daarvoor een applicatiebeheerder in dienst. De inrichting van het dashboard dat de kwetsbaarheden in beeld brengt, kost volgens Respondent C veel tijd. "Maar, het levert echter ook veel op." De ISO-normering van het bedrijf brengt met zich mee dat een goede cyberweerbaarheid een verplichting is richting de afnemers. Op het gebied van 'instellingen' zorgt Bedrijf C voor actieve beveiliging door alleen met online-applicaties te werken. Daarbij wordt vaak gekeken waar het bedrijf zich verder in kan verbeteren. Bedrijf C voert actief 'updates' uit en doet dat ook voor haar klanten, waarmee het bedrijf informatie uitwisselt. Respondent C onderkent het belang van 'toegangsrestricties' en heeft daarvoor een actief wachtwoordbeleid. Concreet betekent dit dat alle werknemers eens in de zoveel tijd hun wachtwoorden compleet moeten veranderen. "Dit is wel eens vervelend, maar de voordelen wegen zwaarder dan dit ene nadeel." De computers van alle medewerkers worden actief en regelmatig gecontroleerd op 'virussen en malware'. Dit gebeurt integraal en door de applicatiebeheerder, daarnaast worden de updates automatisch doorgevoerd.

[19] ISO-27001 is de internationaal erkende norm op het gebied van informatiebeveiliging.

Factoren houding en (zelf)effectiviteit

Respondent C acht zijn organisatie volledig in staat om invloed uit te oefenen op de cyberweerbaarheid. Daar ziet hij dan ook het belang van in. Het lerende vermogen zit enerzijds in de kern van het bedrijf. De werkzaamheden die organisatie C uitvoert, vragen simpelweg een hoge mate van ICT-capaciteit. Anderzijds is het ook interesse. Binnen het bedrijf vinden werknemers het leuk om met de digitale weerbaarheid bezig te zijn en zien ook de belangen in van een goede cyberweerbaarheid. Dit zorgt voor motivatie. Als er situaties zijn waar de benodigde kennis niet binnen de organisatie zelf aanwezig is, wordt dit extern gezocht.

Omgevingsfactoren

De ISO-normering van het bedrijf impliceert dat een goede digitale weerbaarheid een verplichting is richting de afnemers van Bedrijf C. Deze systematiek achter de normering kan ook gebruikt worden ter minimalisering van de risico's. De respondent geeft aan dat dit stimulerend werkt om de zaken op orde te hebben. Het kunnen aantonen van een bepaald niveau van digitale weerbaarheid maakt volgens Respondent C zelfs onderdeel uit van de verkoopstrategie.

Bedrijf C participeert in een aantal actieve netwerken waar allerlei activiteiten worden georganiseerd om de digitale weerbaarheid te vergroten. Dit gaat van onlinevoorlichting voor medewerkers tot onderlinge hackpogingen. Respondent C zegt op geen enkele manier belemmeringen te ervaren vanuit de omgeving. Het enige dat hij benoemt, is dat het niveauverschil in digitale beveiliging tussen het eigen bedrijf en dat van klanten wel eens zorgt voor problemen. Dat komt doordat de klant nog niet dezelfde nieuwere systemen gebruikt als bedrijf C.

Op basis van het eerste interview wordt geconcludeerd dat Bedrijf C zich bevindt in fase 5: de behoudfase. Bedrijf C besteedt zeer veel aandacht aan cyberweerbaarheid. Het huidige niveau willen zij graag vasthouden.

Situatie na de basisscan

Respondent C ziet het belang in van goede, veilige 'instellingen'. Hij geeft aan dat voor de interne instellingen van het bedrijf nog winst te behalen valt. Dat het nog niet op het gewenste niveau zit, komt ten eerste doordat het erg ingewikkeld is en ten tweede omdat het niet gestimuleerd wordt. Bovendien hebben veel leveranciers, zoals Apple, eigen externe instellingen, die lijken te voldoen. Het bedrijf voert tweewekelijks 'updates' uit. Voordat wordt geüpdatet voert het bedrijf eerst een scan uit op potentiële kwetsbaarheden.

Vijf basisprincipes

Respondent C heeft de basisscan op 28 januari 2021 ingevuld. Hij geeft direct bij de start van het interview aan dat de basisscan geen nieuwe inzichten gegeven heeft, het werkt bevestigend ten aanzien van de eigen inzichten.

Factoren houding en (zelf)effectiviteit

De situatie na de basisscan voor respondent C is ongewijzigd. De basisscan heeft de houding niet veranderd, men had de zaken al goed op orde. Respondent C geeft aan dat het inzicht in de digitale weerbaarheid al ruimschoots aanwezig was.

Omgevingsfactoren

De basisscan heeft niet geleid tot meer bewustzijn bij Respondent C. Het gewenste niveau was al bereikt, mede door de ISO-27001 certificering. De netwerken droegen ook bij aan een hoog niveau. Dit is niet veranderd na de basisscan.

Oordeel over de basisscan

Respondent C verwacht dat bedrijven die hun digitale weerbaarheid nog niet goed op orde hebben veel kunnen hebben aan de basisscan maar bij henzelf heeft het niet geleid tot veranderingen. Het bedrijf zat al in de hoogste fase. Het werd gezien als een bevestiging van de eigen professionaliteit.

Bedrijf D: Een nieuwe impuls

Schets van bedrijf D

Respondent D is ICT-consultant. Enerzijds is hij verantwoordelijk voor alles met betrekking tot ICT binnen de organisatie, anderzijds adviseert hij zelf klanten op het gebied van ICT. Bedrijf D is gevestigd in Noord-Nederland en heeft tien medewerkers in dienst. Respondent D denkt bij cyberweerbaarheid aan het voorbereid zijn op digitale aanvallen, zowel van buitenaf als van binnenuit. Het eerste interview is gehouden op 2 december 2020, het tweede interview op 26 januari 2021.

Uitgangspositie

Vijf basisprincipes

Respondent D probeert actief 'kwetsbaarheden' binnen het bedrijf te voorkomen. Het bedrijf heeft een goede firewall en een aantal systemen die de computers en browsers nakijken op kwetsbaarheden. De respondent probeert bewust prioriteiten te stellen op de voor deze organisatie belangrijkste onderdelen. In het interview benoemt hij dat een werkstation potentieel veel kwetsbaarder is dan een mobiele telefoon van een individuele medewerker. De kosten en de tijdsinvestering spelen parten, maar hij schat in dat het bedrijf het met de huidige middelen vrij goed doet. "Een nadeel van updates is dat het bedrijf dan tijdelijk offline is, dit jaar al drie keer." Dit heeft invloed op de mate waarin de updates binnen bedrijf D geaccepteerd worden. Op het gebied van

'toegangsrestricties' zit volgens respondent D een mismatch tussen het management en de ICT-afdeling. "Het management en de administratieve afdelingen willen overal bij kunnen terwijl ik graag, met het oog op de beveiliging, juist restricties wil doorvoeren. Als ik er niet ben willen anderen volledig mijn taken uitvoeren, terwijl dat eigenlijk niet zou moeten." Op het gebied van 'virussen en malware' voert het bedrijf iedere middag een 'QuickScan' uit en wekelijks een uitgebreidere scan: "Ons management vindt dit onderwerp belangrijk, er mag meer in worden geïnvesteerd dan bij de andere cyberonderwerpen van dit onderzoek."

Factoren houding en (zelf)effectiviteit

Respondent D denkt dat hij goed in staat is om invloed uit te oefenen op cyberweerbaarheid: "Het lerend vermogen is groot. Dat komt vooral door mijn eigen interesses rondom dit onderwerp." De beschikbare tijd om actief bezig te gaan met digitale weerbaarheid is beperkt, net als het kapitaal voor eventuele investeringen. Desalniettemin zegt Respondent D: "In relatie tot de hoeveelheid mensen doen we het gewoon heel erg goed." Het belangrijkste volgens respondent D is de interesse vanuit het management. Wanneer dat minder aanwezig is, kan de aandacht voor dit onderwerp snel verslappen.

Omgevingsfactoren

Vanuit de omgeving wordt het bedrijf nauwelijks tot niet gestimuleerd. Respondent D mist dat soms; geslaagde hackpogingen bij andere bedrijven kunnen een urgentiegevoel creëren. "Dat is zeker voor het management van belang zodat er middelen en tijd in worden gestoken." Hij volgt zelf het nieuws over incidenten, maar dit komt nog niet altijd aan bij het management. In die laag valt volgens hem de meeste winst te behalen. Leveranciers van de producten aan bedrijf D hebben volgens hem weinig kennis van cyberweerbaarheid. Hij denkt ook dat de overheid in dit onderwerp een actievere houding zou kunnen aannemen.

Respondent D schat in dat de organisatie onderin fase 5 zit: de behoudfase. De inspanningen worden beloond, de goede elementen worden behouden. Dat het goed gaat komt vooral door eigen interesses in de materie. Er is een aantal onderwerpen die de organisatie erg belangrijk vindt, maar waar volgens de respondent nog niet genoeg aan wordt gedaan.

Situatie na de basisscan

Vijf basisprincipes

Respondent D heeft de basisscan in totaal twee keer gemaakt. Eén keer een aantal weken na het eerste interview, de andere keer op de ochtend van het interview. De tweede keer wilde hij de kennis even opfrissen en ook wilde hij kijken of er zich in de tussentijd veranderingen hadden voorgedaan. De grootste verandering is volgens Respondent D dat er nu aandacht vanuit het management is gekomen voor cyberweerbaarheid. Het

'frappante' is dat dit voornamelijk komt door enkele incidenten die zich hebben voorgedaan in de periode tussen het eerste en tweede interview.

Factoren houding en (zelf)effectiviteit

De basisscan heeft niet bijgedragen aan nieuwe kennis, maar het inzetten van die kennis heeft wel een nieuw impuls gekregen. Hij verwacht dat de organisatie meer aandacht zal besteden aan een goede cyberweerbaarheid. De houding bij het management lijkt wel degelijk veranderd. Respondent D verwacht daardoor dat de professionaliteit van de organisatie een nieuwe impuls krijgt.

Omgevingsfactoren

Door de incidenten in de omgeving is het besef bij het management ontstaan dat het eigen bedrijf kwetsbaarder is dan van tevoren werd gedacht. Hij benoemt dat er voorheen bij het management een soort 'naïviteit' was: "het kan, of zal niet bij ons gebeuren." Dat gevoel is nu veranderd. Vanuit de omgeving hebben zich verder geen veranderingen voorgedaan. De organisatie wil meer informatie ontvangen over cyberweerbaarheid en de potentiële gevaren die het met zich mee kan brengen.

Oordeel over de basisscan

Respondent D schat in dat de combinatie van incidenten in de directe omgeving en de inzichten uit de basisscan ertoe hebben geleid dat er verhoogde alertheid binnen het bedrijf is. Verandering van fase heeft er niet plaatsgevonden. Immers, het bedrijf zat al in fase 5: behoudfase.

Bedrijf E: Nieuw elan in het familiebedrijf

Schets van bedrijf E

Bedrijf E is een groothandel voor landbouwmaterialen en is gevestigd in Noord-Nederland. Het eerste interview is gehouden op 7 december 2020 en het tweede interview op 15 maart 2021. Het bedrijf heeft vier werknemers en is te classificeren als een familiebedrijf. De respondent is ten tijde van het interview van 7 december nog werknemer. Tijdens het tweede interview is respondent E inmiddels eigenaar van de zaak. Wanneer het over cyberweerbaarheid gaat denkt respondent E gelijk aan de mate waarin de organisatie digitaal te kraken valt en de manier waarop het zich kan weren tegen deze digitale risico's. Het bedrijf is, onder aanvoering van een nieuwe generatie, voornemens om meer aandacht te besteden aan digitale weerbaarheid. "Dat zit in professionalisering, maar ook door er meer tijd en aandacht aan te besteden."

Uitgangspositie

Vijf basisprincipes

Op het gebied van 'kwetsbaarheden' geeft Respondent E gelijk aan geen grip te hebben op wat er binnen de organisatie allemaal gebeurt. "Dit is vooral onderling tussen de medewerkers: het op de hoogte zijn van wat de ander op dit gebied zoal doet." Die

invloed is volgens Respondent E vooralsnog een groot gemis. Hij probeert risico's te vermijden door bijvoorbeeld e-mails te filteren, waarbij verdachte zaken worden verwijderd. "Wat andere medewerkers doen heb ik nog geen zicht op. In het verleden is dit binnen de organisatie wel eens fout gegaan, vandaar dat ik hier nu extra aandacht aan besteed. Ik heb een soort van filterfunctie." De 'instellingen' zijn volgens Respondent E prima 'in de cloud te managen'. Maar, verder wordt er relatief weinig gedaan aan de instellingen. 'Updates' worden automatisch geïnstalleerd, respondent E hoeft alleen een akkoord te geven. "Hierdoor is er wel enig zicht op wat er zoal geïnstalleerd wordt binnen de organisatie. Zodra updates interessant zijn voor de organisatie probeer ik hier extra op te letten." Wat betreft de 'toegangsrestricties' wordt gebruik gemaakt van tweefactorverificatie. Het wordt volgens Respondent E gebrekkig wanneer een werknemer de wachtwoorden onder het toetsenbord heeft liggen. Hij wijdt dit aan de generatiekloof, maar ook aan het gebrek aan prioriteit en inzicht in de mogelijke gevaren. "Wij verwachten geen slachtoffer te worden van cybercriminaliteit, dit leidt tot andere prioriteiten." Hij verwacht dat een verschuiving van prioriteit waarschijnlijk pas zal veranderen op het moment dat bij wijze van spreken de buurman slachtoffer wordt van cybercriminelen. Van 'virussen en malware' heeft Respondent E weinig verstand: "Ik heb eerlijk gezegd geen idee wat het bedrijf precies onderneemt op dit gebied."

Factoren houding en (zelf)effectiviteit

Het belang van een goede cyberweerbaarheid ziet Respondent E zeer zeker in: "Het regelmatig updaten en het minder slordig omgaan met wachtwoorden, is uitermate belangrijk." Tegelijkertijd merkt respondent E dat het vooral mis kan gaan doordat er binnen de organisatie te weinig aandacht wordt besteed aan dit onderwerp. "Er wordt automatisch van uitgegaan dat het wel goed gaat. Het besef dat het niet goed kan gaan wordt pas duidelijk als het dicht bij een keer misgaat." Van het uitvoeren updates ziet hij niet in wat de voordelen zijn: "Dit is binnen dit bedrijf een geautomatiseerd proces en dat is prima." Respondent E schat in dat binnen de organisatie genoeg expertise aanwezig is om in te zetten op cyberweerbaarheid. De belangrijkste nadelen om meer in te zetten op cyberweerbaarheid zijn voor hem de kosten die hiermee gepaard gaan, de tijd die het kost en een de motivatie die moet worden opgebracht.

Omgevingsfactoren

Vanuit de omgeving wordt weinig tot geen invloed uitgeoefend op bedrijf E als het gaat om cyberweerbaarheid. Dit heeft volgens hem een aantal oorzaken: "Het is niet echt een onderwerp wat bijvoorbeeld op feestjes ter sprake komt." Hij denk dat in zijn directe omgeving ook weinig gebeurt. Ook dit heeft te maken met interesse, schat hij in: "Zelfs als er al wat gebeurt filter ik dit omdat ik het eigenlijk niet interessant genoeg vind." De partijen die enige invloed uitoefenen, bijvoorbeeld op de sterkte van wachtwoorden, zijn banken en administratiekantoren. "Daarbij moet je voldoen aan hun regels." Respondent E bevindt zich dus in een omgeving waarin er op dit onderwerp weinig gestimuleerd wordt. In het interview wordt óók aangegeven dat op geen enkele wijze

belemmeringen zijn vanuit de omgeving. "Het is in mijn optiek vooral een gebrek aan motivatie."

Geconcludeerd kan worden dat Bedrijf E na het eerste interview in fase 2 zit: de contemplatiefase. Er zijn voorbereidingen getroffen, maar er is nog geen harde actie ondernomen.

Situatie na de basisscan

Vijf basisprincipes

Respondent E heeft de basisscan in de week van 10 maart 2021 gemaakt. De basisscan heeft hem aangezet om een aantal dingen aan te pakken. Met name op de gebieden 'updates' en 'toegangsrestricties'. Dit is, door de basisscan en mee te doen aan dit onderzoek, onder de actieve(re) aandacht gekomen. "Maar, het is nog niet bekend wanneer de updates worden aangepakt. Dit kan binnen twee weken of binnen twee maanden zijn." Op het gebied van wachtwoorden daarentegen is nu al wat veranderd, doordat de respondent hierop werd gewezen in het eerste interview. Er wordt geprobeerd de werknemers bewuster te maken van een goed wachtwoord, ook wordt dit ook actiever bijgehouden. Op de gebieden 'kwetsbaarheden', 'instellingen' en 'virussen en malware' zijn nog geen nieuwe acties ondernomen. "Maar, ik sta hier nu in ieder geval wel opener voor."

Factoren houding en (zelf)effectiviteit

De basisscan heeft Respondent E veel nieuwe inzichten gegeven. Dit zit vooral in de kennis- en bedreigingenkant. "Ik weet nu beter welke mogelijke bedreigingen zich voordoen." Waar de basisscan voor respondent E niet bij heeft geholpen is welke kennis en kunde nodig zijn en wat dit gaat kosten. Zowel materieel als immaterieel. Tegelijkertijd benoemt Respondent E dat dit ook wel aan zijn manier van werken ligt: "Ik wil het zelf uitzoeken."

Omgevingsfactoren

"Het hebben van directe voorbeelden uit mijn omgeving heb ik nog eigenlijk nodig om de urgentie in te zien." Respondent E is zich nadat hij de basisscan heeft gemaakt, bewuster van de overheidscampagnes over dit onderwerp. "Ik verwacht dat dit voornamelijk komt doordat ik er meer mee bezig ben dan voorheen." Respondent E staat er meer voor open, en denkt daardoor ook actiever signalen uit de omgeving op te vangen. Er is niks veranderd aan stimulansen noch belemmeringen door branchegenoten en zakenpartners.

Oordeel over de basisscan

Meedoen aan dit onderzoek heeft bij respondent E geleid tot meer bewustzijn wanneer het gaat om digitale weerbaarheid. De concrete actie is op veel gebieden nog niet ondernomen. Daarom bevindt bedrijf E zich nu in fase 3: de preparatiefase. Hij is van plan om meer in te zetten op de basisprincipes. "Ik beschouw de scan als een erg positief

instrument, vooral omdat ik een dergelijke proactieve houding niet per se had verwacht van een overheidsinstelling." Hij geeft als tip mee dat een bredere, actieve campagne onder soortgelijke bedrijven zou kunnen leiden tot betere digitale weerbaarheid.

Bedrijf F: Eerst de oogst van het land

Schets van bedrijf F

Bedrijf F is een biologisch agrarisch bedrijf dat van oudsher van ouder op kind is overgegaan. Het betreft een maatschap waarin een echtpaar samenwerkt. De maatschap is in Noord-Nederland gevestigd en kent een divers palet aan akkerbouwgewassen. Het eerste interview is gehouden op 12 januari 2021, het tweede interview op 11 maart 2021. Bij cyberbaarheid denkt Respondent F vooral aan de mate waarin zijn bedrijf te kraken valt: "Echt het weren van alle digitale risico's."

Uitgangspositie

Vijf basisprincipes

In het verleden is Bedrijf F, doordat men toen nog minder met digitale weerbaarheid bezig was, slachtoffer geweest van cyberincidenten. Zo had zijn voorganger een keer op een foute e-mail geklikt, waardoor er virussen in de systemen kwamen. Daarom probeert Respondent F nu meer aandacht te besteden aan cyberaspecten in algemene zin. Op het gebied van 'kwetsbaarheden' beschouwt hij zichzelf als filterfunctie voor de rest van het bedrijf. "Doordat het bedrijf in het verleden slachtoffer is geworden via e-mail probeer ik daar nu extra aandacht aan te besteden." Bij 'instellingen' wil de respondent vooral bijblijven. Daarbij wordt als minimumeis gezien dat het bedrijf voldoet aan de eisen van externe partijen, zoals de bank. Respondent F ziet geen bijzondere voordelen van 'updates'. "Ik koop een systeem en dat doet het als het goed is goed, dat vind ik genoeg." Hij schat daarnaast in dat voor soortgelijke bedrijven automatische updates het handigste zijn. Respondent F geeft aan vergevorderd te zijn met de 'toegangsrestricties' en dit graag zo te willen houden. Het bedrijf gebruikt tweefactorverificatie op alle computers en telefoons. Hiervoor worden externe programma's gebruikt: "Ik weet de wachtwoorden zelf niet eens." Om 'virussen en malware' tegen te gaan heeft Bedrijf F een gratis virusscanner: "Die houdt als het goed is malafide websites buiten de deur." De organisatie is in het verleden een keer online 'gegijzeld' geweest. Doordat het niet om gevoelige informatie ging is daar verder niks meegedaan. Dat het bedrijf nog geen betaalde versie van een virusscanner heeft, ligt puur aan de kosten en aan het feit dat de respondent niet weet of de betaalde versie daadwerkelijke beter is.

Factoren houding en (zelf)effectiviteit

Aandacht is volgens Respondent F essentieel: "De meeste onderdelen gaan vooruit wanneer er meer aandacht voor is, daar schuilt natuurlijk een gevaar in. Dat je er dan automatisch vanuit gaat dat het wel goed gaat." Wat volgens Respondent F een medeoorzaak is voor het gebrek aan aandacht, is dat het "voor bedrijven als de onze niet de corebusiness is." Hij acht zichzelf in staat om meer invloed uit te kúnnen oefenen. Hij

vindt de onderwerpen rondom digitale weerbaarheid interessant. Maar, "In de dagelijkse gang van zaken gaan de rest van de werkzaamheden altijd voor."

Omgevingsfactoren

Respondent F: "Iedereen leert op zijn eigen manier, ik leer veel van mijn omgeving. Dus als het een keer in mijn omgeving gebeurt, ga ik er zelfs iets aan doen." Bedrijf F wordt niet door partijen als de overheid, afnemers van zijn producten, externe kennisinstellingen gestimuleerd om (meer) bezig te gaan met digitale weerbaarheid. Vanuit een verzekering is hem wel eens tweefactorverificatie aangeraden.

Op basis van het eerste interview ziet Respondent F zichzelf in fase 4: Actiefase. Er zijn diverse voorbereidingen getroffen en op sommige gebieden zijn ook al acties doorgevoerd. Maar, hier en daar zouden nog stappen gezet kunnen worden.

Situatie na de basisscan

Vijf basisprincipes

Respondent F heeft de basisscan in januari gemaakt. De basisscan gaf een hogere score dan dat de respondent zelf had ingeschat. "Kwetsbaarheden werden geïnventariseerd in het eerste interview [...] de basisscan was meer een formalisatie van het eerste interview." Op de gebieden 'instellingen' en 'updates' heeft de respondent niks veranderd. Bij 'virussen en malware' is de virusscanner geüpdatet. Hij geeft aan dat de basisscan verder niet direct heeft geleid tot harde actie, maar dat het instrument wel heeft bijgedragen aan nieuwe kennis. "Ik ben op de hoogte gebracht van wat ik nog kon doen, dat heb ik nu gedaan."

Factoren houding en (zelf)effectiviteit

De basisscan heeft bij respondent F bijgedragen aan het herkennen van de meerwaarde van digitale weerbaarheid binnen zijn organisatie. "Dit was al bekend, maar de basisscan heeft dit gedachtegoed geactiveerd." Ook heeft de basisscan Respondent F bewuster gemaakt van de inspanningen die hij nog moet leveren om zijn digitale weerbaarheid te vergroten. Meedoen aan dit onderzoek heeft ook geleid tot meer kennis over de zwakheden van de organisatie en welke eventuele toekomstige bedreigingen op zijn pad kunnen komen. Waar de basisscan niet aan heeft bijgedragen is een inventarisatie van mogelijke kosten die gepaard gaan met een betere digitale weerbaarheid en de tijdsinvestering die de verbeteringen kost.

Omgevingsfactoren

Respondent F wordt niet door overheidsinstellingen gestimuleerd om (meer) in te zetten op digitale weerbaarheid. "Als ze de basisscan naar bedrijven zouden sturen zou dat actief en stimulerend werken." Ook van branchegenoten en kennisinstellingen merkt Respondent F niet meer dan in de eerste meting. Hetzelfde geldt voor zakenpartners. "De enige partij die op enige wijze stimuleert is de bank." Respondent F zou een

proactieve houding van de overheid waarderen. "De overheid hoort ondernemers te stimuleren. We weten überhaupt niet dat een dergelijk instrument er is."

Oordeel over de basisscan

Tot een verandering van fase heeft de basisscan niet geleid. Respondent F bevindt zich nog steeds in fase 4: actiefase. "Er kwamen geen schokkende dingen uit. Als er dingen waren geweest waar je nog nooit aan had gedacht dan was het urgenter geweest. Maar dat is niet aan de orde." Respondent F heeft nog een tweetal tips voor de basisscan: "Geef actievere voorbeelden en zorg voor een bredere verspreiding van de basisscan."

Bedrijf G: Wat een gedoe

Schets van het bedrijf

Organisatie G is een onderzoeksbureau. Het bedrijf is gevestigd in Noord-Nederland en is een eenmansbedrijf. Respondent G is eigenaar van het onderzoeksbureau; hij voert allerlei onderzoeken uit voor overheden, private organisaties en andere partijen. Het eerste interview is gehouden op 2 juni 2021 en het tweede interview op 10 juni 2021. Respondent G heeft als associaties met cyberweerbaarheid: "Dat als er iets gebeurt, dat je dan weet wat je moet doen om dit (in het vervolg) tegen te houden." De term cyberweerbaarheid is enigszins nieuw voor de respondent, terwijl hij aangeeft van de technische kant wel op de hoogte te zijn.

Uitgangspositie

Vijf basisprincipes

Respondent G is zich bewust van 'kwetsbaarheden' binnen zijn organisatie. Hij geeft aan te denken over wat hij wel of niet op onlinesystemen als Google Drive en OneDrive zet.[20] "Risicovollere gegevens komen op de harde schijf, het bewustzijn is er." Bedrijf G heeft een werklaptop van een van de noordelijke gemeenten, daardoor vertrouwt hij op de 'instellingen' die daar zijn geïnstalleerd. "Ik verwacht dat die laptop goed beveiligd is, qua [Microsoft] Office en Teams." Respondent G gebruikt deze laptop ook alleen voor zijn werk, zodat het zo 'schoon' mogelijk blijft. 'Updates' gaan ook via de gemeente waarvoor respondent G veel werkzaamheden uitvoert. "Ik doe er zelf helemaal niks aan." 'Toegangsrestricties' ervaart respondent G vooral als irritant. "De gemeente waar ik veel voor werk heeft een wachtwoordbeleid, dat doe ik dan. Maar bij mijn eigen e-mail doe ik het niet vaak. Ik stel het voor mij uit. Vanuit gemakzucht." 'Virussen en malware' wordt eveneens via de systemen van de gemeente buiten de deur gehouden. "Als het niet via de gemeente zou gaan, zou ik er zelf niet zo veel aan doen."

[20] Google Drive en OneDrive zijn voorbeelden van zogenoemde cloud-diensten die gebruikt worden voor online opslag en het delen van documenten.

Factoren houding en (zelf)effectiviteit

Het inzetten op een goede digitale weerbaarheid vindt respondent G overigens wel belangrijk. "Het op orde hebben leidt tot een professionele opstelling richting klanten." Volgens hem kan de (reputatie)schade groter zijn dan de mogelijke investering die digitale weerbaarheid kost. Maar, respondent G geeft aan het een heel saai onderwerp te vinden. Dit resulteert in een gebrek aan motivatie om in te zetten op digitale weerbaarheid. De complexiteit van alles wat zou kunnen helpt volgens respondent G ook niet mee, net als de hoeveelheid. "De situatie moet wel werkbaar blijven, als ik te veel aandacht besteed aan digitale weerbaarheid gaat dit ten koste van mijn overige werkzaamheden." Hij acht de kans klein dat hij slachtoffer kan worden van cybercriminelen: "Van een kale kip kun je niet plukken."

Omgevingsfactoren

"Ikzelf ben de belangrijkste omgevingsfactor." Respondent G geeft aan veel onderzoek te hebben gedaan naar cybersafety, waardoor de kennis om meer te kunnen doen aanwezig is. Respondent G is ook wel eens door een businesspartner of verzekeraar gewezen op bijvoorbeeld wachtwoordgebruik. "Je wordt wel semi-gedwongen om over dit onderwerp na te denken." Vanuit de overheid, buiten een van de vaste afnemers, ervaart respondent G geen stimulansen noch belemmeringen om in te zetten op digitale weerbaarheid. Hetzelfde geldt voor kennispartners. "Ik zou dit over een aantal jaren wel beter geregeld willen hebben."

Op basis van het eerste interview wordt geconcludeerd dat bedrijf G zich bevindt in niveau 3: preparatiefase.

Situatie na de basisscan

Respondent G wilde in beginsel graag meewerken aan een tweede interview, maar bij nader inzien vond de respondent de vraagstelling van de bassiscan van kwalitatief onvoldoende niveau. De respondent had zich eerder, vanuit de beroepsethiek, voorgenomen niet mee te werken aan instrumenten die methodologisch onvoldoende onderbouwd zijn. "Er is te weinig ruimte voor de nuance binnen de organisatie en tussen de medewerkers waardoor met mijn antwoorden op de vragen in de basisscan verkeerde conclusies kunnen worden getrokken."

Bedrijf H: Vertrouwen in Mac-apparatuur

Schets van het bedrijf

Bedrijf H is werkzaam in de reclamebranche. Het bedrijf heeft vijf werknemers en is gevestigd in Zuid-Nederland. Respondent H is eigenaar van het bedrijf. Hij geeft als associaties met cyberweerbaarheid aan: "De mate waarin en de manier waarop je externe factoren en kwaad kan weerstaan en het hoofd kan bieden." Het eerste interview werd gehouden op 6 april 2021 en het tweede interview op 21 april.

Uitgangssituatie

Vijf basisprincipes

Van 'kwetsbaarheden' geeft respondent H aan het belang te onderkennen en hier de nodige actie op te ondernemen. Hij probeert bijvoorbeeld bij het maken van keuzes over de inrichting een paar stappen vooruit te kijken. Ook op het gebied van 'instellingen' is Bedrijf H proactief. Het bedrijf investeert in een firewall en er wordt gewerkt met VPN-verbindingen[21]. 'Updates' worden minimaal een keer per maand handmatig uitgevoerd. Respondent H onderkent het belang van 'toegangsrestricties' en geeft aan hier de nodige aandacht aan te besteden: "Iedereen heeft een eigen inlogcodes en de toegang tot bestanden en systemen is per medewerker gedifferentieerd." Ook wordt er gebruik gemaakt van passwordmanagers[22], waarbij de wachtwoorden bovendien volledig in een digitale omgeving staan. Waar het mogelijk is, wordt er gebruik gemaakt van tweefactorverificatie. Bijvoorbeeld bij PayPal en iCloud.[23] Bij 'virussen en malware' geeft respondent H aan dat er sterk wordt vertrouwd op de automatische updates van de leverancier. Bedrijf H kent een 'Mac-only-policy': "Wij vertrouwen op Apple."

Factoren houding en (zelf)effectiviteit

Respondent H geeft aan dat bedrijfscontinuïteit voor hem van groot belang is, ondanks dat er allerlei zaken afgevuurd worden op het bedrijf. "Het stil komen te liggen van de organisatie is het ergste wat ons kan overkomen. Dit kost tijd en heeft financiële gevolgen." Respondent H vindt het belangrijk om hier actief mee bezig te zijn: "Uitstellen is dus geen optie." Hij probeert het gehele digitale proces beter te doorgronden om daarmee de instellingen beter te kunnen reguleren. Respondent H geeft echter ook aan dat het continu implementeren van nieuwe systemen risico's met zich meebrengt. Het kan altijd misgaan met nieuwe versies. Bijvoorbeeld doordat er nieuwe functionaliteiten zijn, of de software nog niet helemaal 'bug-free' is. Alles moet dan weer opnieuw geconfigureerd worden. Niet alleen in technisch maar ook in sociaal opzicht. De respondent acht zichzelf capabel ten aanzien van cyberweerbaarheid. Hij kent het bedrijf, de software en de instellingen. Waar nodig wordt voor gespecialiseerde kennis aanvullende expertise aangetrokken. Verder vertrouwt het bedrijf op Applesystemen.

Omgevingsfactoren

Respondent H benadrukt nogmaals dat hij als eigenaar zelf bepaalt welk beleid op welke wijze wordt uitgevoerd. Dat de media steeds meer aandacht heeft voor cybercrime, helpt volgens hem voor de bewustwording. Zo heeft hij het boek 'Ik weet je wachtwoord' gelezen en houdt hij regelmatig nieuwsberichten en websites over dergelijke onderwerpen in de gaten. Zo blijft hij op de hoogte en past hij zo nodig zaken binnen het bedrijf aan. Daarnaast vertrouwt Respondent H op geautomatiseerde

[21] VPN staat voor virtueel particulier netwerk en kan worden gezien als een beveiligde of versleutelde verbinding tussen de gebruiker en het internet.
[22] Passwordmanagers zijn een soort digitale kluis waarin wachtwoorden opgeslagen kunnen worden.
[23] PayPal is een onlinebetaalsysteem en iCloud is een cloud-dienst voor de online-opslag van data.

systemen om phishingmails buiten het bedrijf te houden. Hij acht zichzelf daartoe goed in staat en heeft geen behoefte aan nadere bemoeienis van de overheid, bijvoorbeeld op het gebied van wetgeving. Naar aanleiding van dit interview ziet bedrijf H zich in categorie 4: de actiefase.

Situatie na de basisscan

Respondent H heeft aangegeven de basisscan in de week van 16 april te hebben gemaakt. Hij geeft aan iets lager te scoren dan hij van tevoren ingeschat had.

Vijf basisprincipes

Wat betreft de 'kwetsbaarheden', 'toegangsrestricties', 'updates' en 'virussen en malware' heeft Bedrijf H geen aanleiding gezien om aanvullende acties te ondernemen. Het bedrijf heeft wel, niet per se door het maken van de basisscan maar eerder door het eerste interview, een nieuwe server aangeschaft met een up-to-date besturingssysteem. Wat betreft de 'instellingen' geeft de respondent aan dat gebruikersgemak en veiligheid met elkaar op gespannen voet staan. "Als je steeds toestemming moet vragen om in de systemen ergens bij te kunnen werkt dat niet erg motiverend."

Factoren houding en (zelf)effectiviteit

Respondent H geeft zich aan zich nu meer bewust te zijn van de concrete inspanningen die hij (nog) moet doen en dat hij beter weet welke bedreigingen zich kunnen voordoen. Hij vertelt dat inzicht in de meerwaarde voor het inzetten van digitale weerbaarheid wel al aanwezig was. Ook heeft de scan geen nieuwe zwakheden in de organisatie aan het licht gebracht. "Kennis en kunde waren al reeds aanwezig in de organisatie." Respondent H geeft aan dat de scan ook geen nauwkeuriger beeld heeft opgeleverd ten aanzien van de kosten en de tijdsinvestering.

Omgevingsfactoren

Respondent H geeft aan vanuit de overheid weinig stimulansen te ervaren om de digitale weerbaarheid te vergroten. Ook van branchegenoten of brancheverenigingen komt weinig initiatief, vindt hij. Ditzelfde geldt in grote lijnen voor kennisinstellingen met die nuance dat hij de initiatie van DTC en NHL Stenden Hogeschool als een positieve ontwikkeling heeft ervaren. Vanuit banken en verzekeraars ervaart respondent H geen invloed in positieve noch negatieve zin. Een belangrijk inzicht dat respondent H wil delen is: "De complexiteit van software, hardware en regelgeving is de afgelopen tien jaar in razend tempo groter geworden. Er is bovendien veel meer aanbod en alle informatie moet met beperkte tijd en capaciteit gefilterd worden."

Oordeel over de basisscan

Respondent H concludeert dat het niet zozeer de basisscan is geweest die heeft aangezet tot veranderingen in de bedrijfsvoering, maar dat hij hierin wel de bevestiging zag. Niettemin is de respondent iets voorzichter ten aanzien van het ingeschatte gedragsniveau. Aanvankelijk schatte de respondent in dat het om niveau vier ging (actie)

maar nadat de basisscan gemaakt is schat hij in dat fase drie (preparatiefase) toch beter past. Hij is iets kritischer gaan kijken naar de mate van cyberweerbaarheid.

Bedrijf I: Affiniteit met het onderwerp

Schets van bedrijf I

Bedrijf I is een eenmanszaak actief in de projectmanagementbranche. Het is gevestigd in Oost-Nederland. Respondent I is de oprichter van het bedrijf en werkte daarvoor lange tijd voor een grote zakelijke dienstverlener. Tegenwoordig is de respondent actief als zzp'er bij verschillende opdrachtgevers. Als associatie met de term cyberweerbaarheid geeft Respondent I aan dat hij denkt aan een goede beveiliging in het algemeen maar vooral ook bewustzijn rond technische aspecten als malware, phishing en cybercriminaliteit. De respondent geeft aan dat hij daaronder ook de maatregelen verstaat om er geen slachtoffer van te worden: "Dat je oplettend bent en alert blijft."

Uitgangssituatie

Vijf basisprincipes

Met betrekking tot het in kaart brengen van de 'kwetsbaarheden' geeft respondent I aan het belang te onderkennen en ook al de nodige actie te ondernemen. Zo worden de vaste computer, de laptops en de servers regelmatig en professioneel onderhouden. Hij zorgt ervoor dat er ook echt iets mee gebeurt en er niet alleen cosmetische ingrepen worden gedaan. Dit sluit aan bij het basisprincipe 'instellingen' waarvan de respondent ook het belang onderkent en ervoor zorgt dat hij goed op de hoogte is van de juiste en noodzakelijke instellingen. Wat betreft de 'updates' geeft Respondent I aan dat de veiligheidsupdates automatisch plaatsvinden. Functionele updates vinden daarentegen handmatig plaats. Dit gebeurt zeker een keer per maand maar wel onregelmatig: "Ik moet er even aan denken en er dan ook tijd voor hebben." Wat betreft 'toegangsrestricties' geeft Respondent I aan het belang te zien en daar ook naar te handelen, zo bekijkt hij de logboeken op regelmatige basis. Zo nodig wordt een buitenstaander geblokkeerd. Respondent I geeft aan het besturingssysteem Linux te gebruiken en daarom geen aparte antivirussoftware te installeren. Hij ziet wel waarschuwingen. Wat betreft het basisprincipe 'virussen en software' bevindt de respondent zich naar eigen inschatting in de preparatiefase: "Ik moet eigenlijk nog meer actie ondernemen."

Factoren houding en (zelf)effectiviteit

Respondent I geeft aan dat met betrekking tot 'kwetsbaarheden' vooral de tijdsfactor een rol speelt. "Als zzp'er ben je liever bezig met je corebusiness al wil je natuurlijk wel zicht hebben op de 'cyberhygiëne' in je eigen bedrijf." Wat betreft het beheer van de 'instellingen' geeft de respondent aan dat daarvoor niet alleen tijd maar ook de nodige kennis voor nodig is. Hij heeft gelukkig veel verstand van Linux en dat is ook wel nodig. Hij is dus in staat om dit zelf adequaat te installeren en te beheren. Respondent I heeft de administratieve rechten voor al zijn computers, hij snapt wat hij moet doen en weet hoe het zit. Hij is wat dat betreft 'in control'. Wat betreft de 'updates' en

'toegangsrestricties' ziet de respondent als voordeel dat achterdeurtjes tijdig en professioneel worden gesloten. Om er echt zicht op te houden zou er ook meer tijd in gestoken moeten worden hetgeen ook geldt voor de 'virussen en malware'.

Omgevingsfactoren

Respondent I geeft aan dat hij vooral door nieuwsberichten op de hoogte blijft van mogelijke gevaren vanuit cyberspace. Het is niet dat hij wordt belemmerd door de omgeving maar hij vindt het eigenlijk merkwaardig dat er niet vanuit de overheid wordt ingezet op het verstrekken van bijvoorbeeld een antivirusprogramma: "Nu ben je vooral overgeleverd aan de markt en wat betreft instellingen ben je er zelf voor verantwoordelijk." De respondent merkt dat hij door het gebruik van open source-software redelijk op de hoogte blijft van nieuwe ontwikkelingen. Het is wat transparanter en opener. Alles overziend speelt de pers toch wel een belangrijke rol bij het bewustzijn, aldus Respondent I. De verhalen over hacken en gijzelingen werken in die zin wel activerend. "Wat betreft de commerciële partijen moet je erop vertrouwen dat zij hun zaakjes in technisch en organisatorisch opzicht in orde hebben. Als niemand fouten in de software herstelt, kan ik er ook niks aan veranderen." Ook zijn er veel aanbieders en is het voor bedrijf I lastig in te schatten wat de kwaliteit is van de geleverde producten en diensten. Respondent I geeft aan dat er ook andere factoren meespelen zoals nieuwe wetgeving, op het gebied van privacy. "Je moet zelf goed je ogen en oren openhouden maar de overheid moet het ook goed communiceren. Je kunt niet alles weten."

Naar aanleiding van het eerste gesprek ziet Respondent I zich in fase 4: de actiefase. Er is een sterkte mate van bewustzijn en er wordt, op basis van kennis en kunde, de nodige actie ondernomen.

Situatie na de basisscan

Respondent I heeft aangegeven de basisscan op 28 april 2021 te hebben ingevuld. Hij geeft aan in lijn met het eerste interview te scoren, er waren geen grote afwijkingen. Alles was op orde en stond op groen maar als tip kreeg hij mee om een scheiding aan te brengen tussen de netwerken. Volgens Respondent I moet dat goed haalbaar zijn.

Vijf basisprincipes

Wat betreft de basisprincipes geeft Respondent I aan dat hij nogmaals herinnerd is aan het belang van cyberweerbaarheid en hij heeft zich dan ook voorgenomen alle instellingen, de software, en kwetsbaarheden nog eens na te lopen. De door de basisscan aangereikte tip ten aanzien van de scheiding van netwerken neemt hij ter harte.

Factoren houding en (zelf)effectiviteit

Respondent I geeft aan nog dezelfde mate van urgentiebesef te hebben ten aanzien van cyberweerbaarheid, maar hij is zich wel iets bewuster van de inspanningen die hij nog moet leveren. Daarbij verwijst hij naar de aangereikte suggestie. Ook geeft de

respondent aan dat hij zich enigszins bewuster is geworden van de zwakheden van zijn bedrijfsvoering, hetgeen ook geldt voor toekomstige bedreigingen zoals het risico dat hij loopt dat om via de openbare server binnen te dringen. Respondent I weet nu beter wat te doen. Hij heeft de kennis en kunde daarvoor wel in huis dus op dat gebied draagt de basisscan niet zoveel bij. Ook ten aanzien van de kosten is Respondent I niet veel wijzer geworden omdat daar geen aandacht aan besteed wordt. Dit geldt ook voor het tijdsaspect dat aan verdere professionalisering verbonden is.

Omgevingsfactoren

Respondent I geeft aan dat hij meer is gaan letten op uitingen van overheidswege. Hij ziet nu meer 'reclame' voor het onderwerp dan voorheen. Van andere kennisinstellingen hoort hij nog steeds weinig. Respondent I vindt dat zakenpartners, die soms de spelregels bepalen, niet altijd goed omgaan met weerbaarheidsaspecten. Soms wordt hij nog gevraagd om persoonlijke gegevens via de post aan te leveren terwijl dit, mits goed afgeschermd, digitaal in principe veel veiliger zou moeten kunnen.

Oordeel over de basisscan

Respondent I staat neutraal ten aanzien van de basisscan. Aan de ene kant heeft hij een waardevolle tip gekregen maar aan de andere kant mist hij informatie over tijdsaspecten en kosten. Dit zijn belangrijke overwegingen in het bestaan van een zzp'er. De respondent prijst zich gelukkig met de kennis en kunde die hij zelf in huis heeft. Van een verandering van gedragsfase is dan ook geen sprake. De actiefase is nog steeds van toepassing op hem.

Bedrijf J: Urgentiebesef groeit

Schets van Bedrijf J

Bedrijf J is gevestigd in Oost-Nederland en richt zich op websiteontwikkeling, applicatiebeheer en ICT-dienstverlening. Sinds de oprichting in het jaar 2000 is het gegroeid van twee naar tien medewerkers. Het bedrijf kent een uiteenlopende klantenkring qua grootte en naamsbekendheid. Respondent J is directeur-grootaandeelhouder van het bedrijf. Als associatie met de term cyberweerbaarheid geeft respondent J aan dat hij vindt dat de professionaliteit ten aanzien van cybersecurity beter kan binnen zijn bedrijf. Het bedrijf wil ISO-27001 gecertificeerd worden, maar nog onduidelijk is hoe dat gerealiseerd kan worden. Respondent J ziet cyberweerbaarheid als zeer belangrijk, voor nu maar zeker ook voor de toekomst. Hij ziet ook in zijn omgeving dat het vaak slecht gesteld is met de weerbaarheid en ook dat bedrijven niet weten hoe ze hun bedrijfsvoering moeten professionaliseren. Respondent J spreekt in dat verband over 'een tikkende tijdbom'.

Uitgangssituatie

Vijf basisprincipes

Met betrekking tot het in kaart brengen van de 'kwetsbaarheden' en 'updates' geeft respondent J aan dat hij dat belangrijk vindt en dat zijn bedrijf ook al de nodige actie onderneemt. Het bedrijf faciliteert ook webdiensten voor klanten dus het is erg belangrijk dat dat veilig gebeurt. Respondent J spreekt in dat verband van 'Vulnerability Management'[24]. Viermaal per jaar wordt een 'QuickScan' uitgevoerd waaruit een lijst van kwetsbaarheden volgt. Vooral bij de ontwikkeling van nieuwe diensten ziet de respondent echter dat het veiligheidsniveau moet worden opgeschroefd.

Wat betreft de 'instellingen' geeft respondent J eveneens aan het belang te onderkennen en reeds de nodige actie te ondernemen. Zo zorgen zij voor tweefactorverificatie en encryptie[25] van de harde schijven. Ook wordt toegezien op het gebruik van sterke wachtwoorden. Patchmanagement, de laatste versie van software installeren, wordt ook actief uitgevoerd. De respondent geeft echter aan dat binnen zijn kleine bedrijf wel meer beleving zou moeten zijn ten aanzien van adequaat computerbeheer. Met betrekking tot 'toegangsrestricties' refereert respondent J aan de passwordmanagers. Verbetering ziet hij in het beleid rondom 'least privilege' (zo min mogelijk medewerkers kunnen bij bepaalde bestanden) en 'LastPass' (een type passwordmanager). Aan 'virussen en malware' besteedt respondent J nog (te) weinig tijd en aandacht. Vooral de menselijke component, onder andere het klikken op linkjes, vraagt om meer urgentiebesef.

Factoren houding en (zelf)effectiviteit

Respondent J geeft aan dat hij als adagium heeft dat er pas echte kwetsbaarheden zijn als je ze niet herkent. "Je moet dus up-to-date blijven en actief zijn met het aanbrengen van verbeteringen." Elke verandering brengt ook weer potentiële nieuwe zwakten en bedreigingen met zich mee, aldus respondent J. Het bijhouden en monitoren van nieuwe ontwikkelingen kost veel tijd en geld. Ook moet voldoende kennis aanwezig zijn en duidelijk zijn welke verbeteringen wel en welke niet doorgevoerd moeten worden. Ook geeft respondent J aan dat niet iedereen in de organisatie er te veel mee belast moet worden en dat het daarom extra belangrijk is om de basisconfiguraties goed te documenteren. Het belangrijkste op korte termijn is dat er geen 'achterdeurtjes' meer openstaan. Omdat medewerkers verschillende belangen en achtergronden hebben, kan niet van iedereen hetzelfde gedrag worden verwacht. Het ICT-beheer moet slim worden ingericht en er moet flexibel gehandeld kunnen worden. "Klanten verwachten dat trouwens ook." Respondent J ziet een duidelijk spanningsveld tussen wendbaarheid en creativiteit (het echte bestaansrecht) van de organisatie enerzijds en strikt beheer

[24] Vulnerability Management (vrij vertaald: kwetsbaarheidsbeheer) betreft een cyclisch proces van identificeren, classificeren, prioriteren, herstellen en verminderen van softwarekwetsbaarheden.
[25] Encryptie, ofwel versleuteling, betreft het coderen (versleutelen) van gegevens op basis van een bepaald algoritme.

anderzijds. "Er moet een goede balans tussen deze twee gevonden worden." Respondent J geeft aan dat hij inschat dat zijn bedrijf hoger scoort dan het gemiddelde in de branche. Om nog beter te scoren zal veel extra geïnvesteerd moeten worden. Het uurtarief zal omhoog moeten om een betere kwaliteit van dienstverlening aan te bieden waartegenover dan het vertrouwen in de organisatie staat. De vraag is of investeerders en klanten de extra kosten hiervan zullen accepteren. Wat dat betreft lijkt het Respondent J een aardig idee om te kijken of vanuit overheidswege een soort veiligheidslabel ontwikkeld kan worden.

Omgevingsfactoren

Respondent J geeft aan dat met name de klantwensen hem stimuleren om de cyberweerbaarheid te vergroten. Hij wil zijn klanten beloven om het beter doen dan de concurrenten. "Imagoschade wil je zeker niet oplopen." Respondent J ziet voor zijn eigen bedrijf kansen om veiligheidsdiensten te verrichten voor nieuwe klanten. Die kunnen dan verder met hun corebusiness. Respondent J is voorts van mening dat vanuit opleidingsinstituten te weinig aandacht wordt geschonken aan digitale weerbaarheid. Volgens hem is immers niet ieder bedrijf in staat om gespecialiseerde werknemers in dienst te nemen. Respondent J vindt het prettig als hij door klanten wordt gewezen op mogelijke zwakheden. Hij heeft echter de indruk dat dat niet altijd gebeurt, hetgeen als een gemiste kans beschouwd kan worden. "Men zou wat scherper op elkaar kunnen zijn, wat dat betreft verwacht je wat meer druk vanuit de keten." Daarbij ziet de respondent dat het inhuren van kennis het risico met zich meebrengt dat je steeds meer geld kwijt bent aan onderhoud en beheer. "Waar stop je op een gegeven moment?" Daarnaast is factureerbaarheid een belangrijk issue. Elk uur besteed aan interne ICT betekent minder omzet. Dat is dus zoeken naar een balans. Wat dat betreft zou het goed zijn als er subsidies in het leven zouden worden geroepen om de eerste hobbels weg te nemen. Van meer regulering en wetgeving verwacht respondent J niet veel. Dat verhoogt alleen maar de regeldruk en ook handhaving is een issue. Het bedrijf zal zelf 'calculated risks' moeten nemen.

Naar aanleiding van het eerste gesprek ziet Bedrijf J zich in fase 4: De actiefase. Men is zich bewust van het belang van cyberweerbaarheid. Veel noodzakelijke acties zijn al ondernomen, maar qua bewustzijn kan nog het nodige verbeterd worden.

Situatie na de basisscan

Vijf basisprincipes

Respondent J heeft aangegeven de basisscan op 11 mei 2021 te hebben gemaakt. Ten aanzien van de nulmeting ziet Respondent J weinig verandering. Het bevestigt zijn eigen beeld en de basisscan heeft hem niet echt nieuwe inzichten opgeleverd. Omdat respondent J naar eigen zeggen altijd vrij kritisch is, was hij daar zelf wel tevreden over. Als tip kreeg hij mee om een scheiding aan te brengen tussen de verschillende netwerken, hetgeen volgens respondent J goed haalbaar moet zijn. Op het gebied van 'virussen en malware' bleek ook dat aanvullende acties ondernomen kunnen worden. Tot

concrete actie heeft dit nog niet geleid. Hij denkt wel dat in de toekomst een nieuwe virusscanner gekocht gaat worden. Het bedrijf wil er alles aan doen om de producten voor hun afnemers zo veilig mogelijk te houden.

Factoren houding en (zelf)effectiviteit

Respondent J geeft aan meer zicht te hebben op de inspanningen die gedaan moeten worden op het gebied van digitale weerbaarheid. Daarentegen heeft de basisscan geen invloed gehad op kennis van zwakheden in de organisatie: "Kennis en kunde is aanwezig." Respondent J heeft geen nieuw inzicht gekregen in de mate van toekomstige bedreigingen. Ook geldt dit voor de kosten in zowel tijd als geld. Wel heeft respondent J het gewaardeerd dat de basisscan hem een spiegel heeft voorgehouden. De kennis werd eigenlijk bevestigd maar hij vindt de scan te globaal voor diepere inzichten.

Omgevingsfactoren

Respondent J geef aan niet zelf direct te worden gestimuleerd van overheidswege anders dan via de AVG. Ditzelfde geldt grosso modo voor kennisinstellingen. Hij weet dat er van alles gebeurt vanuit het onderwijs en onderzoek maar concreet is dat nog niet voor hem van waarde gebleken. Branchegenoten in de ICT-sector daarentegen zijn wel een stimulerende factor. Ditzelfde geldt voor zakenpartners. "Je bent ook in concurrentie dus je moet je qua cyberweerbaarheid ook onderscheiden." Respondent J zou baat hebben bij een duidelijke roadmap c.q. stappenplan richting ISO-certificering. Daarbij speelt een gebrek aan vertrouwen in partijen die daarbij kunnen helpen. Hij weet niet hoe betrouwbaar deze partijen zijn en hoeveel tijd en geld dit gaat kosten. "Het is bij zo'n certificering wel alles of niets dus je moet wel weten hoeveel tijd en geld een en ander gaat kosten." Daar zou volgens hem een rol van de overheid kunnen liggen.

Oordeel over de basisscan

Respondent J geeft aan dat er geen verandering van fase is geweest. Het bedrijf zit nog steeds in fase 4: de actiefase. "Concrete gedragsverandering vergt meer tijd." Wat betreft de basisscan geeft respondent J aan dat de deze wel 'heel hoog over' is. Er valt eigenlijk alleen een basisniveau vast te stellen. De waarde voor bedrijf J is beperkt, men is al dagelijks bezig met de cyberweerbaarheid. Als de scan meer interactief zou zijn geweest en meer diepgang had geboden (bijvoorbeeld door mogelijkheden tot doorvragen) dan was er duidelijk sprake geweest van meerwaarde, zeker als deze dan ook nog concrete tips had opgeleverd.

Bedrijf K: Klanten gaan voor

Schets van bedrijf K

Bedrijf K is al jaren actief in de watersportsector. Het handelt in nieuwe en tweedehands boten en buitenboordmotoren. Het bedrijf is gevestigd in Noord-Nederland. Respondent K is de eigenaar van het bedrijf en werkt nauw samen met een compagnon die het technische onderhoud van het materiaal verzorgt. Het eerste interview is afgenomen op 20 mei 2021 en het tweede interview op 2 juni 2021. Als associatie met de term

cyberweerbaarheid geeft respondent K aan dat hij vooral denkt aan de mate waarin mensen en bedrijven zich willen weren tegen aanvallen en bedreigingen van buitenaf. Het gaat hem dus niet alleen om technische aspecten, maar ook over de mate van bewustzijn en het ontwikkelen van een alerte houding.

Uitgangssituatie

Vijf basisprincipes

Met betrekking tot het in kaart brengen van de 'kwetsbaarheden' geeft de respondent aan dat hij zichzelf ziet als de meest kwetsbare schakel. Respondent K is hier echter heel alert op, hij krijgt zeker een keer per dag een verdacht bericht. Meestal via sms en mail maar soms ook via Whatsapp: "Genoeg reden om niet overal in mee te gaan en om alert te blijven." In termen van fasering stelt hij dus dat hij het belang onderkent en de nodige actie onderneemt. Wat betreft 'instellingen' geeft hij aan dat zijn bedrijf iets scherper zou kunnen opereren. Hij is hier nog niet echt mee bezig, maar heeft daar wel de intentie toe. Hij vertrouwt er grotendeels op dat zijn apparatuur (Apple) verdachte zaken blokkeert. "Tot nu toe is er nog geen urgentie geweest." Wachtwoorden en instellingen veranderen doet hij marginaal. Respondent K geeft aan dat hij hier 'slecht' in is. Wat betreft 'updates' geeft respondent K aan dat iOS automatisch in de nacht updates verzorgt. Hij vertrouwt hier grotendeels op, maar controleert wel of de patches ook daadwerkelijk zijn binnengekomen en zijn geïnstalleerd: "Zo blijf ik beschermd tegen bedreigingen van buitenaf." Respondent K is zich dus bewust van de gevaren en onderneemt de nodige actie. Dit geldt ook voor 'toegangsrestricties' waarbij respondent K direct aangeeft dat hij zelf degene is die alles beheert. "Ik gebruik sterke wachtwoorden, combinatie van letters cijfers en tekens die niet voor de hand liggen." Wat betreft het basisprincipe 'virussen en malware' bevindt de respondent zich ook in de actiefase. Hij geeft aan dat Apple een gesloten omgeving is en gaat er dus vanuit dat het systeem geen scans uitvoert op softwarematig gebied. Zijn eigen alertheid is leidend in wat hij online doet. "Ik weet waar en bij wie ik inkoop en met wie ik zakendoe."

Factoren houding en (zelf)effectiviteit

Respondent K geeft aan dat zijn adagium is: voorkomen is beter dan genezen! Daarbij vermeldt hij direct dat het ook veel tijd en energie kost om alles helemaal goed te doen. Hij vindt het dan ook niet echt een leuk onderwerp om mee bezig te zijn en ziet het daarom echt als een investering: "Als je het goed voor elkaar hebt, heb je statistisch minder kans om slachtoffer te worden, zo moet je maar denken." Het voordeel van iOS vindt hij dat veel automatisch gaat. Hij hoeft alleen maar te checken. Mocht er toch iets aan de hand zijn, dan is het voldoende om alert te zijn en direct de nodige actie te ondernemen. "Als je het niet interessant of te moeilijk vindt heb je wel een probleem want dan komt het onderaan de prioriteitenlijst." Respondent K wil hiervoor waken. Zijn bedrijf is niet complex, en hij kan bij bevriende ondernemers en kennissen terecht voor advies, maar respondent K kan zich voorstellen dat het bij grotere bedrijven ingewikkelder is. "Opsporen is de kern, je bent zelf de poortwachter en dus verantwoordelijk."

Omgevingsfactoren

Respondent K acht zichzelf in staat om de nodige maatregelen te nemen tegen toekomstige bedreigingen. Hierbij voelt hij zich gesteund door de ontwikkelingen in de techniek: "het wordt steeds gebruiksvriendelijker, aan de andere kant kunnen criminelen natuurlijk ook weer op sluwe wijze gebruik maken van nieuwe technieken om je geld afhandig te maken." Respondent K geeft aan goed kennis te nemen van verhalen uit zijn directe omgeving. "Als je met collega-bedrijven, kennissen of familie spreekt over [digitale] dreigingen word je vanzelf alerter. Je wilt niet dat jou hetzelfde overkomt." Zakenpartners belemmeren Respondent K niet, eerder voelt hij zich gestimuleerd. "Je hebt het er wel eens over waardoor de alertheid ook weer toeneemt."

Naar aanleiding van het eerste gesprek ziet bedrijf K zich in fase 4: de actiefase. Er is een sterke mate van bewustzijn en er wordt, op basis van alertheid en naar bewind van zaken, de nodige actie ondernomen.

Situatie na de basisscan

Respondent K heeft aangegeven de basisscan op 25 mei 2021 te hebben uitgevoerd. De uitkomsten komen grotendeels overeen met de bevindingen uit het eerste interview. Hij ziet bevestigd dat zijn bedrijf ingeschaald kan worden in fase 4: de actiefase.

Vijf basisprincipes

Wat betreft de basisprincipes geeft Respondent K aan nog geen verdere actie te hebben ondernomen. "Het heeft op dit moment simpelweg geen prioriteit, het is druk in de zaak vanwege de start van het watersportseizoen en al mijn aandacht gaat uit naar de klanten." De tip die hij kreeg ten aanzien van multifactorverificatie was waardevol maar heeft hij nog niet kunnen uitvoeren.

Factoren houding en (zelf)effectiviteit

Respondent K geeft aan dat de basisscan, in combinatie met de interviews, meerwaarde heeft in de zin dat hij het belang van cyberweerbaarheid nog meer inziet. Ook weet de respondent nu beter wat hij concreet moet doen en welke kennis en kunde daarvoor nodig is. De basisscan heeft hem echter geen nieuwe inzichten opgeleverd over de zwakheden binnen zijn organisatie en de toekomstige bedreigingen: "die had ik immers wel al in de gaten." Wat verdere professionalisering gaat kosten in termen van geld en tijd blijft voor hem ook nog erg onduidelijk.

Omgevingsfactoren

Respondent K geeft aan dat hij, na het maken van de basisscan geen verschil ziet in de mate waarin de overheid een rol speelt in de bewustwording rondom cyberweerbaarheid. Wel ziet hij dat branchegenoten steeds actiever worden en kennis delen. Tevens spreekt Respondent K zijn waardering uit voor participatie in dergelijk onderzoeken van een kennisinstelling, "waarbij je op een positieve manier naar je eigen

bedrijf kijkt." Respondent K is niet anders gaan oordelen over de stimulerende dan wel belemmerende invloed van zakenpartners. Wel is respondent K, door een incident in zijn directe omgeving, nogmaals met zijn neus op de feiten gedrukt.

Oordeel over de basisscan

Alles overziend concludeert Respondent K dat hij neutraal staat ten aanzien van de basisscan. Het is een goede spiegel, maar voor het doorvoeren van vervolgacties geldt dat de tips niet concreet genoeg ware. Daarbij is het prioriteitsbesef op dit moment afwezig. "Het is gewoon een heel erg drukke tijd, waarin de focus ligt op het primaire proces: ik wil klanten helpen."

Bedrijf L: Wij voelen ons verantwoordelijk

Schets van bedrijf L

Bedrijf L is actief in de advertentie-branche. Het bedrijf werkt met vijf vaste zzp'ers. Het kantoor is gevestigd in het westen van het land. De respondent is (mede)eigenaar van het bedrijf. Het eerste interview is gehouden op 19 april 2021 en het tweede interview op 26 april 2021. Respondent L benoemt als associaties met cyberweerbaarheid: "De manier waarop het bedrijf is beschermd tegen de buitenwereld en tegen mensen die het bedrijf kwaad willen doen." Daarbij vervolgt Respondent L: "Voor de meeste werkzaamheden gebruikt het bedrijf software van derden waardoor we vertrouwen moeten hebben dat deze bedrijven de cyberweerbaarheid goed op orde hebben." Het bedrijf is zich uitermate bewust dat cyberweerbaarheid tegenwoordig hoog op de agenda moet staan.

Uitgangssituatie

Vijf basisprincipes

Bedrijf L bereidt zich voor om concrete acties te ondernemen met betrekking tot het in kaart brengen van 'kwetsbaarheden'. De software die het bedrijf gebruikt om werkzaamheden uit te voeren, moeten zij ook kunnen vertrouwen. Via klanten wordt namelijk geld uitgegeven op platforms op internet." Wij voelen ons hiervoor verantwoordelijk." Respondent L denkt dat door het gebruik van Apple-computers er minder kans is op kwetsbaarheden in het systeem. Ten aanzien van 'instellingen' heeft het bedrijf nog geen harde actie ondernomen maar het belang hiervan wordt wel ingezien. Respondent L gebruikt 'Last Pass' waardoor geen standaardwachtwoorden gebruikt worden. Hij gebruikt waar nodig ook 'verificatiecodes'. Het uitvoeren van 'updates' wordt volgens Respondent L stelselmatig gedaan. Ook benoemt hij opnieuw dat het bedrijf afhankelijk is van software van derden. "Als deze software niet naar behoren werkt, is er kans om slachtoffer te worden van cybercriminaliteit." Het aanbrengen van 'toegangsrestricties' is een belangrijk onderdeel van de bedrijfsvoering. De eigenaren van het bedrijf hebben administratierechten, andere medewerkers kunnen geen aanpassingen doen. Sommige zakenpartners gaan volgens Respondent L laks om met toegangsrestricties waardoor onnodig derden bij gegevens kunnen komen. Bedrijf L helpt hen hier bewuster mee om te gaan. Tenslotte onderkent het bedrijf het belang

om 'virussen en malware' buiten te deur te houden. Het bedrijf werkt met een gesloten 'source' en denkt zo minder snel slachtoffer te worden van cybercriminaliteit. Wel ontvangt hij vaak phishingmails, die over het algemeen in de spambox belanden.

Factoren houding en (zelf)effectiviteit

Respondent L geeft aan dat gebruiksvriendelijkheid zeer belangrijk is in het bedrijf. De medewerkers loggen vaak in en uit op verschillende softwareprogramma's en moeten snel kunnen schakelen. Dan is het wel een obstakel als steeds verschillende verificatiestappen gezet moeten worden. "Iedereen gaat zorgvuldig om met gevoelige gegevens. Klanten geven ons ook toegang tot betaalgegevens. Hierdoor moet vertrouwelijk te werk worden gegaan." Alle werkzaamheden worden uitgevoerd via Apple-apparatuur. Respondent L vindt dat de meest veilige manier van werken. Bedrijf L moet zich naar de klant kunnen verantwoorden als er iets verkeerd gaat op het gebied van cyberweerbaarheid.

Omgevingsfactoren

Respondent L benoemt zakenpartners zowel als belemmering als stimulans. "Het bedrijf is afhankelijk van de grote netwerken waarmee samengewerkt wordt. Daardoor zijn er niet veel mogelijkheden om zelf te kunnen kiezen welke software door het bedrijf gebruikt kan worden." Hij stimuleert medewerkers om alert te zijn op eigen cyberweerbaarheid. Respondent L geeft aan sterk te vertrouwen op de kennis en kunde van zijn mede-eigenaar.

Op basis van het eerste interview wordt geconcludeerd dat het bedrijf zich in fase 4 bevindt: de actiefase. De hoogste prioriteit is dat het bedrijf veilig kan werken op andere netwerken om zo de beste resultaten te leveren aan klanten.

Situatie na de basisscan

Vijf basisprincipes

Respondent L geeft aan op 21 april 2021 de basisscan ingevuld te hebben en dat de uitslag grotendeels overeenkwam met zijn verwachtingen. "Niet alle basisprincipes bleken echter goed meetbaar te maken voor mijn bedrijf." Bedrijf L is immers afhankelijk van klanten die opdrachten verstrekken. De respondent geeft aan dat in de toekomst alle basisprincipes nog belangrijker worden. Er is actie ondernomen ten aanzien van inventariseren van 'kwetsbaarheden'. De uitkomsten van zowel het interview als de basisscan zijn besproken met de andere eigenaar. "Er is besloten om een harde schijf aan te schaffen. Hier worden alle documenten op verzameld in plaats van in de 'cloud'. Hierdoor loopt het bedrijf minder kans op inbreuk op de systemen." Voor de overige basisprincipes 'instellingen', 'updates', 'toegangsrestricties' en 'virussen en malware' zijn (nog) geen concrete acties uitgevoerd. Eerst moeten de eigenaren met elkaar om tafel om dit verder te bespreken.

Factoren houding en (zelf)effectiviteit

Respondent N geeft aan zich, naar aanleiding van de basisscan ten meer bewust te zijn van de meerwaarde van het inzetten op digitale weerbaarheid. Ook weet hij beter welke inspanning de organisatie nog moet verrichten en welke bedreigingen er zijn. Daarentegen heeft de basisscan geen of weinig verandering gebracht in de kennis van zwakheden in de organisatie en de kennis en kunde die in huist gehaald moeten worden. Ook ontbreekt nog een nauwkeuriger beeld van het kostenplaatje en de tijdsindicatie.

Omgevingsfactoren

Door dit onderzoek, waarvan de basisscan onderdeel is, is Respondent L zich bewuster van het belang van cyberweerbaarheid. Stimulansen komen vooral uit de technische- en sociale netwerken. Grote partijen hebben cyberweerbaarheid goed op orde en deze worden door ons als voorbeelden gezien, aldus Respondent L.

Oordeel over de basisscan

Ten aanzien van de basisscan concludeert Respondent L dat het instrument een bijdrage heeft geleverd aan inzicht in het bedrijf en de noodzakelijke vervolgstappen. Voor concrete verdere acties moeten de eigenaren eerst beter met elkaar in overleg. In de toekomst kunnen meer veranderingen doorgevoerd worden maar specifieke veranderingen kunnen op dit moment dus nog niet gedefinieerd worden. Tot een verandering in gedragsfase heeft de basisscan, waarover Respondent L verder ook geen expliciet oordeel heeft, nog niet geleid.

Bedrijf M: Weinig online, dus beperkte risico's

Schets van Bedrijf M

Bedrijf M is een montagebedrijf dat gespecialiseerd is in interieurbouw. Het is een eenmanszaak, gevestigd in Noord-Nederland. Het eerste interview is gehouden op 21 april 2021 en het tweede interview op 19 mei 2021. Associaties van Respondent M bij de term cyberweerbaarheid: "Dat cybercriminelen niet inbreken op de website van het bedrijf. Ook dat goede wachtwoorden gebruikt worden en zo persoonsgegevens beschermd worden." De respondent geeft aan niet continu aandacht te besteden aan cyberweerbaarheid omdat werkzaamheden fysiek gebeuren waarbij het gebruik van internet een ondergeschikte rol speelt. Daarnaast denkt Respondent M niet aantrekkelijk te zijn voor cybercriminelen.

Uitgangssituatie

Vijf basisprincipes

Wat betreft het in kaart brengen van 'kwetsbaarheden' geeft de respondent aan hierin voorbereidingen te treffen maar op dit moment te volstaan met een goede scanner op de computer en websitebeveiliging door een extern bedrijf. Het beheren van 'instellingen' vindt respondent M belangrijk. Hij denkt ten aanzien van 'updates' vergevorderd te zijn. "Automatisch updaten en werken met de laatste versies is volgens mij voldoende op dit moment." Van 'toegangsrestricties' onderkent hij het belang. Zo

wordt er gebruik gemaakt van Apple-computers en de functie 'wachtwoordvoorstellen', waarbij sterke wachtwoorden vereist worden. Er is een incident geweest waarbij e-mails door onbevoegden werden verstuurd. Dit is destijds door het externe bedrijf opgelost. Als het gaat om 'virussen en malware' vindt hij dat het bedrijf eveneens vergevorderd is. Er draaien continu virusscanners op de computers. De respondent ziet de noodzaak van cyberweerbaarheid, maar zet het niet bovenaan de prioriteitenlijst.

Factoren houding en (zelf)effectiviteit

Respondent M geeft aan het belang in te zien van goede beveiliging voor het gebruik van het internet. "Dat je geen gekke virussen en inbraken hebt op eigen website en boekhoudprogramma's." De respondent ziet in dat sommige acties permanent genomen moeten worden. Zoals een virusscanner, updates uitvoeren en het gebruik van verschillende wachtwoorden. Apple-computers gebruiken ook vingerafdrukdetectie zodat onbevoegden niet kunnen inloggen op de computers.

Omgevingsfactoren

Respondent M geeft aan dat het bedrijf gestimuleerd wordt door mediaberichten. "Er gebeuren cyberincidenten bij andere bedrijven waardoor wel een vorm van alertheid ontstaat." Respondent M acht de kans klein dat dit binnen het bedrijf gebeurt. Hij schat in dat hij voldoende doet om veilig te werken. De website vormt het grootste risico voor cybercriminaliteit, daarvoor is nu dat externe bedrijf verantwoordelijk.

Op basis van het eerste interview wordt geconcludeerd dat Bedrijf M zich bevindt in fase 4: de actiefase. Het bedrijf is niet continu bezig met cyberweerbaarheid, maar neemt wel zo veel mogelijk verantwoordelijkheid als het gaat om veilig werken.

Situatie na de basisscan

Vijf basisprincipes

Respondent M heeft op 16 mei 2021 de basisscan ingevuld. De uitkomsten van de basisscan waren overeenkomstig met de resultaten uit het eerste interview. Alle basisprincipes waren op orde. Hij begrijpt dat bij een groter bedrijf meer medewerkers verantwoordelijkheden hebben. Dat medewerkers moeten weten hoe zij veilig kunnen werken en omgaan met wachtwoorden. In dit bedrijf wordt het beheer daarvan door de respondent zelf uitgevoerd en hij neemt daarvoor ook alle verantwoording. Als het gaat om acties ten opzichte van de basisprincipes is een controle uitgevoerd of alles naar behoren werkt, zoals de virusscanner. Respondent M vindt dat alles op orde is en is daarom niet van plan iets te veranderen op het gebied van de basisprincipes.

Factoren houding en (zelf)effectiviteit

Respondent M geeft aan zich, naar aanleiding van de basisscan meer bewust te zijn van de meerwaarde om in te zetten op digitale weerbaarheid en de inspanningen die hij zou kunnen verrichten. Ook heeft hij nu wat meer kennis van de zwakheden en inzicht in de benodigde kennis en kunde. Respondent M denkt dat de basisscan hem beter in staat

stelt om bedreigingen tegen te gaan. Over toekomstige bedreigingen en het kostenplaatje in termen van geld en tijd is hij echter niet veel wijzer geworden.

Omgevingsfactoren

De basisscan heeft geen verandering gebracht naar de manier waarop de respondent aankijkt tegen invloed van de omgeving. In het eerste interview kwam naar voren dat verhalen uit de media een stimulans zijn. Bedrijf M ervaart belemmeringen noch stimulansen vanuit de overheid, kennisinstellingen en branchegenoten. Ook andere actoren, wellicht uitgezonderd de media, spelen geen rol van betekenis voor Respondent M.

Oordeel over de basisscan

Respondent M concludeert dat de basisscan heeft bijgedragen aan het regelmatig controleren van de instellingen op eigen computers. Tot een verandering in gedragsfase heeft het bij hem (nog) niet geleid. Doordat alle basisprincipes op orde waren, ziet de respondent de noodzaak niet in om aanvullende actie te ondernemen. Respondent M vond de basisscan duidelijk.

Bedrijf N: Inzetten op digitale vaardigheden

Schets van bedrijf N

Bedrijf N is een technische groothandel in producten voor de maakindustrie. Het bedrijf heeft ongeveer zestig mensen in dienst en is gevestigd in Noord-Nederland. De respondent is mede-eigenaar van de onderneming en maakt deel uit van het managementteam. Het eerste interview is gehouden op 22 april 2021 en het tweede interview op 10 mei 2021. Als associaties met cyberweerbaarheid noemt Respondent N: "De manier waarop men omgaat met bedreigingen vanuit verschillende soorten cybercrimedelicten." In hoeverre is ons bedrijf daar resistent voor, dat is de vraag. De digitale vaardigheden zijn onvoldoende ontwikkeld binnen het bedrijf terwijl er meerdere situaties zijn geweest waarbij cybercriminelen hebben geprobeerd om binnen te komen." Respondent N weet uit eigen ervaring wat de impact is van cybercriminaliteit.

Uitgangssituatie

Vijf basisprincipes

Respondent N is zich bewust van het basisprincipe in kaart brengen van 'kwetsbaarheden'. Het beleid in het bedrijf is veranderd: hardware en software zijn nu uitbesteed aan een externe systeembeheerder. Dit komt omdat het bedrijf meerdere malen slachtoffer is geweest van cybercriminaliteit. Een voorbeeld hiervan is dat er een vorm van CEO-fraude is gepleegd. Hierbij is een fors bedrag naar een buitenlandse rekening overgeschreven. Gelukkig kon het geld nog via de bank worden teruggestort. Ten aanzien van het beheren van 'instellingen' is Bedrijf N hier niet zelf mee bezig, maar onderkennen zij wel degelijk het belang hiervan. De systeembeheerder houdt bij of

ongebruikelijke transacties of gebeurtenissen plaatsvinden. Ook het uitvoeren van 'updates' is voor Bedrijf N van wezenlijk belang. In het bedrijf wordt dit zowel geautomatiseerd als handmatig uitgevoerd. De handmatige updates worden uitgevoerd omdat sommige aangegeven tijden niet goed uitkomen. Met 'toegangsrestricties' is Bedrijf N nog niet bezig. "Wij hebben wel de intentie om te professionaliseren." Respondent N geeft aan dat wachtwoorden slecht onthouden worden. Dat betekent dus dat een vorm van wachtwoordbeheer ingesteld moet worden, zoals het inzetten van passwordmanagers. Ten slotte beseft Bedrijf N dat het van belang is om 'virussen en malware' buiten de deur te houden. Hiervoor is nu de externe systeembeheerder verantwoordelijk.

Factoren houding en (zelf)effectiviteit

Respondent N geeft aan dat bedrijfscontinuïteit een topprioriteit is. "Verschillende inbreuken in het bedrijf hebben geleid tot het besef dat alles op alles gezet moet worden om incidenten te vermijden. Hiervoor is budget vrijgemaakt en is expertise ingehuurd." Voorafgaand moeten medewerkers extra handelingen uitvoeren, zoals het regelmatig wijzigen van (standaard) wachtwoorden en het gebruikmaken van tweefactorverificatie. Daarnaast wil het bedrijf te weten komen waar de risico's liggen. "Door het uitvoeren van updates en door gebruik van virusscanners beperkt het bedrijf de risico's." Binnen het bedrijf zijn toegangsrestricties aanwezig, waardoor de vertrouwelijkheid van informatie gewaarborgd blijft.

Omgevingsfactoren

Respondent N geeft aan de aanvallen van buitenaf een stimulans zijn geweest om het thema cyberweerbaarheid op de agenda te zetten. Hij verwacht dat het bedrijf ook de komende jaren met cybercriminaliteit te maken zal krijgen, vandaar dat voor een strategische benadering is gekozen. Door de systeembeheerder wordt bedrijf N gestimuleerd om tweefactorverificatie toe te passen. Volgens Respondent N komen de voornaamste kwetsbaarheden binnen het bedrijf door medewerkers die niet op tijd updates laten uitvoeren of uit naïviteit reageren op mails. "Ik kan daarom niet uitsluiten dat cybercriminelen alsnog weten binnen te dringen."

Op basis van het eerste interview is geconcludeerd dat het bedrijf zich bevindt in fase 3: de preparatiefase. De hoogste prioriteit is het bewustzijn van medewerkers verhogen en daarbij de cyberweerbaarheid te versterken. "Wij denken hierbij aan het inzetten van een e-learning of informatieve presentaties."

Situatie na de basisscan

Vijf basisprincipes

Respondent N geeft aan dat hij op 10 mei 2021 de basisscan heeft ingevuld en dat de score overeenkwam met zijn verwachtingen. "De adviezen die werden gegeven lagen in lijn met de uitkomsten van het eerste interview." Dit geldt bijvoorbeeld voor het principe 'kwetsbaarheden'. Uit de basisscan kwam naar voren dat de basisprincipe 'instellingen'

nog niet op orde is. Naar aanleiding van de 'updates' zijn back-ups gemaakt van bestanden. "Dat moet regelmatig gaan gebeuren. In die zin is er wel actie ondernomen." Respondent N heeft met de systeembeheerder gesproken over het eerste interview. De systeembeheerder gaf een bevestiging dat het wachtwoordbeleid binnen het bedrijf verbeterd moet worden. Dit valt onder de basisprincipe 'toegangsrestricties'. Wat betreft 'virussen en malware' hebben geen wijzigingen plaatsgevonden. Dit ligt bij de externe beheerder. De intentie van het bedrijf is om met de hiervoor genoemde verbetermogelijkheden aan de slag te gaan. De basisscan geeft een bevestiging dat het bedrijf met de basisprincipes aan de slag moet. "Dat gebeurt nu met meer prioriteit."

Factoren houding en (zelf)effectiviteit

Respondent N ziet nu meer de meerwaarde van digitale weerbaarheid voor zijn organisatie in. Ook is het voor hem duidelijker geworden welke inspanningen nog geleverd moeten worden. Hij geeft aan dat er nu meer kennis is over toekomstige bedreigingen. Daarentegen heeft de scan weinig of geen verandering gebracht in kennis van de zwakheden en welke kunde nog in huis gehaald moet worden. Ook is er geen nauwkeuriger beeld over wat het gaat kosten, zowel qua tijd als qua financiën. Hij heeft geen vernieuwde kennis opgedaan over toekomstige bedreigingen.

Omgevingsfactoren

Respondent N geeft aan dat deelname aan dit onderzoek (waarvan de basisscan onderdeel is) heeft bijgedragen aan een verhoogd niveau van alertheid. Hij is gestimuleerd om meer in te zetten op digitale weerbaarheid. Dit was tevens de eerste keer dat hij vanuit een onderwijsinstelling is benaderd voor een dergelijk onderzoek. Andere actoren die van belang zouden kunnen zijn worden door Respondent N niet onderscheiden.

Oordeel over de basisscan

Respondent N concludeert dat de basisscan heeft geholpen om inzichten te verkrijgen in de acties die ondernomen moeten worden om het bedrijf beter bestand te maken tegen aanvallen van buitenaf. Tot een verandering in gedragsfase heeft dat (nog) niet geleid. "Het tijdsbestek was te kort om veranderingen daadwerkelijk door te voeren, maar we geven er meer prioriteit aan."

Bedrijf O: Wakker geschud door de media

Schets Bedrijf O

Bedrijf O is een eenmanszaak en biedt sportlessen aan. Het bedrijf is gevestigd in Noord-Nederland. Het eerste interview is gehouden op 26 april 2021 en het tweede interview op 10 mei 2021. "Bij cyberweerbaarheid denk ik aan dat er veilig op de laptop gewerkt kan worden zonder dat criminelen deze kunnen hacken of andere dingen kunnen uithalen." Respondent O geeft aan er nooit bij stil te hebben gestaan dat ook zijn bedrijf slachtoffer kan worden van cybercriminaliteit. Dit gevoel veranderde toen hij in april 2021

een televisieprogramma zag waarin het thema cyberweerbaarheid werd besproken. "Dat programma heeft mij wakker geschud."

Uitgangssituatie

Vijf basisprincipes

Met het in kaart brengen van 'kwetsbaarheden' is respondent O niet bezig. "Wel is een gezichtsherkenner aanwezig op mijn werklaptop." Er worden geen inspanningen gedaan ten behoeve van de 'instellingen'. "Ik heb daar te weinig kennis over, maar ik vind het wel belangrijk om digitaal weerbaar te zijn." Bedrijf O heeft de intentie om meer aandacht te besteden aan 'updates'. De updates worden automatisch uitgevoerd. Wanneer de opslagcapaciteit van de laptop vol is worden de updates handmatig aangezet. "Er wordt dan ook niet altijd gekeken of er nieuwe updates zijn." Ten aanzien van 'toegangsrestricties' geeft respondent O aan, wanneer dat door externe partijen verplicht wordt, tweefactorverificatie te gebruiken. "Ik gebruik wel vaak dezelfde wachtwoorden voor verschillende accounts." Hij heeft geeft aan de intentie te hebben om zijn wachtwoorden te verbeteren. Tenslotte onderkent het bedrijf O het belang om 'virussen en malware' buiten de deur te houden: "Ik heb een betaalde virusscanner die automatisch mijn laptop scant op virussen en malware. Dit vind ik belangrijk en essentieel."

Factoren houding en (zelf)effectiviteit

Respondent O geeft aan dat het van belang is dat zijn persoonlijke gegevens niet gestolen kunnen worden. "Het is belangrijk om hier aandacht aan te besteden zodat niet alle (persoonlijke) gegevens van een computer kunnen worden gestolen." De grootste belemmering om meer in te kunnen zetten op digitale weerbaarheid is volgens Respondent O een gebrek aan kennis. "Wanneer deze kennis er komt, biedt dit mij meer zekerheid." Respondent O denkt na over het aanschaffen van nieuwe hardware, waarbij met behulp van een IT-expert alles goed ingesteld kan worden.

Omgevingsfactoren

Respondent O geeft aan vooral gestimuleerd te worden via de media. Andere actoren stimuleren het bedrijf niet. Vanuit de omgeving wordt Bedrijf O op geen enkele wijze belemmerd. Op basis van het eerste interview wordt geconcludeerd dat Bedrijf O zich bevindt in fase 3: Preparatiefase.

Situatie na basisscan

Vijf basisprincipes

Respondent O heeft op 10 mei 2021 de basisscan ingevuld. "De uitkomsten zijn redelijk in lijn met het eerste interview." De score vanuit de basisscan ligt hoger. Respondent O benadrukt dat zijn bewustwording ten opzichte van de eerste meting vergroot is. De score op het basisprincipe 'instellingen' viel lager uit dan op de andere basisprincipes. Respondent O is voornemens een nieuwe laptop aanschaffen waarbij alle instellingen direct goed staan. "Bij 'toegangsrestricties' gaf de basisscan de tip om een

wachtwoordmanager in te voeren. "Dit staat op de planning om doorgevoerd te worden. Zo staan alle wachtwoorden veilig in een kluis en hoeft ik maar één wachtwoord te onthouden." Respondent O onderneemt nu meer actie op het gebied van 'updates'. "Ik kijk nu actief of de updates worden uitgevoerd." Met de andere basisprincipes: het inventariseren van 'kwetsbaarheden' en het voorkomen van 'virussen en malware' is hij niet bezig. "Deze basisprincipes waren al redelijk op orde." Respondent O ziet de toekomst met vertrouwen tegemoet: "Ik wil veranderingen doorvoeren om de cyberweerbaarheid te vergroten. Het wordt tijd om hier nog serieuzer mee bezig te gaan."

Factoren houding en (zelf)effectiviteit

Respondent O geeft aan bewuster te zijn van de meerwaarde om in te zetten op digitale weerbaarheid. Ook heeft hij meer kennis van de interne zwakheden te hebben gekregen en weet hij welke kunde in huis gehaald moet worden. Respondent O is zich ook bewuster hoe hij beter weerstand kan bieden tegen toekomstige bedreigingen. Volgens hem is het nu ook duidelijker welke inspanningen nog gedaan moet worden om de weerbaarheid te vergroten. Daarentegen heeft de basisscan geen of weinig inzichten gegeven in de tijd die de verbeteringen gaan kosten. Ook financieel heeft de basisscan geen inzichten gegeven.

Omgevingsfactoren

Het onderzoek is een belangrijke factor geweest voor Respondent O om veranderingen door te voeren. Ook de media hebben hieraan bijgedragen. Respondent O geeft aan niet vanuit de overheid te worden gestimuleerd of belemmerd. Hetzelfde geldt voor kennisinstellingen, branchegenoten en zakenpartners, zij inspireren noch belemmeren het bedrijf over digitale weerbaarheid.

Oordeel over de basisscan

Respondent O vindt dat hij, door mee te doen aan dit onderzoek, zich bewuster is geworden van de cyberweerbaarheid binnen het bedrijf. "Er wordt nu meer actie ondernomen op de onderwerpen die nog niet in orde zijn, de cyberweerbaarheid is nu beter geregeld dan voorheen. "Bedrijf O bevindt zich een fase hoger dan in de eerste meting: fase 4, de actiefase. "De basisscan is een duidelijke tool om te kijken in hoeverre het bedrijf cyberweerbaar is."

Bedrijf P: Ondergeschoven kindje

Schets van bedrijf P

Bedrijf P is gespecialiseerd in het projectmatig inrichten van gebouwen en ruimtes. Er werken dertig mensen en het bedrijf is gevestigd in Noord-Nederland. Respondent P is werkzaam als afstudeerder en voert onderzoek uit over de cyberweerbaarheid van het bedrijf. Het eerste interview is afgenomen op 29 maart 2021 en het tweede interview op 13 april 2021. Bij cyberweerbaarheid denkt Respondent P aan het uitvoeren van gepaste acties bij cyberincidenten. Volgens hem ligt hier een belangrijke rol voor de

medewerkers. "Het bedrijf heeft als wens dat medewerkers zelf kunnen inschatten wat er gedaan moet worden als het misgaat en dat zij weten waar zij de incidenten kunnen melden." Het bedrijf moet volgens Respondent P verdere stappen ondernemen om de cyberweerbaarheid te vergroten.

Uitgangssituatie

Vijf basisprincipes

Recent zijn er een aantal cyberincidenten geweest bij de door het bedrijf ingehuurde systeembeheerder. De normale werkzaamheden konden binnen Bedrijf P hierdoor niet uitgevoerd worden. "Daardoor is cyberweerbaarheid actiever onder de aandacht van het managementteam gekomen." Een eerste stap is dat Respondent P is aangenomen om te onderzoeken hoe het bedrijf ervoor staat op het gebied van cyberweerbaarheid. Het bedrijf heeft de intentie om 'kwetsbaarheden' in beeld te brengen. "Daar is het bedrijf door het aantrekken van mij nu actief begonnen." Het beheren van 'instellingen' valt onder de verantwoordelijk van een externe systeembeheerder. Het bedrijf ziet het belang in van 'updates'. "De externe systeembeheerder is actief bezig met het verbeteren van het ICT-landschap binnen het bedrijf. Een nadelig gevolg van de updates is dat iedere werknemer uit het systeem moet zodat 'patches' gedicht kunnen worden. Het werk ligt dan stil." De intentie is aanwezig om 'toegangsrestricties' aan te brengen. Respondent P heeft, samen met het directieteam en de externe systeembeheerder, al over bepaalde acties gesproken zoals het invoeren van wachtwoordmanagers en het gebruik van tweefactorverificatie. "De medewerkers voelen zich geroepen om aan alle veranderingen mee te werken." Het laatste basisprincipe 'virussen en malware' valt onder de verantwoording van de systeembeheerder. "De medewerkers van ons bedrijf zijn zich (nog) niet bewust van de risico's van virussen en malware."

Factoren houding en (zelf)effectiviteit

Het bedrijf probeert veel te ondernemen om de cyberweerbaarheid van de organisatie te vergroten. "Zo wordt de interne kennis over cybersafety aangevuld door het aannemen van mij." Waar het bedrijf intern onvoldoende kennis heeft wordt een externe systeembeheerder geraadpleegd. De systeembeheerder voert bijvoorbeeld alle updates uit. Er moet volgens Respondent P nog worden gewerkt aan het bewustzijn van de risico's van cyberincidenten onder de medewerkers. "Medewerkers zijn een belangrijke component om de organisatie cyberweerbaar te maken. Wanneer medewerkers de noodzaak inzien kunnen er tijdiger beheersmaatregelen geïmplementeerd worden."

Omgevingsfactoren

Respondent P geeft aan gestimuleerd te worden door cyberincidenten die in de omgeving plaatsvinden. "Na een incident wordt de noodzaak meer ingezien." Met zijn afstudeerscriptie en medewerking aan dit onderzoek wordt een concreet plan gemaakt om het thema cyberweerbaarheid onder de aandacht van de medewerkers te brengen. De externe systeembeheerder probeert al meer aandacht te genereren voor het thema.

Door drukte lukt dat niet altijd. "Wij krijgen veel opdrachten waardoor het onderwerp een ondergeschoven kindje is. Wie weet lukt het gezamenlijk."

Op basis van het eerste interview wordt geconcludeerd dat Bedrijf P zich in fase 3 bevindt: preparatiefase. Het bedrijf heeft voorbereidingen getroffen, maar mag nog meer actie ondernemen.

Situatie na de basisscan

Vijf basisprincipes

Respondent P heeft op 7 april 2021 de basisscan ingevuld. "Er is bevestigd dat er verbeteringen moeten worden doorgevoerd, zodat alle basisprincipes in orde zijn." Drie van de vijf basisprincipes zijn (redelijk) op orde. Dit zijn de werkzaamheden die worden uitgevoerd door de externe systeembeheerder." Twee basisprincipes zijn nog niet op orde: het beheren van 'instellingen' en het voorkomen van 'virussen en malware'. Op dit moment zijn nog geen concrete acties ondernomen ten aanzien van deze twee basisprincipes. De resultaten worden meegenomen in het interne onderzoek dat wordt uitgevoerd. De volgende stap is dat de uitslag wordt voorgelegd aan het management, zodat verdere stappen ondernomen kunnen worden. "Het management beslist welke maatregelen genomen worden om de cyberweerbaarheid te vergroten. Het managementteam weet al dat er nog stappen gezet moeten worden."

Factoren houding en (zelf)effectiviteit

Respondent P geeft aan zich nu bewuster te zijn van de inspanningen die nog gedaan moeten worden. Ook ziet hij hier meer de meerwaarde van in. Hij heeft door de basisscan nadere kennis van de zwakheden gekregen en weet bedreigingen beter het hoofd te bieden. Daarnaast heeft de organisatie een nauwkeuriger beeld van de kosten en tijdsindicatie. Daarentegen heeft de basisscan geen inzichten gegeven over toekomstige bedreigingen. Ook heeft de basisscan niet per se geleid tot nieuwe kennis. "Er stond niet iets nieuws in. Bovendien, wat we niet weten pakt de externe systeembeheerder op."

Omgevingsfactoren

Door de basisscan weet Respondent P beter welke partijen in de omgeving het bedrijf kunnen stimuleren om bezig te gaan met digitale weerbaarheid. "Dit is bijvoorbeeld een overheidspartij als het DTC, maar ook via sociale media en nieuwssites." Daarnaast geeft hij aan te weten waar meer informatie gevonden kan worden over het onderwerp cyberweerbaarheid. "Dat wil ik actiever gaan doen en ik wil die kennis inzetten."

Oordeel over de basisscan

Ten aanzien van de basisscan concludeert Respondent P dat het instrument geholpen heeft om in te zien dat het bedrijf nog niet goed genoeg digitaal onderlegd is. Tot een verandering in gedragsfase heeft het (nog) niet geleid. De uitslag wordt voorgelegd aan het managementteam, zodat zij kunnen bepalen welke stappen de organisatie moet zetten om de digitale weerbaarheid te vergroten.

Bedrijf Q: Cyberweerbaarheid: een continu proces

Schets van bedrijf Q

Bedrijf Q is gespecialiseerd in arbeidsveiligheid. Het bedrijf heeft zestig medewerkers in dienst en is gevestigd in Noord-Nederland. Respondent Q is procesmanager ICT, hij begeleidt interne ICT- processen zoals netwerk- en applicatiebeheer. Het eerste interview is gehouden op 9 april 2021 en het tweede interview op 22 april 2021. Respondent Q geeft als associatie van cyberweerbaarheid: "Dat ervoor wordt gezorgd dat het bedrijf geen prooi kan worden van een hacker of crimineel die gegevens wil stelen. En dan vooral persoonsgegevens." Het bedrijf ziet cyberweerbaarheid als een continu proces en wil blijvende alertheid voor dit onderwerp creëren.

Uitgangssituatie

Vijf basisprincipes

Het in kaart brengen van 'kwetsbaarheden' wordt steeds belangrijker. Het bedrijf wil aan klanten laten zien dat digitale weerbaarheid heel belangrijk is voor het bedrijf. Hetzelfde geldt voor het beheren van 'instellingen'. Het bedrijf werkt met een centrale server. Doordat medewerkers thuis moesten werken zijn laptops aangeschaft, hierdoor is het risico tot besmetting van een laptop groter geworden omdat verschillende netwerken worden gebruikt. Respondent Q onderkent het belang van 'updates'. "Dit is in het bedrijf eveneens een continu proces." Bedrijf Q heeft een netwerkpartner ingeschakeld die alle updates regelt. "Als er bijvoorbeeld een lek is in een server wordt dit opgepakt door de netwerkpartner en dan ondernemen zij snel actie." Ook 'toegangsrestricties' vindt de respondent belangrijk. "Dit is ingericht en er is beperkte toegang tot verschillende zaken. Echter valt hier nog wel winst te behalen bij het inrichten en updaten van gebruikersprofielen." Volgens de respondent is het bedrijf al ver gevorderd als het gaat om het buiten de deur houden van 'virussen en malware'. Het bedrijf heeft een actieve firewall. Ook wordt er frequent een bedreigingsrapport gemaakt om te kijken of eventuele acties ondernomen moet worden.

Factoren houding en (zelf)effectiviteit

"Cyberweerbaarheid is voor ons belangrijk, het is een continu vraagstuk waar wij geld, tijd en energie insteken." Respondent Q zegt dat verschillende acties stelselmatig worden ondernomen om cyberweerbaar te zijn. "Wij achten onszelf in staat om onze cyberweerbaarheid goed op orde te laten zijn." Waar het bedrijf Q zelf niet lukt, wordt er geïnvesteerd in kennis van externe partners. "Deze partners helpen ons deels bij applicatie- en netwerkbeheer."

Omgevingsfactoren

Het bedrijf wordt onder andere door netwerkpartners gestimuleerd om in te zetten op digitale weerbaarheid. "Hierdoor weten wij waar we alert op moeten zijn. Deze informatie wordt wekelijks via een informatiebrief aan onze medewerkers verstuurd." Ook accountants en klanten stimuleren Bedrijf Q. De respondent ziet geen belemmeringen vanuit de omgeving. "Wel spelen interne werkprocessen een rol als het gaat om belemmeringen, zoals het gebruik van tweefactorverificatie."

Op basis van het eerste interview wordt geconcludeerd dat bedrijf Q zich in fase 5 bevindt: de behoudfase. Het bedrijf kijkt nu al waar zij over twee of drie jaar staan op het gebied van cyberweerbaarheid. Bedrijf Q is bovendien continu bezig met de verbetering van digitale processen.

Situatie na basisscan

Vijf basisprincipes

Respondent Q heeft op 9 april 2021 de basisscan gemaakt. "Waar grotendeels de resultaten in lijn waren met het eerste interview kwam ook naar voren dat nog niet alles even goed op orde is." In het eerste interview gaf de respondent aan dat medewerkers moeite hadden om overal een wachtwoord voor te gebruiken. "Bij het basisprincipe 'instellingen' kwam voren om wachtwoordmanagers in te zetten. Dit is daadwerkelijk ook geïmplementeerd." Het basisprincipe 'virussen en malware' kwam minder goed uit de basisscan dan de respondent had ingeschat: "De reden hiervan is bij ons onbekend, wij doen voor ons gevoel al alles." Er is geen actie ondernomen op de andere basisprincipes: het inventariseren van 'kwetsbaarheden', het aanbrengen van 'toegangsrestricties' en het uitvoeren van 'updates'."

Factoren houding en (zelf)effectiviteit

Respondent Q heeft de intentie om nog meer in te zetten op digitale weerbaarheid. De basisscan heeft geen of weinig verandering gebracht over kennis van zwakheden en kennis over toekomstige bedreigingen. "Externe partijen wijzen ons bedrijf al op welke kunde nog in huis gehaald moet worden." Respondent Q was zich reeds bewust welke inspanningen nog gedaan moeten worden en hoe bedreigingen gemitigeerd kunnen worden.

Omgevingsfactoren

Sinds het eerste interview zijn er naast de basisscan ook andere factoren geweest die bij hebben gedragen aan het bewustzijn van respondent Q. "Zo hebben wij ons aangemeld voor door de overheid geïnitieerde phishing-testen." Ook ziet de respondent meer in dat kennisinstellingen aandacht besteden aan het onderwerp cyberweerbaarheid, net als zakenpartners. "Met een toekomstige ISO-certificering willen wij aan klanten laten zien dat wij met digitale weerbaarheid vergevorderd zijn."

Oordeel over de basisscan

De basisscan heeft Respondent Q geholpen om enkele zaken aan te scherpen, zoals het implementeren van wachtwoordmanagers. Tot verandering van gedragsfase heeft dit niet geleid. Respondent Q had zijn organisatie in het eerste interview al in de hoogste fase geplaatst: de behoudfase. Tot slot heeft respondent Q nog een tip: "Specifieke(re) tips over de basisprincipes kan leiden tot uitvoeren van concrete acties."

Deze tip van Respondent Q vormt het slotstuk van het empirische onderzoek naar de werking van de basisscan van het DTC. Het laatste hoofdstuk bevat de conclusies die uit het onderzoek getrokken kunnen worden en de aanbevelingen die we het DTC in overweging geven.

Bedrijf R: Zeg nooit nooit

Schets van bedrijf R

Bedrijf R voert verschillende werkzaamheden uit op het gebied van bewindvoering, curatele en administratie. Het bedrijf is gevestigd in West-Nederland en heeft negen werknemers. Het eerste interview is afgenomen op 26 mei 2021 en het tweede interview op 23 juni 2021. Als associatie met de term cyberweerbaarheid geeft Respondent R, bij monde van de bij het interview uitgenodigde externe ICT-dienstverlener, aan dat hij vooral denkt aan de beveiliging binnen het bedrijf zoals software en systemen. Ook geeft hij steekwoorden zoals phishing via mail of sms, wachtwoorden, encryptie, virussen en cryptolocker (ransomware).

Uitgangssituatie

Vijf basisprincipes

Met betrekking tot het in kaart brengen van de 'kwetsbaarheden' geeft de respondent aan dat er al een aantal dingen in kaart zijn gebracht, maar ook zeker verbeterd kunnen worden. Zo heeft het bedrijf een beleid over wachtwoordbeheer en wordt gebruik gemaakt van wachtwoordmanagers. Op dit moment is Respondent R bezig om de website veiliger te maken en denkt hij na over het e-mailsysteem. Wat betreft 'instellingen' geeft hij aan dat de basis oké is. "Medewerkers kunnen soms wel instellingen uitzetten, zoals scherm blokkering bij een inactiviteit van twee minuten." Bedrijf R is op het gebied van 'updates' al vergevorderd. Alle Windows-updates worden standaard uitgevoerd en ook andere updates worden ook voortvarend opgepakt. Het bedrijf maakt, uit het oogpunt van gebruiksgemak, gebruik van 'Software as a Service'[26]. Ten aanzien van 'toegangsrestricties' is het bedrijf volgens Respondent R in vergelijking met andere bedrijven al verder: "Er wordt gebruikt gemaakt van twee verschillende netwerken waardoor de gast-wifi en bedrijfs-wifi gescheiden worden gehouden." Ook geeft respondent R aan dat printers en scanners van buitenaf niet toegankelijk zijn. Wel

[26] Software as a Service (afgekort SaaS) "stelt gebruikers in staat om via internet verbinding te maken met toepassingen in de cloud en deze te gebruiken" (Azure.Microsoft.com, z.d.).

zou tweefactorverificatie nog kunnen worden toegevoegd. Volgens Respondent R is het bedrijf op het gebied van 'virussen en malware' vergevorderd. Op de Linux-server draait open source software waarin virusscanners zijn inbegrepen. "We wijzen medewerkers erop om bewust handelingen uit te voeren, wat bijdraagt aan de weerbaarheid. Er wordt bijvoorbeeld samen gekeken naar een verdacht mailtje."

Factoren houding en (zelf)effectiviteit

Volgens Respondent R moet er een speciale risicoanalyse uitgevoerd worden. Dit bedrijf ondervindt andere risico's dan bedrijven uit vakgebieden. Bedrijf R heeft veel vertrouwelijke gegevens in bezit en criminelen verzinnen steeds nieuwe manieren op toegang te krijgen tot systemen. Elk jaar wordt gekeken hoe dit aangepakt moet worden. Dit geeft de mede-eigenaar naar eigen zeggen 'rust'. "Als je bij elke muisklik denkt dat iemand mee kan kijken kan je beter stoppen met je werk." Verder is bedrijf R vooral bezig met de bewustwording van medewerkers binnen de organisatie, ook al is de basis wat dat betreft wel op orde. "Het is goed om dit regelmatig opnieuw op te frissen." Soms vinden medewerkers het nog wel lastig om nieuwe wachtwoorden te verzinnen waardoor oude weer opnieuw gebruikt worden. Daarnaast geeft Respondent R aan: "wij zeggen nooit we hebben alles honderd procent op orde en we worden geen slachtoffer, want dat is niet met zekerheid te zeggen."

Omgevingsfactoren

Respondent R acht zichzelf in samenwerking met externe partners in staat om de nodige maatregelen te nemen. De technische achtergrond ligt echt bij de beheerder en het bedrijf gaat hierin mee waardoor de implementatie snel uitgevoerd kan worden. Daarbij spelen de reguliere audit en de media ook een rol. Er worden verhalen opgepikt over phishing en oplichting binnen bedrijven en dit willen ze voorkomen. Bedrijf R vindt gegevens van klanten beschermen het belangrijkste. "We zijn soms afhankelijk van externe applicaties waardoor wij erop moeten vertrouwen dat externe bedrijven alles zaken goed op orde hebben." Hierdoor zijn andere actoren ook verantwoordelijk voor de veiligheid van klantgegevens.

Naar aanleiding van het eerste gesprek ziet bedrijf R zich in fase 4: de actiefase. Er worden verschillende maatregelen genomen, maar er kan nog extra actie ondernomen worden om de cyberweerbaarheid van de organisatie te verbeteren.

Situatie na de basisscan

Respondent R heeft aangegeven de basisscan op 26 mei 2021 te hebben uitgevoerd. De uitkomsten komen grotendeels overeen met de bevindingen uit het eerste interview. Hij bevestigd dat het bedrijf opnieuw ingeschaald kan worden in fase 4: de actiefase.

Vijf basisprincipes

Wat betreft de basisprincipes geeft Respondent R aan dat komende kwartaal bepaalde acties doorgevoerd gaan worden. Zo wordt gecontroleerd of de wachtwoorden sterk

genoeg zijn, het gebruiken van tweefactorverificatie en bewustwording over openbare wifi voor buitenpersoneel te vergroten. Ook wordt gecontroleerd of apparaten automatisch updates uitvoeren en wordt gekeken of een centrale login gebruikt kan worden. Daarnaast moeten bij een aantal computers gebruikersrechten ingeperkt worden. En wat zouden medewerkers doen met usb-sticks? Respondent R wil het bedrijf hier bewuster over maken.

Factoren houding en (zelf)effectiviteit

Respondent R geeft aan dat de basisscan een meerwaarde heeft in de zin dat hij het belang van cyberweerbaarheid nog meer inziet. Ook weet de respondent nu beter wat hij concreet moet doen en welke kennis en kunde daarvoor nodig is. De basisscan heeft hem daarnaast ook nieuwe inzichten opgeleverd over de zwakheden en kunde binnen zijn organisatie. De uitslag van de basisscan in combinatie met de website heeft het inzichtelijk gemaakt welke toekomstige bedreigingen op zijn pad kunnen komen. Respondent R is echter naar eigen zeggen niet beter in staat bedreigingen het hoofd te bieden. "Je weet niet wat de specifieke risico's zijn en welke stappen genomen moeten worden. Elk bedrijf implementeert dit anders." Hij heeft ook geen nauwkeuriger beeld gekregen over kosten en tijdsaspecten om de organisatie in de toekomst weerbaarder te maken.

Omgevingsfactoren

Respondent R geeft aan dat hij, na het maken van de basisscan geen verschil ziet in de mate waarin de overheid een rol speelt in de bewustwording rondom cyberweerbaarheid. Wel is kennis delen met branchegenoten en ketenpartners als belangrijk aandachtspunt naar voren gekomen. Het bedrijf werkt namelijk veel samen met de rechtbank. Tevens ziet Respondent R in steeds grotere mate dat kennisinstellingen inzetten op digitale weerbaarheid Volgens Respondent R wordt het bedrijf niet belemmerd door zakenpartners. "Ik zie wel bij kleinere instellingen dat zij nog gegevens via de mail willen sturen, officieel kan dit natuurlijk niet."

Oordeel over de basisscan

Respondent R concludeert dat de basisscan heeft bijgedragen aan opstellen van een implementatieplan. Alle acties staan op papier en moeten alleen nog de komende tijd doorgevoerd worden. "Zo wordt het veiliger voor cliënten en onszelf." Wel heeft hij nog een paar opmerkingen over de basisscan. "Ik mis een 'niet van toepassing' antwoord omdat elke branche de basisprincipes anders invult." Ook mist Respondent R de antwoorden die gegeven zijn en de impact die zij hebben gehad op de score. De voorgelegde stellingen waren daarentegen wel duidelijk.

4. Conclusies en Aanbevelingen

4.1 Conclusies

Dit afsluitende hoofdstuk geeft antwoord op de hoofdvraag van dit onderzoek, te weten: In hoeverre draagt de Basisscan Cyberweerbaarheid van het DTC bij aan gedragsverandering van ondernemers? Dit onderzoek geeft inzicht in het samenstel van drijfveren, externe factoren en concrete gedragingen van ondernemers. Uit dit onderzoek blijkt eens te meer dat 'de ondernemer' niet bestaat. Om recht te doen aan deze complexiteit en aan de variëteit binnen de doelgroep is het goed om grofweg drie categorieën bedrijven te onderscheiden, te weten:

1. Ondernemers die cyberweerbaarheid al op de agenda hebben staan en de scan voornamelijk als een spiegel gebruiken;
2. Ondernemers die prioriteiten elders leggen en weinig steun ervaren van de overheid;
3. Ondernemers die groot belang hechten aan cyberweerbaarheid maar in de basisscan een zekere diepgang en dynamiek missen.

Ad1) De eerste categorie van de ondernemers zoekt en vindt in de basisscan een bevestiging van de ondernomen of reeds voorgenomen acties. Dit betreft over het algemeen bedrijven die al hoog scoren qua gedragsfase (4 of 5). Zij zien de scan als een spiegel waarin ze de bevestiging zien om cyberweerbaarheid op de agenda van het management te houden en reeds voorgenomen acties daadwerkelijk te implementeren. Bedrijfscontinuïteit staat bij hen voorop, schade dient te worden voorkomen! Deze categorie laat zich niet alleen leiden door intrinsieke motieven maar vooral ook door druk vanuit klanten en leveranciers. De bedrijven vinden de scan over het algemeen te globaal om echt nieuwe inzichten aan te ontlenen. Daarvoor ontbreekt inzicht in de implementatieaspecten zoals kosten en tijdsbesteding.

Ad2) Het tweede categorie heeft simpelweg geen tijd om zich echt met het onderwerp cyberweerbaarheid bezig te houden. De klanten gaan voor, het dagelijkse werk is leidend, zo is de gedachte. Opvallend aan deze groep is dat zij voor een groot deel, in tegenspraak met de adviezen van het DTC, vertrouwen op bepaalde software (bijvoorbeeld iOS of Linux) en de hardware (Apple). Men gaat ervan uit dat het een kwestie is van automatische updates laten uitvoeren en gebruik te maken van bijvoorbeeld een vingerscan, en daarmee de kous af is. Deze categorie laat zich leiden door berichten uit de sociale media en directe contacten via werk of vriendenkring. Deze bedrijven scoren gemiddeld iets lager op de basisscan (fase 3 of 4) omdat zij zelf voor de minimale variant kiezen. Het eigenlijke werk heeft altijd prioriteit. Vanuit overheid of kennisinstellingen ervaren zij weinig steun. Dit betreft bedrijven die vooral als eenmanszaak of in vennootschap opereren.

Ad3) De derde categorie van ondernemers geeft aan wel degelijk baat te hebben gehad bij de basisscan. Zij zijn nieuwe inzichten op het spoor gekomen op het gebied van

zwakheden in de organisaties of wachtwoordbeheer. Deze bedrijven geven aan zich zorgen te maken over de kwaliteit van hun eigen dienstverlening en continuïteit van de bedrijfsvoering. Zij zien het als een professionele plicht om de zaken goed op orde te hebben omdat zij vaak zelf ook actief zijn in de dienstverlening via het internet. Deze bedrijven zijn kritisch op zichzelf en op anderen en scoren (zichzelf) relatief laag op de basisscan. Deze bedrijven opereren in een sterk dynamisch speelveld. Het lijkt erop dat eergevoel, oprechte zorg en interesse in het vakgebied de belangrijkste drijfveren vormen voor deze groep. Certificering speelt een belangrijke rol op de achtergrond waarbij ook verantwoordelijkheid voor het professionele netwerk (o.a. klanten en leveranciers) een uitgangspunt vormt.

Al met al kunnen we concluderen dat de basisscan, hoewel die qua opzet, techniek en inhoud voldoet, in beperkte mate en voor een specifieke groep bijdraagt aan gedragsverandering van ondernemers. Ondernemers missen vooral, de met elkaar samenhangende aspecten interactie, diepgang en het tijdsaspect.

4.2 Beperkingen

Een van de beperkingen die we willen toelichten heeft te maken met het evaluatieve karakter van het onderzoek. Allereerst willen we benadrukken dat de nulmeting een 'tussenstand' betreft. Immers, elke ondernemer heeft een verschillende startpositie als het gaat om bijvoorbeeld kennis en kunde op het gebied van digitale weerbaarheid. Ook kunnen we niet garanderen dat de verandering tussen de nul- en eenmeting exclusief te herleiden is tot het uitvoeren van de basisscan. Immers, de media staan bol van nieuws over cybersecurity-incidenten en regelmatig worden vanuit diverse kanalen tips verspreid over hoe bij te dragen aan de (eigen) digitale weerbaarheid. Ook kan de nulmeting ertoe hebben geleid dat ondernemers met kennissen spraken over het onderwerp en op die manier aangezet werden tot beweging. Dit is belangrijk om in ogenschouw te hebben bij de interpretatie van de resultaten.

Een tweede beperking van het onderzoek ligt in het aantal mkb'ers dat met dit onderzoek is bereikt. De eerste reden dat respondenten moeilijk verleid konden worden tot deelname is waarschijnlijk het moment van dit onderzoek. Door de corona-crisis stonden veel ondernemers in een overlevingsstand. Hoewel cybersecurity-vraagstukken niet behoren tot de eerste prioriteit van ondernemers, was dat in deze situatie wellicht nog minder het geval. Hetzelfde kan gezegd worden over tijdsbesteding aan het meewerken aan onderzoek. Jansen e.a. (2017) melden dat redenen van mkb'ers om niet mee te werken aan onderzoek veelal tijdsgebrek is, waarbij tijd ook uitgedrukt kan worden in geld. Vanuit ons eigen netwerk kregen we soms de reactie terug dat men niet wil weten hoe ze ervoor staan, omdat ze verwachten dat dit niet goed zal zijn.

De tweede reden waarom ondernemers mogelijk terughoudend zijn geweest ligt wellicht aan de wijze van aanmelding. Het aanmelden voor het onderzoek geschiedde aanvankelijk via koppelingen in mails en berichten via sociale media. Hoewel een

duurdere methode, is het wellicht toch effectiever om via een fysieke mailing de respondenten te werven. In vervolgonderzoek zou ook gekeken kunnen worden naar mogelijkheden om gebruik te maken van panels.

Positief is dat op basis van eigen netwerk respondenten zich hebben aangemeld voor het onderzoek. Onze resultaten zijn dus voornamelijk gebaseerd op een zogenoemde 'convenience sample'. Een beperking van deze selectiewijze is dat resultaten moeilijker generaliseerbaar lijken. Echter, gezien het doel van deze studie, is dit geen belemmering. We menen in het licht van het doel van dit onderzoek voldoende kwalitatieve informatie te hebben om betrouwbare en valide uitspraken te kunnen doen.

4.3 Aanbevelingen

Gedragsverandering is moeilijk te bewerkstelligen, laat staan dat dit via een eenmalige actie lukt. En als gedragsverandering al lijkt te slagen, dan zien we dat deze niet altijd duurzaam is. Men vervalt na een tijdje weer in oude gewoonten (o.a., Bullée 2017). Dit betekent dat een bepaalde cyclus van herhaling of reactivering nodig zal zijn (o.a., Jansen, 2018), zonder dat men hier onnodig mee wordt vermoeid. Immers, de belangrijkste prioriteiten van ondernemers liggen bij hun bedrijfsvoering. De aanbevelingen voor het DTC richten zich op drie punten die uit het onderzoek naar voren komen: interactie, diepgang en dynamiek.

Ten eerste wordt aanbevolen om bij een eventuele volgende versie van de basisscan of bij de ontwikkeling van alternatieve instrumenten meer in te zetten op interactie met de ondernemers. Respondenten geven namelijk aan dat het niet alleen de basisscan is, die aanzet tot gedragsverandering maar vooral ook het gesprek met een deskundige (in dit geval de onderzoekers). De scan is te afstandelijk en te statisch, vinden zij. Zowel bij bedrijven die intrinsiek gemotiveerd zijn als bedrijven die zich door externe factoren laten beïnvloeden, is het van belang dit gesprek op gang te brengen. De eerste groep vindt het leerzaam en nuttig terwijl de tweede groep het als noodzaak ziet. Concreet kan gedacht worden aan chatfuncties, (online) trainingen en regionale bijeenkomsten.

Wat het tweede punt betreft, de diepgang, valt te overwegen om een onderscheid te maken tussen verschillende typen bedrijven. Sommige bedrijven zijn vooral geïnteresseerd in de kosten (in tijd en geld) die een bepaalde maatregel met zich meebrengt, terwijl andere bedrijven juist het overzicht en het globale karakter waarderen. Te overwegen valt om een vorm van maatwerk na te streven ook waar het gaat om de implementatie van de aangedragen verbeterpunten.

Ten derde vraagt daadwerkelijke gedragsverandering om een langdurig commitment van zowel de respondent als het DTC. In die zin valt te overwegen om meerjarig te monitoren en door vooral gedragsverandering centraal te stellen in plaats van de technisch inhoudelijke aspecten van de basisscan op één moment.

Dit onderzoek bood een interessante blik in de keuken van ondernemers. De wijze waarop zij het instrument basisscan daarbij inzetten liep zeer uiteen, maar duidelijk werd dat vooral behoefte bestaat aan een actieve en betrouwbare begeleiding vanuit overheid en kennisinstellingen. Waarbij wij de volgende hoofdrichting in overweging geven: van statisch naar dynamisch.

4.4 Slotbeschouwing

Om de werking van de basisscan te optimaliseren, hebben we een drietal aanbevelingen gedaan. Op het gebied van interactie, diepgang en het tijdsaspect kan de methodiek van de basisscan worden verbeterd en zodoende verder bijdragen aan het vergroten van de digitale weerbaarheid van mkb'ers. Dit is gezien de grote mate van afhankelijkheid van ICT een absolute vereiste. Het belang van online veiligheid voor ondernemers verdient meer nadruk. In die zin fungeert het DTC als een belangrijk voorbeeld voor anderen.

Een belangrijke stap voorwaarts die recent is aangekondigd zijn de wetsvoorstellen die het DTC, alsook het NCSC, beter in staat moeten stellen om dreigings- en incidentinformatie te delen. Dit zijn belangrijke momenten om de doelgroepen te bereiken en daarbij ook te voorzien van specifieke (alsmede algemene) handelingsperspectieven die bijdragen aan het vergroten van de digitale weerbaarheid. De basisscan kan in dergelijke communicatie worden uitgelicht om mkb'ers bewust te maken om hun bedrijf ook op andere onderdelen, dan betreffende specifieke dreigingen, door te lichten, en waar mogelijk actie te ondernemen.

Al heeft maar een deel van de mkb'ers baat bij de scan in de huidige vorm, zoals de conclusies indiceren, dan blijft het zeer van belang door te blijven gaan met het aanbieden van de scan en deze uit te bouwen en te optimaliseren. Een uitdaging blijft het bereiken van de doelgroep, en met name die mkb'ers die het meest baat hebben bij een dergelijke scan. Hoewel cybersecurity-maatregelen, zowel technisch, menselijk als organisatorisch, van belang zijn en een noodzakelijke randvoorwaarde is, blijft het voor veel ondernemers een abstract onderwerp. Enerzijds ligt een groot deel van het probleem bij mkb'ers zelf; die verantwoordelijk zijn voor hun eigen (online)gedrag. Anderzijds ligt er een maatschappelijke taak om hen digitaal weerbaar(der) te worden.

Het DTC staat overigens niet alleen voor deze uitdaging. Ook andere stakeholders kunnen en moeten hier hun steentje aan bijdragen. Denk aan andere overheidspartijen, kennisinstellingen, ondernemers- en belangenverenigingen. Maar ook ontwikkelaars van bijvoorbeeld software en systemen spelen een rol. Ter illustratie, met de scan kunnen ondernemers ertoe worden bewogen om de standaard instellingen te wijzigen, maar als ontwikkelaars deze reeds instellen met security en privacy als uitgangspunt (bijvoorbeeld als een nieuwe default of verplichte stap bij installatie), dan kan op voorhand al veel ellende worden voorkomen. Mogelijk dat het DTC ook die indirecte route voor ondernemers bewandelen. Met de boodschap dat niet alleen ondernemers in

beweging gezet moeten worden, maar ook andere actoren in de keten een rol hebben, besluiten we dit rapport.

Literatuurlijst

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Anderson, C. L. & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215

Bandura, A., & McClelland, D. C. (1977). *Social learning theory (vol. 1)*. Prentice Hall: Englewood cliffs.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. C*omputers & Security*, *32*, 90–101.

Deci, E. L., & Ryan, R. M. (1985). The general causality orientations scale: Self-determination in personality. Journal of research in personality, 19(2), 109-134.

Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. MA: Addison-Wesley.

Fishbein, M. & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. New York: Taylor & Francis.

Hendriks, A. M., Kremers, S., Wirix, A., & Jansen, M. (2017). Van fictie naar actie: naar een politiek-bestuurlijk gedragen integrale aanpak van overgewicht. *Tijdschrift voor gezondheidswetenschappen, 95(7-8)*, 288-295.

[i]Furnell, S., & Vasileiou, I. (2017). Security education and awareness: Just let them burn? *Network Security, 2017*(12), 5-9.

Hoff-de Goede, S., Kleij, R., Weijer, S., & Leukfeldt, R. (2019). *Hoe veilig gedragen wij ons online?* Den Haag: De Haagse Hogeschool - Centre of Expertise Cybersecurity.

Hollnagel, E. (2015). Disaster management, control, and resilience. In *Disaster management: Enabling resilience* (pp. 21-36). Springer, Cham.

Hartel, P. H., & Suryana Herman, N. (2012). Information Security. In E. R. Leukfeldt, & W. P. Stol (Eds.), *Cyber Safety: An Introduction* (pp. 281-291). Eleven International Publishers.

Hulst, R. C. van der & Neve, R. J. M. (2008). *High tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie*. Den Haag: Boom Juridische Uitgevers.

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

Jansen, J., Veenstra, S., Zuurveen, R. & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology, 35*(5), 368-379.

Kleij, R. van der, & Leukfeldt, R. (2019). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. In *Proceedings of the International conference on applied human factors and ergonomics* (pp. 16–27).

Kleij, R. van der, 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, *97*, 101970.

Lee, Y. C., & Wu, W. L. (2018). Factors in cyber bullying: The attitude-social influence-efficacy model. *Anales De Psicología/Annals of Psychology*, *34*(2), 324-331.

Leiden, I. V., Appelman, T., Ham, T. V., & Ferwerda, H. (2014). *Ondergaan of ondernemen*. Arnhem: Bureau Beke.

Matzenberger, J. (2013). A novel approach to exploring the concept of resilience and principal drivers in a learning environment. *Multicultural Education & Technology Journal*, *7*(2/3), 192-206.

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.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2021). *Cybersecuritybeeld Nederland (CSBN) 2021*. Den Haag: NCTV.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2021). *Cybersecuritybeeld Nederland (CSBN) 2021*. Den Haag: NCTV.

Notté, R., & Slot, L. (2017). *Hoe cybersecure is het mkb? Nulmeting cybersecurity in het mkb*. Den Haag: De Haagse Hogeschool - Centre of Expertise Cyber Security.

Prochaska, J.O., DiClemente, C. C., & Norcross, J. C. (1993). In search of how people change: Applications to addictive behaviors. *Addictions Nursing Netwerk, 5*(1), 2-16.

Ridder, C. de, & Lechner, L. (2004). Overschatting van het eigen bewegingsgedrag: Gevolgen voor determinanten en stages of change. *Tijdschrift voor Gezondheidswetenschappen, 82*(5), 290-298.

Rijksoverheid (2011). *Gedragsverandering via campagnes: Literatuuronderzoek in opdracht van Dienst Publiek en Communicatie*. Den Haag: Ministerie van Algemene Zaken.

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12-15.

Rotmans, S. (2005). *Bewegen, wat houdt jou tegen?! Een onderzoek naar de gedragsdeterminanten van het al dan niet lid worden van een fitnesscentrum*. Enschede: Universiteit Twente (bachelor thesis).

Sools, A. M. (2011). Narratief onderzoek. In F. de Boer, & A. Smaling (Eds.), Benaderingen in kwalitatief onderzoek (pp. 27-36). Den Haag, Nederland: Boom Lemma uitgevers.

Stol, W., Veenstra, S., & Zuurveen, R. (2015). *Cybercrime onder bedrijven*. Lectoraat Cybersafety, NHL Hogeschool & Politieacademie, Faculteit Cultuur- en Rechtswetenschappen, Open Universiteit.

Vries, H. de, Mudde, A. N., Dijkstra, A., & Willemsen, M. C. (1998). Differential beliefs perceived social influences, and self-efficacy expectations among smokers in various motivational phases. *Preventive medicine, 27*(5), 681-689.

Vasileiou, I. & Furnell, S. (Eds.) (2019). *Cybersecurity education for awareness and compliance*. Hershey, PA (USA): IGI Global.

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.

Bijlage I: Interviewprotocol nulmeting

Introductie
Dank voor uw medewerking! U heeft zich aangemeld voor ons onderzoek naar de effectiviteit van de basisscan cyberweerbaarheid van het Digital Trust Center (onderdeel van het ministerie van Economische Zaken en Klimaat). De onderzoeksgroep Cybersafety, onderdeel van NHL Stenden Hogeschool in Leeuwarden, voert het onderzoek uit voor het DTC. Met de resultaten van het onderzoek, dus met uw feedback, kan het DTC beter inspelen op de behoeften van ondernemers. Het onderzoek bestaat uit twee interviews waarvan dit eerste interview bestaat uit vijf onderdelen, te weten:

1. Even checken of uw gegevens van het aanmeldformulier nog juist zijn;
2. Een eerste globale inschatting, ook wel QuickScan genoemd, van de mate waarin u aandacht besteedt aan cyberweerbaarheid en de fase waarin uw organisatie zich nu in dat opzicht bevindt;
3. Een diepte interview over de mate waarin u aandacht besteedt aan de vijf pijlers van cyberweerbaarheid, te weten: het in kaart brengen kwetsbaarheden, het zorgen voor juiste instellingen voor software en systemen, het uitvoeren van software updates, het reguleren van toegang tot systemen en data, de zorg voor virusdetectie & bestrijding;
4. Een korte samenvatting van het interview;
5. Afspraken over het inplannen van het tweede interview.

Uw gegevens worden geanonimiseerd verwerkt. Uw bedrijfsnaam en eigen naam worden niet gepubliceerd. Ik (de onderzoeker) noteer de antwoorden via een Google-forms formulier. Heeft u nog vragen voordat we kunnen beginnen? *Vereist

1. E-mailadres*

2. Wat is uw naam? (vragen om bevestiging)*

3. Voor welke bedrijf werkt u? (vragen om bevestiging)*

4. Wat is uw functie binnen het bedrijf?*

5. Kloppen de gegevens van het aanmeldformulier: a) aantal werknemers, b) verantwoordelijkheid, c) branche, d) provincie

QuickScan: We gaan nu van start met de QuickScan. Een open vraag om mee te beginnen en daarna, bij wijze van zelftest, vijf vragen waarbij u steeds kunt kiezen uit vijf antwoorden. Ok?

6. Wat zijn uw associaties bij de term cyberweerbaarheid? *

7. We gaan nu de vijf verschillende aspecten van cyberweerbaarheid langs om in te schatten in welke fase uw bedrijf nu zit. (Ik als onderzoeker, noteer de punten) Reageert u snel, het gaat om een eerste beeld, er is geen 'goed' of 'fout'. De eerste vraag is: In hoeverre bent u bezig om kwetsbaarheden in uw digitale systemen in beeld te brengen? *
   Vink alle toepasselijke opties aan.

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

8. Kunt u kort benoemen wat uw bedrijf daaraan nu doet?

9. In hoeverre bent u bezig om via instellingen van software en computers uw weerbaarheid te vergroten? *
   Vink alle toepasselijke opties aan.
- Daar zijn we niet mee bezig omdat we niet weten hoe of omdat we het niet belangrijke vinden en we hebben er ook geen intentie toe
- We zijn er nog niet mee bezig maar hebben daar wel de intentie toe
- We zijn bezig voorbereidingen te treffen maar hebben nog geen harde actie ondernomen
- Dat vinden we belangrijk en zijn ook al druk bezig
- We vinden het belangrijk en zijn al erg ver gevorderd, dit willen we zo houden

10. Kunt u kort benoemen wat uw bedrijf daaraan nu doet?

11. In hoeverre bent u (bewust) bezig om via software-updates de weerbaarheid van uw organisatie te vergroten? *
    Vink alle toepasselijke opties aan.
- Daar zijn we niet mee bezig omdat we niet weten hoe of omdat we het niet belangrijke vinden en we hebben er ook geen intentie toe.
- We zijn er nog niet mee bezig maar hebben daar wel de intentie toe
- We zijn bezig voorbereidingen te treffen maar hebben nog geen harde actie ondernomen
- Dat vinden we belangrijk en zijn ook al druk bezig
- We vinden het belangrijk en zijn al erg ver gevorderd, dit willen we zo houden

12. Kunt u kort benoemen wat uw bedrijf daaraan nu doet?

13. In hoeverre bent u bezig om via toegangsrestricties (o.a. wachtwoorden) de weerbaarheid van uw organisatie te vergroten?
    Vink alle toepasselijke opties aan.
- Daar zijn we niet mee bezig omdat we niet weten hoe of omdat we het niet belangrijke vinden en we hebben er ook geen intentie toe.
- We zijn er nog niet mee bezig maar hebben daar wel de intentie toe
- We zijn bezig voorbereidingen te treffen maar hebben nog geen harde actie ondernomen
- Dat vinden we belangrijk en zijn ook al druk bezig
- We vinden het belangrijk en zijn al erg ver gevorderd, dit willen we zo houden

14. Kunt u kort benoemen wat uw bedrijf daaraan nu doet?

15. In hoeverre bent u bezig om virussen en malware buiten de deur te houden om zo de weerbaarheid van uw organisatie te vergroten?
    Vink alle toepasselijke opties aan.

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

16. Kunt u kort benoemen wat uw bedrijf daaraan nu doet?

17. Score: 5 t/m 8 = fase1, score 9 t/m 12 = fase 2, score 13 t/m 17 = fase 3, score 1821 = fase 4, score 22 t/m 25 = fase 5. Als we de scores op de vorige vijf vragen bekijken, lijkt uw bedrijf zich te bevinden in fase (nummer + naam van de fase + toelichting door onderzoeker!) Herkent u zich daarin en bent u bereid om met ons wat verder te kijken? *

Voordelen/nadelen: We gaan nu in op wat het als bedrijf zou kunnen opleveren/ kosten om meer aandacht te besteden aan de 5 basisaspecten. (eerst voordelen dan pas de nadelen)

18. Wat zijn de voordelen én nadelen om meer aandacht aan het inventariseren van kwetsbaarheden te besteden? *

19. Wat zijn de voordelen én nadelen om meer aandacht aan beheren van instellingen te besteden? *

20. Wat zijn de voordelen én nadelen om meer aandacht aan uitvoeren van updates van uw computersystemen en software te besteden? *

21. Wat zijn de voordelen én nadelen om meer aandacht aan het aanbrengen van toegangsrestricties te besteden? *

22. Wat zijn de voordelen én nadelen om meer aandacht aan de detectie en bestrijding van virus en malware te besteden? *

Stimulatie omgeving: De volgende vragen gaan over de stimulatie/ belemmering van de omgeving.

23. In welke mate en op welke wijze wordt u vanuit uw omgeving gestimuleerd én belemmerd om kwetsbaarheden in kaart te brengen? *

24. In welke mate en op welke wijze wordt u vanuit uw omgeving gestimuleerd én belemmerd om instellingen te beheren? *

25. In welke mate en op welke wijze wordt u vanuit uw omgeving gestimuleerd én belemmerd om updates uit te voeren? *

26. In welke mate en op welke wijze wordt u vanuit uw omgeving gestimuleerd én belemmerd om toegangsrestricties aan te brengen? *

27. In welke mate en op welke wijze wordt u vanuit uw omgeving gestimuleerd én belemmerd om virussen en malware op te sporen en te bestrijden? *

Zelfstandigheid: We gaan nu in op hoe het bedrijf zichzelf in staat acht middels de 5 basisprincipes. Dit aan de hand van verschillende factoren.

28. In welke mate en op welke wijze acht u zichzelf en uw bedrijf in staat om kwetsbaarheden in kaart te brengen? Denkt u hierbij aan vaardigheden, lerend vermogen, kapitaal, capaciteit *

29. In welke mate en op welke wijze acht u zichzelf en uw bedrijf in staat om instellingen te beheren? Denkt u hierbij aan vaardigheden, lerend vermogen, kapitaal, capaciteit *

30. In welke mate en op welke wijze acht u zichzelf en uw bedrijf in staat om updates uit te voeren? Denkt u hierbij aan vaardigheden, lerend vermogen, kapitaal, capaciteit *

31. In welke mate en op welke wijze acht u zichzelf en uw bedrijf in staat om toegangsrestricties aan te brengen? Denkt u hierbij aan vaardigheden, lerend vermogen, kapitaal, capaciteit *

32. In welke mate en op welke wijze acht u zichzelf en uw bedrijf in staat om virussen en malware op te sporen en te bestrijden? Denkt u hierbij aan vaardigheden, lerend vermogen, kapitaal, capaciteit *

In kaart brengen basisaspecten en factoren: En last but not least. Hoe gaat u om met het in kaart brengen van de basisprincipes of zijn er ook andere factoren?

33. Denkt u dat het zin heeft om kwetsbaarheden in kaart te brengen of denkt u dat andere factoren die buiten uw bereik liggen zoals ontwikkelingen in techniek of wetgeving een doorslaggevende betekenis hebben? *

34. Denkt u dat het zin heeft om instellingen te beheren of denkt u dat andere factoren die buiten uw bereik liggen zoals ontwikkelingen in techniek of wetgeving een doorslaggevende betekenis hebben? *

35. Denkt u dat het zin heeft om updates uit te voeren of denkt u dat factoren die buiten uw bereik liggen zoals ontwikkelingen in techniek of wetgeving een doorslaggevende betekenis hebben? *

36. Denkt u dat het zin heeft om toegangsrestricties aan te brengen of denkt u dat andere factoren die buiten uw bereik liggen zoals ontwikkelingen in techniek of wetgeving een doorslaggevende betekenis hebben? *

37. Denkt u dat het zin heeft om virussen en malware op te sporen en te bestrijden of denkt u dat andere factoren die buiten uw bereik liggen zoals ontwikkelingen in techniek of wetgeving een doorslaggevende betekenis hebben? *

38. Aan het begin constateerden we op basis van de QuickScan dat uw organisatie zich bevindt in fase <in te vullen door onderzoeker. >..... Klopt dat naar uw idee nog steeds? *

39. In welke fase schat u nu in dat uw organisatie zich bevindt? *
Markeer slechts één ovaal.
- o Precontemplatie: Geen intentie, geen actie
- o Contemplatie: Wel intentie, geen actie
- o Preparatie: Wel voorbereidingen, geen harde actie
- o Actiefase: Belangrijk! Concrete actie wordt ondernemen ter verbetering
- o Behoudfase: Veel actie al ondernomen, nu gericht op behoud van resultaten

Afsluiting. Graag maken we nu, ter afronding van dit gesprek, afspraken voor het tweede interview (akkood, datum inplannen en link sturen). Danken voor de intensieve sessie! *

Bijlage II: Interviewprotocol eenmeting (gedragsverandering)

Nogmaals dank voor uw medewerking aan dit onderzoek. U neemt deel aan ons onderzoek over de basisscan cyberweerbaarheid van het Digital Trust Center (onderdeel van het ministerie van Economische Zaken en Klimaat). Wij van de onderzoeksgroep Cybersafety (onderdeel van de NHL Stenden Hogeschool) voeren het onderzoek uit. Met de resultaten van het onderzoek, dus met uw feedback, wil het DTC kijken of de basisscan het weerbaarheidsgedrag van ondernemers verandert. Het onderzoek bestaat uit twee interviews, waarvan dit het tweede interview is. Dit interview bestaat uit vijf onderdelen, te weten:

1) Resumé: We zoomen in op de antwoorden uit het vorige interview 'Nulmeting' (uitleg fases)
2) Open vragen: We kijken naar in hoeverre u acties heeft ondernomen ten opzichte van de vijf basisprincipes (kwetsbaarheden, instellingen, updates, toegang en virussen/malware).
3) Stellingen: Er wordt u een aantal stellingen voorgehouden die uw overwegingen inzichtelijk maken. De stellingen hebben te maken met uw houding, (zelf)effectiviteit en de omgeving.
4) We kijken in welke fase u zichzelf inschat na het maken van de basisscan.
5) Slotvragen, over de basisscan algemeen en afronding van het interview.

Uw gegevens worden wederom geanonimiseerd verwerkt. Uw bedrijfsnaam en eigen naam worden niet gepubliceerd. Ik (de onderzoeker) noteer de antwoorden via een Google-forms formulier. Heeft u nog vragen voordat we kunnen beginnen?

Organisatienaam:

○ Resumé

We starten het interview met een korte samenvatting van het vorige interview. Wij (onderzoekers) lezen goed in over de geïnterviewde. Kort de fasen toelichten: pre-contemplatie t/m behoudfase.

1. Wanneer heeft u de basisscan gemaakt?

2. In hoeverre was de score die u uzelf gaf in het eerste interview in lijn met de 'resultaten' of de opmerkingen die de basisscan u gaf?

○ Acties ten opzichte van de basisprincipes

In het volgende onderdeel vragen wij u wat u hebt veranderd op het gebied van de vijf basisprincipes, ten opzichte van het eerste interview. Dus: de situatie nadat de ondernemer de basisscan heeft gemaakt.

3. In hoeverre hebben de resultaten van de basisscan u aangezet tot actie op een of meerdere basisprincipes?

4. Wat heeft u veranderd op het gebied van het inventariseren van kwetsbaarheden?

5. Wat heeft u veranderd op het gebied van instellingen van software en computers?

6. Wat heeft u veranderd op het gebied van (software-)updates?

7. Wat heeft u veranderd op het gebied van toegang(restricties)?

8. Wat heeft u veranderd op het gebied van het voorkomen van virussen en andere malware?

9. Wat waren op hoofdlijnen voor u de overwegingen al dan niet veranderingen door te voeren?

Stellingen

Wij zouden graag uw overwegingen inzichtelijk willen maken, dat willen wij doen door twaalf stellingen aan u voor te leggen.

○ Onderwerp 1: Houding

Voor- en nadelen om bezig te zijn met digitale weerbaarheid

10. Stelling 1) Ik vind nu dat meer inzetten op digitale weerbaarheid een meerwaarde is voor mijn organisatie.
    - ○ Ja
    - ○ Nee

11. Stelling 2) Ik ben mij bewust(er) geworden van de inspanningen die ik (nog) moet doen.
    - ○ Ja
    - ○ Nee

12. Toelichting: Open antwoord

○ Onderwerp 2: (zelf)Effectiviteit

Effectiviteit vertaald in: capaciteit, vaardigheden, kapitaal en lerend vermogen.

13. Stelling 3) Ik heb door de basisscan meer kennis van de zwakheden in mijn organisatie.
- Ja
- Nee

14. Stelling 4) De basisscan heeft inzichtelijk gemaakt welke toekomstige bedreigingen op mijn pad kunnen komen.
- Ja
- Nee

15. Stelling 5) Ik weet beter wat mij te doen staat om bedreigingen het hoofd te bieden.
- Ja
- Nee

16. Stelling 6) De basisscan heeft mij geholpen te bepalen welke kunde ik in huis moet halen.
- Ja
- Nee

17. Stelling 7) Ik heb een nauwkeuriger beeld van wat het gaat kosten om mijn organisatie in de toekomst digitaal weerbaarder te maken.
- Ja
- Nee

18. Stelling 8) Ik heb een nauwkeuriger beeld van wat voor tijd het gaat kosten om mijn organisatie in de toekomst digitaal weerbaarder te maken.
- Ja
- Nee

19. Toelichting: Open antwoord

○ Onderwerp 3: Omgeving

Stimulansen en belemmeringen: naast de basisscan kunnen ook andere actoren (denk aan overheid, kennisinstellingen en branchegenoten) vanuit de omgeving de ondernemer beïnvloeden. De ondernemer kan gestimuleerd, maar ook belemmerd worden.

20. Stelling 9) De overheid stimuleert mij – op andere manieren dan de basisscan - om mijn digitale weerbaarheid te vergroten.
- Ja
- Nee

21. Stelling 10) Branchegenoten inspireren mij niet over digitale weerbaarheid.
- Ja
- Nee

22. Stelling 11) Kennisinstellingen leren mij om in te zetten op digitale weerbaarheid.
- Ja
- Nee

23. Stelling 12) Zakenpartners belemmeren mij om in te zetten op digitale weerbaarheid (denk aan banken, verzekeringen, etc.)
- Ja
- Nee

24. Zijn er andere actoren die u stimuleren dan wel belemmeren?

25. Toelichting: Open antwoord

Fase van gedragsverandering

26. In welke fase van gedragsverandering denkt u dat u nu zit?
- Pre-contemplatiefase
- Contemplatiefase
- Preparatiefase
- Actiefase
- Behoudfase

27. In hoeverre heeft het maken van de bassiscan geleid tot eventuele verandering van fase?

28. Waarom heeft dit wel/niet tot verandering geleid van fase?

Basisscan algemeen

Zijn er nog andere op- en aanmerkingen aan de basisscan?

29. Wat wilt u nog kwijt over de basisscan?

30. Heeft u nog tips voor de ontwikkelaars van de basisscan?

Afsluiting interview

We zijn bij het einde van het interview aangekomen. Wij willen u bedanken dat u heeft meegedaan aan dit onderzoek! Wij gaan de resultaten anoniem verwerken in het onderzoek. Als u verder nog vragen heeft, kunt u ons benaderen.

---

i