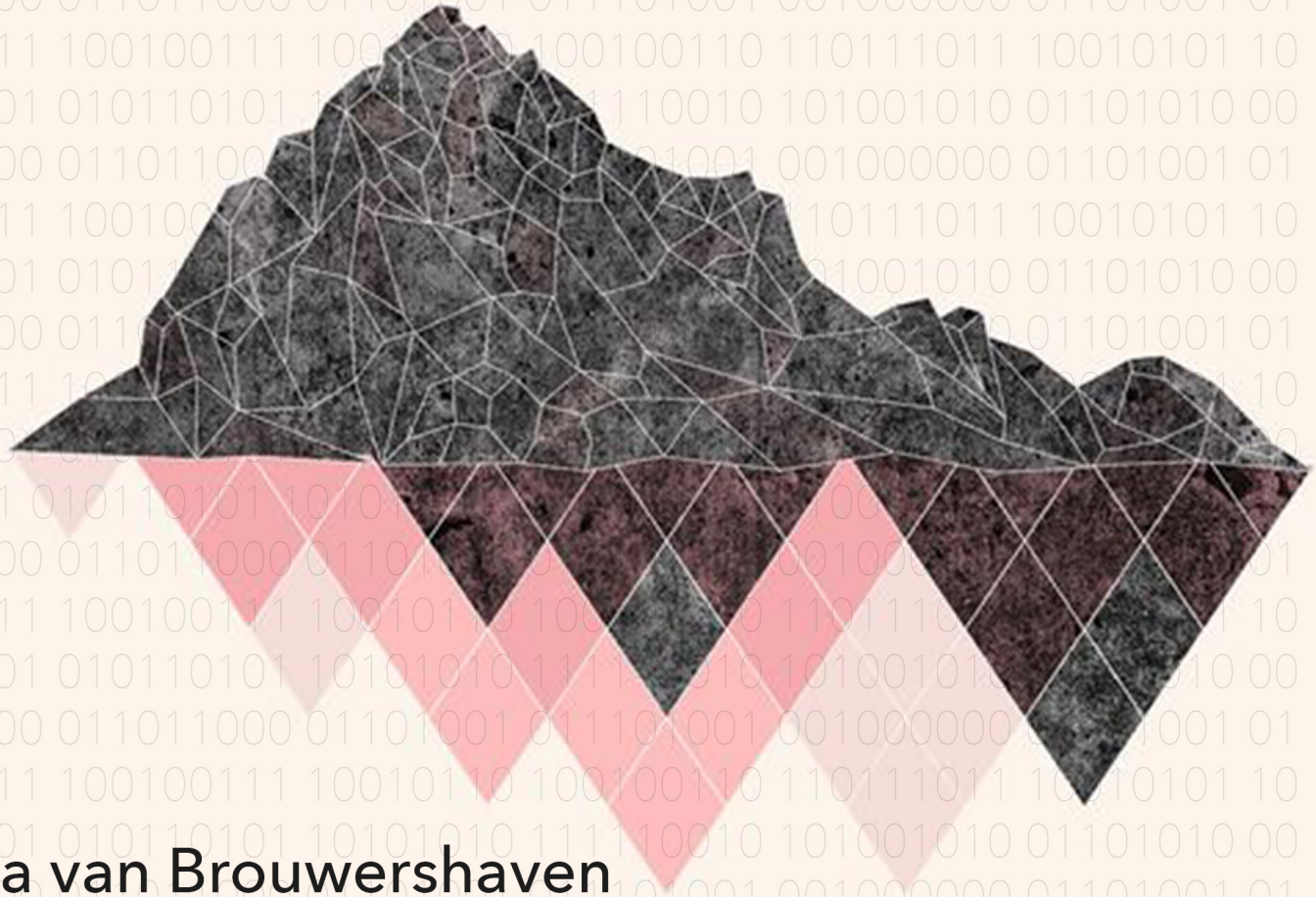
BLIND VERTROUWEN

Een kwalitatief onderzoek naar de rol van de onzichtbaarheid van het internet in het vertrouwen dat webshopmanagers in de mkb-detailhandel hebben in hun risicobenadering van cybercrime.



Josta van Brouwershaven

Masterscriptie Organisaties, verandering en management

NEDERLANDS CYBER COLLECTIEF

Universiteit Utrecht

BLIND VERTROUWEN

Een kwalitatief onderzoek naar de rol van de onzichtbaarheid van het internet in het vertrouwen dat webshopmanagers in de mkb-detailhandel hebben in hun risicobenadering van cybercrime.

Josta van Brouwershaven

Master Organisaties, verandering en management

Utrechtse School voor Bestuurs- en Organisatiewetenschappen

Begeleider en eerste lezer

Dr. Maikel Waardenburg

Tweede lezer

ir. Peter Linde MLD

Een onderzoek in opdracht van het Nederlands Cyber Collectief.

Utrecht University

NEDERLANDS CYBER COLLECTIEF

“I don't know why people are so keen to put the details of their private life in public; they forget that invisibility is a superpower.”

- Banksy

Voorwoord

"Lieve"…"Nee." "Beste"… "Nee." "Hallo"… "Ja, dat zal wel een prima begin zijn." Ik was dertien en zat in het eerste jaar van de middelbare school toen ik mijn eerste e-mailadres kreeg. Met de hele klas gingen we corresponderen met een klas uit Curaçao. Ik weet nog dat de klas het wel spannend vond. Het was net 2000 en er was toch 'iets' met computers, internet en het vergaan van de wereld? "Nou ja, als de juffrouw het goed vindt zal het wel goed zijn." Op een blaadje stond het e-mailadres en de naam van het meisje waar ik naar moest mailen. Ik weet nog dat ik niet zo goed wist wat ik moest schrijven of wat ik wilde weten. De docente vertelde ondertussen hoe bijzonder het was dat we nu gemakkelijk met mensen van over de hele wereld contact konden hebben, hoeveel tijd ons dit zou besparen en o ja, we moesten ons wachtwoord wel onthouden en mochten dit aan niemand anders vertellen. Aan het eind van de les verzond ik tevreden mijn allereerste mailtje en ging ik naar huis.

Een week later moest ik op gesprek komen bij dezelfde docente. Ze was woedend. Hoe haalde ik het in mijn hoofd om zo'n mail te sturen?! Ik snapte er niks van. "Was ik iets vergeten?" "Stonden er spelfouten in?" Ik weet nog dat ik mij heel naar en onzeker voelde, want het was wel duidelijk dat mijn mail fout was. Na een paar minuten liet ze mij de mail lezen. Ik wist niet wat ik zag. Het was een gemene mail vol scheldwoorden. "Deze mail heb ik niet geschreven!" Maar dit geloofde de docente niet, want de mail was immers verstuurd vanaf mijn account. "En je hebt je wachtwoord toch aan niemand gegeven?" Nee, dat had ik niet, maar ik had ook niet die mail gestuurd. Ik voelde me machteloos. Want hoe kon ik mijn onschuld bewijzen, terwijl voor mij het 'bewijs' lag dat ik schuldig was? Uiteindelijk besloot de docent aan de rest van de klas te vragen of iemand anders dit had gedaan. Dit was het geval. Twee leerlingen gaven toe dat zij de mail hadden gestuurd. Gewoon, omdat het kon. Hoewel het meisje waarmee ik contact had in eerste instantie boos was, was het contact na een paar excuusmails weer 'hersteld'. Of eigenlijk, konden we toen pas beginnen. Ik had nog geen week een e-mailadres en kreeg al te maken met een keerzijde van het internet: identiteitsfraude. Klasgenoten hadden zich voorgedaan als mij en ik kon niet bewijzen dat ik onschuldig was…

Ruim zestien jaar later is *cybercrime* aan de orde van de dag. En hoewel de misdaadvorm al lang bestaat, is cybercrime en de bescherming daartegen – *cybersecurity* – in de organisatiewetenschap nog een onderbelicht onderwerp. Dat ik dit onderzoek kon doen, heb gedaan en tot een goed einde heb weten te brengen heb ik te danken aan een aantal mensen.

Het laatste half jaar van mijn studie is een bijzondere tijd geworden omdat ik de kans kreeg mij te verdiepen in een onderwerp waar ik mij graag in wil specialiseren: cybersecurity. Chris, ik wil jou als eerst bedanken voor de kans die je mij hebt gegeven om dit onderzoek voor het Nederlands Cyber Collectief te mogen uitvoeren. Maar ook voor de vrijheid om dit op een manier te doen die aansloot bij zowel jullie wensen, als die van de USBO en mij. En tot slot voor je scherpe en praktische blik als ik om feedback vroeg. Mary-Jo, ik wil jou bedanken voor alle inspirerende gesprekken over cybercrime en jouw visie hierop. Ik heb veel van je geleerd! Robert, bedankt voor je hulp om mee te denken hoe een brug te slaan tussen het NCC en de USBO. Jouw constructieve blik heeft mij verder geholpen. Verder wil ik het *Cyberteam* als geheel bedanken voor het waardevolle inzicht dat jullie mij hebben gegeven over hoe een private-organisatie kijkt naar cybercrime en met passie probeert het mkb te bereiken.

Daarnaast wil ik graag alle webshopmanagers bedanken. Bedankt voor jullie tijd en voor jullie openheid over de wijze waarop jullie de wereld van cybercrime en cybersecurity zien. Maar ook voor jullie dapperheid om te praten over een onderwerp waar de meeste van jullie niks over wisten. Zonder jullie had ik dit onderzoek niet kunnen voltooien.

De combinatie van een private organisatie die voornamelijk gericht is op de praktijk in combinatie met de kwalitatieve interpretatieve onderzoeksmethode van dit onderzoek was meer dan eens een uitdaging. Maikel, bedankt dat je de wetenschapper in mij bewaakt hebt op de momenten dat het erop leek dat ik te praktisch werd. Je kritische blik op de theorie maakt dat hier nu een wetenschappelijk onderzoek ligt. Peter, bedankt voor je feedback op mijn concept. Jouw andere blik vulde voor mijn gevoel de visie van Maikel aan, waardoor ik op verschillende punten mijn onderzoek heb kunnen aanscherpen. Ik vond de combinatie daarom erg waardevol.

Kees, jij liet mij tijdens de stage bij D66 (weer) inzien dat cybersecurity een belangrijk, intrigerend en leuk onderwerp is. Dankzij dit inzicht besloot ik hier meer over te willen leren en er mijn scriptie over te schrijven. Bedankt daarvoor! Onno, Anna, Eline en Marloes, wat ontzettend fijn dat ik jullie dit jaar heb leren kennen! Van handen warm houden in Manchester tot 'haarfijne analyses', mede dankzij jullie was de master een onvergetelijk tijd. Bedankt! En dan natuurlijk nog mama, Jan Willem, Debby, Mano, papa en Dennis. Bedankt dat jullie er de afgelopen jaren voor mij waren! Voor steun, maar ook voor leuke afleiding op de juiste momenten. Mede dankzij jullie ligt dit onderzoek hier. En tot slot wil ik in het bijzonder opa Beke bedanken. Jaren geleden beloofde ik u om te gaan studeren. U bent er al elf jaar niet meer, maar ik heb altijd aan ons gesprek van toen gedacht op de momenten dat ik het even niet meer zag zitten. Het motiveerde mij om door te gaan, waardoor u de afgelopen jaren een onzichtbare, maar belangrijke steun voor mij was.

Josta van Brouwershaven

Utrecht, 31 augustus 2017

Abstract

Dit onderzoek formuleert een antwoord op de vraag hoe webshopmanagers in de mkb-detailhandel omgaan met de onzichtbaarheid van het internet en welke rol deze onzichtbaarheid speelt in hun risicobenadering van *cybercrime*. De webshopmanagers uit deze casus hebben persoonlijke, werk en collectieve (nieuwsberichten) ervaringen met cybercrime. De betekenis die ze hieraan geven, gebeurt niet volgens de rationele benadering, maar volgens de intuïtieve benadering. Waarbij ze afgaan op hun gevoel. De onzichtbaarheid van het internet neemt met zich mee dat de meeste webshopmanagers geen zichtbare of tastbare schade ondervinden. Dit geeft hen het idee dat hun bedrijf geen slachtoffer is van cybercrime en dat hun *cybersecuritybeleid* tot op heden succesvol is. Het cybersecuritybeleid van de onderzochte webshops, bestaat uit twee hoofdonderdelen. Allereerst zijn er zichtbare vertrouwens-factoren die de webshopmanagers zelf als consument belangrijk vinden en tevens doorvoeren in hun eigen webshop. Ten tweede is er het vertrouwen in experts die zorgen voor zichtbare beveiliging zoals SSL-certificaten, *Payment Service Providers* en keurmerken. Het grote vertrouwen dat webshopmanagers hebben in experts, hoeft niet gerechtvaardigd te zijn, maar omdat zichtbare of voelbare schade uitblijft hebben de webshopmanagers niet het gevoel dat een wijziging van het cybersecuritybeleid nodig is.

Inhoudsopgave

1. Inleiding

1.1 Introductie cybercrime en cybersecurity

Met de komst van het internet is ook een nieuwe vorm van criminaliteit opgestaan: *cybercrime*. De politie definieert cybercrime als "criminaliteit met ICT als middel én doelwit." (website politie, 2017). Daders van deze criminaliteit worden ook wel cybercriminelen of hackers genoemd. Niet alle hackers zijn cybercriminelen. Zo zijn er ook ethische hackers, die met hun computerinbraak enkel een beveiligingsrisico aan het licht willen brengen (Timmerman, 2013, p. 1). Er zijn verschillende vormen van cybercrime, maar voor dit onderzoek zijn de hackers die geld willen verdienen aan de digitale inbraak of de informatie die zij kunnen ontvreemden via websites het belangrijkst. Hierbij kan gedacht worden aan *ransomeware*, waarbij criminelen gegevens op de computer 'gijzelen' en deze pas vrijgeven als hier losgeld voor is betaald. Een andere vorm van cybercrime is dat de hacker via *malware* – zonder dat de gebruiker dit doorheeft – privacygevoelige gegevens, van wachtwoorden tot creditcardgegevens, verzamelt (website politie, 2017).

Organisaties die informatie opslaan op de computer en verbinding hebben met het internet kunnen slachtoffer worden van cybercrime. Als een webshop bijvoorbeeld onbeveiligd is, kunnen hackers relatief gemakkelijk gevoelige informatie stelen. Het beschermen van de informatie wordt *cybersecurity* genoemd. De definitie die de Rijksoverheid hiervoor aanhoudt is "het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT" (website NCTV, 2017). Hoewel cybercrime onopgemerkt (onzichtbaar) kan plaatsvinden, laten twee recente – wereldwijde – aanvallen met gijzelsoftware zien dat de (fysieke) gevolgen van slecht cybersecuritybeleid groot kunnen zijn. Als eerst werden er op 12 mei 2017 in vele landen computers van verschillende ziekenhuizen en bedrijven gegijzeld door het programma *WannaCry* (website NOS A, 2017). De tweede ransomeware-aanval begon een maand later, op 27 juni 2017, en gijzelde voornamelijk grote bedrijven. Zo lag een groot havenbedrijf in Rotterdam (APM) er dagenlang uit en werd ook pakketbezorger TNT getroffen (website NOS B, 2017). De tastbare gevolgen van deze cybercrime waren als eerste het financiële verlies dat organisaties hadden door zowel het betalen van losgeld als door de vertraging die zij opliepen. Ten tweede konden zij ook waarnemen welke informatie gegijzeld werd. Ten derde geeft een aanval in het ziekenhuis weer dat cybercrime ook voor fysieke schade kan zorgen als hackers bijvoorbeeld knoeien met patiëntgegevens. Zo konden sommige kankerpatiënten hun chemokuur niet krijgen. De onzichtbare gevolgen van cybercrime kunnen onder andere zijn dat gestolen persoonsgegevens, zoals een paspoortkopie en creditcardgegevens, verhandeld worden op het *dark web*, de ondergrondse wereld van het internet waar anoniem internetverkeer plaatsvindt.

1.1.1 Wetgeving

De ontwikkelingen op het gebied van cybercrime laten zien dat de kans aanwezig is dat organisaties hier slachtoffer van worden. Om hen te dwingen om informatie van burgers, zoals klanten en medewerkers, beter te beschermen zijn er vanuit de overheid twee wetten aangenomen. Ten eerste is er de Wet Bescherming Persoonsgegevens (WBP) die stelt dat een organisatie persoonsgegevens op een bepaalde manier moet opslaan. Vanaf 2018 zal deze wet vervangen worden door de Algemene Verordening Gegevensbescherming (AVG). Deze geldt voor de hele Europese Unie, waar de wet de naam *General Data Protection Regulation* (GDPR) draagt (website autoriteit persoonsgegevens, 2017). Mocht er toch

een datalek zijn, dan is er ten tweede de Meldplicht Datalekken. Dit is een uitbreiding op de WBP. Deze wet verplicht publieke en private organisaties melding te maken van een inbreuk op de beveiliging die kan leiden tot diefstal, verlies of misbruik van persoonsgegevens (website Rijksoverheid A, 2017).

Zowel de Meldplicht Datalekken als de AVG lijken tot nu toe weinig invloed te hebben. Zo sprak de Autoriteit Persoonsgegevens in februari 2017 uit dat zij vermoeden dat organisaties datalekken niet melden (website Tweakers, 2017). Dat dit vermoeden klopt blijkt uit een onderzoek waarin staat dat maar een derde van de bedrijven met dertig of meer medewerkers datalekken melden (website Kaspersky, 2017). Daarnaast blijkt uit een surveyonderzoek onder 900 besluitvormers van bedrijven in Europa dat het bedrijfsleven nog niet klaar is voor de AVG. Zo geeft 91 procent van de respondenten aan zich zorgen te maken over hun organisatievermogen om aan deze wet te voldoen. Slechts 22 procent ziet het nakomen van deze wet als een topprioriteit en maar 26 procent denkt dat hun organisatie op tijd passend beleid heeft (website Symantec, 2016). Hoewel het cybersecuritybeleid bij grote organisaties ook niet helemaal in orde is, zijn zij zich over het algemeen bewuster en hebben dan ook uitgebreider cybersecuritybeleid. Ook maken zij duidelijke afspraken met ICT-leveranciers over wat, wanneer aan wie mag worden verstrekt (Martijn en Tokmetzis 2016, p. 105). Dit in tegenstelling tot het mkb. Diverse rapporten van publieke- en private organisaties tonen aan dat het cybersecuritybeleid in het mkb onvoldoende is (Rathenau, 2017; Interpolis 2015).

1.1.2 Risico benadering

Omgaan met het risico op cybercrime kan op twee manieren benaderd worden: rationeel en intuïtief. In economisch wetenschappelijke literatuur wordt op een rationele manier naar risico's gekeken. Risicoanalisten, experts en beleidsmedewerkers maken risicoanalyses op basis van of iets gaat gebeuren en hoe slecht de uitkomst van zo'n gebeurtenis is. De uitkomst van een berekening die zij hierop loslaten leidt tot de *expected value* (Stone, 2012, p. 131-132). Op deze manier kan je volgens aanhangers van de rationele benadering objectief een risico inschatten en hiernaar handelen. Hiertegenover staat de intuïtieve benadering uit de economisch-psychologische wetenschappelijke literatuur. Hierbij gaan wetenschappers er vanuit dat mensen risico's niet rationeel benaderen omdat mensen snel keuzes maken en afgaan op intuïtieve antwoorden (Kahneman, 2011, p.52). Het gaat vaak om een gevoel en niet om feiten en cijfers (Stone, 2012, p. 134). Onderzoek naar de risicobenadering van burgers laat zien dat zij risico's vaak over- of onderschatten. Zo bleek uit Amerikaans onderzoek dat Amerikanen meer vlieg- en terreurangst kennen dan angst voor autorijden. Dit terwijl er meer mensen overlijden aan een auto-ongeluk dan aan een terreuraanslag (Dan Gardner, 2008 in: Gabriels, 2017). De vlieg- en terreurangst is in dit geval een overschat risico, terwijl het risico op een auto-ongeluk wordt onderschat.

Organisaties hebben de verantwoordelijkheid om de informatie die zij van klanten en medewerkers hebben te beschermen. Om te weten welke mate van cybersecurity zij nodig hebben, moeten zij het risico op cyberaanvallen inschatten. Op basis van deze inschatting kunnen zij hun cybersecuritybeleid aanpassen. Het risico op cybercrime wordt tot op heden rationeel benaderd door zowel wetenschappers, als bijvoorbeeld verzekeringsmaatschappijen. De focus ligt op hoe organisaties moeten handelen op basis van de *expected value*. Er is in de organisatiewetenschap nog geen kwalitatief onderzoek gedaan naar de risicobenadering van organisaties op cybercrime. Dit onderzoek geeft hier inzicht in en laat zien dat specifiek webshopmanagers het risico op cybercrime intuïtief benaderen.

1.1.3 Onzichtbaarheid

De intuïtieve benadering houdt rekening met het belang van zichtbaarheid. Mensen trekken conclusies en maken beslissingen op basis van dat wat zij zien, *"what you see is all there is"* (Kahneman, 2013, p. 93). Organisaties zijn met de komst van het internet zichtbaarder geworden. Zo zijn organisaties onder andere transparanter geworden over het beleid dat zij voeren (Zyglidopoulos & Fleming, 2011, 692). Dit doen zij mede omdat de zichtbaarheid ook problemen met zich meebrengt, namelijk: negatieve zaken over onethisch handelen of risicovolle praktijken komen sneller aan het licht (Zyglidopoulos & Fleming, 2011, 692). Een goed voorbeeld hiervan zijn de berichten over slechte arbeidsomstandigheden in textielfabrieken. Kledingmerken worden zo door de maatschappij gedwongen te investeren in ethisch beleid (Bowen, 2000, p. 94). Hoewel het internet de wereld en haar mensen en bedrijven zichtbaarder maakt, is het paradoxale dat het internetproces zelf voor velen onzichtbaar is. Hierdoor kunnen cybercriminelen intentioneel onzichtbaar misbruik maken van het internet en zo gevoelige informatie ontvreemden van organisaties (Moore, 1985, p. 272). En het massaal inzetten van ethisch hackers om kwetsbaarheden te onthullen kan alleen volgens strenge richtlijnen (*Responsible Disclosure* geheten), omdat onthullingen ervoor kunnen zorgen dat kwaadwillende partijen hier misbruik van maken (rapport CSBN, 2017). Anders dan bij andere maatschappelijke infrastructuur, is het internet (voorlopig) grotendeels onzichtbaar (ondergrondse kabels en kasten, digitale data en etherfrequenties in de lucht). Naar de rol van deze onzichtbaarheid is tot op heden geen onderzoek gedaan. Dit onderzoek vult deels de lacune door te laten zien welke rol onzichtbaarheid speelt in de betekenis die webshopmanagers geven aan het omgaan met de kans op cybercrime.

1.2 De probleemstelling

1.2.1 De cybercrime benadering van het Nederlands Cyber Collectief

Het Nederlands Cyber Collectief (NCC) is onderdeel van Nationale Nederlanden (NN) en speelt in op de situatie dat het mkb zich nog niet voldoende beschermt tegen cybercrime. In box 1 geef ik kort weer hoe het NCC zich verhoudt tot NN en wat hun doel is.

Box 1

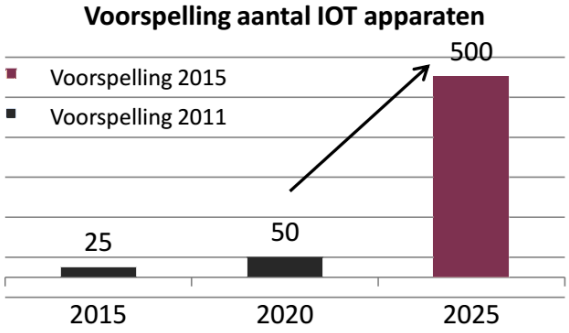
Nationale Nederlanden is een financiële dienstverlener. In 2015 startte zij een innovatielab: Sparklab. "In Sparklab worden kansen onderzocht, nieuwe markten gevonden en verrassende producten en diensten ontwikkeld voor de wereld van overmorgen"… "Zo testen we hoe het toekomstige business model van een financiële dienstverlener eruit kan zien." Het Nederlands Cyber Collectief is hier onderdeel van en is sinds 29 november 2016 publiekelijk actief.

Het doel van het collectief is: "Samen Nederland Internetveilig maken." Ze willen het onderwerp cybercriminaliteit toegankelijk maken voor de mkb-er, in de taal van de ondernemer. Dit pogen zij te doen door van de huidige versnippering in aanpak, één geheel te maken. In samenwerking met commerciële en niet-commerciële partijen brengen zij de risico's in kaart. Dit doen zij door middel van verschillende diensten, informatie en tips.

Bron: website Nationale Nederlanden, 2017.

In de allereerste week van mijn onderzoek gaf het '*cyberteam*' meerdere presentaties die goed inzicht geven in hun motivatie om het mkb te bereiken. Zij focussen zich hierbij ten eerste op de ontwikkelingen van de 'cyberwereld' en gebruiken de bijbehorende feiten en cijfers om aan te tonen dat het risico op cybercrime groot is en de komende jaren alleen maar toeneemt. Ten tweede koppelen zij dit vervolgens aan rapporten die inzicht geven in de verwachte cybercrime toename in het mkb. Zij benaderen het risico op cybercrime op een rationele manier. Om inzage te geven in de denkwijze van het NCC geef ik hieronder, op basis van de PowerPoints, beknopt in zes stappen weer hoe het NCC redeneert:

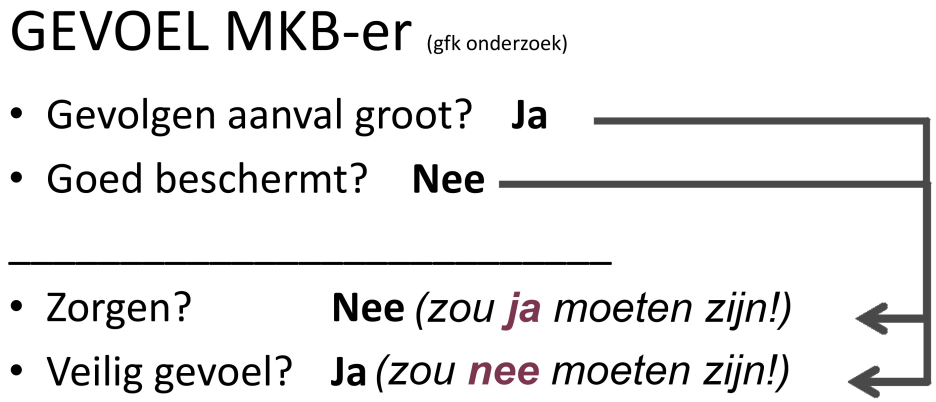
1. "Er is een enorme toename van aantal met het internet verbonden apparaten (het Internet of Things, IOT) en de hoeveelheid data neemt exponentieel toe." Afbeelding 1 laat de verwachting van het aantal verbonden apparaten met internet per miljard zien:



Afbeelding 1

2. "Door de toename van de hoeveelheid aan internet verbonden apparaten en data ontstaat er een cyber risico."…"In de VS wordt geschat dat 60% van het mkb failliet gaat binnen 6 maanden na een cyberaanval."
3. "Cybercriminaliteit veroorzaakt in Nederland jaarlijks nu al voor 8,8 miljard schade hetgeen gaat verdrievoudigen in 5 jaar tijd."…"Schatting schade wereldwijd: 400 miljard in 2014 wat verdrievoudigt naar 1200 miljard in 2019."
4. "Experts geven aan dat het mkb attractieve targets zijn omdat ze minder goed beveiligd zijn en omdat automatisering cybercriminelen in staat stelt om op grote schaal aanvallen te doen tegen lage investering."
5. "Er wordt gedacht dat deze criminelen zich richten op het middenbedrijf omdat ze niet meer tegen de geavanceerde cybersecurity technologie bij grote corporaties op kunnen."
6. "80 procent van het mkb heeft zijn cybersecuritybeleid nog niet in orde."

Daarom biedt het NCC in samenwerking met partners verschillende cybersecurity-producten aan voor het mkb (PowerPoint A & B NCC, 2017). Producten die gezien het risico op cybercrime kunnen passen bij de behoeften van deze doelgroep. Tot op heden lukt het hen nog niet om het mkb goed te bereiken. Zij wijzen mij op een kwantitatief onderzoek van het GFK (voor het NCTV) dat het gebruikersperspectief van consumenten en professionals in kaart brengt. Het rapport geeft inzicht in onder andere het mkb, maar geeft geen verdieping over de betekenis die mensen aan bijvoorbeeld 'slachtofferschap' geven. Het NCC vult dit daarom zelf in. Op basis van conclusies uit het onderzoek heeft het NCC de volgende slide gemaakt:



Afbeelding 2, Bron: PowerPoint C NCC, 2017.

Afbeelding 2 laat zien dat het gevoel van de mkb-er volgens het NCC niet klopt. Met de feiten en cijfers over cybercrime en het mkb lukt het hen tot op heden niet goed om het mkb te overtuigen van hun cybersecurity-producten. Daarom is de vraag van het NCC aan mij: "Hoe kan het Nederlands Cyber Collectief het mkb proberen te bereiken?"

De onderzoekscasus: van 'het mkb' naar mkb-detailhandel

Aangezien ik niet het hele midden- en kleinbedrijf kon onderzoeken, heb ik een sector uitgekozen. Ik heb gekozen voor de detailhandel en hierbinnen specifiek voor webshops. Dit omdat uit de omzet van alle webwinkels samen blijkt dat steeds meer mensen online producten kopen. Zo steeg de omzet van alle webwinkels samen met 19,4 procent in 2016. Binnen de webshops zijn online-kledingwinkels de belangrijkste categorie. Sinds 2013 steeg de omzet bij kledingwebshops met 68 procent en nam het aantal webshops met 62 procent toe (websites CBS A, B & C 2017). Ruim 97 procent van het bedrijfsleven maakt deel uit van het mkb (Rathenau Instituut, 2017, p. 23). Dit betekent dat veel (nieuwe) webshops hier deel van uitmaken. De groei van het aantal webshops geeft ook aan dat klanten steeds vaker persoonlijke informatie achterlaten bij de desbetreffende organisatie. Dit doen zij niet zonder zorgen. Zo blijkt uit een kwantitatief onderzoek van Symantec (2015) dat klanten in Europa weinig vertrouwen hebben in de manier waarop webshops omgaan met hun klantdata (p. 20). Slechts 14 procent denkt dat retailers hun data goed beschermen. Het vertrouwen is mede zo laag omdat klanten zich zorgen maken over het profijt dat organisaties hebben bij het verzamelen van persoonlijke informatie. Zo denkt 70 procent van de respondenten dat hun persoonlijke informatie wordt doorverkocht aan derde partijen (Symantec, 2015, p. 20 – 23).

De keus voor webshops in de detailhandel is een interessante casus vanwege de stijging in zowel aantal als omzet, maar ook omdat klanten deze sector het minst vertrouwen terwijl zij hier ondertussen wel persoonlijke gegevens achterlaten. Binnen de webshops in de mkb-detailhandel heb ik ervoor gekozen om met webshopmanagers te praten, omdat zij beslissingen maken op het gebied van cybersecurity. In hoofdstuk 3, paragraaf 3.2.2 geef ik gedetailleerder inzicht over de selectie van de webshopmanagers en bijbehorende kenmerken.

Het lukt het Nederlands Cyber Collectief dus niet goed om het mkb te bereiken. Zij hebben daarom meer inzicht nodig in het standpunt van deze doelgroep op het gebied van cybercrime. In dit onderzoek probeer inzicht te geven in de visie van de webshopmanager in de mkb-detailhandel. Op deze manier probeer ik het NCC handvatten te geven hoe zij de webshopmanager in het mkb met meer succes kunnen benaderen. Dit leidt tot de eerste doelstelling van dit onderzoek:

Doelstelling 1: Advies geven over de manier waarop het Nederlands Cyber Collectief de webshopmanagers in de mkb-detailhandel kunnen benaderen.

Dit onderzoekt vormt de basis voor deze doelstelling, maar wordt uitgewerkt in een adviesrapport.

1.2.2 Risico benadering

De feiten en cijfers laten zien dat de kans op een cyberaanval groot is en de overheid heeft al wetten aangenomen om organisaties te dwingen burgers te beschermen. De onderzoeken gaan vaak over hoe het mkb moet handelen en een kwantitatief communicatie-onderzoek over het gebruikersperspectief van consumenten en professionals, geeft geen kwalitatief inzicht over de manier waarop het mkb omgaat met cybercrime, maar heeft als doel te beoordelen hoe "veilig of onveilig men zich online gedraagt" (GFK, p. 4). In paragraaf 1.1.3 beschreef ik dat risico's op een rationele en intuïtieve manier benaderd kunnen worden. Eerder onderzoek naar de risicobenadering van burgers laat zien dat zij risico's intuïtief benaderen en deze daardoor vaak over- of onderschatten. Uit dit onderzoek blijkt dat webshopmanagers het risico op cybercrime ook op organisatieniveau intuïtief benaderen. In de organisatiewetenschap is de intuïtieve benaderingswijze van het risico op cybercrime nog onderbelicht. Dit onderzoek draagt daarom ook bij aan de empirische kennis op dit vlak door dit hiaat deels te vullen met inzichten over hoe webshopmanagers met deze risico's omgaan. Dit leidt tot de tweede doelstelling:

Doelstelling 2: Inzicht verkrijgen in de wijze waarop webshopmanagers omgaan met de risico's van cybercrime.

1.2.3 Rol van onzichtbaarheid

Uit de gesprekken met de webshopmanagers blijkt dat ervaringen een grote rol spelen bij de manier waarop zij betekenis geven aan het risico op cybercrime. Betekenisgeving behelst een voortdurende ontwikkeling van plausibele beelden die rationaliseren wat mensen aan het doen zijn (Weick & Sutcliffe, 2005, p. 409). Dit gebeurt via taal, gesprekken en communicatie en is niet rationeel omdat mensen hun eigen ervaringen gebruiken als basis voor het begrijpen van situaties en het nemen van actie in de organisatie (Choo, 1996; Weick & Sutcliff, 2005). In paragraaf 1.1.3 beschreef ik al dat het internetproces onzichtbaar is, waardoor cybercriminelen onzichtbaar misbruik kunnen maken van het internet en zo gevoelige informatie kunnen ontvreemden van organisaties. Hierdoor hoeven mensen niet te ervaren dat zij bestolen zijn. Dit maakt dat de rol van onzichtbaarheid belangrijk is voor de betekenis die webshopmanagers geven aan het omgaan met cybercrime. Enkel afgaan op dat wat je zelf ervaart staat haaks op de rationele benadering van het NCC. Meer inzicht krijgen in de rol van onzichtbaarheid bij de beoordeling van de risico's op cybercrime is voor hen belangrijk omdat zij zo meer helderheid krijgen over hoe zij het mkb kunnen benaderen. In de organisatie-wetenschappelijke literatuur is wel aandacht besteed aan de rol van zichtbaarheid, maar hierbij gaat het voornamelijk over het zichtbaar maken of

worden van problemen die duiden op onethisch handelen of risicovolle praktijken. De rol van de onzichtbaarheid van het internet in organisaties is onderbelicht. Hierdoor is het enkel voor cybercriminelen of ethisch hackers mogelijk om te controleren hoe organisaties omgaan met cybercrime. Dit onderzoek laat daarom zien dat juist onzichtbaarheid een groter podium verdient in de organisatiewetenschap. Dit leidt tot de derde doelstelling van dit onderzoek:

Doelstelling 3: Begrip krijgen van de rol van onzichtbaarheid bij het beoordelen van het risico op cybercrime.

Uit mijn onderzoek blijkt dat onzichtbaarheid een rol speelt bij de wijze waarop webshopmanagers betekenis geven aan het vertrouwen in hun huidige cybersecuritybeleid. Etzioni (2017) laat zien dat het internet verandering heeft gebracht in onze vertrouwensnorm, namelijk: *"it raised being a stranger to a new order of magnitute by providing a very high level of anonymity"* (p. 2). Uit zijn onderzoek blijkt dat zichtbaarheid belangrijk is voor het online vertrouwen van consumenten. Zo halen zij vertrouwen uit bijvoorbeeld het design van de website en zichtbare samenwerkingen met zogenoemde *trust-building platforms* (Etzioni, 2017, pp. 3-8). Dit onderzoek geeft inzicht in de betekenis die webshopmanagers geven aan deze bronnen van vertrouwen. Etzioni (2017) gaat in zijn onderzoek uit van een gelijkwaardige vertrouwensband tussen de klant en verkoper, maar onderzoek van McEvily, Zaheer en Fudge Kamal (2017) naar interorganisationeel vertrouwen wijst uit dat er altijd gevaren zijn – *exchange hazards* – die kunnen leiden tot een onevenredige vertrouwensband (Etzioni, 2017, p. 2; McEvily et al., 2017, pp. 76-77). Of een band gelijkwaardig is hangt af van de unieke doelen, voorkeuren en kwetsbaarheden van organisaties (McEvily et al., 2017, p. 75). McEvily et al. (2017) geven aan dat er nog meer onderzoek gedaan moet worden naar de vertrouwensband tussen organisaties. Uit dit onderzoek blijkt dat de webshopmanagers veel vertrouwen hebben in experts. Dit onderzoek maakt een start door inzicht te geven in de betekenis die webshopmanagers geven aan het vertrouwen in experts. Het voortbouwen op de theorieën over vertrouwen leidt tot de vierde en laatste doelstelling:

Doelstelling 4: Begrip krijgen van de rol van vertrouwen bij de benadering van het risico op cybercrime.

Deze vier doelstellingen vormen samen de volgende hoofdvraag voor dit onderzoek:

Welke rol speelt de onzichtbaarheid van het internet in het vertrouwen dat webshopmanagers in de mkb-detailhandel hebben in hun risicobenadering van cybercrime?

1.3 Relevantie

In deze paragraaf zet ik kort de wetenschappelijke en maatschappelijke relevantie van het onderzoek op een rij.

Wetenschappelijke relevantie

Zowel cybercrime als cybersecurity zijn thema's die onderbelicht zijn in de wetenschappelijke literatuur. Er is dan ook nog veel wat onderzocht kan worden. Dit onderzoek richt zich op drie wetenschappelijke lacunes. Ten eerste gaat dit onderzoek in op een lacune in de literatuur over de wijze waarop organisaties het risico op cybercrime benaderen. Tot op heden richten zowel wetenschappers als organisaties zich op de rationele benadering van het risico op cybercrime (Moore et al., 2015). Dit geeft voornamelijk het inzicht dat organisaties op basis van de expected value tot op heden niet voldoende doen aan cybersecurity. Dit onderzoek laat het perspectief van de webshopmanagers zien en gaat in op de *intuïtieve benadering* van het risico op cybercrime.

De tweede lacune richt zich op de rol die de onzichtbaarheid van het internet speelt in organisaties. Tot op heden is de rol van onzichtbaarheid van het internet zo goed als onzichtbaar in de organisatie-wetenschappelijke literatuur. Dit terwijl het internet een belangrijke factor is voor organisaties. In dit onderzoek kijk ik naar de rol die *onzichtbaarheid* speelt in organisaties. Dit doe ik aan de hand van theorie die juist over zichtbaarheid gaat. Bowen (2000) geeft aan dat zichtbaarheid een probleem kan zijn voor organisaties (p. 93). Dit komt door dat het internet negatieve zaken over onethisch handelen of risicovolle praktijken sneller aan het licht brengt (Zyglidopoulos & Fleming, 2011, 692). In dit onderzoek ga ik in op de relatie tussen onzichtbaarheid van het internet en de betekenis die webshopmanagers van (steeds zichtbaardere) bedrijven geven aan het risico op cybercrime.

De derde lacune gaat in op een recent onderzoek van McEvily, Zaheer en Fudge Kamal (2017) over ongelijkwaardigheid tussen interorganisationele vertrouwensbanden. Zij geven aan dat er nog meer onderzoek nodig is naar deze vertrouwensbanden door de perceptie van actoren over de macht van de de partij waarmee zij samenwerken te onderzoeken(McEvily et al., 2017, p. 89). Dit onderzoek gaat hierop in en geeft weer hoe de webshopmanagers kijken naar de relatie die zij hebben met de experts die hun cybersecuritybeleid uitvoeren en geeft inzicht in hun visie op de vertrouwensband.

Maatschappelijke relevantie

Dagelijks verschijnen er nieuwsberichten over cybercrime in het nieuws en rapporten wijzen uit dat het cybersecuritybeleid in het mkb tot op heden niet voldoet aan de wettelijk gestelde normen. Het is een maatschappelijk vraagstuk vanwege de mogelijke gevolgen voor burgers. Het is voor de maatschappij om ten minste twee redenen relevant om meer inzicht te krijgen in de benadering van webshopmanagers op het risico op cybercrime. Ten eerste laat paragraaf 1.1 laat zien wat de gevolgen kunnen zijn van cybercrime aan de hand van recente nieuwsartikelen. Bij cybercrime kunnen gegevens van burgers gestolen worden wat dan ten koste gaat van de privacy van burgers. Het is voor de maatschappij van belang om inzicht te krijgen hoe organisaties kijken naar en omgaan met het beschermen van klantdata. Ten tweede speelt het internet een belangrijke rol in de levens van burgers, omdat zij afhankelijk zijn geworden van het internet. Dit maakt dat zowel de beveiliging als de beschikbaarheid hiervan steeds belangrijker wordt voor de maatschappij.

Deze toenemende maatschappelijke relevantie is ook zichtbaar in de politieke arena. Afgelopen jaar is het Kabinet met diverse wetten en beleidsregels gekomen, om burgers en bedrijven beter te beschermen tegen internetcriminelen en of criminaliteit via het internet. De belangrijkste waren de nieuwe wet op de inlichtingen- en veiligheidsdiensten (wiv) en de wet Computercriminaliteit III (website Rijksoverheid B, 2017 en de Eerste Kamer, 2017). Deze wetten geven inlichtingendiensten en opsporingsdiensten (politie) nieuwe bevoegdheden in het digitale domein. Dat dit ingrijpende gevolgen voor burgers en bedrijven kan hebben, bleek uit de langdurige behandeling in het parlement. Waarbij vele wetswijzingen werden voorgesteld. De wiv heeft zelfs geleid tot een burgeraanvraag voor een nieuw raadgevend referendum (website NOS C, 2017). Andere onderwerpen die in de Tweede Kamer aan de orde kwamen, waren onder meer het *Internet of Things*, het toezicht op dataopslag door bedrijven en de beveiliging van vitale infrastructuur, ook in het licht van veilige verkiezingen. De komende jaren zal de aandacht voor internetgerelateerde onderwerpen alleen nog maar toenemen.

Tot slot vertaalt de maatschappelijke relevantie zich ook naar de markt voor cybersecurity. Het toenemende belang van cybersecurity, maakt dat er steeds meer bedrijven proberen een graantje mee te pikken. Dat dit niet altijd betrouwbare experts zijn, blijkt uit een publicatie van het Financieele Dagblad (website Financieele Dagblad, 2017). Het feit dat cybercrime en cybersecurity op al deze niveaus een rol speelt, maakt dat dit onderzoek ook een grote maatschappelijke relevantie heeft.

2. Theorie

In dit hoofdstuk zet ik de belangrijkste concepten voor dit onderzoek uiteen. Als eerst bespreek ik in paragraaf 2.1 de wijze waarop men het risico op *cybercrime* kan benaderen. Hierbij vertrek ik vanuit het concept veiligheid en ga vervolgens in op twee typen benaderingen: de rationele benadering en de intuïtieve benadering, die heel belangrijk blijkt te zijn. Een kenmerk van de intuïtieve benadering is dat mensen betekenis geven aan dat wat zij zien. Daarom ga ik in paragraaf 2.2 in op het concept betekenisgeving. Uit mijn onderzoek blijkt dat de onzichtbaarheid van het internet een belangrijk gegeven is voor de manier waarop webshopmanagers betekenis geven aan cybercrime. Dit terwijl zichtbaarheid een belangrijke rol speelt in organisaties. Daarom ga ik in paragraaf 2.3 in op de concepten zichtbaarheid en onzichtbaarheid. Tot slot bespreek ik in paragraaf 2.4 een belangrijk concept waar webshopmanagers in dit onderzoek ook betekenis aan geven, namelijk: vertrouwen.

2.1 Risico benadering

2.1.1 Veiligheid

Als er gegarandeerd geen slechte dingen kunnen gebeuren, waardoor niemand zich zorgen hoeft te maken, dan kan je spreken van volledige veiligheid. Veiligheid creëren doen mensen met het oog op mogelijke toekomstige gebeurtenissen die onveilig zijn. Hierbij maken zij zich zorgen over iets slechts dat kan gebeuren (Stone, 2012, p. 130). Dat mensen niet uitgaan van volledige veiligheid, bewijst de centrale rol die veiligheid heeft in de politiek. Veiligheid kan volgens Jackson en Sørensen (2012) gezien worden als een sociale waarden die "zo fundamenteel is voor het menselijk welzijn, dat zij op een bepaalde manier hiertegen beschermd of verzekerd moeten zijn" (p. 5). De overheid moet mensen beschermen tegen interne en externe dreiging. Hierbij maakt de overheid het veiligheidsbeleid en voert dit (samen met [sociale] organisaties) uit (Jackson & Sørensen, 2012, p. 5).

Typen veiligheid in organisaties

Zo zijn organisaties verantwoordelijk voor het waarborgen van bepaalde veiligheidseisen. Zij kunnen deels verantwoordelijk worden gehouden voor ten minste twee veiligheidsvormen. Ten eerste voor algemene veiligheid. Dit houdt onder andere bescherming tegen ongelukken in (Stone, 2012, p. 129). Hierdoor zijn organisaties bijvoorbeeld verplicht te zorgen voor brandveiligheid, bedrijfshulpverleners en passende fysieke beschermingsmiddelen (website Rijksoverheid C, 2017). De tweede veiligheidsvorm waar organisaties mee te maken hebben is persoonlijke veiligheid. Dit kan gedefinieerd worden als beveiliging tegen misdaad en vormen van geweld. Hier valt cybersecurity onder (Stone, 2012, p. 129). Naast de definitie van de Rijksoverheid, zoals gegeven in de inleiding, betekent cybersecurity in relatie tot organisaties dat computers en bedrijfsgegevens beschermd worden tegen hackers waardoor onder andere de (financiële) identiteit van mensen niet gestolen kan worden (Stone, 2012, p. 129). De AVG en Meldplicht Datalekken zijn wetten die organisaties dwingen hieraan te voldoen. Jacobs en Deamen (2016) stellen dat cybersecurity zes belangrijke doelen heeft. Allereerst gaat het om vertrouwelijkheid, waarbij niemand anders content kan lezen niet voor hem of haar bestemd is. Het tweede doel is integriteit, waarbij niemand anders de content van de communicatie kan veranderen. Ten derde gaan het om authenticiteit, waarbij helder moet zijn met wie iemand communiceert. Het vierde doel is onloochenbaarheid, waardoor men niet kan ontkennen dat er communicatie heeft plaatsgevonden. Ten vijfde draagt cybersecurity bij aan het hebben van bezittingen. En tenslotte moet cybersecurity het

mogelijk maken een schuldige aan te wijzen wanneer de veiligheid niet is gehandhaafd (Jacobs & Deamen, 2016).

Cyberveiligheid in organisaties

In de organisatiewetenschappelijke literatuur is onderzoek naar cybersecurity nog nieuw. Hierbij ligt de focus vrijwel altijd op het gebrek aan veiligheid op dit gebied en aanbevelingen hoe dit beter kan. Voorbeelden hiervan zijn verschillende onderzoeken naar cybersecurity in ziekenhuizen (Blum, 2013; Rushanan et al., 2014; Thimbleby, 2017;) en onderzoeken naar hoe cybersecurity gemanaged kan worden (Ganesan et al., 2017; Gordon & Loeb, 2006; Moore et al., 2015). De benaderingswijze verschilt niet veel van de manier waarop het Nederlands Cyber Collectief kijkt naar de risico's van cybercrime. Zij benaderen dit allen rationeel en dragen daardoor rationele oplossingen aan die kijkend naar dit onderzoek mogelijk niet aansluiten bij de benadering van organisaties. Deze *top-down* benadering maakt dat de visie van mensen binnen deze organisaties tot op heden onderbelicht blijft.

2.1.2 De Rationele benadering van veiligheid

Volgens het rationele perspectief kan je op een rationele manier inschatten of je je terecht zorgen maakt of niet. Veel beleidsmakers, risicoanalisten en experts benaderen het creëren van veiligheid rationeel. Hierbij kijken zij niet alleen naar of er iets slechts gaat gebeuren, maar ook naar hoe slecht de uitkomst van zo'n gebeurtenis is. De impact op mens en maatschappij. Om de verwachte waarde van gevaar te berekenen moet je de waarde van de omvang hiervan (aantal doden, financiële verliezen, etc.) vermenigvuldigen met de kans dat het daadwerkelijk gebeurt. Dit samen vormt de *expected value* (Stone., 2012, p. 131). Deze formule is rationeel, wetenschappelijk en universeel. Deze kan daardoor toegepast worden op allerlei verschillende situaties, waardoor het mogelijk is om kansen voor verschillende gebeurtenissen met elkaar te vergelijken. De kans op een risico is dus objectief te benaderen, waardoor je helder de consequenties van mogelijke gebeurtenissen kan inschatten (Stone, 2012, p. 132, 139). Zo kan iedereen zich op een rationele en correcte manier gedragen als hij/zij te maken krijgt met een onveilige situatie. Cass Sunstein (2002) zegt hierover:

> *"If you face a 1 percent chance of getting sick, you should act differently from how you would act if you faced a 99 percent chance of getting sick. People who are sensible, or even sane, do not treat a 1 percent risk of loss the same as the certainty of loss"* (p. 55).

Deze rationele benadering is terug te zien in de wijze waarop het NCC het risico op cybercrime benadert, namelijk op basis van feiten en cijfers over cybercrime (waarden) en uitslagen. Bij de rationele benadering ligt de focus op het inschatten van daadwerkelijke risico's en hun omvang. De uitkomst van een risicoanalyse geeft aan hoe groot of klein de kans is dat iets gebeurt. Op basis van risicoanalyses door het NCC, blijkt dat de kans op een hackaanval groot is. Als webshopmanagers het risico op cybercrime rationeel zouden benaderen, dan zou het NCC het mkb waarschijnlijk gemakkelijker bereiken. Maar de rationele manier van denken over cybersecurity is mogelijk niet de juiste benadering. Veiligheid is namelijk niet per definitie iets waar rationele overwegingen bij komen kijken.

2.1.3 De Intuïtieve benadering van Veiligheid

Volgens Stone (2012) kan een gevoel van veiligheid worden beïnvloed door objectieve omstandigheden, maar veiligheid zelf is voor het individu een gevoel (p. 133). Daardoor is de expected value niets meer dan een papieren werkelijkheid. Beleid en de bijbehorende retoriek die voortkomen uit de politieke of

wetenschappelijke context werken daardoor niet per se effectief (Stone, 2012, p. 133-134). Waar risicoanalisten de mate van veiligheid calculeren, laten verschillende voorbeelden zien dat mensen deze manier van denken niet overnemen in het dagelijks leven en hun keuzes. Een goed voorbeeld hiervan komt van Dan Gardner (2008). In zijn studie Risk: *The Science and Politics of Fear* schrijft hij dat er in 2001 1595 Amerikanen meer zijn omgekomen door een auto-ongeluk, dan door de terreuraanslagen van 11 september. Mensen werden na dit jaar echter niet banger om auto te rijden, terwijl de vlieg- en terreurangst wel toenam. Een irrationele manier van denken, aangezien de cijfers laten zien dat er zes keer zoveel mensen zijn omgekomen bij een auto-ongeluk, dan bij de aanslagen van 9/11 (Dan Gardner, in: Gabriels, 2017). Dit voorbeeld illustreert dat mensen afgaan op hun gevoel bij het beoordelen van een risico. Daarom is de zogenaamde intuïtieve benadering relevant in mijn onderzoek.

Kahneman (2011) laat zien dat intuïtie sterk de overhand heeft in onze manier van denken bij het maken van inschattingen en beslissingen. Voor zijn uitleg gebruikt hij twee 'hoofdpersonages': Systeem 1 en Systeem 2.

> "Systeem 1 werkt automatisch en snel, op basis van beschikbare informatie, met weinig of geen inspanning en geen gevoel van controle."…"Systeem 2 omvat bewuste aandacht voor de mentale inspanningen die worden verricht, waaronder ingewikkelde berekeningen. De werking van Systeem 2 wordt vaak gekoppeld aan de subjectieve ervaringen van handelingsvermogen, keuze en concentratie" (Kahneman, 2013, p. 28).

Systeem 2 zou in theorie kunnen zorgen voor rationele en weloverwogen keuzes, omdat dit deel het intuïtieve Systeem 1 overneemt en soms corrigeert bij complexe situaties. Zo dient Systeem 2 als een monitor en controleert zo continu de gedachten en handelingen die door Systeem 1 worden 'aangedragen'. Volgens Kahneman is het echter zo dat Systeem 2 lui is en er te vaak vanuit gaat dat ons eerste antwoord klopt en keurt dus het intuïtieve antwoord goed. Bij het inschatten van risico's leunen we sterk op het intuïtieve Systeem 1. Managers geven daarbij betekenis aan de ervaringen die zij hebben met cybercrime. Hieronder leg ik daarom het concept betekenisgeving uit.

2.2 Betekenisgeving

In 1995 introduceerde Karl Weick het begrip *sensemaking in organizations*. Dit begrip is in veel onderzoeken gebruikt om te verklaren hoe organisatieleden betekenis geven aan situaties. *Sensemaking* betekent letterlijk het geven van betekenis (Weick, 1996, p. 4). Er is echter nog geen onderzoek gedaan naar de betekenisgeving van cybercrime binnen organisaties. In dit onderzoek staat de betekenisgeving van webshopmanagers rondom het risico van cybercrime centraal. Daarom leg ik hieronder meer uit over dit concept.

2.2.1 Het sensemaking-proces

Sensemaking behelst een voortdurende ontwikkeling van plausibele beelden die rationaliseren wat mensen aan het doen zijn (Weick & Sutcliffe, 2005, p. 409). Het doel van sensemaking in organisaties is dat organisatieleden een gezamenlijk begrip creëren voor waar de organisatie voor staat en wat het doet. Voordat dit mogelijk is moeten mensen eerst zelf betekenis geven aan dat wat er gebeurt in de omgeving (Choo, 1996, p. 330 - 332). Weick en Sutcliffe (2005) omschrijven het proces van sensemaking in zeven stappen, die ik hier kort zal toelichten. Het startpunt van sensemaking is chaos, waarbij een gebeurtenis afwijkt van dat wat mensen kennen en zij dit opmerken en in beelden vastleggen (*bracketing*) (p. 411)

Hierbij kan gedacht worden aan de interpretatie van nieuwsberichten over de omgeving of een specifiek onderwerp (Choo, 1996, p. 330). De eerste vraag van betekenisgeving is dan ook: "Wat is hier aan de hand?" Vervolgens proberen mensen de informatie die zij hebben te ordenen door te gaan labelen en categoriseren, om zo de stroom aan ervaringen te stabiliseren (Weick & Sutcliffe, 2005, p. 411). Hier zie je dat mensen selectief zijn en dat wat zij selecteren worden de kenmerken waar zij zich bewust van worden en relevant zijn voor de actie die zij ondernemen (James in: Weick, 1995, p. 65). Een derde kenmerk in het proces is retroperspectief. Dit betekent dat mensen betekenis willen geven aan de puzzel die zij moeten oplossen, door te kijken naar hoe iets was en hoe iets nu is. Aan dat verschil tussen toen en nu geeft men een waarde en als iets vaker gebeurt, dan wordt dit herkend als een patroon. We weten in een nieuwe situatie voorafgaand niet hoe hier goed naar te handelen, waardoor een handeling achteraf verkeerd blijkt (Weick & Sutcliffe, 2005, p. 412). *"the now of mistakes collides with the then of acting with uncertain knowledge. Now represents the more exact science of hindsight, then the unknown future coming into being"* (Paget, 1988 in: Weick & Sutcliffe, 2005, p. 412). Het gaat ten vierde over vermoedens, waarbij het abstracte gekoppeld wordt aan dat wat concreet is. Ten vijfde wordt betekenis in de sociale wereld gevormd door mensen. Dit gaat via taal, gesprekken en communicatie (Weick & Sutcliffe, 2005, pp. 409, 412). Het zesde kenmerk is de actie waarbij mensen reageren op dat waar ze betekenis aan hebben gegeven. Deze betekenis is persoonlijk en geldt voor een bepaald moment. Het is een persoonlijke waarheid die door de tijd verandert, ontwikkelt en vorm krijgt. Waarbij een belangrijke notie is dat als mensen een situatie als 'de werkelijkheid' definiëren, dit de werkelijkheid is in hun belang (Thomas & Thomas, 1928 in: Weick, 1995, p. 66). Tot slot gaat het bij betekenisgeving in organisaties over sensemaking via communicatie. Hierbij kan communicatie gezien worden *"as an ongoing process of making sense of the circumstances in which people collectively find ourselves and of the events that affect them"* (Weick & Sutcliffe, 2005, p. 13).

2.2.2 Het belang van consistentie bij betekenisgeving

Om nog beter begrip te krijgen van hoe wij zo omgaan met betekenis geven aan ervaringen, moeten we volgens Kahneman (2013) kijken naar onze behoefte aan consistentie (p. 67). Hij legt aan de hand van de twee systemen uit dat we hierdoor niet rationeel beslissen. Als eerste gaat Systeem 1 af op alles wat we zien en beoordeelt vragen als "gaat alles goed? Is er een bedreiging? Gebeurt er iets nieuws?" Dit is het eerste onderdeel in het sensemaking-proces. Systeem 2 gaat pas werken als hier een afwijking (lees: chaos) in zit (2013, p. 67). Vervolgens slaat Systeem 1 alle ervaringen op en stelt zo een model van de persoonlijke belevingswereld samen uit "associaties tussen ideeën, gebeurtenissen, handelingen en ontwikkelingen die met enige regelmaat plaatsvinden, tegelijkertijd of binnen een redelijk kort tijdsbestek" (Kahneman, 2013, p. 79). Het bedrieglijke is dat frequente herhalingen niet per definitie de (enige) waarheid vormen, waardoor er een onjuist beeld ontstaat over een situatie. Ons brein kan waarheid en bekendheid niet goed onderscheiden en gaat dus af op dat wat bekend is (Kahneman, 2013, p. 70). Een mogelijk gevolg is wat Nassim Taleb (2008) de 'omkeerfout' noemt. Het ontbreken van bewijzen bewijst niet dat iets volledig ontbreekt (p. 68-69). Als we dit in de context van cybercrime en cybersecurity plaatsen, betekent dit dus dat als een specifiek (cybersecurity)probleem niet gevonden is, dat nog niet bewijst dat er algemene (cyber)veiligheid is.

2.2.3 Betekenisgeving en nieuwsberichten

Kijkend naar misdaad in het algemeen is het nieuws voor mensen vaak dé bron om het risico en de ernst in te schatten. Dit omdat het de primaire bron is over de omvang, de aard en de ernst van het misdrijf (Jackson, 2011). Dit houdt in dat mensen vaak via media iets krijgen te horen over criminaliteit en hier betekenis aan geven, terwijl dit vaak niet het volledige beeld over de situatie geeft (Stone, 2012, p. 134). Media selecteren kenmerken van een gebeurtenis voor ons en mensen selecteren daar vervolgens weer uit. Kahneman (2013) stelt dat media onze verwachtingen kleuren door de invloed ervan en de emotionele intensiteit. Ons gevoel of gedachten bij een bericht is daardoor geen exacte replica van de werkelijkheid (p. 146). Daarbij wennen we aan gebeurtenissen als deze vaker voorkomen in het nieuws. Het gevolg is volgens Kahneman (2013) het *halo-effect*: vooringenomenheid en bias vormen onze gedachten over mensen of een situatie. Dit beeld is eenvoudiger en samenhangender dan het werkelijk is en leidt tot het onterecht systematisch opvatten van willekeurige gebeurtenissen (Kahneman, 2013, p. 80, 91, 125). Anders gezegd: op basis van beschikbare (beperkte) informatie denken we te weten hoe het zit, terwijl de werkelijkheid anders, ingewikkelder en genuanceerder is.

2.2.4 Betekenisgeving verloopt intuïtief

In tegenstelling tot de economische school (met de rationele actor) gaat de organisatietheorie over sensemaking er vanuit dat mensen niet rationeel handelen aangezien zij hun mening baseren op eigen ervaringen en deze gebruiken als basis voor het begrijpen van situaties en het nemen van actie in de organisatie (Choo, 1996, p. 333). Zo vergroot nieuws over criminaliteit een onveilig gevoel als deze resoneert aan persoonlijke ervaringen of als de misdaad in de eigen buurt heeft plaatsgevonden (Chiricos et al., 2000; Healt & Gilbert, 1996; Visser et al., 2013 in: Riek, Böhme & Moore, 2014, p. 9). Waarbij daadwerkelijk slachtoffer zijn vaker leidt tot daadwerkelijke gedragsverandering (Riek et al., 2014, p. 8). Zo schrijven Riek et al. (2014) dat blootgesteld worden aan een zwakke vorm van cybercrime, zoals spam, er al voor zorgt dat klanten minder kopen en hun vertrouwen verminderd (p. 10). Het waarnemen van cybercrime heeft volgens Riek et al. (2014) de meeste impact op online shoppen (p. 23). Recent onderzoek van Martijn en Tokmetzis (2016) naar het internetgedrag van mensen laat echter juist zien dat mensen vrij weinig doen rondom het beschermen van hun privacy. Dit terwijl mensen wel zeggen dat ze hun privacy belangrijk vinden. Dit noemen zij de privacyparadox: mensen hebben wel de neiging om privacy belangrijk te vinden, maar handelen er niet of nauwelijks naar (p. 37). We beoordelen op basis van wat wij zelf waarnemen en ervaren. Hierdoor zijn we geneigd te handelen op grond van slecht onderbouwde meningen en indrukken.

Er is veel onderzoek gedaan naar de manier waarop organisatieleden betekenis geven aan situaties binnen organisaties. Aangevuld met de wetenschappelijke literatuur uit de economisch-psychologische literatuur, geeft dit een goed beeld van hoe mensen betekenis geven aan ervaringen. Dit onderzoek vult de organisatie-wetenschappelijke literatuur aan door een start te maken met de betekenisgeving van cybercrime-ervaringen in organisaties. Waarbij betekenisgeving in dit onderzoek niet organisatie-breed een rol speelt, maar ingaat op de betekenis die webshopmanagers geven aan het risico op cybercrime. Een belangrijk kenmerk van de betekenisgeving is dat mensen betekenis geven aan dat wat zij zien. Zo speelt zichtbaarheid enerzijds een belangrijke rol in de beslissingen van bedrijven en is het anderzijds juist een belangrijke factor in de werking van het internet. Echter, het internet brengt juist de onzichtbaarheidsfactor met zich mee.

2.3 Zichtbare bedrijven en het onzichtbare internet

In deze paragraaf staan de concepten zichtbaarheid en onzichtbaarheid centraal. Allereerst ga ik in op het concept zichtbaarheid en laat zien welke rol dit fenomeen speelt voor bedrijven. Vervolgens ga ik in op de illusie die zichtbaarheid met zich meebrengt in de sociale wereld aan de hand van de *invisibility cloak illusion*. Deze theorie fungeert als brug naar het tweede concept: onzichtbaarheid in het internet.

2.3.1 Zichtbaarheid in organisaties

"*Visibility captures the extent to which phenomena can be seen or noticed*" (Bowen, 2000, p. 93). Organisaties zijn vandaag de dag zichtbaarder dan ooit vanwege onder andere social media. In de organisatietheorie wordt het concept zichtbaarheid voornamelijk op twee manieren gebruikt. Ten eerste als kenmerk van een organisatie en ten tweede als kenmerk van een probleem. Zichtbaarheid als kenmerk van de organisatie houdt in dat relevante personen - zoals stakeholders – gemakkelijk zicht hebben op de organisatie (Bowen, 2000, p. 93). Een goed voorbeeld hiervan is dat organisaties door de komst van het internet steeds transparanter zijn geworden. Zowel op de website van de organisatie zelf als via verschillende mediabronnen kan een organisatie zichtbaar zijn (Zyglidopoulos & Fleming, 2011, p. 692). Bowen (2000) stelt dat organisaties door de zichtbaarheid blootgesteld worden aan institutionele druk in het sociale systeem (p. 93). Dit leidt ook tot het tweede kenmerk: zichtbaarheid als een probleem. Problemen zijn zichtbaar als zowel groepen binnen als buiten de organisatie deze problemen gemakkelijk waarnemen (Bowen, 2000, p. 93). Doordat organisaties transparanter zijn en journalisten toegewijd zijn aan '*digging the dirt*', komen negatieve zaken over onethisch handelen of risicovolle praktijken sneller aan het licht (Zyglidopoulos & Fleming, 2011, p. 692). Dit maakt dat organisaties sneller *getriggerd* zijn om te reageren op sociale of politieke vraagstukken, om zo reputatieschade te voorkomen (Bowen., 2000, p. 94).

Problemen van zichtbaarheid

Verschillende voorbeelden uit de organisatieliteratuur laten zien dat bepaalde thema's extra aandacht krijgen in organisaties nadat zij zichtbaar worden (gemaakt). Hierbij kan je denken aan thema's als gender, racisme en arbeidsomstandigheden. Een voorbeeld hiervan is de reactie van kledingmerken nadat op 24 april 2013 kledingfabriek Rana Plaza instort. Bij het ongeval kwamen 1138 mensen om het leven en raakten er 2515 mensen gewond (website One World, 2017). Voor de hele wereld was het zichtbaar dat veel kledingmerken zich schuldig maakten aan moderne slavernij. Sindsdien komt het onderwerp regelmatig in het nieuws als fabrieksarbeiders vertellen dat de omstandigheden nog steeds slecht zijn (website RTL, 2017) of als er een rapport uitkomt waaruit blijkt dat de omstandigheden niet zijn verbeterd (website SOMO, 2017). Daarnaast zijn er verschillende documentaires uitgebracht die inzicht geven in het productieproces, zoals 'De slag om de klerewereld' (NPO A, 2017). En de Sociaal Economische Raad (SER) kwam in juli 2017 met een lijst waar drieduizend naaiateliers op staan, waardoor zij precies kunnen achterhalen of Nederlandse ketens zaken doen met omstreden textielfabrieken (website SER, 2017). Tot slot hebben kledingmerken tegenwoordig vaak op hun website staan wat zij doen om duurzaam te ondernemen. Dit voorbeeld laat zien dat zichtbaarheid veel impact kan hebben op een organisatie. Zichtbaarheid maakt processen zichtbaar en als men dit als negatief ervaart, kan dit ertoe leiden dat zowel politiek als maatschappij verandering afdwingen.

De illusie van zichtbaarheid

De rationele benadering houdt met de expected value geen rekening met het belang van zichtbaarheid. *"We can't so easily attach pictures or emotions to the probability part"* (Stone, 2012, p. 135). Dit terwijl mensen wel uitgaan van dat wat zij zien. Een goed voorbeeld is hoe wij hier in de fysieke wereld mee omgaan. Boothby, Clark en Bargh (2016) spreken van een invisibility cloak illusion als het gaat over de manier waarop mensen omgaan met het observeren van anderen en geobserveerd worden. Deze illusie kenmerkt zich in twee verwante vooroordelen die samen leiden tot een derde vooroordeel. Ten eerste denken mensen dat zij zelf zeer sociaal kunnen waarnemen en dit beter kunnen dan andere mensen. Ten tweede geloven mensen dat zij zelf minder geobserveerd worden dan andere mensen. Ze kijken zelf wel naar andere mensen, maar gaan er toch vanuit dat zij zelf niet zo worden bekeken. Dit heeft als gevolg dat mensen geloven dat *zij* andere mensen meer observeren in de sociale omgeving dan *anderen* hen observeren (Boothby, Clark & Bargh, 2016, p. 1). Ons brein verzint het best mogelijke verhaal op basis van geactiveerde ideeën, dingen die we waarnemen. Intuïtief trekken we daarom snel conclusies op basis van beperkte (zichtbare) informatie (Kahneman, 2013, p. 93). Doordat mensen niet ervaren dat ze worden geobserveerd, denken ze ook dat ze minder geobserveerd worden. Dit terwijl zij zelf wel uitgaan van dat wat zij observeren en dus ervaren. In de wereld van het internet is dit nog complexer, aangezien we dan via een (onzichtbaar) object verbonden zijn met de sociale wereld.

2.3.2 De onzichtbaarheid van het internet

Het internet maakt organisaties zichtbaarder. De paradox is dat het proces van het internet zelf onzichtbaar is. Al in 1985 kwam James Moore met het belang van zichtbaarheid en het gebrek hieraan bij de omgang met computers. We kunnen precies weten wat de in- en output is, maar weten vrijwel niks over het interne proces (Moore, 1985, p. 272). En door die onzichtbaarheidsfactor is het mogelijk om intentioneel onzichtbaar misbruik te maken van het internet door bijvoorbeeld binnen te dringen in het eigendom en privacy van anderen (Moore, 1985, p. 273). "We zien niet welke overheden, criminelen en bedrijven op onze data jagen, hoe ze dat doen, waarom ze dat doen, wat ze er uiteindelijk mee doen en hoe dit onze levens beïnvloedt…Zij zien ons wel, maar wij hen niet" (Martijn & Tokmetzis 2016, p. 15). Esther Keymolen (2016) stelt dat doordat we op het internet alleen de interface zien, we slechts het gebruikersniveau ervaren: "Onze beoordeling gaat vaak niet verder dan: werkt het of werkt het niet?"... "Het probleem is dat de ervaring daar stopt. Je ervaart niet dat je gegevens gestolen kunnen worden voor identiteitsfraude" (Keymolen in Martijn & Tokmetzis 2016, p. 65-66). En dat wat je niet ziet is er niet, want "informatie die niet uit het geheugen wordt opgehaald, kan net zo goed niet bestaan." (Kahneman, 2013, p. 93). "*What You See Is All There Is*" stelt Kahneman (2013), en het gebrek aan zichtbaarheid bij cybercrime maakt dat we dus conclusies trekken op basis van de uitkomsten (p. 94). Niet alleen organisaties, maar ook mensen worden meer bekeken (geobserveerd) door het internet. Mensen kunnen organisaties beter in de gaten houden, maar vergeten dat zij zelf ook – zonder dat zij dit doorhebben – bekeken kunnen worden. Dit onlosmakelijke kenmerk van het internet versterkt de werking van Systeem 1 en daarmee de intuïtieve benadering en inschatting van het risico op cybercrime.

Problemen van onzichtbaarheid

We gaan als mensen af op dat wat wij observeren en ervaren. In de organisatiecontext geven mensen op basis daarvan betekenis aan de betrouwbaarheid van een webshop of andere organisatie. Hierbij is de basishouding dat we elkaar vertrouwen en ervan uit gaan dat onze privacy niet geschonden wordt.

Volgens Nissenbaum (2011) ervaren we "alleen privacyschending als we de informatiestromen niet gepast vinden"… "Als de bakker je tas wil onderzoeken is dit een privacyschending, maar als de douane bij Schiphol dit doet niet." (Nissenbaum, 2011 in: Martijn & Tokmetzis 2016, p. 33-35). Dit zijn zichtbare handelingen. Online vertrouwen we elkaar ook op zichtbare kenmerken. Etzioni (2016) laat zien dat we elkaar online vertrouwen op basis van het design van de website, het uiterlijk van mensen, de inrichting van de woning, de recensies die we lezen en de logo's van trust-building-platforms: alle elementen hebben te maken met zichtbaarheid. Zo wijst onderzoekt uit dat ratings wel een basis zijn voor het beoordelen van Airbnb verblijven, maar het uiterlijk van de bewoners en de inrichting zijn doorslaggevend in het vertrouwen van gasten (Ert. et al., 2016, in: Etzioni, 2017, p. 5). Handelen naar observaties en de ervaring die dit met zich meebrengt rondom cybercrime is bedrieglijk omdat je niet hoeft te ervaren dat iemand gegevens steelt. Maurits Martijn en Dimitri Tokmetzis (2016) zeggen hierover: "We weten helemaal niet welke gegevens we allemaal weggeven. We hebben geen idee wie er – bevoegd of onbevoegd – toegang tot die data hebben"…"Wat ze ermee doen en welke beslissingen over ons worden genomen op basis van die data" (p. 181-182). In dit onderzoek laat ik zien dat managers ook betekenis geven aan de betrouwbaarheid van zaken op basis van dat wat ze niet zien. Daarom bespreek ik in de volgende paragraaf het concept vertrouwen.

2.4 Vertrouwen

Vertrouwen is een concept waar al veel onderzoek naar gedaan is. Recente literatuur van McEvily, Zaheer en Fudge Kamal (2017) over interorganisationeel (IOT) vertrouwen en Etzioni (2017) over online vertrouwen, bieden nieuwe inzichten. Zo stellen McEvily et al. (2017) dat er bij vertrouwen tussen organisaties in de interorganisationele wetenschappelijke literatuur onterecht vanuit wordt gegaan dat de vertrouwensband bij een uitwisseling of samenwerking gelijkwaardig is. Etzioni (2017) laat in zijn onderzoek naar online vertrouwen zien dat mensen websites vertrouwen op basis van zichtbare kenmerken en experts. Hij laat zien dat het online vertrouwen voornamelijk een gevoelskwestie is en dus niet rationeel. Een belangrijke algemene definitie van vertrouwen is: *"Trust is a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviors of another"* (Rousseau et al., 1998, in: Etzioni, 2017, p. 1). In IOT-literatuur is de meest geaccepteerde definitie voor vertrouwen *"as expectation that another organization can be relied upon fulfill its obligations, will behave in a predictable manner, and will act and negotiate fairly when the possibility for opportunism is present"* (Zaheer et al., 1998 in: McEvily et al., 2017, p. 76). Hoewel deze laatste definitie rationeel oogt, vanwege de te verwachtte ingecalculeerde houding van organisaties naar elkaar, laat ik hieronder zien dat het juist past bij de intuïtieve benadering.

(On)gelijkwaardig vertrouwen

Bijna alle beslissingen die mensen maken zijn gebaseerd op vertrouwen en tot voor kort was vertrouwen afhankelijk van face-to-face interactie in het zakelijke verkeer. Dit geldt niet voor de persoonlijke wereld, waar vreemden elkaar al lange tijd zonder reden vertrouwen. Het internet heeft verandering gebracht in onze vertrouwensnorm omdat *"it raised being a stranger to a new order of magnitute by providing a very high level of anonymity"* (Etzioni, 2017, p. 2). Ondanks die anonimiteit blijkt uit onderzoek dat in Amerika het online vertrouwen toeneemt, terwijl offline het vertrouwen afneemt (Etzioni 2017, p. 8). Op het gebied van webshops is er volgens Etzioni (2017) in de online-wereld als het ware sprake van een gelijkwaardige vertrouwenscontract tussen de klant en verkoper: als klant vertrouw je erop dat het product dat besteld is

voldoet aan bepaalde kwaliteit en als verkoper vertrouw je erop dat de klant binnen een redelijke termijn betaalt. Hierbij willen beide partijen geen tijd besteden aan het controleren op betrouwbaarheid (p. 2). Deze benadering is volgens Poppo et al. (2008) tot op heden dominant en is gebaseerd op reciprociteit (in McEvily et al., p. 76). Men gaat uit van wederkerigheid waarbij gesproken kan woorden over mirror images omdat voor beide partijen dezelfde voor- als nadelen gelden (Young-Ybarra & Wiersema, 1999: McEvily et al., 2017, p. 76). Volgens McEvily et al. (2017) is de vertrouwensband echter niet zo gelijkwaardig als het in eerste instantie lijkt. Zij stellen dat verwachtingen over het "vertrouwen in de geloofwaardigheid van een andere partij", "de intentie om te vertrouwen" en "vertrouwd gedrag" gevormd worden door individuen en niet te sturen is door een organisatie. Zij hebben het dan ook over gevaren die komen kijken bij vertrouwen en spreken van exchange hazards als bijvoorbeeld een klant en verkoper zakendoen (p. 76-77). Exchange hazards is een combinatie tussen *asset specificity* en onzekerheid. Asset *specificity* verwijst naar "*the extend to which investments to support a particular transaction lose value if redeployed for use in the best alterative use*" (Klein et al., 1978 in: McEvily et al. 2017, p. 77). Onzekerheid refereert aan de onmogelijkheid om het onvoorziene te voorspellen (John and Weitz, 1988 in: McEvily et al. 2017,p. 77). Vertrouwen tussen personen en organisaties hangen af van de unieke doelen, voorkeuren en kwetsbaarheden van beide partijen (McEvily et al., 2017,p. 75). Etzioni heeft alleen naar het online vertrouwen van de klant gekeken. Webshopmanagers zijn in hun persoonlijke leven ook klant zijn van andere webshops. In de vorige paragraaf stelt theorie over sensemaking dat mensen betekenis vormen op basis van eigen ervaringen. Hierdoor is het mogelijk dat hun klantervaring ook een bijdrage levert aan de betekenisgeving rondom het risico op cybercrime.

Cybertrust

Los van de soort vertrouwensband die verkopers en klanten hebben, verschilt offline vertrouwen wezenlijk van online vertrouwen want "*consumers are interacting with websites rather than actual storefronts.*" (Etzioni, 2017, p. 2). Online wint vertrouwen dan ook op andere manieren terrein. Etzioni noemt drie manieren. Ten eerste speelt het design van de website een grote rol omdat "*[a] consumer's interaction with a store is somewhat similar to his or her interaction with a website.*" (Bart et al., 2005, in: Etzioni, 2017, p. 3). Dat dit verder gaat dan enkel online vertrouwen bewijst een onderzoek naar de rol van foto's die een verhuurder op Airbnb plaatst. De conclusie was dat de mate van vertrouwen in een verhuurder gebaseerd is op het uiterlijk van zowel de verhuurder als de woning. Hoe beter dit eruit ziet, hoe meer men bereid is ervoor te betalen (Ert et al., 2016 in: Etzioni, 2017, p. 5). Ten tweede spelen recensies een rol in het online vertrouwen. Zo speelt feedback een belangrijke rol op het profiel van verkopers op eBay. De verkoper kan de feedback niet verwijderen en is afhankelijk van zijn klanten voor zijn score en aanbevelingen. Het is belangrijk dat die goed zijn, want uit onderzoek blijkt dat kopers een bekende verkoper met een hogere reputatiescore meer vertrouwen dan onbekende verkopers met minder of een lage reputatiescore (Rensick et al. 2006, in: Etzioni, 2017, p. 6). Tot slot zijn t*rust-building platforms* (TBP) van belang voor het online vertrouwen. Hierbij kan gedacht worden aan onder andere *Payment Services Providers* (PSP) en keurmerken, zoals Thuiswinkel Waarborg. Aansluitend aan PSP's spelen creditcardmaatschappijen een grote rol, omdat zij ervoor zorgen dat klanten de verkoper niet hoeven te vertrouwen. Zij zorgen hierdoor als het ware voor een verschuiving in het risico van de koper naar de creditcardmaatschappij. Keurmerken geven certificaten af aan bijvoorbeeld webshops en geven zo een signaal naar de klant dat de organisatie voldoet aan bepaalde criteria wat betreft privacybescherming (Etzioni, 2017, p. 8). TBP's zijn dus gespecialiseerd in een bepaald cyber onderwerp

en kunnen daarom gezien worden als experts. Uit een onderzoek van IBM uit 2006 gaf 70 procent van de respondenten aan alleen te shoppen bij een webshop met keurmerk (IBM News in: Etzioni, 2017, p. 8). Het belang van een keurmerk lijkt voornamelijk te gelden voor kleinere webshops, omdat consumenten bij grote webshops het merk al vertrouwen (Bart et al., 2005, in: Etzioni, 2017, p. 9). Etzioni plaatst twee kanttekeningen bij het imago van keurmerken. Ten eerste kan de consument niet controleren wanneer een organisatie voor het laatst is gecontroleerd door het keurmerk. Ten tweede is het de vraag "*who guards the guardians?*", want daar waar offline auditoren diploma's moeten halen, hoeven online-auditoren dit niet (Etzioni, 2017, p. 8-9). Volgens Etzioni is er tot op heden geen effectieve manier gevonden "*to guard the guardians*" (2017, p. 9).

Vertrouwen in experts

Bovenstaande laat zien dat klanten een website vertrouwen op basis van zichtbare kenmerken (layout van de webshop en recensies) en op basis van experts (TBP's). McEvily et al. (2017) stellen dat er bij een IOT-vertrouwensband sprake kan zijn van een onbalans in macht. Hierbij is de ene partij (meer) afhankelijk van de andere partij dan andersom (p. 78). Of er sprake is van onbalans hangt af van de mogelijkheid tot alternatieven. Dit wordt ook wel een verdor lock-in genoemd. Hierbij kan gedacht worden aan omschakelingskosten bij het stopzetten van de samenwerking of een kennisklоof bij een organisatie die daardoor niet kan inschatten wat hij nodig heeft van de andere organisatie. Hierbij kan bijvoorbeeld gedacht worden aan de macht van een TBP. Een webshop kan zich gedwongen voelen hierbij aan te sluiten, omdat klanten anders niet kopen. Zij worden gezien als de mensen die er verstand van hebben en krijgen het vertrouwen dat zij de privacy van klanten beschermen. De exchange hazard kan in dit geval zowel een gevaar als een signaal zijn. Voor de ene partij vormt de exchange hazard een gevaar van opportunisme, terwijl het voor de andere partij gezien wordt als signaal dat de organisatie zich aan de afspraken houdt (McEvily et al., 2017, p. 87). Zo kunnen experts in een vertrouwensrelatie meer macht hebben vanwege hun kennis.

Vanuit een rationele visie is de mening van de experts daarom vaak heilig: *"Experts are generally right, and ordinary people are generally wrong"* (Stone, 2012, p. 136). Dit zou betekenen dat de experts de risico's per definitie goed inschatten. Dit is volgens Paul Slovic (2000) onjuist, omdat:

> "Risico niet iets is wat 'er is', los van ons denken en onze culturele opvattingen, klaar om gemeten te worden. Mensen hebben het concept van risico bedacht om beter te kunnen omgaan met de gevaren en onzekerheden van het leven.

Deze gevaren zijn weliswaar reëel, maar er is niet zoiets als "reëel risico" of "objectief risico." Sunstein is het hier fundamenteel mee oneens. Hij stelt dat slechte regelgeving mensenlevens en geld kost. Hij vindt dan ook dat "wet- en regelgevende instanties wellicht te veel luisteren naar irrationele zorgen van de burger, om electorale redenen en omdat ze zelf ontvankelijk zijn voor dezelfde cognitieve bias" (Sunstein in: Kahneman, 2013, p.149-150). Volgens Slovic (2000) klopt zijn beeld van experts niet, omdat mensen over het algemeen beperkingen hebben om kleine risico's in te schatten. "We negeren ze eenvoudigweg of blazen ze buiten proportie op- er bestaat geen tussenweg." (Slovic, in: Kahneman, 2013, p. 151). Toch is het vertrouwen in experts groot en blijft de illusie dat zij goed kunnen voorspellen en daardoor juiste risicoanalyses kunnen maken in stand. Zo zitten er elke avond bij programma's als Jinek, Nieuwsuur en RTL Late Night allerlei type experts aan tafel om te praten over wat er is gebeurd en om vervolgens een voorspelling te geven van de toekomst. Uit een onderzoek van Philip Tetlock (2005) blijkt echter dat

experts nauwelijks beter zijn in het voorspellen van de toekomst dan niet specialisten (Tetlock in: Kahneman, 2013, p. 229). Vertrouwen op een expert lijkt zo te bezien dan ook eerder irrationeel, dan rationeel.

Kunnen we dan helemaal niet vertrouwen op de intuïties van experts? Kahneman heeft samen met Gary Klein een onderzoek gedaan die antwoord geeft op de vraag: "Wanneer kun je op een ervaren professional vertrouwen als deze zich op een intuïtie beroept? De twee wetenschappers zijn het niet met elkaar eens, maar komen samen wel tot waardevolle inzichten. Het verschil van mening komt doordat zij verschillende typen experts onderzoeken. Kahneman deed voornamelijk onderzoek naar medici, beleggingsadviseurs en politieke wetenschappers "die proberen onhoudbare voorspellingen op lange termijn te doen." Klein deed daarentegen onderzoek naar (vak)mensen met werkelijke expertise, zoals brandweerlieden en verpleegkundigen. Uit hun onderzoek komt naar voren dat de betrouwbaarheid van een expert afhangt van de regelmatigheid van een omgeving. Hierbij kun je twee vragen stellen: 1. voorspelt de expert over een complexe omgeving met veel factoren? En zo nee: 2. Kan de expert deze regelmatigheid door langdurige oefeningen leren? Samen komen zij tot de conclusie dat iemand met een lange leergeschiedenis in een overzichtelijke omgeving betrouwbaar is (Kahneman, 2013, p. 246 – 252). Kijkend naar de context van cybersecurity zou je kunnen betogen dat dit een complexe omgeving is. De technologie is continu in beweging, er zijn veel verschillende protocollen, infrastructuren. Kijkend naar cybercrime lijkt er ook op dit gebied geen sprake te zijn van een stabiele omgeving. Het is daarnaast nog een relatief nieuwe business. Experts hebben dan ook vaak geen lange leergeschiedenis, omdat ze door nieuwe – snel veranderende – technologie en andere ontwikkelingen telkens nieuwe situaties moeten beoordelen. De experts zijn daardoor mogelijk niet zulke hele betrouwbare specialisten op het gebied van voorspellingen doen.

2.5 Tot slot

In dit hoofdstuk heb ik de volgende theoretische concepten behandeld. Te weten de rationele en intuïtieve benadering, betekenisgeving, vertrouwen, zichtbaarheid en onzichtbaarheid. Met deze concepten kan ik mijn bevindingen (hoofdstuk 4) in hoofdstuk 5 duiden en analyseren. In het volgende hoofdstuk bespreek ik eerst mijn onderzoeksmethoden.

3. Methoden

In dit hoofdstuk bespreek en verantwoord ik de keuzes die ik heb gemaakt gedurende het onderzoeksproces.

3.1 Onderzoeksbenadering

In dit onderzoek staat de wijze waarop webshopmanagers in de mkb-detailhandel betekenis geven aan het vertrouwen dat zij hebben in hun risicobenadering van *cybercrime* centraal. Dit houdt in dit onderzoek in dat de webshopmanagers verhalen vertellen die ik als onderzoeker interpreteer. Daarom heb ik gekozen voor de kwalitatieve interpretatieve onderzoeksmethoden. Het interpretavisme hoort bij de epistemologie en gaat over hoe ik het onderzoek wil uitvoeren en kennis over de werkelijkheid vergaar. Aansluitend bij het constructivisme gaat dit epistemologische perspectief er vanuit dat kennis niet objectief is, omdat iedereen door een andere bril kijkt. Dit geldt ook voor mij als onderzoeker. Ik kan mezelf niet buiten de sociale werkelijkheid plaatsen waardoor bijvoorbeeld mijn normen, waarden, achtergrond en studie het onderzoek beïnvloeden. Maar ook mijn keuzes binnen het onderzoek hebben consequenties voor de uitkomst van het onderzoek. Hier moest ik rekening mee houden tijdens het onderzoek. Hoe ik dit precies heb gedaan leg ik uitgebreider uit in paragraaf 3.1.2.

Dit type onderzoek sluit aan op de onderzoeksvraag omdat ik de leidinggevende een stem wil geven in de discussie over cyberveiligheid. Verschillende partijen hebben kwantitatief onderzoek gedaan naar de handelingen van het mkb op het gebied van cyberveiligheid. Experts en onderzoekers benaderen het mkb echter rationeel, waardoor de onderzoeken voornamelijk gemotiveerd zijn om de ondernemers via cijfers en feiten te wijzen op hun tekortkomingen. Ook het Nederlands Cyber Collectief (NCC) pakt het op deze manier aan. Dit onderzoek staat aan de andere kant van het spectrum en vertelt het verhaal van de webshopmanager. Verdieping over waarom het mkb bepaalde beslissingen maakt en welke betekenissen zij daaraan geven staan hier centraal. Om deze reden heb ik gekozen voor een kwalitatieve en interpretatieve onderzoeksvorm.

Deze verhalen staan los van de al bestaande 'verhalen' van onderzoekers en experts, maar gezien de vraag van het NCC is het interessant om te kijken of de huidige benadering aansluit bij de visie van de webshopmanager. Aangezien hier al veel documenten van aanwezig zijn, zal een deel van dit onderzoek gebaseerd zijn op theorie en heeft daardoor een deductieve aanpak, die in eerste instantie niet direct aansluit bij het sociaal constructivisme. Met de concepten uit het theoretisch kader duid ik de bevindingen. De theorie die ik gebruik toets ik dus niet, maar het dient als middel om mijn bevindingen te interpreteren. Het onderzoek zal daarom uiteindelijk gekenmerkt worden door een inductieve aanpak.

3.1.1 Rol van onderzoeker

Tijdens mijn zoektocht naar een afstudeerplek ben ik heel bewust op zoek gegaan naar een organisatie die zich bezighield met *cybersecurity*. De eerste periode bij het Nederlands Cyber Collectief (NCC) heb ik besteed aan zoveel mogelijk lezen over dit onderwerp en praten met mensen die hier verstand van hebben. Deels uit persoonlijke interesse, maar ook omdat ik het gevoel had dat ik meer kennis moest vergaren voordat ik daadwerkelijk kon beginnen met interviewen. Door mijn

onderzoek in de ik-vorm te schrijven, maak ik kenbaar dat dit onderzoek mijn interpretaties weergeven en dus niet objectief is. Kennis is namelijk niet neutraal, waardoor mijn achtergrond en veronderstellingen van invloed waren op de webshopmanagers en beslissingen die ik tijdens dit onderzoek heb gemaakt (Henn, Weinstein & Foard, 2006, p. 68). Tijdens het onderzoek kwam ik voor een twee ethische dilemma's te staan. De keuzes die ik hierin heb gemaakt hebben invloed gehad op het interview, de bevindingen en daarmee uiteindelijk ook op de uitkomst van het onderzoek. Hieronder bespreek ik de keuzes en licht ik deze toe.

Het niet benoemen van het NCC en het onderzoeksonderwerp

Het doel van dit onderzoek is dat het perspectief van de webshopmanagers rondom het onderwerp cybercrime helder naar voren komt. Daarvoor was het van belang te onderzoeken hoe de webshopmanagers over dit onderwerp denken. Veel of juist weinig? Hoe praten ze hierover? Wat is hun eerste gevoel bij het onderwerp? Het interview mocht geen test worden om de cybersecurity kennis van de webshopmanagers te toetsen. De vraag was hoe ik dit kon voorkomen. Een belangrijk kenmerk van ethisch verantwoord onderzoek doen, is dat de onderzoeker open en eerlijk is over het onderzoek, zodat respondenten zelf kunnen kiezen of ze hier aan mee willen werken (Löfman, 2004, p. 334). Het eerste dilemma was: vertel ik eerlijk dat ik mijn onderzoek voor het Nederlands Cyber Collectief doe *of* zeg ik alleen dat ik een student en respondenten zoek voor mijn masterscriptie? Ik heb er bewust voor gekozen om mijzelf bij webshopmanagers kenbaar te maken als een student en niet als afstudeerder bij het NCC. Dit omdat ik het gevoel had dat de naam van het NCC te veel impact kon hebben op de inhoud van het interview. Hier ga ik in het tweede dilemma dieper op in. Daarnaast is het NCC onderdeel van Nationale Nederlanden. Zij benaderen het risico op cybercrime rationeel en hebben als grote organisatie ook belang bij een bepaalde uitkomst. Ik wilde hier als onderzoeker los van staan. Ook gezien mijn kwalitatieve en interpretatieve onderzoeksmethoden. Mijn manier van onderzoek doen sluit niet aan bij de manier waarop het NCC normaal gesproken onderzoek doet. Ik heb er dan ook voor gekozen om mij gedurende het onderzoek terug te trekken uit de organisatie en zelfstandig het onderzoek uit te voeren. Wel met de afspraak dat ik het onderzoek voor het NCC uitvoer. Mijn keuze om niet te benoemen dat het onderzoek voor het NCC is, heeft invloed gehad op de keuze van de respondenten. Zij dachten namelijk dat ze enkel te maken hadden met een student en dat de informatie voor mij alleen was. Ik voelde mij hier wel schuldig over en heb toen nagedacht hoe ik deze keuze zo ethisch mogelijk kon voortzetten. Dit heb ik gedaan door de webshopmanagers te garanderen dat zij anoniem blijven en het dus niet te achterhalen is voor welke organisatie zij werken. Dit houdt concreet in dat ik deze gegevens ook niet heb gedeeld met het NCC. Daarnaast is het onderzoek straks niet alleen voor het NCC, maar wordt het openbaar. Hierdoor krijgt het NCC uiteindelijk dezelfde informatie als ieder ander die het onderzoek leest. Doordat ik mij terugtrok uit de organisatie en de gegevens van de webshopmanagers niet heb gedeeld met het NCC, werd ik als het ware ook weer meer een student die zelfstandig onderzoek deed. Maar daar had ik slechts het eerste probleem mee opgelost.

Het tweede dilemma was namelijk: vertel ik heel precies waar mijn onderwerp over gaat *of* schets ik enkel de context en benoem ik het onderwerp cybercrime niet? Mijn dilemma was dat ik wel eerlijk wilde zijn, maar tegelijkertijd wilde ik niet dat de webshopmanagers al te veel informatie hadden. Dit laatste, omdat ik de kans mogelijk achtte dat de webshopmanagers zich voorafgaand aan het interview

zouden inlezen over het onderwerp en ik dan sociaal wenselijke antwoorden zou krijgen. Het leek mij het beste om het woord cybercrime of cybersecurity te vermijden, maar heb dit in eerste instantie niet gedaan, omdat ik al niet volledig ethisch handelde door het NCC niet te benoemen. Maar na een paar weken liep ik steeds tegen dezelfde afwijzing aan, namelijk dat potentiële webshopmanagers mijn verzoek voor een interview afwezen omdat ze niks over het onderwerp wisten. De drempel om over cybercrime en cybersecurity te praten bleek te hoog. Dit was juist interessant. Ik wilde weten hoe de managers hierin stonden, veel kennis of geen kennis, er waren geen verkeerde antwoorden. Daarom besloot ik om 'vaag' te blijven over het precieze onderwerp van het interview en deze te verpakken als een "onderzoek naar de rol van managers in het hedendaagse, digitale tijdperk." Dit keer reageerden de webshopmaners wel positief. Bijkomend voordeel is dat ik op deze manier heb kunnen voorkomen dat webshopmanagers voorafgaand aan het interview informatie over cybersecurity gingen opzoeken, waardoor ik denk dat de antwoorden de werkelijkheid beter weergeven. Deze afwegingen zijn daardoor ten goede gekomen aan het onderzoek. Het effect op de webshopmanagers was dat ze tijdens het interview verrast werden door het onderwerp en de richting van het gesprek; "Ik dacht dat het gewoon een simpel interview zou zijn over de rol van de manager", en soms het gevoel hadden dat ze mij niet goed hadden geholpen; "Sorry dat ik hier zo weinig vanaf weet, volgens mij heb je niks aan mijn antwoorden."

Meer kennis

Doordat ik in tegenstelling tot de webshopmanagers wel ingelezen was, had ik vaak meer kennis over cybersecurity dan de webshopmanagers. Dit werd gedurende het interview toch wel duidelijk, omdat ik semi-gestructureerde interviews hield. Hierdoor kreeg ik een soort rol als "expert" en dat had soms effect op het gedrag van de respondent. Zo begon ik zelf een aantal keer over bepaalde wetten en merkte dat ik dan sociaal wenselijke antwoorden kreeg. Om deze reden heb ik sommige vragen bij latere interviews niet meer gesteld en ging ik alleen nog maar over onderwerpen, zoals bijvoorbeeld de AVG praten, als dit ter sprake kwam. Tot slot viel het op dat ik webshopmanagers vaak aan het denken zette door met hen te praten over cybersecurity. Gezien mijn visie en kennis zag ik dit ook als een kans om hen bewuster te maken over het onderwerp door hen te voorzien van meer kennis. Daarom heb ik alle webshopmanagers na afloop van het interview documenten en linkjes gemaild over cybersecurity in het mkb. Ik was mij erg bewust van de sturende rol die ik innam en heb daarom informatie gekozen die aansluit bij de Algemene Verordening Gegevensbescherming (AVG), zoals bijvoorbeeld "Ieder bedrijf heeft zorgplichten" (Wolters. & Jansen, 2017) en "Ketenweerbaarheid tegen cyberdreigingen (Van Ruijven & Keijser, 2017). Op deze manier had ik het gevoel dat ik oprecht iets kon terugdoen en niet bezig was met reclame maken voor bijvoorbeeld het NCC. Dit heeft mogelijk effect gehad bij een bedrijf dat nog geen ssl certificaten had gedurende het interview en een week later wel.

3.1.2 Rol van theorie

Theorie heeft in dit kwalitatieve onderzoek gedurende het hele proces een abductieve rol gespeeld. "Bij abductie gaat het erom de best passende verklaring te vinden voor waarneming en dan is het handig wanneer onderzoekers uit verschillende theoretische vaatjes kunnen tappen" (Boeije, 2015). Het startpunt en mijn zoektocht naar artikelen kon ik vormgeven door gebruik te maken van *sensitizing* concepts. De concepten die ik in eerste instantie heb gebruikt zijn "cybersecurity" en "cybersecurity in

het mkb." Het eerste concept kwam voort uit het feit dat vaststond dat de context van mijn onderzoek over cybersecurity zou gaan en ik wilde begrijpen wat dit precies inhield. Het tweede concept gaf de focus aan die voortkwam uit de vraag van het Nederlands Cyber Collectief, namelijk: Hoe kunnen wij het mkb bereiken? Aan de hand van deze concepten heb ik verschillende (wetenschappelijke artikelen) gelezen over cybersecurity en de verschillende theorieën die verklaren waarom het volgens hen in het mkb gaat zoals het gaat. Na deze eerste ronde van dataverzameling kwam ik erachter dat ik vaak het woord "onzichtbaar" had opgeschreven. Hoewel de theorie daar niet over ging bleef dit woord hangen en via een seminar over *Internet of Things* vertelde Katleen Gabriels over de *onzichtbaarheidsfactor* van filosoof James Moore. Dit concept was voor mij verhelderend, omdat het inzicht gaf in de complexiteit van het abstracte onderwerp waar ik over wilde praten met webshopmanagers. Ik zag het theoretische concept als een kans om meer te halen uit de diepte-interviews, zonder de inductieve werkwijze uit het oog te verliezen. Na een aantal gesprekken met webshopmanagers gevoerd te hebben, kwam het concept "keuzes maken" duidelijk naar voren. Hierdoor kwam ik al snel op theorie van Kahneman, die de psychologische en meer intuïtieve kant van keuzes maken beïnvloedt. Hierbij kwam het belang van ervaringen naar voren en hoe we daar betekenis aan geven. Dit sloot precies aan bij de denkwijze van webshopmanagers en daarom ben ik vanuit deze theorie verder gaan zoeken. Waardoor het concept *betekenisgeving* in beeld kwam. Tot slot kwam ik er gedurende de dataverzameling achter dat *vertrouwen* een belangrijke rol speelt in de manier waarop webshopmanagers het risico op cybercrime benaderen.

3.1.3 Plek in organisatie

Zoals in paragraaf 3.1.1 duidelijk werd had ik als onderzoeker tijdelijk mijn eigen rol binnen het NCC. Het onderzoek stond vrijwel los van de organisatie, waardoor ik weinig op locatie was en ik het onderzoek zelfstandig heb uitgevoerd. Alle interviews vonden plaats op de werkplek van de manager en telefonische interviews heb ik thuis gedaan, zodat ik zeker was van een stille omgeving. Regelmatig heb ik contact gehad met de leidinggevende van het NCC om de voortgang en resultaten te bespreken. En aangezien de webshopmanagers niet wisten dat ik het onderzoek voor het NCC deed, deelde ik slechts de uitkomsten van de interviews en bleven zij verder anoniem. Het NCC gaf mij de ruimte en het vertrouwen om op deze manier te werken.

3.2 Onderzoeksontwerp

In deze paragraaf ga ik dieper in op het type onderzoek dat ik heb gedaan en vervolgens omschrijf ik welke methoden ik heb gebruikt om data te verzamelen.

3.2.1 Meervoudige casestudy

Dit onderzoek kenmerkt zich als een meervoudige casestudie, aangezien ik vijftien webshopmanagers intensief bestudeerd heb (boeije, 2015, p. 62). Omdat deze managers allen werken in de detailhandel van een mkb, is er sprake van een *exemplifiying case* (Bryman, 2012, p. 70). Voor deze vorm is gekozen omdat het voor het NCC van belang is dat ik de betekenisgeving van de gesproken managers kan generaliseren. De webshopmanagers kunnen gezien worden als vertegenwoordigers van webshopmanagers uit de detailhandel in het mkb (Bryman, 2012, p. 70).

3.2.2 Dataverzameling

Mijn data heb ik verzameld aan de hand van interviews, tekeningen van webshopmanagers en een webshop-analyse van de bijbehorende organisaties. Hieronder zal ik eerst toelichten hoe ik de webshopmanagers heb geselecteerd. Daarna zal ik dieper ingaan op de methoden zelf.

Selectie van webshopmanagers

Ik ben op drie manieren aan de webshopmanagers gevonden: 1. Via purpose sampling ging ik strategisch op zoek naar managers die relevant zijn voor mijn onderzoek; 2. Vervolgens wezen diverse webshopmanagers nieuwe, relevante managers aan en tot slot 3. Ben ik via mijn netwerk aan managers gekomen (Bryman, 2012, pp. 418 en 424). Voordat ik op zoek ben gegaan naar webshopmanagers, had ik besloten dat ik graag mensen wilde spreken die invloed hebben op de werkvloer, maar ook aan de uitvoerende kant zitten. Het profiel van de manager kan daardoor kort omschreven worden als: webshopmanagers uit de detailhandel in het mkb. Om dit profiel nog verder af te bakenen heb ik gekozen voor webshops die kleding (en accessoires) of interieurartikelen verkopen, omdat dit producten zijn die vaak online worden gekocht. Vervolgens ben ik als eerst via purposive sampling op zoek gegaan naar webshopmanagers door online webshops te zoeken en heb ik hen telefonisch en/of via de mail benaderd. In totaal heb ik 45 webshops geselecteerd. Uiteindelijk heb ik vier webshopmanagers via deze weg kunnen interviewen. Ook ben ik langs een aantal bedrijven te gaan om zo face-to-face te vragen of de manager wilde meewerken aan mijn onderzoek. Dit heeft mij vijf webshopmanagers opgeleverd. Ik merkte dat het erg lastig was om koud binnen te komen bij een organisatie. Daarom heb ik mijn vraag naar webshopmanagers ook uitgezet op LinkedIn en heb ik aan vrienden en familie gevraagd of zij contacten voor mij hadden. Op deze manier ben ik aan drie webshopmanagers gekomen. Vervolgens waren er nog drie webshopmanagers die mij doorverwezen naar een andere wegshopmanager die binnen het profiel pasten.

Interviews

In mijn hoofdvraag staan de ervaringen van de webshopmanager en de gevolgen hiervan voor het cybersecuritybeleid centraal. Hierdoor was het al direct duidelijk dat het belangrijk was om de managers persoonlijk te spreken. Dit wilde ik doen via semigestructureerde interviews, omdat ik een aantal topics moest aansnijden om antwoord te krijgen op mijn hoofdvraag. In totaal heb ik vijftien interviews afgenomen. De eerste drie interviews waren gestructureerder dan de interviews die daarop volgden. Dit kwam omdat ik nog moest inkomen en ik niet goed kon inschatten hoe een respondent zou reageren en was ik bang dat ik niet alle topics binnen de tijd kon beantwoorden. Later liet ik de tijd los, omdat ik merkte dat de webshopmanagers wel door bleven praten. Hierdoor voelde ik de ruimte om de webshopmanagers het gesprek te laten leiden en kwam er altijd wel een moment waarop ik kon aanhaken met vragen over de belangrijke topics. Het feit dat ik opnam had wel invloed op de webshopmanagers. Dit merkte ik vaak vooral na afloop aan zowel de non-verbale communicatie - ze gingen dan weer ontspannener zitten - als aan de opluchting die soms hoorbaar was – "Zo, het is wel moeilijk om over iets te praten wat niet tastbaar is." Ik denk dat het opnemen van het gesprek in combinatie met het "lastige" onderwerp in zekere maten invloed had op de mate waarop een respondent zich op zijn gemak voelde. Echter ben ik van mening dat het feit dat webshopmanagers het een moeilijk onderwerp vonden erg waardevol is geweest voor het onderzoek. Daarom heb ik deze aanpak niet gewijzigd.

De interviews vonden voornamelijk plaats op de werkplek van de webshopmanagers. Voor mij was het van belang dat de manager zich vrij voelde om te praten. Daarom heb ik hen de locatie laten uitkiezen en kwam ik daar naartoe. Vier webshopmanagers hadden geen tijd om af te spreken. Deze interviews vonden daarom telefonisch plaats. Ik vond het lastiger om te interviewen via de telefoon, omdat het door de afstand lastiger was om een band op te bouwen met de respondent en het daardoor soms ongemakkelijk voelde om dieper in te gaan op antwoorden die vroegen om meer verdieping. Dit omdat de vragen voor sommigen toch al lastig te beantwoorden waren vanwege het abstracte en complexe onderwerp. Ik liet hierdoor minder lange stiltes te laten vallen, omdat ik niet kon aanvoelen of er meer bedenktijd nodig was en kon ik niet zien wat de respondent op het moment van het interview deed. Een ander gevolg was dat ik meer moest doorvragen dan bij een face-to-face interview. Gemiddeld duurden de interviews drie kwartier tot vijftig minuten, waarbij het kortste interview een half uur duurde en het langste interview anderhalf uur. De interviews vonden in de ochtend of middag plaats en nam ik op met mijn telefoon. Dit was onder andere waardevol omdat ik op deze manier goed kon luisteren naar wat de webshopmanagers zeiden en mijn vragen hierop aanpassen en werd ik achteraf niet beperkt door de limitatie van mijn geheugen of mijn voorkeuren (Bryman, 2012, p. 482; Boeije, 2015, p. 88). Voorafgaand aan het interview heb ik toestemming gevraagd voor het opnemen en gaf ik aan dat ze niet de naam van zichzelf of het bedrijf hoefden te noemen. Mocht de opname dan toch in verkeerde handen terecht komen, dan kon dit niet gekoppeld worden aan de organisatie of de manager. Uiteindelijk heb ik de interviews getranscribeerd, maar niet letterlijk, tenzij er een opvallend lange 'ehh' viel of iets dergelijks. Dit kon ik op deze manier doen omdat ik voorafgaand al wist dat ik geen narratieve analyse ging doen.

In de bevindingen spelen de quotes van de webshopmanagers een grote rol. Samen vertellen ze als het ware hun gezamenlijke verhaal over de ervaringen die zij hebben met cybersecurity en wat de gevolgen hiervan zijn. Omdat ik anonimiseer kan ik niet hun echte namen gebruiken, maar ik vond dat benoemingen als "webshopmanager A vertelt" afbreuk deed aan de persoonlijke lading van het verhaal. Daarom heb ik ervoor gekozen om pseudoniemen te gebruiken. Hieronder geef ik in een schema weer welke namen ik heb gebruikt voor de webshopmanagers. Tevens is deze lijst aangevuld met kenmerken over henzelf en het type webshop:

Pseudoniem	m/v	Branche	Grootte	Pseudoniem	m/v	Branche	Grootte
Anna	v	Mode	1-15	**Ian**	m	Mode	1-15
Bob	m	Mode	1-15	**Julian**	m	Mode	100-150
Coen	m	Woning	50-100	**Kay**	m	Woning	1-15
Daniëlle	v	Mode	1-15	**Leon**	m	Mode	1-15
Ewoud	m	Woning	1-15	**Marijn**	m	Mode	15-50
Floor	m	Woning	15-50	**Noah**	m	Mode	100-150
Gill	v	Mode	100-150	**Olivier**	m	Woning	1-15
Harm	m	Mode	1-15				

Tekeningen

Aanvullend op de verhalen uit de interviews heb ik gebruik gemaakt van visuele beeldspraak, omdat het gebrek aan zichtbaarheid volgens eerdere onderzoeken zo'n belangrijke factor speelt in de ervaring van het internet en het gebrek aan cyberveiligheid. De traditionelere onderzoeksmethoden zorgen ervoor dat het onderwerp abstract en onzichtbaar blijft. Door zichtbaarheid te creëren verwacht ik dat de data op een waardevolle manier kan worden aangevuld (Leavy, 2015, p. 232). Aangezien de deelnemers geen professionele kunstenaars zijn, zal de esthetische kwaliteit niet altijd even hoog zijn. Desondanks was deze methoden heel krachtig zijn om emoties en betekenissen over te brengen. (Leavy, 2015, p. 232). De tekeningen die het algemene verhaal van de managers samen duidelijk verbeelden voeg ik toe in mijn bevindingen.

Webshop-analyse

Aan de hand van de verhalen uit de interviews en de tekeningen kreeg ik een goed beeld van de positie van de manager. Het was voor mij echter lastig om te kunnen verifiëren in welke mate dit ook daadwerkelijk overeenkwam met de werkelijkheid. De managers zelf observeren leek zinloos, aangezien ik wist dat cyberveilig handelen op de werkvloer voor geen van de webshopmanagers een rol speelt. Aan de manier van handelen, praten en communicatie komt dan een vertekenend beeld, aangezien ik wist dat cyberveiligheid bij managers voornamelijk een rol speelt op het technische vlak, ofwel de webshop. Dit is het platform waarmee ze communiceren naar de klant toe. Het is hun visitekaartje. Hoe communiceren zij naar de klant toe op het gebied van cyberveiligheid? Voor het analyseren van de webshops zie ik een parallel met de waarde van een observatie. Een observatie kan nieuwe zaken aan het licht brengen. Zo kan het besproken zaken bevestigen of het kan juist tegenstrijdigheid omhoog halen tussen dat wat gezegd is in het interview en de observatie (Kawulich, 2005). Tijdens het interview vond de waarneming voornamelijk plaats door goed te luisteren, tijdens het tekenen speelden zowel luisteren als kijken een rol en tijdens het observeren van de webshops kon ik enkel afgaan op dat wat ik zag. Om systematisch te werk te gaan heb ik de website beoordeeld op basis van drie factoren die volgens Etzioni (2017) van toepassing zijn op het online vertrouwen: 1. Website design, 2. Recensies en 3. Trust-building platforms.

3.3 Data-analyse

Het analyseren van de data bestond uit drie codeerfasen. Het codeerproces begon ten eerste met open coderen waarbij ik mijn data ging afbreken, bestuderen, onderzoeken, vergelijken, conceptualiseren en categoriseren (Strauss & Corbin, 2007 in: Boeije, 2015, p. 112).De tweede fase bestond uit axiaal coderen, waarbij ik de codes uit het open codeerproces ging structureren en onderverdeelde in categorieën. Tot slot begon na het structureren van het axiaal coderen volgde het selectief coderen, waarbij ik verbanden legde tussen de eerder gevonden categorieën (Boeije, 2015, pp. 125 en 133). Ik begon na vijf interviews met open coderen in NVivo. Dit heb ik gedaan tot ik tien interviews had. Toen ben ik begonnen met axiaal coderen en heb ik grotere thema's binnen de onderwerpen gezocht. Hier werd duidelijk waar de managers het over eens waren. Tot slot ben ik met deze overeenkomsten verder gaan werken.

3.4 Kwaliteit van het onderzoek

Om een waardevolle bijdrage te kunnen leveren aan zowel de wetenschap als het Nederlands Cyber Collectief, is het van belang dat mijn onderzoek betrouwbaar is. De kwaliteit van mijn onderzoek kan daarom getoetst worden aan de hand van criteria die aansluiten bij de kwalitatieve en interpretatieve onderzoeksvorm. Deze wijken af van de 'standaard' positivistische criteria – betrouwbaarheid en validiteit - omdat in dit onderzoek het begrijpen van een specifieke context en de betekenisgeving hiervan het doel is (Schwartz-Shea & Yanow, 2012, pp. 91-92). Dat vraagt om meer uitleg over mijn keuzes en het beoordelen van de kwaliteit van het onderzoek. Trustworthiness voldoet hieraan en zal hieronder beschreven worden aan de hand van vier criteria die hieronder vallen: credibility, transferability, dependability en confirmability (Bryman, 2012, p. 390).

Credibility

Bij credibility gaat het erom dat het onderzoek goed is uitgevoerd en de resultaten besproken zijn met de participanten. Dit laatste zodat ik kan controleren of ik de sociale werkelijkheid van de managers wel goed heb begrepen (Bryman, 2012, pp. 390). Gedurende het onderzoek heb ik verschillende keuzes gemaakt die naar mijn weten behoren tot het doen van 'goed onderzoek'. De enige keuze die ik minder goed acht, is die waarbij ik naar de webshopmanagers toe heb verzwegen dat ik onderzoek doe voor het Nederlands Cyber Collectief en dat ik minimale informatie heb gegeven over het onderwerp. Ter compensatie heb ik wel geprobeerd te handelen alsof het onderzoek los van het NCC stond door webshopmanagers anoniem te houden en het NCC niet te 'promoten.' De webshopmanagers mail ik allemaal met de bevindingen om te controleren of zij zich hierin kunnen vinden. Daarnaast heb ik ook aan een aantal webshopmanagers gevraagd of ze feedback willen geven op mijn aanbevelingen. Op deze manier probeer ik de stem van de manager zo goed mogelijk te vertegenwoordigen in mijn onderzoek.

Transferability

In dit deel gaat het om de eigenschappen van het onderzoek die een beeld moeten geven over de context van de sociale wereld die ik heb onderzocht en hoe ik dit deze heb onderzocht (Bryman, 2012, pp. 390-392). De context van het onderzoek heb ik in de inleiding omschreven. Ik heb zo helder mogelijk geprobeerd weer te geven waarom ik nu precies dit onderzoek heb gedaan. Vervolgens heb ik in dit hoofdstuk inzichtelijk gemaakt hoe ik het onderzoek heb uitgevoerd en waarom ik dit zo heb gedaan.

Dependability

Deze criteria staat gelijk aan betrouwbaarheid in kwantitatief onderzoek en gaat over dat ik inzicht kan geven alle fasen van het onderzoek, zodra iemand hier om vraagt (Bryman, 2012, p. 392). De keuzes die ik tijdens dit onderzoek heb gemaakt zijn gebaseerd op gedachten die ontstonden na het lezen van theorie en verhalen over het onderwerp, maar ook aan de hand van gesprekken met verschillende mensen. Ik heb verschillende gedachten en keuzes genoteerd, maar niet alles, omdat ik geen autobiografisch onderzoek doe. Per respondent heb ik een map waarin het transcript van het interview, de bijbehorende tekening, de analyse van de webshop en aantekeningen van uitspraken (buiten het interview) of mails in staan. Het bijhouden ordenen hiervan heeft ervoor gezorgd dat ik

gedachten en informatie los kon laten gedurende het onderzoek en weer kon ophalen zodra ik het nodig had.

Confirmability

Deze criteria gaat erom of ik binnen de mogelijkheden zo objectief mogelijk gehandeld heb (Bryman, 2012, p. 392). Objectiviteit kan gedefineerd worden als "to stand outside the subject of study – meaning, to have both physical and emotional distance from it" (Schwartz-Shea & Yanow, 2012, p. 95). Dit is met kwalitatief en interpretatief onderzoek niet mogelijk en zelfs onwenselijk aangezien de bijvoorbeeld fysieke aanwezigheid van mij als onderzoeker belangrijk is geweest om een vertrouwensband op te bouwen, waardoor zij meer gingen vertellen en ik de betekenisgeving van de respondent beter kon begrijpen. Maar kijkend naar het startpunt van mijn onderzoek, kan gesteld worden dat mijn doelgerichte zoektocht naar een onderzoek over cybersecurity niet objectief is. Evenals de literatuur die ik hierover kreeg aangereikt door gelijkgestemde bij het NCC en verder vooronderzoek die leidde tot nieuwe inzichten en afbakening van mijn onderzoek (Schwartz-Shea & Yanow, 2012, p. 98). Ik was mij bewust van mijn eigen standpunten en worstelde in de eerste interviews met de angst dat ik te oordelend zou zijn tegenover webshopmanagers die een andere mening zouden hebben. Ik was daardoor extra voorzichtig en durfde niet echt door te vragen. Uiteindelijk heb ik mijn kennis en standpunten kunnen omzetten naar een kracht. Door kritische vragen te stellen, zonder dat ik een waardeoordeel gaf. Na een aantal interviews kon ik mijn eigen mening loslaten en dit kwam ook juist omdat ik zo nieuwsgierig was naar de betekenisgeving van de webshopmanagers. Het hielp voor mij ook om zo min mogelijk naar het NCC te gaan, omdat ik wist dat zij het niet eens waren met de houding van de webshopmanagers. Dit terwijl ik gedurende het onderzoek steeds meer open begon te staan voor hun visie en ik de stelligheid over de 'slechte houding' van het mkb anders begon te zien. Dit zag ik als een voordeel, omdat ik zo meer in staat ben de stem van de webshopmanagers te vertegenwoordigen.

4. Bevindingen

In dit hoofdstuk bespreek ik mijn bevindingen. De bevindingen heb ik gehaald uit de gesprekken met de webshopmanagers, de tekeningen die zij hebben gemaakt en de webshop-analyse. Uit deze gesprekken kwam naar voren dat zij betekenis geven aan situaties over en ervaringen met *cybercrime*. Op een aantal uitzonderingen na (die ook terug te lezen zijn in dit hoofdstuk) was vooral de eensgezindheid in hun verhalen typerend. In dit hoofdstuk laat ik het perspectief van de webshopmanagers zien door hun verhalen samen te bundelen tot een verhaal. Dit doe ik in vijf delen. Om meer context te geven over wie de webshopmanagers zijn, start ik in paragraaf 4.1 met een weergave van hun inhoudelijke taken en de rol die zij voor zichzelf zien met betrekking tot het cybersecuritybeleid. Vervolgens zal ik in paragraaf 4.2 bespreken hoe de webshopmanagers denken over veiligheid en wat zij doen om zichzelf te beschermen. In paragraaf 4.3 geef ik aan welke ervaringen de webshopmanagers tot op heden hebben met cybercrime. Daarna ga ik in paragraaf 4.4 in op de aanpak van het cybersecuritybeleid van de webshopmanagers. En in paragraaf 4.5 ga ik kort in op hoe de webshopmanagers hun cybersecuritybeleid beoordelen. Tot slot vat ik in paragraaf 4.6 kort de belangrijkste uitkomsten samen.

4.1 Context

Introductie van dé webshopmanagers

De gesprekken met de managers geven inzichten in hun taken en hieruit kon ik het volgende concluderen: dé webshopmanager bestaat niet. Om de doelgroep beter in te kunnen kaderen, is het goed om te weten dat *cybersecurity* eigenlijk nooit de enige taak is. Vaak is hun takenpakket heel breed en is cybersecurity slechts een bijzaak. Dit moet in ogenschouw worden genomen wanneer je kijkt hoe webshopmanagers met cybersecurity omgaan. Zo vertelt Bob bijvoorbeeld:

> "…omdat het ook een klein bedrijf is, pak je heel veel verschillende taken op. Over veel gedeeltes heb ik de eindverantwoordelijkheid. Zeker in het productiegedeelte, in het designgedeelte geef ik mijn mening. Maar aan het eind van de dag sta ik ook gewoon pakketjes in te pakken wanneer dit nodig is."

Harm is samen met zijn broer eigenaar van de organisatie. Zijn focus voor het managen van de webshop ligt voornamelijk op de marketingkant. Over zijn functie zegt hij:

> "…Ik probeer ervoor te zorgen dat we genoeg verkopen krijgen. Dus ik zorg voor promotie van de winkel en van de webshop. Ja en alles wat erbij komt kijken. Maar het is vooral de verkoopkant van het bedrijf. Dat is mijn hoofdfunctie."

Sommige webshopmanagers zijn niet de eigenaar, maar voelen zich wel eindverantwoordelijk en hebben zoveel taken dat ook webshopmanager zijn slechts een klein onderdeel is van hun takenpakket lijkt. Ian zei hierover:

> "Ik ben eindverantwoordelijk voor dit bedrijf. Ik hou me bezig met de strategie, maar ik heb mezelf ook als product owner opgeworpen voor een van de platformen. Ik doe daarnaast alle HR dingen en alles wat er verder voorbijkomt. En ik stuur dus aan op de werkvloer. Van alles wat. Leuk, maar wel hectisch soms."

Slechts één webshopmanager heeft een duidelijk afgebakende taak, met daarbij de focus op IT, Julian. Hij omschrijft zijn taak als volgt:

> "mijn functie heeft te maken met het creëren van waarden met IT voor het bedrijf, waaronder webwinkels, B2B e-commerce, ERP-systemen, interne infrastructuur, eigenlijk de hele ICT-mikmak."

Hierdoor heeft hij een afwijkend profiel, omdat hij (bijna vanzelfsprekend) meer kennis heeft dan gemiddeld over IT-zaken en daardoor ook over cybercrime en cybersecurity. Om dit te benadrukken noem ik hem naast 'Julian' ook 'de IT-webshopmanager'.

Webshopmanagers en het cybersecuritybeleid

Naast de diverse en soms uiteenlopende taken van webshopmanagers, viel het mij ook op dat geen enkele webshopmanager het regelen van cybersecurity uit zichzelf noemt als officieel onderdeel van zijn of haar werkzaamheden. Cybersecurity is een bijzaak en staat daardoor niet hoog op de agenda. Pas als ik specifiek vraag welke rol cybersecurity dan wel speelt bij de werkzaamheden van de webshopmanager, krijg ik antwoord. Sommige managers geven dan deels een sociaal wenselijk antwoord. Anna en Coen zeggen bijvoorbeeld:

> Anna: "Ik moet zeggen dat ik mij niet focus op beveiliging, maar het zijn wel dingen waar we ons bewust van moeten zijn."
>
> Coen: "Mijn en onze rol als organisatie is hierin klein, maar de verantwoordelijkheid blijft ten alle tijden hoog! Wettelijk gezien moeten wij klantgegevens beschermen. Welke mate van bescherming is natuurlijk vrij subjectief."…"Het is niet onze prio."

Ian denkt aan de ene kant dat hij meer zou moeten doen, maar vindt het aan de andere kant niet helemaal zijn taak:

> "Nou ik denk dat ik misschien meer verantwoordelijkheid zou moeten hebben daarin dan ik me daar nu van bewust ben. Aan de andere kant, kijk, ik geloof ook niet dat ik de persoon moet zijn die het in detail weet. Ik ga het ook niet uitvoeren. Daar zijn andere mensen voor."

Er zijn ook managers die redenen geven waarom cybersecurity geen grote rol speelt, zoals Bob:

> "Ik heb hierin een leidende rol. Maar ik denk dat we heel vaak, omdat we een klein bedrijf zijn, dat iedereen elk gedeelte moet oppakken als het druk is. En het is nogal vaak druk. Dat je bepaalde dingen misschien gewoon, nou dat je er gewoon geen tijd voor hebt om bepaalde dingen op te pakken."

Maar er zijn ook managers die heel direct aangeven dat het geen prioriteit heeft. Zo zegt Harm:

> "Nou eerlijk gezegd heb ik mij daar nog nooit echt mee bezig gehouden. Ik ga ervan uit dat het goed wordt gedaan. Daar moet ik op vertrouwen."

Alleen bij Kay en de IT-webshopmanager speelt cybersecurity een grotere rol in de dagelijkse werkzaamheden. Dit blijkt dan ook uit de antwoorden die zij geven in paragraaf 4.2, omdat zij gedetailleerder dan andere webshopmanagers kunnen vertellen over cybercrime en cybersecurity. Het hebben van cybersecuritybeleid hangt in deze casus niet af van de dagelijkse prioriteit die webshopmanagers eraan geven. Dit komt omdat zij het uitbesteden aan externe partijen met expertise. In paragraaf 4.2.3 ga ik hier dieper op in, maar eerst vertellen de webshopmanagers in de volgende paragraaf over hun ervaringen met cybercrime en cybersecurity.

4.2. Veiligheid in ogenschouw

In deze paragraaf bespreek ik hoe de webshopmanagers omgaan met hun veiligheid. Dit doe ik aan de hand van vijf korte paragrafen. Ten eerste bespreek ik het algemene veiligheidsgevoel van de webshopmanagers. Daarna ga ik ten tweede in op de manieren van de webshopmanagers om voor veiligheid te zorgen. De derde paragraaf gaat over hoe de webshopmanagers zichzelf online beschermen. Tot slot bespreek ik hoe de webshopmanagers omgaan met het nemen van online risico's.

4.2.1 Een veilig gevoel

Webshopmanagers wanen zich over het algemeen veilig. Het merendeel neemt wel wat maatregelen om zichzelf tegen allerlei soorten gevaar te beschermen, maar ze willen hier niet al te veel bij stilstaan. Zo vertelt Floor:

> "Ik sta heel losjes in het leven als het daar om gaat. Gelukkig. Dus ja veiligheid is voor mij nooit zo'n issue. Natuurlijk neem ik wel maatregelen. Als ik in de auto stap doe ik mijn gordel om. Maar er zijn zoveel omstandigheden die je niet in de hand hebt. En daar moet je in mijn optiek heel luchtig mee omgaan. En dat doe ik dan ook."

Floor omschrijft een aantal simpele veiligheidsmaatregelen die weinig tijd kosten. Maar het algemene beeld wat de webshopmanagers afgeven is dat reageren op een onveilige situatie, vooral reactief gebeurt. Zo zegt Ian:

> "Bij situaties in het ov, festivals, plaatsen waar veel mensen zijn. Als er iets aan de hand is gebeurt het dan en reageer je dan. Maar ik ga niet naar een festival met de gedachte "ik ga achteraan staan, want als er iets gebeurt ben ik sneller bij de nooduitgang." Dat heb ik niet in mijn systeem. Dus als er iets gebeurt dan is het op het moment."

Reactief handelen lijkt ook een natuurlijke reactie, want het merendeel van de webshopmanagers voelt zich in het algemeen veilig en heeft daardoor geen angst. Danielle denkt zelf dat haar gebrek aan angst ook onveilig kan zijn. Zij vertelt hierover:

> "Ik heb zelf geen angst. Dus dat is een zwakte vind ik. Want ik kan rustig in het bos 's nachts lopen en hardlopen en dat er niemand is en het is pikkedonker. Dat maakt mij niet uit. Ik ben niet bang aangelegd. Terwijl, eigenlijk zou je dat wel een beetje moeten zijn, om je veiligheid te creëren."

De webshopmanagers voelen zich relatief veilig en nemen over het algemeen simpele maatregelen om zichzelf te beschermen tegen mogelijk gevaarlijke situaties. Maar over het algemeen hebben zij het gevoel dat zij pas kunnen reageren op een onveilige situatie als deze zich voordoet.

4.2.2 Laat angst niet regeren

De webshopmanagers lijken het gevoel van veiligheid te willen vasthouden. Er gebeuren veel slechte dingen in de wereld, maar ze zien in en accepteren dat ze niet alles kunnen voorkomen en geven aan dat een negatieve gebeurtenis iedereen kan overkomen. Tijdens de gesprekken kwam omgaan met de kans op een terroristische aanslag meerdere malen aan bod. Een risico waar geen van de webshopmanagers ervaring mee heeft. Zij gebruikten dit voorbeeld over hoe ze omgaan met veiligheid in het algemeen, maar ook vaak om te illustreren hoe ze omgaan met het risico op cybercrime. Een algemeen gevoel dat overheerst is dat als criminelen – en dus ook cybercriminelen – slechte intenties hebben, het ze uiteindelijk ook wel lukt om een misdaad te plegen. Kay zegt hierover:

> "Ja. Ik denk dat het wel heel lullig is dat het uiteindelijk zo is. Heel vervelend. Maar ik denk dat het daar wel op neerkomt, ja. Je kan alles eraan doen en je kan er zo goed mogelijk mee omgaan, maar nog steeds denk ik dat het overal kan voorkomen. Het [cybercrime] is net als … Het is eigenlijk een beetje als terrorisme."

Cybercrime is volgens meerdere webshopmanagers net als terrorisme iets wat iedereen kan overkomen. En het heeft volgens hen simpelweg geen zin om je hier voorafgaand druk over te maken. Ze willen zich niet onnodig onveilig voelen. Marijn omschrijft het gevoel van de webshopmanagers goed:

> "Ja, wat kan ik eraan doen. In stress leven? Nee, als het zo mocht zijn dat me dat gebeurt, dan heb ik liever dat ik in de aanloop ernaar toe een lekker leven leid, dan dat ik mijn hele leven in de stress ben

gaan zitten en het dan alsnog het gebeurt. Dan heb ik een stressvol leven gehad en gebeurt het alsnog. Mijn moeder heeft ooit een spreukje op de koelkast gehangen daar stond op: "Je kunt je zorgen maken, maar gebeurt er niets met je, dan heb je voor niks je zorgen gemaakt. Je kunt je zorgen maken en er gebeurt wel wat, dan heb je je altijd zorgen gemaakt en dat heeft dus niet geholpen."

Kortom, het heeft volgens de webshopmanagers geen zin om je continu zorgen te maken over een cyberaanval die mogelijk kan gaan plaatsvinden in de toekomst. Ze willen over het algemeen zo min mogelijk bezig zijn met veiligheid en genieten van het leven. Toch hebben de managers – net als voor in de fysieke wereld – wel simpele veiligheidsmaatregelen waar ze op letten als ze online zijn.

4.2.3 Logisch nadenken

Het algemene beeld van de webshopmanagers is dat als een cybercrimineel wil hacken, dit ook lukt. Maar dit betekent volgens hen niet dat je helemaal niks kan doen. De webshopmanagers geven aan dat zij online wel degelijk letten op een aantal kenmerken die wijzen op cybersecurity. De mogelijkheid die de meeste webshopmanagers geven voor het voorkomen van cybercrime is 'logisch nadenken.' Dit kan volgens hen mede door goed te kijken naar bijvoorbeeld de inhoud van e-mails. Ian vertelt hierover:

> "Ja, ik klik niet op e-mails die ik binnenkrijg waarvan ik denk "dat is vragen om problemen" of "ING stuurt niet deze e-mails", dus daar ga ik niet op klikken. Maar daar stop het ook wel mee. Ik heb niet een uitgebreid *security* plan voor mezelf."

Een ander kenmerk waar webshopmanagers op letten is het design van een website of tekenen van een keurmerk. Zo zegt Daniëlle:

> "Je moet het ook wel zien of een site betrouwbaar is. Of ze een Thuiswinkel logo hebben of dat soort dingen. Ik kijk daar echt wel naar… Ik moest afgelopen keer iets bestellen voor het bedrijf en die site die had geen algemene voorwaarden en die zag er een beetje louche uit. Ja, daar ga je niet mee akkoord natuurlijk. Daar ga ik niet mijn gegevens achter laten."

Daniëlle geeft aan nog nooit gehackt te zijn en is tevreden over de manier hoe zij controleert of een webshop betrouwbaar is. Haar handelswijze lijkt nog nooit het tegendeel te hebben bewezen. Op basis van haar ervaringen heeft zij een profiel opgebouwd voor kenmerken van een veilige webshop. Een kenmerk daarvan is ook dat de webshop een bekende naam moet hebben. Zij zegt hierover:

> "… je moet wel een beetje *common sense* gebruiken. Maar verder als het gewoon een goede site is, zoals een Zara of zo, die algemeen bekend staat als *delivery's*..."

Ander webshopmanagers delen de mening van Daniëlle. Zo ook de IT-webshopmanager. Als vindt hij het wel lastiger om uit te gaan van dat wat hij typeert als veilig, maar uiteindelijk gaat hij hier toch op af. Hij vertelt hierover:

> Nou ik weet hoeveel je moet doen om een Thuiswinkel Waarborg certificaat te halen. Daar zijn we ook even mee bezig, dus daar geloof ik nu wel in. Maar ik vind het altijd een beetje lastig beoordelen. Want je kan zo makkelijk een plaatje erop zetten. Tuurlijk kan Thuiswinkel er wel iets aan doen, maar wie weet ben je net te laat. Dus ik kijk gewoon of ik zo'n site vertrouw. En ik koop sowieso het meest bij een site als Cool Blue. Dat heeft te maken met de goede service, maar daarnaast weet je dat je daar niet wordt opgelicht."

Ook de 'kenner' onder de webshopmanagers vertrouwt op grotere webshops en platforms, omdat hij daar goede ervaringen mee heeft. Het vertrouwen in grote webshops is groot, terwijl veel webshopmanagers ook verwijzen naar nieuwsberichten over cybercrime, waar juist grotere organisaties worden uitgelicht. Het voelt voor sommige webshopmanagers dan ook tegenstrijdig om juist grote

organisaties te vertrouwen, maar aan de andere kant hebben grotere organisatie meer beveiliging. Kay vertelt hierover:

> "Ja, dat is altijd heel moeilijk om te zeggen. Ik hoop dat ze er goed mee omgaan. En zeker als ik bij grote, Nederlandse bedrijven koop. Dan ga ik ervan uit dat er goed mee omgegaan wordt. Maar ook die bedrijven zijn gevoelig. Die zijn eigenlijk veel gevoeliger nog voor aanvallen en data diefstal eigenlijk. Een hacker of een hackerspartij zou zich op ons kunnen richten, alleen dan halen ze niet zoveel als ze bij Bol.com halen. Of bij een Ahold of waar dan ook. Je gaat er dan vanuit dat het veilig is, omdat het bij een hele grote partij ligt. Maar ja, of dat dan echt zo is, dat vind ik ook heel moeilijk te zeggen. Ik ben niet heel actief in hacken, dus ik volg het eigenlijk ook niet heel erg."

Kay denkt dat grote organisaties sneller het doelwit zijn omdat hier meer te halen valt, maar heeft ook het gevoel dat grote organisaties voor betere cybersecurity kunnen zorgen. Als een website betrouwbaar oogt, dan lijken de webshopmanagers het risico te durven nemen. In de volgende paragraaf ga ik hier dieper op in.

4.2.4 Risico's nemen

Alle webshopmanagers geven aan zelf online te shoppen. De acceptatie voor het nemen van privacy risico's tijdens het online shoppen lijkt vanzelfsprekend. Het dilemma is niet óf maar wáár zij wel of niet hun producten willen kopen als klant. De webshopmanagers vinden het niet erg om persoonlijke gegevens achter te laten op een website. Gill heeft het gevoel dat dit ook wel moet om mee te gaan met de tijd. Ze geeft aan dat ze de consequenties kent, maar maakt zich geen zorgen. Zo vertelt zij:

> "Als ik in een webshop ga shoppen ben ik mij wel bewust van wat ik invul, maar ik til er niet heel snel aan. Dus ik weet wel wat ik doe, maar het is omdat de wereld die kant op wil en is veranderd, dus dan ga je daar in mee. Je wil toch online bestellen dus je vult je gegevens in en betaalt gewoon online. En ik realiseer mij goed door het bedrijf, dat de big data die je daarmee verstrekt dan zijn werk zal doen. Dus alle gegevens die je wil, jouw koopgedrag, muisklikgedrag, alles is meetbaar, registreerbaar, bruikbaar om voor een volgende situatie klantgedrag in kaart te brengen en te sturen."

Maar voor sommige webshopmanagers zitten er wel grenzen aan de informatie die zij willen afgeven. Zo vertelt Daniëlle:

> "Nou ze vragen best wel veel informatie nu, tegenwoordig, op het internet. Ik ben daar niet zo heel erg moeilijk in. Dus mijn gegevens of zo mogen ze best hebben. Zolang het niet te persoonlijk wordt vind ik het prima. Maar bijvoorbeeld niet "heb je een ziekte?" of zo. Echt dat hele persoonlijke, dat hoeft van mij niet."

Harm gaf aan dat het bij hem voornamelijk gaat om snelheid van de levering en het vermijden van financiële risico's online. Zo zegt hij hierover:

> "Nou stel je voor, je hebt vier winkels en die hebben allemaal dezelfde artikelen voor dezelfde prijs, dan ga ik wel eerder voor de webshop met een thuiswinkel logo. Maar ik denk wel dat als ergens anders zonder logo de levertijd sneller is, de overweging om daar te kopen wel groter is. Maar dan moet je het wel snel nodig hebben. Als je geen haast heb...ja… dat zie je ook wel in de markt bij ons." Dat dit mogelijk ten koste gaat van zijn privacy vindt Harm niet erg: "Nee, daar let ik dan niet op. Kijk, ik bestel natuurlijk wel het een en ander online. En als ik iets in het buitenland bestel, dan ben ik geneigd dit met een creditcard te kopen, omdat ik dan wel een stukje zekerheid heb."

Over het algemeen maken de webshopmanagers zich weinig zorgen als zij online shoppen. Zij letten op een aantal veiligheidskenmerken en er zijn nuance verschillen in de de grenzen die zij hanteren voor het

afgeven van informatie. Gill verwoordt tot slot het algemene gevoel van de manager helder: "Nou, ik ben zelf heel makkelijk. Ik heb niet zo'n probleem met gegevens. Ik zit niet als een paranoia iemand achter de computer van 'zal ik dit wel of niet invullen'." Online shoppen lijkt vooral te gaan over het gemak en als zij de hele tijd met mogelijke veiligheidsrisico's bezig moeten zijn, dan is dit voordeel er niet meer. Daarnaast geeft het merendeel van de webshopmanagers aan dat zij tot op heden weinig ervaring te hebben met cybercrime. Hier vertellen de webshopmanagers in de volgende paragraaf meer over.

4.3 Aanzien doet gedenken

In deze paragraaf staan de ervaringen die de webshopmanagers met cybercrime hebben centraal. Hierbij gaat paragraaf 4.3.1 over het gevoel van gebrek aan schade bij cybercrime. Daarna gaat het in paragraaf 4.3.2 over de nieuwservaringen met cybercrime en geven de webshopmanagers aan hoe zij hier op professioneel vlak mee om gaan.

4.3.1 Ervaring met cybercrime

Weinig tot geen materiële schade

Het merendeel van de webshopmanagers geeft als antwoord op de vraag of zij wel eens slachtoffer zijn geworden van cybercrime het antwoord dat dit niet het geval is. Als webshopmanagers aangaven geen ervaring met cybercrime te hebben, leek het voor hen een lastig onderwerp om over te praten. Want wat is cybercrime dan precies? De zwakke vormen van cybercrime lijken niet te behoren tot een kernmerk waarbij een webshopmanager zegt slachtoffer te zijn. Iedereen krijgt namelijk wel spam of phishing-mails en tot op heden lijkt het internet geen negatieve gevolgen te hebben. De uitspraken van Floor en Ian illustreren dit:

> Floor zegt: "Natuurlijk heb ik weleens verkeerde mailtjes gehad, maar het heeft nog nooit tot schade geleid."
>
> Ian vertelt: "Weet je, ik heb er gewoon niet zo veel last van. Mijn identiteit is nog nooit gejat. Er is nog nooit iets gebeurd. I don't know. Ik weet ook niet wat de impact is als het wel fout gaat. Wat als iemand mijn e-mailadres ergens vandaan trekt? Spam krijgen we allemaal, dat is ook niet uitzonderlijk. Sterker, dat is heel normaal. Ik denk dat je pas en dat is heel vervelend, maar heel hard gaat nadenken op het moment dat het fout gaat."

Door gebrek aan ervaring ondervindt hij geen hinder aan het internet. Hij spreekt van een spam-norm als het gaat om ongewenste e-mailberichten. En geeft aan dat het voornamelijk een kwestie is van reactief handelen. Bob heeft wel ervaring met cybercrime en is ook van mening dat dit voornamelijk reactief is op te lossen, omdat het voor die tijd niet zichtbaar is dat er iets mis is. De ervaring die hij heeft lijkt niet zoveel indruk op hem te maken:

> "Mijn Xbox-account is een keer gehackt en toen hebben ze daarvandaan mijn creditcard kunnen gebruiken. Hebben ze een afschrijving kunnen doen van 10 euro of zo. Voor de rest eigenlijk nooit nee."

De laconieke houding lijkt aan te geven dat een ervaring met cybercrime waarbij 10 euro ontvreemd is, niet zo heel erg is. Hij lijkt zich dan ook niet echt een slachtoffer te voelen, omdat hij niet onder de hack geleden heeft. Dit zie je ook terug bij Coen. Hij geeft aan geen ervaring te hebben met cybercrime, maar dat zijn Hotmail-account waarschijnlijk wel een keer gehackt is:

> "Nee, eigenlijk niet. Ik- nee. Niet echt meegemaakt. Ik heb wel een keer meegemaakt dat m'n Hotmail gehackt is en dat daardoor heel veel wachtwoorden- heel veel gezeik zeg maar. Denk wel dat iemand

een keer in mijn Hotmail geeft ingebroken, maar ik werd wel gebeld door Microsoft zelf, die hadden het zelf geconstateerd dat er was ingebroken. Die hebben het ook geblokkeerd en mij gebeld van joh, luister Coen, je email hebben we even geblokkeerd, want iemand probeert erin te komen."

De webshopmanager ervaart zijn gehackte e-mailaccount niet als cybercrime. Zolang de (poging tot) cybercrime niet tot schade leidt, ervaren de webshopmanagers geen problemen.

Als webshopmanagers geen ervaring met cybercrime ervaren, dan blijven zij handelen zoals zij al handelen. Leon geeft als enige webshopmanager aan wel schadelijke ervaring te hebben, omdat de organisatie vorig jaar te maken heeft gehad met ransomware. Hij was dit in eerste instantie even vergeten, maar zegt vervolgens:

"Nou trouwens, vorig jaar had hier iemand een mailtje geopend wat niet helemaal goed was… Ransomware. Toen waren er twee computers kapot. Nu je dat zo zegt, ik ben er wel bedachtzaam op, dat we hier niet effentjes dat virus [*WannaCry* en *NotPetya*] openen."

Door zijn ervaring met ransomware, is Leon er bedachtzaam op dat dit niet nog een keer gebeurt. Voornamelijk omdat dit ertoe kan leiden dat content voor de website kwijtraakt of gegevens die bijdragen aan een goede klantenservice. Zo zegt hij:

"Zoals updaten of opzoeken van content. Dat zou dan wel in één klap weg zijn, tot aan het begin van 2010, zeg maar. Sinds 2010 houden we dat allemaal bij. Als iemand ons mailt met de vraag: "Ik heb dit horloge", dan kunnen we nooit meer terugzoeken waar dat vandaan komt. Dat zou wel jammer zijn."

Het zou volgens Leon wel jammer zijn als content verdwijnt. Dit wil hij zeker voorkomen, maar de manier waarop hij erover praat geeft mij niet het gevoel dat het echt een grote ramp zou zijn.

Geen fysieke schade

In paragraaf 4.2 liet ik zien dat de managers zich veilig voelen. Zij voelen zich fysiek veilig. De webshopmanagers ervaren dat cybercrime of de kans op cybercrime de veiligheid tot op heden niet aantast, zelfs niet als het een concrete fysieke dimensie heeft. Hierdoor ondervinden ze er geen hinder aan. Ian illustreert aan de hand van een voorbeeld over het beschermen van zijn dochter van drie, dat volgens hem de impact niet groot is als foto's van haar van zijn telefoon worden gestolen:

"Nee, het gevolg is niet zo. Je voelt het niet. Kijk als een foto van mijn dochter in haar nakie op het strand om wat voor reden dan ook op een pedofielen netwerk terecht komt, zou ik dat heel naar vinden, maar het doet met haar niet zo heel veel. Ze loopt er niet meer gevaar door, tenzij ze weten wie ze is. Maar dat geloof ik dus niet dat het zo werkt. Daar ben ik echt niet bang voor. Dus dat zij daar zou staan zou ik naar vinden, maar over een jaar herken je haar niet meer, want zo snel groeien ze. Wat is dan de consequentie van dat die foto gejat wordt. Die is dus niet zo groot. Dan kan je nog zeggen, "maar ethisch gezien mag het niet" ja dat klopt, dat mag ook niet, maar de schade is niet zo groot."

Ian geeft hier heel eerlijk een niet sociaal wenselijk antwoord. Het lijkt erop dat zolang de ervaring niet al te negatief is, webshopmanagers risico's blijven nemen door geen of minimale preventieve maatregelen te nemen. Al wordt deze afweging door Ian niet bewust gemaakt: "Ik ben er niet zo mee bezig en ik denk dat dit heel goed is, want anders heb je volgens mij echt een heel vervelend leven, als je alleen maar met je eigen veiligheid bezig bent."

4.3.2 Nieuwsberichten over cybercrime

De ervaringen die webshopmanagers hebben met cybercrime die schadelijk was, komen voort uit nieuwsberichten. Via deze weg weten webshopmanagers dat grote organisaties getroffen worden door cybercrime en dat dit mogelijk gevolgen heeft voor hun persoonlijke data. Toch zorgen de nieuwservaringen waaruit kansen voor datalekken voortkomen niet voor verandering in hun koopgedrag. Noah licht dit toe aan de hand van een metafoor:

> "Als je in een bos loopt en je hebt gewoon geleerd: "Die besjes zijn rood. Die blauwe besjes moet je niet pakken, want die zijn giftig." Dan kom je opeens groene besjes tegen. Wat doe je dan? Zijn ze wel of niet goed? Ga je dan weer terug het pad op waar dan die rode of blauwe besjes zijn?"... "Slecht nieuws sla je sneller op, want dat bepaalt ook jouw veiligheidsgevoel. Daarom wordt er altijd onveilig nieuws geprojecteerd. Omdat je dat beter opslaat. Dat zijn de groene besjes die je dan tegenkomt. "O, wacht even. Gevaar. Wat is dit? Hoe moet ik hiermee omgaan?" Analyseren, oké. Dan heb je helemaal aangevoerd dit en dat. "O, ik heb iemand anders zien eten." De volgende dag niet ziek? Nee, überhaupt niet ziek. Geen erge effecten. "Nu durf ik hem wel aan te pakken om te eten. Groene besjes zijn hartstikke lekker…Dan wordt het geaccepteerd en dan gaan we ermee verder."

Noah illustreert hier het belang van ervaring. De groene besjes kunnen bijvoorbeeld gezien worden als nieuwe webshops of webshops die gehackt zijn en daarmee in het nieuws komen. Bij een nieuwsbericht dat een (grote) webshop gehackt is staan klanten op scherp. Iemand gaat vervolgens na hoe 'gevaarlijk' het is om bij deze organisatie iets te kopen. Als hij ervaart dat de hack bij hem en niemand in zijn omgeving tot schade leidt, berichtgeving over schade bij andere mensen uitblijft en nieuwe aankopen gaan goed, dan zal de klant concluderen dat het (weer) veilig is om bij de webshop te kopen.

Het mkb is geen target

De nieuwsberichten over cybercrime lijken alleen te gaan over grote organisaties. Hierdoor hebben de managers het gevoel dat hun kleine webshop geen target is voor cybercriminelen. Anna vertelt hierover:

> "Je hoort weleens in het nieuws dat er wordt gehackt of dat er een website platligt, dus ik denk dan meer aan grotere bedrijven…dan concreet iets persoonlijks of op het werk."

Het gevoel dat het mkb geen target is delen andere managers ook. Floor zegt hierover:

> "Ik troost me al met de gedachte dat ik geen grote bank ben. Dus niet zo'n interessant target voor dat soort criminaliteit als het gaat om wat de laatste tijd in het nieuws is."

Als ik doorvraag over de impact van het nieuws geven de meeste webshopmanagers aan dat ze dan wel even nadenken over cybersecurity, maar tot nu toe zijn er geen aanwijzingen dat het mis gaat. Anna licht dit toe:

> "…dat het [cybercrime] zoiets is als "oja, het zou nuttig zijn om hier iets aan te doen." Maar door gebrek aan tijd is het iets op je wensenlijst waar je nooit aan toe komt. Dus dat je wel beseft dat daar wel stappen op te ondernemen zijn en dat je kan verbeteren, maar er staan veel concretere dingen op mijn lijst. Dagelijkse dingen waardoor je denkt "dat komt wel een keer".

Leon, die ervaring heeft met ransomware, heeft niet het idee dat de nieuwsberichten over cybercrime een signaal zijn voor zijn winkel om meer op te letten. Hij stelt dat vooral andere organisaties en landen getroffen worden. Zo vertelt hij:

> "Nee, de enige dingen die ik hoor, is op het nieuws. Ziekenhuizen die platliggen in Engeland. Heel Oekraïne dat platlag. Hier in Nederland een kippenboer die op een verkeerd mailtje had geklikt. Dat soort dingen hoor ik. Ja, datalek dit, datalek zo."…"Ik verwacht niet dat een webwinkeltje zoals die van

ons, ineens een prooi zal zijn voor een hacker, die onze gegevens wil stelen"… "Ik doe dit tien jaar, er is nog nooit voorgekomen, dat er iets gebeurd is op dit vlak. Dus ik zou niet weten waarom dat in één keer zou moeten veranderen. "

De ervaringen van andere grotere organisaties voelen niet als een serieuze wake-up call om zelf ook meer te doen. Zij besteden hun cybersecuritybeleid voornamelijk uit en ervaren dat dit goed werkt. Zowel de webshopmanagers met kennis als zonder kennis ervaren dit.

4.4 Op eigen ogen vertrouwen

De vorige twee paragraven geven inzicht in de ervaringen die webshopmanagers hebben op het gebied van (online) veiligheid en cybercrime. In deze paragraaf ga ik in op de wijze waarop de webshopmanagers hun cybersecuritybeleid inrichten, wat nagenoeg volledig inhoudt: uitbesteden aan experts op het gebied van cybersecurity. In paragraaf 4.4.1 bespreek ik eerst kort de motivatie van de webshopmanagers. In paragraaf 4.4.2 ga ik vervolgens in op de type experts die de webshopmanagers hun cybersecurity toevertrouwen. Tevens gebruik ik in deze paragraaf naast de interviews, ook de webshop-analyse die ik heb uitgevoerd en tekeningen van de webshop-managers zelf om het verhaal van de webshopmanager te verduidelijken.

4.4.1 Motivatie voor uitbesteding

Cybersecurity is voor het merendeel van de managers een onbegrijpelijk iets. Ze weten dat het nodig is en besteden hier dan ook geld aan. De webshopmanagers geven aan dat cybersecurity voornamelijk een technische aangelegenheid, waardoor uitbesteding ook nodig is, willen ze de beveiliging goed geregeld hebben. Anna zegt hierover: "Ik denk dat het toch een stukje gebrek aan kennis is. Door informatie die ik mis dat ik ook niet weet welke stappen ik zou kunnen ondernemen." En Bob zegt: "Ik ben niet technisch aangelegd." Julian, de IT-webshopmanager licht het standpunt uitgebreider toe en zegt:

> "Ik ben wel van het specialiseren in bepaalde taken. Het beveiligen van servers is een vrij specialistische taak. Laat daar dan mensen op zitten die dat leuk vinden, die daar goed in zijn, dat daar hun baan vanaf hangt of ze dit goed doen of niet. Dat vind ik een logischere stap."…" "Dus je verschuift eigenlijk die verantwoordelijkheid van die security."

Het uitbesteden van de beveiliging aan specialisten lijkt niet alleen goed voor het niveau van de beveiliging, maar zorgt ook voor een verschuiving in de verantwoordelijkheid. En dat is Volgens Noah mogelijk omdat cybersecurity-organisaties volgens hem snel moeten handelen op cybercrime, omdat het hun bedrijfsprofiel is en het bedrijf failliet gaat als ze niet goed blijken te zijn. Zo vertelt hij:

> "Als ze risico lopen, dan hebben ze een batterij van duizend man erop zitten om het te fixen. Voor die 20.000 klanten. Ze lijden anders zoveel schade … Het is hun bedrijfsprofiel, weet je wel. Veiligheid, daar begin je mee. Als je dat niet kan garanderen, dan stapt niemand in jouw product."

Het kunnen uitbesteden van cybersecurity ervaren de webshopmanagers dan ook als prettig. Niet alleen omdat zij aangeven dat zij geen kennis hebben over cybersecurity, maar óók omdat zij geen kennis willen hebben over cybersecurity. De beveiliging van zowel hun eigen informatie, als de informatie van klanten, is daarmee ook veiliger in de handen van experts. Noah vertelt dat uitbesteden volgens hem juist betrouwbaar is, omdat hij zelf denkt dat ze bij een hack zouden zeggen: "We hadden beter op moeten letten" Terwijl het volgens hem is: "Nee, je wilde niet opletten." Het niet willen opletten geeft aan dat de prioriteiten voor Noah ergens anders liggen dan bij cybersecurity en dat is iets wat andere webshopmanagers ook delen. Daarom besteden zij het cybersecuritybeleid uit en hebben veel

vertrouwen in de experts die volgens hen zorgen voor cybersecurity. In de volgende paragraaf bespreek ik de ervaringen die de webshopmanagers hebben met verschillende type experts.

4.4.2 Outsourcing naar experts

Uit de gesprekken met de webshopmanagers kwam naar voor wie en welke organisaties zij de cybersecurity toevertrouwen. De type experts waar de webshopmanagers het over hadden kunnen grofweg onderscheiden worden in drie types: 1. Technische experts 2. *Payment Service Providers* en 3. Keurmerken. In deze paragraaf bespreek ik van elk type wat de webshopmanagers hieronder verstaan en waarom zij hen zo vertrouwen. Hierbij maakt ik gebruik van twee tekeningen die het verhaal van de webshopmanagers illustreren. Daarnaast zal ik per onderdeel kort de webshop-analyse koppelen aan de verhalen van de webshopmanagers.

1. Technische experts

Onder technische experts vallen mensen of organisaties die de platformen beheren, de *front* en *back-end development* van de website doen, servers beheren en software leveren. Kay is een webshopmanager die iets meer verstand heeft van cybersecurity. Hierdoor kon hij redelijk gedetailleerd uitleggen wat zij waar uitbesteden en waarom. Hij voegt eraan toe dat hij veel vertrouwen heeft in de experts. Hij vertelt hierover:

> "We werken met SSL, sowieso. We werken met derde systemen die in de cloud werken, eigenlijk. We hebben een onbekende software die we daarvoor gebruiken. Dat is ons ERP-systeem, dat is van NetSuite. Dat is dan weer van Oracle. Oracle is heel groot natuurlijk. Wij maken gebruik van hun online-diensten. Dat is gewoon een hele grote, stabiele en betrouwbare partij. Ik neem aan dat de gegevens die we daar opslaan ook"…"Tenminste, dat neem ik niet aan. Dat is zo. Zij voldoen aan allemaal certificaten, zij slaan hun data op in Europa."

Opvallend is dat bijna al deze experts onzichtbaar zijn voor de klant. Kay, maar ook andere webshopmanagers noemen SSL als belangrijk kenmerk voor een betrouwbare website. Ik noem het daarom een vertrouwensfactor. In tabel 1 is te zien dat ik als klant kan waarnemen dat zij dit allemaal hebben.

Webshopmanagers	A	B	C	D	E	F	G	H	I	J*	K	L	M	N	O
Type vertrouwensfactor															
SSL-certificaat	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Tabel 1 *IT-manager

Kay geeft aan dat hij veel vertrouwen heeft in de partijen die hij inschakelt voor de cybersecurity. Bij webshopmanagers die er minder verstand van hebben dan hij is dit vertrouwen er ook, maar juist omdat zij er zelf niks vanaf weten. Volgens Harm hoeft dit ook niet, omdat het niet zijn taak is. Hij heeft binnen zijn organisatie de taak om de beveiliging uit te besteden en niet om zelf voor cybersecurity te zorgen. Hij vertelt hierover:

> "Dat laat ik over aan mensen die er verstand van hebben." Want: "Het is minder begrijpelijk. Het hoort niet tot mijn takenpakket. De beveiliging hoort bij hun. Ik vind die veiligheid wel belangrijk, maar het is technisch en die wetgeving verandert heel veel. Vandaar dat ik dit ook heb uitbesteed…En als ze daar

inbreken, dan kunnen die gegevens op straat komen te liggen, maar die server is naar mijn weten goed beveiligd. Dus wat dat betreft maak ik mij geen zorgen."

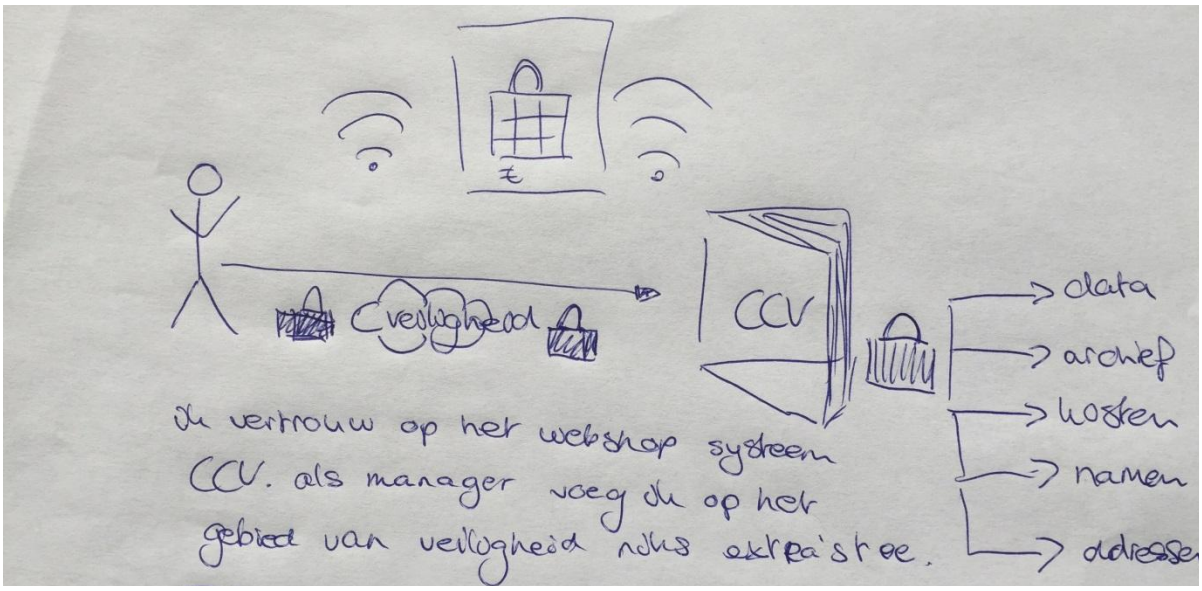
Op de vraag hoe hij dit weet zegt Harm: "Nou ja, dat dat draait gewoon bij een server die extreem goed beveiligd is en daar ga ik dan vanuit." Hij beseft zich dat veiligheid belangrijk is, maar vindt zelf niet dat hij hier iets vanaf hoeft te weten, omdat hij vertrouwt dat de experts dit goed regelen. Ian bevestigt dit argument en geeft aan dat het vertrouwen er is dat de experts preventief beveiliging en als het mis gaat reactief snel handelen. Zo vertelt hij:

"kijk, ik geloof ook niet dat ik de persoon moet zijn die het in detail weet. Ik ga het ook niet uitvoeren. Daar zijn andere mensen voor… We werken in WordPress. Dat is wat we ook tegen iedereen zeggen. We houden wel in de gaten hoe lek dat is. Niet zozeer dat we dat zelf testen, maar ja, er zitten ontzettend weinig lekken in. En als het al een keer zover is, dan wordt het heel snel *gepatcht* en uitgerold. Dus er zit heel veel vertrouwen in dat soort systemen, want zij houden dat gewoon super goed bij."

Het vertrouwen in het tegenhouden en oplossen van cybercrime geeft de webshopmanagers meer vertrouwen in de experts. Ook Bob heeft hier ervaring mee en legt uit dat het platform Shopify hen inlicht als er een risico is:

"Wij hebben ook wel een aantal keer aanvallen gehad. Mensen hebben geprobeerd bij ons in te loggen en dan krijgen we daar meldingen van"…"Shopify is daar wel redelijk bekwaam in om dat soort dingen snel op te vangen. Ook met creditcard *schemes*. Daar krijg je meteen een soort melding van dat het een hoge risicofactor heeft en dat je dan bepaalde dingen moet doen."

Door al deze goede ervaringen vertrouwen webshopmanagers volledig op de organisaties die hun website beheren, want zoals Noah nog kort toelicht: "Zij hebben een back-up systeem. Zij hebben veiligheidsprotocollen. Want het kan gewoon niet misgaan." De tekening van Anna illustreert bovenstaand verhaal helder:



Tekening van Anna

2. Payment Service Provider

Webshopmanagers	A	B	C	D	E	F	G	H	I	**J***	K	L	M	N	O
Type vertrouwensfactor															
PSP**	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

tabel 2 *IT-manager ** Payment Service Provider

Een ander type specialist waar iedere webshopmanager mee te maken heeft zijn zogenaamde Payment Service Providers (PSP's). Net als bij de vertrouwensfactor van SSL-certificaten, kunnen klanten zien of een webshop hier gebruik van maakt. Zoals te zien is in tabel 2, maken alle webshopmanagers gebruik van een PSP. De IT-webshopmanager legt uit dat een organisatie zichzelf niet zomaar een PSP kan noemen, waardoor het een betrouwbare vertrouwensfactor is:

> "Als je betalingsverkeer wil managen over het internet, dan moet je wel een flinke investering doen om qua infrastructuur dat te mogen doen, wettelijk gezien. Moet je ook niet zelf willen…Dus webshops gebruiken Molly en iDeal met behulp van een andere - je hebt er honderdduizend. Wij gebruiken Multi Safe Pay voor Nederland. Maar het is zo ingewikkeld en het moet zo veilig zijn, dus dat moet je niet zelf willen. En zij pakken een percentage van de transactie."

Betalingen laten doen door een PSP is volgens Julian dus niet alleen veilig, het scheelt volgens hem ook veel tijd en geld om dit te laten doen door een organisatie die onder toezicht staat van de Nederlandsche Bank.[1] Volgens sommige managers is een bijkomend voordeel van PSP's dat zij op die manier minder klantgegevens krijgen van de klant. Want minder klantgegevens betekent ook dat er minder cybersecurity nodig is om deze gegevens te beschermen. Leon vertelt:

> "Wij behandelen niet de betaalgegevens…Wij verwijzen mensen ook gewoon door. Wij hoeven daar ook niet te zijn. Wij krijgen alleen maar een seintje terug als de betaling voltooid is. Wij zien ook maar vier cijfers van een creditcard. Je ziet een bankrekeningnummer, maar daar kun je natuurlijk verder ook niks mee. We proberen ook altijd duidelijk te maken aan de klant, dat wij hun gegevens niet bewaren of nodig hebben."

Het niet hebben van de volledige betaalgegevens van klanten, lijkt Leon het gevoel te geven dat hij zich over de beveiliging van dit onderdeel minder zorgen hoeft te maken.

3. Keurmerken: een "prettig gevoel"

Tot slot kwam naar voren dat veel webshopmanagers waarde hechten aan een keurmerk. Zoals in paragraaf 4.2.3 naar voren kwam, kijken de webshopmanagers hier ook naar als zij zelf online willen shoppen. Het is dan ook opvallend dat niet iedereen voor zijn bedrijf gebruik lijkt te maken van een keurmerk. Hoewel in tabel 3 te zien is dat drie van de vijftien webshops zichtbaar een keurmerk hebben, weet ik dat drie andere webshops hier nog mee bezig zijn. Waaronder de webshops van de twee managers met de meeste kennis: Kay en Julian. Hier merkte ik dat mijn observatie beïnvloed werd door de gesprekken met de webshopmanagers. Het is opvallend dat de website van de webshop met de IT-webshopmanager niet het betrouwbaarst lijkt door het nog te missen keurmerk-logo.

[1] https://www.dnb.nl/en/supervision/consumer-and-supervision/registers/WFTBI/

Webshopmanagers	A	B	C	D	E	F	G	H	I	**J***	K	L	M	N	O
Trust-building platforms															
Keurmerk					X			X		/	/	X			/

Tabel 3 *IT-manager

Thuiswinkel is onder de managers het meest bekende keurmerk. Harm geeft aan dat hij zijn winkel cyberveilig acht door te voldoen aan hun eisen. Hij heeft daardoor het gevoel dat zijn website op het gebied van veiligheid altijd up-to-date is:

> "Je ziet steeds meer van die DDoS aanvallen en dat soort dingen. Maar ja, op zich, wij hebben dus zo'n Thuiswinkel waarborg en dan moet je aan een aantal veiligheidsvoorwaarden voldoen als webshop. En dan wordt dat getest en in principe ja, dus wat dat betreft hebben wij wel een veilige webshop … En ik vind het ook wel prettig om zo'n logo te hebben zodat je weet dat je altijd up-to-date bent met veiligheid. Dat vind ik een prettig gevoel en dat vind ik ook belangrijk."

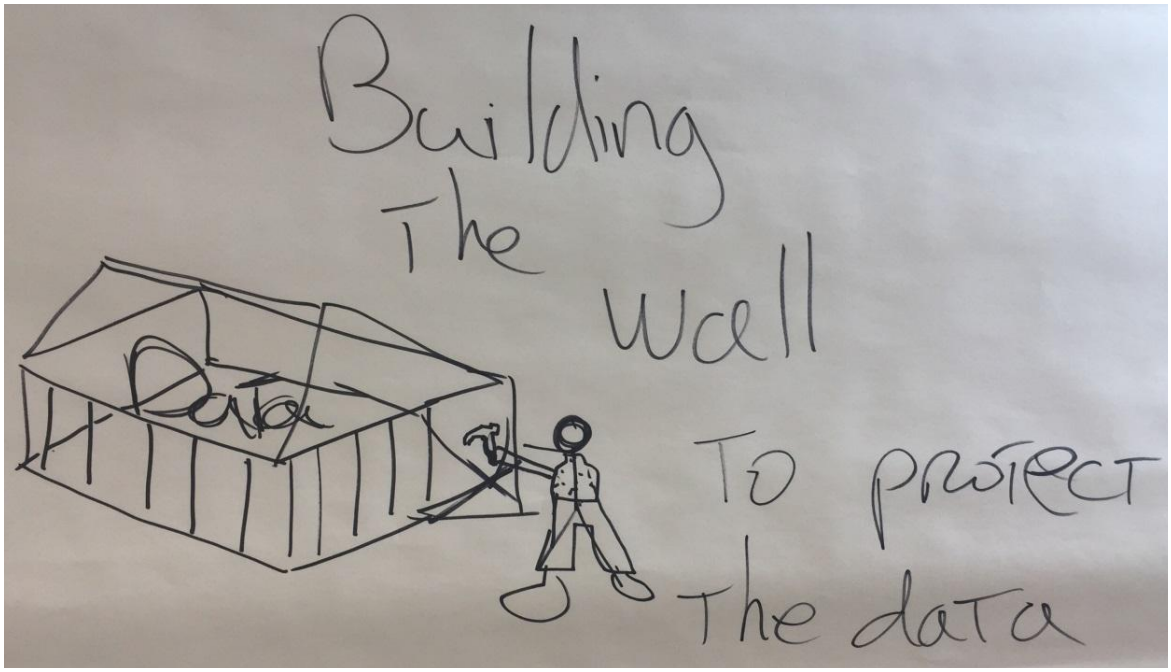
Het hebben van een keurmerk verlicht Harm van het omkijken naar cybersecurity, want de technische experts zorgen ervoor dat de website aan de eisen voldoet en: "Nou, ja als zij dit goed geregeld hebben, dan hoeven wij niet meer zoveel te doen." Leon bevestigt het beeld van Harm en benoemt vooral de *vulnerability* test van Thuiswinkel als punt voor gedegen cybersecuritybeleid:

> "Die scan geeft altijd aan dat wij geen zwakheden hebben. Dus dat is in principe ook prima. Daar is trouwens nog nooit iets aan het licht gekomen. Van die scan hè, dat we kwetsbaarheden hadden. Zolang we dat niet hebben, dan geloof ik gewoon dat het allemaal goed is."

Het vertrouwen in deze test lijkt er ook voor te zorgen dat Leon vertrouwen heeft in het platform waar zijn bedrijf zit: "Klantgegevens worden beveiligd door Magento. Daar hou ik mij helemaal buiten. Wij doen geen extra beveiliging daarop." Zolang de scan van Thuiswinkel goed is, heeft Leon vertrouwen in zijn cybersecuritybeleid. Het vertrouwen in Thuiswinkel is groot en geeft deze webshopmanagers het gevoel dat het cybersecuritybeleid in goede handen is, waardoor zij zich kunnen richten op andere taken. De organisatie van de IT-manager is op dit moment bezig met de aanmelding bij Thuiswinkel. Hij geeft echter aan dat zij het waarborg logo niet willen om te controleren of ze veilig genoeg zijn:

> "Je kan sowieso het een en ander aan de infrastructuur zelf regelen. Dus al je verbindingen over SSL, zodat je ook met dat slotje linksboven in beeld hebt. Dat kan je gewoon afdwingen, dat je geen verkeer hebt als het niet https is. Dat moet je softwarematig zelf regelen. Moet je ook als je geen Thuiswinkel hebt." Volgens Julian is Thuiswinkel dan ook: "meer dan alleen maar beveiliging. Algemene voorwaarden hebben we nu bewust niet. Vonden we wel duidelijk en leuk…Daar zagen we het nut niet van in. Maar nu moeten we de algemene voorwaarden van Thuiswinkel Waarborg erop zetten. Nou ja, daar gaan we dan natuurlijk eerst goed naar kijken, maar op zich is Thuiswinkel gemaakt om de consument te beschermen en dat deden we sowieso al. Dus dat we dat nu op papier zetten."

Het hebben van een Thuiswinkel Waarborg logo op de website dient in dit geval vooral als teken van vertrouwen naar de klant toe. Hoewel Julian vertrouwen heeft in Thuiswinkel, ziet hij zichzelf als de persoon die beoordeelt of het beleid veilig genoeg is. Dit zie je ook terug in zijn illustratie:



Tekening van Julian (IT-webshopmanager)

4.5 De grens in zicht

Paragraaf 4.4 laat zien dat de webshopmanagers vertrouwen op experts voor hun cybersecuritybeleid. De webshop-analyse laat zien dat merendeel van de webshops zelf ook zichtbaar gebruik maakt van factoren die volgens henzelf staan voor een betrouwbare webshop. Wat ik niet zie op de websites van de webshops is een uitleg met wat zij allemaal precies doen om online veiligheid te garanderen. Hierdoor weet ik niet wie welke gegevens van mij krijgt, waar deze worden opgeslagen en wat de mogelijke risico's zijn van het beleid dat de organisaties op dit moment handhaven. Ook geven de websites geen inzicht in het cybersecuritybeleid op de werkvloer. Dit laatste is er ook niet. In deze paragraaf lichten de webshopmanagers kort toe waarom zij tevreden zijn over hun huidige cybersecuritybeleid en dat meer of andere beveiliging volgens hen op dit moment niet nodig is.

Tevreden over cybersecurityniveau

Dat de webshopmanagers voldoende vertrouwen hebben in het huidige cybersecuritybeleid kwam naar voren als het gesprek ging over de kosten van cybersecurity en de mogelijkheid om het anders te doen als geld geen probleem zou zijn. Eigenlijk gaf bijna iedere webshopmanager aan dat zij tevreden zijn over het huidige cybersecuritybeleid. Kay geeft aan dat het wel beter kan door proactief scans te doen of delen te automatiseren, maar zegt ook direct dat ze dit niet gaan doen. Vanwege het gebrek aan kennis en budget, maar vooral omdat hij ervan overtuigd is dat zij op dit moment voldoende doen aan cybersecurity. Zo vertelt hij:

> "maar ja, in ons MKB-bedrijf is dat eigenlijk niet te doen. Want je hebt én het budget er niet voor en ook niet de kennis." Toch vindt hij dat de organisatie voor nu voldoende doet: "We zijn ons echt wel bewust van de potentiële problemen. We zijn ons ook bewust dat het heel erg lastig is voor ons om daar het maximale aan te doen. Maar ik denk, zolang wij samenwerken met grote, goede partners, dat wij zelf als bedrijf al een heel eind geholpen zijn. Dat wij ook zelf zouden willen dat er zo omgegaan wordt door andere partijen waar we onze data achterlaten."

Leon geeft ook aan niks anders te doen als er meer geld beschikbaar zou zijn.

"Nee, wij hebben de duurst mogelijke SSL-certificaat. Helemaal met zo'n balkje. Zo'n hele balk, weet je wel. Net zoals de bank heeft met zo'n slotje erop. Onze hele website is ook 'https', ondanks dat dát wel wat meer surfkracht vereist. Dat hebben we bewust gedaan, omdat je dan overal dat groene balkje ziet."

Zijn prioriteit was dus om binnen het cybersecuritybudget meer geld vrij te maken voor de duurste SSL-certificaat en dat heeft hij gedaan.

Meer cybersecurity is niet nodig

Net als in hun persoonlijke omgang met fysieke veiligheid vinden de webshopmanagers dat er grenzen zitten aan de online beveiliging. Het hebben van een webshop brengt risico's met zich mee. "Het is een wereld van de cowboys en je moet jezelf daarin staande zien te houden", zegt Gill. De webshopmanagers nemen voornamelijk preventieve maatregelen op technisch vlak en hebben minimale maatregelen op de werkvloer. De maatregelen die webshopmanagers hebben gaan voornamelijk over vertellen aan medewerkers dat ze niet op een verkeerd linkje moeten klikken en dat ze goede wachtwoorden moeten gebruiken. Leon en Ian lichten dit toe:

Leon: "Ik probeer wel iedereen hier duidelijk te maken, dat ze niet op bijlages mogen klikken, die of .zip zijn of andere rare extensies hebben, waarvan we de afzender ook niet kennen."

Ian: "Wat we wel doen is service goed beveiligen, goede VPN-verbinding, zorgen dat mensen goede wachtwoorden gebruiken. Dat je ook snapt waarom je iets gebruikt. Mensen ervan doordringen dat het slim is om niet weer [Ian]2017 te gebruiken, maar dat het wel wat complexer mag en dat er manieren zijn om dat te kunnen doen, zonder dat je dat op een briefje moet schrijven en in je portemonnee moet plakken."

Het viel mij op dat weinig webshopmanagers iets vertelden over preventief cybersecuritybeleid op de werkvloer. Voor Anna heeft dit ook te maken met vertrouwen hebben in medewerkers. Zo vertelt Anna: "Je wil ook vertrouwen hebben in de mensen waarmee je werkt…Je wil ook je stagiaires het vertrouwen geven." Ze geeft hiermee aan dat ze het vertrouwen wil hebben en heeft het vertrouwen, tot dat bewezen wordt dat dit vertrouwen onterecht is. Op een enkele organisatie na, gaat het beleid niet verder dan webshopmanagers wijzen op het gevaar van phishing mails. Noah illustreert aan de hand van een metafoor dat online ondernemen volgens hem nu eenmaal risico's met zich mee brengt en dat te veel beveiliging verstikkend kan werken:

"Gaan we dan niet het bos in? Ga je het dan beperken om 'wat'? Nee… Je schat dan je risico's in. Je gaat niet overal die beren zoeken. Dat is gewoon zo. Je moet gewoon lopen en op een gegeven moment heb je gewoon een pad … Er komt helemaal geen beer, weet je wel. Heel vaak zijn er helemaal geen beren. Dat weet je niet, maar die zijn er gewoon niet. En dan schat je gewoon in … Als je die beren tegenkomt, dan ben je ervoor gewapend."

Noah geeft aan dat je niet op zoek moet gaan naar iets wat er niet is. De beren zijn cybercriminelen en de cybercriminelen zijn er vaak niet. Maar hij geeft wel aan dat je gewapend moet zijn voor als er een hacker op je pad komt. Op de vraag welke wapens zegt hij:

"Je hebt wat wapens bij je, weet je wel. Je luistert en je zorgt dat het eten allemaal netjes op hoogte is en dat hij niet bij je tentje komt. Daar zorg je allemaal voor. Maar als inderdaad toevallig net bij die beer komt en hij heeft net een paar kleine beertjes bij zich … Hij voelt zich bedreigt en hij valt je aan … Je kunt alles dichtkitten, maar dan onderneem je niets. Dan zit je in dat hutje en die beer komt er echt niet in. Helemaal veilig. Maar je vergaat van de honger, want je hebt niets te eten."

Volgens Noah is het verstandig om je zo te beveiligen dat je wel nog vrij kan bewegen. Te veel beveiliging zorgt er volgens hem voor dat je veilig bent, maar ook dat je zelf geen kant meer op kan. Hij onderstreept het algemene punt dat al in de bevindingen naar voren is gekomen, namelijk dat ze zichzelf voldoende beschermen, maar niet tot het allerhoogste niveau, omdat zij dit niet nodig achten.

4.6 Tot slot

In dit hoofdstuk besprak ik mijn onderzoeksbevindingen door aan de hand van mijn interpretaties achteraf de webshopmanagers zelf aan het woord te laten en hun ervaringen over cybercrime te laten vertellen. Als eerste vertelden zij in paragraaf 4.1 in een context hoofdstuk wat hun taken zijn en gaven zij kort weer welke betekenis zij geven aan het risico op cybercrime. Daarna vertelden de webshopmanagers in paragraaf 4.2 hoe zij omgaan met hun veiligheid. In paragraaf 4.3 gingen de webshopmanagers dieper in op hun ervaringen met cybercrime. Vervolgens gaat paragraaf 4.4 over de wijze waarop de webshopmanagers hun cybersecuritybeleid inrichten, waarbij de focus ligt op het uitbesteden aan experts. Tot slot gingen zij nog kort in op hoe zij hun eigen cybersecuritybeleid interpreteren. In het volgende hoofdstuk analyseer ik mijn bevindingen door deze te duiden aan de hand van de theoretische concepten die ik in hoofdstuk 2 heb besproken.

5. Analyse

In dit hoofdstuk analyseer ik de bevindingen uit hoofdstuk 4. Dit doe ik aan de hand van drie onderdelen. Ten eerste ga ik in paragraaf 5.1 in op de betekenissen die de webshopmanagers zelf geven aan ervaringen die zij hebben *cybercrime, cybersecurity* en nieuwsberichten over cybercrime. De onzichtbare rol van het internet zit verweven door de hele analyse, maar krijgt in paragraaf 5.2 een hoofdrol als ik de relatie tussen de webshopmanager en de klant analyseer. Tot slot gaat paragraaf 5.3 over de relatie tussen de webshopmanager en de expert.

5.1 Betekenisgeving

Weick en Sutcliffe (2005) betogen dat het proces van betekenisgeving langs zeven wegen gaat. Dit proces zie je in de analyse terug. Ik weergeef hier nog even kort het proces. Als eerst signaleren de webshopmanagers een situatie en gaan na "wat is hier aan de hand?" Vervolgens gaan ze in alle informatie die ze over deze situatie binnenkrijgen selecteren, labelen en categoriseren. Ten derde vergelijken de webshopmanagers de situatie in retroperspectief. Ook koppelen ze abstracte vermoedens over de situatie aan concrete ervaringen. Ten vijfde geven de managers betekenis aan een bepaalde situatie door communicatie met andere mensen. Het zesde kenmerk is de actie die voortkomt uit de eerdere betekenisgeving, op dat moment hun werkelijkheid, die zij aan de situatie hebben gegeven. Tot slot is betekenisgeving een proces dat continu in ontwikkeling is en krijgt een situatie in een organisaties door communicatie een collectieve betekenis (pp. 409-413). Waarbij het laatste punt in dit onderzoek zal gaan over de collectieve betekenis van webshopmanagers. Onderdelen van dit proces zijn terug te zien in drie verschillende situaties waar de webshopmanagers betekenis aan geven. In paragraaf 5.1.1 analyseer ik de betekenis die managers geven aan cybercrime. In paragraaf 5.1.2 analyseer ik de betekenis die webshopmanagers geven aan cybersecurity. De laatste situatie analyseer ik in paragraaf 5.1.3 en gaat over de betekenis die webshopmanagers aan nieuwsberichten geven.

5.1.1 Cybercrime - Wij zijn geen slachtoffer

Bij de webshopmanagers is er als het ware sprake van gebrek aan negatieve persoonlijke ervaring met cybercrime. De collectieve betekenis die zij geven aan de ervaring met zwakke vormen van cybercrime of cybercrime die niet leidt tot fysieke of ernstige financiële schade, is dat zij zichzelf dan niet zien als slachtoffer van cybercrime. Zwakke vormen van cybercrime, zoals spam, zijn normaal, want die "krijgt iedereen" en ook het ontvangen van phishing-mails lijkt steeds normaler te worden. Het lijkt erop dat de betekenis die zij geven aan cybercrime afhangt van de schade die de webshopmanagers zelf ervaren. De meeste webshopmanagers voelen zich tot op heden nog niet fysiek of financieel benadeeld door cybercrime. Zo stelt Ian dat als hij op dit moment is gehackt, de gevolgen tot op heden niet groot zijn. Mochten er zonder zijn weten foto's van zijn dochtertje gestolen zijn en beland in een pedofielen netwerk, dan ondervindt zij hier volgens hem fysiek geen hinder aan. Dus ervaart hij geen probleem. Het is dan enkel "ethisch onverantwoord", maar daar maakt hij zich geen zorgen over, want "over een jaar ziet zij er alweer anders uit." De webshopmanagers die te maken hebben gehad met andere vormen van cybercrime, ervaren vaak geen schadelijke of onoverkomelijke gevolgen. Zo kon een manager gemakkelijk zijn creditcard blokkeren nadat er tien euro was afschreven en werd een andere manager gebeld door Microsoft

toen zijn mailaccount was gehackt. Anders dan eerder onderzoek van Riek et al. (2014) uitwees, ervaren de webshop-managers geen hinder aan zwakkere vormen van cybercrime. Zij zien zichzelf dan ook niet als slachtoffer van cybercrime. De webshopmanagers lijken binnen het slachtofferschap van cybercrime selectief te zijn in wanneer zij zichzelf ook daadwerkelijk als slachtoffer zien. Hierdoor ontbreekt het – volgens de theorie – belangrijkste element voor gedragsverandering, namelijk: slachtoffer-ervaring (Riek et al., 2014, p. 8). De wereld van cybercrime en het gevoel gehackt te kunnen worden is in feite een ver-van-hun-bed-show.

5.1.2 Cybersecuritybeleid - Wij denken logisch na

In de gesprekken met de webshopmanagers kwam naar voren dat zij op basis van zichtbare aanwijzingen en ervaringen beslissen hoe zij omgaan met het risico op cybercrime. Deze twee kenmerken vormen samen de intuïtieve *expected value*. Een tegenhanger van de rationele expected value, waarbij men de verwachte waarde van gevaar berekent door de waarde van de omvang (aantal doden, financiële verliezen etc.) te vermenigvuldigen met de kans dat het daadwerkelijk gebeurt (Stone, 2012, p. 131). In deze paragraaf laat ik zien dat het risico op cybercrime rationeel *geframed* wordt door webshopmanagers, terwijl hun onderbouwing juist aansluit bij de intuïtieve benadering.

“Logisch nadenken”

De webshopmanagers suggereren in de gesprekken dat jezelf weren tegen cybercrime voornamelijk een kwestie is van logisch nadenken. Als het om mailberichten gaat kijken zij bijvoorbeeld naar zowel de opmaak als de inhoud van de mail. De webshopmanagers hebben in feite een aantal intuïtieve stappen van ‘logisch nadenken’ te hebben, zoals:

1. Heeft de website een SSL-certificaat?
2. Ziet de inhoud en het design van de mail er betrouwbaar uit?
3. Werkt een webshop samen met *trust-building platforms*?

Als de antwoorden hierop ‘ja’ zijn, dan ‘tellen’ ze deze als het ware op bij hun ervaringen. Een positieve uitkomst lijkt te beteken dat zij dit als teken van een webshop veilig zien. Kijkend naar het *sensemaking* proces, ontstaat hier de indruk dat zij abstracte vermoedens over het kunnen vertrouwen van een website, koppelen aan de concrete ervaring dat het tot op heden goed gaat. En dat zij op basis hiervan het risico op cybercrime goed kunnen inschatten. Daarbij bekijken ze ook de situatie in retroperspectief en krijgen daardoor het gevoel dat er een positief patroon te zien is waar zij op kunnen vertrouwen. De webshopmanagers gebruiken hun persoonlijke ervaringen als basis voor het begrijpen van cybercrime en wat ze moeten doen om dit te voorkomen. Dit kan gezien worden als een eerste aanwijzing voor het intuïtief benaderen van het risico op cybercrime. Alle feiten en cijfers over het mkb waar de manager niks van heeft gemerkt en ingrijpende voorspellingen over de toekomst tellen niet zo zwaar als dat wat zij zelf ervaren. Hun eigen ervaringen zijn de (onvolledige) feiten die de doorslag geven. Dat wat ze zien is alles wat er is, want “Informatie die niet uit het geheugen wordt opgehaald, kan net zo goed niet bestaan.” (Kahneman, 2013, p. 93).

5.1.3 Nieuwsberichten - Wij worden niet gezien

Boothby, Clark en Bargh (2016) spreken van een *invisibility cloak illusion*. Hierbij stellen zij ten eerste dat mensen denken dat zij zelf zeer goed sociaal kunnen waarnemen en dit beter kunnen dan andere mensen. Ten tweede geloven mensen dat zij zelf minder geobserveerd worden dan anderen. Dit heeft als gevolg dat mensen geloven dat zij andere mensen meer observeren in de sociale omgeving dan anderen hen observeren (Boothby, Clark & Bargh, 2016, p. 1). De verhalen van de webshopmanagers vertonen gelijkenissen met de invisibility cloak illusion. Alleen dan online. Ik betoog hier dan ook dat er een online variant is en er bij de webshopmanagers sprake is van een *online invisibility cloak illusion*. De hoofdrolspelers zijn in de online wereld anders dan in de sociale wereld. Het gaat hier om de webshopmanagers in het mkb en cybercriminelen. In het kort uit de online invisibility cloak illusion zich als volgt: Ten eerste observeren webshopmanagers nieuwsberichten en zien hier dat grote organisaties, staten en ziekenhuizen het doelwit zijn van cybercrime. Dit is voor webshopmanagers het bewijs dat grote organisaties in het vizier van cybercriminelen zijn. Ten tweede geloven de webshopmanagers dat hun eigen mkb-webshops online minder geobserveerd worden door cybercriminelen dan dat cybercriminelen grote organisaties observeren. Deze twee punten maakt dat de webshopmanagers geloven dat cybercriminelen grote organisaties meer observeren dan het mkb. Hieronder licht ik de drie kenmerken nog kort toe.

Het eerste kenmerk is dat de webshopmanagers aangeven dat ze voornamelijk via het nieuws in aanraking komen met cybercrime. Hier zien zij dat het hoofdzakelijk grote organisaties zijn die slachtoffer worden van (schadelijke) cybercrime. Dit is voor de webshopmanagers het bewijs dat dat voornamelijk grote organisaties geobserveerd worden door cybercriminelen. Het tweede kenmerk is dat de meeste managers hierdoor het idee krijgen dat vooral grote organisaties gehackt worden en dat er bij hun eigen organisatie niks te halen valt. Hier zie je het onderdeel van betekenisgeving over selecteren, labelen en categoriseren in terug. Ze lijken deze abstracte vermoedens over de situatie te koppelen aan concrete ervaringen. Paragraaf 5.1.1 laat zien dat de meeste webshopmanagers geen of weinig ervaring hebben met cybercrime en zich hier tot op heden geen slachtoffer van voelen. Het niet ervaren van cybercrime zien zij als een goed teken (en een bevestiging). De managers gaan er vanuit dat als zij niks merken de organisatie geen slachtoffer is van cybercrime. Hier zie je de omkeerfout van Taleb (2008) in terug: “Het ontbreken van bewijzen bewijst niet dat iets volledig ontbreekt.” Daarnaast laat bovenstaande zien dat de managers op basis van de informatie die ze hebben ervaringen koppelen, omtoveren tot een consistent verhaal en dit verhaal valide achten (Kahneman, 2013, p. 79). Uit de gesprekken met de webshopmanagers kwam vrijwel iedere keer dezelfde redenatie terug:

Media corresponderen over cybercrime.
Het mkb komt hier niet in voor.
Het mkb is dus minder vatbaar voor cybercrime.

Bovenstaande twee kenmerken vormen samen het derde kenmerk en dat is dat de webshopmanagers geloven dat cybercriminelen grote organisaties meer observeren dan het mkb.

Het gegeven feit dat cybercrime geheel onzichtbaar kan plaatsvinden, wordt niet meegenomen. Alleen de zichtbare ervaring geldt en grote webshops worden vaker zichtbaar gehackt. Dit zorgt voor het *halo-effect*, waardoor de webshopmanagers vooringenomen zijn over cybercrime. Hun beeld lijkt daardoor eenvoudiger en samenhangender dan dat de werkelijkheid is. Hierdoor is het mogelijk dat de managers dit onterecht opvatten als een systematische gebeurtenis. Zij geven betekenis aan de situatie door de ervaringen die ze hebben aan elkaar te koppelen en bouwen zo hun "persoonlijke belevingswereld op" over cybercrime. Dit kan, zoals Kahneman (2013) aangeeft, leiden tot een (onterecht) causaal verband waarbij zij geen cybercrime ervaren en daardoor het gevoel hebben dat zij niet worden gehackt in tegenstelling tot andere – grotere – organisaties (p. 79) .

De als klein ingeschatte kans om slachtoffer te kunnen worden, weerhoudt de webshopmanagers ervan om meer te leren over of cybercrime of meer maatregelen te nemen dan zij nu doen. Zij kiezen er bewust voor om niet meer kennis te genereren vooraf, maar preventief te leren achteraf. Het lijkt erop dat de webshopmanagers deze keuze rechtvaardigen aan de hand van het geloof dat criminelen – zowel fysiek als online – als ze willen, toch wel slagen. De webshopmanagers lichtte dit vaak toe door een parallel te trekken met de kans op een terroristische aanslag. Iemand die zichzelf wil opblazen in een drukke menigte doet dit toch wel. Hetzelfde geldt voor iemand die graag wil hacken. De managers reageren hier gelaten op. Ze spraken hier rustig over en kwamen niet gefrustreerd over dat ze dit niet kunnen voorkomen. Het lijkt een ontembaar probleem waar je nooit genoeg aan kan doen. Dat ze dit zo ervaren is ook sterk persoonsgebonden, omdat zij aangeven dat veiligheid sowieso een thema is waar zij zich liever niet mee bezig houden. Stone (2013) stelt dat mensen veiligheid creëren als ze zich zorgen maken over toekomstige gebeurtenissen die onveilig zijn (p. 130). Het lijkt erop dat de webshopmanagers zich geen zorgen maken over een mogelijke cybercrime aanval. Door voornamelijk technische cybersecurity maatregelen te nemen, voelen zij zich al veilig genoeg.

5.2 Het comfort van onzichtbaarheid

Bowen (2000) stelt dat organisaties vandaag de dag zichtbaarder zijn vanwege het internet en geeft aan dat dit een probleem met zich meebrengt voor organisaties. De onzichtbaarheid van het internet maakt het echter juist minder noodzakelijk voor de webshopmanagers om zichtbaar te maken aan klanten wat ze precies doen aan cybersecurity. In paragraaf 5.2.1 ga ik in op de relatie tussen het zichtbaarheidsprobleem van bedrijven en de onzichtbaarheid van het internet en cybersecurity. Vervolgens ga ik in paragraaf 5.2.2 in op hoe webshopmanagers hun cybersecuritybeleid alsnog zichtbaar proberen te maken .

5.2.1 Hoe onzichtbaarheid het zichtbaarheidsprobleem verlicht

Bowen (2000) gaf aan dat zichtbaarheid gezien kan worden als probleem voor organisaties (p. 93). Dit komt omdat onethisch handelen en risicovolle praktijken sneller aan het licht komen door mediaberichten (Zyglidopoulos & Fleming, 2011, p. 692). Door het internet is een probleem op dit gebied dan direct zichtbaar voor stakeholders en organisaties kunnen zich daardoor onder druk gezet voelen om te reageren op sociale of politieke vraagstukken. Om reputatieschade te voorkomen, zijn bedrijven sneller geneigd een zichtbaar probleem aan te pakken (Bowen., 2000, p.

94). Dit onderzoek laat zien dat merendeel van de webshopmanagers het gevoel heeft ethisch te handelen en weinig risico te nemen op het gebied van cybersecurity, omdat zij voldoen aan zichtbare vertrouwensfactoren, zoals bijvoorbeeld SSL-certificaten en het hebben van een keurmerk. De onzichtbaarheid van het internet maakt dat (de meeste) klanten niet kunnen controleren of er daadwerkelijk voldoende cybersecurity is. Daarnaast gaan klanten volgens Etzioni (2017) zelf ook af op zichtbare vertrouwensfactoren, waardoor de controle nooit verder lijkt te gaan dan dat wat al zichtbaar is. Zo verlicht de onzichtbaarheid van het internet het zichtbaarheids-probleem van webshopmanagers. Er kan onzichtbaar van alles mis zijn, maar de klantbeoordeling lijkt niet verder te gaan dan dat wat mensen zien. De meeste webshopmanagers geven aan weinig met cybersecurity te hebben en zijn ervan overtuigt dat een kwaadwillende toch wel binnen kan komen als hij dit wil. Toch moeten ze iets met de complexe materie en kunnen nu met behulp van experts redelijk eenvoudig zichtbaar het cybersecuritybeleid naar een bepaald niveau brengen.

De onzichtbaarheid van het internet geeft de webshopmanagers zo in zekere zin een comfortabele positie, omdat alleen zichtbare cybersecurity belangrijk lijkt te zijn voor klanten. Afgaand op het privacy-onderzoek van Martijn en Tokmetzis (2016) lijkt het er ook op dat klanten niet snel op zoek zullen gaan naar mogelijk risicovolle praktijken en onethisch handelen van webshops. Zij geven namelijk aan dat mensen vrij weinig doen aan hun privacy en stellen dat er sprake is van een privacyparadox: Mensen hebben wel de neiging om privacy belangrijk te vinden, maar handelen er niet of nauwelijks naar (p. 37). Bij zichtbare organisatieproblemen, zoals de slechte moderne slavernij in textielfabrieken, komen er veel mensen in opstand om hier tegen te strijden als dit in het nieuws komt. Bijvoorbeeld door een *boycot*. Los van de daadwerkelijke uitkomst worden organisaties – van mkb tot grote *corporates* – van tijd tot tijd regelmatig gedwongen om zich weer (even) met een bepaald onderwerp bezig te houden en hier iets mee te doen. Terwijl dit bij nieuwsberichten over cybercrime niet gebeurt. Het lijkt er daarom op dat de webshops zich voor de samenleving alleen hoeven te houden aan zichtbare veiligheidskenmerken, terwijl deze niet per se staan voor goed cybersecuritybeleid.

De betekenissen die webshopmanagers geven aan ervaringen met verschillende situaties, zoals uitgelegd in paragraaf 5.1 en de comfortabele positie vanwege het onzichtbare internet, lijken beide het gevoel te geven dat hetgeen wat zij nu doen voldoet aan goed cybersecuritybeleid. Ook al kunnen de meeste webshopmanagers dit zelf niet beoordelen. Hier ga ik uitgebreider op in, in paragraaf 5.3, maar eerst ga ik dieper in op hoe de webshopmanagers zichtbaar willen maken dat zij voldoende cybersecuritybeleid hebben.

5.2.2 Cybersecuritybeleid zichtbaar maken

Paragraaf 5.1 laat zien dat onzichtbaarheid een grote rol speelt in hoe webshopmanagers betekenis geven aan het risico op cybercrime. Zo ervaren zij geen (schadelijke) cybercrime en hebben daardoor het gevoel dat zij niet gehackt worden. Daarnaast worden zij in nieuwsberichten geconfronteerd met cybercrime in grote organisaties, waardoor cybercrime in het mkb onzichtbaar is. Webshopmanagers hebben daarom het gevoel dat hun type organisatie niet gevoelig is voor cybercrime, omdat daar "niets" te halen valt. Ook gaan ze er allemaal vanuit dat als een

cybercrimineel wil inbreken, dit toch wel lukt. Toch zijn er voor de webshopmanagers wel "logische" kenmerken die staan voor een betrouwbare, veilige website.

Etzioni (2017) heeft met zijn theorie gekeken naar het online vertrouwen van de consument. Uit zijn onderzoek blijkt dat online vertrouwen op drie manieren terrein wint, namelijk via het design van de website, recensies en trust-building platforms (Etzioni, 2017, pp. 3-8). Ik noemde dit (al eerder) de online vertrouwensfactoren. Uit de gesprekken met de webshopmanagers blijkt dat twee van de drie online vertrouwensfactoren een grote rol spelen in de manier waarop webshopmanagers professioneel de website beoordelen. Ten eerste het design van de website en ten tweede via trust-building platforms. De standaard die de webshopmanagers als consument aanhouden, vertalen zij namelijk ook door naar hun eigen website. De website moet er goed uitzien en ze werken samen met diverse *trust-building platforms*. Deze als betrouwbare gepercipieerde organisaties zorgen voor cybersecurity of controleren de cybersecurity. Zo vertrouwen zij erop dat een *Payment Service Provider* de financiële beveiliging volledig overneemt en gaat een meerderheid er vanuit dat een partij als Thuiswinkel Waarborg aan de bel trekt als hun cybersecurity niet in orde is. Bijvoorbeeld aan de hand van een *vulnerability scan*. Komt de website goed uit de test, dan is het beleid volgens veel webshopmanagers in orde. Hier is de omkeerfout van Taleb (2008) weer te zien. Het feit dat de scan geen specifieke problemen vindt, bewijst nog niet dat er algemene cyberveiligheid is. Daarnaast valt het op dat de vertrouwensfactoren in het geval van de webshopmanagers niet enkel gelden in het privédomein, maar ook gebruikt worden op professioneel vlak. De webshopmanagers zien deze zichtbare vertrouwensfactoren ook als dé kenmerken waarop zij kunnen controleren of een website veilig is, ook al geeft het merendeel aan geen kennis te hebben van het onderwerp. De huidige ervaringen lijken een bewijs voor de managers dat het huidige cybersecuritybeleid volstaat omdat er geen merkbare problemen zijn. Paragraaf 5.2.1 laat zien dat de onzichtbaarheid van het internet het ook mogelijk maakt voor de webshopmanagers om zich enkel te focussen op zichtbare vertrouwensfactoren, omdat er geen klanten weglopen vanwege mogelijk onzichtbare problemen. De webshopmanagers hebben het gevoel dat het huidige cybersecuritybeleid voldoende is en zij zich daarom ook niet meer hoeven te verdiepen in de materie dan zij nu doen. Dit omdat vrijwel alle webshopmanagers de verantwoordelijkheid voor het cyberveilig maken van de website *outsourcen* naar experts.

5.3 Blind vertrouwen

Vrijwel alle webshopmanagers zetten het cybersecuritybeleid uit bij experts. Opvallend genoeg, ongeacht hun kennisniveau. Dit zijn mensen die er in de ogen van de webshopmanager verstand van hebben en dit volgens hen ook leuk vinden om te doen. De webshopmanagers onderscheiden drie type experts: 1. Technische experts 2. Payment Service Providers en 3. Keurmerken. De webshopmanagers dragen de verantwoordelijkheid aan hen over. De IT-webshopmanager spreekt in dit geval over het verschuiven van verantwoordelijkheden. Iets wat de meeste webshopmanagers een prettige gedachte vinden, omdat ze doorgaans geen affiniteit hebben met het onderwerp en daarom liever andere dingen doen. Dit bevalt tot op heden goed. Ze ervaren namelijk geen (schade van) cybercrime en geven hier een concrete betekenis aan. De webshopmanagers hebben door het gebrek aan ervaring namelijk het gevoel dat zij de experts die aan hun website werken of de website beheren, erop kunnen vertrouwen dat zij hun werk goed

doen. En als er sprake is van een zichtbaar lek, dan lossen de experts dit "snel" op. De webshopmanagers lijken daardoor niet kritisch te zijn op de experts. Als er geen zichtbare cybercrime plaatsvindt doen ze hun werk goed en als cybercrime wel zichtbaar plaatsvindt lossen zij dit goed op. Dat dit in werkelijkheid heel anders kan uitpakken, werd recent uitgelicht door het Financieele dagblad, dat een artikel publiceerde over de "cowboys" op de cybersecurity-markt. Iemand die zich als expert voordoet, is niet per definitie betrouwbaar (website Financieele Dagblad, 2017). Echter, op een enkeling na vertrouwen de meeste webshopmanagers blind op het werk van de experts.

Naast het vertrouwen in de experts die volgens hen het cybersecuritybeleid uitvoeren, hebben de managers tegelijkertijd ook veel "vertrouwen" in de cybercriminelen, die je ook kan zien als experts (maar dan met kwade bedoelingen). Alle webshopmanagers zijn namelijk van mening dat als iemand echt informatie wil stelen, dit ook wel lukt. Honderd procent zekerheid is er nooit, dus geven ze aan te vertrouwen dat het goed gaat, tot het tegendeel is bewezen. Meer kennis krijgen over cybersecurity lijkt dan ook niet nodig om hun werk naar behoren te doen. Aangezien er genoeg experts zijn die graag willen beveiligen, laten zij hen de beveiliging tegen betaling regelen en hebben ze er zelf geen omkijken meer naar. De experts zorgen voor zichtbare vertrouwensfactoren en de webshopmanagers ervaren geen cybercrime. Dit geeft de webshopmanagers het gevoel te kunnen vertrouwen dat het goed gaat en hoeven zij geen tijd te steken in het begrijpen van cybersecurity.

5.3.1 Op wie vertrouwen de webshopmanagers eigenlijk?

Etzioni (2017) gaat in zijn onderzoek uit van een gelijkwaardig vertrouwenscontract tussen de klant en verkoper: als klant vertrouw je erop dat het product dat besteld is voldoet aan bepaalde kwaliteit en als verkoper vertrouw je erop dat de klant binnen een redelijke termijn betaalt. De webshopmanagers hebben het gevoel dat er sprake is van een vertrouwenscontract dat gebaseerd is op wederkerigheid. Doordat zij blind vertrouwen op de experts lijken zij op dit punt de rationele benadering van vertrouwen op experts volgen; "experts are generally right". Dit terwijl de experts niet voldoen aan de eisen die Kahneman en Klein (2009) stellen aan het type experts die je daadwerkelijk kan vertrouwen (pp. 246-252). De experts zitten namelijk niet in een regelmatige/voorspelbare omgeving en door de voortschrijdende technologie ontberen ze een lange leergeschiedenis. Daarnaast is het een noemenswaardig detail dat de experts vertrouwen hebben in de experts waarmee zij willen samenwerken. Hierdoor is het volledig vertrouwen op experts in feite meer een intuïtieve keuze die goed voelt dan een rationele overweging met bewezen resultaat.

In tegenstelling tot Etzioni, stellen McEvily et al. (2017) dat er in een zakelijke relatie altijd sprake is van een ongelijkwaardige vertrouwensband (p. 76). Dit komt vanwege de unieke doelen, voorkeuren en kwetsbaarheden van beide partijen. De uitruil van factoren die de vertrouwensband uit balans brengt noemen zij *exchange hazards* (McEvily et al., 2017, pp. 75-77). Dit onderzoek laat tenminste een exchange hazard zien, namelijk: onbalans in macht tussen de interorganisationele vertrouwensband. De webshopmanagers lijken op het gebied van kennis over cybersecurity afhankelijk te zijn van de kennis die experts hebben. Als partijen waarmee zij samenwerken niet zo

afhankelijk zijn van de webshopmanagers, dan is er geen sprake van een wederkerige vertrouwensband. McEvily et al. (2017) stellen dat bij een ongelijke machtsverhouding opportunisme een gevaarlijke rol kan spelen (p. 87). Het is bijvoorbeeld mogelijk dat Thuiswinkel opportunistisch gaat handelen, omdat zij beslissen wanneer een website cyberveilig is en de webshopmanagers mogelijk niet inhoudelijk kunnen beoordelen of al deze eisen daadwerkelijk nodig zijn. Daarnaast kan het zo zijn dat er voor de webshop geen alternatieve keurmerken zijn die dezelfde waarden hebben. En omdat uit zowel het artikel van Etzioni (2017) als de gesprekken met de webshopmanagers zelf blijkt dat zij als klant websites met een keurmerk meer vertrouwen, kan te veel afhankelijkheid leiden tot een zogenaamde *vendor lock-in*. Dit terwijl Etzioni ook opmerkt dat trust-building platforms zelf tot op heden niet gecontroleerd worden – *"who guards the guardians?* – waardoor webshopmanagers ook nergens kunnen nakijken of de platformen betrouwbaar zijn. Dit geeft hen mogelijk een slechtere positie in de vertrouwensband die de samenwerkende partijen hebben. Maar tot op heden zijn de webshopmanagers tevreden en voldoen zij aan hun wensen. Omdat de meeste managers aangeven niet bezig te willen zijn met veiligheid, ontlasten de experts de webshopmanagers ook van een taak die ze niet leuk vinden. Het gaat tot op heden niet zichtbaar mis en dat wat mis gaat hoeft niet zichtbaar te worden. Zolang de experts zichtbaar goed bezig zijn, geeft de onzichtbaarheid van het internet de expert vrij spel.

5.4. Tot slot

In dit hoofdstuk heb ik aan de hand van literatuur uit hoofdstuk 2 de belangrijkste bevindingen uit hoofdstuk 4 geanalyseerd. Deze analyse maakt het mogelijk om antwoord te geven op de hoofdvraag. In het volgende en laatste hoofdstuk geef ik onder andere antwoord op deze vraag.

6. Conclusie, discussie en aanbevelingen

In dit laatste onderzoek bespreek ik in paragraaf 6.1 de conclusie. Hierin geef ik antwoord op de hoofdvraag en vat ik de belangrijkste uitkomsten samen. Daarna ga reflecteer ik in paragraaf 6.2 op de onbewuste invloeden die ik op de bevindingen heb gehad. Tot slot geef ik in paragraaf 6.3 suggesties voor vervolgonderzoek.

6.1 Conclusie

In dit onderzoek stond de volgende hoofdvraag centraal:

Welke rol speelt de onzichtbaarheid van het internet in het vertrouwen dat webshopmanagers in de mkb-detailhandel hebben in hun risicobenadering van cybercrime?

Om deze vraag te beantwoorden heb ik 15 webshopmanagers uit de mkb-detailhandel gesproken over de betekenis die zij geven aan het risico op *cybercrime*. Hier kwamen drie kenmerken uit naar voren die de visies van de manager typeren. Ten eerste benaderen de webshopmanagers het risico op cybercrime intuïtief. Deze intuïtieve benadering hangt nauw samen met het tweede kenmerk, te weten de rol die de onzichtbaarheid van het internet speelt in de manier waarop webshopmanagers het risico op cybercrime ervaren. Ik betoog tot slot in dit onderzoek dat het gebrek aan zichtbare cybercrime ervaringen een belangrijke rol speelt in het vertrouwen dat webshopmanagers hebben in hun huidige *cybersecuritybeleid*.

Het antwoord op de hoofdvraag is dat onzichtbaarheid van cybercrime de webshopmanagers het gevoel geeft dat zijzelf of de organisatie een klein risico lopen om slachtoffer te worden van cybercrime. De webshopmanagers negeren de onzichtbaarheid van het internet grotendeels en geven hoofdzakelijk betekenis aan de zichtbare ervaringen die zij persoonlijk (zowel privé als professioneel) met cybercrime hebben of aan nieuwsberichten over cybercrime. Het gebrek aan (voelbaar schadelijke) zichtbare cybercrime op zowel persoonlijk vlak als werkgebied en het uitblijven van nieuwsberichten over cybercrime in het mkb, geven de webshopmanagers het gevoel dat zij kunnen vertrouwen op hun huidige, intuïtieve benadering van het risico op cybercrime. Waarbij zij blind vertrouwen op het (zichtbare) werk van experts die zij inhuren voor de cybersecurity van hun webshop.

Dit onderzoek geeft inzicht in hoe webshopmanagers betekenis geven aan drie situaties. Ten eerste aan de ervaring die de webshopmanagers hebben met cybercrime. Ten tweede aan de kenmerken die volgens de webshopmanagers duiden op een betrouwbare en veilige website. En ten derde aan de aan nieuwsberichten over cybercrime. De betekenissen die ze hieraan geven laten zien dat de webshopmanagers het risico op cybercrime intuïtief benaderen. Eerst gaven zij betekenis aan hun ervaringen met cybercrime. De webshop-managers positioneren zichzelf niet als slachtoffer van cybercrime en zeggen bijna allemaal geen ervaring te hebben met cybercrime. Zo krijgen zwakkere vormen van cybercrime, zoals spam, niet het label cybercrime. Webshopmanagers die wel ervaring hebben met cybercrime ervaren dit niet als (heel) schadelijk, waardoor ook zij in eerste instantie aangeven geen slachtoffer te zijn. Mogelijk onzichtbare cybercrime raakt hen net als andere vormen van misdaad nu niet fysiek of financieel, waardoor ze er geen last van ondervinden. De webshopmanagers

voelen zich dan ook over het algemeen veilig. Ten tweede vertellen de webshopmanagers dat zij denken tot op heden geen te slachtoffer zijn van cybercrime, omdat zij 'logisch' nadenken. Hierbij gaan zij af op een intuïtieve versie van de *expected value* waarbij ze voor het beoordelen van een website afgaan op zichtbare vertrouwensfactoren en in retroperspectief kijken naar de uitkomst van eerdere ervaringen hiervan. Deze intuïtieve 'berekening' laat zien dat de webshopmanagers niet de rationele expected value berekening hanteren, zoals het NCC doet. De webshopmanagers blijven voor hun oordeel dicht bij hun eigen, concrete, ervaringen en koppelen dit aan abstracte berichten over cybercrime. Dat wat ze zien is alles wat er is, want "Informatie die niet uit het geheugen wordt opgehaald, kan net zo goed niet bestaan." (Kahneman, 2013, p. 93). Tot slot geven de webshopmanagers aan dat de ervaring die zij hebben met schadelijke cybercrime, afkomstig is uit nieuwsberichten en lijkt er sprake te zijn van een *online invisibility cloak illusion*. Ten eerste observeren webshopmanagers nieuwsberichten en zien hier dat grote organisaties, staten en ziekenhuizen het doelwit zijn van cybercrime. Dit is voor webshopmanagers bewijs dat grote organisaties op het vizier van cybercriminelen staan. Ten tweede geloven de webshopmanagers dat hun eigen mkb-webshops online minder geobserveerd worden door cybercriminelen dan dat cybercriminelen grote organisaties observeren. Dit maakt dat de webshopmanagers geloven dat cybercriminelen grote organisaties meer observeren dan het mkb. Dit in combinatie met het gebrek aan eigen ervaring met cybercrime maakt dat webshopmanagers deze gebeurtenis als het ware zo labelen dat vooral grote organisaties geobserveerd worden door cybercriminelen en het mkb niet. De meeste webshopmanagers lijken het beeld over cybercrime eenvoudiger en samenhangender te maken dan het in werkelijkheid is. Kahneman (2013) noemt dit ook wel het *halo-effect* (p. 79).

De betekenissen die de webshopmanagers aan bovenstaande situaties en ervaringen geven, maken dat de webshopmanagers het gevoel hebben dat hun huidige cybersecuritybeleid in orde is. De onzichtbaarheid van het internet speelt hierin een rol omdat cybercrime hierdoor ongemerkt kan plaatsvinden. Webshopmanagers weten dit en zijn zich bewust van de complexiteit die het internet daardoor met zich meebrengt. Zo stellen zij ook dat cybercrime eigenlijk niet tegengehouden kan worden, omdat zij ervan overtuigd zijn dat cybercriminelen altijd binnen kunnen komen als zij willen. Toch vertrouwen de meeste webshopmanagers erop dat de huidige vertrouwensfactoren, zoals voldoen aan de eisen van een keurmerk en het hebben van een SSL-certificaat, de website voldoende beschermt tegen kwaadwillenden. Klanten gaan volgens Etzioni (2017) ook af op dit soort vertrouwensfactoren. Bowens (2000) legt in zijn theorie over zichtbaarheid uit dat het een probleem kan zijn voor organisaties, omdat onder andere journalisten en klanten organisaties kunnen wijzen op onethisch handelen of risicovolle praktijken. Zichtbaarheid lijkt in dit geval, het geval van het onzichtbare internet, juist verlichtend te werken voor de mate waarin de webshopmanagers zich bezig moeten houden met cybersecurity. Dit omdat bekend is dat er onzichtbaar van alles mis kan zijn, maar de klantbeoordeling gaat niet verder dan de zichtbare vertrouwensfactoren. De zichtbare vertrouwensfactoren geven de webshopmanagers zo juist een comfortabele positie en het gevoel dat dat dit dé onderdelen van voldoende cybersecuritybeleid zijn waar zij op kunnen vertrouwen.

Een ander onderdeel van het cybersecuritybeleid is de outsourcing naar experts. De webshopmanagers onderscheiden drie type experts: 1. Technische experts 2. *Payment Service Providers* en 3. Keurmerken. Tot op heden ervaren zij geen (schade van) cybercrime en geven hier de concrete betekenis aan dat ze het gevoel hebben dat de experts goed hun werk doen. De webshopmanagers lijken daardoor niet

kritisch te zijn op de experts. Als er geen zichtbare cybercrime plaatsvindt doen ze hun werk goed en als cybercrime wel zichtbaar plaatsvindt, lossen zij dit goed op. De meeste webshopmanagers vertrouwen blind op het werk van de expert. Dit kan mogelijk duiden op een onbalans in macht tussen de vertrouwensband van in dit geval de webshopmanagers en de experts. Waardoor de webshopmanagers door een kennisachterstand mogelijk afhankelijk zijn van de experts. Maar vanwege de positieve ervaringen hebben de meeste managers het gevoel dat meer leren over dit cybersecurity niet nodig is. Daarnaast willen zij dit ook niet en zijn ze tot op heden tevreden. De experts ontlasten de webshopmanagers met het cybersecurityvraagstuk en doen in de ogen van de webshopmanagers zichtbaar goed hun werk. En dat geeft de webshopmanagers een (voldoende) veilig gevoel.

6.2 Discussie

In dit onderzoek wilde ik een bijdrage leveren aan de wetenschappelijke literatuur door in te gaan op drie lacunes. Ten eerste richt de huidige (organisatie)wetenschappelijke literatuur zich op de realistische benadering van het risico op cybercrime. De positie van organisaties zelf is daarin onderbelicht. Daarom wilde ik met dit onderzoek inzicht geven in de wijze waarop webshopmanagers het risico op cybercrime benaderen. Ik heb daarin laten zien dat zij het risico op cybercrime niet rationeel, maar intuïtief benaderen. Ten tweede ging ik met dit onderzoek in op een nog onzichtbaar thema in de organisatiewetenschappelijke literatuur, namelijk: de rol die de onzichtbaarheid van het internet speelt in de beleidskeuzen van organisaties. Dit onderzoek laat zien dat ook de onzichtbaarheid van het internet een rol speelt in de intuïtieve keuzes van de webshopmanagers. Tot slot heb ik met de derde lacune inzicht willen geven in de betekenis die webshopmanagers geven aan hun vertrouwensband met de experts die het cybersecuritybeleid uitvoeren.

Kanttekeningen onderzoek

Bij mijn onderzoek zijn een aantal kanttekeningen te plaatsen. Ik licht er in dit stuk vier toe. Ten eerste heb ik op voorhand van het onderzoek duidelijke keuzes gemaakt over de context waarover ik mijn onderzoek wilde schrijven. Zo wist ik al dat ik met de webshopmanagers dat ik wilde praten over cybercrime en cybersecurity en heb ik hier voorafgaand aan de interviews veel kennis over opgenomen. Daarnaast had het Nederlands Cyber Collectief een gerichte vraag. Dit gegeven maakt dat ook de semi-gestructureerde vragenlijst afgestemd was op deze vraag en mijn kennis waardoor ik voorafgaand al richting gaf aan het gesprek. Hoewel de invulling niet volledig vast stond, betekent dit ook dat ik tijdens het onderzoek – onbewust – heb geluisterd of ik dingen hoorde die ik al verwachtte te horen. Zo heb ik het thema onzichtbaarheid niet zelf ter sprake gebracht, maar haakte ik hier wel op aan toen alle webshopmanagers in hun bewoordingen lieten doorschemeren dat het zo “abstract” of “ontastbaar” was. Hierdoor staan de bevindingen niet los van mij als onderzoeker. Dit heeft ten tweede ook effect gehad op de keuzes die ik heb gemaakt in de al bestaande literatuur om mijn bevindingen te duiden. Ook hiervoor geldt dat ik gericht op zoek ben gegaan naar literatuur die aansluit op mijn bevindingen en waarbij ik de mogelijkheid zag om wetenschappelijk iets toe te voegen. Het is een bewuste keuze geweest om mij te beperken tot de gekozen literatuur en de rest buiten beschouwing te laten. Ten derde duurde het onderzoek slechts zes maanden, waardoor ik beperkt de tijd had om – de drukbezette – web-shopmanagers te spreken. Dit maakt dat ik in totaal 15 webshopmanagers heb gesproken, waardoor de uitspraken van mijn onderzoek niet gegeneraliseerd kunnen worden naar de mkb-detailhandel branche. Hier is meer onderzoek voor nodig. Tot slot heeft mijn keuze om de webshopmanagers voorafgaand niet

in te lichten over het onderwerp van mijn onderzoek, er wellicht toe geleid dat ik geen volledig beeld heb gekregen van het daadwerkelijke beleid. Dit maakt ook dat ik geen vergelijking kan maken tussen de respondenten over het cybersecuritybeleid dat zij hebben. Nu lijken de benaderingen heel erg op elkaar, maar wellicht dat er in de daadwerkelijke uitwerking meer verschil zit.

6.3 Aanbevelingen

Zoals ik in de inleiding al beschreef zijn zowel cybercrime als cybersecurity onderbelichte thema's in de wetenschappelijke literatuur. In mijn onderzoek is een aantal bevindingen naar voren gekomen die naar mijn mening in de toekomst verder onderzocht kunnen worden. Ten eerste is dit onderzoek een startpunt voor meer kwalitatief organisatiewetenschappelijk onderzoek naar hoe organisatieleden in het mkb intuïtief betekenis geven aan het risico op cybercrime. In dit onderzoek koppel ik daarvoor de organisatiewetenschappelijke literatuur over betekenisgeving van Karl Weick (1996) aan de economisch-psychologisch-wetenschappelijke literatuur over intuïtief handelen van Kahneman (2013). De integratie van deze twee theorieën lijkt vruchtbaar, omdat de literatuur van Kahneman dieper ingaat op hoe wij als mensen keuzes maken en kan daarmee een diepere invulling geven aan het betekenisproces van Karl Weick. Echter is er nog meer onderzoek nodig om dit te verifiëren en de mogelijkheden hiervoor verder te verkennen. Daarnaast zou meer onderzoek naar webshopmanagers in de mkb-detailhandel en andere sectoren in het mkb, wellicht meer inzicht bieden in hun risicobenadering van cybercrime en kunnen zorgen voor een effectievere en gerichtere aanpak van het cybersecurity vraagstuk. Daarnaast heb ik mij nu enkel gefocust op de webshopmanagers in organisaties, terwijl het in de toekomst mogelijk ook interessant is om te kijken naar de betekenissen die organisaties als geheel geven aan dit onderwerp, omdat dit nog meer inzicht kan bieden in waarom een organisatie handelt zoals hij handelt..

Ten tweede ga ik in dit onderzoek in op een onderzoek van Boothby, Clark en Bargh (2016) over de invisibility cloak illusion en beargumenteer dat deze illusie zich in het geval van de webshopmanagers ook online lijkt af te spelen. Ik noem dit de online invisibility cloak illusion. Het is wellicht voor toekomstig organisatiewetenschappelijk onderzoek interessant om hier langer onderzoek naar te doen om te kijken of deze online illusie ook geldt voor andere organisaties. Ten derde geef ik aan dat de onzichtbaarheid van het internet er paradoxaal genoeg voor zorgt dat de webshopmanagers in een comfortabele positie zitten. Dit omdat de klanten volgens Etzioni (2017), maar ook kijkend naar het klantgedrag van de webshopmanagers zelf, enkel gericht lijken te zijn op zichtbare online vertrouwensfactoren. Hierdoor lijkt er geen aandacht te zijn voor mogelijke risico's of onethisch handelen. De rol van onzichtbaarheid lijkt een belangrijke rol te spelen in de keuzes van webshopmanagers. Het is daarom mogelijk waardevol om in de toekomst te onderzoeken welke rol de onzichtbaarheid van het internet precies speelt in organisaties.

Tot slot speelt het concept vertrouwen een belangrijke rol in dit onderzoek en brengt verschillende uitkomsten met zich mee waar in volgend onderzoek wellicht meer aandacht aan besteed kan worden. Zo ga ik in op een lacune die voortkomt uit het onderzoek van McEvily, Zaheer en Fudge Kamal (2017) over ongelijkwaardigheid tussen interorganisationele vertrouwensbanden. Dit onderzoek geeft aan hoe de webshopmanagers kijken naar hun relatie met de experts. Om daadwerkelijk uitspraken te kunnen doen over de vertrouwensband tussen de webshopmanagers en de experts, zal ook het perspectief van de desbetreffende experts onderzocht moeten worden.

Literatuurlijst

Blum, J. (2013) Controlling for cybersecurity risks of medical device software. Communications of the ACM 56 (10): 35-37.

Boeije, H. (2015). Analyseren in kwalitatief onderzoek. Den Haag: Boom Lemma uitgevers

Bowen, 2000 Environmental visibility: A trigger of green organisational response? Business Strategy and the Environment. 9: 92–107.

Boothby, E. J., Clark, M. S., & Bargh, J. A. (2016, December 15). The Invisibility Cloak Illusion: People (Incorrectly) Believe They Observe Others More Than Others Observe Them. Journal of Personality and Social Psychology. Advance online publication.

Bryman, A. (2012). Social research methods. Oxford University Press

Choo, C.W. (1996) The knowing organization: How organizations use information to construct meaning, create knowledge and make decisions. International Journal of Information Management 16 (5): 329 -340.

Etzioni, A. (2017) Cyber Trust. Journal of Business Ethics.

Gabriels, K (2016) OnLife. Hoe de digitale wereld je leven bepaalt. Tielt: Uitgeverij Lannoo nv.

Ganesan, R., Jajodia, S. & Cam, H. (2017) Optimal Scheduling of Cybersecurity Analysts for Minimizing Risk. ACM Transactions on Intelligent Systems and Technology (TIST) - Special Issue: Cyber Security and Regular Papers, 8 (4).

GFK (2015) Cybersecurity 2015. Awareness, gedrag & digitaal verantwoord ondernemen.

Gordon, L.A. & Loeb, M.P. (2006) Economic aspects of information security: An emerging field of research. Information Systems Frontiers 8 (5): 335–337

Henn, M., Weinstein, M. & Foard, N. (2006) A short introduction to social research. London: The Cromwell Press.

Jackson, 2011

Jackson, R. & Sørensen, G. (2012) Introduction to International Relations. Theories and Approaches. Oxford: Oxford University Press.

Jacobs, B. & Deamen, J. (2017). Computer Security: Intro, slide 39. Gedownload op 3 september 2017, van http://www.sos.cs.ru.nl/applications/courses/security2016/intro.pdf

Kahneman, D. (2013) Ons feilbare denken. Thinking, fast and slow. Amsterdam: Uitgeverij Business Contact.

Kawulich, B.B. (2005) Participant Observation as a Data Collection Method. Forum: Qualitative Social Research Sozialforschung. Volume 6 (2)

Leavy, P. (2015) Method meets arts. Arts-Based Research Practice. New York: The Guilford Press.

Löfman, P., Pelkonen, M. & Pietilä, A.M. (2004) Ethical issues in participatory action research. Scand J Caring Sci, 18, 333–340

Martijn, M. & Tokmetzis, D. (2016) Je hebt wél iets te verbergen. Over het levensbelang van privacy. Zutphen: Koninklijke Wöhrmann.

McEvily, B., Zaheer, A. en Fudge Kamal, D.K. (2017) Mutual and Exclusive: Dyadic Sources of Trust in Interorganizational Exchange. Organization Science 28(1):74-92

Moore J.H. (1985) What is computer ethics? Metaphilosophy, 16 (4): 266 – 275.

Moore, T., Dynes, S. & Chang, F.R. (2015) Identifying How Firms Manage Cybersecurity Investment.

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

Ministerie van Veiligheid en Justitie. Nationaal Coordinator Terrorismebestrijding en Veiligheid (NCTV) (2017) Cybersecuritybeeld Nederland.

Riek, M., Böhme, R. & Moore, T. (2014) Understanding the influence of cybercrime risk on the e-service adoption of European Internet users.

Ruijven, van T. & Keijser, B. (2017) Ketenweerbaarheid tegen cyberdreigingen. Uitgangspunten, good practices en een stappenplan voor het vergroten van cyber-ketenweerbaarheid. Rijswijk: TNO.

Rushanan, M., Rubin, A.D., Foo Kune, D., Swanson, C.M. (2014) SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks.

Schwartz-Shea, P. & Yanow, D. (2012) Interpretive Research Design. Concepts and Processes. New York: Taylor & Francis.

Stone, D. (2012) Policy Paradox. The art of political decision making. New York: W.W. Norton & Company Ltd.

Sunstein, C.R. (2002). Risk and reason: Safety, law, and the environment. Cambridge: Cambridge University Press.

Taleb, N. (2016) Zwarte Zwaan. Amsterdam: Uitgeverij Nieuwezijds.

Thimbleby, H., 2017 Cybersecurity problems in a typical hospital (and probably in all of them) Developing Safe Systems, Proceedings of the 25th Safety-Critical Systems Symposium, Pages: 415 - 439

Timmerman, M.A.P. (2013) Goedwillende hackers, responsible disclosure en strafrecht, Nederlands Juristenblad 87 (8): 483-484.

Website Autoriteit Persoonsgegevens
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming (Laatst geraadpleegd op 28.08.2017)

Website CBS A
https://www.cbs.nl/nl-nl/nieuws/2017/03/meeste-omzetgroei-bij-webwinkels-zonder-winkelpand (Laatst geraadpleegd op 03.09.2017)

Website CBS B
https://www.cbs.nl/nl-nl/nieuws/2017/14/minder-etalages-meer-beeldschermwinkels (Laatst geraadpleegd op 03.09.2017)

Website CBS C
https://www.cbs.nl/nl-nl/nieuws/2017/09/omzet-detailhandel-in-2016-bijna-twee-procent-hoger (Laatst geraadpleegd op 03.09.2017)

Website Eerste Kamer
https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii (Laatst geraadpleegd op 03.09.2017)

Website Financieel Dagblad
https://fd.nl/ondernemen/1215315/steeds-meer-cowboys-bestormen-de-markt-voor-cyberbeveiliging (Laatst geraadpleegd op 03.09.2017)

Website Interpolis
https://www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_mkb.pdf (Laatst geraadpleegd op 03.09.2017)

Website Kaspersky
http://newsroom.kaspersky.eu/fileadmin/user_upload/nl/Downloads/meldplichtdatalekken.pdf (Laatst geraadpleegd op 03.09.2017)

Website NCTV
https://www.nctv.nl/organisatie/cs/index.aspx (Laatst geraadpleegd op 03.09.2017)

Website NOS A

https://nos.nl/artikel/2172895-de-angel-lijkt-eruit-verspreiding-gijzelsoftware-gestopt.html (Laatst geraadpleegd op 03.09.2017)

Website NOS B

https://nos.nl/artikel/2180375-miljoenenschade-door-virus-containerterminals-blijven-dicht.html (Laatst geraadpleegd op 03.09.2017)

Website NOS C

https://nos.nl/artikel/2190836-kiesraad-referendum-aftapwet-stap-dichterbij.html (Laatst geraadpleegd op 03.09.2017)

Website NPO

http://www.npo.nl/de−slag-om-de-klerewereld/09-01−2015/VPWON_1231624 (Laatst geraadpleegd op 19.03.2015)

Website One World

http://www.oneworld.nl/van−t−web/modemerken−slechts−10−duurzaam (Laatst geraadpleegd op 03.09.2017)

Website Politie

https://www.politie.nl/themas/cybercrime.html (Laatst geraadpleegd op 03.09.2017)

Website Rijksoverheid A (inleiding)

https://www.rijksoverheid.nl/actueel/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht (Laatst geraadpleegd op 27.08.2017)

Website Rijksoverheid B

https://www.rijksoverheid.nl/onderwerpen/bevoegdheden-inlichtingendiensten-en-veiligheidsdiensten/wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv (Laatst geraadpleegd op 03.09.2017)

website Rijksoverheid C

https://www.rijksoverheid.nl/onderwerpen/arbeidsomstandigheden/vraag-en-antwoord/wat-is-arbobeleid-en-waar-moet-mijn-werkgever-voor-zorgen (Laatst geraadpleegd op 03.09.2017)

website RTL

https://www.rtlnieuws.nl/buitenland/slechte-omstandigheden-kledingfabrieken-behandel-ons-niet-als-slaven (Laatst geraadpleegd op 03.09.2017)

website SER

http://www.internationalrbc.org/garments-textile/factories?sc_lang=en (Laatst geraadpleegd op 03.09.2017)

website SOMO
https://www.somo.nl/nl/ (Laatst geraadpleegd op 03.09.2017)

Website Symantec
https://www.symantec.com/en/uk/about/newsroom/press-releases/2016/symantec_1018_01 (Laatst geraadpleegd op 27.08.2017)

Website Tweakers
https://tweakers.net/nieuws/120765/nederlandse-bedrijven-hebben-vermoedelijk-18500-datalekken-niet-gemeld.html (Laatst geraadpleegd op 03.09.2017)

Weick, KE.. (1995) Sensemaking in Organizations. California: SAGE Publications, Inc.

Weick, K.E., Sutcliffe, K.M., Obstfeld, D. (2005). Organizing and the process of sensemaking. Organization Science, 16(4).

Wolters, P. & Jansen, C. (2017) Ieder bedrijf heeft zorgplichten. Een handreiking voor bedrijven op het gebied van cybersecurity. Nijmegen: Radboud Universiteit in opdracht van de Cyber Security Raad.

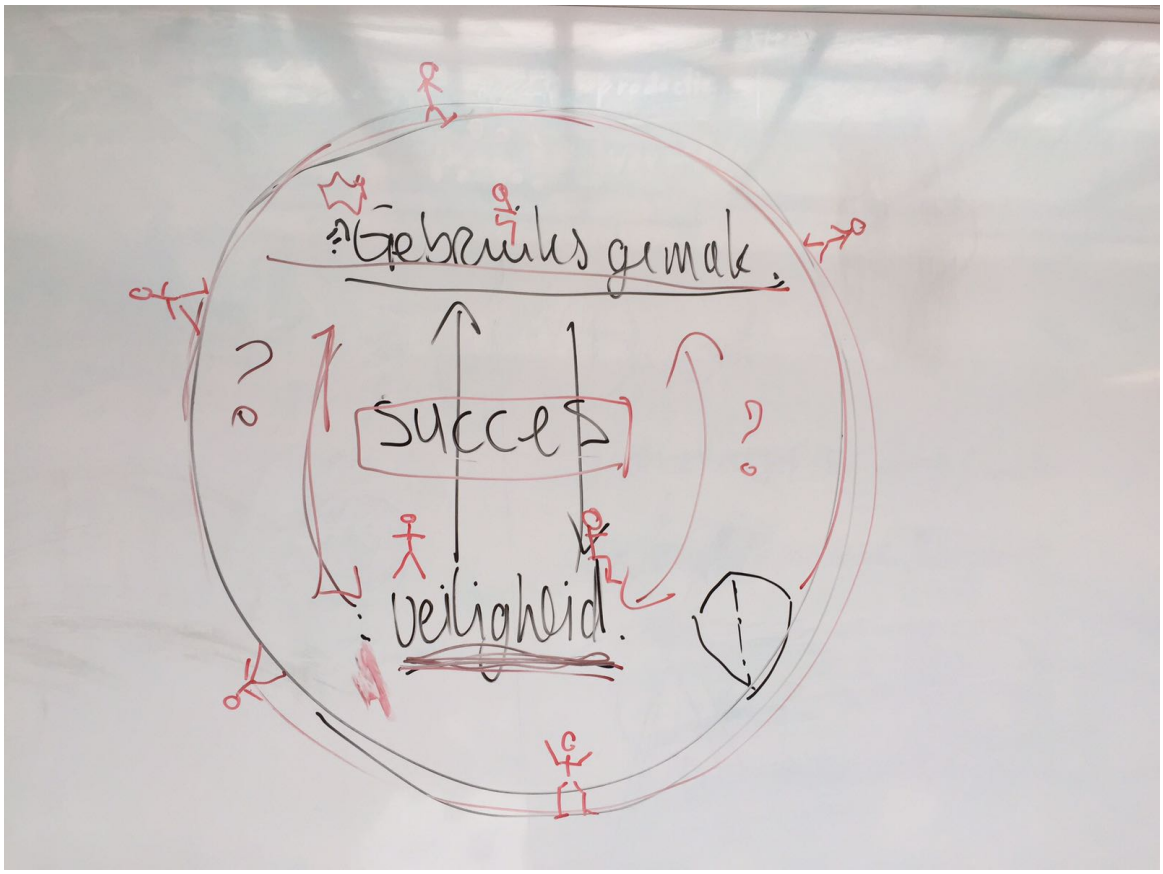
Zyglidopoulos, S. en Fleming, P. (2011) Corporate accountability and the politics of visibility in 'late modernity'. Organization, 18 (5): pp. 691–706

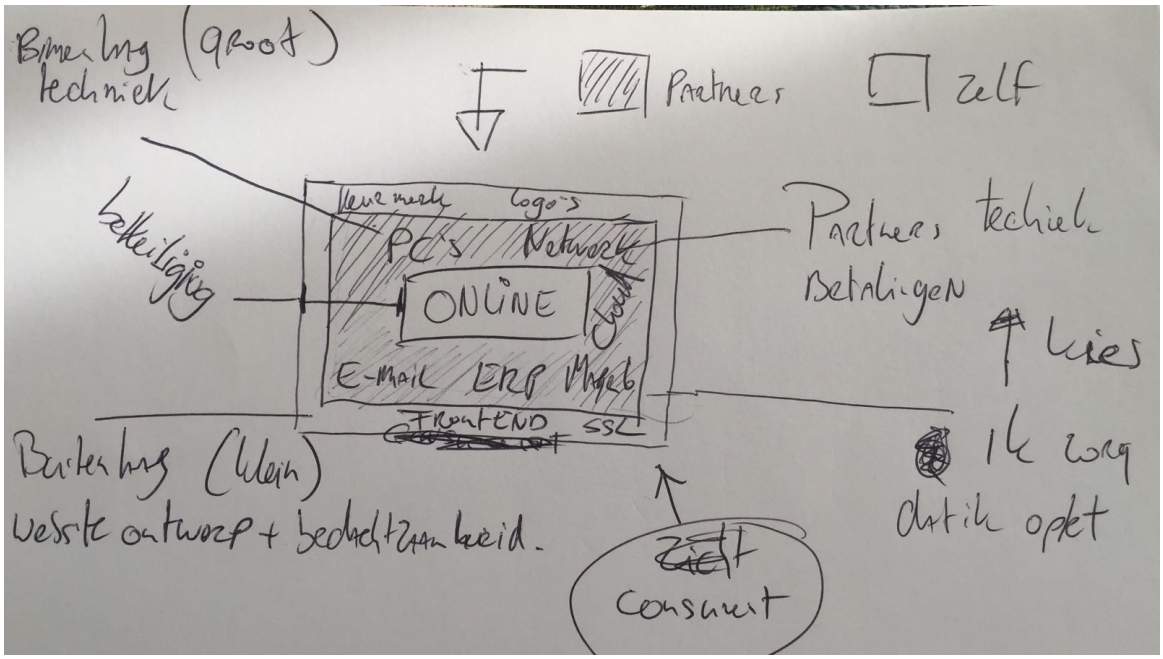
Bijlage A

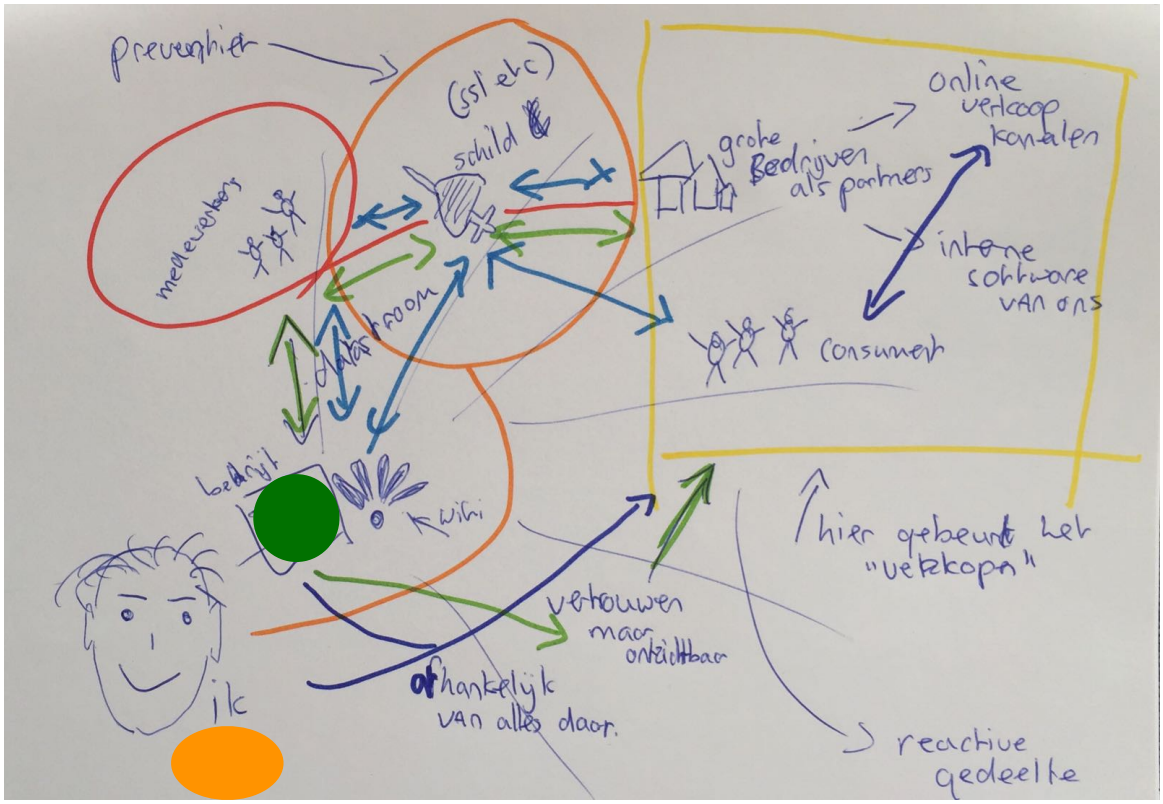
Onderwerp	Verdieping
Algemeen	Hoe groot is het bedrijf Wat is zijn/haar functie? Hoeveel medewerkers stuur hij/zij aan? Staat hij/zij tussen directeur en medewerkers in?
Veiligheid persoonlijk	1. Wat is veiligheid? 3. Wat is privacy? 4. Speelt privacy een rol bij veiligheid? 5. Hoe bescherm jij je eigen privacy?
Observaties en ervaringen	6. Waar denk je aan bij het woord cybercrime? 7. Waar denk je aan bij het woord cybersecurity? 8. Wat krijg je mee van debatten en artikelen over cybercrime of cybersecurity? 9. Heb je zelf weleens te maken gehad met cybercrime? 10. Wat kan je ertegen doen?
Online veiligheid	11. Waar denk je aan bij online veiligheid? 12. Hoe vind je dat webshops omgaan met jouw veiligheid? 13. Hoe kunnen cybercriminelen bij informatie komen? 14. Is er een verschil tussen hoe je met informatie omgaat in een fysieke winkel dan in een online winkel? Waarom?
Veiligheid op de werkvloer	15. Hoe ga je om met Informatie? 16. Hoe verschilt jouw handelen naar privacy op de werkvloer met hoe je jouw eigen privacy beschermd? 17. Voer je zelf bepaalde handelingen uit om informatie te beschermen? Zo ja, welke? 18. Heb jij als manager een rol bij het managen van klantdata? 19. Is er een verschil met hoe je omgaat met jouw eigen informatie en die van de organisatie?
Verantwoordelijkheid	20. Zie je jezelf als een voorbeeldfunctie op de werkvloer? 21. Welke rol heb jij als manager bij het zorgen voor de beveiliging van informatie?
Tekenen	Teken jouw rol in het cybersecuriybeleid. Licht deze tekening kort toe.

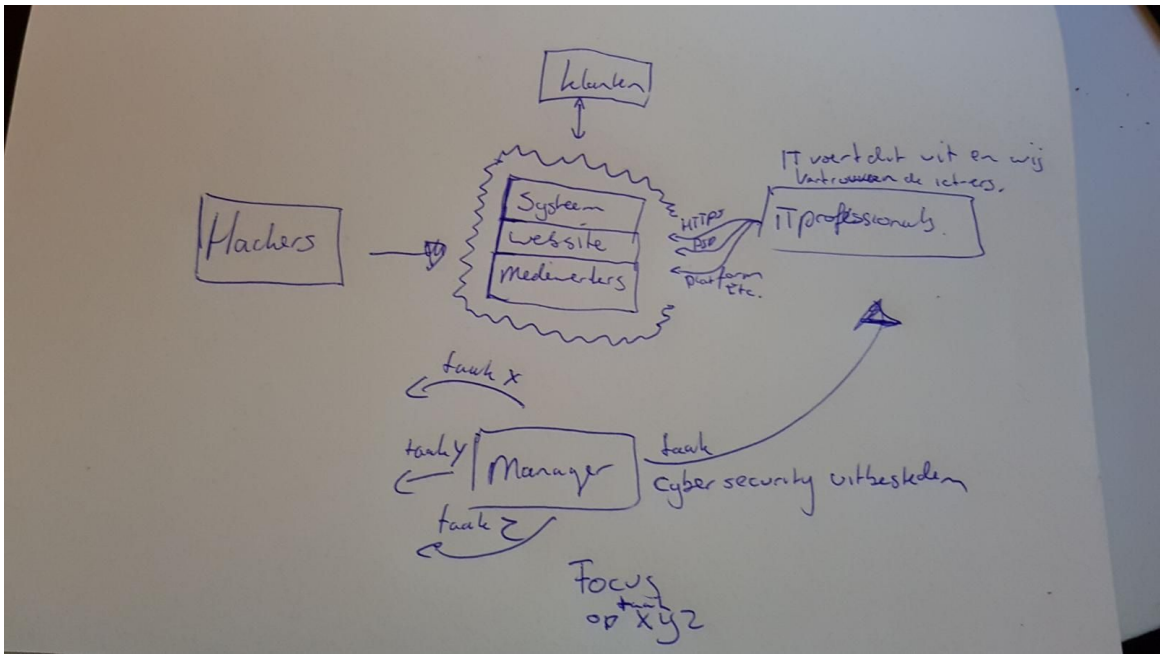
Bijlage B

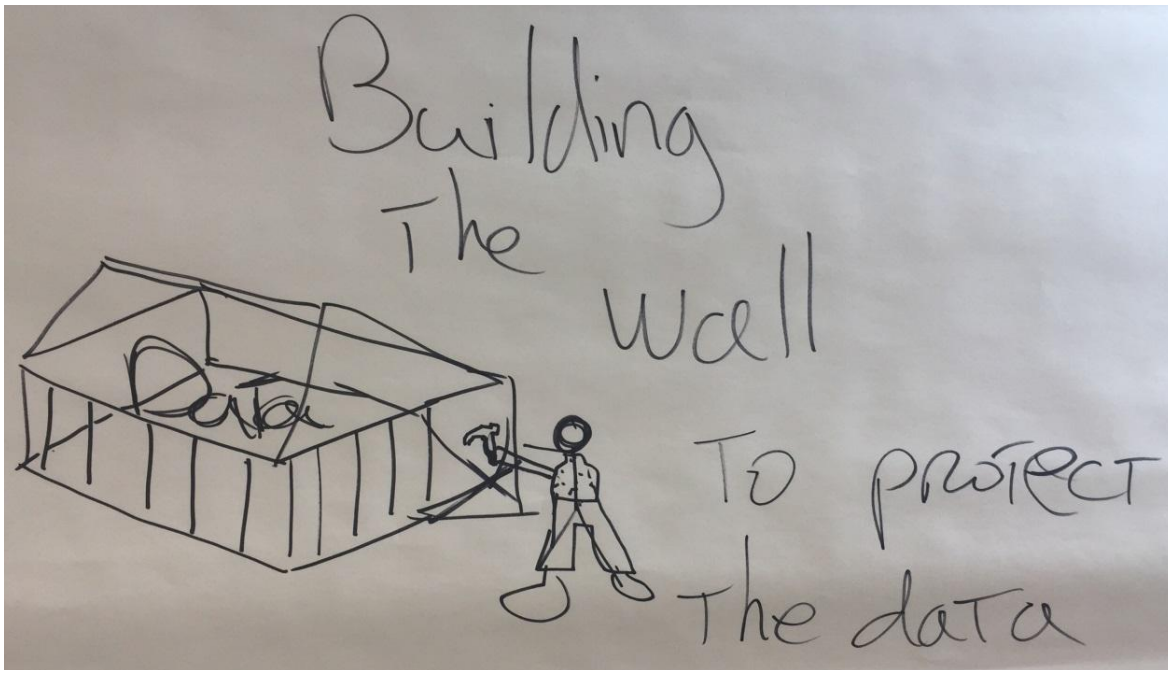
Tekeningen van de webshopmanagers.

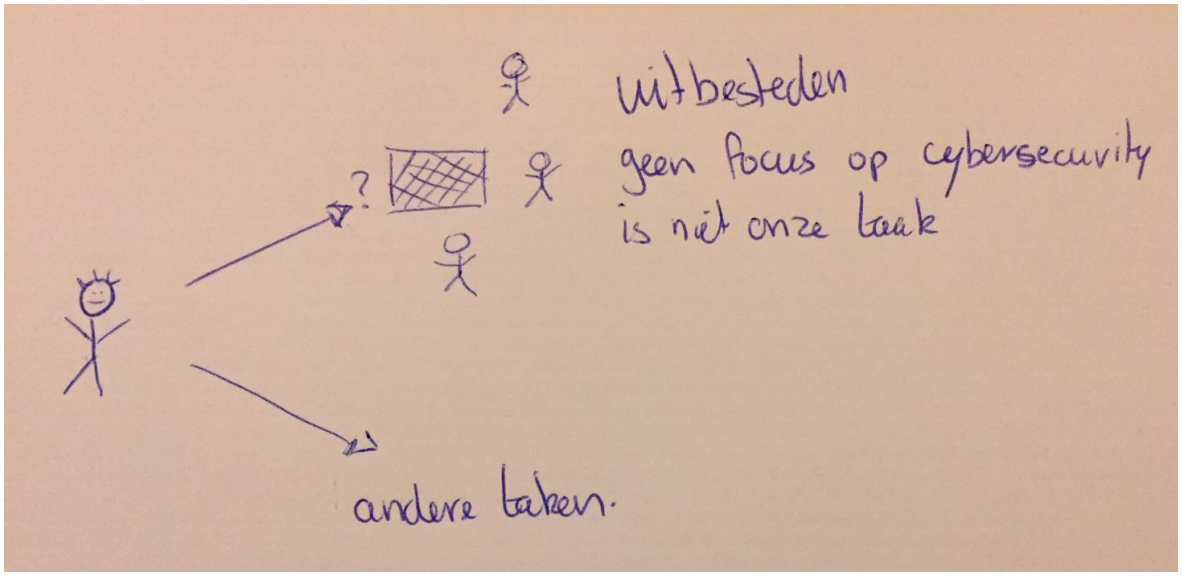


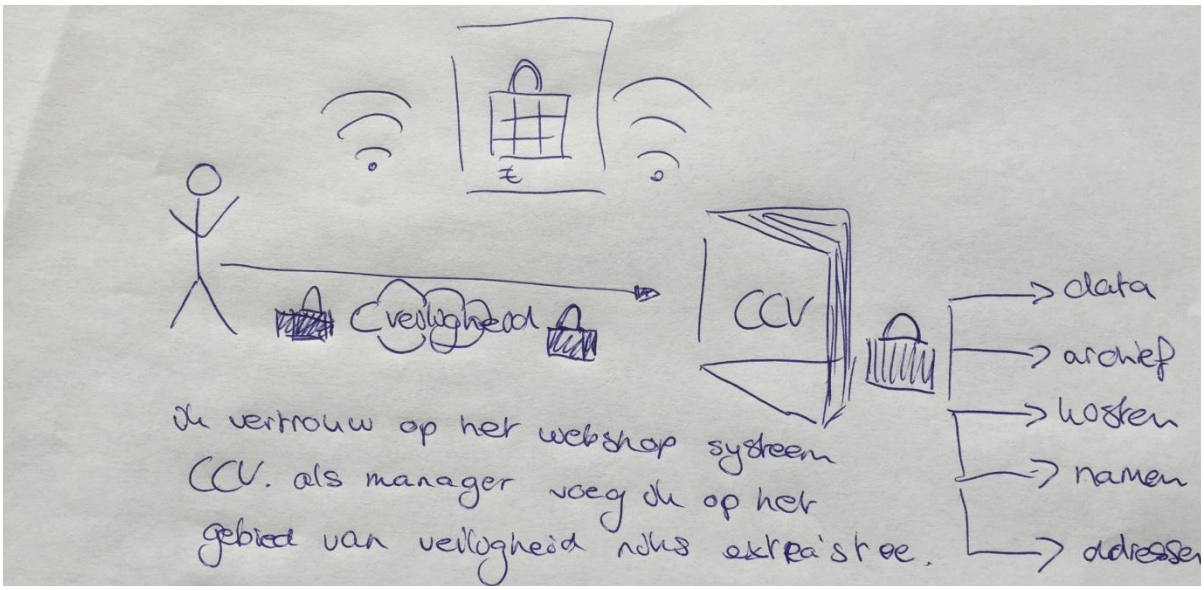


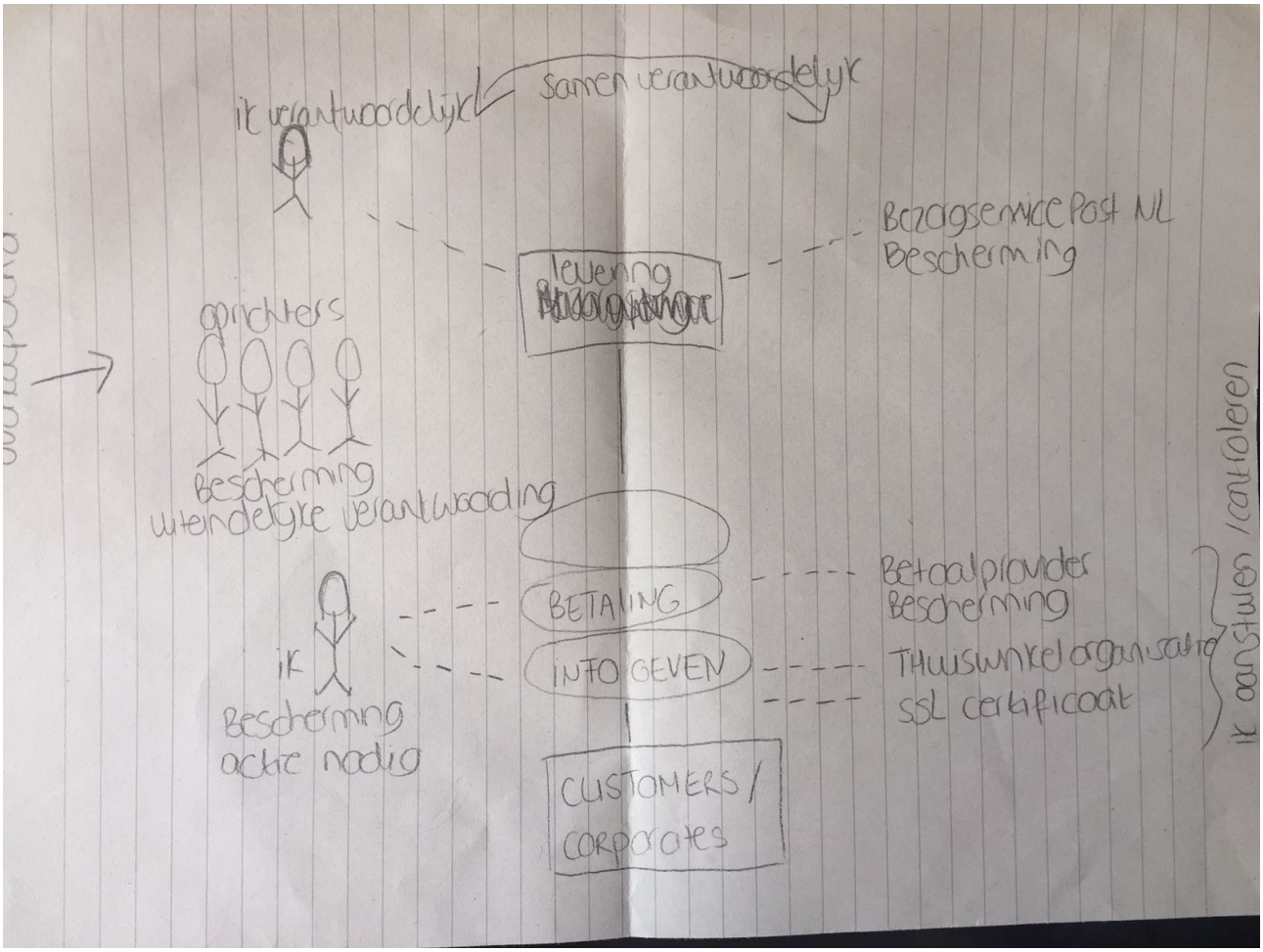

Preventief
(ssl etc)
schild
medewerkers
grote Bedrijven als partners
online verkoop kanalen
interne software van ons
consumenten
Wiki
vertrouwen maar controleer
hier gebeurt het "verkopen"
ik
reactive gedeelte


Hackers
Systeem
website
medewerkers
IT professionals
taak x
taak y
Manager
taak
Cyber security uitbesteden
taak z
Focus


Building
The
Wall
Data
To protect
The data


uitbesteden
geen focus op cybersecurity
is niet onze taak
?
andere taken.


veiligheid
CCV
data
archief
kosten
namen
adressen
ik vertrouw op het webshop systeem CCV. als manager voeg ik op het gebied van veiligheid iets extra's toe.


ik verantwoordelijk
samen verantwoordelijk
Bezorgservice Post NL
Bescherming
levering
gerichters
Bescherming
uiteindelijke verantwoording
BETALING
Betaalprovider
Bescherming
INFO GEVEN
THUISWINKEL organisatie
SSL certificaat
ik
Bescherming
actie nodig
CUSTOMERS / CORPORATES
ik aanstuwen / controleren