PILOTONDERZOEK CYBERWEERBAARHEID MKB-RETAILERS IN DE REGIO DEN HAAG

ONDERZOEKSRAPPORTAGE

De Haagse Hogeschool, lectoraat Cybersecurity in het mkb

Dr. Rick van der Kleij, Iris de Bruin, Dr. Susanne van 't Hoff – De Goede, &
Dr. Rutger Leukfeldt

Datum: 7 maart 2019

MANAGEMENT SAMENVATTING

Aanleiding: Cybercriminaliteit heeft een relatief grote impact op het mkb. Mkb'ers hebben vaak onvoldoende kennis en hulpbronnen om zichzelf hiertegen te beschermen. Eerder onderzoek laat zien dat twee van de vijf mkb'ers in een jaar tijd te maken heeft gehad met cybercriminaliteit. Eén op de vijf heeft bovendien schade hiervan ondervonden.[1] Het idee bestaat dan ook dat mkb'ers meer cyberweerbaar zouden moeten zijn.

Doel: In opdracht van de gemeente Den Haag en in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) onderzocht het Lectoraat Cybersecurity in het mkb van De Haagse Hogeschool hoe het is gesteld met de cyberweerbaarheid van het mkb in de regio Den Haag. Het doel is om een beeld te krijgen van de huidige cyberweerbaarheid van mkb'ers en van factoren die met die weerbaarheid samenhangen. Omdat dit een pilot betreft is ervoor gekozen om het onderzoek uit te voeren onder een specifieke groep mkb'ers, namelijk retailers. Er is gekozen voor onderzoek onder retailers omdat de bedrijfssector waarin zij werken, namelijk de detailhandel, een risicogroep vormt.[2]

Methode: Cyberweerbaarheid is het vermogen van het mkb om weerstand te bieden tegen bekende en onbekende vormen van cybercriminaliteit en snel te herstellen van een cybercrisis. Dit betekent dat het mkb in staat moet zijn om te anticiperen op bedreigingen en kansen en deze ook moet kunnen detecteren als deze zich voordoen in de organisatie. Ook moet het mkb adequaat kunnen reageren op incidenten en begrijpen wat er heeft plaatsgevonden zodat ervan kan worden geleerd. Cyberweerbaarheid is gemeten met behulp van een vragenlijst met stellingen. Een voorbeeld van een stelling is: 'Medewerkers in ons bedrijf vinden de bestrijding van cybercriminaliteit op het werk belangrijk'. Hoe hoger een bedrijf scoort op deze stellingen, hoe meer cyberweerbaar het bedrijf is. Het onderzoek is uitgevoerd in september en oktober 2018 in 6 winkelgebieden in Den Haag en omstreken. In totaal zijn 375 retailers benaderd. Hiervan hebben 57 leidinggevenden uit 56 bedrijven een enquête ingevuld.[3]

Resultaten: Bijna de helft (48 %) van de retailers geeft aan slachtoffer te zijn geweest van cybercriminaliteit in de laatste 12 maanden. Zeven bedrijven (12 %) hebben ook daadwerkelijk schade hiervan ondervonden. Schade als gevolg van cybercriminaliteit kan zich op verschillende vlakken voordoen. Zo kan een bedrijf financiële schade oplopen. Ook kunnen belangrijke bedrijfsgegevens gestolen of vernietigd zijn. Schade kan ook bestaan uit tijdverlies, doordat de bedrijfsprocessen tijdelijk stilliggen. Daarnaast kan een bedrijf imagoschade oplopen. Als we kijken naar de cyberweerbaarheid dan valt op dat mkb-retailers maar in beperkte mate weerbaar zijn. Er lijkt ruimte te zijn voor verbetering. Deelnemende retailers zijn relatief gezien het best in staat om te 'reageren' en het minst goed in staat zijn om te 'leren', maar de verschillen zijn niet groot. Een mogelijke voorspeller van de cyberweerbaarheid blijkt de IT-kennis van het personeel te zijn. Bedrijven met medewerkers die relatief veel IT-kennis hebben, scoren hoger op cyberweerbaarheid. Ook blijkt dat bedrijven die een sanctiebeleid voor medewerkers hebben die zich cyber onveilig gedragen doorgaans meer cyberweerbaar zijn. Veel bedrijven hebben al voorschriften over cyber veilig gedrag. Ons onderzoek

[1] https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf
[2] https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018
[3] https://ccv-secondant.nl/platform/article/cybercriminaliteit-leeft-niet-onder-retailers

laat zien dat het van belang is om hiernaast ook een sanctiebeleid te voeren op het niet naleven van deze voorschriften.

Conclusie: Er is ruimte voor verbetering van de cyberweerbaarheid van mkb-retailers in de regio Den Haag. Dit is in lijn met de verwachtingen op basis van eerder onderzoek. Meer IT-kennis bij het personeel en een strikter sanctiebeleid kunnen helpen om de cyberweerbaarheid te vergroten.

INHOUD

INLEIDING

Midden- en kleinbedrijven vormen het overgrote gedeelte van de Nederlandse economie.[4] Het mkb in Nederland levert ongeveer drie miljoen banen op en heeft een omzet van honderden miljarden euro's. Cybercriminaliteit heeft een relatief grote impact op het mkb. Mkb'ers hebben vaak onvoldoende kennis en hulpbronnen om zichzelf te beschermen tegen cyberincidenten.[5] Een nulmeting van het Centre of Expertise Cybersecurity van De Haagse Hogeschool laat zien dat twee op de vijf mkb-bedrijven te maken heeft gehad met cybercriminaliteit en dat één op de vijf daadwerkelijk slachtoffer is geworden.[6] Cybercriminaliteit bestaat uit (1) delicten die worden gepleegd met behulp van en gericht tegen computers of het internet (cybercriminaliteit in enge zin), en (2) traditionele delicten die worden gefaciliteerd door of gepleegd met behulp van computers of het internet (cybercriminaliteit in brede zin).[7] Onderzoek uit 2014 wijst uit dat het mkb voornamelijk slachtoffer wordt van cyberdelicten zoals malware, phishing, e-fraude (zoals acquisitiefraude) en hacken.[8] Tevens laat dit onderzoek uit 2014 zien dat bedrijven die slachtoffer geworden zijn van cybercriminaliteit vaak niet weten hoe dat zo is gekomen. Ook stapt maar een klein percentage van de slachtoffers naar de politie. Mkb'ers hebben dus niet alleen onvoldoende kennis om zich te weren tegen cybercriminaliteit, maar het schort hen ook aan kennis over hoe gereageerd moet worden op slachtofferschap. Vanwege de betekenis van het mkb voor de Nederlandse economie is het van belang inzicht te krijgen in hoe het mkb zich beter kan weren tegen cybercriminaliteit.

Onder cyberweerbaarheid verstaan wij de vermogens van mkb'ers om weerstand te kunnen bieden tegen bekende en onbekende vormen van cybercriminaliteit en om snel te kunnen herstellen van een crisis als gevolg van een cyberincident. [9] Dit betekent dat het mkb aan de ene kant in staat moet zijn om te kunnen anticiperen op bedreigingen en kansen en deze ook moet kunnen detecteren als ze zich voordoen in de organisatie. Aan de andere kant moet het mkb adequaat kunnen reageren op incidenten en ook snappen wat er heeft plaatsgevonden zodat ervan kan worden geleerd. Hierbij speelt de menselijke factor, de medewerker, een belangrijke rol. Cyberveilig gedrag van medewerkers kan namelijk helpen om een organisatie te beschermen tegen cybercriminaliteit.

De retail vormt een relatief grote risicogroep binnen het mkb. Onder retail verstaan wij in dit onderzoek het leveren van diensten en goederen voor persoonlijk gebruik aan consumenten. De

[4] Leukfeldt, E. R. (2018). De 'human' factor in cybersecurity [Intreerede]. Geraadpleegd van https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/intreerede-dr-rutger-leukfeldt.pdf?sfvrsn=26b8908_2

[5] Olsthoorn. S., & Koot, J. (2017). 'Goede cyberbeveiliging te duur voor mkb'er'. *Financieel Dagblad.* Geraadpleegd van https://fd.nl/economie-politiek/1190183/mkb-is-kwetsbaar-voor-hackers

[6] Notté, R., & Slot, L. (2017). Hoe cybersecure is het mkb? Nulmeting cybersecurity in het mkb. Geraadpleegd van https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf

[7] Domenie, M. M. L., Leukfeldt, E. R., Wilsem, J. A. van, Jansen, J., & Stol, W. Ph. (2013). Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit. Den Haag: Boom Lemma uitgevers.

[8] Veenstra, S., Zuurveen, R., Jansen, J., Kloppenburg, S., & Stol, W. (2014). MKB en cybercrime: Slachtofferschap onder het Nederlandse Midden- en Kleinbedrijf in een gedigitaliseerde samenleving. Leeuwarden: Lectoraat Cybersafety, NHL Hogeschool. Geraadpleegd van https://www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/2014-03-10%20Bedrijf%20en%20digitale%20veiligheid%20DEFINITIEF.pdf

[9] Kleij, R. van der (2018). Digitale weerbaarheid in het mkb: een serieus probleem? *Tijdschrift voor Human Factors, 43*(1), 19-21.

Cybersecuritymonitor 2018 [10] van het Centraal Bureau voor de Statistiek (CBS) wijst uit dat binnen de handelssector, waarin retailers werken, relatief weinig ICT-beveiligingsmaatregelen worden getroffen. Ook blijkt dat bedrijven met een klein aantal werknemers (twee tot tien), zoals mkb-retailers, relatief minder beveiligingsmaatregelen treffen dan bedrijven met een groter aantal werknemers (meer dan tien). Toch gebruiken zij, zij het in beperkte mate, computers en het internet, bijvoorbeeld voor het versturen en ontvangen van e-mails of voor het doen van betalingen. Op deze manier kunnen zij zich blootstellen aan potentiële cybercriminelen. Van de kleine bedrijven die wel beveiligingsmaatregelen treffen, besteedt ongeveer de helft dit werk uit en heeft de andere helft het werk in eigen beheer. Mogelijk houdt de helft van deze bedrijven het werk in eigen beheer vanwege beperkte budgetten om het uit te besteden, hoewel dit niet uit de monitor blijkt. Een andere mogelijkheid is dat de bedrijven het beveiligingswerk in eigen beheer houden omdat zij vinden dat zij zelf verantwoordelijk zijn voor hun digitale beveiliging, zoals volgt uit onderzoek van de Kamer van Koophandel.[11]

Het lectoraat Cybersecurity in het mkb van De Haagse Hogeschool is in opdracht van de gemeente Den Haag en in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een pilotonderzoek gestart naar de cyberweerbaarheid van mkb-retailers in een aantal winkelgebieden in de regio Den Haag. Het doel hiervan is om een beeld te krijgen van de huidige cyberweerbaarheid van mkb-retailers en van factoren die met die weerbaarheid samenhangen. *De centrale vraag in dit onderzoek is: hoe cyberweerbaar zijn mkb-retailers en welke factoren hangen samen met hun cyberweerbaarheid?*

In dit onderzoek wilden we, zoals gezegd, ook onderzoeken of er variabelen zijn die verband houden met cyberweerbaarheid. Zo verwachten we onder andere ten aanzien van het gemiddelde IT-kennisniveau van het personeel dat bedrijven met medewerkers die een hoog IT-kennisniveau hebben meer cyberweerbaar zullen zijn. Deze verwachting komt voort uit onderzoek waaruit blijkt dat *information security awarenesss* of *cybersecurity awareness* positief gerelateerd is aan de attitudes ten opzichte van het vertonen van cyberveilig gedrag.[12] Hieruit kan afgeleid worden dat wanneer medewerkers relatief veel weten van IT-beveiliging, zij ook meer cyberveilig zullen handelen en het bedrijf als geheel meer cyberweerbaar is. Verder verwachten we bijvoorbeeld dat bedrijven die een streng sanctiebeleid hebben op onveilig werken van de medewerkers ook meer cyberweerbaar zullen zijn. Deze verwachting komt voort uit onderzoek waaruit blijkt dat afschrikking middels sancties effectief zou kunnen zijn om positieve attitudes ten opzichte van cyberveilig handelen te creëren.[13] Verder verwachten we dat bedrijven waarvan hun bedrijfsprocessen in grote mate afhankelijk zijn van computers en internet ook meer cyberweerbaar zullen zijn. De Cybersecuritymonitor wijst bijvoorbeeld uit dat grotere bedrijven, die vaak ook een complexere ICT-infrastructuur hebben, meer ICT-veiligheidsmaatregelen treffen dan kleinere bedrijven die niet zozeer afhankelijk zijn van ICT.[14]

---

[10] Centraal Bureau voor de Statistiek (2018). *Cybersecuritymonitor 2018.* Den Haag: Centraal Bureau voor de Statistiek. Geraadpleegd van https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018

[11] Kamer van Koophandel (2017). *Preventie door het mkb tegen digitale fraude.* Utrecht: Kamer van Koophandel. Geraadpleegd van https://www.kvk.nl/download/Onderzoeksrapportage_Fraude_sept170920-2_tcm109-449039.pdf

[12] Zie onder andere: Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548.

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

[14] Centraal Bureau voor de Statistiek (2018). *Cybersecuritymonitor 2018.* Den Haag: Centraal Bureau voor de Statistiek. Geraadpleegd van https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018

METHODE

PARTICIPANTEN

De doelgroep van deze pilotstudie waren mkb-retailers in de regio Den Haag. Om zoveel mogelijk respondenten voor het onderzoek te werven, is ervoor gekozen onderzoek te doen in zes winkelgebieden in de regio. In samenspraak met de gemeente Den Haag en Leidschendam-Voorburg zijn de volgende zes winkelgebieden geselecteerd: Den Haag Centrum, Loosduinse Hoofdplein (Den Haag), Leidsenhage (Leidschendam), Leidschendam Centrum, Huygenskwartier (Voorburg) en Julianabaan (Voorburg). De gemeente heeft via de winkeliersverenigingen in deze gebieden, het verspreiden van nieuwsbrieven en via centrum- en gebiedsmanagers het onderwerp gepromoot bij de mkb'ers. Omdat tijdens het werven van de bedrijven bleek dat de animo om deel te nemen aan het onderzoek beperkt was, is ervoor gekozen om ook bedrijven uit andere sectoren dan de retail die gelegen zijn binnen deze winkelgebieden te betrekken bij het onderzoek. Op deze manier werd geprobeerd een groter aantal respondenten te bereiken.

INSTRUMENTEN

Om de mate van cyberweerbaarheid en verschillende achtergrondkenmerken van de mkb'ers te onderzoeken, is gebruikgemaakt van een enquête (zie Bijlage A). De enquête is zo veel mogelijk mondeling afgenomen, maar kon ook op een later tijdstip schriftelijk worden ingevuld. In het geval dat mondelinge afname niet mogelijk of gewenst was, is een papieren versie achtergelaten en is een afspraak gemaakt om de enquête op een later tijdstip op te halen. Ook was een link naar een digitale versie beschikbaar voor ondernemers. De enquête bestond uit vragen over algemene kenmerken van het bedrijf, zoals aantal werknemers en sector; IT-gerelateerde achtergrondkenmerken, zoals de mate waarin de bedrijfsprocessen afhankelijk zijn van computers en internet, de gemiddelde IT-kennis van het personeel en sanctiebeleid op cyberonveilig gedrag; vragen over slachtofferschap van cybercriminaliteit; en vragen over de verschillende componenten (anticiperen, monitoren, reageren, leren) van cyberweerbaarheid. Om sanctiebeleid te meten is een gevalideerde schaal vertaald, namelijk voor *punishment severity* [15]. Voor de vragen over slachtofferschap en schade ten gevolge van cybercriminaliteit is gebruikgemaakt van de nulmeting van het Centre of Expertise Cybersecurity.[16]

PROCEDURE

Voor het werven van mkb-retailers voor deelname aan dit pilotonderzoek is een projectteam ingesteld. De kern van dit team bestond uit onderzoekers, docenten en stagiairs van De Haagse Hogeschool, een

[15] Peace, A. G., Galetta, D. F., & Thong, J. Y. L. (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems, 20*(1), 153-177.

[16] Notté, R., & Slot, L. (2017). Hoe cybersecure is het mkb? Nulmeting cybersecurity in het mkb. Geraadpleegd van https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf

Adviseur Veiligheid van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), de coördinator van het Regionaal Samenwerkingsverband Integrale Veiligheid (RSIV) en stagiairs van de gemeente Den Haag en het RSIV. Daarnaast sloten soms ook de centrum- of winkelstraatmanagers van de winkelgebieden en andere medewerkers van de gemeente Den Haag en De Haagse Hogeschool aan bij het werven van de bedrijven.

Op vier verschillende dagen verspreid over september en oktober is het projectteam langsgegaan bij de mkb'ers in de zes gebieden. Hierbij is gebruikgemaakt van een afvinklijst met de namen en adressen van mkb'ers uit de zes winkelgebieden zoals deze stonden geregistreerd bij de Kamer van Koophandel.

Het doel van deze bezoekmomenten was in eerste instantie om de enquête direct af te kunnen nemen bij de mkb'er, hetzij digitaal via een meegebrachte tablet, hetzij op papier. Als dit niet uitkwam voor de mkb'er maar hij wel geïnteresseerd was in deelname, werd aangeboden om op een ander moment langs te komen om de enquête af te nemen of werd een URL aangeboden om de enquête digitaal in te kunnen vullen. Contactgegevens van deze mkb'ers werden gevraagd en genoteerd om ze op een later moment te kunnen bellen om te vragen of het invullen van de enquête was gelukt.

Op de eerste drie dagen werden steeds twee winkelgebieden per dag bezocht. Leden van het projectteam bezochten ofwel in tweetallen, ofwel alleen de mkb'ers. Na de eerste drie dagen werd een lijst opgemaakt van bedrijven die hadden toegezegd de enquête op een later moment in te vullen en van bedrijven die niet bereikt konden worden tijdens het bezoekmoment (bijvoorbeeld omdat het bedrijf gesloten was of omdat het er te druk was). Vervolgens zijn de bedrijven die hadden toegezegd de enquête later in te vullen gebeld door de stagiairs uit het projectteam. Hen werd gevraagd of het al was gelukt om de enquête in te vullen, en zo niet, of zij alsnog bereid waren dit te doen. Op de vierde dag werden de bedrijven bezocht die op de eerste drie bezoekmomenten gesloten waren of anderszins niet bereikt konden worden. Ook aan hen werd gevraagd de enquête direct of op een later moment in te vullen.

ANALYSES

Met het statistische analyseprogramma SPSS zijn beschrijvende analyses uitgevoerd om een algemeen beeld te krijgen van de achtergrondkenmerken en het niveau van cyberweerbaarheid van de deelnemende bedrijven. Daarnaast zijn correlatieanalyses uitgevoerd om te onderzoeken of de verschillende in het onderzoek opgenomen variabelen een samenhang vertonen met het niveau van cyberweerbaarheid van het mkb.

RESULTATEN[17,18]

ALGEMENE OMSCHRIJVING VAN DE RESPONDENTEN

Van de 399 bedrijven in de regio hebben we persoonlijk contact gehad met 375 bedrijven, telefonisch dan wel *face-to-face.* Sommige bedrijven waren gesloten en konden nadien ook niet telefonisch worden bereikt. Uiteindelijk is de enquête ingevuld door 56 unieke bedrijven. Dit is een responspercentage van 14,9 procent. Binnen een bedrijf hebben twee managers de enquête ingevuld, waardoor de enquête uiteindelijk 57 respondenten heeft. Hiervan zijn zes bedrijven (10,7%) gelegen in Leidschendam Centrum, veertien bedrijven (25%) in het Huygenskwartier, vier bedrijven (7,1%) in Leidsenhage, tien bedrijven (17,9%) aan de Julianabaan, tien bedrijven (17,9%) aan het Loosduinse Hoofdplein en twaalf bedrijven (21,4%) in Den Haag Centrum (zie Tabel C1).

Van de deelnemende mkb'ers behoren 33 mkb'ers (57,9%) tot de retail-sector, vier (7%) tot de horeca, twee (3,5%) tot overige zakelijke diensten, dertien (22,8%) tot een andere bedrijfssector en één mkb'er (1,8%) weet niet tot welke sector zijn mkb behoort (zie Tabel C2).[19]

OVERIGE RELEVANTE ACHTERGRONDKENMERKEN

De deelnemende mkb'ers hebben overwegend een (zeer) klein aantal werknemers in dienst die minstens vijftien uur per week werken. Acht bedrijven (14%) hebben één werknemer, 27 bedrijven (47,4%) hebben twee tot vijf werknemers, twaalf bedrijven (21,1%) hebben zes tot tien werknemers, negen bedrijven (15,8%) hebben elf tot vijftig werknemers en één bedrijf (1,8%) heeft 51 tot honderd werknemers. Er is geen enkel bedrijf dat meer dan honderd werknemers in dienst heeft (zie Tabel C3).

24 mkb'ers (42,1%) hebben aangegeven het (volledig) eens te zijn met de stelling dat de bedrijfsprocessen volledig afhankelijk zijn van computers en internet (zie Tabel C4). Achttien mkb'ers (31,6%) hebben de IT-beveiliging volledig uitbesteed, acht (14%) hebben de IT-beveiliging deels uitbesteed, 24 (42,1%) hebben de IT-beveiliging volledig in eigen beheer en drie (5,3%) weten niet wie de IT-beveiliging beheert (zie Tabel C5). Uit gesprekken met de ondernemers bleek tevens dat zij de IT-beveiliging soms uitbesteden aan kennissen of familieleden met verstand van IT. Verder wezen gesprekken ook uit dat in sommige ondernemingen nauwelijks sprake was van een degelijk IT-beveiligingsbeleid en dat zij de IT-beveiliging zelf beheren; het heeft in elk geval geen grote prioriteit. Het gemiddelde IT-kennisniveau van het personeel is overwegend laag. 26 mkb'ers (45,6%) schatten de gemiddelde IT-kennis namelijk heel laag tot redelijk laag in, 22 mkb'ers (38,6%) schatten de gemiddelde IT-kennis als gemiddeld in en negen mkb'ers (15,8%) schatten de gemiddelde IT-kennis redelijk hoog tot heel hoog in (zie Tabel C6).

Ook is gevraagd naar het sanctiebeleid dat de mkb'ers voeren op cyberonveilig handelen van medewerkers. Dit is gemeten met behulp van twee stellingen en een 5-puntsschaal, waarbij een

[17] Zie Infographic: Hoe cyberweerbaar zijn mkb-retailers in de regio Den Haag (Bijlage B).
[18] Voor een overzicht van beschrijvende statistiek zie Bijlage C.
[19] De percentages zullen niet altijd optellen tot honderd procent, omdat sommige vragen niet door iedere respondent zijn ingevuld.

hogere score duidt op een strenger sanctiebeleid (zie Bijlage A). Hierop scoorden de mkb'ers gemiddeld 2,54, met een standaarddeviatie van 1,08. Dit betekent dat overwegend sprake is van een matig tot geen (streng) sanctiebeleid.

27 mkb'ers hebben aangegeven in de afgelopen twaalf maanden te maken te hebben gehad met minstens één cyberdelict (48,2%). Phishing wordt hierbij veruit het vaakst genoemd (31,6%), virussen worden vervolgens het vaakst genoemd (10,5%). Delicten als ransomware, digitale fraude en hacking komen nauwelijks of slechts bij enkele bedrijven voor (zie Tabel C7). Van de 27 bedrijven die aangaven slachtoffer te zijn geworden, hebben echter zeven bedrijven (12,3%) ook daadwerkelijk schade ondervonden van het slachtofferschap. Dit kon zowel financiële schade betreffen, als imagoschade, als het stilliggen van de bedrijfsprocessen, als diefstal of vernietiging van de bedrijfsgegevens.

De kans dat het eigen mkb slachtoffer wordt van cybercriminaliteit wordt door de mkb'ers gemiddeld ingeschat als een kans van negentien procent, met een standaarddeviatie van 20,58. De kans dat een mkb in het algemeen slachtoffer wordt van cybercriminaliteit wordt echter hoger ingeschat, namelijk 34 procent, met een standaarddeviatie van 24,25.

CYBERWEERBAARHEID

Cyberweerbaarheid is gemeten door middel van 42 stellingen die zijn voorgelegd aan de managers van de mkb-bedrijven (zie Bijlage A). De stellingen meten de capaciteit, gelegenheid en motivatie om te anticiperen op cyberincidenten, om ze te detecteren, om erop te reageren en om ervan te leren.[20]Ten tweede meten de stellingen de capaciteit, de gelegenheid en de motivatie om cyberveilig te handelen.[21] De houding van de mkb'ers ten aanzien van de stellingen werd gemeten met een 6-puntsschaal, waarbij een hogere score duidt op een betere cyberweerbaarheid. 1 = volledig oneens, 2 = grotendeels oneens, 3 = lichtelijk oneens, 4 = lichtelijk eens, 5 = grotendeels eens, 6 = volledig eens. Een 4 of hoger is een voldoende.

De deelnemende mkb-retailers scoorden gemiddeld 3,46 op cyberweerbaarheid, met een standaarddeviatie van 0,99. Dit is net geen voldoende. Op het vermogen anticiperen werd gemiddeld 3,34 gescoord (standaarddeviatie = 1,00); op monitoren 3,57 (standaarddeviatie = 1,12); op reageren 3,74 (standaarddeviatie = 1,16); en op leren 3,17 (standaarddeviatie = 1,26). De mkb'ers scoorden gemiddeld dus het best op reageren en het minst goed op leren (zie Tabel C8).

Met behulp van Spearman rangcorrelatieanalyses is onderzocht welke achtergrondkenmerken een correlatie hebben met cyberweerbaarheid. Hieruit volgt dat sanctiebeleid en cyberweerbaarheid significant correleren, $\rho = 0{,}413$; $\alpha < 0{,}01$. Dit is een positief verband en houdt in dat naarmate het sanctiebeleid van een bedrijf strenger is, het bedrijf meer cyberweerbaar is. De sterkte van het verband is zwak tot gemiddeld[22]. Ook de gemiddelde IT-kennis van het personeel en cyberweerbaarheid correleren significant, $\rho = 0{,}312$; $\alpha < 0{,}05$. Dit is een positief verband en houdt in dat naarmate de

[20] Kleij, R. van der (2018). Digitale weerbaarheid in het mkb: een serieus probleem? *Tijdschrift voor Human Factors, 43*(1), 19-21.
[21] Michie, S., Stralen, M. M. van, & West, R. (2011). The behaviour change wheel: A new method for characterizing and designing behaviour change interventions. *Implementation Science, 6*(42), 1-11. DOI: 10.1186/1748-5908-6-42.
[22] Field, A. (2013). *Discovering Statistics Using SPSS (4th Edition).* Londen: Sage Publications.

gemiddelde IT-kennis van het personeel hoger is, het bedrijf meer cyberweerbaar is. Ook de sterkte van dit verband is zwak tot gemiddeld.

Het uitvoeren van correlatieanalyses tussen de achtergrondkenmerken en de vier verschillende componenten van cyberweerbaarheid is achterwege gelaten vanwege het beperkte aantal respondenten.

CONCLUSIE EN DISCUSSIE

Het doel van deze pilotstudie was om een eerste beeld te krijgen van de huidige cyberweerbaarheid van mkb-retailers in de regio Den Haag. Omdat het vanuit beleidsperspectief tevens nuttig is om te weten welke factoren de cyberweerbaarheid van het mkb kunnen vergroten, is ook onderzocht welke factoren samenhangen met de cyberweerbaarheid van mkb-retailers.

De resultaten laten zien dat de cyberweerbaarheid van mkb-retailers in de regio Den Haag voor verbetering vatbaar is. Gemiddeld genomen scoren deelnemende mkb'ers net geen voldoende. Het mkb moet kunnen anticiperen op bedreigingen en kansen en deze ook moet kunnen detecteren als ze zich voordoen in de organisatie. Ook moet het mkb adequaat kunnen reageren op incidenten en ook snappen wat er heeft plaatsgevonden zodat ervan kan worden geleerd. Deze studie laat zien dat mkb'ers het best in staat zijn om te reageren op cyberincidenten, maar het minst goed in staat zijn om hiervan te leren. De gevonden resultaten indiceren dat het mkb in de regio Den Haag dus beperkt cyberweerbaar is. Dit is in lijn met de verwachtingen op basis van eerder onderzoek. Zoals gezegd heeft het mkb een tekort aan middelen en kennis om zichzelf goed te beschermen tegen cyberincidenten.[23] Verder heeft de Cybersecuritymonitor 2018[24] uitgewezen dat kleine bedrijven, zoals mkb-retailers, weinig maatregelen nemen om de eigen IT-beveiliging op orde te houden. De resultaten van dit onderzoek zijn met deze uitkomst te rijmen.

Wat betreft achtergrondkenmerken liet de eerder besproken Cybersecuritymonitor verder zien dat een groot gedeelte van de kleine bedrijven überhaupt geen IT-beveiligingsmaatregelen neemt. Ook in dit onderzoek kwam in gesprekken met ondernemers naar voren dat IT-beveiliging vaak geen grote prioriteit heeft. Daarnaast wees de monitor uit dat als mkb'ers IT-beveiligingsmaatregelen nemen dit ongeveer even vaak is uitbesteed aan externe leveranciers als dat het in eigen beheer is. Het huidige onderzoek laat ongeveer een gelijke verhouding zien. Wel valt op dat mkb'ers die hun IT-beveiliging uitbesteden dit regelmatig doen aan vrienden of kennissen. Niet noodzakelijkerwijs hebben deze vrienden of kennissen kennis van IT-beveiliging. Verder laten de resultaten van dit onderzoek zien dat ongeveer de helft van de mkb'ers te maken heeft gehad met cybercriminaliteit. Ook dit resultaat is in lijn met het eerder uitgevoerde landelijke onderzoek. [25]

Een belangrijk doel van dit onderzoek was om te kijken welke factoren samenhangen met de cyberweerbaarheid van mkb- retailers. De resultaten wijzen uit dat een goed (strikt) sanctiebeleid voor

[23] Olsthoorn, S., & Koot, J. (2017). 'Goede cyberbeveiliging te duur voor mkb'er'. *Financieel Dagblad.* Geraadpleegd van https://fd.nl/economie-politiek/1190183/mkb-is-kwetsbaar-voor-hackers
[24] Centraal Bureau voor de Statistiek (2018). *Cybersecuritymonitor 2018.* Den Haag: Centraal Bureau voor de Statistiek. Geraadpleegd van https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018
[25] Notté, R., & Slot, L. (2017). Hoe cybersecure is het mkb? Nulmeting cybersecurity in het mkb. Geraadpleegd van https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf

medewerkers op cyberonveilig gedrag en investeringen in het IT-kennisniveau van het personeel zouden kunnen bijdragen aan het vergroten van de cyberweerbaarheid van het mkb. Overige factoren lijken vooralsnog geen verband te houden met de cyberweerbaarheid. Daarbij moet wel worden opgemerkt dat het gezien de kleine steekproef lastig is om eventuele verbanden te kunnen aantonen.

Dit onderzoek is een pilot en kent dan ook een aantal beperkingen.[26] Een belangrijke beperking is het lage aantal respondenten. Ondanks alle inspanningen door het team van onderzoekers om respondenten te verkrijgen, hebben slechts 56 mkb'ers deelgenomen aan dit onderzoek, een responspercentage van 14,9 procent. Uit het lage responspercentage voor dit onderzoek en uit gesprekken met de ondernemers kan worden afgeleid dat mkb-retailers niet wakker liggen van cyberdreigingen. [27] Computers en internet worden geen belangrijke rol toegeschreven in de dagelijkse bedrijfsvoering. Men ziet dan ook niet altijd het belang in van cyberveiligheid. Mkb'ers zijn soms dan ook moeilijk te overtuigen van het nut van het nemen van maatregelen ter preventie van slachtofferschap. Een interessante richting voor het vervolg van dit onderzoek zou kunnen liggen in het verbeteren van de risicocommunicatie.[28] Risicocommunicatie betekent dat voorlichting wordt geboden en gecommuniceerd wordt over risico's waaraan mensen kunnen blootstaan voordat zich een ramp voordoet, zoals slachtofferschap van cybercriminaliteit.[29] Onderzoek naar effectieve risicocommunicatie voor het mkb omtrent cybercriminaliteit kan mogelijk helpen om deze doelgroep te overtuigen van het belang van cyberveiligheid.

Het geringe aantal respondenten die bovendien vooral zijn gevonden binnen de retail heeft ook gevolgen voor de geldigheid van de resultaten. Die zijn beperkt tot de retail. Met het oog op vervolgonderzoek valt dan ook te denken aan onderzoek naar cyberweerbaarheid bij bedrijven in een ander sector. Dan kunnen uitspraken worden gedaan over hoe de weerbaarheid zich verhoudt tussen sectoren. Bedrijven in andere sectoren, zoals de industrie, hebben mogelijk een grotere afhankelijkheid van ICT voor de bedrijfsvoering dan retailers. Cybercriminaliteit vormt voor deze bedrijven dan ook mogelijk een grotere bedreiging dan voor retailers. De vraag is echter of deze sector dan ook meer cyberweerbaar is. En zo ja, leidt dit dan tot minder incidenten en lagere schade?

Tenslotte lijkt er behoefte te zijn aan concrete handvatten voor mkb'ers om eenvoudig zelf de veiligheid te kunnen vergroten. Er zijn al verschillende stappenplannen te vinden online (zie bijvoorbeeld de Cybersecurity Health Check[30]). Niet altijd is echter duidelijk waarop deze zijn gebaseerd. Een idee voor toekomstig onderzoek is het ontwikkelen van een checklist of stappenplan waarop mkb'ers kunnen vinden hoe zij hun cyberweerbaarheid kunnen vergroten.

[26] Zie ook: Bruin, I. de, & Kleij, R. van der (2018). *Hoe cyberweerbaar zijn mkb retailers in de regio Den Haag? Artikel in voorbereiding.*

[27] Zie ook: Van den Berg, M. & Reijmer, T. (2015). *Cybersecurity in het MKB.* (NB: In opdracht van Interpolis). Verkregen op 15.02.2018 van: https:// www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_ mkb.pdf.

[28] https://www.communicatierijk.nl/vakkennis/r/risico--en-crisiscommunicatie

[29] https://www.ifv.nl/kennisplein/risicocommunicatie

[30] Koninklijk Nederlandse Beroepsorganisatie van Accountants (2018). *Cybersecurity Health Check middelgrote bedrijven.* Geraadpleegd van https://www.nba.nl/globalassets/over-de-nba/pers/2018148_nba-cyber-healt-check_web_nw.pdf

BIJLAGEN

BIJLAGE A: ENQUÊTE

DE HAAGSE HOGESCHOOL CCV centrum voor criminaliteitspreventie en veiligheid Den Haag

Mkb cyberweerbaarheidsscan

Beste mkb'er,

Het Regionaal Samenwerkingsverband Integrale Veiligheid (RSIV), het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), de gemeente Den Haag en de Haagse Hogeschool (HHs) willen u als ondernemer voorzien van inzicht en advies op het gebied van cybersecurity.

Hiertoe vragen wij u om deel te nemen aan een kort vragenlijstonderzoek over cyberweerbaarheid: het vermogen van uw bedrijf om adequaat om te gaan met cyberincidenten.

Op basis van deze scan wordt duidelijk hoe cyberweerbaar u bent en, indien relevant, hoe u meer weerbaar kunt worden. De resultaten van de scan worden medio november plenair gepresenteerd bij u in de buurt. Meer informatie hierover volgt nog.

Het invullen van de vragenlijst zal ongeveer 15 minuten van uw tijd in beslag nemen. Er zal betrouwbaar met uw persoonlijke (bedrijfs)gegevens worden omgegaan. Deze worden niet met derden gedeeld of openbaar gemaakt in wat voor vorm dan ook.

Mocht u nog vragen of opmerkingen hebben over het onderzoek, of kennis willen nemen van uw resultaten, neem dan contact met mij op via r.vanderkleij@hhs.nl.

Alvast hartelijk dank voor uw deelname.

Met vriendelijke groet,

Dr. Rick van der Kleij, Senior onderzoeker Lectoraat Cybersecurity in het mkb, Haagse Hogeschool

Een paar vragen over uw bedrijf :

1) * Waar is uw bedrijf gevestigd? (geef hier uw eigen standplaats)

- ☐ Leidschendam Centrum
- ☐ Huygenskwartier
- ☐ Leidsenhage
- ☐ Julianabaan
- ☐ Den Haag Loosduinse Hoofdplein
- ☐ Den Haag City Center
- ☐ Anders, namelijk ...

2) * Wat is uw huidige functie binnen het bedrijf?

- ☐ Directeur/ eigenaar/ filiaalmanager
- ☐ IT verantwoordelijke
- ☐ Medewerker (iedereen die geen bestuursfunctie heeft/ IT verantwoordelijke is)

3) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Volledig oneens	Oneens	Noch mee oneens, noch mee eens	Eens	Volledig eens
Ik ben bereid om meer moeite te doen dan normaliter wordt verwacht om te helpen dit bedrijf succesvol te maken.	☐	☐	☐	☐	☐
Ik geef veel om het lot van dit bedrijf.	☐	☐	☐	☐	☐
Voor mij is dit het beste bedrijf van alle mogelijke bedrijven om voor te werken.	☐	☐	☐	☐	☐

4) * Hoeveel werknemers werken er (bij benadering) tenminste 15 uur per week voor het bedrijf? Let op : dit is inclusief uzelf!

☐ 1 ☐ 2-5 ☐ 6-10 ☐ 11-50 ☐ 51-100 ☐ 101-249 ☐ 250 of meer

5) * In welke sector is uw bedrijf vooral actief?

- ☐ Handel/ Retail
- ☐ Industrie
- ☐ Horeca
- ☐ Bouwnijverheid
- ☐ Overige zakelijke diensten
- ☐ Vervoer en opslag
- ☐ Informatie en communicatie
- ☐ Anders, namelijk ...
- ☐ Weet niet

6) * Is uw bedrijf een familiebedrijf? (bedrijf waarbij een familie direct of indirect een meerderheid van zeggenschap heeft)

☐ Ja ☐ Nee ☐ Weet niet

7) * Hoe oud is uw bedrijf?

☐ Startend (jonger dan 3 jaar) ☐ Jong (tussen de 3 en 5 jaar) ☐ Gevestigd (ouder dan 5 jaar)

8) * Wat is het gemiddelde IT-kennisniveau van het personeel

- ☐ Heel laag
- ☐ Laag
- ☐ Redelijk laag
- ☐ Gemiddeld
- ☐ Redelijk hoog
- ☐ Hoog
- ☐ Heel hoog

9) * Stelling: De bedrijfsprocessen in mijn bedrijf zijn volledig afhankelijk van computers en internet (ICT)?

- ☐ Volledig oneens
- ☐ Oneens
- ☐ Noch mee oneens, noch mee eens
- ☐ Eens
- ☐ Volledig eens

10) Wat is de jaaromzet van uw bedrijf, in euro´s?

- ☐ 0 tot 100.000 €
- ☐ 100.000 tot 500.000 €
- ☐ 500.000 - 1.000.000 €
- ☐ 1.000.000 tot 2.500.000 €
- ☐ meer dan 2.500.000 €
- ☐ Dat zeg ik liever niet
- ☐ Weet niet

(Onder IT-beveiliging verstaan we de set van technische beveiligingssystemen in de geautomatiseerde bedrijfsomgeving, zoals firewalls en antivirussoftware, het up-to-date houden van software of een *intrusion detection system*. De IT-beveiliging kan in eigen beheer zijn of zijn uitbesteed, bv. aan een commercieel IT-bedrijf of een zelfstandige IT-er)

11) * In welke mate is de IT-beveiliging binnen uw bedrijf uitbesteed?

- ☐ De IT-beveiliging is volledig uitbesteed
- ☐ De IT-beveiliging is deels uitbesteed
- ☐ De IT-beveiliging is volledig in eigen beheer
- ☐ Weet niet

12) * Wat is het jaarlijkse budget voor IT-beveiliging (bij benadering)?

- ☐ Nul: er is geen apart budget voor IT-beveiliging
- ☐ Minder dan 10.000 euro
- ☐ Tussen de 10.000 en 50.000 euro
- ☐ Tussen de 50.000 en 100.000 euro
- ☐ Meer dan 100.000 euro
- ☐ Weet niet

Een paar vragen over cybercriminaliteit :

13) * Heeft uw bedrijf in de afgelopen 12 maanden te maken gehad met de volgende vormen van cybercriminaliteit?

	Ja	Nee	Weet niet
Bedreiging & terrorisme (bedreigen van medewerkers of uw bedrijf door radicale personen of groeperingen)	☐	☐	☐
Denial of Service (DoS)-aanval (digitale aanvallen op het bedrijfssysteem waardoor dit wordt overbelast en niet meer beschikbaar is, bv. het platleggen van de website van uw bedrijf)	☐	☐	☐
Defacing (het veranderen, bekladden, vernielen of vervangen van de website van uw bedrijf)	☐	☐	☐
Diefstal van gegevens of spionage (bv. van vertrouwelijke informatie of persoonsgegevens van klanten)	☐	☐	☐
Digitale afpersing (het moeten afgeven van geld of goederen door dreiging met smaad of openbaarmaking van gevoelige informatie)	☐	☐	☐
Digitale fraude of oplichting (waarbij goederen of gegevens via nietsvermoedende medewerkers afhandig zijn gemaakt)	☐	☐	☐
Hacking (inbraak op het computersysteem van uw bedrijf)	☐	☐	☐
Identiteitsmisbruik via internet (het misbruik maken van identiteitsgegevens van uw bedrijf, bv. om producten of diensten te verkrijgen of een creditcard te bestellen op de naam van het bedrijf)	☐	☐	☐
Ongeautoriseerd misbruik van het bedrijfsnetwerk (bv. voor het downloaden of verspreiden van illegale software of spam)	☐	☐	☐
Phishing (bv. via email informatie ontfutselen)	☐	☐	☐
Ransomware (een programma dat de computer blokkeert en vervolgens de gebruiker geld vraagt om de computer weer te 'bevrijden')	☐	☐	☐
Skimming (het aanpassen van het pinapparaat van uw bedrijf)	☐	☐	☐
Smaad of laster via internet (het opzettelijk aantasten van de goede naam van uw bedrijf)	☐	☐	☐
Vernieling van digitale gegevens (het opzettelijk vernielen of ontoegankelijk maken van gegevens)	☐	☐	☐
Virussen (een virus kan gevoelige informatie wissen en verspreiden of je computer onklaar maken)	☐	☐	☐

Cyberonveilig handelen kan aan de basis liggen van een cyberincident, zoals het klikken door een medewerker op een link in een zogenaamde phishing email of het nalaten van het updaten van software, waardoor virussen op het bedrijfsnetwerk kunnen komen.

14) Hoe groot is het percentage cyberincidenten dat is veroorzaakt, direct of indirect, door nalatigheid of het risicovol handelen van een medewerker binnen uw bedrijf ?

☐ 0 ☐ 10 ☐ 20 ☐ 30 ☐ 40 ☐ 50 ☐ 60 ☐ 70 ☐ 80 ☐ 90 ☐ 100

15) Indien uw bedrijf te maken heeft gehad met cybercriminaliteit, heeft uw bedrijf schade opgelopen, bv. financiele schade, reputatieschade of tijdverlies?

☐ Ja ☐ Nee ☐ Weet niet

16) Indien ja, wat voor soort schade betrof dit (meerdere antwoorden mogelijk)?

☐ Geld gestolen/ financiële schade
☐ Bedrijfsgegevens gestolen/ vernietigd
☐ Bedrijfsprocessen lagen stil/ tijdverlies
☐ Imago- of reputatieschade
☐ Juridische en/of contractuele schade
☐ Anders, namelijk ...

17) Indien uw bedrijf te maken heeft gehad met cybercriminaliteit, heeft uw bedrijf hiervan aangifte of melding gedaan bij een instantie, zoals bij de politie of een meldpunt?

☐ Ja ☐ Nee ☐ Weet niet

18) Indien ja, bij wie? (bv. de Fraudehelpdesk.nl, politie, Meld misdaad anoniem, bank, etc.)

_____

De volgende stellingen gaan over de manier waarop uw bedrijf, het management en de medewerkers *rekening houden met toekomstige ontwikkelingen* op het gebied van cybercriminaliteit.

19) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Volledig oneens	Grotendeels oneens	Lichtelijk oneens	Lichtelijk eens	Grotendeels eens	Volledig eens	Geen idee
Medewerkers in ons bedrijf weten hoe ze cybercriminaliteit op het werk kunnen voorkomen	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf zijn slecht voorbereid op een aanval door cybercriminelen	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf zijn goed op de hoogte van de laatste ontwikkelingen die van invloed zijn op de digitale veiligheid op het werk	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf heeft een cultuur gericht op het voorkomen van cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf heeft de cyberbeveiligingsrollen en -verantwoordelijkheden eenduidig vastgesteld	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf neemt maatregelen om te zorgen dat ons werk is beschermd tegen cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf zoekt actief naar kansen op een betere bescherming tegen cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf heeft duidelijk cyberbeveiligingsbeleid	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf vinden cyberbeveiliging maar onzin	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf vinden het belangrijk om cybercriminaliteit te voorkomen	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf maken zich zorgen om cybercriminaliteit op het werk	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf hebben de neiging om het risico op cybercriminaliteit te onderschatten	☐	☐	☐	☐	☐	☐	☐

De volgende stellingen gaan over de manier waarop uw bedrijf, het management en medewerkers de omgeving en eigen bedrijfsprocessen *monitoren* teneinde cyberrisico's en kwetsbaarheden in een vroeg stadium te detecteren

20) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Volledig oneens	Grotendeels oneens	Lichtelijk oneens	Lichtelijk eens	Grotendeels eens	Volledig eens	Geen idee
Medewerkers in ons bedrijf weten hoe ze cybercriminaliteit kunnen herkennen	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf zijn vaardig in het detecteren van cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf weten hoe zij cybercriminaliteit moeten melden	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf hoeven niet te rekenen op waardering als zij een cyberaanval opmerken	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf hebben goed zicht op hoe anderen in de organisatie omgaan met een cyberaanval	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf heeft duidelijke normen voor wat cybercriminaliteit is en wat niet	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf stimuleert medewerkers in het onderling delen van informatie over cyberbeveiliging en -criminaliteit	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf zijn gemakzuchtig in het melden van kwetsbaarheden in de cyberbeveiliging	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf vinden het belangrijk dat de veiligheidsvoorschriften rondom cyberbeveiliging worden opgevolgd	☐	☐	☐	☐	☐	☐	☐
Medewerkers in het bedrijf vinden het belangrijk om te weten hoe ze cybercriminaliteit kunnen herkennen	☐	☐	☐	☐	☐	☐	☐

De volgende stellingen gaan over de manier waarop uw bedrijf, het management en medewerkers *reageren* op cybercriminaliteit

21) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Volledig oneens	Grotendeels oneens	Lichtelijk oneens	Lichtelijk eens	Grotendeels eens	Volledig eens	Geen idee
Medewerkers in ons bedrijf kunnen goed omgaan met een verstoring in hun normale werkprocessen	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf weten wat ze moeten doen in het geval van cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf hebben een duidelijk beeld van hun rol in geval van een aanval door cybercriminelen	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf heeft heldere voorschriften over hoe om te gaan met verstoringen in de bedrijfsvoering als gevolg van cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf biedt assistentie (bv. in de vorm van een helpdesk) in het geval cybercriminaliteit heeft plaatsgevonden	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf houdt voorschriften up-to-date over hoe om te gaan met cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf geeft de bestrijding van cybercriminaliteit een hoge prioriteit	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf zijn bang om anderen om hulp te vragen bij het oplossen van de gevolgen van cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf vinden de bestrijding van cybercriminaliteit belangrijk	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf vinden het belangrijk om cybercriminaliteit altijd direct te rapporteren	☐	☐	☐	☐	☐	☐	☐

De volgende stellingen gaan over het vermogen van uw bedrijf, het management en medewerkers om te *leren* van ervaringen met cybercriminaliteit.

22) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Volledig oneens	Grotendeels oneens	Lichtelijk oneens	Lichtelijk eens	Grotendeels eens	Volledig eens	Geen idee
Medewerkers in ons bedrijf zijn goed in het vinden van oplossingen voor problemen door cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf zijn op de hoogte van cybercriminaliteit zoals die in het verleden heeft plaatsgevonden binnen het bedrijf	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf zijn door schade en schande wijs geworden op het gebied van cyberbeveiliging	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf informeert de medewerkers regelmatig over hoe om te gaan met cybercriminaliteit, bv in de vorm van nieuwsbrieven, berichten op het intranet, lezingen of trainingen	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf test regelmatig de procedures, taken en verantwoordelijkheden over hoe om te gaan met cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf houdt bij wat de effecten zijn van maatregelen gericht op het voorkomen van cybercriminaliteit	☐	☐	☐	☐	☐	☐	☐
Ons bedrijf traint medewerkers regelmatig in cyberbeveiliging	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf vinden het beoefenen van een cybercrises maar onzin	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf zijn bereid om deel te nemen aan trainingen en oefeningen op het gebied van cyberbeveiliging	☐	☐	☐	☐	☐	☐	☐
Medewerkers in ons bedrijf nemen regelmatig de tijd om na te denken over wat goed gaat en wat beter kan met betrekking tot hun cyberveiligheid	☐	☐	☐	☐	☐	☐	☐

23) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Heel onwaarschijnlijk	Onwaarschijnlijk	Noch onwaarschijnlijk, noch waarschijnlijk	Waarschijnlijk	Heel waarschijnlijk
Hoe waarschijnlijk is het dat een incident op het gebied van cyberbeveiliging in uw bedrijf tot een productieverlies zal leiden?	☐	☐	☐	☐	☐
Hoe waarschijnlijk is het dat een incident op het gebied van cyberbeveiliging in uw bedrijf tot een financieel verlies zal leiden?	☐	☐	☐	☐	☐
Hoe waarschijnlijk is het dat het bedrijf gevoelige informatie kan verliezen als gevolg van een incident op het gebied van cyberbeveiliging?	☐	☐	☐	☐	☐

24) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Volledig oneens	Oneens	Noch mee oneens, noch mee eens	Eens	Volledig eens
Ik vind dat ons bedrijf kwetsbaar is voor cyberaanvallen	☐	☐	☐	☐	☐
Ik vind dat de productiviteit van ons bedrijf wordt bedreigd door cyberaanvallen	☐	☐	☐	☐	☐
Ik vind dat de winstgevendheid van ons bedrijf wordt bedreigd door cyberaanvallen	☐	☐	☐	☐	☐

25) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Volledig oneens	Oneens	Noch mee oneens, noch mee eens	Eens	Volledig eens
Mijn organisatie legt zware straffen op aan medewerkers die regels omtrent cyberbeveiliging breken	☐	☐	☐	☐	☐
Mijn organisatie beëindigt het contract van medewerkers die regels omtrent cyberbeveiliging regelmatig breken	☐	☐	☐	☐	☐
De werkzaamheden van medewerkers worden uitstekend gecontroleerd op schendingen van cyberbeveiligingsbeleid	☐	☐	☐	☐	☐
Medewerkers die het cyberbeveiligingsbeleid schenden lopen een grote kans om te worden betrapt	☐	☐	☐	☐	☐

26) * Geef telkens aan in welke mate u het eens bent met de betreffende stelling:

	Volledig oneens	Oneens	Noch mee oneens, noch mee eens	Eens	Volledig eens
Ik deel regelmatig mijn kennis over cyberbeveiliging met mijn collega's om het risico omtrent cyberincidenten te verkleinen.	☐	☐	☐	☐	☐
Ik neem deel aan activiteiten gericht op kennisdeling over cyberbeveiliging.	☐	☐	☐	☐	☐
Ik denk dat het delen van kennis over cyberbeveiliging mij helpt om het nut van het cyberbeveiligingsbeleid binnen mijn bedrijf beter te begrijpen.	☐	☐	☐	☐	☐
Ik denk dat het delen van kennis over cyberbeveiliging een effectieve manier is om het risico op schendingen van het cyberbeveiligingsbeleid te verkleinen.	☐	☐	☐	☐	☐
Ik denk dat het delen van kennis over informatiebeveiliging waardevol is binnen bedrijven.	☐	☐	☐	☐	☐

27) * Hoe groot schat u de kans (in procenten) dat een mkb-bedrijf in Nederland in een periode van 12 maanden slachtoffer wordt van cybercrime (pogingen niet meegerekend)?

☐ 0 ☐ 10 ☐ 20 ☐ 30 ☐ 40 ☐ 50 ☐ 60 ☐ 70 ☐ 80 ☐ 90 ☐ 100

28) * Hoe groot schat u de kans (in procenten) dat uw bedrijf in een periode van 12 maanden zelf slachtoffer wordt van cybercrime (pogingen niet meegerekend)?

☐ 0 ☐ 10 ☐ 20 ☐ 30 ☐ 40 ☐ 50 ☐ 60 ☐ 70 ☐ 80 ☐ 90 ☐ 100

29) * Wat is de naam van uw bedrijf ?

(nb. Deze vraag is voor administratieve doeleinden en wordt niet meegenomen in de verdere analyse)

_____

Als u naar aanleiding van deze enquête contact met ons wilt of de resultaten wilt ontvangen; laat dan hieronder aanvullende gegevens achter, zoals uw emailadres. Deze gegevens worden op geen enkele wijze gekoppeld aan uw antwoorden.

Als dit een testinvulling betreft door een medewerker van het projectteam dan gelieve dat hier te vermelden.

30) Heeft u nog opmerkingen?

_____

BIJLAGE B: FACTSHEET

Hoe cyberweerbaar zijn mkb-retailers?

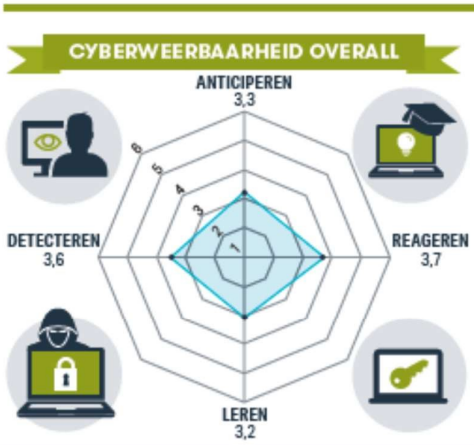
Regio Den Haag

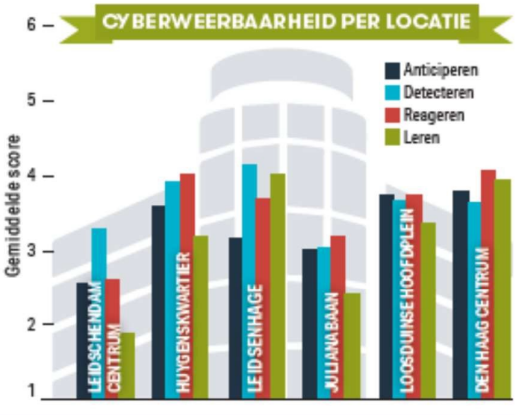
Wat is cyberweerbaarheid?

Cyberweerbaarheid is het vermogen van het mkb om weerstand te bieden tegen bekende en onbekende vormen van cybercriminaliteit en snel te herstellen van een cybercrisis. Dit betekent dat het mkb in staat moet zijn om te anticiperen op bedreigingen en kansen en deze ook moet kunnen detecteren als deze zich voordoen in de organisatie. Ook moet het mkb adequaat kunnen reageren op incidenten en begrijpen wat er heeft plaatsgevonden zodat ervan kan worden geleerd.

Cyberweerbaarheid gemeten

Cyberweerbaarheid is gemeten met behulp van een vragenlijst met stellingen. Een voorbeeld van een stelling is: 'Medewerkers in ons bedrijf vinden de bestrijding van cybercriminaliteit op het werk belangrijk'. Hoe hoger een bedrijf scoort op deze stellingen, hoe meer cyberweerbaar het bedrijf is. De score loopt van 1 tot en met 6 punten per stelling. De gemiddelde score voor cyberweerbaarheid is 3,46. Het mkb scoort het hoogst op 'reageren' en het laagst op 'leren'.





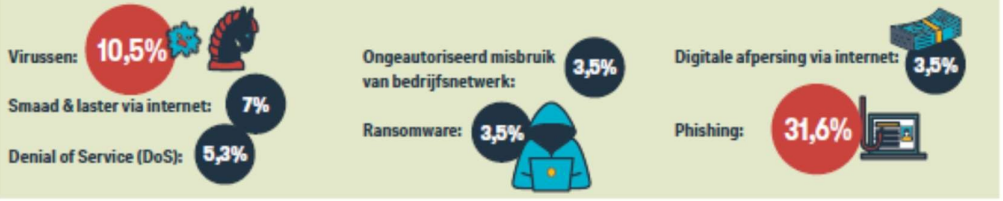
Onderzoeksopzet en respons

In september en oktober 2018 heeft De Haagse Hogeschool in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een pilotonderzoek uitgevoerd in opdracht van de gemeente De Haag bij mkb-retailers.

Hiermee is een eerste beeld opgehaald over de cyberweerbaarheid van mkb retailers in 6 winkelgebieden in Den Haag en omstreken. In totaal hebben 57 leidinggevenden uit 56 bedrijven een enquête ingevuld.

DE HAAGSE HOGESCHOOL

De volgende cyberdelicten kwamen het meest voor bij de 56 mkb-bedrijven



Slachtofferschap van cybercrime

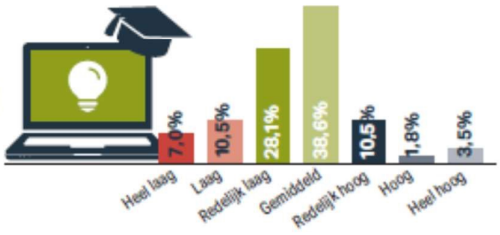
Bijna de helft (48 %) van de retailers geeft aan slachtoffer te zijn geweest van cybercriminaliteit in de laatste 12 maanden. Zeven bedrijven (12 %) hebben ook daadwerkelijk schade hiervan ondervonden. Schade als gevolg van cybercriminaliteit kan zich op verschillende vlakken voordoen. Zo kan een bedrijf financiële schade oplopen. Ook kunnen belangrijke bedrijfsgegevens gestolen of vernietigd zijn. Schade kan ook bestaan uit tijdverlies, doordat de bedrijfsprocessen tijdelijk stilliggen. Daarnaast kan een bedrijf imagoschade oplopen.

Sanctiebeleid cyberonveilig gedrag

In het onderzoek is ook gevraagd naar het sanctiebeleid dat de mkb-retailers voeren op cyberonveilig handelen van medewerkers. Een sanctiebeleid verschaft duidelijkheid over wat wel of niet wordt geaccepteerd binnen een bedrijf en welke maatregelen er kunnen worden getroffen indien een werknemer zich cyber-onveilig gedraagt. Wat blijkt? Hoe strikter het sanctiebeleid van een bedrijf, hoe méér cyber-weerbaar het bedrijf is.

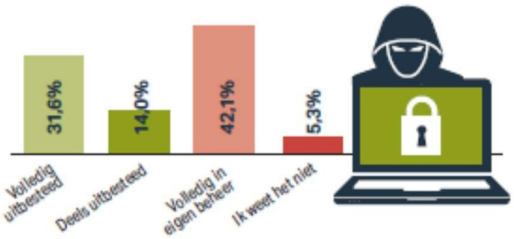
Gemiddelde IT-kennis personeel

Naarmate de gemiddelde IT-kennis van het personeel hoger is, is een mkb-bedrijf ook méér cyberweerbaar.



Bedrijfsprocessen afhankelijk van ICT?

Is de IT-beveiliging uitbesteed?



Conclusies

Dit onderzoek laat zien dat de cyberweerbaarheid van de mkb-retailers in de regio Den Haag omhoog kan. Vooral het vermogen om te leren van cyberincidenten kan worden versterkt. IT-kennis van het personeel en een strikt sanctiebeleid op cyber onveilig gedrag kunnen bijdragen aan meer cyberweerbaarheid van het mkb.

Contact:

Dr. Rick van der Kleij
Lectoraat Cybersecurity in het mkb
De Haagse Hogeschool

@ r.vanderkleij@hhs.nl

DE HAAGSE HOGESCHOOL

BIJLAGE C: TABELLEN

Tabel C1. Respons per winkelgebied

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Leidschendam Centrum	7	12,3	12,3	12,3
	2 Huygenskwartier	14	24,6	24,6	36,8
	3 Leidsenhage	4	7,0	7,0	43,9
	4 Julianabaan	10	17,5	17,5	61,4
	5 Den Haag Loosduinse Hoofdplein	10	17,5	17,5	78,9
	6 Den Haag City Center	12	21,1	21,1	100,0
	Total	57	100,0	100,0	

De percentages uit de tabel komen niet volledig overeen met de percentages die zijn gepresenteerd in de tekst. Zoals gezegd heeft één mkb de enquête door twee personen in laten vullen. Bij het projectteam was bekend om welk bedrijf dit ging en in welk winkelgebied dit bedrijf is gelegen. Met deze informatie is rekening gehouden bij het presenteren van de resultaten in de lopende tekst.

Tabel C2. Respons per sector

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Handel/ Retail	33	57,9	62,3	62,3
	3 Horeca	4	7,0	7,5	69,8
	5 Overige zakelijke diensten	2	3,5	3,8	73,6
	8 Weet niet	1	1,8	1,9	75,5
	9 Anders, namelijk	13	22,8	24,5	100,0
	Total	53	93,0	100,0	
Missing	-99	4	7,0		
Total		57	100,0		

Tabel C3. Aantal werknemers (dat minstens vijftien uur per week werkt)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 1	8	14,0	14,0	14,0
	2 2-5	27	47,4	47,4	61,4
	3 6-10	12	21,1	21,1	82,5
	4 11-50	9	15,8	15,8	98,2
	5 51-100	1	1,8	1,8	100,0
	Total	57	100,0	100,0	

Tabel C4. Afhankelijkheid bedrijfsprocessen van ICT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Volledig oneens	7	12,3	12,5	12,5
	2 Oneens	13	22,8	23,2	35,7
	3 Noch mee oneens, noch mee eens	12	21,1	21,4	57,1
	4 Eens	14	24,6	25,0	82,1
	5 Volledig eens	10	17,5	17,9	100,0
	Total	56	98,2	100,0	
Missing	-99 n.v.t. of missing	1	1,8		
Total		57	100,0		

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Afh_bedrijfsprocessen_ICT Stelling: De bedrijfsprocessen in mijn bedrijf zijn volledig afhankelijk van computers en internet (ICT)?	56	1	5	3,13	1,308
Valid N (listwise)	56				

Tabel C5. Beheer van de IT-beveiliging

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 De IT-beveiliging is volledig uitbesteed	18	31,6	34,0	34,0
	2 De IT-beveiliging is deels uitbesteed	8	14,0	15,1	49,1
	3 De IT-beveiliging is volledig in eigen beheer	24	42,1	45,3	94,3
	4 Weet niet	3	5,3	5,7	100,0
	Total	53	93,0	100,0	
Missing	-99 n.v.t. of missing	4	7,0		
Total		57	100,0		

Tabel C6. Gemiddelde IT-kennis van het personeel

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Heel laag	4	7,0	7,0	7,0
	2 Laag	6	10,5	10,5	17,5
	3 Redelijk laag	16	28,1	28,1	45,6
	4 Gemiddeld	22	38,6	38,6	84,2
	5 Redelijk hoog	6	10,5	10,5	94,7
	6 Hoog	1	1,8	1,8	96,5
	7 Heel hoog	2	3,5	3,5	100,0
	Total	57	100,0	100,0	

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Gem_IT_kennis_niveau Wat is het gemiddelde IT-kennisniveau van het personeel	57	1	7	3,54	1,283
Valid N (listwise)	57				

Tabel C7. Percentage mkb-bedrijven dat in de afgelopen twaalf maanden te maken heeft gehad met verschillende cyberdelicten

Bedreiging & terrorisme		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	1	1,8	1,8	1,8
	2 Nee	50	87,7	87,7	89,5
	3 Weet niet	6	10,5	10,5	100,0
	Total	57	100,0	100,0	
DoS-aanval (Denial of Service)		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	3	5,3	5,3	5,3
	2 Nee	48	84,2	84,2	89,5
	3 Weet niet	6	10,5	10,5	100,0
	Total	57	100,0	100,0	
Defacing		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	1	1,8	1,8	1,8
	2 Nee	50	87,7	87,7	89,5
	3 Weet niet	6	10,5	10,5	100,0
	Total	57	100,0	100,0	

Digitale fraude of oplichting		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	1	1,8	1,8	1,8
	2 Nee	48	84,2	84,2	86,0
	3 Weet niet	8	14,0	14,0	100,0
	Total	57	100,0	100,0	

Hacking		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	1	1,8	1,8	1,8
	2 Nee	46	80,7	80,7	82,5
	3 Weet niet	10	17,5	17,5	100,0
	Total	57	100,0	100,0	

Identiteitsmisbruik via internet		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	1	1,8	1,8	1,8
	2 Nee	49	86,0	86,0	87,7
	3 Weet niet	7	12,3	12,3	100,0
	Total	57	100,0	100,0	

Ongeautoriseerd misbruik van het bedrijfsnetwerk		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	2	3,5	3,5	3,5
	2 Nee	45	78,9	78,9	82,5
	3 Weet niet	10	17,5	17,5	100,0
	Total	57	100,0	100,0	

Phishing		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	18	31,6	31,6	31,6
	2 Nee	30	52,6	52,6	84,2
	3 Weet niet	9	15,8	15,8	100,0
	Total	57	100,0	100,0	

Ransomware		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	2	3,5	3,5	3,5
	2 Nee	49	86,0	86,0	89,5
	3 Weet niet	6	10,5	10,5	100,0
	Total	57	100,0	100,0	

Skimming		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	0	0	0	0
	2 Nee	51	89,5	89,5	89,5
	3 Weet niet	6	10,5	10,5	100,0
	Total	57	100,0	100,0	

Smaad/laster via internet		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	4	7,0	7,0	7,0
	2 Nee	46	80,7	80,7	87,7
	3 Weet niet	7	12,3	12,3	100,0
	Total	57	100,0	100,0	
Vernieling van digitale gegevens		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	1	1,8	1,8	1,8
	2 Nee	49	86,0	86,0	87,7
	3 Weet niet	7	12,3	12,3	100,0
	Total	57	100,0	100,0	
Virussen		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	6	10,5	10,5	10,5
	2 Nee	39	68,4	68,4	78,9
	3 Weet niet	12	21,1	21,1	100,0
	Total	57	100,0	100,0	
Digitale afpersing		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	2	3,5	3.5	3,5
	2 Nee	50	87,8	87,8	91,3
	3 Weet niet	5	8,7	8,7	100,0
	Total	57	100,0	100,0	
Diefstal van gegevens/ spionage		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 Ja	2	3,5	3.5	3,5
	2 Nee	50	87,8	87,8	91,3
	3 Weet niet	5	8,7	8,7	100,0
	Total	57	100,0	100,0	

Tabel C8. Cyberweerbaarheid per vermogen

	N	Minimum	Maximum	Gemiddelde	Standaarddeviatie
Anticiperen	53	1,73	5,75	3,3352	1,00346
Detecteren	49	1,00	6,00	3,5709	1,11909
Reageren	49	1,43	6,00	3,7416	1,16314
Leren	48	1,40	5,67	3,1689	1,25875
Totale score	54	1,86	5,61	3,4577	0,98873