VAN THEORIE NAAR PRAKTIJK

DE GELEERDE LESSEN VAN 4 JAAR ONDERZOEK NAAR CYBERSECURITY IN HET MKB

Rutger Leukfeldt

nscr Nederlands Studiecentrum Criminaliteit en Rechtshandhaving

DE HAAGSE HOGESCHOOL

VAN THEORIE NAAR PRAKTIJK

DE GELEERDE LESSEN VAN 4 JAAR ONDERZOEK NAAR CYBERSECURITY IN HET MKB

Rutger Leukfeldt

Voorwoord

Voor u ligt een boek met een overzicht van de vele onderzoeken die zijn uitgevoerd door onderzoekers van het lectoraat cybersecurity in het mkb in de periode 2017-2021.

Doel van dit boek is om een overzicht te bieden van de belangrijkste resultaten van deze onderzoeken. Welke kennis hebben we opgedaan over slachtofferschap, daderschap, cyberweerbaarheid en de aanpak van cybercrime?

Normaal gesproken wordt een dergelijke terugblik geschreven als een onderzoeksprogramma stopt. Dat is nu niet het geval. Integendeel, er is overduidelijk nog genoeg te doen op dit thema en we werken de komende jaren hard door om nog meer relevante kennis op te doen en te delen. We gebruiken dit overzichtswerk dan ook vooral om te evalueren. Welke thema's binnen de onderzoeksagenda zijn onderbelicht gebleven, waar moeten we de komende jaren extra op inzetten en moet het onderzoeksprogramma worden bijgesteld?

Vooral ook is dit een hele feestelijke uitgave. Het laat zien hoe enorm veel werk er de afgelopen jaren is verricht. Ik ben dan ook heel erg trots op al onze onderzoekers en de vele samenwerkingen die we hebben met andere onderzoeksgroepen, het onderwijs en praktijkpartners. Ik ben dan ook veel personen dank verschuldigd. Te veel om hier op te sommen. Hopelijk doe ik iedereen recht door bij afgeronde onderzoeken alle relevante referenties op te nemen en bij lopende onderzoeken de betrokken onderzoekers, samenwerkingspartners en financiers te benoemen.

Dit boek bestaat uit drie delen. Deel 1 gaat over de belofte die ik deed toen ik werd aangesteld als lector en dit onderzoeksprogramma ontwikkelde. Deel 2 bevat de belangrijkste uitkomsten van afgeronde onderzoeken. De vier onderzoekslijnen staan hierbij centraal: de aard en omvang van slachtofferschap, de aard van cybercriminaliteit, cyberweerbaarheid en de aanpak van cybercrime. Voor de goede orde: niets in deze uitgave is dus nieuw. Het bevat de belangrijkste uitkomsten van al gepubliceerd werk. Een uitzondering vormt het laatste deel van dit boek. Dat deel bevat namelijk een korte vooruitblik: waar gaan we ons de komende jaren op richten?

Rutger Leukfeldt

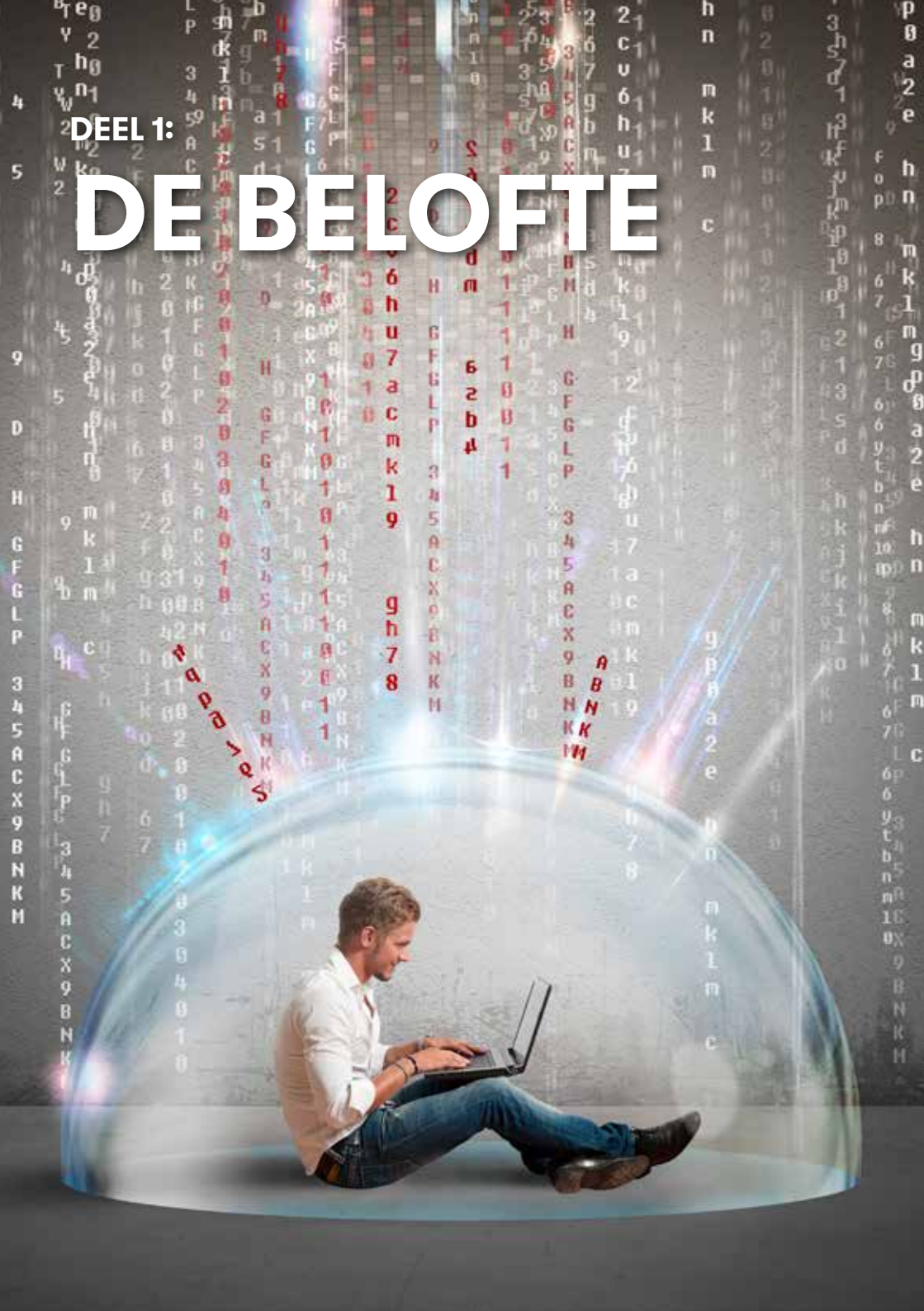
DE HAAGSE HOGESCHOOL

Johanna Westerdijkplein 75
2521 EH Den Haag
www.dehaagsehogeschool.nl

2021. Dit is een publicatie van De Haagse Hogeschool, Nederland.

Ontwerp: Afdeling Onderwijs, Kennis & Communicatie, De Haagse Hogeschool.

INHOUDSOPGAVE


DEEL 1:
DE BELOFTE

De belofte

In mijn intreerede maakte ik deze twee observaties die ten grondslag liggen aan ons onderzoeksprogramma:

> *"Cybercrime – en daarmee cybersecurity – is een groot maatschappelijk probleem. De criminologische bestudering van cybercrime staat nog in de kinderschoenen. Het is echter niet alleen noodzakelijk om goed wetenschappelijk onderzoek uit te voeren ('de lange termijn'), maar om ook met de praktijk de acute problemen en uitdagingen van vandaag en morgen te onderzoeken."*

> *"Het merendeel van het onderzoek op dit gebied – en dan heb ik het over zowel fundamenteel wetenschappelijk als praktijkgericht onderzoek – komt tot nu toe uit de hoek van de technische wetenschappen. Technologie speelt natuurlijk ook een belangrijke rol bij cyberincidenten, maar we hebben het over mensen die cyberaanvallen uitvoeren, mensen die – wetend of onwetend – meewerken aan die cyberaanvallen, mensen die slachtoffer worden en mensen die zich bezig-houden met het tegenhouden van cyberaanvallen."*

De constatering dat onderzoek naar de menselijke factor binnen cyber-crime en cybersecurity nog in de kinderschoenen staat, terwijl er een grote vraag is naar evidence-based praktisch toepasbare kennis is de reden dat De Haagse Hogeschool (HHs) en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) de handen ineengeslagen hebben voor de totstandkoming van dit lectoraat.

Het lectoraat richt zich daarbij op een specifieke doelgroep: het midden- en kleinbedrijf (mkb). Het mbk is de backbone van de Nederlandse economie. Mkb'ers worden echter relatief vaak slachtoffer van cyberaanvallen en hebben niet de capaciteit om zich te weren tegen dergelijke aanvallen. Dit staat in schril contrast met het onderzoek dat wordt uitgevoerd op dit gebied. Onderzoek naar deze doelgroep ontbreekt bij de start van dit lectoraat nagenoeg compleet.

Het doel van het lectoraat is om de kennispositie van het mkb op het gebied van cybercrime en cybersecurity te vergroten om zo het slachtofferschap en de impact van cyberaanvallen onder mkb'ers te verlagen.

Omdat er nagenoeg geen studies zijn gedaan naar cybersecurity in het mkb zullen eerst basale vragen beantwoord moeten worden. Zo is inzicht nodig in slachtofferschap onder mkb'ers. Hoe vaak komen aanvallen op mkb bedrijven voor? Welke mkb bedrijven worden slachtoffer van cyberaanvallen en zijn er factoren die risicoverhogend of risicoverlagend werken? Wat is de werkwijze van criminelen? En van welke zwakke plekken maken criminelen gebruik om hun aanvallen uit te voeren?

Tegelijkertijd moet worden onderzocht hoe mkb'ers zichzelf weerbaarder kunnen maken. Weten mkb'ers welke risico's ze lopen, hoe ze aanvallen kunnen detecteren en afslaan? Welke factoren beïnvloeden de weerbaarheid? Welke interventiemogelijkheden zijn er om de weerbaarheid te verhogen? De bescherming van het mkb tegen cyberaanvallen ligt echter niet alleen bij het mkb zelf. Ook andere partijen hebben hierbij een rol. Daarom moet onderzocht worden welke rol politie en justitie nog hebben bij de aanpak van cybercrime gericht op het mkb.

Leukfeldt, E.R. (2018) De 'human' factor in cybersecurity (inaugural speech). Den Haag: Haagse Hogeschool.

Het lectoraat kent ook vier onderzoekslijnen, waarbinnen steeds het mkb centraal staat:

1. aard en omvang van slachtofferschap;
2. aard van cybercriminaliteit;
3. cyberweerbaarheid;
4. de aanpak van cybercriminaliteit.

DEEL 2:

DE RESULTATEN

ONDERZOEKSLIJN 1:

AARD EN OMVANG VAN SLACHTOFFERSCHAP

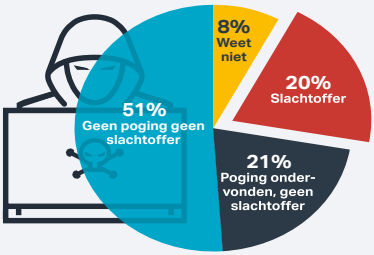
Nulmeting cybersecurity in het mkb: slachtofferschap en risicofactoren

Dit onderzoek biedt inzicht in de stand van zaken met betrekking tot cybersecurity en slachtofferschap van online criminaliteit in het mkb. Deze studie zet een eerste stap door een beeld te schetsen van de cybersecurity in 799 Nederlandse midden-klein-bedrijven.

Slachtofferschap

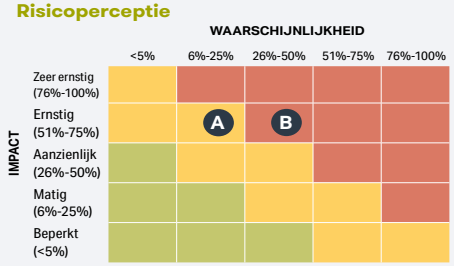
Eén op de vijf onderzochte bedrijven (19,4%) geeft aan een cyber incident te hebben ervaren, waarvan zij schade hebben ondervonden. In slachtofferschap is onderscheid gemaakt tussen slachtofferschap van cybercrime (17,9%) en gedigitaliseerde criminaliteit (8,8%).

Slachtoffers van cybercrime



Bedrijven met meer dan **50 medewerkers** zijn significant vaker slachtoffer van een cybercrime (**39,1%** van deze groep), dan bedrijven met **10 a 50 medewerkers** (**21,8%** van deze groep) en bedrijven met minder dan **10 medewerkers** (**15,1%** van deze groep).

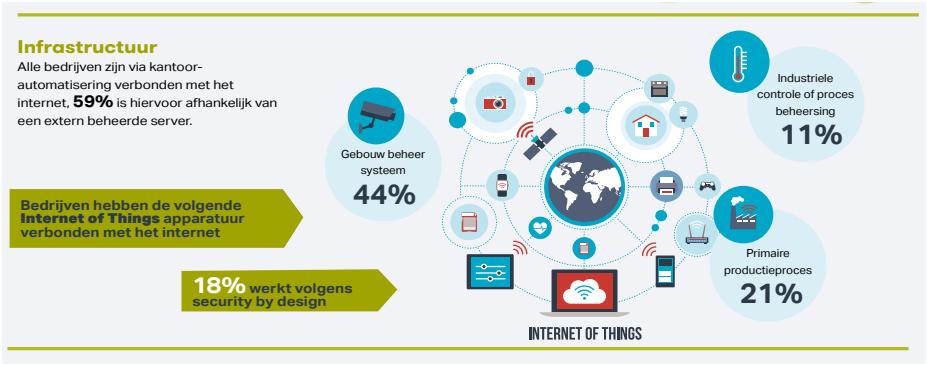
Risicoperceptie



Impact: Voor 62% is het bedrijf volledig afhankelijk van IT.
Waarschijnlijkheid is de kans dat
- *uw bedrijf* komend jaar slachtoffer wordt van een cybercrime: 20% A
- een *soortgelijk bedrijf* komend jaar slachtoffer wordt van een cybercrime 41% B

Risico

Het aantal medewerkers van een bedrijf hangt samen met slachtofferschap van online criminaliteit. Bedrijven met minder dan 10 medewerkers (15%) zijn minder vaak slachtoffer dan bedrijven met 10 à 50 (22%) of meer dan 50 (39%) medewerkers. Sommige ICT gedragingen of apparatuur hangen eveneens samen met slachtofferschap en kunnen als risicovol worden benoemd. Het hebben van IoT apparatuur dat is verbonden aan het bedrijfsnetwerk correleert met slachtofferschap, ditzelfde geldt voor het toestaan dat alle medewerkers toegang hebben tot alle bedrijfsinformatie en ten slotte toestaan dat gasten via de Wi-Fi verbinding kunnen maken met het bedrijfsnetwerk.



Hulpbehoefte

Een van de doelstellingen van het lectoraat is mkb-bedrijven weerbaarder te maken tegen online risico's en daardoor de schade van online criminaliteit te verkleinen. Hiervoor is het van belang om een koppeling te maken tussen onderzoeksresultaten en praktisch toepasbare initiatieven voor het mkb. Essentieel hiervoor is inzicht in wat de behoefte is van mkb'ers..

Een overgrote meerderheid van de respondenten geeft aan geïnteresseerd te zijn in deze hulp (88,4%). Bedrijven geven aan het meeste geholpen te zijn met informatie, enerzijds passief in de vorm van voorlichting of een (digitale) cursus, anderzijds actief in de vorm van een online of telefonische vraagbaak. Midden-kleine bedrijven geven nog vaker aan geholpen te zijn met voorlichting (77,4%) dan micro bedrijven (53,0%). Daarnaast bestaat er ook een grote wens naar, met name gratis, tooling en expert hulp in de vorm van een bedrijfsanalyse of een penetratietest. Micro bedrijven geven vaker aan geholpen te zullen zijn met gratis tools (55,2% versus 28,2%/27,5%), kleine en middenkleine bedrijven verlangen vaker een penetratietest (46,4%/50% versus 25,6%), een bedrijfsanalyse (40,6%/47,7% versus 18,6%), een expertgesprek (20,3%/29,5% versus 7%).

Notté, R.J., L. Slot, S. van 't Hoff-de Goede & E.R. Leukfeldt (2019) Cybersecurity in het mkb. Nulmeting. Den Haag: De Haagse Hogeschool.

Whatsappfraude in Nederland

Mensen die **geen** geld overmaakten werden bijvoorbeeld wantrouwig doordat **de oplichter vroeg om geld (49%), door opvallend taalgebruik (36%), omdat er haast bij was (33%), omdat de oplichter zich voordeed als een onbekend familielid/vriend (27%), of omdat de oplichter niet kon bellen of langskomen (18%)**.

Van 't Hoff-de Goede, S. & E.R. Leukfeldt (2021) Whatsappfraude komt veelvuldig voor in Nederland. Secondant: WhatsAppfraude komt veelvuldig voor in Nederland (ccv-secondant.nl)

CRIMINELEN VROEGEN

€	%
<50	27%
50-750	26%
750-2500	29%
2500-5000	12%
>5000	7%

SLACHTOFFERS BETAALDEN

€	%
<50	34%
50-750	20%
750-2500	27%
2500-5000	13%
>5000	6%

GELD TERUG-GEKREGEN?

9% deels
25% volledig
66% nee

SLACHTOFFERS ERVAARDEN NEGATIEVE GEVOLGEN

(schaal: geen gevolgen (1) tot zeer grote gevolgen (5))

Financiële gevolgen	Psychische en/of emotionele gevolgen	Andere gevolgen
2,3	2,8	2,1

CONTACT MET ORGANISATIES

	% NAM CONTACT OP	TEVREDENHEID (SCHAAL: zeer ontevreden (1) tot zeer tevreden (5))
Politie	71%	3,2
Bank	81%	3,5
Fraudehelpdesk	37%	3,6
WhatsApp	7%	3,1
Andere organisatie	12%	3,2

Slachtoffers die contact opnamen met de politie, de Fraudehelpdesk of Whatsapp deden dit het vaakst om het delict te melden of aangifte te doen (72-83%). Contact met hun bank namen zij het vaakst op voor hulp en/of informatie alsmede het melden van het delict.

Aan dit onderzoek deden **20.917 NEDERLANDERS** mee uit het I&O Research Panel. De data zijn gewogen en daarmee representatief voor de Nederlandse bevolking van 18 jaar en ouder naar leeftijd, geslacht en opleiding. De dataverzameling vond plaats in week 51 en 52 van 2020 en ervaringen werden uitgevraagd over de 12 maanden hiervoor.

ALTERNATIEVE NAAM:

- vriend-in-noodfraude
- sms-fraude
- hulpvraagfraude

Bij WHATSAPP-FRAUDE krijgt u via WhatsApp zogenaamd een dringend verzoek van een vriend(in), familielid of bekende om snel geld over te maken. In werkelijkheid komt het appje van een oplichter die zich voordoet als een bekende en u op slinkse wijze geld wil aftroggelen.

Hoe onveilig is het? De aard, omvang, impact en omgang met cyberrisico's tijdens de coronacrisis

Achtergrond

Door het coronavirus en de coronamaatregelen in 2020 en 2021 hebben waarschijnlijk nog nooit zoveel Nederlanders tegelijk vanuit huis gewerkt. In de media hebben verschillende experts gewezen op de cyberrisico's van thuiswerken. Dit is voor het mkb zeer relevant omdat mkb-bedrijven de ruggengraat vormen van de Nederlandse economie (61% van het BBP, 70% van de werkgelegenheid, totale omzet van 888 miljard euro), terwijl we ook weten dat deze groep bedrijven relatief vaak slachtoffer wordt van cyberaanvallen en weinig middelen ter beschikking heeft om zich hiertegen te wapenen. Tegelijkertijd zijn mkb-bedrijven waarschijnlijk niet goed ingericht op het ondersteunen van (massaal) thuiswerken en hebben daarom in allerijl en met veelal beperkte middelen moeten improviseren om het thuiswerken mogelijk te maken. Dit onderzoek richt zich op de vraag in hoeverre het coronavirus en het thuiswerken geleid hebben tot meer cyberonveiligheid voor burgers en het mkb en wat we hiervan kunnen leren voor de toekomst. Hierbij willen we kijken naar de aard en omvang van dreigingen en incidenten, naar de impact die incidenten hebben gehad en hoe burgers en mkb-bedrijven daarmee omgegaan zijn. Dit inzicht is voor het mkb van groot belang om te kunnen beoordelen welke maatregelen zij kunnen c.q. moeten nemen en wat die maatregelen mogen kosten. Uit eerder onderzoek weten we dat mkb-bedrijven weinig inzicht hebben in het risico (doordat aard en omvang vaak onduidelijk zijn) en (daardoor) niet weten welke maatregelen zij moeten treffen. Daarnaast hebben mkb-bedrijven vaak weinig middelen en kennis in huis om zich goed te kunnen wapenen tegen cybercriminelen. Door het delen van geleerde lessen en het geven van best practices aan mkb-bedrijven, is de praktijkwaarde van dit onderzoek daarom groot.

Doelen

1. Achterhalen in hoeverre de aard en omvang van cyberdreigingen door het coronavirus veranderd zijn. We interviewen 10 experts die werkzaam zijn in verschillende publieke en private organisaties (NCSC, MKB Nederland, Digital Trust Centre, KvK, politie).

2. Inzichtelijk maken wat de aard, omvang en impact was van cyberincidenten ten tijde van het coronavirus en het massaal thuiswerken We voeren twee metingen uit om inzicht te krijgen in de aard, omvang en impact. Een eerste vragenlijst zal worden uitgezet onder een steekproef van ongeveer 500 eigenaren van mkb-bedrijven. Een tweede vragenlijst onder een representatieve steekproef van ongeveer 500 burgers in Nederland. Hierdoor wordt een uniek beeld verkregen van de effecten van het coronavirus en het massaal thuiswerken. Daarnaast voeren we verdiepende interviews uit om de resultaten uit de meting te duiden. We nemen interviews af bij respondenten van 10 verschillende mkb-bedrijven (eigenaar en/of IT verantwoordelijke) en de 10 experts die al eerder voor doelstelling 1 benaderd zijn.

3. Inzichtelijk maken hoe mkb-bedrijven zijn omgegaan met de cyberrisico's tijdens de coronacrisis en het thuiswerken en welke lessen hieruit getrokken kunnen worden De methoden die gebruikt zijn om doelstelling 1 en 2 te beantwoorden geven inzicht in hoeverre eigenaren van mkb-bedrijven het thuiswerken hebben gefaciliteerd, hoe zij het risico op thuiswerken hebben ingeschat en welke (aanvullende) maatregelen zij eventueel genomen hebben. Ook worden de geleerde lessen en best practices verzameld.

Lopend onderzoek (2020-2021). Gefinancierd door NWA. Uitgevoerd door het NSCR en de Haagse Hogeschool. Betrokken onderzoekers: Steve van de Weijer, Jelle Groenendaal en Rutger Leukfeldt.

De impact van slachtofferschap van online criminaliteit

Dit onderzoek is een eerste verkenning in Nederland naar de impact op slachtoffers van online delicten, de behoeften van slachtoffers en de verantwoordelijkheden van politie, justitie en andere instanties bij de afhandeling van dergelijke delicten. Daarbij is er bijzondere aandacht voor de vraag in hoeverre en hoe de situatie en behoeften van slachtoffers van online criminaliteit afwijken van de situatie en behoeften van slachtoffers van traditionele offline delicten. Immers, als daar meer zicht op is wordt ook duidelijk of het bestaande slachtofferbeleid – dat ontwikkeld is voor traditionele offline delicten – voorziet in de behoeften van slachtoffers van online criminaliteit.

Om beter inzicht te krijgen in de behoeften van slachtoffers van online delicten op het punt van de hulp en ondersteuning, en de verwachtingen die zij hebben van de aanpak door politie en justitie, zijn 19 slachtoffers geïnterviewd. Daarnaast zijn bij 18 Nederlandse experts en 4 internationale experts interviews afgenomen.

Uit de interviews met slachtoffers van online delicten en experts blijkt dat de meeste gevolgen die slachtoffers van online delicten melden niet nieuw zijn en in grote lijnen overeenkomen met de gevolgen van traditionele offline delicten. Dit is in overeenstemming met eerder onderzoek naar de gevolgen van slachtofferschap van online delicten.

Door de kenmerken van het online delict kan de impact echter veel groter zijn dan de impact van offline delicten. Het online aspect versterkt samenvattend de gevolgen voor het slachtoffer op verschillende momenten, onder meer door de grote schaal waarop bijvoorbeeld beelden worden gedeeld na een hack en omdat slachtofferschap niet altijd stopt in de tijd. Beelden kunnen altijd weer opduiken. Bij technische delicten blijft vaak onbekend wie de mogelijke dader was.

Lang niet altijd wordt in de behoefte van slachtoffers voorzien. Een voorbeeld is de bevrediging van de behoefte om als slachtoffer erkend te worden. Slachtoffers zien vaak de politie als organisatie die hen kan helpen, terwijl de politie op dit moment niet aan deze verwachting voldoet. Een tweede behoefte heeft betrekking op het strafproces. Slachtoffers geven aan het van belang te vinden dat de dader gestraft wordt, aangifte te kunnen doen en – in de gevallen dat er sprake is van opsporing – op de hoogte te worden gehouden van de voortgang van het opsporingsonderzoek en strafproces. Bij de afhandeling van online delicten speelt echter een aantal problemen waardoor lang niet altijd in deze behoeften voorzien

kan worden. Slechts bij een heel klein deel van de slachtoffers is er een verdachte opgepakt en veroordeeld. De belangrijkste financiële behoefte van slachtoffers is die aan schadevergoeding. De meeste slachtoffers die dit wensten, kregen dit echter niet, om redenen die eerder hierboven zijn genoemd.

De geschetste problemen met het voorzien in behoeften van slachtoffers zijn niet nieuw: ook bij traditionele offline delicten voelen slachtoffers zich niet altijd erkend, wordt niet altijd aangifte opgenomen of wordt er geen opsporingsonderzoek gestart. Maar juist bij online delicten hebben politiemedewerkers volgens experts en slachtoffers onvoldoende kennis en schatten ze dergelijke delicten als complex in. Dit knelt temeer omdat slachtoffers aangeven met name de politie te zien als verantwoordelijk actor na slachtofferschap.

Leukfeldt, E.R., R.J. Notté, M. Malsch (2018) Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordlijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit. Den Haag: Ministerie van Justitie en Veiligheid.

Leukfeldt, E.R., R.J. Notté & M. Malsch (2019) Slachtofferschap van online criminaliteit kan ingrijpend zijn. Secondant. https://ccv-secondant.nl/platform/article/slachtofferschap-van-online-criminaliteit-kan-ingrijpend-zijn

Leukfeldt, E.R., R.J. Notté & M. Malsch (2019) Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. Victims and Offenders. DOI:10.1080/15564886.2019.1672229

Notte, R. J., Leukfeldt, E.R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. International Review of Victimology, 27(3), 272-294. https://doi.org/10.1177/02697580211010692

RESULTATEN ONDERZOEKSLIJN 2:

AARD VAN CYBERCRIMINALITEIT

Insider threats

Insider threats zijn incidenten die veroorzaakt zijn door bewuste of onbewuste handelingen van eigen personeel. Zo kan een voormalige medewerker gegevens van een server verwijderen doordat deze persoon onterecht nog steeds toegang heeft tot die server, kan een medewerker op een onveilige wijze gegevens delen waardoor deze zijn in te zien door derden, of kan een stagiair een foto op sociale media plaatsen waarop gevoelige informatie van de organisatie wordt weergegeven. Vanuit het lectoraat is dan ook een onderzoekslijn gestart naar insider threats om bij te dragen aan de veiligheid van organisaties in Nederland. Momenteel voeren we twee parallelle onderzoeken uit: een systematische review van de empirische literatuur over deze bedreigingen van binnenuit en een onderzoek naar de aard en omvang van dergelijke incidenten in Nederland.

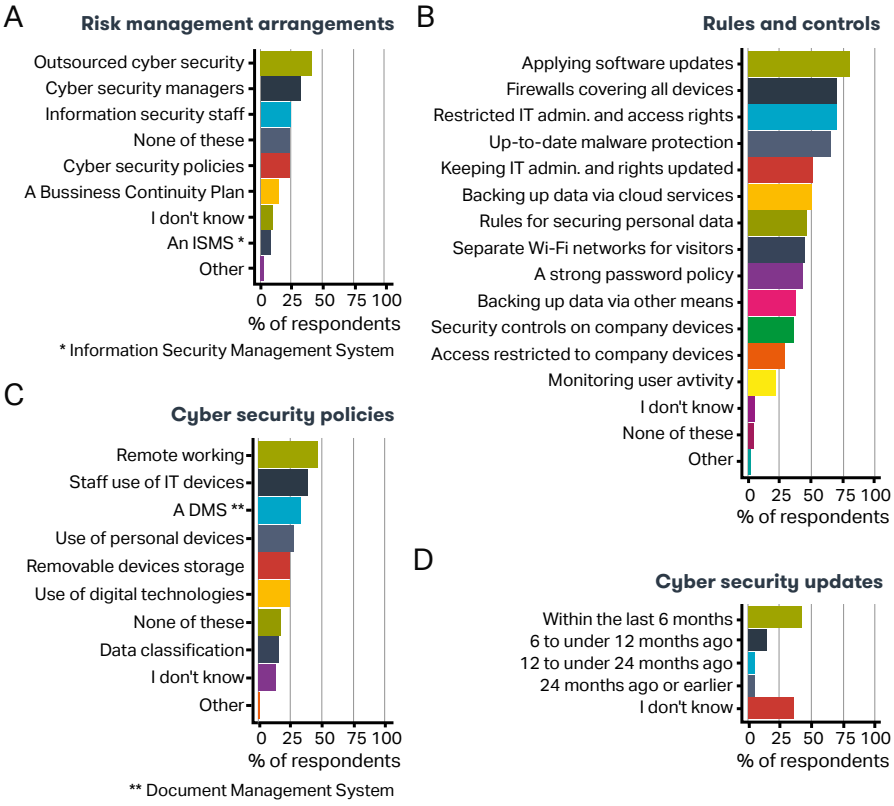
Het empirische onderzoek naar de aard en omvang van incidenten in Nederland voeren we uit middels een vragenlijstonderzoek. We maken verder onderscheid tussen verschillende soorten incidenten: kwaadwillig, nalatig en goedbedoeld. In een eerste publicatie streven we drie doelen na: het bepalen van de prevalentie en frequentie van de verschillende soorten insider-incidenten die in Nederlandse mkb-bedrijven worden gemeld; de meest opvallende incidenten om de gevolgen voor de bedrijven beschrijven en bepalen hoe mkb's op dergelijke incidenten reageren.

Om dit te doen, hebben onderzoekers een online vragenlijst afgenomen bij een panel van ondernemers met personeel en werknemers in een leidinggevende functie binnen het mkb. In totaal hebben we gegevens van 496 respondenten. De vragenlijst ging in op in hoeverre organisaties zich gewapend hebben tegen dergelijke incidenten, of ze insider-incidenten hebben meegemaakt en welk cyberbeveiligingsbeleid en -procedures ze hebben.

Uit voorlopige resultaten blijkt dat 7,1% van de mkb-bedrijven in de afgelopen 12 maanden minstens één insider-incident hebben meegemaakt en dat er in dezelfde periode ten minste 87 incidenten werden gemeld.

Insider incidenten zorgen ervoor dat de bedrijven extra tijd moeten investeren in het oplossen ervan of het informeren van getroffen klanten. Na een eerste slachtofferschap investeren mkb'ers in nieuwe beschermingsmaatregelen om de veroorzaakte financiële schade te beperken (welke varieërde van minder dan € 500 tot meer dan € 100.000).

Wat cyberbeveiligingsmaatregelen betreft, lijkt het erop dat de maatregelen die door mkb'ers worden genomen nog steeds minimaal zijn. In een enkel geval worden zelfs hele basale maatregelen zoals een sterk wachtwoordbeleid of de implementatie van beveiligingscontroles op bedrijfsapparaten niet uitgevoerd.



Lopend onderzoek (2020-2022). Uitgevoerd door de Haagse Hogeschool. Betrokken onderzoekers: Asier Moneva en Rutger Leukfeldt.

Moneva, A., & Leukfeldt, E. R. (in review). Insider Incidents Among Dutch SMEs: Prevalence, Incidence, Frequency, Consequences, and Cyber Security Policies.

Moneva, A., Leukfeldt, E. R., & Trinidad, A. (registered). A Scoping Review of the Empirical Literature on Insider Threats.

Social engineering

Studenten van de Haage Hogeschool doen onderzoek naar de vatbaarheid van organisaties voor social engineeringsaanvallen. Onderzoekers van het lectoraat publiceerden hierover in het vakblad Informatiebeveiliging waarbij een analyse werd gemaakt van 98 aanvallen binnen dertig organisaties. Studenten maakten gebruik van drie typen social engineeringsaanvallen: 1. fysiek, 2. telefonisch (vishing) en 3. digitaal (phishing). Studenten bepaalden eerst samen met de opdrachtgever welke informatie er bemachtigd moest worden. Variërend van elektronische dossiers tot inloggegevens van medewerkers.

De belangrijkste uitkomsten van dat artikel zijn:

"Bij succesvolle aanvallen werden verschillende beïnvloedingstechnieken gebruikt. Het principe sympathie is vaak succesvol toegepast, vooral bij een fysieke aanval. Ook is vaak, met name bij de telefonische aanval, succesvol gewerkt met de principes schaarste en autoriteit. Een andere veelgebruikte overtuigingstechniek is distraction, waarbij een emotie werd opgewekt als verrassing of afschuw. Het principe schaarste werkt ook op deze manier. Bijvoorbeeld door tijdsdruk op te leggen om inloggegevens te verstrekken, omdat anders het systeem crasht."

"Het belang van vooronderzoek is duidelijk terug te zien. Het blijkt heel makkelijk om schijnbaar onschuldige informatie over medewerkers te verkrijgen via openbare bronnen, vooral social media. Deze informatie kan ingezet worden als hefboom om personeel van de organisatie te manipuleren. Door een telefoontje konden studenten eenvoudig de naam van IT-systeembeheerder achterhalen of het e-mailadres van de directeur. Een phishingmail kan dan al snel worden gemaakt."

"Kennis over de organisatiecontext helpt om aan te sluiten bij de herkenbare omgeving. Dit heet 'framing' en is vaak toegepast. Door observaties was bijvoorbeeld de 'dresscode' eenvoudig te achterhalen en maakte tailgating succesvol. Enige terughoudendheid bij het prijsgeven van schijnbaar onschuldige informatie, zoals een e-mailadres van het werk en een specifieke functie via social media, is aanbevelingswaardig."

"Een bepaalde organisatiecultuur lijkt een rol te spelen in het makkelijker prijsgeven van voor cybercriminelen relevante informatie. Studenten wisten regelmatig informatie te verkrijgen over doelen door in te spelen op de servicegerichtheid van medewerkers zoals in de zorg en overheidssector. Een medewerker die zeer behulpzaam was en het leuk vond over zijn vak te vertellen, liet studenten, die zich voordeden als studenten Bouwkunde, foto's maken op een beveiligde locatie."

Een belangrijke voorwaarde – maar zeker geen garantie – voor het succesvol pareren van een aanval is dat de organisatie de basisbeveiliging op orde heeft, zoals gedragsprotocollen, functiescheiding en toegangsbeleid.

Ancher, M., R. van der Kleij & E.R. Leukfeldt (2019) Studenten treden in voetsporen cybercriminelen om meer inzicht te krijgen in social engineering. Informatiebeveiliging. 19(2)26-33.

Cybercriminele netwerken: mogelijkheden voor een lokale aanpak?

In essentie is een belangrijke boodschap uit de onderzoeken naar cybercriminele netwerken dat het bij dergelijke netwerken niet alleen gaat om dreiging uit verre landen, om internationale politiesamenwerking bij de aanpak ervan en de noodzaak van de bescherming van alleen de vitale infrastructuur.

Er zijn zeker internationaal opererende cybercriminele netwerken die aanvallen uitvoeren op organisaties in Nederland. Echter is dankzij de steeds verdergaande digitalisering de bescherming tegen cybercrime iets geworden dat van belang is voor iedereen, van de Rotterdamse haven tot de kleine zelfstandige met een webwinkel en individuele burgers, en waar dus ook verschillende actoren mee te maken krijgen, van internationale gespecialiseerde politieteams tot de buurtagent, van de rijksoverheid tot lokale overheden.

Dat komt doordat het beeld van cybercriminele netwerken genuanceerder is dan alleen de dreiging uit verre landen. Onderzoek laat zien dat er grofweg twee typen cybercriminele netwerken kunnen worden onderscheiden. Allereerst zijn dat gespecialiseerde ‘nieuwe’ criminele netwerken die zich met name toeleggen op het plegen van cybercrimes. Daarnaast zijn er traditionele netwerken die zich nu ook bezighouden met het plegen van cybercriminaliteit. Dergelijke netwerken houden zich vaak al langere tijd bezig met allerlei andere traditionele criminele activiteiten en nemen nu ook cyberaanvallen op in hun criminele repertoire.

Een overeenkomst tussen beide typen is dat zij veelal lokaal ingebed moeten zijn om succesvol te opereren. Zo blijken offline en online sociale banden tussen netwerkleden nog altijd van groot belang te zijn en kennen leden van netwerken elkaar niet zelden ‘uit de buurt’. Daarnaast blijven voor veel financieel gemotiveerde cybercriminele netwerken zogenaamde geldezels of money mules van groot belang om geld weg te sluizen. Ook hier is een lokale inbedding van soms internationale criminaliteit te zien.

Ondanks het schijnbare ‘grenzeloze’ karakter van cybercrime, zijn er dus toch mogelijkheden voor een nationale of zelfs lokale aanpak van cybercrime.

Leukfeldt, E.R. & E.R. Kleemans (2021) Breaking the walls of silence: analyzing criminal investigations to better understand cybercrime. In: Lavorgna, A. & Holt. T.J. (eds.) *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*". Pp 127-144. Palgrave Macmillan, Cham.

Leukfeldt, E.R. & R. Roks (2020) Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior.* DOI: 10.1080/01639625.2020.1755587.

Roks, R.A., E.R. Leukfeldt & J.A. Densley (2020) The Digitized Opportunity Structure of Street Offending. *British Journal of Criminology*. https://doi.org/10.1093/bjc/azaa091

Leukfeldt, E.R., T.J. Holt (2019) Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. *International Journal of Offender Therapy and Comparative Criminology* 64(5) 522-538.

Leukfeldt, E.R., E.R. Kleemans, E.W. Kruisbergen, R. Roks (2019) Organized Financial Cybercrime: Criminal Cooperation, Logistic Bottlenecks, and Money Flows. In: Holt T., Bossler A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham.

Defacers: het digitaal bekladden van websites

Deze onderzoekslijn richt zich op een bijzondere groep cyberaanvallers: defacers. Dergelijke aanvallers maken gebruik van verschillende technieken om toegang te krijgen tot websites en passen die vervolgens aan. Om meer inzicht te krijgen in deze specifieke groep daders maken we gebruik van de database van Zone-H, waarin veel van deze aanvallen gerapporteerd worden.

Zo onderzochten we bijvoorbeeld de relatie tussen de motieven van aanvallers en de keuze voor doelwitten. We maakten daarbij gebruik van een steekproef van 138.361 webdefacements die werden uitgevoerd op websites die werden gehost binnen de Nederlandse IP-ruimte van januari 2011 tot april 2017. Samengevat laat dit onderzoek zien dat er een verband is tussen dadermotivatie en doelwitselectie. Ideologisch gemotiveerde actoren vallen vaker hetzelfde doelwit aan, gebruiken daarvoor verschillende technieken en richten zich voornamelijk op de hoofdpagina van een website. Aanvallers die worden gedreven door motieven die de waarden van de hacker-subcultuur weerspiegelen, zijn eerder geneigd tot zogenoemde mass defacements en kiezen voor minder vaak gebruikelijke aanvalsmethoden. Daarnaast deden we longitudinaal onderzoek naar de ontwikkelingstrajecten van actieve hackers die webdefacements uitvoeren. De gegevens voor dit onderzoek bestonden uit 2.745.311 aanvallen uitgevoerd door 66.553 hackers en gerapporteerd aan Zone-H tussen januari 2010 en maart 2017. Semi-parametrische op groepen gebaseerde trajectmodellen werden gebruikt om zes verschillende groepen hackers te onderscheiden op basis van de timing en frequentie van hun defacements. De resultaten toonden enkele gemeenschappelijke relaties aan met traditionele vormen van misdaad, aangezien een kleine populatie van defacers verantwoordelijk was voor de meerderheid van de defacements tegen websites. Bovendien verschilden de methoden en targetingpraktijken van defacers op basis van de frequentie waarmee ze in het algemeen defacements uitvoerden.

Holt, T.J., E.R. Leukfeldt & S. Van de Weijer (2020) An Exploration of the Factors Associated with Expressive Motives to Engage in Cyberattacks against Dutch Web Sites. *Criminal Justice and Behavior* 47(4) 487-505.

Van de Weijer, S., T.J. Holt & E.R. Leukfeldt (2021) Heterogeneity in trajectories of cybercriminals: a longitudinal analyses of web defacements. Computers in Human Behavior Reports. doi.org/10.1016/j.chbr.2021.100113.

Romagna, M. (2020). Evolution of Hacktivism: From Origins to Now. In O. Guntarik, & V. Grieve-Williams (Eds.), From Sit-ins to #revolutions. Media and the Changing Nature of Protests (pp. 65-76). Bloomsbury Academic. https://doi.org/10.5040/9781501336980.ch-005

Romagna, M. (2020). Hacktivism: Conceptualization, Techniques, and Historical View. In T. J. Holt, & A. M. Bossler (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 743-769). Springer Publishing.

MONEY MULES: EEN BELANGRIJKE SCHAKEL

Bekkers, L., J. Schiks & E.R. Leukfeldt (2020) Naar een interventie tegen geldezels. Een pilot in de gemeente Haarlem. Den Haag: Centre of Expertise Cybersecurity, Haagse Hogeschool.

Leukfeldt, E.R., & E.R. Kleemans (2019) Cybercrime, money mules and situational crime prevention. In: S.Hufnagel & A. Moiseienko (eds.) *Criminal Networks and Law Enforcement*: Global Perspectives on Illicit Enterprise. London: Routledge.

Naar een interventie tegen geldezels
Een pilot in de gemeente Haarlem

Een geldezel of money mule is iemand die zijn of haar bankrekening laat misbruiken voor criminele doeleinden.

Doel:

Inzicht krijgen in kenmerken van geldezels, de rol van geldezels in de werkwijze van cybercriminele netwerken en mogelijke interventies die hierbij aansluiten.

Methode:

Analyse wetenschappelijke literatuur, 10 expert interviews (met jongerenwerkers, politie, reclassering, HALT, Openbaar Ministerie, bank), 2 focus groepen met lokale en regionale stakeholders (o.a. gemeente Haarlem, politie, jongerenwerkers, HALT).

Conclusies:

- **Weinig empirisch onderzoek**.
  Er is nog weinig empirisch onderzoek gedaan naar geldezels.

- **Geldezels vormen een cruciale schakel binnen crime scrips.**
  Geldezels worden gebruikt door criminelen om het financiële spoor van een delict naar de criminelen te verbergen. Illegaal verkregen geld wordt cash opgenomen vanaf de rekening van de geldezel.

- **Geen duidelijk profiel.**
  Geldezels vormen een heterogene groep en het opstellen van een profiel is dan ook lastig. Wel komt naar voren dat het vooral lijkt te gaan om kwetsbare personen die als geldezel worden ingezet. Uit de literatuur en expertinterviews zijn de volgende terugkerende kenmerken van geldezels te herkennen:
  - Man
  - Jong
  - Lager opgeleid
  - Afkomstig uit wijken met een lagere sociaaleconomische status

- **Ronselen gebeurt via-via.**
  Het ronselen van geldezels lijkt met name via-via plaats te vinden. Dit gebeurt zowel online (via oproepen op sociale mediakanalen als Telegram, Snapchat en Instagram) als offline (via sociale kringen op onder meer scholen). Minder genoemde methoden zijn 'job scams' en spam.

- **Motieven zijn lastig te bepalen.**
  Net als het profiel, is ook het motief lastig vast te stellen, met name omdat niet altijd duidelijk is of het om daders of slachtoffers gaat. Drie motieven die het vaakst voorkomen volgens de literatuur en respondenten:
  - Snel geld willen verdienen
  - Verwerven van status
  - Geloven in smoesjes die ronselaars vertellen

- **Situationele criminaliteitspreventie.**
  Er is sprake van een subcultuur onder jongeren waarin status en geld een belangrijke rol spelen. Verstoor de subcultuur die het crimineel gedrag van geldezels normaliseert.

Lectoraat maatschappelijke-veiligheid, Saxion

Lectoraat cybersecurity in het mkb, De haagse hogeschool

RESULTATEN ONDERZOEKSLIJN 3:

CYBERWEERBAARHEID

Van theorie naar praktijk: het cyberweerbaarheidsmodel

De basis van ons onderzoek naar cyberweerbaarheid vormt het model dat we publiceerden in 2019. Cyberweerbaarheid is hier gedefinieerd als het vermogen om weerstand te bieden tegen bekende en onbekende vormen van cyber-criminaliteit en snel te herstellen van een cybercrisis. In die publicatie stellen we een raamwerk voor om de menselijke aspecten van cyberweerbaarheid binnen organisaties te kunnen meten. Het raamwerk biedt organisaties diagnostische mogelijkheden om zich beter voor te bereiden op cyberdreigingen. Het model ziet er als volgt uit:

Om mkb'ers in staat te stellen hun cyberweerbaarheid te verhogen, heeft de Haagse Hogeschool, samen met het Platform Veilig Ondernemen (PVO) en de VeiligheidsAlliantie regio Rotterdam (VAR) het theoretische model omgezet in een webapplicatie. Voor de financiering van de webapplicatie heeft het PVO een subsidie ontvangen van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Naast het ontwikkelen van de app is het doel om mkb'ers in de regio Rotterdam die de app hebben gebruikt:

1. meer bewust te maken van de risico's van cybercriminaliteit in zijn algemeenheid en ook voor hun bedrijf specifiek;

2. inzicht te geven in weten welke maatregelen ze kunnen treffen om slachtofferschap te voorkomen en schade bij slachtofferschap te beperken;

3. daadwerkelijk aan de slag te laten gaan met de gegeven tips.

Kleij, van der R. & E.R. Leukfeldt (2019) Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In: Ahram T., Karwowski W. (eds) Advances in Human Factors in Cybersecurity. AHFE 2019. Advances in Intelligent Systems and Computing, vol 960. Springer, Cham

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

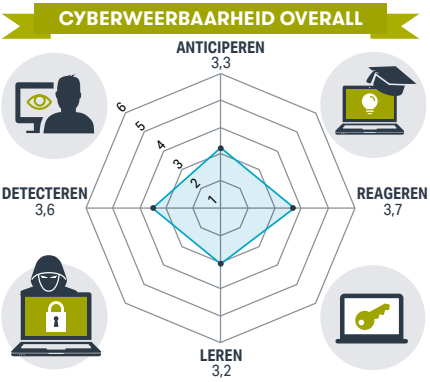
Cyberweerbaarheid gemeten

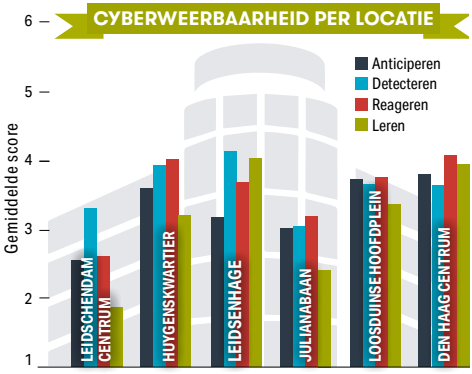
Onderzoeksopzet en respons

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 Den 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.

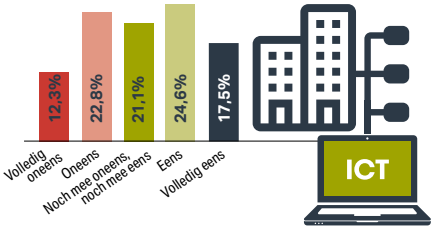
Cyberweerbaarheid gemeten

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'.

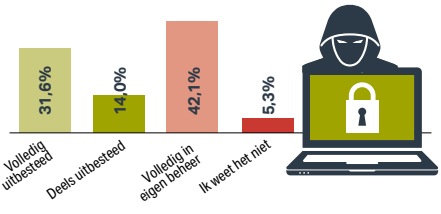




Bedrijfsprocessen afhankelijk van ICT?



Is de IT-beveiliging uitbesteed?

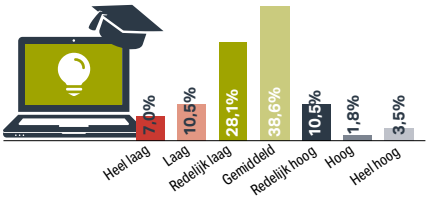


Sanctiebeleid cyberonveilig gedrag

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 word 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.



Kleij, van der, R., I. de Bruin, S. van 't Hoff-de Goede & E.R. Leukfeldt (2019) Pilotonderzoek cyberweerbaarheid mkb-retailers in de regio Den Haag. Den Haag: De Haagse Hogeschool.

Van der Kleij, R., I. de Bruin, S. van 't Hoff-de Goede, M. Ancher & E.R. Leukfeldt (2019) Cybercriminaliteit leeft niet onder retailers. Secondant. https://ccv-secondant.nl/platform/article/cybercriminaliteit-leeft-niet-onder-retailers.

Naar een bruikbaar risicomodel voor het mkb

Bestaande risicomodellen voor cybersecurity lijken in de praktijk lastig bruikbaar voor mkb-bedrijven. In dit onderzoek staan daarom de volgende vragen centraal: (1) Op welke wijze organiseren midden-en kleinbedrijven in de metaalsector hun cybersecurity risicomanagement; en (2) hoe kan dit proces worden verbeterd?

Doel van dit project is om via onderzoek te komen tot een voor het mkb te hanteren risicomodel dat kan worden gebruikt om het cybersecurity risicomanagement van mkb-metaalbedrijven te verbeteren. Om dit te bereiken zijn drie stappen ondernomen. Ten eerste is een literatuurstudie uitgevoerd. Ten tweede is een theoretisch cybersecurity risicomodel ontwikkeld. Ten derde is het model vervolgens getoetst in de praktijk.

Onderzoeksopzet

Om tegemoet te komen aan de praktijk ontwikkelden wij op basis van de internationaal meest gehanteerde standaarden voor informatiebeveiliging en risicomanagement een cybersecurity risicomodel voor mkb-metaalbedrijven (ISO/IEC 27001, 2013; ISO/IEC 3100, 2009; ISO/IEC 27005, 2011). Hiermee kunnen mkb-metaalbedrijven hun cybersecurity beter organiseren. Het risicomodel is een stappenplan dat is opgedeeld in twee fasen: een fase waarin het beoordelen van het risico centraal staat en een fase waarin de aanpak van het risico centraal staat. Vervolgens vindt een herevaluatie van het resterende risico plaats en het opnieuw doorlopen van het stappenplan, dat als een continu te doorlopen cyclus dient te worden gezien.

Het cybersecurity risicomodel voor mkb-metaalbedrijven is vervolgens getoetst in de praktijk middels 27 interviews met directeuren en medewerkers van 10 mkb-metaalbedrijven. Twee onderwerpen stonden in deze interviews centraal: (1) Het gebruik van risicomanagement voor cybersecurity binnen metaalbedrijven; en (2) Het doorlopen van het door ons ontwikkelde risicomodel voor cybersecurity met metaalbedrijven.

Conclusie

We onderzochten op welke wijze mkb-bedrijven in de metaalsector hun cybersecurity en de bijbehorende beveiligingsmaatregelen organiseren en hoe dit proces verbeterd kan worden. Het blijkt dat onderzochte bedrijven volledig gedigitaliseerd zijn en voor het primaire proces afhankelijk van ICT. De implementatie en het onderhoud van deze ICT wordt uitbesteed aan externe ICT-leveranciers. Vele directeuren besteden daarbij (deels) ook de beveiliging uit aan deze ICT-leveranciers. Dit heeft tot gevolg dat deze ICT-leveranciers generieke technische maatregelen implementeren, zonder specifiek naar de organisatie in kwestie en haar risico's te kijken. Cruciale maatregelen gericht op de organisatie van het bedrijf en het gedrag van personeel blijven vervolgens veelal achterwege.

Dit onderzoek laat zien dat er mogelijkheid voor verbetering is. Aangezien de deelnemende organisaties feitelijk helemaal geen risicomodel gebruiken is de ontwikkeling van een simpel te gebruiken risicomodel al een hele winst. Met zo'n model kunnen mkb-bedrijven het proces waarmee zij sturing geven aan cybersecurity verbeteren. Mkb-metaalbedrijven kunnen met dit model bijvoorbeeld hun cybersecurity context analyseren en indien nodig verbeteren door gebruik te maken van cybersecurity risicomanagement. Dit wordt tot op heden in de deelnemende bedrijven nog nauwelijks gedaan. Desgevraagd zijn directeuren en medewerkers van metaalbedrijven echter goed in staat een overzicht te geven van de cruciale informatie en systemen in de eigen organisatie, alsmede waar de belangrijkste cybersecurity risico's liggen. Daarbij is het van belang dat een dergelijk model ook beleidsmaatregelen en maatregelen gericht op het gedrag van personeel omvat. Terwijl de technische maatregelen kunnen worden uitbesteed, dienen maatregelen rondom de menselijke factor van cybersecurity veelal door het bedrijf zelf te worden genomen. In een vervolgstudie kan daarom op basis van de resultaten van dit onderzoek een praktisch toepasbaar model worden ontwikkeld waarmee bedrijven in staat zijn per bedrijfsproces in kaart te brengen waar cybersecurity risico's liggen. Vervolgens kunnen maatregelen genomen worden op het gebied van techniek, beleid en personeel.

Notté, R.J., S. van 't Hoff-de Goede & E.R. Leukfeldt (2019) Cybersecurity in de metaalsector. De ontwikkeling van een praktisch cybersecurity risicomodel voor midden- en kleinbedrijven in de metaalsector. Den Haag: De Haagse Hogeschool.

(On)veilig online gedrag

Binnen deze onderzoekslijn richten we ons op het online gedrag van Nederlanders. Immers: een belangrijke voorwaarde voor online veiligheid is veilig cybergedrag. Zeven gedragsclusters staan centraal: gebruik van wachtwoorden, opslaan van belangrijke bestanden, installeren van updates, gebruik van beveiligingssoftware, alertheid tijdens internetgebruik, delen van persoonlijke gegevens en omgaan met bijlagen en hyperlinks in e-mails.

Onveilig gedrag blijkt in hoge mate voor te komen: bijna 90 procent gebruikt een zwak wachtwoord, 40 procent downloadt onveilige software en ongeveer 30 procent deelt persoonlijke gegevens, zoals hun volledige naam, geboortedatum en e-mailadres. Als respondenten phishing e-mails krijgen voorgelegd dan blijkt dat ruim 20 procent een onveilige keuze maakt: ze klikken op de hyperlink of kopiëren de URL naar de webbrowser.

We onderzochten zowel zelfgerapporteerd gedrag als objectief gemeten gedrag. Daar blijken behoorlijke verschillen tussen te bestaan. Respondenten hebben een te rooskleurig beeld van hun eigen gedrag. Een voorbeeld: respondenten geven over het algemeen aan een veilig wachtwoordbeleid te voeren, terwijl uit de objectieve meting iets heel anders blijkt. Meer dan 40 procent van de respondenten gebruikt een zwak wachtwoord bestaande uit minder dan zeven karakters voor het beveiligen van hun persoonsgegevens in dit onderzoek.

Als we kijken naar mogelijkheden om gedragsinterventies te ontwikkelen dan blijkt dat erg lastig: er geen panacee is voor het bevorderen van veilig cybergedrag. Online gedrag is complex, verschillende cybergedragingen kennen andere bronnen. Ook is het van groot belang dat interventies op het juiste moment worden aangeboden.

Het ontwikkelen van specifieke interventies is dus geen sinecure. Daarom richt ons toekomstig onderzoek zich op het ontwikkelen en evalueren van een specifieke set van interventies voor de door ons gevonden onveilige gedragingen. Daarvoor maken we onder andere gebruik van het Human factor in cybersecurity lab.

Van 't Hoff-de Goede, S., R. van der Kleij, S. van de Weijer & E.R. Leukfeldt (2019) Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders. Den Haag: De Haagse Hogeschool.

Van 't Hoff-de Goede, S., E.R. Leukfeldt, R. van der Kleij & S. Van de Weijer (2021) The online behaviour and victimization study: the development of a research instrument for measuring and explaining actual online behavior and online victimization. p21-42. In: Weulen Kranenbarg, M. & E.R. Leukfeldt (eds) Cybercrime in Context: the Human Factor in Victimization, Offending, and Policing. Springer.

Van der Kleij, R. & E.R. Leukfeldt (2019) Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In: Ahram T., Karwowski W. (eds) Advances in Human Factors in Cybersecurity. AHFE 2019. Advances in Intelligent Systems and Computing, vol 960. Springer, Cham

Van der Kleij, R., S. van 't-Hoff de Goede, S. van de Weijer & E.R. Leukfeldt (2020) Ons cybergedrag is veel onveiliger dan dat we zelf denken. Implicaties voor effectief beïnvloedingsbeleid door de overheid. *Justitiële Verkenningen* 20(2)113-128.

Van 't Hoff-de Goede, S., R. van der Kleij, S. Van de Weijer & E.R. Leukfeldt (2020) Onveilig gedrag op internet. *Secondant*. https://ccv-secondant.nl/platform/article/onveilig-gedrag-op-internet

Van der Kleij R., van 't Hoff-De Goede S., van de Weijer S., Leukfeldt R. (2021) How Safely Do We Behave Online? An Explanatory Study into the Cybersecurity Behaviors of Dutch Citizens. In: Zallio M., Raymundo Ibañez C., Hernandez J.H. (eds) Advances in Human Factors in Robots, Unmanned Systems and Cybersecurity. AHFE 2021. Lecture Notes in Networks and Systems, vol 268. Springer, Cham. https://doi.org/10.1007/978-3-030-79997-7_30

Slachtofferschap en online gedrag

In dit onderzoek kijken we naar de oorzakelijke relatie tussen onveilig online gedrag en slachtofferschap van cybercriminaliteit. We hebben onder een grote populatie Nederlanders daadwerkelijk online gedrag geobserveerd en hen een jaar later gevraagd of zij in het afgelopen jaar slachtoffer zijn geworden van cybercriminaliteit. Voorlopige resultaten laten zien dat mensen die geneigd zijn te klikken op onveilige hyperlinks en persoonlijke gegevens online te delen, significant vaker slachtoffer worden van cybercriminaliteit. Respondenten die op onveilige hyperlinks klikken hebben bijvoorbeeld 2 keer zoveel kans om het jaar erna slachtoffer te zijn geworden van phishing.

Lopend onderzoek (2021-2022). Uitgevoerd door de Haagse Hogeschool en het NSCR. Betrokken onderzoekers: Susanne van 't Hoff-de Goede, Rutger Leukfeldt en Steve van de Weijer.

KETENWEERBAARHEID

Een verkennend onderzoek naar dreigingen, kwetsbaarheden

Doelstelling

Het krijgen van meer inzicht in het fenomeen cyber-ketenweerbaarheid in verschillende economische sectoren om daarmee de overheid te ondersteunen in advisering en ontwikkeling van beleid.

Onderzoeksvragen

1. Welke cyberspecifieke dreigingen ontstaan bij ketens en welke kwetsbaarheden spelen daarbij een rol?
2. Wat zijn geleerde lessen bij het voorkomen en bestrijden van cyberincidenten gerelateerd aan het opereren in een keten?

Methode

De onderzoeksvragen zijn beantwoord aan de hand van literatuuronderzoek en interviews. De interviews zijn uitgevoerd bij in totaal 12bedrijven uit drie economische sectoren: agrarisch, sierteelt en handel. De bedrijven zijn binnen hun sector geschakeld (als afnemer en leverancier) en vormen daarmee een keten.

Conclusies

- **Ketens hebben last van specifieke dreigingen en kwetsbaarheden.** Met name ransomware en stepping stone-aanvallen zijn een dreiging. Een belangrijke kwetsbaarheid is technologie die op afstand kan worden bediend via internet door een derde partij, zoals klimaatregelaars en sorteersystemen.
- **Maatregelen gericht op de keten worden slechts sporadisch genomen.** Cyberveiligheid is veelal geen onderwerp in contracten met leveranciers, (structureel) overleg tussen partners op cybersecurity gebied blijft uit en informatiedeling over cyberrisico's en geleerde lessen op ketenniveau is beperkt.
- **De ene keten is de andere niet.** Verschillen in genoemde dreigingen, kwetsbaarheden en geleerde lessen tussen bedrijven zijn te verklaren door het type bedrijf en diens omvang, de volwassenheid van de organisatie op ICT-gebied en de positie van een bedrijf in de keten. Zo lijken met name ICT-dienstverleners en grote bedrijven zicht te hebben in en te handelen op keten-gerelateerde dreigingen en kwetsbaarheden
- **Hulp is nodig.** Ketens kunnen hulp gebruiken met het op orde brengen van de cyberveiligheid van de individuele partners, de cyberveiligheid tussen schakels en de cyberveiligheid van keten als geheel. Hierbij kan worden gedacht aan het beschikbaar stellen van voorbeeldcontracten met leveranciers, het faciliteren van (structureel) overleg tussen partners en ondersteuning van de informatiedeling op ketenniveau.

Bekkers, L., R. van der Kleij & E.R. Leukfeldt (2020) Cyber-ketenweerbaarheid. Een verkennend onderzoek naar dreigingen, kwetsbaarheden en geleerde lessen. Den Haag: Centre of Expertise Cybersecurity, Haagse Hogeschool.

Delen van cybersecurity informatie

Bedrijven bevinden zich tegenwoordig vaak in een keten. Een keten kan worden beschouwd als een verzameling organisaties die een virtueel netwerk delen waar informatie, diensten, goederen of geld doorheen stroomt. Hierbij staan ICT-systemen veelal centraal. Deze afhankelijkheid werkt in de hand dat cyber-gerelateerde risico's een opmars maken binnen ketens. Niet elke ketenorganisatie beschikt echter over de middelen en kennis om zichzelf te beschermen: om tot sterke ketens te komen is informatiedeling tussen ketenorganisaties over actuele dreigingen en incidenten van belang. Een doel van dit verkennend onderzoek, dat is uitgevoerd in opdracht van het Nationaal Cyber Security Centrum (NCSC), is om inzicht te bieden in de succesfactoren van informatiedeling-initiatieven op het gebied van cyberveiligheid. Met deze kennis kan het NCSC haar accounthouders en adviseurs helpen om de doelgroepen positief te motiveren om actie te nemen ter versterking van ketenweerbaarheid. Tevens wordt met dit onderzoek beoogd om aanknopingspunten voor vervolgonderzoek te identificeren.

Het identificeren van succesfactoren vond plaats op basis van een literatuurstudie en gestructureerde interviews met in totaal zes leden uit drie verschillende bestaande informatiedeling-initiatieven rondom cybersecurity: het Managed Service Provider (MSP) Information Sharing and Analysis Centre (ISAC), Energie ISAC en de securitycommissie van de Nederlandse Energie- Data Uitwisseling (NEDU). Alle respondenten zijn informatiebeveiligingsexperts die hun organisatie vertegenwoordigen in de samenwerkingsverbanden.

In totaal zijn 20 succesfactoren geïdentificeerd. Deze factoren zijn vervolgens gecategoriseerd tot vier thema's die bijdragen aan een succesvolle informatie-deling. De thema's zijn samen te vatten als teamfactoren, individuele factoren, managementfactoren en faciliterende factoren.

De vier meest genoemde succesfactoren zijn:

- **Expertise:** Leden met onderscheidende en gespecialiseerde kennis bevorderen de informatiedeling en zijn ondersteunend aan het individuele leerdoel van de leden.
- **Vertrouwen:** Vertrouwen is een essentiële voorwaarde voor de bereidheid om samen te werken en informatie te delen. Tijd is hierin een cruciale factor: tijd is nodig voor vertrouwen om te ontstaan.
- **Lidmaatschapseisen:** Expliciete en impliciete lidmaatschapseisen zorgen voor een selectie op geschikte deelnemers en faciliteren daarmee het onderling vertrouwen.
- **Structurele opzet:** Een samenwerking dient georganiseerd te zijn volgens een structuur en met een stabiele bezetting van voldoende omvang.

Vervolgonderzoek zou zich kunnen richten op het identificeren van strategieën voor het opstarten van samenwerkingsverbanden en het over de tijd behouden van enthousiasme onder de leden in de informatiedeling-initiatieven rondom cybersecurity. Ook onderzoek naar de eigenschappen of kwaliteiten van de voorzitter en hoe deze bijdragen aan het succesvol initiëren en onderhouden van een samenwerkingsverband zijn genoemd.

Ook is nog onvoldoende duidelijk hoe gedeelde of juist onderscheidende expertise van de leden bijdraagt aan succes van de informatiedeling-initiatieven. Verder is er behoefte aan kennis over hoe de samenwerking tussen ketenpartners op het gebied van cyberveiligheid buiten bestaande samenwerkingsverbanden is ingericht. Denk hierbij aan een uitbreiding van de huidige studie, maar met een focus op kleinere bedrijven die deel uitmaken van ketens, maar waarbij IT niet de corebusiness is, aangezien die volgens respondenten als risicovol worden gezien voor de keten.

Bekkers, L., R. van der Kleij & E.R. Leukfeldt (2020) Verkenning best practices cybersecurity informatiedeling. Den Haag: Centre of Expertise Cybersecurity, Haagse Hogeschool.

Bekkers, L., R. van der Kleij & E.R. Leukfeldt (2020) Succesfactoren voor het delen van cybersecurity informatie. Informatiebeveiliging Magazine 2020(5) 8-11

Communiceren over cybersecurity met mkb'ers: hoe krijgen we ze in beweging?

- **Deelnemers : 631 mkb-ondernemers**
- **59% man en 41 % vrouw**
- **De gemiddelde leeftijd is 57 jaar (min 16, max 85 jaar)**

Misana-ter Huurne, E., Y. van Houten, R. Spithoven, R.J. Notté & E.R. Leukfeldt (2020) Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercrime onder jongeren en mkb'ers. Deventer/Den Haag: Saxion Hogeschool, De Haagse Hogeschool.

Hoe kunnen we de cyberweerbaarheid bij mkb'ers verhogen?

1. **Focus op de aangetroffen, stevige optimistic bias: "het kan ook jóu overkomen".**
2. **Let op: Geef concreet aan wat men zelf (makkelijk!) kan doen om zichzelf beter te beschermen (zelfeffectiviteit) en daarnaast waarom dit nuttig is of hoe dit helpt je te beschermen (responseffectiviteit).**
3. **Let op: mkb'ers zijn geneigd meer zelfbeschermende maatregelen te treffen, wanneer zij het idee hebben dat dit van hen verwacht wordt in de (sociale) omgeving.**
4. **Zorg voor gelaagdheid in informatie: de behoefte aan informatie is groot, maar dynamisch; iedere mkb'er heeft weer zijn eigen informatiebehoefte. Zorg daarom voor een koppeling tussen de campagne en een (online) platform waarop mkb'ers onafhankelijke en betrouwbare informatie kunnen vinden over algemene informatie en actuele trends op het gebied van cybercriminaliteit.**

We hebben onderzocht:

1. **Hoe beleven mkb'ers de risico's en mogelijke schade van cybercriminaliteit?**
2. **In hoeverre weten mkb'ers hoe zij zichzelf kunnen beschermen tegen of voorbereiden op de risico's van cybercriminaliteit?**
3. **In welke mate vertonen mkb'ers zelf beschermend gedrag ten aanzien van cybercriminaliteit?**
4. **Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van mkb'ers bij cybercriminaliteit?**

We zien:

- Mkb'ers zijn zich bewust van de risico's van cyber criminaliteit.
- Mkb'ers zijn verdeeld over hun kennis van zelf-beschermend gedrag ten aanzien van cybercriminaliteit.
- Mkb'ers zien wel het nut in van zelfbeschermende maat-regelen en veel mkb'ers willen hierover ook extra informatie ontvangen. De meeste mkb'ers vertonen een relatief hoge mate van zelfbeschermend gedrag.

Onderzoeksrapport

Misana-ter Huurne, E., Y. van Houten, R. Spithoven, R.J. Notté & E.R. Leukfeldt (2020) Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercrime onder jongeren en mkb'ers. Deventer/ Den Haag: Saxion Hogeschool, De Haagse Hogeschool.

Uitvoerders Lectoraat Maatschappelijke Veiligheid, **Hogeschool Saxion**
Lectoraat Cybersecurity in het mkb, **De Haagse Hogeschool**

In opdracht van Veiligheidsalliantie Regio Rotterdam, onder financiering van het Ministerie van Justitie en Veiligheid

Valse email?

Meld het via de meldknop

Twee experimenten in de weerbarstige pratijk: mkb'ers ontvankelijk maken voor cybersecurity informatie en mkb'ers maatregelen laten nemen

Dit onderzoek richt zich op het ontvankelijk maken van mkb-ers (en hun medewerkers) voor informatie over het voorkomen van cybercriminaliteit en het motiveren van mkb-ers (en hun medewerkers) om preventieve beschermingsmaatregelen te nemen om het risico op slachtofferschap van cybercriminaliteit te verkleinen.

Om de ontvankelijkheid voor informatie en het motiveren voor het nemen van maatregelen te onderzoeken voeren we twee veldexperimenten uit met verschillende bedrijven.

Het eerste experiment richt zich op het ontvankelijk maken voor informatie over cyberveiligheid. Daarbij is de doelgedraging: mkb'ers lezen informatie over cyberveiligheid en mkb'ers zoeken informatie op over cyberveiligheid. Een grote groep ondernemers krijgt via een digitale nieuwsbrief informatie aangeboden over cybersecurity. Om het bericht verder te lezen moet op de link in het bericht worden geklikt. Vervolgens meten we hoeveel mensen klikken en hoelang ze op de pagina met informatie blijven. Er zijn drie condities: neutraal, anti-neutralisatie en geanticipeerde spijt. Het blijkt dat de berichten met geanticipeerde spijt zorgen voor een significante hogere klikrate.

Het tweede experiment richt zich op preventieve beschermingsmaatregelen. Hierbij is de doelgedraging: medewerkers klikken niet op een link in verdachte e-mails en medewerkers melden verdachte e-mails bij een intern meldpunt. Verschillende deelnemende mkb-bedrijven stellen voor dit onderzoek een intern meldpunt voor verdachte e-mails in, installeren een digitale meldknop in outlook, krijgen een handreiking voor leidinggevenden en krijgen een gedragscampagne inclusief onder andere posters en digitale flyers. Vervolgens krijgen de bedrijven binnen verschillende condities drie keer een nepmail waarbij we kijken naar het aantal medewerkers dat klikt en het aantal medewerkers dat een melding doet. Verder onderzoeken we achteraf de beleving en ervaringen met deze interventie.

Lopend onderzoek (2019-2021). Uitgevoerd door Inspire to Act en de Haagse Hogeschool. Gefinancierd door MKB Nederland en het Ministerie van Justitie en Veiligheid. Betrokken onderzoekers: Karin Bongers, Rick van der Kleij, Luuk Bekkers, Michelle Ancher en Rutger Leukfeldt.

RESULTATEN ONDERZOEKSLIJN 4:

DE AANPAK

Aangiftebereidheid na slachtofferschap

Centraal in deze onderzoeken staat de vraag waarom burgers en bedrijven zelden aangifte doen na slachtofferschap van cybercriminaliteit. In de verschillende studies zijn zowel het beoogde rapportagegedrag als het daadwerkelijke rapportagegedrag gemeten. Ook is gekeken of en in hoeverre slachtoffers contact opnemen met andere organisaties dan de politie en is gevraagd naar ervaringen tijdens het aangifteproces.

De aangiftebereidheid blijkt inderdaad laag. 13 procent van de burgers en 14 procent van mkb'ers stapt naar de politie na slachtofferschap.

Een andere belangrijke bevinding is echter dat er een groot verschil is tussen het voorgenomen aangifte- en meldingsgedrag en het daadwerkelijke aangifte- en meldingsgedrag van burgers en mkb'ers. Als burgers en mkb'ers vragen worden voorgelegd over wat ze zouden doen in een bepaalde situatie, dan geeft een significant groter deel aan naar de politie te stappen (70 procent van de mkb'ers), terwijl de cijfers over daadwerkelijk aangiftebereidheid een ander beeld laat zien. Dit maakt maar weer eens duidelijk dat zelfgerapporteerd gedrag echt iets anders is dan daadwerkelijk gedrag.

Dan de vraag welke delict- en slachtofferkenmerken van invloed zijn op de beoogde en daadwerkelijke aangifte bij de politie en andere organisaties. Het blijkt dat met name de delictskenmerken een belangrijke rol spelen bij de afweging om wel of geen aangifte te doen. Daarbij is het type cyberdelict van belang. Opvallend is dat hoe technischer een delict is (hacken, ransomware), hoe lager de aangiftebereidheid. Verder is de gepercipieerde ernst van het delict van belang: ernstigere delicten worden vaker gerapporteerd dan minder ernstige delicten. Opvallend is verder dat er geen invloed lijkt te zijn van het aantal aangiftemogelijkheden op de aangiftebereidheid.

Weijer, S., E.R. Leukfeldt & S. van der Zee (2020) Slachtoffer van cybercriminaliteit, wat nu? Een onderzoek naar aangiftebereidheid onder burgers en mkb'ers. Politie en Wetenschap.

Van de Weijer, S., E.R. Leukfeldt & S. Van der Zee (2020) Reporting cybercrime victimization: determinants, motives, and previous experience. *Policing: an international journal* 43(1) 17-34.

Jong, L., E.R. Leukfeldt & S. van de Weijer (2018) Aangiftebereidheid na slachtofferschap van cybercrime. *Tijdschrift voor Veiligheid*. 17(1-2) 66-78.

Weijer, van de, S., E.R. Leukfeldt, & W. Bernasco (2018) Reporting crime to the police: a comparison between traditional crime and cybercrime. *European Journal of Criminology*. DOI: 10.1177/1477370818773610.

Van de Weijer, S., E.R. Leukfeldt & S. Van der Zee (2021) Reporting cybercrime victimization of SMEs: determinants, motives, and previous experience. p303-325. In: Weulen Kranenbarg, M. & E.R. Leukfeldt (eds) Cybercrime in Context: the Human Factor in Victimization, Offending, and Policing. Springer.

Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime

Ambtenaren openbare orde en veiligheid spelen een centrale rol in de zorg voor maatschappelijke veiligheid. Hun focus ligt van oudsher op de preventie van slachtofferschap van veelvoorkomende criminaliteit (zoals diefstal, vernielingen en vandalisme) en high impact crime (zoals woninginbraak, overvallen en straatroven) binnen hun verzorgingsgebied. Intussen heeft de digitalisering van de samenleving een ongeëvenaarde gelegenheid voor criminaliteit gecreëerd. De totale maatschappelijke schade van cybercrime werd voor 2018 op 10 miljard euro geschat (1% van BNP). Uit cijfers van het CBS blijkt dat tussen 2012 en 2018 het slachtofferschap van hacken zelfs hoger lag dan dat van fietsendiefstal.

Nederlandse gemeenten hebben cybercrime in de afgelopen twee jaar dan ook breed als beleidsprioriteit omarmd. Maar in de vertaling van deze beleidsprioriteit naar concrete acties gaat het mis. Duidelijk is dat de ambtenaren openbare orde en veiligheid een taak voor zichzelf zien in de preventie van cybercrime, maar waar te beginnen? In dit project bundelen professionals uit twaalf gemeenten en vier regionale veiligheidsnetwerken hun slagkracht met onderzoekers van twee hogescholen en het NSCR voor de cyberweerbaarheid van de samenleving.
De hoofdvraag van dit project luidt: *Met welke interventies kunnen ambtenaren openbare orde en veiligheid de cyberweerbaarheid van burgers en bedrijven binnen hun gemeente vergroten?*

Middels actieonderzoek werken professionals van gemeenten en regio's samen met onderzoekers aan het verbeteren van bestaande en het ontwikkelen van nieuwe interventies. Daarbij verscherpen zij hun beeld van de omvang en achtergronden van slachtofferschap van cybercrime. Ook onderzoeken zij achtergronden en verklaringen voor het risicobewustzijn en preventief gedrag onder doelgroepen. Deze inzichten worden in verschillende iteraties aangevuld met effectstudies, om tot een set beproefde interventies te komen waarmee de cyberweerbaarheid van burgers en bedrijven zal toenemen.

In het eerste deelrapport staan de volgende twee vragen centraal:

- Voor welke doelgroepen zijn interventies om het risicobewustzijn en het preventieve gedrag te vergroten het meest noodzakelijk?

- Voor welke typen cybercrime zijn interventies om het risicobewustzijn en het preventieve gedrag van deze doelgroepen te vergroten het meest noodzakelijk?

Op basis van een literatuurstudie en interviews met experts en praktijkpartners komen we tot drie doelgroepen waarvoor interventies ontwikkeld gaan worden: jongeren, ouderen en mkb'ers. Binnen die doelgroepen richten we ons vervolgens op specifieke delicten: phishing, shame sexting / sextortion, malware/ ransomware, vriend- in-noodfraude en geldezelen.

Lopend onderzoek (2019-2022). Uitgevoerd door Saxion Hogeschool, De Haagse Hogeschool en NSCR. Gefinancierd door SIA. Betrokken onderzoekers: Remco Spithoven, Rutger Leukfeldt, Susanne van 't Hoff-de Goede, Luuk Bekkers, Ellen Misana-ter Huurne, Ynze van Houten en Michelle Walther.

Publicaties binnen dit lopende onderzoek:

Leukfeldt, E.R., R. Spithoven & E. Misana-ter Huurne (2020) De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. Cahiers Politiestudies 2020(3) 203-223.

Misana-ter Huurne, E., S. van 't Hoff-de Goede, L. Bekkers, Y. van Houten, M. Walther, R. Spithoven & E.R. Leukfeldt (2021) Cyberweerbaarheid. Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime Kwetsbare doelgroepen en bijbehorende typen cyberdelicten Geïntegreerd deelrapport werkpakketten 1 en 2. Deventer/Den Haag: Saxion Hogeschool / De Haagse Hogeschool.

Cybercrisis en de rol van de gemeente

Gemeenten kunnen op twee manieren betrokken raken bij een cybercrisis: als slachtoffers of als actor bij de bestrijding ervan. Gemeenten zijn zelf tegenwoordig in hoge mate afhankelijk van digitale systemen. Uitval van deze systemen kan grote gevolgen hebben. Recente voorbeelden hebben we gezien bij de gemeenten Lochem (2019) en Hof van Twente (2020). Verder kunnen gemeenten een rol spelen bij het minimaliseren van fysieke gevolgen van een cybercrisis bij een organisatie gevestigd in de gemeente. Bijvoorbeeld een groot ziekenhuis dat door een cyberaanval de deuren (deels) moet sluiten. Ook dan kunnen gemeenten betrokkenen zijn en samen met de veiligheidsregio(s) en andere partners moeten acteren om de problemen aan te pakken.

Cybercrisis binnen gemeenten zijn daarom binnen dit onderzoek op twee manieren bekeken: de gemeenten als slachtoffer of als betrokkene.

Onderzoeksdoelen en vragen

Doel is om inzicht te verschaffen in de ervaringen die gemeentelijke medewerkers hebben met cybercrisis als 'slachtoffer' en 'betrokkene' en hoe zij kijken naar de rollen en uitdagingen die er zijn. Dit doel is opgesplitst in twee hoofdvragen:

- Welke uitdagingen ervaren gemeenten bij (de voorbereiding op) cybercrisis die de gemeentelijke organisatie raken?

- Welke uitdagingen ervaren gemeenten bij (de voorbereiding op) cybercrisis die plaatsvinden bij organisaties gevestigd in de gemeente en (kunnen) leiden tot problemen in het fysieke domein?

Helaas moeten we concluderen dat gemeenten beperkt voorbereid zijn op cybercrisis en onvoldoende zicht hebben op in hoeverre bestaande plannen en niet geformaliseerde werkwijzen voldoende zijn om de impact van cybercrisis te kunnen beperken. Dit komt mede omdat er niet of weinig wordt geoefend. Verder blijkt dat de CISOs en AOV-ers elkaar nog niet goed genoeg kunnen vinden.
Ten slotte blijkt dat de deelnemende gemeenten binnen dit onderzoek nog geen ervaring hebben met cybercrisis waarbij ze enkel 'betrokkene' zijn.

Ebbers,S., J. Koch, J. Jansen, J. Groenendaal, W. Bantema & E.R. Leukfeldt (2021) Cybercrisis bij gemeenten: een verkennend onderzoek naar de voorbereidingen, ervaringen en uitdagingen. Den Haag/Leeuwarden: De Haagse Hogeschool / NHLStenden Hogeschool.

Parels in de lokale aanpak van cybercrime

Met de digitalisering van onze samenleving krijgen steeds meer delicten een digitale component. Het kan daarbij bijvoorbeeld gaan om het inbreken in een computer van een ex-partner, het platleggen van de website van een school middels een DDoS-aanval, of het plegen van fraudes via online verkoopsites. Criminelen maken geen onderscheid tussen offline en online methoden om hun doel te bereiken en hebben inmiddels de mogelijkheden die digitalisering hun biedt omarmd. Daarbij is te zien dat sommigen zich specialiseren in het plegen van cybercriminaliteit, terwijl anderen het gebruiken als uitbreiding van hun criminele repertoire en gedigitaliseerde vormen van criminaliteit plegen. Online delicten zullen steeds vaker onderdeel worden van het dagelijkse werkaanbod van politiemedewerkers. Slachtofferschap van dergelijke delicten is nu al hoog – Nederlanders worden inmiddels vaker slachtoffer van hacken dan van fietsendiefstal (respectievelijk 4,9% en 4%) – en neemt met de steeds verdergaande digitalisering alleen maar toe.

Dat "de wereld naar de wijk is gekomen" blijkt ook uit de Strategische Agenda Politieacademie 2018-2022 waarin "politiewerk verbonden met wijk, web en wereld" een belangrijke pijler is. Feitelijk is 'digitaal' nu 'normaal' geworden en krijgen politiemedewerkers door de hele organisatie heen met allerlei varianten van online criminaliteit te maken – op nationaal, regionaal en lokaal niveau. De aanpak van online criminaliteit heeft eerst op nationaal niveau (bijvoorbeeld met de oprichting van het Team High Tech Crime en het Dark Web Team) en later op eenheidsniveau (met de komst van de zogenaamde cybercrime teams) de laatste jaren vorm gekregen. Ook op lokaal niveau bestaan allerlei initiatieven zoals de digitale buurtagent.

De hoofdvraag van dit onderzoek is: Wat zijn de parels (best practices) bij de regionale en lokale afhandeling van online criminaliteit? Hoe zien de parels er uit en zijn ze toepasbaar binnen andere eenheden? Met de kennis die dit onderzoek oplevert kunnen eenheden van elkaar leren en procesmatige veranderingen binnen regionale en lokale eenheden – de parels – doorvoeren.

Lopend onderzoek (2019-2022). Uitgevoerd door Jim Schiks, Susanne van 't Hoff-de Goede en Rutger Leukfeldt. Gefinancieerd door Politie en Wetenschap.

HACKSHIELD

- **HackShield is een project, spel en maatschappelijke beweging.** HackShield is een project, spel en maatschappelijke beweging om kinderen van 8 tot 12 jaar en Nederland cyberveiliger te maken. De 'Hero-centred-design' filosofie van de makers van het spel staat hierbij centraal. Hierin wordt de eindgebruiker centraal gesteld en een (fictieve) rol gegeven die de gebruiker niet heeft in de echte wereld. De filosofie is gebaseerd op literatuur over 'storytelling', 'gamification' en 'problem solving'.

- **De uitvoering van het initiatief is gestandaardiseerd met ruimte voor eigen (lokale) invulling.** Het initiatief heeft binnen de onderzochte gemeenten bestaan uit een promotiecampagne om kinderen HackShield te laten spelen, een periode waarin kinderen het spel spelen en een huldiging van de beste spelers door de burgemeester en politie. Vooraf hebben gemeenten informatie en instructies gehad over de invulling van het initiatief en tegelijkertijd ruimte gehad om hiervan af te wijken. Verschillen bestaan in communicatiekanalen die zijn gebruikt en de wijze waarop huldigingen hebben plaatsgevonden.

- **Deelnemers, ouders en uitvoerders zijn tevreden.** Deelnemers, ouders en uitvoerders zijn tevreden over het verloop van het project. Uitvoerders zijn tevreden omdat er duidelijke instructies en goede begeleiding was en omdat er door het project meer aandacht is voor cybercriminaliteit. Bijna alle uitvoerders zouden bij een toekomstige projectronde opnieuw meedoen. Deelnemers zijn enthousiast omdat zij het spel leuk en leerzaam vinden. Alle ouders zouden het spel aanbevelen aan anderen.

- **Sterke punten en verbeterpunten.** De inzet van partners die betrokken zijn bij het initiatief, de goede ondersteuning vanuit de initiatiefnemers en de kleine inspanning die het vraagt voor gemeenten om mee te doen zorgen voor een goed verloop van het initiatief. Winst is te behalen door scholen beter bij het project te betrekken en door meer levels aan het spel toe te voegen.

- **Voer een effectevaluatie uit.** Voor de meeste uitvoerders is het onduidelijk in hoeverre de doelen van HackShield worden behaald. Deelnemers geven allemaal aan iets te hebben geleerd, bijvoorbeeld over sterke wachtwoorden, het herkennen van phishing mails en hoe je kunt voorkomen dat je wordt gehackt. Onduidelijk blijft echter wat de daadwerkelijke effecten zijn van het initiatief. Vervolgonderzoek in de vorm van een effectevaluatie is een noodzakelijke volgende stap. Zo kan er een voor- en nameting plaatsvinden met betrekking tot de kennis die deelnemers en ouders daadwerkelijk opdoen, door vragenlijsten op te stellen die deze kennis toetsen.

1 De dataverzameling heeft plaatsgevonden tussen september 2020 en februari 2021.

2 Bijna de helft van de geïnterviewde deelnemers is 'tester'. Testers zijn kinderen die alle levels van het spel uitgespeeld hebben en aangeven dat ze tester willen worden om het spel te verbeteren. De resultaten van het onderzoek zijn dan ook gebaseerd op de meest fanatieke spelers, wat een vertekend beeld kan geven.

Lectoraat Maatschappelijke Veiligheid
Hogeschool Saxion

Centre of Expertise Cybersecurity
De Haagse Hogeschool

Schiks, J., S. Hansen, E. Foppen, E.R. Leukfeldt en R. Spithoven (2021). Hackshield in Noord-Holland. Een evaluatie van de implementatie en resultaten van HackShield in Noord-Hollandse gemeenten. Deventer/Den Haag: Saxion Hogeschool, De Haagse Hogeschool.

Evaluatie van de pilot HackShield in gemeenten Noord-Holland

Doel

Het initiatief 'HackShield in gemeenten Noord-Holland' evalueren door middel van een beknopte plan- en procesevaluatie[1].

Methode

Documentanalyse en 30 interviews met ontwikkelaars, uitvoerders en deelnemers[2].

HACKSHIELD

NH Samen Veilig

Hack_Right: een alternatief voor jeugdige hackers?

Hack_Right is een alternatief of aanvullend straftraject voor jeugdige daders die hun eerste delict cybercriminaliteit plegen. Het is de eerste interventie in Nederland die zich richt op (jonge) cybercriminelen en is daarmee een unieke interventie.

Wij voerden een plan- en procesevaluatie uit van Hack_Right. De volgende onderzoeksvragen staan centraal: (1) Wat is Hack_Right en hoe is Hack_Right theoretisch onderbouwd? (2) Hoe zijn de tot nu toe uitgevoerde Hack_Right trajecten verlopen? (3) Hoe hebben alle betrokkenen de tot nu toe uitgevoerde Hack_Right trajecten ervaren?

In totaal zijn 28 interviews afgenomen met respondenten die op verschillende manieren betrokken zijn bij de Hack_Right interventie: twee interventieontwikkelaars, vijf toewijzers, elf uitvoerders en tien deelnemers.

Hack_Right is ontstaan vanuit signalen uit de praktijk: een grote toestroom van verdachten met een 'nieuw' of 'ander' profiel waar nog geen effectieve interventie voor bestaat. De onderzoekers concluderen echter dat de wetenschappelijke basis voor deze aanleiding ontbreekt. Empirisch onderzoek naar kenmerken van cybercriminelen ontbreekt simpelweg nagenoeg. We weten dus of, als we het hebben over cybercriminelen, we het hebben over een groep daders met een afwijkend profiel ten opzichte van de daders van allerlei vormen van traditionele offline criminaliteit.

Dat wetenschappelijke inzichten in enkele belangrijke aspecten van Hack_Right ontbreken erkennen de ontwikkelaars, maar tegelijk geven ze aan dat het belangrijk is om te starten en daarbij nieuwe inzichten uit de wetenschap in de gaten te blijven houden. Het onderzoek laat zien dat, om te kunnen doorgroeien tot een volwaardige interventie, er een stevigere basis nodig is. Onderhavig onderzoek is daarbij een eerste stap, maar zeker niet de laatste. Inzichten in bijvoorbeeld kenmerken en criminogene factoren van de doelgroep zijn noodzakelijk om een effectieve interventie op te zetten.

De uitvoerders van de interventie zijn over het algemeen tevreden over het verloop van de Hack_Right trajecten omdat deelnemers de trajecten positief hebben afgerond en wat hebben geleerd. Deelnemers verschillen echter van mening over de mate waarin zij tevreden zijn over het Hack_Right programma. Minder tevreden deelnemers geven aan dat opdrachten te makkelijk waren of dat er geen duidelijk programma was. Een belangrijke aanbeveling is dan ook om de programma-

integriteit te verbeteren. Door de vele verschillende invullingen die Hack_Right deelnemers hebben gehad is niet duidelijk welke componenten van de interventie kunnen leiden tot bepaalde uitkomsten. Uitgewerkte producten en handleidingen voor de uitvoering van die producten ontbreken. Voor een goede uitvoering van de interventie, maar ook als eis voor een goede evaluatie van de werkzame elementen van de interventie is het noodzakelijk dit te verbeteren.

Schiks, J.A.M., S. van 't Hoff-de Goede & E.R. Leukfeldt (2021) Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right. Den Haag: Sdu uitgevers.

DEEL 3:

VOORUITBLIK

Vooruitblik

Dit boek geeft een mooi overzicht van de onderzoeken die we de afgelopen jaren hebben uitgevoerd. Hopelijk laat het ook zien dat we de belofte die we bij de start van het onderzoeksprogramma deden grotendeels waar hebben gemaakt. Dat oordeel laat ik verder aan de lezer over. Wat in ieder geval duidelijk mag zijn is dat binnen alle vier de onderzoekslijnen flink wat onderzoeken zijn geïnitieerd.

Slachtofferschap van cyberaanvallen blijkt veelvoorkomend zijn. We hebben echt te maken met een groot maatschappelijk probleem. Grootste lacune is momenteel dat het mkb vaak als één geheel wordt gezien. Dat doet geen recht aan de verschillen tussen bedrijven (in omvang, IT-afhankelijkheid, branche, etc). Toekomstig onderzoek naar slachtofferschap moet daarom veel meer aandacht hebben voor de diversiteit binnen het mkb.

De impact van cyberaanvallen is een tweede aspect van slachtofferschap dat momenteel nog onderbelicht is. We weten dan wel dat slachtofferschap hoog is, maar wat precies de gevolgen zijn is lang niet altijd duidelijk. Ook daar moet de komende jaren nog veel onderzoek naar gedaan worden.

Weerbaarheid was al één van de onderzoekslijnen binnen ons onderzoeks-programma. Op dat thema hebben we inmiddels behoorlijk wat onderzoek gedaan, maar ook hier is duidelijk dat we er nog niet zijn. Weerbaarheid is een van de sleutels om slachtofferschap en de impact daarvan omlaag te krijgen. De digitalisering van onze samenleving gaat echter steeds verder. Tijdens de coronapandemie hebben we al goed kunnen zien hoe de toekomst er uit gaat zien: we gaan veel meer vanuit huis of andere locaties werken en worden nog van technologie. Slachtofferschap is dus bijna een voldongen feit. Meer inzicht in hoe theoretische modellen over weerbaarheid in de praktijk gebracht kunnen worden blijft dan ook hard nodig.

Een belangrijke observatie - die wellicht niet direct terug is te zien in dit overzicht van onderzoeksresultaten – is dat het in de praktijk ongelofelijk lastig blijkt om ondernemers te bereiken. De afgelopen jaren heb ik tal van goede initiatieven gezien om ondernemers te helpen en deden we zelf relevant onderzoek voor en met ondernemers. De doelgroep zelf blijkt echter lastig in beweging te krijgen. Uit onderzoek weten we inmiddels dat ondernemers zich wel degelijk bewust zijn van cyberrisico's. Alleen voorlichting over de gevaren online zal ze dus niets wijzer maken (sterker nog, kan een tegenovergesteld effect hebben). Ondernemers blijken vooral de kans op eigen slachtofferschap en de gevolgen daarvan te onderschatten.

Daarbij besteden veel ondernemers hun IT uit en denken daarmee ook grotendeels af te zijn van verantwoordelijkheid omtrent hun cybersecurity. Fundamenteel en praktijkgericht onderzoek is nodig naar hoe we ondernemers dan wel kunnen bereiken en hoe we ze kunnen aanzetten tot het nemen van maatregelen.

Een ander thema dat pas in een wat later stadium een plaats kreeg in ons onderzoeksprogramma is ketenweerbaarheid. Na het uitvoeren van enkele verkennende onderzoeken lijkt ook dit een veelbelovende manier om te komen tot weerbaardere organisaties. Vrijwel alle bedrijven zitten immers in ketens: van toeleveranciers tot samenwerkingspartners en bedrijven die letterlijk een pand delen. Toekomstig onderzoek moet zich dan ook richten op hoe je binnen ketens samenwerking op het gebied van cybersecurity kunt stimuleren.

Tot zover de aanvullingen die we gaan doen binnen de onderzoekslijnen 'aard en omvang van slachtofferschap' en 'cyberweerbaarheid'. Het moge duidelijk zijn dat we behoorlijk wat onderzoeken gedaan hebben binnen beide thema's en dat er ook de komende jaren nog genoeg te doen is. Twee onderzoekslijnen waar we nog flink aan de weg moeten timmeren zijn 'aard van cybercriminaliteit' en 'aanpak van cybercriminaliteit'. Daar moeten we dan ook de komende jaren vooral in investeren.

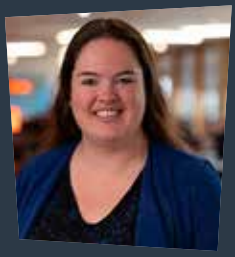
Zoals in het overzicht in dit boek te zien is zijn binnen die twee onderzoekslijnen al diverse onderzoeken geïnitieerd. Echter staat het onderzoek binnen die twee lijnen nog echt in de kinderschoenen. Er is relatief veel kwalitatief en verkennend onderzoek gedaan en het is hoog tijd om meer te investeren in hoogwaardig praktijkgericht onderzoek naar de criminelen en naar de aanpak van cybercrime. Immers, zonder zicht op de criminelen is het bijna onmogelijk om effectieve maatregelen te ontwikkelen die slachtoffers moeten beschermen tegen diezelfde criminelen. Daarnaast gaat de aanpak van cybercrime nu vaak niet verder dan het bestuderen van de rol van de politie, eventueel in samenwerking met private partijen en ligt er vooral veel verantwoordelijkheid bij de ondernemer zelf: die moet maar zorgen voor een betrouwbare leverancier die de juiste bescherming biedt tegen onbekend gevaar. Deze onderwepen krijgen de komende jaren dan ook een centrale plek binnen ons onderzoeksprogramma.

De onderzoekers

Dr. Rutger Leukfeldt is lector Cybersecurity in het mkb en directeur van het Kenniscentrum Cybersecurity bij de Haagse Hogeschool. Tevens is Rutger senior onderzoeker bij het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). Daarnaast is Rutger voorzitter van de Cybercrime Working Group van de European Society of Criminology. Rutger heeft zo'n 15 jaar ervaring met praktijkgericht wetenschappelijk onderzoek naar cybersecurity en cybercrime voor zowel publieke als private opdrachtgevers.

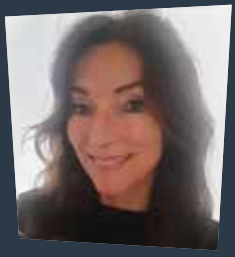
Dr. Rick van der Kleij

Rick van der Kleij is psycholoog en voor 0,5 FTE senior onderzoeker bij het lectoraat. Daarnaast is Rick voor 0,5 FTE verbonden aan TNO. Zijn onderzoek naar cybersecurity richt zich op manieren om de veerkracht van bedrijven tegen cyberaanvallen te verhogen. Een veerkrachtige organisatie heeft de capaciteit om adequaat te reageren op cyberincidenten en kan bovendien in veel gevallen voorkomen dat er problemen ontstaan.



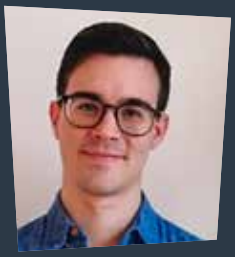
Dr. Susanne van 't Hoff-de Goede

Susanne van 't Hoff-de Goede is criminoloog en voor 0,7 FTE als onderzoeker verbonden aan het lectoraat Cybersecurity in het mkb. Haar onderzoek richt zich op het verkrijgen van inzicht in cybercriminaliteit en de aanpak van cybercriminaliteit gericht op mkb'ers.



Maaike Vergeer

Senior Managementassistent en spin in het web van het lectoraat.



Dr. Asier Moneva Pardo

Asier is postdoctoraal onderzoeker op het gebied van de menselijke factor in cybercrime aan De Haagse Hogeschool en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving. Met een achtergrond in criminologie behaalde hij zijn PhD over de toepasbaarheid van het kader voor omgevingscriminologie en criminaliteitsanalyse op cybercriminaliteit aan de Miguel Hernandez-universiteit in Elche (Spanje). Zijn onderzoek richt zich op de analyse en preventie van cybercriminaliteit vanuit een situationeel perspectief, waarbij hij gebruik maakt van kwantitatieve methoden.

Raoul Notté Ma MSc

Raoul Notté heeft een achtergrond in de bestuurs- en organisatiewetenschappen en informatiemanagement. Raoul werkt voor 0,6 FTE bij het lectoraat en is voor 0,4 FTE verbonden aan de opleiding HBO-ICT. Zijn onderzoek naar cybersecurity richt zich enerzijds op de (organisatie van) maatregelen voor het voorkomen van incidenten, anderzijds richt hij zich op de impact van cyber incidenten en de behoeften die hieruit voortvloeien.

Michelle Ancher MSc

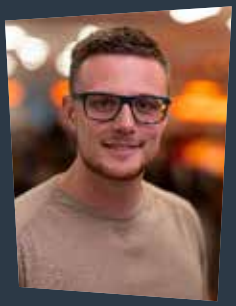
Michelle Ancher is docent bij de opleiding HBO-ICT (richting Information Security Management) en als onderzoeker voor 0,2 FTE verbonden aan het lectoraat. Ze is sociaal psycholoog en richt zich op de menselijke factor van information security. Haar onderzoek richt zich op factoren die het menselijk (cyber) gedrag beïnvloeden en creatieve manieren waarop je gedrag kunt veranderen.

Marco Romagna LLM Ma

Marco Romagna is lecturer in 'Legal and criminological aspects of cyber security' and has a 0,6 FTE appointment as researcher for the Centre of Expertise Cyber Security. He is external PhD candidate at Leiden University with a project on "Hacktivism: honorable cause and/or serious threat?". Beside hacktivism and cyber security, his main research interests focus on cybercrime, criminology and the related criminal law.

Jim Schiks MSc

Jim Schiks is voor 0,5 FTE junior onderzoeker op het gebied van cybercriminaliteit bij de Haagse Hogeschool en ook voor 0,5 FTE verbonden aan het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving. Hij heeft een achtergrond in bedrijfskunde en criminologie. Jim verricht onderzoek naar de wijze waarop personen bij cybercriminaliteit betrokken raken en naar interventies waar deze personen aan worden onderworpen door politie en justitie.



Luuk Bekkers MSc

Luuk Bekkers is voor 1,0 FTE verbonden aan het lectoraat als junior onderzoeker. Luuk heeft een master in zowel de psychologie als in de criminologie. Bij het kenniscentrum kan hij beide expertises toepassen binnen het werkveld van cybercriminaliteit en slachtofferschap daarvan, waarbij menselijke aspecten vaak een centrale rol spelen. Luuk doet praktijkgericht onderzoek naar onder meer het cyber(on)veilig gedrag van werknemers en het ontwikkelen van interventies om dit gedrag te verbeteren.

Joeri Loggen

Joeri loggen is voor 1,0 FTE verbonden aan het lectoraat als promovendus. Joeri heeft een master criminologie en doet onderzoek naar interventies tegen cybercriminaliteit.

Sifra Matthijssen

Sifra Matthijssen is voor 1,0 FTE verbonden aan het lectoraat als promovendus. Siftra heeft een master criminologie en doet onderzoek naar crime scripts van cybercrimelen.

Dr. Elif Kiesow Cortez

Between 2018-2020, Elif Kiesow Cortez was appointed for 0,2 FTE to the Lectoraat. Elif is also a lecturer in data protection and privacy compliance in the International and European Law Program. Elif's research is focused on utilizing economic analysis of law to provide recommendations for solving cooperation problems between public and private actors in the domains of data protection and privacy.

Dr. Juul Gooren

In 2019 en 2020 was Juul Gooren verbonden aan het lectoraat. Juul is docent bij de Faculteit Bestuur, Recht en Veiligheid bij de opleiding Integrale Veiligheidskunde/Safety & Security Management Studies. Juul doet onderzoek naar 'Resilience' als theoretisch model voor zowel industriële als publieke veiligheid.

nscr
Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

DE HAAGSE
HOGESCHOOL

Johanna Westerdijkplein 75
2521 EH Den Haag