Lectoraat Cybersecurity in het mkb

JAARVERSLAG 2019

Dr. Rutger Leukfeldt

27 februari 2020

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

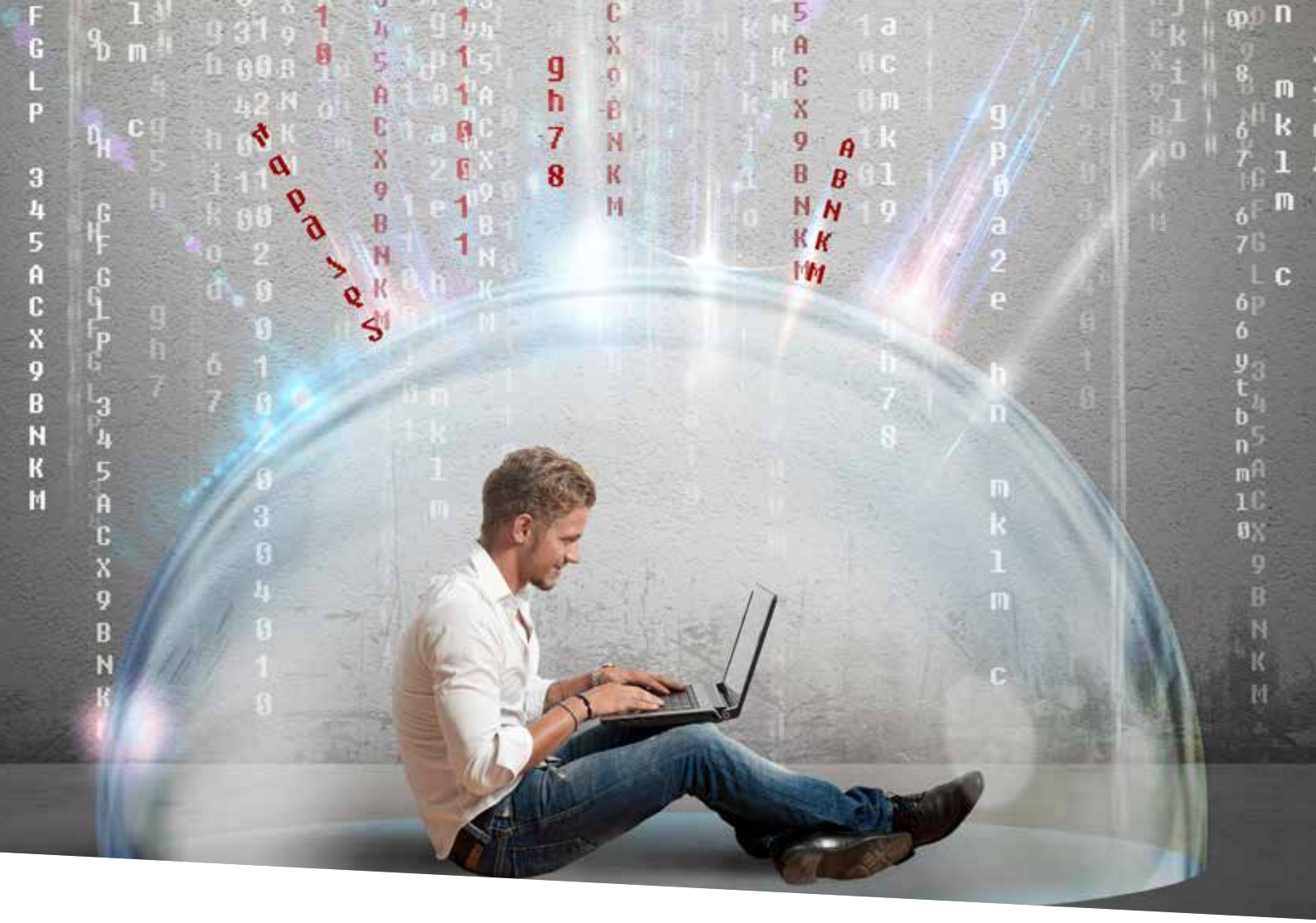
Aanleiding

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 – 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 bezighouden met het tegenhouden van cyberaanvallen.

“Cybercrime – en daarmee cybersecurity – is een groot maatschappelijk probleem.”

Rutger Leukfeldt, lector

Rutger Leukfeldt, lector



Empirisch onderzoek naar de menselijke factor bij cybercrime en cybersecurity is schaars. De onder de redactie van de lector uitgebrachte onderzoeksagenda 'The human factor in cybercrime en cybersecurity' maakt dit helder. In die onderzoeksagenda zijn tientallen onderwerpen geïdentificeerd waar de komende jaren onderzoek naar moet worden gedaan omdat basale kennis ontbreekt. Tegelijkertijd zit het werkveld te springen om bruikbare kennis over manieren om zich te beschermen tegen cyberaanvallen. Dat laatste is iets wat we zeker gemerkt hebben de afgelopen jaren. Al voor de officiële start van het lectoraat stroomden de verzoeken binnen van gemeenten, brancheorganisaties en bedrijven om gezamenlijk onderzoek te doen. Dit is dan ook de reden dat we ondanks dat het lectoraat nog maar kortgeleden is ingesteld, we al flink wat onderzoeken voor en met de praktijk uitvoeren.

Het lectoraat richt zich specifiek op cybercrime en cybersecurity in het mkb[1]. Het mbk is de backbone van de Nederlandse economie. Mkb-bedrijven vormen 61% van het Nederlandse BBP, zorgen voor 70% van de werkgelegenheid en hebben een totale omzet van 888 miljard euro. Mkb'ers worden echter relatief vaak slachtoffer van cyberaanvallen en hebben niet de capaciteit om zich te weren tegen dergelijke aanvallen. Als sector is het mkb weliswaar groot, maar de omvang van individuele bedrijven is beperkt. Dit brengt kwetsbaarheid met zich mee. Het is voor mkb-bedrijven moeilijker dan voor grote ondernemingen om voldoende capaciteit vrij te maken om de secundaire processen in hun organisatie effectief te organiseren. Dat geldt ook voor cybersecurity. Een vooronderzoek van het Centre of Expertise Cyber Security van de Haagse Hogeschool[2] laat dan ook zien dat een op de vijf mkb-ondernemers die deelnamen aan het onderzoek slachtoffer zijn geworden van een cyberaanval.

1 Onder mkb verstaan we bedrijven met minder dan 250 werknemers en waarvan de jaaromzet niet hoger is dan 50 miljoen euro en het jaarlijkse balanstotaal niet hoger is dan 43 miljoen euro. Voor de goede orde: hier vallen dus ook zelfstandigen zonder personeel onder.

2 https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf

Missie

Van groot belang bij het uitvoeren van onderzoeken binnen de in dit document beschreven onderzoekslijnen is het in stand houden en verder uitbouwen van de regionale community van mkb'ers, overheidsinstellingen, politie en justitie en cybersecurity bedrijven die de HHs nu heeft. Hierdoor kunnen de ontwikkelingen in de grootste problemen die mkb'ers ondervinden geïdentificeerd worden. Bovendien biedt dit gelegenheid tot praktijkgericht onderzoek samen met mkb'ers. Daarnaast kunnen deze praktijkgerichte onderzoeken gebruikt worden om te inventariseren wat veelbelovende richtingen zijn voor theorievormend onderzoek. Wetenschappelijk onderzoek naar cybercrime en cybersecurity staat namelijk nog in de kinderschoenen. Er is daarom een grote behoefte aan theorievormend onderzoek. De onlangs uitgebrachte onderzoeksagenda 'The Human Factor in Cybercrime and Cybersecurity' laat dit duidelijk zien. Het merendeel van de wetenschappelijke onderzoeken naar cybercrime en cybersecurity kent een sterk technologisch karakter. De focus ligt op het ontwikkelen van tools en technieken om incidenten te detecteren of tegen te houden. Onderzoek naar de menselijke factor binnen cybercrime en cybersecurity is noodzakelijk om de stap te maken van het tegenhouden van incidenten naar het voorkomen ervan.

“ Visie op praktijkgericht onderzoek: Vertrekken vanuit de praktijk zonder de theorie te vergeten ”

Doelen

De bevinding dat het mkb van groot belang is voor de Nederlandse economie én dat datzelfde mkb vaak slachtoffer is van cyberaanvallen staat in schril contrast met het wetenschappelijk en praktijkgericht onderzoek dat wordt uitgevoerd op dit gebied. Sociaalwetenschappelijk onderzoek naar cybersecurity en cybercrime staat nog in de kinderschoenen (zie bijvoorbeeld Leukfeldt e.a. 2017, Holt en Bossler, 2014), maar op een enkele verkennende studie na ontbreekt dit type onderzoek compleet als het gaat om cybercrime en cybersecurity in relatie tot het mkb.

Het doel van het lectoraat is dan ook om de kennispositie van het mkb op het gebied van cybercrime en cybersecurity te vergoten om zo het slachtofferschap en de impact van cyberaanvallen onder mkb'ers te verlagen. Omdat er nagenoeg geen studies gedaan zijn 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? Selecteren ze specifieke mkb-bedrijven of vallen ze simpelweg zoveel mogelijk bedrijven aan? En van welke zwakke plekken maken criminelen gebruik om hun aanvallen uit te voeren? Tegelijkertijd moet worden onderzocht hoe mkb'ers weerbaarder gemaakt kunnen worden. Het is immers een gegeven dat het slachtofferschap onder mkb groot is en dat een aanzienlijk deel van het mkb vroeger of later te maken krijgt met een cyberaanval. Hoe weerbaar zijn mkb'ers op dit moment eigenlijk? Weten ze 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 een rol bij het beschermen tegen cyberaanvallen. Daarom moet onderzocht worden welke rol politie en justitie nog hebben bij de aanpak van cybercrime gericht op het mkb en welke andere partijen een rol zouden moeten hebben.

“ Het vergroten van de kennispositie van het mkb op het gebied van cybercrime en cybersecurity om zo het slachtofferschap en de impact van cyberaanvallen onder mkb’ers te verlagen. ”

Vier onderzoekslijnen

Het doel van dit lectoraat – de kennispositie van het mkb op het gebied van cybercrime en cybersecurity vergroten om zo het slachtofferschap en de impact van cyberaanvallen onder mkb’ers te verlagen – wordt bereikt door het uitvoeren van praktijkgericht wetenschappelijk onderzoek. Zoals hierboven beschreven staat zijn verschillende thema’s van belang. Het lectoraat kent dan ook vier onderzoekslijnen, waarbinnen steeds het mkb centraal staat:

1. Aard en omvang van slachtofferschap
2. Aard van cybercriminaliteit
3. Weerbaarheid
4. De aanpak van cybercriminaliteit

Onderzoeksthema's Haagse Hogeschool

De constatering dat onderzoek naar de menselijke factor binnen cybercrime 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. Zowel de HHs als het NSCR hebben cybersecurity en cybercrime al enkele jaren geleden als prioriteit benoemd en en hebben elk afzonderlijk onderzoeksprogramma's op dit gebied. Het is echter steeds duidelijker dat bij onderzoek naar cybercrime en cybersecurity het beste van beide werelden nodig is. Voor de HHs geldt dat onderzoeken toepassingsgericht moeten zijn en dat de nieuwste onderzoeksmethoden en –technieken moeten worden toegepast om hoogwaardige producten op te leveren. Voor het NSCR geldt dat onderzoeken niet alleen fundamentele kennis moeten opleveren, maar liefst ook relevant voor de praktijk zijn. Het lectoraat heeft dan ook de nadrukkelijke opdracht deze twee onderzoeksprogramma's te verbinden. Ik zal in deze inleiding een beknopte schets geven van de onderzoeksprogramma's van deze organisaties, en van de toekomstige onderzoeken binnen het lectoraat.

De HHs is sinds 2004 actief op het gebied van cybersecurity en heeft een Centre of Expertise Cybersecurity (CoECS). Het CoECS heeft tot doel om praktijkgericht onderzoek uit te voeren om zo organisaties te helpen die zelf niet voldoende middelen en/of expertise hebben om zich te beschermen tegen cyberaanvallen. Onder het CoECS ressorteren naast het lectoraat Cybersecurity in het mkb ook het lectoraat Cyber Security & Safety van Marcel Spruit en het lectoraat Network & Systems Engineering Cyber Security van Thomas Quillinan. Deze twee lectoraten richten zich op respectievelijk de organisatiekant van cybersecurity bij individuen en in middelgrote overheidsorganisaties, en op de technische kant van de beveiliging van IT systemen, met een bijzondere focus op het 'internet of things'. Het lectoraat Cybersecurity in het mkb focust op de menselijke kant van cybersecurity en sluit daarom aan op de bestaande lectoraten binnen het CoECS.

Binnen het lectoraat cybersecurity in het mkb werken onderzoekers die verbonden zijn aan de HHs en het NSCR samen aan cybercrime en cybersecurity onderzoek. De kennis en ervaring met het fundamentele onderzoek naar cybercrime van het NSCR wordt gekoppeld aan het toepassingsgerichte onderzoek aan de HHs. Hierdoor ontstaat een integraal onderzoeksprogramma dat het hele spectrum van relevant onderzoek naar cybercrime en cybersecurity beslaat: binnen het NSCR wordt het meer theoriegedreven fundamentele onderzoek uitgevoerd, vooral gericht op daders en dadersnetwerken, binnen de HHs wordt het meer 'slachtoffer- en aanpakgeoriënteerde' onderzoek uitgevoerd, en dan specifiek gericht op het mkb.

Over de lector

Dr. Rutger Leukfeldt

Dr. Rutger Leukfeldt is lector Cybersecurity in het mkb bij de Haagse Hogeschool en senior onderzoeker cybercrime en coördinator van het cybercrime cluster van het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). Leukfeldt heeft ruim 10 jaar ervaring met praktijkgericht wetenschappelijk onderzoek naar cybersecurity en cybercrime voor zowel publieke als private opdrachtgevers. Inmiddels heeft hij circa honderd publicaties op dit gebied en geeft jaarlijks tientallen lezingen bij zowel wetenschappelijke bijeenkomsten als bijeenkomsten van professionals. Enkele voorbeelden zijn onderzoek naar de cyberweerbaarheid van organisaties, werkwijzen en daderkenmerken van cybercriminelen, onderzoek naar slachtofferschap van cybercrime onder burgers en bedrijven en onderzoek naar de doorstroom van cybercrimezaken binnen de strafrechtketen. Leukfeldt promoveerde op een onderzoek waarbij hij naar de ontstaans- en groeiprocessen en criminele mogelijkheden van cybercriminele netwerken en ontwikkelde een model voor de politie en banken dat gebruikt kan worden om cyberaanvallen effectiever te bestrijden. Verder kreeg Rutger twee prestigieuze onderzoeksbeurzen om onderzoek naar cybercrime en cybersecurity te doen. In 2015 een Marie Curie Individual Fellowship (EU-subsidie voor veelbelovende onderzoekers) en in 2017 een Venisubsidie (NWO-subsidie voor onderzoekstalent). Ten slotte is Rutger voorzitter van de Cybercrime Working Group van de European Society of Criminology.

Kenniskringleden

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 verbonden als onderzoeker bij het lectoraat Cybersecurity in het mkb. Haar onderzoek richt zich op inzicht krijgen in cybercriminaliteit en de aanpak van cybercriminaliteit gericht op mkb'ers

Dr. Elif Kiesow Cortez
Elif Kiesow Cortez is 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.

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.

WIE ZIJN WIJ?

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 within the Faculty of IT & Design. 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.

Catherine Garcia van Hoogstraten, LL.M, J.D.
Catherine Garcia van Hoogstraten, is lecturer in Data Governance, Cybersecurity Law & Policy, ICT Law and eGovernance in the International Public Management Programme. Catherine has a 0,4 FTE position at the Lectoraat. Her research concerns Public Private Partnerships (PPPs) countering Cybercrimes.

Dr. Juul Gooren
Juul Gooren is docent bij de Faculteit Bestuur, Recht en Veiligheid bij de opleiding Integrale Veiligheidskunde/ Safety & Security Management Studies. Sinds medio 2019 is Juul voor 0,2 FTE verbonden aan het lectoraat. Juul doet onderzoek naar 'Resilience' als theoretisch model voor zowel industriële als publieke veiligheid.

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.


werkt

Onderzoekslijnen

Het doel van het lectoraat is het verbeteren van de kennispositie van het mkb op het gebied van cybercrime en cybersecurity om zo het slachtofferschap en de impact van cyberaanvallen onder mkb'ers te verlagen. Om dit doel te bereiken worden onderzoeken gedaan binnen de volgende onderzoekslijnen:

1. Aard en omvang van slachtofferschap
2. Aard van cybercriminaliteit
3. Weerbaarheid
4. De aanpak van cybercriminaliteit

Onderzoeksprojecten

ONDERZOEK 1: Slachtofferschap van cyberaanvallen

Doel: inzicht bieden in de aard en omvang van slachtofferschap van cyberaanvallen onder het mkb.
Betrokkenheid studenten/docenten: studenten hebben een deel van de dataverzameling gedaan en hebben tijdens onderzoeksblokken verder kunnen werken aan de ontwikkeling van een instrument om slachtofferschap te meten. Een docentonderzoeker is betrokken bij alle facetten van dit project.

ONDERZOEK 2: Cyberweerbaar maken mkb

Doel: Onderzoek naar weerbaarheid en cyberveilig gedrag in het midden- en kleinbedrijf (mkb) en manieren om via interventies en beleidsmaatregelen dit gedrag en daarmee de weerbaarheid te beïnvloeden.
Betrokkenheid studenten/docenten: 200+ studenten van ITD hebben een eerste versie van deze scan getest. Tijdens de pilot en de doorontwikkeling naar de app hebben diverse stagiaires meegewerkt aan de afname van de scans en de analyse van de resultaten. Een docentonderzoeker is betrokken bij alle facetten van dit project.

ONDERZOEK 3: Risicomodel voor cybersecurity mkb metaalbedrijven

Het doel van dit project is het ontwikkelen van een cybersecurity risicomodel dat toepasbaar is door mkb-metaalbedrijven. Met dit model krijgen ondernemers handvatten om zelfstandig cyberrisico's in kaart te brengen en de cybersecurity binnen hun organisatie te verbeteren.
Betrokkenheid studenten/docenten: Een docentonderzoeker is betrokken bij alle facetten van dit project. Studenten kunnen op basis van deze eerste verkenning vervolgonderzoeken uitvoeren.

ONDERZOEK 4: Verhogen aangiftebereidheid

Samengevat staat in deze studie daarom de vraag centraal waarom burgers en bedrijven zelden aangifte doen na slachtofferschap van cybercriminaliteit. De onderzoeksvraag van dit onderzoek is drieledig: allereerst onderzoeken we welke kenmerken van het cyberdelict (type cybercriminaliteit, ernst van het delict, etc.) en van de respondent (burger of organisatie) het doen van aangifte vergroten. Daarnaast zullen respondenten gevraagd worden naar hun motieven om wel of geen aangifte te doen van cybercriminaliteit. Ten slotte vragen we naar eerdere ervaringen met de politie met betrekking tot cybercriminaliteit en hoe deze ervaringen de aangiftebereidheid hebben beïnvloed.

ONDERZOEK 5: Cyberveilig gedrag

Het doel van dit onderzoek is om in kaart te brengen hoe het gesteld is met het cyberbewustzijn van burgers in Nederland, of ze daadwerkelijk cyberbewust handelen en om een eerste aanzet te geven interventies te ontwikkelen om het cyberbewustzijn op een hoger niveau te tillen.
Betrokkenheid studenten/docenten: Een docentonderzoeker is betrokken bij alle facetten van dit project. Studenten zijn betrokken bij het opzetten, uitvoeren en toetsen van de diverse interventies die ontwikkeld worden op basis van dit project. Op dit moment zijn we bezig om een virtueel lab op te zetten met studenten waarbinnen we experimenten kunnen doen op het gebied van veilig cybergedrag. Dit onderzoek is daar de directe aanleiding voor.

PROJECT 6: The Human Factor in Cybercrime

Editors: Rutger Leukfeldt, Thomas Holt (Michigan State University, US) Dit boek gaat over de menselijke factor in cybercriminaliteit: de daders, slachtoffers en organisaties die betrokken zijn bij de aanpak van cybercriminaliteit. Cybercriminaliteit wordt vaak gezien als een technisch misdrijf waarvoor alleen technische oplossingen nodig zijn, zoals antivirusprogramma's of geautomatiseerde hackingdetectietools. Deze misdaden worden echter gepleegd door individuen of netwerken van mensen, zijn gericht op individuen (als individuele burgers of als doelwitten binnen organisaties) en worden opgespoord en vervolgd door personen in dienst van publieke en private organisaties. Als gevolg hiervan speelt de menselijke besluitvorming een substantiële rol in de loop van criminele activiteiten.

Hoewel in bestaand onderzoek getracht is deze vragen afzonderlijk te beantwoorden, is er behoefte aan één boek waarin deze vragen worden beantwoord om een totaaloverzicht te geven van onze kennis over de menselijke factor in cybercriminaliteit. Dit boek probeert dit doel te bereiken door een verzameling werken van internationaal toonaangevende criminologen die vele facetten van daderschap, slachtofferschap en beleidsreacties behandelen.

PROJECT 7: Op zoek naar de parels van de lokale aanpak van cybercrime

Doel project: Inventarisatie en evaluatie van projecten van de politie die de aanpak van cybercrime moeten verbeteren. Beoogde resultaten/deliverables komend jaar voor onderwijs, praktijk en kennisdomein: Inzicht in wat effectieve projecten zijn die zorgen voor een betere aanpak van cybercrime. Direct bruikbaar resultaat voor de politie en lokale overheden. Indirect levert dit heel veel contacten op voor afstudeerders.

PROJECT 8: Hack_right. Evaluatie interventie.

Doel project: Evaluatie interventie gericht op jeugdige Nederlandse cybercriminelen. Beoogde resultaten/deliverables komend jaar voor onderwijs, praktijk en kennisdomein: inzicht in pathways die naar cybercrime leiden, inzicht in motieven van jonge cybercriminelen, inzicht in de effectiviteit van een nieuw interventieprogramma

PROJECT 9: Human factors in cybersecurity

Doel project: Interventies ontwikkelen om het mkb cyberweerbaarder te maken. Beoogde resultaten/deliverables komend jaar voor onderwijs, praktijk en kennisdomein: Interventies ontwikkelen en toetsen om het mkb cyberweerbaarder te maken. Interventies zijn direct bruikbaar in de praktijk. Studenten kunnen aan de slag met interventies in behavior labs (in oprichting).

PROJECT 10: Slachtofferschap in een gedigitaliseerde samenleving.

Doel project: Het onderzoek kijkt naar het maatschappelijk perspectief versus individueel perspectief van online slachtofferschap. Beoogde resultaten/deliverables komend jaar voor onderwijs, praktijk en kennisdomein: PhD thesis docent.

PROJECT 11: Scanning for cyber vulnerabilities

Doel project: Scannen van kwetsbaarheden in wifi, bluetooth en andere verbindingen. Beoogde resultaten/deliverables komend jaar voor onderwijs, praktijk en kennisdomein: Werkende scanner. Vergelijking resultaten scans met patronen van criminaliteit, sociaaleconomische kenmerken op straatniveau. Lokale overheden krijgen inzicht in buurten waar veel kwetsbaarheden zijn. Theorievorming mbt zwaktes in cyberbeveiliging. Studenten werken mee aan ontwikkeling en uitvoering van de scans.

Partners en netwerk

Extern

Het Lectoraat kent enkele vaste samenwerkingspartners die zich voor een langere periode gecommitteerd hebben aan het Lectoraat. Het gaat om de gemeente Den Haag, de gemeente Zoetermeer, het Ministerie van Justitie en Veiligheid en MKB Nederland. Daarnaast is er een samenwerking met het NSCR (een NWO-instituut) voor de periode 2017-2021. Verder heeft het lectoraat inmiddels diverse projecten uitgevoerd met de Erasmus Universiteit en met Saxion Hogeschool. Financiers die meerdere projecten hebben gefinancierd zijn de Veiligheidsalliantie Rotterdam, Politie en Wetenschap en het Ministerie van Justitie en Veiligheid). Hieronder een lijst met alle partners waarmee structureel wordt samengewerkt.

Samenwerking kennisinstellingen bij lopende projecten

Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)
Erasmus Universiteit Rotterdam
Michigan State University
Centrum voor Criminaliteit en Veiligheid (CCV)
Saxion Hogeschool
Universiteit Leiden
Universiteit van Tilburg

Opdrachtgevers/financiers werkveld

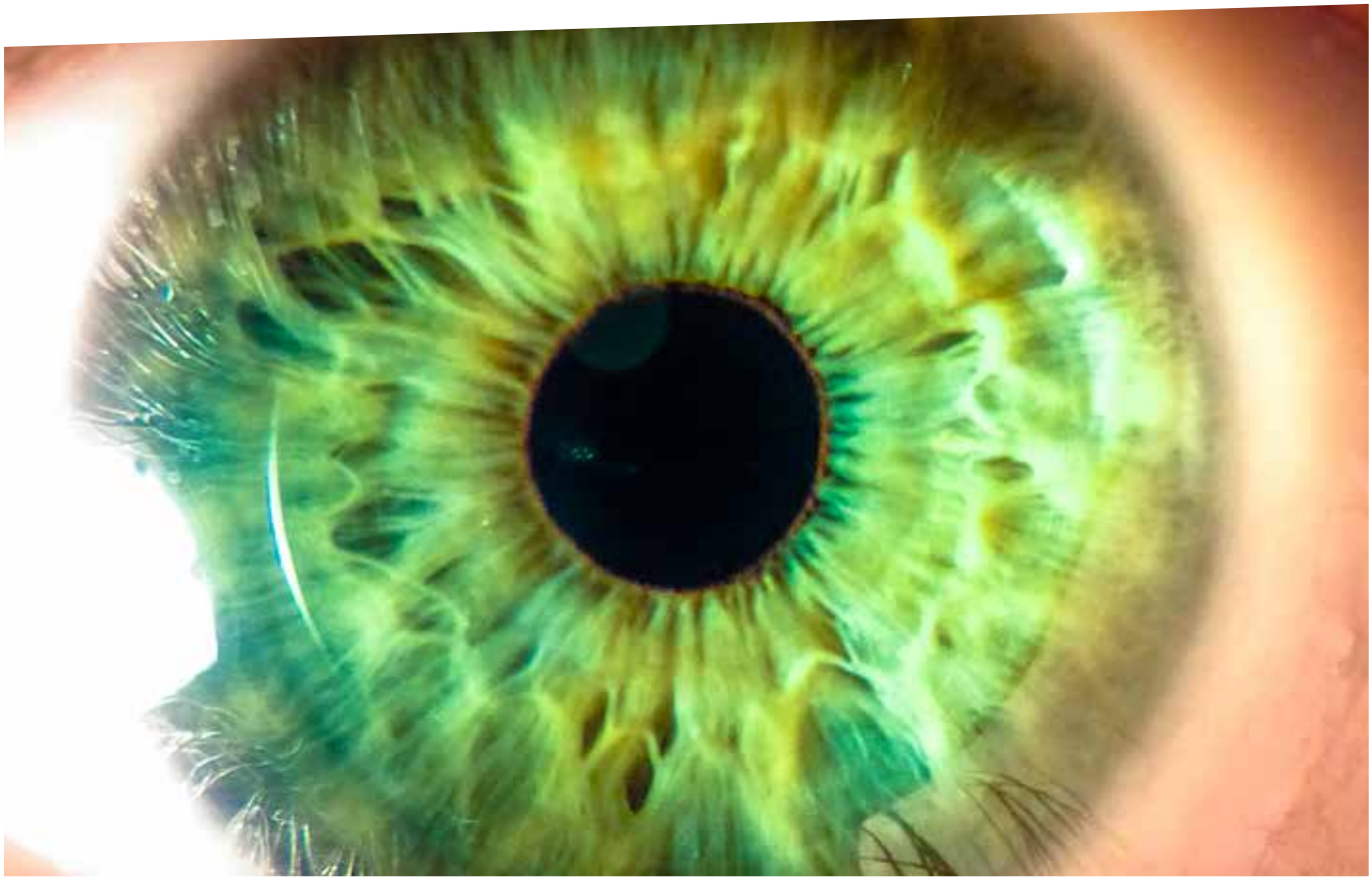
Ministerie van Justitie en Veiligheid
Gemeente Den Haag
Gemeente Zoetermeer
Veiligheidsalliantie Rotterdam
Politie en Wetenschap
SIA (KIEM)
Stichting ECP
MKB Nederland

Intern

Docentonderzoekers verbonden aan het lectoraat zijn nauw betrokken bij (de coördinatie) van verschillende BRV en ITD-opleidingen. Twee prominente programma's zijn de minor Cybersecurity en de FIOD Zero Day Challange. Aan de minor Cybersecurity nemen voornamelijk studenten deel van de faculteit IT&D en BRV. Binnen de minor zijn goede mogelijkheden om de nieuwste onderzoeksresultaten te delen en om studenten te betrekken bij onderzoeken van partners. Verder heeft het lectoraat de FIOD Zero Day Challenge geïnitieerd. Binnen dit programma, dat toegankelijk is voor studenten vanuit de hele HHS, werken multidisciplinaire studentgroepen onder begeleiding van docentonderzoekers verbonden aan het lectoraat aan onderzoeken op het gebied van cyber voor de FIOD. Deze twee programma's zijn een goed voorbeeld van hoe op een flexibele manier nieuwe kennis kan worden ingezet binnen het onderwijs. Voor 2020 en verder hebben we de ambitie om beide programma's flink uit te breiden, zowel in tijd (een extra blok erbij) als wat betreft de onderzoekscomponent.

Met de opleiding ISM zijn goede contacten door de inzet van docentonderzoekers binnen het lectoraat. Ook hebben we regelmatig stagiaires en afstudeerders van ISM. Daarnaast werken we op eenzelfde manier samen met andere opleidingen (zie overzicht hieronder). Op dit moment is de samenwerking vooral gericht op: professionaliseren van docenten door deelname in kenniskring, curriculum vernieuwing door het coördineren van minoren en andere onderwijsprogramma's, studenten betrekken bij veldwerk en de mogelijkheden bieden voor stages en afstudeerders. Tevens heeft het lectoraat goede samenwerking met enkele cybersecuritybedrijven die hun eigen expertise kunnen inbrengen binnen de opleidingen. Relevante contacten proberen we te delen. Een overzicht van opleidingen waar docentonderzoekers betrokken bij zijn:

ISM Cyber Operations	Faculty ITD (HBO-ICT)
ISM Governance Auditing and Compliance	Faculty ITD (HBO-ICT)
Minor Cyber Security	Faculty ITD & Faculty BRV
Minor Law and Technology	Faculty BRV
Research trends and technology	Faculty ITD (HBO-ICT)
Discovering the world of research	Faculty ITD (HBO-ICT)
Data Governance & Internet Policy at Introduction to Law	Faculty BRV
Cybersecurity Law & Policy at International Law	Faculty BRV
Human Rights & Technology at Human Rights &CR	Faculty BRV
Digital Governance, Technology and Public Tech at eGovernance	Faculty BRV
Data Governance & Digital Economy at Minor Doing Bussiness in LatAm	International Bussiness & Management
Governance, Law and Technology	Master Global Governance
Compliance Minor: Data protection and Privacy Compliance course	Faculty BRV
Legal Technology Minor	Faculty BRV
Data Protection Regulation	Master course for THUAS Cybersecurity Engineering
Actors and Behaviour in Cyberspace	Master course for Leiden/THUAS/Delft Executive Master in Cybersecurity
Business Resilience.	Faculty ITD (HBO-ICT)
Security Behaviour en Research	Faculty ITD (HBO-ICT)



Resultaten lectoraat

Tabel 1: Overzicht output 2019

Categorie	Aantal binnen categorie	Aantal studenten	aaantal docenten	Aantal personen uit beroepspraktijk/ maatschappij	Aantal (praktijkgerichte) onderzoekers
Adviesgesprekken of adviestrajecten met beroepspaktijk	7				
Artikelen in tijdschriften	10				
Begeleiding afstudeeropdracht	2	5			
Betrokkenheid bij curriclumvernieuwing	1				
Bijdragen aan minoren of keuzemodulen	5	227			
Bijdragen aan onderzoekslijn in curriculum	2				
Boeken	1				
Deelnamen aan langdurige samenwerkingsverbanden met beroepspraktijk	3				
Gewonnen prijzen	2				
Hoofdstukken in boeken	6				
Lezingen of (gast)colleges	40	1433	151	986	257
Lidmaatschap wetenschappelijk redactie	7				
Ontwikkelde onderwijsmaterialen	5	25			
Organisatie van evenementen of congressen	5	35	1	1345	621
Projecten waarbij studenten actief betrokken zijn in de uitvoering van onderzoek (anders dan afstuderen)	7	262			
Publicaties sociale/ populaire media	4				
Rapporten gericht op beroepspraktijk of	4				
Wetenschappelijke congresbijdragen	13				
Totaal aantal	**124**	**1987**	**152**	**2331**	**878**

Onderwijs en professionalisering

Docentonderzoekers zijn de link tussen onderzoek en onderwijs. Via de betrokken docentonderzoekers kunnen andere docenten en studenten bereikt worden. Verder proberen we regelmatig artikelen aan te leveren aan H/nieuws en organiseren we bijeenkomsten. Ook geven alle kenniskringleden regelmatig gastcolleges binnen diverse opleidingen. Belangrijkste doel van interne communicatie is dat docenten en studenten moeten weten welke onderzoeken (gaan) lopen zodat geïnteresseerden kunnen aanhaken.

Beroepspraktijk en maatschappij

Lectoraatsleden geven regelmatig presentaties op congressen voor het werkveld, worden gevraagd voor het geven van lunchlezingen etc. Verder schrijven we over ieder afgerond onderzoek minimaal 1 artikel in een vakblad. Peer-reviewed artikelen worden indien mogelijk (lees: betaalbaar in een hoog aangeschreven blad) open access gepubliceerd. LinkedIn gebruiken we actief om alle activiteiten van kenniskringleden te delen met ons netwerk. We doen mee aan nieuwe innovatie initiatieven om het werkveld en studenten te bereiken, bijvoorbeeld de internationale Cybersecurity Revolution (bij SECREV2018 en SECREV2019) livestream conferentie die via YouTube live te volgen is en naderhand terug is te kijken.

Tabel 2: Overzicht artikelen

Categorie	Aantal binnen categorie
Artikelen in tijdschriften	10
Niet peer-reviewed	3
Peer-reviewed	7
Totaal aantal	**10**

Categorie	Aantal binnen categorie
Artikelen in tijdschriften	10
Internationaal	6
Nationaal	4
Boeken	1
Internationaal	1
Hoofdstukken in boeken	6
Internationaal	5
Nationaal	1
Totaal aantal	**17**

Bijdrage aan onderzoeksdomein

Binnen het lectoraat cybersecurity in het mkb werken onderzoekers die verbonden zijn aan de HHs en het NSCR samen aan cybercrime en cybersecurity onderzoek. De kennis en ervaring met het fundamentele onderzoek naar cybercrime van het NSCR wordt gekoppeld aan het toepassingsgerichte onderzoek aan de HHs. Hierdoor ontstaat een integraal onderzoeksprogramma dat het hele spectrum van relevant onderzoek naar cybercrime en cybersecurity beslaat: binnen het NSCR wordt het meer theoriegedreven fundamentele onderzoek uitgevoerd, vooral gericht op daders en dadersnetwerken, binnen de HHs wordt het meer 'slachtoffer- en aanpakgeoriënteerde' onderzoek uitgevoerd, en dan specifiek gericht op het mkb. Dat de combinatie van praktijkgericht en fundamenteel wetenschappelijk werkt is te zien in de output. Niet alleen werkt dit lectoraat samen met flink wat partijen uit het werkveld, ook weten betrokken onder-zoekers de opgedane kennis gepubliceerd te krijgen in peer-reviewed tijdschriften.

Naast een aantal projecten waarvoor reeds subsidie is verworven zijn er ook lopende subsidieaanvragen die mogelijk uitmonden in onderzoeksprojecten die (ook) in 2020 lopen. Zo is er samen met Saxion Hogeschool een RAAK Publiek aanvraag gedaan om inzicht te krijgen in hoe gemeenten het beste ondernemers kunnen helpen om hun cybersecurity op orde te krijgen. Voor dit 2-jarige onderzoek worden huidige onderzoekers van het lectoraat ingezet, maar dit project vergt ook (extra) inzet van docentonderzoekers. Verder is samen met NSCR, CBS, Universiteit van Tilburg en enkele maatschappelijke partijen een NWA aanvraag gedaan.

Met de opleiding ISM zijn goede contacten door de inzet van docentonderzoekers binnen het lectoraat. Ook hebben we regelmatig stagiaires en afstudeerders van ISM. Daarnaast werken we op eenzelfde manier samen met andere opleidingen. Vanaf medio 2019 start een nieuwe docentonderzoeken die verbonden in aan de opleiding IVK. We hopen ook daar op eenzelfde manier een goede samenwerking mee op te zetten.

Bijlage 1:

Lijst met partners van het lectoraat

Samenwerking kennisinstellingen bij lopende projecten

- Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)
- Erasmus Universiteit Rotterdam
- Michigan State University
- Centrum voor Criminaliteit en Veiligheid (CCV)
- Saxion Hogeschool
- Universiteit Leiden
- Universiteit van Tilburg

Opdrachtgevers/financiers werkveld

- Ministerie van Justitie en Veiligheid
- Gemeente Den Haag
- Gemeente Zoetermeer
- Veiligheidsalliantie Rotterdam
- Politie en Wetenschap
- SIA (KIEM)
- Stichting ECP
- MKB Nederland

Bijlage 2:
Publicatielijst

Artikel in wetenschappelijk tijdschrift

- 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
- Holt, T.J., S. Van de Weijer & E.R. Leukfeldt (2019) An Exploration of the Factors Associated with Expressive Motives to Engage in Cyberattacks against Dutch Web Sites. Criminal Justice and Behavior.
- 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.
- Kruisbergen, E.W., E.R. Leukfeldt, E.R. Kleemans, R. Roks (2019) Money talks. Money laundering choices of organized crime offenders in a digital age. Journal of crime and justice. DOI:10.1080/0735648X.2019.1692420
- Leukfeldt, E.R., E.R. Kleemans, E.W. Kruisbergen, R. Roks (2019) Criminal Networks in a Digitized World: On the Nexus of Borderless Opportunities and Local Embeddedness. Trends in Organized Crime. DOI:10.1007/s12117-019-09366-7

Artikel in vaktijdschrift

- 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
- 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**.
- 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.

Boek

- Leukfeldt, E.R. & T.J. Holt (2019) (eds) The Human Factor of Cybercrime. London: Routledge.

Hoofdstuk in boek

- 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
- Leukfeldt, E.R. & J. Jansen (2019) Financial cybercrimes and situational crime prevention. In: E.R. Leukfeldt & T.J. Holt (eds.) The Human Factor of Cybercrime. London: Routledge.
- 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.
- 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.
- Leukfeldt, E.R., E.R. Kleemans & W.P Stol (2019) Cybercriminele netwerken: een bloemlezing. In: F. Koenraadt, K. 't Lam & M. Lancel. Internet en sociale media. Een complexe realiteit in de forensische psychiatrie en strafrechtpleging. Nijmegen: Wolf Legal Publishers.
- Kiesow-Cortez, E. (2019), Data Breaches and GDPR. In: Holt T. & Bossler A. (eds.) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham.
- Romagna, M. (2019), Hacktivism: conceptualization, techniques and historical view. In: Holt T. & Bossler A. (eds.) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham.
- Romagna, M. (2019), Evolution of hacktivism: from origins to now. In: Guntarik O. & Grieve Williams V. (eds.) Sit-Ins to #revolutions: Media and the Changing Nature of Protests. Bloomsbury Academic, New York.

Rapport

- 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.
- 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.
- 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.
- 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.

Bijdrage aan wetenschappelijk congres:

- Leukfeldt, E.R. (2019) The Human Factor Applied. The Human Factor in Cybercrime and Cybersecurity. Dcypher Symposium 2019, 3rd December, Utrecht, the Netherlands.
- Notté, R., E.R. Leukfeldt & M. Malsch (2019) The impact of online crime: needs and consequences following victimization. European Society of Criminology (ESC), 18-21 September 2019, Ghent, Belgium.
- Van 't Hoff de Goede, S., R. van der Kleij, S. van de Weijer & E.R. Leukfeldt (2019) Cyber awareness versus actual online behaviour: a population based survey experiment. 2nd annual conference on the human factor in cybercrime. 16-18 October, Oud Poelgeest, the Netherlands.
- Van 't Hoff-de Goede, S., R. van der Kleij, S. van de Weijer & E.R. Leukfeldt (2019) Online Behavior and Cybercrime Victimization: A Population Based Survey Experiment. European Society of Criminology (ESC), 18-21 September 2019, Ghent, Belgium.
- Van de Weijer, S. & E.R. Leukfeldt (2019) Developmental Trajectories of Defacements: a Longitudinal Study among Hackers in The Netherlands. European Society of Criminology (ESC), 18-21 September 2019, Ghent, Belgium.
- Leukfeldt, E.R. (2019) Intervention for juvenile hackers. Security and Human Behavior Workshop. 5-6 June, Boston, USA.
- Kleij, van der, R. & E.R. Leukfeldt (2019) Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. AHFE 2019, Washington, USA.
- Notté. R. (2019) Slachtofferschap in een gedigitaliseerde samenleving. Nederlandse Vereniging voor Criminologie (NVC), 20-21- juni 2019, Leiden, Nederland.
- Notté, R. (2019) Victims of online crime. SECREV 2019 online conference, 4-5 september.
- Romagna, M. (2019) Hacktivism and techniques of neutralization. European Society of Criminology (ESC), 18-21 September 2019, Ghent, Belgium.

Media

Zie voor een recent overzicht:
https://www.dehaagsehogeschool.nl/onderzoek/lectoraten/details/cybersecurity-in-het-mkb#actueel

DE HAAGSE HOGESCHOOL

www.dehaagsehogeschool.nl/