+31(0)70 4457173
coecs@DeHaagseHogeschool.onmicrosoft.nl

DE HAAGSE HOGESCHOOL

Postadres:
Postbus 13336
2501 EH Den Haag
Bezoekadres:
Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl

Research topic: Cyber Security
Safety of the New World
Centre of Expertise Cyber Security (CoECS)

Topic introductie

In een samenleving waar mensen en organisaties steeds meer de kansen van digitalisatie inzetten, nemen ook cyberrisico's en digitale bedreigingen toe. Dat is een groot probleem in onze informatiemaatschappij waar de veiligheid in de digitale wereld en de veiligheid in de 'gewone' fysieke wereld onlosmakelijk met elkaar zijn verbonden.
Mensen en organisaties gebruiken steeds meer digitale systemen en netwerken en zijn daar steeds afhankelijker van geworden. Echter, de motivatie, de kennis en de vaardigheid voor het borgen van de veiligheid in de digitale maatschappij, van cyber security, is nog onvoldoende bij mensen en organisaties aanwezig, terwijl het belang hiervan alleen maar zal toenemen.

Dit roept het vraagstuk op:
Hoe kan de snel digitaliserende wereld veilig worden en blijven?

Bron: https://s-media-cache-ak0.pinimg.com/originals/f9/af/c6/f9afc66f28484d5e38acbbbb2d5f04f8.jpg

+31(0)70 4457173
coecs@DeHaagseHogeschool.onmicrosoft.nl

DE HAAGSE HOGESCHOOL

Postadres:
Postbus 13336
2501 EH Den Haag
Bezoekadres:
Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl

Centre of Expertise Cyber Security

Om hierop in te spelen heeft De Haagse Hogeschool de onderzoeksgroep 'Centre of Expertise Cyber Security' (CoECS) opgericht.

Algemene inleiding

Het CoECS wil organisaties ondersteunen die zelf niet over voldoende expertise beschikken om zich te beschermen tegen en om te anticiperen op de gevolgen van cyberdreigingen. Dit betreft een breed scala aan publieke en private organisaties, variërend van waterschappen tot ziekenhuizen en midden- en kleinbedrijf.
Om deze organisaties te helpen, combineren we inzichten uit verschillende disciplines, zoals informatietechnologie, computerkunde, criminologie, gedragswetenschappen, governance en management.

Het centrum heeft één overkoepelende onderzoeksvraag:

- Hoe kunnen we de cybersecurity verbeteren bij organisaties die niet of onvoldoende zijn toegerust om cyberdreigingen aan te pakken of die zich onvoldoende van deze dreigingen bewust zijn?

Binnen deze brede vraag richten we ons op vier deelvragen:

1. Hoe kunnen we inspelen op de technische uitdagingen op het gebied van cybersecurity in publieke en private organisaties?
2. Hoe kunnen we inspelen op de uitdagingen op het gebied van de governance van cybersecurity in publieke en private organisaties?
3. De menselijke factor wordt beschouwd als de 'zwakste schakel'. Hoe kunnen we deze schakel versterken en organisaties helpen hun cybersecurity effectiever aan te pakken?
4. Hoe kunnen we cybercriminaliteit bij deze organisaties aanpakken? Specifiek: hoe kunnen we de risico's identificeren en in de toekomst helpen die risico's te beperken?

Binnen het Centre of Expertise zijn drie lectoraten (onderzoeksgroepen):

- Cyber Security & Safety / Marcel Spruit
- Networks & Systems Cyber Security / Thomas Quillinan
- Cyber Security in het MKB / Rutger Leukfeldt

https://www.dehaagsehogeschool.nl/onderzoek/kenniscentra/coecs

DE HAAGSE HOGESCHOOL

+31(0)70 4457173
coecs@DeHaagseHogeschool.onmicrosoft.nl

Postadres:
Postbus 13336
2501 EH Den Haag
Bezoekadres:
Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl

Opdracht

Wij houden ons binnen het CoECS dagelijks (vanuit diverse disciplines en expertises) bezig met het vraagstuk: *Hoe kan de snel digitaliserende wereld veilig worden en blijven?* En daar hebben we graag jullie hulp bij.

Momenteel zijn wij met de volgende vraagstukken bezig waaruit jullie er één kunnen kiezen om vervolgens er je eigen onderzoek bij op te zetten.
Let wel! Dit zijn grote vraagstukken, dus voor de haalbaarheid van jullie onderzoek zal je zelf een scope moeten kiezen binnen een van deze vragen.

Doelgroep - Zorg:

- *Hoe risicobewust op het gebied van cybersecurity zijn patiënten en de verschillende geledingen van zorgverleners binnen de zorg?*
- *Van welke factoren is het risicobewustzijn op het gebied van cybersecurity bij patiënten en de verschillende geledingen van zorgverleners binnen de zorg afhankelijk?*
- *Hoe is het risicobewustzijn op het gebied van cybersecurity bij patiënten en de verschillende geledingen van zorgverleners binnen de zorg te verbeteren?*
- *Waar worden privacygevoelige gegevens gegenereerd, opgeslagen en gebruikt binnen de zorg?*
- *Is het genereren, opslaan en gebruik van privacygevoelige gegevens binnen de zorg conform de algemene verordening gegevensbescherming (AVG)?*
- *Welke maatregelen kunnen het proces rondom het generen, opslaan en gebruiken van privacygevoelige gegevens binnen de zorg verbeteren?*
- *Hoe is de autorisatie van deze privacygevoelige gegevens georganiseerd en gefaciliteerd?*
- *Hoe kan de autorisatie van deze privacygevoelige gegevens beter georganiseerd en gefaciliteerd worden?*
- *Hoe veilig zijn de verschillende mobile equipementen die (realtime) communiceert met zorgverleners die privacygevoelige en gezondheid beïnvloedende gegevens uitwisselen?*
- *Hoe kunnen de verschillende mobile equipementen die (realtime) communiceert met zorgverleners die privacygevoelige en gezondheid beïnvloedende gegevens uitwisselen beter worden beveiligd?*

Doelgroep - Kinderen:

- *Wat is het huidige niveau van kennis en vaardigheden op het gebied van cybersecurity binnen het primaire onderwijs?*
- *Wat is het huidige niveau van kennis en vaardigheden op het gebied van cybersecurity binnen het voortgezette onderwijs?*
- *Hoe kan de kennis over cybersecurity en de vaardigheid van mensen op het gebied van cybersecure gedrag worden gemeten?*
- *Welke kennis- en vaardigheidsniveaus zijn "goed" voor welk leerjaar en opleidingsniveau binnen het primaire onderwijs?*
- *Welke kennis- en vaardigheidsniveaus zijn "goed" voor welk leerjaar en opleidingsniveau binnen het voortgezette onderwijs?*
- *Welke producten moeten er worden ontwikkeld om het kennis en vaardigheidsniveau van POVO leerlingen op verschillinde niveaus te verhogen en tot het gewenste niveau te kunnen brengen?*

CENTRE
OF EXPERTISE
CYBER SECURITY

+31(0)70 4457173
coecs@DeHaagseHogeschool.onmicrosoft.nl

DE HAAGSE HOGESCHOOL

Postadres:
Postbus 13336
2501 EH Den Haag
Bezoekadres:
Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl

- *Hoe en via welke kanalen moeten deze producten worden aangeboden?*

Thema – Smartphone connecties aan het internet:
Veel mensen laten hun WiFi en Bluetooth connecties aan staan.

- *Kunnen mensen met het gebruik van passieve sensoren gevolgd worden?*
- *Welke dreigingen zijn er op dit gebied en hoe kunnen we dit soort dreigingen detecteren en mitigeren?*
- *Hoe kunnen we smartphones dwingen om te downgraden naar oudere, zwakkere protocollen?*

Doelgroep – MKB
Thema – slachtofferschap van cyberaanvallen:

- *Hoe vaak worden mkb'ers (succesvol) aangevallen?*
- *Wat is de impact van die aanvallen op de bedrijfsvoering?*
- *Welke factoren zorgen voor een verhoogde of verlaagde kans op slachtofferschap?*

Doelgroep – MKB
Thema – behoeftes van slachtoffers:

- *In welke opzichten verschillen de situatie en behoeften van slachtoffers van online criminaliteit van de situatie en behoeften van slachtoffers van klassieke delicten?*
    a. *Welke financiële, psychologische en/of emotionele gevolgen ervaren slachtoffers van online criminaliteit?*
    b. *Ervaren slachtoffers secundair slachtofferschap? Zo ja, waar wordt dat door veroorzaakt (bijv. door de manier waarop politie/justitie de zaak afhandelde)?*
    c. *Hoe gaan slachtoffers om met slachtofferschap van online criminaliteit? Hoe zorgen zij ervoor dat ze nadat ze slachtoffer zijn geworden weer goed kunnen functioneren in de maatschappij?*
    d. *Welke behoeften hebben slachtoffers aan hulp en ondersteuning (zowel door politie en justitie als door andere relevante partijen)? Hebben deze slachtoffers deze hulp ook gekregen nadat ze slachtoffer zijn geworden? Vinden slachtoffers dat zij een sterke positie in het recht hebben en voldoende erkend en ondersteund worden?*
    e. *Wie zien slachtoffers als verantwoordelijke partij om hen te ondersteunen (politie/justitie en/of private partijen, publiek-private meldpunten, etc.)? Welke ondersteuning verwachten zij van deze en andere partijen te ontvangen?*
- *In hoeverre komen de ervaren gevolgen van online slachtofferschap overeen met de gevolgen van slachtofferschap van traditionele delicten, en waar liggen de verschillen?*
    a. *In hoeverre vallen verschillen te verklaren door de andere kenmerken van online delicten ten opzichte van traditionele delicten (samenkomst in tijd en ruimte van slachtoffers en daders is niet noodzakelijk, massaliteit van slachtofferschap, grensoverschrijdend karakter van online criminaliteit, etc.)?*
    b. *In welke mate speelt de ongrijpbaarheid van sommige vormen van online criminaliteit een rol bij eventuele verschillen in ervaren gevolgen?*
- *Hoe gaan politie en justitie om met slachtofferschap van online criminaliteit?*
    a. *Zien politie en justitie zichzelf als verantwoordelijke partij wat betreft slachtofferschap van online criminaliteit? Zo ja, hoe ziet die rol er dan uit?*
    b. *Behandelen politie en justitie slachtofferschap van online criminaliteit op dezelfde manier als slachtofferschap van online criminaliteit? Als dit verschilt, hoe komt dat?*

CENTRE
OF EXPERTISE
CYBER SECURITY

+31(0)70 4457173
coecs@DeHaagseHogeschool.onmicrosoft.nl

DE HAAGSE HOGESCHOOL

Postadres:
Postbus 13336
2501 EH Den Haag
Bezoekadres:
Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl

   c. *Hoe wordt slachtofferschap van online criminaliteit gewogen door politie en justitie? Wat zijn de verschillen en overeenkomsten met slachtofferschap van traditionele criminaliteit?*
   d. *Welke andere partijen dan politie/justitie hebben een rol bij de afhandeling van online criminaliteit?*
   e. *Welke andere partijen dan politie/justitie zouden een rol bij de afhandeling van online criminaliteit moeten spelen?*
- *Hoe wordt de aanpak van online criminaliteit in een aantal andere landen, te weten Engeland, Duitsland, Estland en de Verenigde Staten, vormgegeven?*
- *In welke opzichten is het vigerende slachtofferbeleid, gebaseerd op de uitkomsten van onderzoeksvraag 1, 2 en 3, aan herijking toe?*

Doelgroep – MKB
Thema – cyberweerbaarheid

- *Wat is weerbaarheid, waarom is dit van belang en hoe kunnen we dit meten?*
- *Welke factoren beïnvloeden de weerbaarheid van het mkb?*
- *Wat is cyber(on)veilig gedrag, welke categorieën zijn er te onderscheiden en met welke vormen van gedrag heeft het mkb te maken?*
- *Wat weten de HHS-studenten over cyberveilig gedrag? (bv. via het maken van vragenlijst en afname vragenlijst onder studenten)*
- *Hoe kun je gedrag beïnvloeden (algemeen)?; welke modellen zijn er m.b.t. gedragsbeïnvloeding en hoe kunnen we dit vertalen naar cybersecurity?*
- *Hoe kunnen we interventies ontwikkelen op maat voor het mkb en hoe kunnen we de effectiviteit bepalen van deze interventies in de praktijk?*

Wat gaat het CoECS doen met jullie onderzoeken en resultaten?

Kunnen jullie ons op nieuwe ideeën brengen en met vernieuwende inzichten komen waarmee wij de snel digitaliserende wereld veiliger kunnen helpen worden en houden?

Zowel de onderzoeksvragen, onderzoeksopzetten als de resultaten van de onderzoeken zijn interessant voor het CoECS.

Vind jij het echt leuk om met dit onderzoek bezig te zijn, kom dan zeker even bij het CoECS langs om de mogelijkheden voor stage en afstuderen te bespreken.

Contactpersoon en beschikbare bronnen voor studenten

Studenten kunnen via Lisanne Slot, het CoECS vragen om mee te denken en om te sparren. Daarbij zal Lisanne eventueel aangevuld door andere collega's vanuit het CoECS aanwezig zijn bij de aangegeven spreekuren in Den Haag of in Zoetermeer.

Let wel!

+31(0)70 4457173
coecs@DeHaagseHogeschool.onmicrosoft.nl

DE HAAGSE HOGESCHOOL

Postadres:
Postbus 13336
2501 EH Den Haag
Bezoekadres:
Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl

Het Centre of Expertise zal niet de eventueel nodige materialen, onderzoekspopulatie/respondenten voor jullie organiseren. Deze zijn afhankelijk van jullie eigen onderzoek en jullie zullen zelf moeten nadenken en organiseren dat je toegang krijgt tot de voor de uitvoering van jullie onderzoek benodigde onderdelen.

Contactpersoon:

Lisanne Slot MSc
Projectleider bij het Centre of Expertise Cyber Security
L.K.Slot@hhs.nl
06-86805992

Bereikbaar op werkdagen gedurende kantooruren.