



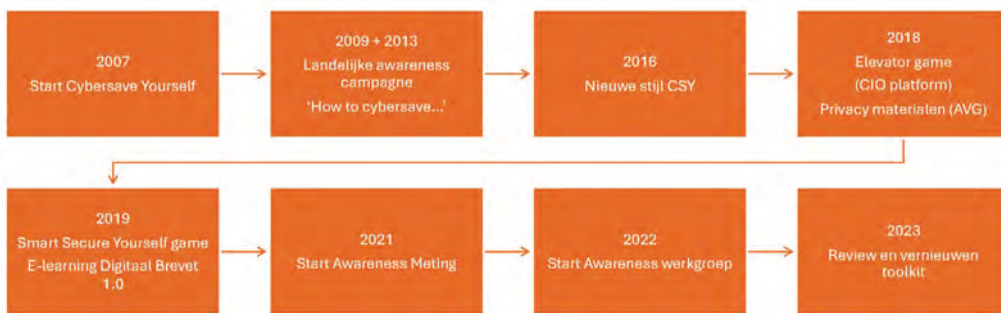
Auteur: Rosanne Pouw is Product Manager Awareness & Training bij SURF. Zij ondersteunt instellingen en organisaties in de sector onderwijs en onderzoek met het verhogen van security- en privacy-awareness bij docenten, studenten en medewerkers. Rosanne is te bereiken via: rosanne.pouw@surf.nl.

17 jaar na introductie Cybersave Yourself toolkit voor onderwijs en onderzoek

Blijven werken aan awareness



Het SURF Cyberdreigingsbeeld onderwijs en onderzoek 2023 (1) toont aan dat universiteiten, hogescholen, mbo-instellingen, UMC's en onderzoeksinstituten gebrek aan awareness bij medewerkers als een groot risico zien. De behoefte aan cybersecurity-awareness in deze sector werd al in 2007 onderkend. In dat jaar zag Cybersave Yourself het licht: de awareness toolkit voor onderwijs en onderzoek. Het uitgangspunt is dat awareness-materiaal voor en door instellingen wordt ontwikkeld en gedeeld, gecoördineerd vanuit SURF. In dit artikel een terugblik op zeventien jaar samenwerken aan awareness, de veranderingen in aanpak van awareness en de uitdagingen die onderwijsinstellingen tegenkomen bij het uitrollen van cybersecurity-awareness.



Tijdlijn CSY.

SURF is een coöperatie van Nederlandse onderwijs- en onderzoeksinstituten waarin de leden hun krachten bundelen. Binnen SURF werken universiteiten, hogescholen, mbo-instellingen, UMC's (Universitair Medische Centra) en onderzoeksinstituten samen om de best mogelijke digitale diensten in te kopen of te ontwikkelen en om kennisdeling te stimuleren door steeds te blijven innoveren. De leden zijn eigenaar van SURF. SURF ontwikkelt en beheert meerdere security- en privacydiensten, waaronder Cybersave Yourself.

Na het besluit in 2007 om samen aan awareness te werken kwam in 2009 een grote, landelijke campagne uit, gericht op studenten en medewerkers. Deze campagne bevatte een breed scala aan

materiaal. Instellingen konden de bestanden uit de toolkit gebruiken om zelf materiaal te drukken zoals flyers, crime scene-tape en zadelhoesjes voor fietsen. Ook waren er materialen zoals advertenties, posters en bureaubladafbeeldingen. Gekozen werd voor oranje als kenmerkende kleur. Sommige materialen waren al eerder door een instelling ontwikkeld en omgezet naar de Cybersave Yourself huisstijl.

Belangrijke thema's waren het veilig omgaan met datadragers zoals USB-sticks, het gebruik van virusscanners, het herkennen van onbetrouwbare websites en het veilig omgaan met wachtwoorden. Ook was er aandacht voor social engineering en het afsluiten van je scherm. De campagne werd positief ontvangen en bij meerdere instellingen op hetzelfde moment uitgevoerd bij de start van het nieuwe schooljaar.

Omdat het opzetten van een campagne op deze schaal tijdrovend en complex is, was er een tweede grootschalige campagne in 2013. In de tussentijd werden de materialen

beschikbaar gesteld in de Cybersave Yourself toolkit en werd er samengewerkt en informatie gedeeld in de securitycommunity.

Bedreigde cybersoorten

In 2016 werd een nieuwe stijl geïntroduceerd rond het centrale inzicht dat digitale onveiligheid dichterbij is dan je denkt. Het basisconcept voor een Cybersave Yourself-campagne bestaat vanaf dat moment uit de introductie van nieuwe (niet bestaande) woorden. In elk woord werd een bedreiging of risico met een persoon of situatie uit de directe omgeving gecombineerd.

Cybersecuritybedreigingen werden omgevormd tot een fictieve diersoort (een 'bedreigende cybersoort'), een analogie met een gevaarlijk roofdier. Elk cybersoort kreeg een eigen habitat, gedragspatroon en persoonlijkheid. Zo werd phishing bijvoorbeeld de 'misleidinggevende', onveilige routers werden 'meekijk-wifi's' en de verkoper van persoonlijke gegevens: de 'datadealer'. Dit jaar werden ook voor het eerst bijbehorende animaties geïntroduceerd. De filmpjes waren een mini-parodie op natuurdocumentaires, waarin te zien is hoe gevaarlijk de 'cybersoort' is. Er werd gekozen geen technische details te verwerken in de animaties, waardoor deze een verrassend tijdloze uitstraling kregen. De eerste vier thema's waren: social engineering, het doorverkopen van data door online apps, uitkijken bij het gebruik van openbare wifinetwerken en phishing.

Deze aanpak maakte de toolkit flexibeler: instellingen konden zelf kiezen wanneer en op welke manier de thema's ingezet werden. De bijbehorende huisstijlgids, Photoshop- en Indesignbestanden hielpen instellingen campagnes te maken in de Cybersave Yourself huisstijl. Inmiddels werd duidelijk dat het verhogen van awareness een wedstrijd van de lange adem was. Instellingen kozen zelf hoeveel tijd en aandacht ze aan awareness konden besteden en op welke momenten in het jaar.

Games en aandacht voor privacy

Voor deze campagnes werd nauw samengewerkt met securityprofessionals bij instellingen. Uit de feedback bleek dat er meer behoefte was aan een luchtige en interactieve manier om awareness aandacht te geven. De in 2016 door het CIO platform ontwikkelde Elevator Game werd in 2018 opgenomen in de Cybersave Yourself toolkit. Met deze app konden twee spelers in de rol van mystery guest en hacker een scenario doorlopen om

beveiligingslekken te vinden bij een fictief bedrijf. Het doel was om elke verdieping te doorlopen en de lift te bereiken. Alleen door samen te werken kon het spel uitgespeeld worden.

2018 was ook het jaar dat er veel aandacht was voor de AVG en privacygerelateerde onderwerpen. De Cybersave Yourself toolkit werd uitgebreid met e-learning modules over privacy en privacyposters voor medewerkers en studenten. De posters hadden onderwerpen als: 'Waar moet ik op letten als ik persoonsgegevens van anderen wil gebruiken', of 'Help, iemand wil mijn persoonsgegevens gebruiken. Mag dat?'.

Voor privacy werden ook meerdere thema's toegevoegd in de stijl die in 2016 geïntroduceerd werd. De privacyprutser (privacy-by-design) en

dataknoeier (datalek) werden ingezet om medewerkers en studenten bewust te maken dat omgaan met persoonsgegevens risico's met zich meebrengt. Privacy-awareness is sindsdien steeds belangrijker geworden voor instellingen.

Het Digitaal Brevet

Eind 2019 werd de Universiteit van Maastricht getroffen door een ransomware-aanval. De aanvallers kwamen binnen via een phishingmail. Veel instellingen voelden daardoor de noodzaak om meer in te zetten op awareness bij medewerkers. De behoefte aan trainingen voor medewerkers en studenten om beter om te kunnen gaan met cyberdreigingen werd groter. De





Awareness- en trainingaanbod.

toename van phishingaanvallen en andere cyberdreigingen werd voelbaar: awareness werd steeds urgenter. Iedereen zou voldoende basiskennis moeten opdoen om veilig te kunnen werken en studeren. Bijvoorbeeld door een basismodule toe te voegen aan het curriculum, of een module aan alle medewerkers aan te bieden.

Het Digitaal Brevet werd ontwikkeld in 2019: een e-learning waarin medewerkers in een uur en studenten in een half uur de basisprincipes leerden om veilig te kunnen leren en werken. Deze modules werden aangeboden in verschillende bestandsformaten, zodat instellingen ze in hun eigen LMS konden importeren, bewerken en implementeren. Security- en privacyprofessionals van instellingen hebben bijgedragen aan de vorm en de inhoud van deze module, zodat de e-learning goed aansluit bij de cultuur en taalgebruik in het onderwijs. Omdat meerdere instellingen een tweetalig beleid hebben, werd het Digitaal Brevet en al het andere materiaal in de Cybersave Yourself toolkit in het Nederlands én in het Engels aangeboden.

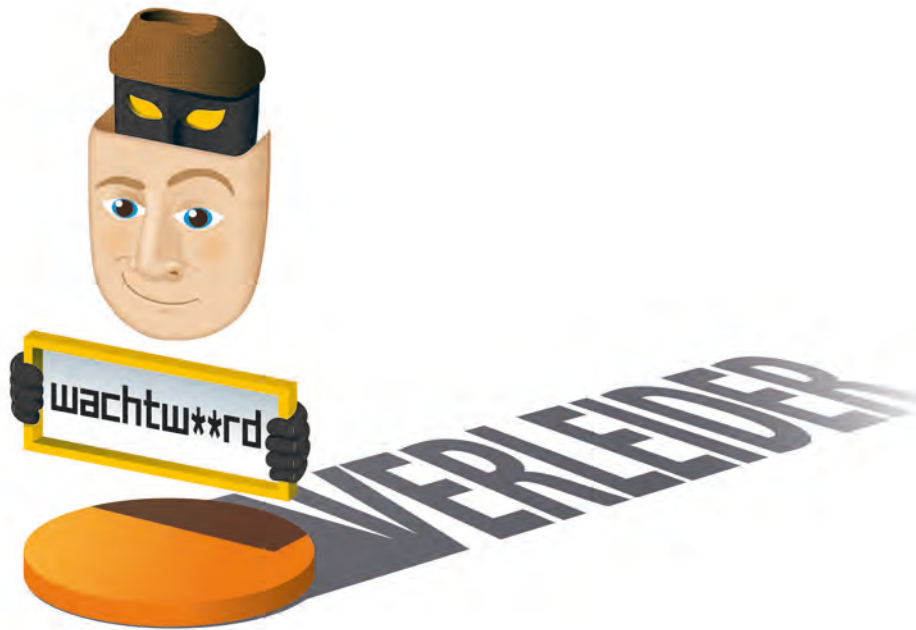
De adaptatie van deze modules was minder breed dan gehoopt. Zo is de module tot nu toe niet terechtgekomen in het curriculum voor studenten. Meerdere instellingen hebben deze

module geïmplementeerd voor medewerkers en is bij een aantal nog steeds in gebruik.

Van materiaal naar kennisdeling

De daaropvolgende jaren werd de toolkit regelmatig uitgebreid met actuele thema's. Er ontstond intussen steeds sterker de behoefte om te meten hoe bewust medewerkers bij instellingen zijn, en wat medewerkers nodig hebben om veiliger te kunnen werken. In 2021 konden dertig instellingen zich opgeven om aan de SURF awarenessmeting mee te doen, waarna SURF een awareness-sectorrapportage publiceerde. Hiermee kregen instellingen inzicht in het kennisniveau van hun medewerkers. Deze meting wordt sindsdien elk jaar door SURF uitgevoerd.

De toenemende behoefte om ervaring uit te wisselen, leidde tot de Awareness Werkgroep in 2022. Deze werkgroep bestaat uit een mailinglijst, een maandelijkse online bijeenkomst en in het najaar een fysieke awareness-dag. Door regelmaat aan te brengen in de bijeenkomsten ontstond momentum om de toolkit in 2023 te reviewen, materiaal te updaten en nieuwe awareness-producten te ontwikkelen. Het huidige aanbod voor awareness en training is daardoor veel breder dan de Cybersave Yourself toolkit.



Veranderingen in awareness

Terugkijkend op deze periode van zeventien jaar zijn er grote veranderingen te zien in de aanpak van awareness en training bij onderwijsinstellingen:

- Verschuiving van communicatie over dreigingen naar training van cyberveilig gedrag
- De invoering van de AVG heeft een boost gegeven aan privacy-awareness waardoor awareness tegenwoordig gericht is op cyberveilig en privacybewust gedrag;
- Cybersecurity-awareness onderwerpen zijn ondanks vernieuwingen grotendeels stabiel: veilig omgaan met gegevens, het herkennen van phishing, datalekken en ransomware, en social engineering zijn nog steeds heel belangrijk
- Awareness leuk en aantrekkelijk maken door gamification, is populair bij onderwijsinstellingen. De instellingen hechten ook erg aan toegankelijk materiaal dat toegespitst is op hun doelgroepen
- Het is steeds belangrijker geworden om het bewustzijnsniveau te meten, bijvoorbeeld met de awareness-meting;
- Door ransomware-aanvallen op onder andere Maastricht University (2019) en ROC Mondriaan (2021) ligt de focus voor awareness en training steeds meer op medewerkers
- Awareness was in de beginperiode een eenmalige, groot-schalige actie bij de start van het schooljaar. Inmiddels is dit veranderd in continue aandacht en meerdere momenten tijdens het jaar om de cyberweerbaarheid te verhogen.

Grote uitdagingen

Onderwijsinstellingen staan voor grote uitdagingen om de awareness van medewerkers en studenten te verhogen. Als eerste is de cultuur bij onderwijsinstellingen niet gericht op compliance gebaseerde implementatie van awareness. Dat betekent dat het verplicht stellen en afnemen van awareness e-learning modules (nog) niet gebruikelijk is.

Om awareness effectief in te zetten, is het belangrijk dat deze risicogebaseerd en doelgroepgericht is. Docenten en onderzoekers stellen hoge eisen aan awareness-trainingen en voor studenten is de vraag hoe deze groep het best bereikt kan worden met awareness-activiteiten. Voor studenten is dankzij technische maatregelen ook een aantal cybersecurity-risico's beperkt. Als een student op een phishingmail klikt, heeft de aanvaller slechts zeer beperkte rechten en komt niet snel verder. Tenslotte is het onderwijs gericht op het uitwisselen van informatie en samenwerken. Binnen de instellingen, maar ook tussen instellingen, bedrijven en met internationale instellingen. Daardoor zijn sommige technische maatregelen zoals het voorkomen dat gegevens uit een systeem gehaald worden, niet altijd mogelijk. Bewustzijn bij medewerkers en studenten over de risico's, processen en handelingsperspectief zijn nog steeds belangrijke randvoorwaarden om een veilige digitale leer- en werkomgeving mogelijk te maken.

Onderwijsinstellingen staan voor grote uitdagingen om de awareness van medewerkers en studenten te verhogen



Nu en in de toekomst

Er wordt in de sector onderwijs hard gewerkt aan cybersecurity-awareness en -training. Naast enorme uitdagingen, zijn medewerkers van onderwijsinstellingen zeer gemotiveerd om zich in te zetten voor een veilige leer- en werkomgeving. Dit blijkt uit de SURF Awareness-sectorrapportage 2023. Uit de rapportage blijkt ook dat medewerkers behoefte hebben aan meer ondersteuning om veilig te kunnen werken, in de vorm van processen en tools.

Wat gelijk gebleven is, is dat in de sector onderwijs structureel kennis wordt gedeeld en waar mogelijk samengewerkt wordt op het gebied van cybersecurity en privacy-awareness. Deze samenwerking zorgt voor innovatie en producten en diensten die passen bij de cultuur van onderwijsinstellingen. En dat awareness en training mee transformeert met de behoefte van de instellingen en de veranderende digitale dreigingen. Samen werken we aan een veiligere digitale leer- en werkomgeving, nu en in de toekomst.

Referentie

(1) <https://www.surf.nl/files/2023-08/cyberdreigingsbeeld-onderwijs-en-onderzoek-2023-nieuw.pdf>

Auteurs: Jacintha Walters is coördinator en docent bij de cybersecuritytrack van Make IT Work. Zij volgde de bachelor cybersecurity aan de Hogeschool van Amsterdam en behaalde een master Applied Artificial Intelligence aan de HvA. Jacintha is bereikbaar via: jj.m.walters@hva.nl. Fred van Noord is adviseur van de cybersecuritytrack van Make IT Work, heeft jarenlange ervaring in informatiebeveiliging en was bestuurslid van PviB. Fred nam recentelijk deel aan de Workinggroup Cybersecurity Skills (ECSF) van ENISA. Hij is bereikbaar via: f.van.noord@hva.nl.



Omscholen op hbo-niveau met de hulp van cybersecurity-experts

Recent onderzoek toont aan dat bijna de helft van de bedrijven wereldwijd worstelt met een tekort aan informatiebeveiligingsexperts (1). Bovendien blijkt het aantal individuen dat voldoet aan het expertiseniveau van organisaties afneemt (2). Deze trend vormt niet alleen een uitdaging voor de organisaties zelf, maar ook voor de maatschappij als geheel die steeds meer afhankelijk is van de veilige en betrouwbare werking van IT-systemen.

Een van de voorgestelde oplossingen voor dit groeiende probleem is het vergroten van de talentpool binnen het cybersecuritydomein (3). Vanuit dit beeld is Make IT Work gestart met een omscholings-traject voor cybersecurity. Make IT Work is opgericht in 2015 als omscholingstraject vanuit de Hogeschool van Amsterdam en heeft geen commercieel doel. Make IT Work

richt zich op het omscholen van individuen uit allerlei domeinen naar het IT-domein zoals Cybersecurity, Business and Data Analytics en Software Engineering,, en biedt daarbij ook kansen aan groepen die voorheen niet actief waren in de IT-sector. Zo trekt Make IT Work een opvallend hoog percentage vrouwen aan, ongeveer 1 op de 3 studenten, vergeleken met 1 op de 13 in de reguliere HBO IT-opleidingen (4). De projecten zijn specifiek

gericht op omscholing van statushouders en vluchtelingen. Op deze manier draagt omscholing bij aan het verkleinen van de tekorten aan cybersecurityspecialisten en worden geschoolde mensen weer opgenomen in het arbeidsproces of komen ze op een werkplek waarmee ze meer affiniteit hebben en hun talenten beter tot hun recht komen.

Hoe werkt Make IT Work?

Omscholing is een intensief traject dat veel van de cursisten vraagt: doorzettingsvermogen, (snel) leervermogen en motivatie zijn vereist. Daarom hanteren we een zorgvuldig selectieproces om ervoor te zorgen dat de kandidaten beschikken over het juiste werk- en denkniveau, maar ook over de juiste mindset en motivatie om de omscholing succesvol af te ronden. Dit rigoureuze selectieproces heeft geleid tot een opvallend laag uitvalpercentage van slechts 8%; aanzienlijk lager dan het uitvalpercentage van 51% bij reguliere bacheloropleidingen (5).

Onze selectieprocedure begint met een assessment, een cognitieve test waarmee kandidaten hun hbo-denkniveau aantonen. Daarnaast ondergaan ze een persoonlijkheidstest, waarmee een profiel van de kandidaat wordt gevormd. Een coach voert vervolgens een gesprek om te beoordelen of Make IT Work de juiste keuze is. Hierop volgt een sollicitatietraining om kandidaten voor te bereiden op de volgende fase.

Als de kandidaat geschikt is beoordeeld, kan zij of hij worden voorgesteld aan de werkgevers die samenwerken met Make IT Work. Kandidaten en werkgevers maken kennis met elkaar op

de banenmarkt, een unieke speeddate-omgeving waar werkgevers die op zoek zijn naar talent rechtstreeks in contact komen met onze kandidaten. Werkgevers nodigen de kandidaten uit die zij geschikt vinden voor de vervolgstappen van hun eigen reguliere sollicitatieprocedure. Kandidaten die met een werkgever een intentieverklaring hebben ondertekend kunnen aan de opleiding beginnen. Deze intentieverklaring zorgt ervoor dat de kandidaten ook baangarantie hebben.

Kandidaten met een intentieverklaring beginnen met een fulltime opleiding van vijf maanden op de Make IT Work campus in Hilversum, gevolgd door zes maanden fulltime werken bij de werkgever. Na succesvolle afronding van het programma ontvangen ze het Make IT Work-certificaat op hbo-niveau en stromen direct door naar hun werkgever.

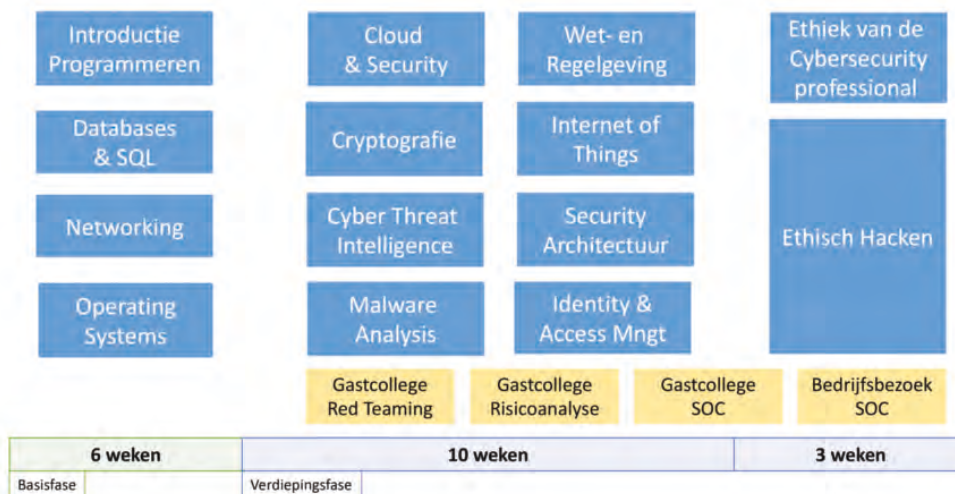
Voor welke werkgevers is Make IT Work interessant?

De omscholing heeft al cursisten opgeleid voor een grote diversiteit aan organisaties, zo werken wij onder andere veel samen met organisaties van overheidsinstanties en IT-consultancybureaus. De werkgevers zijn positief over de voorbereiding van de cursisten op de beroepspraktijk van cybersecurity en hun motivatie en inzetbaarheid. Wat cursisten extra aantrekkelijk voor werkgevers maakt, is dat zij al ervaring hebben met het werken in een organisatie.

Het curriculum van Make IT Work

Make IT Work biedt een dynamisch en interactief leertraject dat nauw aansluit bij de praktijk van cybersecurity.





Programma Cybersecurity.

Een typische lesdag bij Make IT Work ziet er als volgt uit:

- 09:00-11:00: College over het onderwerp van de dag
- 11:00-12:00: Zelfstandig uitvoeren van een mini-practicum
- 13:00-14:00: Verdiepend college
- 14:00-16:00: In teams een relevante casus uitwerken
- 16:00-17:00: Presenteren van de uitwerkingen en feedbacksessies

De hands-on benadering stelt cursisten in staat om direct toe te passen wat ze hebben geleerd, terwijl ze werken aan realistische casestudy's die rechtstreeks uit het werkveld komen.

We bieden een curriculum aan dat voorbereid is op taken van vijf specifieke profielen van het European Cybersecurity Skills Framework (ECSF) van ENISA.

- Incident Responder
- Penetration Tester (= Ethisch Hacker)
- Threat Intelligence Specialist
- Cybersecurity Implementer
- Cybersecurity docent

Het curriculum is opgedeeld in een basisfase van zes weken, waarin de fundamentele van cybersecurity worden gelegd met de vakken programmeren, databases, operating systems en netwerken. De basisfase wordt gevolgd door een verdiepingfase met een breed scala aan cybersecurity-onderwerpen.

Enkele voorbeelden van vakken die in ons curriculum worden behandeld:

- Cyber Threat Intelligence: Het identificeren van potentiële bedreigingen en het bijhouden van ontwikkelingen in de cybersecuritywereld.
- Malware Analysis: Het analyseren van virussen en andere vormen van malware, en het ontwikkelen van strategieën om deze te herkennen en te bestrijden.

- Internet of Things (IoT): Het beveiligen van verbonden apparaten en het identificeren van mogelijke kwetsbaarheden in IoT-netwerken.
- Identity & Access Management (IAM): Ervoor zorgen dat het personeel van een organisatie geautoriseerd wordt en alleen toegang heeft tot de data die personen en organisaties feitelijk nodig hebben.

In het eindproject van ethisch hacken laten cursisten zien hoe zij hun kennis en ontwikkelde vaardigheden toepassen in een real-world scenario. Zij moeten in een klein team een website pentesten om kwetsbaarheden te identificeren. De resultaten leggen zij vast in een rapport samen met aanbevelingen voor mogelijke mitigaties. Zij presenteren hun bevindingen op de laatste dag van de opleiding aan docenten en hun werkgever bij wie ze enkele dagen later aan hun baan beginnen.

Samenwerkingen met bedrijven en instanties

Veel van de lessen worden ontworpen en gegeven door ervaren professionals uit het werkveld. Dit helpt het curriculum nauw aan te laten sluiten bij de praktijk. Daarnaast worden gastcolleges verzorgd door ervaren professionals die vertellen over verschillende onderwerpen (wat doet een Red Team in de praktijk, wat komt er kijken bij het uitvoeren van een risicoanalyse, hoe werkt een SOC/CERT, hoe helpt AI bij cybersecurity, hoe is het om te werken in de context van governance, risk en compliance). Al deze professionals dragen bij aan het beeld van werken in de cybersecurity beroepspraktijk.

Make IT Work werkt samen met organisaties om cursisten te kunnen plaatsen, en gaat ook actief met werkgevers in gesprek om het programma te blijven actualiseren en af te stemmen op de behoeften van de cybersecuritysector.

Succesverhalen van voormalige deelnemers

De cursisten van Make IT Work hebben een hoge intrinsieke motivatie en blijven veelal loyaal aan de werkgever die hun de kans heeft geboden om zich te laten omscholen.

Ömer Şahin - DataDigest

"In de wereld van vandaag, waarin alles verweven is met technologie en techniek, is het niet mogelijk om informatiebeveiliging los te zien van cyberbeveiliging. Zodra ik Make IT Work had afgerond, realiseerde ik me dit opnieuw. In de tweede week van mijn dienstverband bij Datadigest was er een jaarlijkse audit voor ISO27001:2022 certificatie op de werkplek en ik had de gelegenheid om deel te nemen aan twee evaluatiedagen met de auditor. Tijdens onze omscholing waren alle onderwerpen direct gerelateerd aan informatiebeveiliging, en ik realiseerde me opnieuw hoe hoogwaardig en breed de training was die we kregen."

Romario Blijden – DICTU

"Het leertraject Cyber Security van Make IT Work is een leuk traject met ook fijne en interessante docenten/gast sprekers en een gevarieerde klas. Het betreft een breed scala aan onderwerpen, die allemaal uitvoerig worden behandeld. Hierdoor voelt het alsof je een bachelor binnen een half jaar afrondt. Dit zorgt ervoor dat ik goed beslagen ten ijs bij DICTU (een van de grootste ICT-dienstverleners binnen de Rijksoverheid) op de werkvloer ben gekomen. Vanaf dat moment kan en zal ik verdiepende slagen maken (denkend aan het halen van certificaten zoals ISFS, CISSP, BIO, CISM en ECES). Het fijne is dat wij hier al een hoop over hebben geleerd in de afgelopen periode."

Henk Brandon - Practice Lead Cybersecurity Strategy - Ordina

"Een praktische cybersecurity basisopleiding, die de aankomende cybersecurity consultant het vertrouwen geeft om direct aan de slag te gaan met impactvolle klantopdrachten."

Toekomstperspectieven voor MIW en microcredentials

Make IT Work gaat zich op korte termijn ook meer richten op het aanbieden van bij- en nascholing. Niet alleen om werknemers voor te bereiden op cybersecuritytaken, maar het wordt ook steeds belangrijker dat IT-professionals kennis hebben over cybersecurity. Met korte modules kunnen zij die kennis makkelijk bijspijkeren. Deze modules worden afgesloten met microcredentials, door de Europese Unie erkende digitale certificaten van het geaccrediteerde hoger onderwijs. Microcredentials kunnen eenvoudig worden gestapeld en worden ook officieel geregistreerd (6). We streven ernaar om binnenkort al onze vakken voor omscholing en bijscholing af te ronden met microcredentials.

Organisaties die op zoek zijn naar cybersecuritytalent worden aangevoerd om deel te nemen aan ons opleidingstraject. Neem contact op via info@it-omscholing.nl

Ben jij als werkgever op zoek naar IT-talent en wil je meer weten over de kosten en randvoorwaarden? Of ken jij iemand die wil omscholen naar het cybersecuritydomein? Bezoek onze website: www.it-omscholing.nl

Referenties

- (1) Kaspersky. Infosec Experts Shortage - Almost Half of Companies Struggle with Understaffing. Kaspersky Press Release, Available: https://www.kaspersky.com/about/press-releases/2024_infosec-experts-shortage-almost-half-of-companies-struggle-with-understaffing (2024)
- (2) Een derde van bedrijven worstelt met tekort aan cybersecurityspecialisten, ICT Magazine: <https://www.ictmagazine.nl/een-derde-van-bedrijven-worstelt-met-tekort-aan-c/> (2024)
- (3) PvIB, Tekort aan securityspecialisten: <https://www.pvib.nl/kenniscentrum/documenten/tekort-aan-securityspecialisten> (2022)
- (4) Er zijn te weinig vrouwen in de ICT - Vrouwen kunnen echt wel programmeren, HvA.nl <https://hvana.nl/lees/20095/er-zijn-te-weinig-vrouwen-in-de-ict-vrouwen-kunnen-echt-wel-programmeren> (2019)
- (5) Steeds minder hbo-ICT studenten halen hun diploma, AG Connect <https://www.agconnect.nl/carriere/arbeidsmarkt/steeds-minder-hbo-ict-studenten-halen-hun-diploma> (2021)
- (6) Pilot Microcredentials, Versnellingsplan <https://www.versnellingsplan.nl/Kennisbank/pilot-microcredentials-2/>

Auteur: Jos Griffioen is docent/onderzoeker bij het lectoraat Digital Forensics & E-Discovery. Hij is o.a. docent bij de Master Digital Forensics en de bachelor Forensisch ICT. Jos is meer dan 40 jaar werkzaam in de ICT waarvan 23 jaar in het digitaal forensisch onderzoeksdomain. Hij is bereikbaar via: griffioen.j@hsleiden.nl.



Wouter Keuris Fotografie

Forensisch ICT: een andere manier van kijken naar informatica

Hogeschool Leiden leidt al vijftien jaar studenten op tot forensisch ICT'er. Was er in eerste instantie enkel een voltijds bachelor uitstroomrichting, in 2020 kwam er een deeltijd variant bij. In 2023 is de deeltijd masteropleiding gestart en vanaf september 2025 start ook de voltijds master. De belangstelling groeit voor deze aparte richting van ICT. Het nut en de noodzaak groeit ook. Wat maakt dit vakgebied en vooral ook het onderwijs daarin zo bijzonder?

Wat verstaan we onder digitaal forensisch onderzoek? 'In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of

validated tools, repeatability, reporting, and possibly expert testimony.' (1)

Vandaag de dag zijn er bij elk delict wel digitale sporen aanwezig (2) die steeds vaker binnen de rechtsgang als bewijs worden gebruikt. Het belang van meer en goed opgeleide digitaal forensisch onderzoekers neemt hiermee toe.

Het herkennen, vastleggen en analyseren van deze sporen is een vak apart. Alhoewel digitaal rechercheren vanzelfsprekend in de basis alles van doen heeft met ICT, zijn de benodigde skills veel breder: digitale data dient behandeld te worden als DNA, verandering van opslag of inhoud kan desastreuus zijn voor de bewijswaarde. De sporen gaan vooral over activiteiten en gedrag, gerepresenteerd in bits en bytes. Het onderkennen van dit gedrag is essentieel. Technische onderzoeksmogelijkheden zijn soms juridisch niet toegestaan: het is vaak onderzoeken met één arm op de rug.

In 2009 besloot Hogeschool Leiden een specialisatie Forensisch ICT op te zetten binnen de opleiding Informatica. Na een gezamenlijke propedeuse kunnen studenten, naast Software Engineering, Business IT en Mediatechnologie ook kiezen worden voor Forensisch ICT. In september 2010 zaten de eerste zestien studenten hoopvol in de klas: nu ging het gebeuren, CSI werd werkelijkheid! De waarheid was weerbarstiger. Het bleek dat bijvoorbeeld hardware- en netwerktechnologie toch wel erg belangrijk zijn, om überhaupt met het speuren te kunnen beginnen. Daarnaast was programmeren (met name Python) toch het Zwitsers zakmes van de gemiddelde digitaal rechner. Alhoewel een lokaal dagblad iets kopte als 'Hogeschool gaat hackers opleiden', leek de werkelijkheid toch meer op een reguliere Informatica-opleiding, waarbij wel alle aspecten van de informatica even belangrijk bleken, echter vaak op een net andere manier bekeken! Door de jaren heen groeide het aantal belangstellenden gestaag. In de huidige bacheloropleidingsvariant, direct startend in de propedeuse, zien we nu meer dan zestig aanmeldingen.

Onderzoek en multidisciplinair

Kenmerkend voor de opleiding tot forensisch ICT'er zijn de voortdurende nadruk op het doen van goed onderzoek (waarheidsvinding) en het respecteren van de juridische en ethische kaders. In het proces van data naar bewijs dient een voortdurende verificatie plaats te vinden of de gevonden data daadwerkelijk te vertalen is naar de gevraagde informatie en kan dienen als juridisch bewijs. Alhoewel er veel goede analyse-tools beschikbaar zijn, blijken deze door de constante veranderende technologie regelmatig toch niet te voldoen. Denk

bijvoorbeeld aan de snelle updates van apps en OS-en, waardoor analysesoftware geen of verkeerde informatie ophaalt uit de te onderzoeken data. De digitaal rechner zal dan zelf de nieuwe structuren onderzoeken om vervolgens met behulp van eigen software alsnog de waarheid boven tafel te krijgen.

Deze zeer specialistische kennis dient op een zodanige wijze te worden overgedragen, dat een meestal niet technisch onderlegde doelgroep hiermee verder kan: de juristen. Een innige samenwerking tussen deze twee verschillende beroepsgroepen is noodzakelijk om enerzijds op juridisch correcte wijze bewijs te kunnen abstraheren en anderzijds dit bewijs zodanig te presenteren, dat ook niet-ingewijden in de 'diepere ICT' hier vervolgens conclusies uit kunnen trekken! Daarnaast gaat ethiek ook een steeds belangrijkere rol spelen, denk bijvoorbeeld aan de inzet van AI binnen opsporing (gezichtsherkenning), privacy, maar ook de ethische kanten van het behandelen van onderzoeksdata (big data) en resultaten.

Voortdurende aanpassing

De digitalisering van onze samenleving en de voortdurende vernieuwing van de technologie hebben een sterke invloed op het digitaal forensisch onderwijs (3). In 2007 verscheen de eerste iPhone en in 2008 de Android Phone. Dit was een revolutie in onze samenleving, maar ook voor digitaal forensisch onderzoek. In plaats van onderzoek op thuiscomputers of servers kwam er heel veel informatie beschikbaar via die kleine zwarte doosjes: e-mail, contacten, foto's, browsergeschiedenis, locaties etc. Begonnen we in 2010 in Leiden redelijk traditioneel met vakken als Computer Forensics, Network Forensics en E-Discovery, door de jaren heen moest het curriculum voortdurend worden bijgesteld.

Door de opkomst van IoT en andere embedded toepassingen (bijvoorbeeld in de automotive) wordt de kennis van de technische informatica en elektronica cruciaal voor de digitaal rechner. Zonder diepgaande kennis van analoge naar digitale technieken, kan de gevonden informatie niet op zijn juiste waarde worden ingeschat. Iedereen kent wel het voorbeeld van een totaal foutieve gps-locatie in een foto door externe beïnvloeding van het gps-ontvangststelsel. Tegelijkertijd wordt door exponentiële groei van dataskills, datascience een belangrijk wapen. De huidige opmars van AI in de samenleving zien we vanzelfsprekend ook terug in het digitaal forensisch domein. Die biedt kansen door gebruik van AI in opsporing, maar geeft ook nieuwe uitdagingen. Bij gebruik in de opsporing kan de transparantie van bewijsvergaring onder

druk komen te staan. Daarnaast is het herkennen van gebruikte AI, bijvoorbeeld bij deepfakes of specifieke anti forensics technieken niet eenvoudig. Dit kat-en-muis spel is normaal in de wereld van opsporing: nieuwe technologie zorgt voor nieuwe criminaliteit, maar ook voor nieuwe opsporingskansen.

In dit alles veranderen onze opleidingen continu mee, waarbij drie zaken wel gelijk blijven: onderzoek en juridische affiniteit blijven de hoofdrol spelen. Als derde het bovengenoemde kat-en-muis spel; onze studenten worden voortdurend getraind in het zoeken naar nieuwe mogelijkheden.

Mede door het onderzoek vanuit het in 2016 opgerichte lectoraat Digital Forensics & E-Discovery (4) en een nauwe band met de academische Digital Forensics wereld (DFRWS) (5) zijn we in staat deze veranderingen steeds tijdig te blijven inzetten. Studenten van onze master gaan hier vanzelfsprekend ook een belangrijke rol in spelen. Bachelorstudenten studeren nu al af in lectoraat onderzoeksprojecten of werken tijdens stage mee en geven vorm aan eigen onderzoeksprojecten.

Werkveld

Vanaf het begin is het werkveld sterk betrokken bij de opleidingen. Niet alleen de Nationale Politie, NFI of FIOD, maar zeker ook de grote accountancykantoren, cybersecuritybedrijven (DFIR) en recherchebureaus. Samenwerking op het gebied van projectonderwijs, hackatons, gastcolleges of het leveren van hybride docenten.

De opleiding heeft een strategische samenwerking met het NFI, waardoor we gezamenlijk de nieuwste thema's kunnen duiden en een bijdrage leveren aan onderzoek. Voorbeelden hiervan zijn Hansken (6) en Aardwolf (7). Hansken is het digitale zoekplatform van het NFI en wordt gebruikt in ons onderwijs. Door middel van hackatons kunnen studenten extra functionaliteit bouwen. Daarnaast wordt medewerking verleend aan het EU-project Aardwolf, een appsanalyse en referentiedatabase, die de voortdurende updates van meest gebruikte apps bijhoudt. Hierdoor weet een onderzoeker veel sneller op welke wijze en waar bepaalde benodigde data is opgeslagen. Zowel bachelor- als masterstudenten werken hieraan mee.

Doelgroep opleidingen

Vanzelfsprekend is de voltijd bachelor forensisch ICT gericht op de middelbare scholier, die een carrière in het private of publieke domein als digitaal forensisch onderzoeker ambieert. Sommigen worden liever ontwikkelaar van forensische software en enkelen gebruiken hun talenten in het onderwijs en geven les op onze eigen hogeschool.

De deeltijd bachelor is opgezet voor mensen die al werkzaam zijn in het werkveld. Met behulp van deze studie kunnen ze hun specifieke skills uitbreiden naar het niveau van een volledige bachelor. De combinatie van ervaring, werk en onderwijs kan de reguliere studieduur van een bachelor doen verkorten. We zien tot nu toe vooral een instroom vanuit opsporingsdiensten. Er zijn zeker goede aansluitingsmogelijkheden voor werknemers vanuit bijvoorbeeld de cybersecurity (DFIR).

Ook de deeltijd master is gericht op deelnemers werkend in het digitaal forensisch domein. Zij willen zich bezighouden met innovatie: (wetenschappelijk) onderzoek en strategie. Of ze willen beter opgeleid zijn om zeer complexe digitaal forensisch onderzoeken uit te voeren of aan te sturen. Vooraf is een maatwerk pre-master beschikbaar om tot het juiste instap-niveau te komen.

De voltijd master is als eerste een kopstudie boven op onze eigen bachelor, maar kan zeker ook worden gevolgd door andere hbo-ICT studenten (bijvoorbeeld cybersecurity). Deze studenten zullen eerst een pre-master moeten volgen.

Toekomst

Vandaag is het AI wat de hoofdrol speelt, morgen is het misschien wel quantum-computing, hybride intelligentie of cybernetica. Allen met eigen uitdagingen: technisch, juridisch en ethisch. Door de nauwe band tussen ons lectoraat en de diverse opleidingen kunnen tijdig nieuwe trends worden opgemerkt en worden verwerkt in onderwijs. De voortdurend veranderende technologie vereist continu bijgeschoolde digitaal forensisch onderzoekers. Deeltijdopleidingen kunnen een rol spelen in deze bijscholing. Daarnaast zijn diverse mastermodulen nu ook los te volgen als microcredentials (8). De vraag naar specifiek werkveldgericht onderwijs zal enkel toenemen, niet alleen in het digitaal forensisch domein. Een hele uitdaging voor onderwijzend Nederland. Samenwerking zou hierbij kunnen helpen. De toenemende noodzaak van kennis van Digital Forensics binnen cybersecurity heeft ervoor gezorgd, dat Hogeschool Leiden een module Digital Forensics binnen de



Master Cybersecurity Engineering van de Haagse Hogeschool gaat vormgeven. Tegelijkertijd gaat de Haagse Hogeschool een module Malware & Hacking voor onze Master Digital Forensics verzorgen. Op deze wijze maken we optimaal gebruik van de schaarse experts en kan men de bespaarde tijd gebruiken voor nieuw onderzoek en hernieuwing van bestaand onderwijs.

Forensisch ICT is een vakgebied dat een sterke band heeft met disciplines als onderzoek, wetgeving en ethiek. Technologische ontwikkelingen volgen is een voortdurende uitdaging. Als Hogeschool Leiden lukt ons dat door eigen onderzoek via een lectoraat in zowel bachelor- als masteronderwijs en door een goede samenwerking met toonaangevende partijen uit de publieke en private sector.

Referenties

- (1) NIST https://csrc.nist.gov/glossary/term/digital_forensics
- (2) R. Zuurveen, W. Ph. Stol Benutten van Digitale sporen (2020) <https://www.politieenwetenschap.nl/publicatie/politiekunde/2020/benutten-van-digitale-sporen-359>
- (3) Henseler, H. De (R)evolutie van Digitaal Bewijs. Lectorale rede. 21 november 2017
- (4) Lectoraat DF&ED <https://www.hsleiden.nl/digital-forensics>
- (5) Digital Forensics Research Workgroups <https://dfrws.org>
- (6) <https://www.hansken.nl>
- (7) <https://aardwolfproject.eu>
- (8) <https://education.ec.europa.eu/nl/education-levels/higher-education/micro-credentials>

Auteur: Marlon Hartskeerl is coördinator van de Associate Degree opleiding Information Security van de Rotterdam Academy (instituut voor Associate Degrees van de Hogeschool Rotterdam). Ook is hij voorzitter van het landelijk domein-overleg (LADO) Ad Cyber Security. Hij is te bereiken via: mhart@hr.nl.

De lerende driehoek voor praktisch security-onderwijs in Associate Degrees

In de afgelopen jaren zijn er verschillende hbo-securityopleidingen gestart die in twee jaar studenten op tactisch-operationeel niveau opleiden tot nieuwe securitytalenten. Deze opleidingen worden Associate Degree (AD) opleidingen genoemd. Door als organisatie samen te werken met zo'n opleiding ontstaat er een leerdriehoek waar iedere partij van profiteert. Dit artikel bespreekt de AD-securityopleidingen in Nederland en hoe uw organisatie kan profiteren van een samenwerking met zo'n AD-opleiding.



De meeste werkgevers zijn nog niet goed op de hoogte van wat Associate Degrees inhouden en welke waarde ze voor hun organisatie kunnen hebben. Zeker in securityland waar opleidingen vooral op bachelor en wo-niveau (niveau 6 en 7) domineren. De Associate Degrees zijn tweejarige hbo-opleidingen op niveau 5 en richten zich op het tactisch-operationele niveau. In de AD-opleidingen staat de praktijk centraal, zodat studenten na twee jaar direct inzetbaar zijn. En dat gebeurt al sinds 2006 toen de eerste pilots van start gingen. Inmiddels is de Associate Degree verankerd in de wet en zijn er volgens de Vereniging Hogescholen nu ongeveer 326 AD-opleidingen met in 2021 zo'n 20.331 studenten. Dat aantal stijgt nog ieder jaar en dat merken we ook in de inmiddels zes AD's die zich specifiek richten op security.

Doelgroepen van Associate Degrees

De Associate Degree is voor twee doelgroepen aantrekkelijk. De mbo'er en de medewerker die zich graag wil bij- of omscholen om door te groeien. Associate Degrees maken het voor mbo'ers toegankelijker om door te studeren naar hbo-niveau, omdat ze opereren tussen mbo (niveau 4) en vierjarige bachelors (niveau 6). Deze studenten hebben vaak een praktische instelling en leren vooral door te doen. Associate Degrees gebruiken deze praktische mindset om kennis toe te passen in de actuele beroepspraktijk en te gebruiken voor onderbouwing bij gemaakte keuzes in opdrachten.

Associate Degrees zijn ook steeds interessanter voor werkenden. Sommige AD-securityopleidingen bieden een deeltijdopleiding aan waarin studenten in twee jaar een hbo-diploma kunnen halen.)

Eisen aan de opleiding

Securitystudenten op AD-niveau gaan tijdens hun opleiding direct aan de slag. Ze werken bijvoorbeeld aan het implementeren van IB-beleid, het opzetten van risicoanalyses, het uitvoeren van pentests, of het verbeteren van incidentresponse-plannen. De opleidingseisen zijn door de overheid vastgesteld en worden gecontroleerd door de NVAO. Als hbo-opleiding dien je duidelijk te maken waartoe je precies opleidt en hoe dat past op AD-niveau. Daarvoor worden verschillende bronnen gebruikt. De belangrijkste is het werkveld. Samen met hen wordt nagegaan voor welke taken en verantwoordelijkheden de opleiding studenten precies opleidt. Een opleiding heeft vaak meerdere keren per studiejaar met haar werkveldcommissie een bijeenkomst om input uit de praktijk op te halen.

Daarnaast zijn er specifieke bronnen voor IT-opleidingen. Bijvoorbeeld de European Cyber Security Framework, die verschil-

lende rollen in informatiebeveiliging definieert en dit koppelt aan een andere veelgebruikte bron in het onderwijs voor IT-opleidingen, namelijk de e-CF (e-competence framework) Tot slot is er ook de HBO-i domeinbeschrijving.

Een output van dit geheel is vaak een functieprofiel met taken, rollen en verantwoordelijkheden. Zo krijgen studenten een duidelijk beeld waartoe ze worden opgeleid en toekomstige werkgevers wat ze van afgestudeerden van de opleiding kunnen verwachten.

Op dit moment zijn er zes AD-opleidingen specifiek voor security in Nederland. Amsterdam (HvA) bestaat al een aantal jaar, Diemen (Inholland), Amersfoort (HU), en Rotterdam (HR) zijn dit studiejaar gestart. Leeuwarden (NHL Stenden) en Enschede (Saxion) starten in september 2024. De opleidingen komen met een landelijk domeinoverleg bij elkaar om één landelijk AD-profiel voor security te formuleren. Sommige richten zich meer op de technische kant (pentesten en/of blue teaming) voor bijvoorbeeld het SOC- of CERT-team, andere juist meer op de organisatorische kant (risicomanagement en awareness) bijvoorbeeld richting Junior Information Security Officer. Wat alle opleidingen gemeen hebben is dat ze zich focussen op de vijf leerresultaten van Associate Degrees:

1. Methodisch handelen: verbinding maken van aangeleerde theorieën naar de actuele beroepspraktijk
 2. Samenwerken: AD'ers moeten verbinder zijn tussen tactisch en operationeel niveau, waardoor samenwerken met anderen een belangrijk aspect is
 3. Communiceren: doelgericht kunnen verbinden tussen beleid en uitvoering
- Probleemoplossend vermogen: de AD'er analyseert alvorens te handelen door het stellen van de juiste vragen om zo een passende oplossing te realiseren
 - Lerend vermogen: de AD'er blijft zich aanpassen aan de veranderende rol in de omgeving door leervragen te delen

Hoe ziet het onderwijs van een Associate Degree eruit?

Een student aan een AD-opleiding heeft twee studie jaren de tijd om van een mbo'er, havist of deeltijder een gedegen starter te worden op de arbeidsmarkt. De eerdergenoemde securityopleidingen pakken dat op verschillende manieren aan, maar wat steeds meer bekendheid krijgt in het hbo is het formatief evalueren. Waar traditioneel gezien een onderwijsperiode lang les wordt gegeven en aan het eind een toets volgt (wat ook wel 'door een hoepel springen' wordt genoemd), gaat formatief evalueren ervan uit dat er vanaf dag één wordt geëvalueerd hoe ver de student is in zijn leren. Waarin een student een onder-

De Associate Degree is voor twee doelgroepen aantrekkelijk: de mbo'er en de medewerker die zich graag wil bij- of omscholen om door te groeien

wijsperiode de tijd heeft om middels bewijzen aan te tonen dat hij competent is voor de gestelde leerdoelen.

De student moet hierdoor sneller in een actieve houding. Daarnaast moet zij of hij iets doen met ontvangen feedback en leren bewijzen te verzamelen en te reflecteren op het leerproces. Dit zijn belangrijke zogenaamde soft skills voor de beroepspraktijk. Niet alleen omdat ze veel duurzamer zijn voor in hun carrière, denk bijvoorbeeld aan het lerende vermogen, maar ze zorgen er ook voor dat de student een verbinder wordt. Eén die doelgericht een discussie kan aangaan op tactisch niveau en met zelfvertrouwen oplossingen kan presenteren en uitvoeren op de werkvloer. Om dit te bereiken besteden Associate Degrees vanaf de eerste dag aandacht aan de praktijk. Zo krijgen studenten bijvoorbeeld de zes overtuigingsprincipes van Cialdini aangeboden en gebruiken ze deze in social engineering-scenario's om een organisatie op kwetsbaarheden te testen.

Ook doet elke student in die twee jaar één of meerdere stages. In het laatste halfjaar doet de student een afstudeerstage in de praktijk. Niet zozeer om een scriptie te schrijven met vooral onderzoek, maar vooral om een onderzoekende houding te laten zien. Daarmee toont de student startklaar te zijn voor de arbeidsmarkt en is de stagegever er vaak ook al beter van geworden.

De lerende driehoek voor optimaal praktijkonderwijs

Om de praktijk optimaal te integreren in de AD-opleiding is een sterke leerdriehoek tussen opleiding, student en organisatie nodig. Vanuit de organisatie is dit niet alleen goed voor het MVO-beleid, maar ook voor een duurzame instroom van securitytalent. Dat kan enerzijds door bijvoorbeeld de vacatures rondom security nog eens goed te evalueren. Veel vacatures vereisen namelijk CISSP, CISM, SSAP, OSCP etc. en sluiten deze praktische starters daardoor nog uit. Het kan studenten afschrikken om te gaan solliciteren voor een stage of eerste baan. Anderzijds kan de duurzame instroom opgezet worden door een samenwerking aan te gaan met het onderwijs. Daarvoor zien we doorgaans een aantal varianten:

Incidentele samenwerking

Een medewerker van een organisatie geeft een gastcollege en presenteert daarin ook haar werkgever. De organisatie krijgt hierdoor naamsbekendheid bij studenten, maar weet nog niet wat de studenten precies weten en hoe ze optimaal op te nemen in de organisatie.

Periodieke samenwerking

De organisatie geeft één of meerdere onderwijsperioden een opdracht met vaak een gastcollege en het feedback geven op de prestaties van de opdracht. Studenten maken de opdracht, verdiepen zich in de organisatie en de context. De organisatie heeft een betere kijk op de kennis en vaardigheden van de studenten en krijgt wellicht een goede oplossing voor een actueel vraagstuk.

Intensieve samenwerking

Organisaties leveren niet alleen een opdracht, maar dragen actief bij aan het onderwijs. Door bijvoorbeeld in de werkveldcommissie deel te nemen en hierdoor invloed uit te oefenen op het curriculum van de opleiding en/of door hybride docenten in te zetten. Een hybride praktijkdocent geeft 0,05 tot 0,2 fte les en feedback. Ze worden vaak ook ingezet als externe beoordelaar, waardoor de opleiding beter aan kan sluiten op de wensen van de praktijk.

Om goed te kunnen opleiden hebben AD-opleidingen voortdurend contact met de praktijk nodig. Dit betreft opdrachten, het geven van feedback en praktijkdocenten. In ruil daarvoor krijgen organisaties een beter beeld van de studenten en de opleiding. Hierdoor kunnen ze tijdig advies geven over hoe de opleiding beter op de praktijk kan aansluiten. Daarnaast biedt het organisaties het voordeel om studenten gericht uit te nodigen voor stages. Ze kunnen deze studenten op een soepele manier en zonder veel risico in dienst nemen. Dit is voor alle partijen in de leerdriehoek – opleiding, organisatie en student – positief.



Martijn Hoogesteger is Head of Cyber bij S-RM en is bereikbaar via m.hoogesteger@s-rminform.com.

We moeten weer grip krijgen op informatie

Wikipedia is geen echte bron, werd er bij mij op de basisschool al ingestampt. Die kon je niet gebruiken voor je werkstuk, want iedereen kon er van alles opzetten! Vanaf jongs af aan werd ons al geleerd: let goed op waar informatie vandaan komt en hoe je het gebruikt. Sindsdien is de reputatie van Wikipedia een stuk beter, en heeft het zelfs vaak een plek in het onderwijs. Door ermee te leren omgaan kun je ook nadat je scholing af is, op welk niveau dan ook, makkelijk informatie opzoeken en duiden.

Kunnen plaatsen waar informatie vandaan komt, is nog nooit zo'n relevant onderwerp geweest. Vooral kinderen, die nog weinig context aan de wereld kunnen geven, hebben steeds vroeger toegang tot informatiestromen waar we weinig controle op hebben. Waar Wikipedia nog tot doel heeft om waarheidsgetrouwe informatie bij elkaar te puzzelen, gaat dat op social media heel anders. Overheden, extremistische groepen, iedereen kan hun perspectief op de wereld aan de Nederlandse bevolking presenteren. Zo verkeerd is dat wellicht niet, als het alleen om feitelijke waarheden zou gaan. Met steeds meer mogelijkheden om informatie na te maken, onder andere met AI, wordt het wel heel lastig om te bepalen wat realiteit is. Neem daarbij dat ons reptielenbrein ongeveer zeven seconden aandacht geeft aan deze gedachte, en het wordt wel makkelijk om ons te beïnvloeden.

Is dit ook geen informatiebeveiliging? Het gaat misschien niet om het bewaken van de confidentialiteit van je data, of zelfs de beschikbaarheid, maar als mensen opeens andere dingen geloven dan de 'echte' informatie, raakt dat niet de integriteit? Wij zijn in ieder geval degenen die kunnen duiden hoe die informatiestromen tot stand komen, en hoe je onderzoek kunt doen naar de herkomst van informatie.

Hoe leuk zou het zijn als we dit op scholen mee konden nemen in het onderwijsprogramma? Misschien lette mijn school goed op door ons te vertellen hoe we met Wikipedia moesten omgaan; hetzelfde is de komende jaren continu nodig met de huidige ontwikkelingen. Er zijn veel initiatieven om kinderen te leren over social media of cybersecurity, maar vaak zijn ze nog geen deel van het standaard curriculum.

Het zal ook essentieel zijn om op te leiden over de basisprincipes. Alles in cyberland verandert zo snel; als je kinderen alleen maar leert wat goede wachtwoorden zijn, en iedereen gebruikt over tien jaar passkeys, heb je er niet heel veel aan. Basisprincipes, zoals informatieduiding, welke informatie je online achterlaat en in de basis nadenken over security; horen er naar mijn mening sowieso in. Laten we kinderen (en volwassenen) dit ook gebruiken. Maak zelf eens nepinformatie, plaatjes of video's. Speur eens na waar een bepaalde foto is gemaakt of wie er achter een bepaalde post op social media zit. Het is enorm leuk om er op die manier mee bezig te zijn. Je leert denkmethoden die je altijd bijblijven!

Met AI zullen onze onderwijstechnieken waarschijnlijk snel gaan veranderen. Informatie is nog nooit zo toegankelijk, en op een persoonlijke manier aangeboden. Laten we in die verandering direct deze onderwerpen meenemen, anders gaat het een volgende generatie nooit lukken om die grip weer terug te pakken.



Auteur: Kees Teszelsky is hoger onderwijsmanager I-Doctoraat bij I-Partnerschap, hij is te bereiken via: Kees.Teszelsky@rijksoverheid.nl.
Kijk voor meer informatie op: <https://www.rijksorganisatieodi.nl/i-partnerschap>.



De overheid als partner voor wetenschappelijk onderzoek

De rijksoverheid is een rijke bron van onderzoek voor studenten en promovendi. I-Partnerschap kan de onderzoeksbehoefte van onderwijs en wetenschap matchen met de kennisbehoefte van de overheid. En dan vooral (maar niet uitsluitend) voor thema's gerelateerd aan cyberveiligheid, informatiebeheer en -voorziening, AI en softwareontwikkeling. Speciaal voor promovendi die willen werken naast hun onderzoek is het I-Doctoraat opgezet.

Voor een goed bestuur van onze samenleving is een snelle, veilige, betrouwbare en vooral burgervriendelijke digitale dienstverlening van de overheid nodig. Daarom heeft de overheid steeds meer behoefte aan eigen mensen met kennis van thema's op het gebied van informatievoorziening en informatiehuishouding, maar ook aan actuele wetenschappelijke kennis van ontwikkelingen in digitalisering en ICT in de breedste zin van het woord. De overheid kan meer mensen gebruiken als Hemin Hawezy, adviseur politiek & internationaal bij CIO Rijk en promovendus aan de Universiteit Leiden. In 2023 startte hij zijn promotieonderzoek naar het versterken van de besturing op het informatiedomein, benaderd vanuit het 'netwerk governance'-perspectief. Hawezy zegt: "De onderwerpen komen op de overheid af en externe factoren bepalen steeds vaker waar we beleid op maken, hier een paar voorbeelden: quantumcomputing, generatieve AI, digitale soevereiniteit. Dit zijn ontwikkelingen waar de wetenschappelijke wereld al veel langer over nadenkt. Wetenschappers en academici kunnen ons helpen met inzichten over trends om zelf tot inzichten te komen."

Schaarse kennis en expertise

Door de snelle technologische en academische ontwikkelingen is een achterstand ontstaan bij de overheid. Dit doet zich met name voelen bij het op peil houden van het aantal werknemers met inhoudelijke en actuele kennis van eerdergenoemde

thema's. De vergrijzing en de snelle doorstroming op de werkvloer spelen een rol, maar ook het moeilijk kunnen vervullen van vacatures en de gebrekkige aansluiting van het curriculum van hoger onderwijsinstellingen bij de praktijk van de overheid. Antwoorden op de vraag hoe de overheid de uitdagingen van de digitale samenleving moet aangaan, vragen om kennis en expertise die daarom schaars zijn en in sommige rijksonderdelen zelfs ontbreken. Wat zijn nu precies de meest urgente vraagstukken? Welke specifieke kennis is nodig om die vraagstukken op te lossen? En hoe en in welke vorm kan die kennis terecht komen bij rijksorganisaties, zodat een antwoord op deze problemen kan worden gevonden?

Kennis in huis

Te vaak worden antwoorden op dit soort vragen gezocht bij externe inhuur of het aantrekken van consultants buiten de overheid. In 2020 werd € 862 miljoen besteed aan ongeveer 5.500 externe informatieprofessionals en cybersecurityprofessionals (1). Dat is iets minder dan de helft van de totale inhuur van externen. Vaak hebben deze tijdelijke krachten zeer specifieke kennis, die weer verdwijnt uit de organisatie wanneer het contract afloopt.

Die broodnodige kennis is overvloedig aanwezig bij universiteiten en hogescholen die onderzoek doen naar de nieuwste technologische en digitale ontwikkelingen, en lesgeven aan een nieuwe generatie. Promovendus Rens Kievit belandde van een studie

sterrenkunde bij de multidisciplinaire teams informatiehuishouding van I-Interim Rijk. Dat is een rijksorganisatie die tijdelijke projecten uitvoert binnen de overheid. Rens promoveert in het domein datascience en zijn werkgever I-Interim Rijk zoekt opdrachten voor hem die passen bij zijn studie en bij de behoefte van de klant. Hij zegt: "Die casusstructuur past perfect bij de onderzoeksstructuur. En alles wat wij leren als multidisciplinair team brengen wij terug in de organisatie, zodat andere multidisciplinaire teams ook verrijkt worden met de kennis die is opgedaan."

I-Partnerschap

Om die kennis die aanwezig is in het onderwijs naar de overheid te halen, is I-Partnerschap Rijk-Onderwijs in het leven geroepen. I-Partnerschap verbindt de problemen van de overheid met de kennis en expertise van hoger onderwijs en wetenschappelijk onderzoek. Daarbij richt de aandacht zich niet alleen op kennisontwikkeling, kennisdeling en kennisoepassing, maar ook op het aantrekken van nieuw talent vanuit de banken van deze instellingen. Talent dat daadwerkelijk de uitdaging van overheidsvraagstukken aangaat met kennis, expertise en onderzoeksvaardigheden en zich daarbij langdurig wil verbinden met het Rijk.

Zoals juridisch adviseur Arthur van Geenen van Logius, die al langere tijd droomde van een doctoraatsonderzoek. Zijn leidinggevende vond het een goed idee als hij zijn onderzoek zou combineren met zijn baan. Van Geenen wist al snel dat het hoofdthema cybersecurity en cybercrime zou worden, maar hij vond het belangrijk binnen die vakgebieden een koppeling te maken met de actualiteit. Daarover zegt hij: "De kwetsbaarheid van DigiD is veel in het nieuws. We lezen over de impact die misbruik en fraude van DigiD heeft op mensen. Ik heb interesse in de Europese digitale identiteit en fraude. Ik werk bij de overheid en wil betekenisvol werk doen. Als mijn onderzoek mensen meer rugdekking kan geven tegen cyberaanvallen, dan heb ik toch wat bijgedragen aan Nederland."

Onderwerpen voor onderzoek

Wat in grote lijnen de problemen zijn bij het Rijk op i-gebied, is bekend. Onderwerpen worden vanuit overheidswege uitgewerkt in onder meer de Nederlandse Cybersecuritystrategie 2022-2028 (2), het Generiek Actieplan Open op Orde (3) en het programma Werk aan Uitvoering (4), ter verbetering van de publieke dienst-

verlening. In het eerste document worden de ambities van overheid en de benodigde acties voor een digitaal veilige samenleving uiteengezet. Het actieplan Open op orde gaat over de maatregelen ter verbetering van de informatiehuishouding van de Rijksoverheid als reactie op het rapport Ongekend onrecht van de Parlementaire ondervragingscommissie Kinderopvangtoeslag. Al deze plannen en acties moeten uiteindelijk leiden tot positieve maatschappelijke impact en een verbetering van het leven van de burger. Op basis van deze stukken wordt prioriteit gegeven aan vraagstukken op het gebied van informatiehuishouding, data, kunstmatige intelligentie, cybersecurity en post-quantumcryptografie.

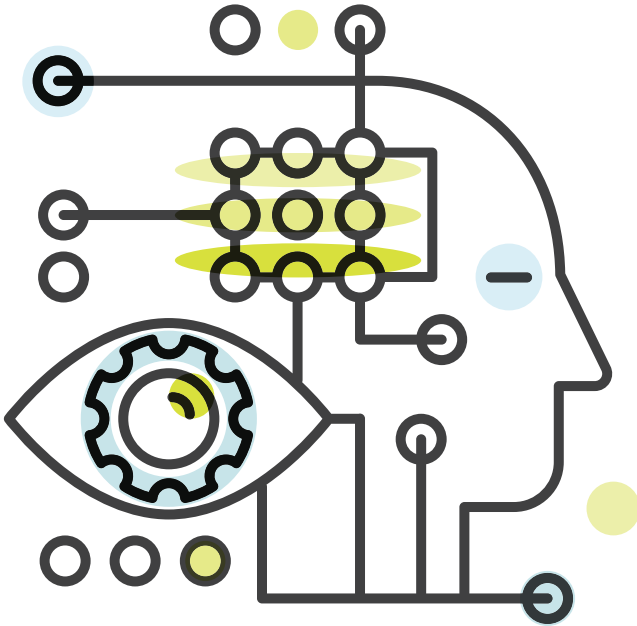
Vertaling theorie en praktijk

I-Partnerschap helpt die vraagstukken te vertalen naar concrete onderzoeksvragen en -trajecten. Vaak begint dit met een letterlijke vertaling; bij veel instellingen is Engels de formele voertaal van wetenschappers en onderzoekers. Na de vertaling van onderzoeksresultaten naar het Nederlands volgt nog een vertaling, die van academische taal en 'ambtenarentaal' (5). De verschillende vakgebieden bij het Rijk hebben een eigen jargon, maar ambtenaren in het algemeen hebben ook een eigen woordkeus. Waar een onderzoeker spreekt van een onderzoeksvraag, heeft een ambtenaar het over een vraagstuk. Het probleem dat het Rijk onderzocht wil hebben, moet worden beschreven in een taal die duidelijk is voor wetenschap en overheid. Andersom moet duidelijk worden wat het nut is van een wetenschappelijke theorie, inzicht of methode voor de overheidspraktijk.

Kortom, de verbinding tussen onderzoek en Rijk begint met een verkenning van de overheidscasuïstiek en het onderzoekslandschap van de wetenschap. I-Partnerschap identificeert die actuele vraagstukken door zoveel mogelijk informatie te verzamelen over welke kwesties spelen en waar. De technische of organisatorische achtergrond daarvan wordt ook meegenomen. Dit gebeurt op basis van een analyse van beleidsstukken en andere documentatie en casuïstiek uit de praktijk.

Kennisportfolio

I-Partnerschap brengt in kaart wie in onderwijs en wetenschap de kennis en expertise hebben van bepaalde vakgebieden waar mogelijk oplossingen liggen voor de vragen van het Rijk (6). Dit kennisnetwerk van mensen bij het hoger onderwijs, het academe-



misch onderzoek en het praktijkgerichte onderzoek bij hogescholen wordt verder uitgeplozen naar thema en specialisatie. Al deze informatie belandt in het kennisportfolio van I-Partnerschap. Dit is waar de magie van vertaling en verbinding plaatsvindt.

Het kennisportfolio beschrijft kort en krachtig de lopende overheidsvraagstukken en het actuele wetenschappelijk kennisaanbod dat daarbij hoort, in de context van maatschappelijke thema's. Gekoppeld aan eerdergenoemde 'kenniskaart' ontstaat een databank van vragen en antwoorden, waarmee het voor I-Partnerschap relatief eenvoudig is een match te maken. I-Partnerschap legt vervolgens de eerste contacten om die match om te toveren tot een concrete verbinding. De achterliggende administratieve taken (denk aan contracten en andere werkovereenkomsten) neemt I-Partnerschap ook voor haar rekening, zodat studenten en onderzoekers zich daar geen zorgen over hoeven maken.

Onderzoeksvormen

De klik tussen vraag en aanbod kan resulteren in een variatie aan onderzoeksvormen (zie kader). Een match kan ook leiden tot een verregaande samenwerking tussen één of meerdere overheidsorganisaties of onderwijsinstellingen in een labconstructie, waar

meerdere wetenschappers, promovendi en studenten aan oplossingen voor met elkaar samenhangende vraagstukken werken. De verbinding werkt twee kanten op. Bevindingen die verkregen zijn door onderzoek in de praktijk, kunnen (indien relevant) ook weer dienen als input voor wetenschappelijk onderzoek of bijdragen aan een onderwijscurriculum dat fijner is afgestemd op de (overheids)praktijk.

Tijdsindeling

De opzet van I-Doctoraat is dat een promovendus gedurende zes jaar twee of drie dagen per week reguliere werkzaamheden verricht (bijvoorbeeld als beleidsmedewerker of strategisch adviseur) en de overige dagen in de week besteedt aan onderzoek binnen de organisatie, op basis van wetenschappelijke onderzoeksmethodes. De promotieonderzoeker fungeert zo voor zes jaar als scharnier tussen het wetenschappelijke kennisnetwerk en de overheid, en als in-house expert of interne deskundige op het vakgebied voor diens collega's en het Rijk. De promovendus kan zo ook de eigen organisatie verbinden met de nieuwste wetenschappelijke inzichten. Uiteindelijk vormt de oplossing die de promovendus op basis van diens onderzoek gaat vinden, de maatschappelijke impact van diens wetenschappelijke onderzoek en dat van de begeleiders. Dit helpt én het Rijk én de wetenschap.

Door de snelle technologische en academische ontwikkelingen is een achterstand ontstaan bij de overheid

Paper en proefschrift

In de kern richt een promovendus zich dus twee dagen in de week volledig op het verbeteren van de eigen organisatie nu en in de toekomst. Het resultaat is in de eerste plaats een bijdrage aan de wetenschap, wanneer wordt voortgebouwd op bestaande bevindingen. In de tweede plaats levert het concrete oplossingen voor vraagstukken uit de praktijk. En als derde is er sprake van kennisontwikkeling bij de overheid, en ook bij de onderwijsinstelling waaraan de promovendus is verbonden.

Daarbij publiceert de promovendus elk jaar een wetenschappelijk peer-reviewed paper. Daarin wordt de kennisbehoefte van de eigen organisatie vertaald naar adviezen, voorstellen, een handleiding of een cursus. Op basis van die wetenschappelijke publicaties komt na gemiddeld zes jaar een verdedigbaar proefschrift tot stand, dat bijdraagt aan de kennisontwikkeling van wetenschap en overheid.

Kortom: de overheid is een interessante partner voor de wetenschap op het gebied van cyberveiligheid en andersom. Een duaal promotietraject biedt uitzicht op persoonlijke ontwikkeling voor werknemers bij de overheid, maar zorgt er ook voor dat kennis en ervaring worden veiliggesteld voor de langere termijn. Digitale veiligheid van Nederland begint met deskundige mensen.

De Rijksoverheid bestaat uit verschillende ministeries, rijksorganisaties, adviesorganen en Hoge Colleges van Staat, elk met hun eigen werkgebied en taak. Op www.werkvoornederland.nl zijn ze allemaal te vinden. Studenten kunnen via verschillende werkvormen kennismaken met het Rijk, in een paar uur of een paar dagen per week. Bijvoorbeeld als stageplek van drie tot zes maanden. Of als groepso opdracht, waarin afgebakende vragen worden beantwoord in een periode van weken of maanden. Een bijbaan bij de overheid is ook mogelijk. Afstudeeropdrachten, hackathons, gezamenlijke onderzoekslabs, parttime onderzoek: I-Partnerschap maakt de match tussen theorie en praktijk.

Onderwijsinstellingen met interesse voor samenwerking kunnen ook contact opnemen.

De geciteerde promovendi in dit artikel zijn kandidaten van het door I-Partnerschap opgezette I-Doctoraatsprogramma. In totaal zijn inmiddels zestien duale promovendi rijksbreed aan het werk bij allerlei verschillende overheidsorganisaties, op onder andere: informatiehuishouding, data, kunstmatige intelligentie, cybersecurity en digital governance.

Referenties

- (1) https://www.piano.nl/sites/default/files/media/documents/2022-04/categorieplan_ict_professionals-december2021.pdf
- (2) <https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022---2028>
- (3) <https://www.open-overheid.nl/over-open-overheid/instrumenten-en-diensten/publicaties/2022/09/19/generiek-actieplan-open-op-orde>
- (4) <https://www.werkaanuitvoering.nl/>
- (5) <https://www.taalcentrum-vu.nl/actueel/blog/ambtenarentaal>
- (6) <https://www.rijksorganisatieodi.nl/i-partnerschap/hoe-het-werkt>

Ontbrekende security-beroepsprofielen

Informatiebeveiliging is aan het formaliseren. Dit kun je duidelijk zien aan het bestaan – en toenemend gebruik – van raamwerken en certificatieschema's. Ook de trend dat die convergeren naar een gemeenschappelijke structuur en verzameling practices draagt er aan bij. Hier heb ik in het verleden al wat columns aan gewijd.

Wat in de praktijk nog lastig is, is hoe organisaties informatiebeveiliging inbedden en hoe dit aansluit op opleidingen. Veel beveiligingscollega's die ik tegenkom in informatiebeveiliging zijn erin gerold op een

creatieve manier. Ikzelf ook. Daar is niets mis mee. Voor de toekomst is het echter niet het model waarmee we kunnen blijven werken. Zeker niet in het licht van de ontwikkelingen die ik hierboven noem.

Er zijn een aantal rollen waarvoor duidelijke, algemene profielen bestaan. De beroepsprofielen IB 2.0 (1) beschrijven de profielen voor securitymanagement (Chief Information Security Officer, Information Security Officer) en technische beveiliging (ICT-beveiligingsmanager en drie niveaus ICT-beveiligingsspecialist).

Het mooie van deze profielen is dat ze gespecificeerd worden in termen van de competenties uit het European e-Competence Framework (e-CF). Daarmee is de afstemming met andere ICT-profielen ook geduid (2). Hiermee wordt de relatie tussen securityprofessionals en ICT-professionals duidelijk.

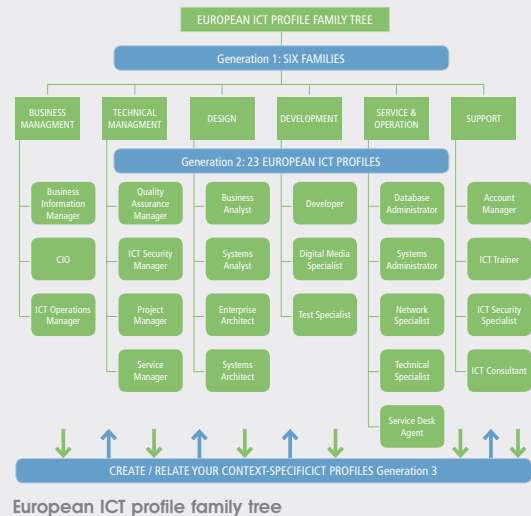
Deze profielen sluiten ook goed aan op de eisen die aan securitygovernance en preventieve maatregelen gesteld worden, vanuit de securityraamwerken. Ze passen minder goed op functies die securitydetectie-maatregelen en responsactiviteiten invullen, zoals de SOC-analist, het CSIRT/CERT-teamlid, de forensisch onderzoeker. Waar vallen die in het raamwerk? Is het operationeel werk? Deels. Is het support? Mogelijk, maar daaronder staan geen passende profielen.

En dan heb je nog de security-onderzoekers. Hun werkzaamheden beslaan het hele security werkveld: dreigingen, kwetsbaarheden, werking maatregelen (preventie/detectie/respons). Als ik ze zou moeten plaatsen, plaats ik ze onder support. Maar het zijn geen typische supportmedewerkers, dus wellicht is hier een hele nieuwe categorie voor nodig.

Het wordt tijd dat we ook deze profielen gestructureerd een plaats geven. Het zijn veelgevraagde functies in het werkveld, je ziet ook veel verschillen in de invulling. Mochten hier al initiatieven voor lopen, dan hoor ik er graag over!

Referenties

- (1) <https://www.pvib.nl/kenniscentrum/documenten/beroepsprofielen-informatiebeveiliging-2-0>
- (2) https://itprofessionalism.org/app/uploads/2019/11/User-guide-for-the-application-of-the-e-CF-3.0_CEN_CWA_16234-2_2014.pdf



Lex Borger is security consultant bij Tesorion en oud-hoofdredacteur van IB Magazine. Lex is bereikbaar via lex.borger@tesorion.nl



Achter Het Nieuws

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.



Wij hebben buitenlandse studenten hard nodig!

De arbeidsmarkt in ons vakgebied kampt al jaren met enorme krapte. De markt groeit, organisaties zijn vanuit allerlei ambities en compliancy naarstig op zoek naar specialisten in security/privacy. Opleidingen leveren minder studenten af dan de actuele marktvraag vereist. Nieuw personeel binnenhalen blijft een voortdurende uitdaging. Wat vinden onze redacteuren van deze dreiging?

Het politieke speerpunt van de grootste partij van Nederland is de instroom van migranten sterk terug te dringen. Voeg daaraan toe het beleid van onze huidige minister van Onderwijs om het aantal buitenlandse studenten aan de Nederlandse universiteiten en hogescholen flink te beperken. Het resultaat: de krapte op de arbeidsmarkt in ons vakgebied loopt verder op.

Wat cijfers ter onderbouwing van de situatie, cijfers van Nuffic:

- o het aantal buitenlandse studenten aan de technische opleidingen van TU-Eindhoven en TU-Delft bedraagt gemiddeld bijna 50%
- o ongeveer 25% van de buitenlandse studenten blijft nog minstens vijf jaar in Nederland werken
- o Nederland biedt afgestudeerde buitenlandse studenten bovendien een zoekjaar aan, waarin ze de tijd krijgen om een baan in Nederland te vinden



Fook Hwa Tan

Chris de Vries

Organisaties, zoals het PvlB, moeten de voorhoede vormen in deze cruciale discussie

Doel van de minister: de zorgen over huisvesting, volle collegezalen en de extra begeleiding die internationale studenten vereisen, weg te nemen. Moet er geen uitzondering worden gemaakt voor ons vakgebied? De minister biedt eventueel een mogelijkheid. Ik denk dat het antwoord op deze vraag een volmondig JA zal zijn. Welke argumenten gaan we daar dan voor aanleveren en wie moet deze boodschap geven? Het PvlB wellicht?

Fook Hwa Tan – Een veilige toekomst: diversiteit en innovatie als schild tegen globale cyberdreigingen

In het hart van onze cybersecuritysector ligt de noodzaak om systemen te beveiligen die vaak meertalige en multiculturele elementen bevatten. Dit maakt diversiteit niet alleen wenselijk, maar absoluut cruciaal. De complexiteit van cybersecurity vereist een breed scala aan perspectieven en vaardigheden, inclusief expertise in software en besturingssystemen die buiten de westerse wereld worden gebruikt. In een tijd waarin internationale spanningen escaleren, wordt het risico van spionage door niet-westerse mogendheden steeds reëler. Het aantrekken van professionals met een diepgaand begrip van niet-westerse technologieën en culturen is essentieel om deze bedreigingen het hoofd te bieden.

Nu is het moment om op te staan en actie te ondernemen. Het pleiten voor een uitzonderingsbeleid voor cybersecurity binnen de Nederlandse immigratie- en onderwijswetten is niet alleen logisch, maar ook van kritiek belang. Dit beleid zal niet alleen helpen de bestaande tekorten op te vullen, maar zal ook de innovatie en effectiviteit van onze cybersecurity-inspanningen significant verhogen. Met de juiste mix van talenten kunnen we onze verdedigingslinie tegen globale bedreigingen versterken en ons land veilig en concurrerend houden in het digitale tijdperk.

Organisaties, zoals het PvlB, moeten de voorhoede vormen in deze cruciale discussie. Gewapend met overtuigende data en krachtige verhalen over het belang van internationale expertise, moeten we een visie creëren die inspireert en mobiliseert. Door internationale talenten te verwelkomen en te behouden, bouwen we aan een robuustere, veiligere en inclusievere cybersecurity-omgeving. Dit is

de weg vooruit; een weg die ons niet alleen technologisch vooruitstrevend houdt, maar ook veerkrachtig tegenover de schaduwen van buitenlandse inmenging. Laat ons samen deze uitdaging aangaan en Nederland transformeren tot een baken van veiligheid en innovatie in het digitale tijdperk.

Chris de Vries – Ver weg of juist dichtbij?

De opgeworpen vraag is intrigerend. Wij leven, zoals Chinezen hun vijanden beleefd vervloeken, in interessante tijden. Rusland voert oorlog en breidt deze mogelijk uit. China kondigt de oorlog om Taiwan aan en Amerikaanse kiezers gaan waarschijnlijk voor een dom America First, net als veel Europese kiezers, elk thuisland first. Dus genoeg ellende, doden en spionage in het vooruitzicht.

Terugziend in de historie kijken wij naar 1933-1939, maar iets verder terug een alternatieve Ode wereldoorlog (06-10-1799) tussen een Engels-Russische legermacht versus De Bataafsche en de Franse Republiek (Slag om Castricum). En nog verder terug de 17e eeuw toen de macht van Nederland enorm groeide mede dankzij de komst van vele (al of niet rijke en intelligente) vluchtelingen uit landen waar men meningen minder tolereerde.

Nederland is een open economie en toegankelijk land, dat heeft ons geen windeieren gelegd. En dat willen wij nu blokkeren, in een tijd dat Europa gezamenlijk moet optrekken om niet de boksbal te worden waar grootmachten tegenaan slaan en schoppen?!

Dus JA, laat buitenlandse studenten komen. Dus NEEN, die komen niet alleen uit Rusland en China om te spioneren, maar juist uit onze bevriende Europese buurlanden. Dus laten wij ons perspectief verplaatsen van ver af naar dichtbij. En laten ook wij bij onze burens gaan studie-buurten! En nog dichterbij: tegenover het geprognosticeerde Nederlandse 40.000 ICT'ers tekort staan ongeveer 30.000 - 40.000 neurodiverse personen en ongeveer 20.000 drop-outs per jaar. Hoezo een tekort? Deze doelgroepen kennen vele talenten in het ICT-werkveld.

Het is onze vereniging die mede de spreekbuis moet zijn voor open grenzen en dat vanuit een absoluut noodzakelijk Europees perspectief. Parafrazerend: 'Vive l'Europe!'.

Cyber Future Event

12
SEPTEMBER
2024

Hét dag evenement voor cybersecurity innovatie en ontwikkelingen, met o.a.:

- Keynote-sprekers AI & cybersecurity experts
- Technical en strategische tracks
- Actieve netwerkmogelijkheden
- Goed verzorgde lunch en borrel
- Expositieruime

Dit is een GRATIS event.

Reserveer alvast je plek via

pinewood.nl/30jaar

pinewood

THE INTERSTELLAR COLLECTION



COLOFON

IB Magazine is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

HOOFDREDACTEUR

Chris de Vries

REDACTIE

Bianca Brooijmans
Alex Dingemanse
Maarten Hartsuijker
Fook Hwa Tan
Lilian Knippenberg
Leo van Koppen
Rachel Marbus
Chris de Vries

BLADMANAGEMENT

MOS bv
Caroline Knobbe
Sam Dekkers
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE

MOS bv
Eric Noordam
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING

Neverseen Art & Design
Dimitri van den Berg

DRUK

Veldhuis Media, Meppel

UITGEVER

Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN

De abonnementsprijs in 2024 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE

Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E secretariaat@pvib.nl



Tenzij anders vermeld valt de inhoud van dit tijdschrift onder een Creative Commons Naamsvermelding-gelijkeDelen 3.0 Nederland Licentie (CC BY-SA 3.0)
ISSN 1569-1063



VERSTERK UW ISO/IEC 27001 MANAGEMENTSYSTEEM!

Wilt u zeker weten of uw organisatie klaar is voor certificering volgens ISO/IEC 27001? Doe de online DNV Self-Assessment en ontvang een rapportage in uw inbox. Of volg de Normkennis ISO/IEC 27001

Kent u de DNV Self-Assessment Suite al? Deze tool stelt u in staat te testen hoe goed u ISO/IEC 27001 kent en te beoordelen in hoeverre uw managementsysteem klaar is voor certificering. De evaluatie is op basis van puntenscores en laat zien waar er tekortkomingen bestaan en waar u verbeteringen kunt doorvoeren.

Stel een nulmeting op, stel kwantitatieve doelen vast voor een specifiek aandachtsgebied en meet regelmatig de geboekte vooruitgang. De Self-Assessment Suite biedt u in alle gevallen een gedetailleerd inzicht in uw kennis of prestaties en uw mate van beheersing.

Wilt u graag uw kennis vergroten over ISO/IEC ISO 27001? Volg dan de Normkennis ISO/IEC 27001 training! De trainer geeft u handige tips en voorbeelden uit de praktijk, zo leert u te kijken naar de norm, zoals een auditor dit doet.

Kijk voor meer informatie over de Self-Assessment Suite op dnv.nl/self-assessment of scan de QR-code als u wilt deelnemen aan de training.





TSTC

ICT en Security Trainingen

Ransomware? Log4j?

ADVANCE YOUR CAREER WITH SECURITY IN 2024

- AIGP** - Certified AI Governance Professional
- CND** - Certified Network Defender v2
- CEH** - Certified Ethical Hacker v12
- OSCP** - Offensive Security PEN-200
- BIO** - Certified Bio Professional
- NIS2** - NIS2 Lead Implementer

GET SKILLED
WWW.TSTC.NL



Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

- CEH** - Certified Ethical Hacker
- CHFI** - Computer Hacking Forensic Investigator
- CPENT** - Certified Penetration Testing Professional
- SSCP** - Systems Security Certified Professional
- OSCP** - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

- CISSP** - Certified Information Systems Security Professional
- CISM** - Certified Information Security Manager
- CISA** - Certified Information Systems Auditor
- CRISC** - Certified In Risk And Information Systems Control
- CJCSO** - Certified Chief Information Security Officer

PRIVACY TRAININGEN

- CIPP/E** - Certified Information Privacy Professional / Europe
- CIPM** - Certified Information Privacy Manager
- CIPT** - Certified Information Privacy Technologist
- CDPO** - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

- CCSP** - Certified Cloud Security Professional

ISO TRAININGEN

- ISO 27001** - Foundation
- ISO 27001** - Lead Implementer
- ISO 27001** - Lead Auditor
- ISO 27005** - Risk Manager
- ISO 27701** - Privacy Management

www.tstc.nl

Onze trainingen zijn klassikaal of Live Online te volgen