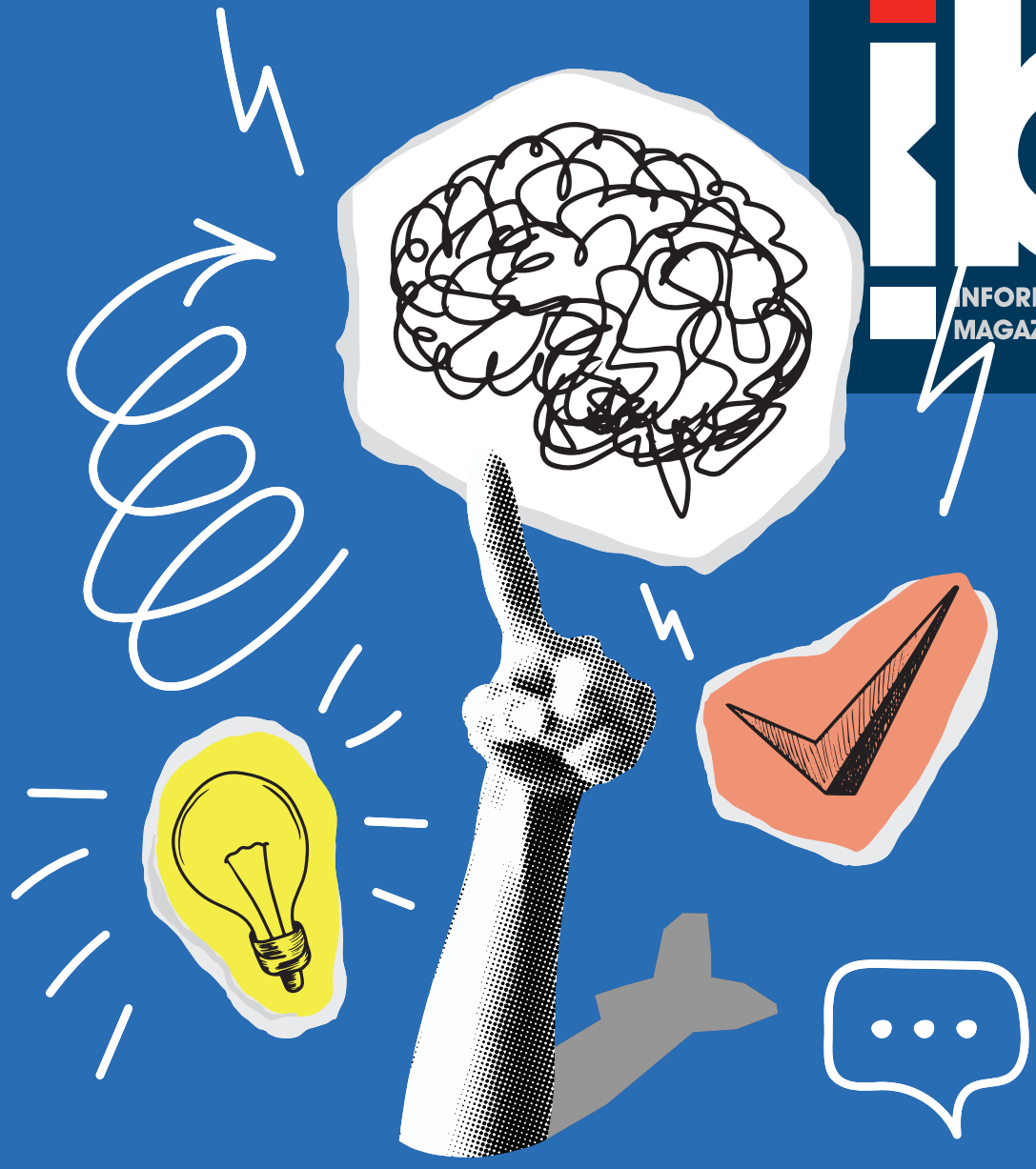
INFORMATIEBEVEILIGING MAGAZINE



Thema: Onderwijs, onderzoek en ontwikkeling

- Kansen en bedreigingen van AI in het onderwijs
- Wij hebben buitenlandse studenten hard nodig!
- Nieuwe columnist Nicole van der Meulen
- Quantum is coming: tijd om te ontwaken

JAARGANG 24 - 2024 - EDITIE 3

ISOPlanner

Eenvoudig Compliance Management in **Microsoft 365**

Hoe EerstelijnsZorg Zoetermeer met ISOPlanner soepel hercertificeerde voor NEN 7510

Stichting Factoring Huisartsenzorg en overige Eerstelijnszorg Zoetermeer was al NEN 7510 gecertificeerd. Zij hadden ook al een werkend managementsysteem opgebouwd uit losse bestanden en overzichten.

Door de samenwerking met ISOPlanner:

- ✓ Nam het overzicht toe.
- ✓ Werd de samenhang tussen risico's, beleid en maatregelen duidelijk.
- ✓ Konden zij hun risicoanalyses en ISMS onafhankelijk beheren.

ISOPlanner is de enige integrale compliance oplossing in Microsoft 365. Uiteraard ook voor de overheid (BIO), ISO 27001 en de NIS2.

Snelle implementatie van je ISMS door meegeleverde voorbeeldmaatregelen, templates en voorbeelddocumenten.

Ik ben heel bij dat we nu dit systeem gebruiken. Achteraf had ik het eerder moeten doen met de kennis die ik nu heb over de toegevoegde waarde van ISOPlanner. Dus ik ben er heel gelukkig mee.

Alex Becker
Eerstelijns Zorg Zoetermeer

Kijk op **www.isoplanner.app** voor meer informatie en jouw gratis proefperiode.

ISO 27001 2024 COMPLIANT · GDPR 2024 COMPLIANT · PENTEST 2024 SECURE

Er valt veel te schrijven over onderwijs

Chris de Vries

'Onderwijs en onderzoek' is het thema. Goed stil te staan bij de betekenis van deze eenvoudige woorden. De primaire synoniemen die je tegenkomt voor **onderwijs** zijn: schoolopleiding, les, instructie en educatie. Aardig om te weten dat school ontleend is aan een Grieks woord 'skholé' wat betekent aan leren bestede vrije tijd of studie en dat educatie voortkomt uit het Latijn: 'educere' wat betekent opvoeden. Daarop volgend de synoniemen: beschaving en vorming. Bij het woord **onderzoek** komen wij uit op: speurwerk, informatie, experiment, observatie en analyse; om maar een paar te noemen.

Kritiek richting onderwijs richt zich op de éénzijdigheid van de communicatie. Het is vanuit de onderwijzer naar de leerling(e) een hiërarchische houding. Nu ziet men liever interactie, een meerzijdige communicatie en dus ná opvoeding en onderwijs vooral vorming. Samenwerking en afstemming op de belevingswereld van de studerende. Coaching treedt in de plaats van sturing. De lerende bepaalt mede de richting van het onderwijs, helpt een andere medestudent(e), dus doceert mee.
Hoe is het geregeld binnen ons vakgebied, is de vraag die wij, als redactie, ons stelden. In dit magazine wordt dat in de volle breedte belicht, vandaar de 52 pagina's (30% meer). Stichting Kennisnet (primair, voortgezet en speciaal onderwijs) en ICT-coöperatie Surf.nl (hbo en wo) komen aan het woord. Zij gaan in op verschillende security-aanpakken en op actuele onderwerpen (inhoudelijk gericht) zoals: AI en cybersecurity (Peter Burghouwt e.a./HHS) en forensisch ICT (Jos Griffioen/HSL).

Ook weten wij dat er een schrijnend tekort is aan deskundigen. Vergroten van de instroom van security professionals via opleidingen Associate Degree (M. Hartskeerl/HRO) en via omscholing van hoger opgeleiden, is nodig en dus de schijnwerpers daarop gericht. Wat (toegepast) onderzoek betreft zien wij TNO ingaan op haar toekomstvisie SOC2030 en de universiteit Leiden (dr. E. de Busser/CSIDE) op het podium verschijnen. Daarnaast nog een artikel van Kees Teszelski over I-partnerschap met stimulering voor kandidaten om zelf een PhD-traject te starten. Met deze scan van de Nederlandse onderwijs- en onderzoekswereld ligt er een grote uitdaging voor de lezers om daar hun weg in te vinden en hun plaats daarbinnen te definiëren. Ten tijde van dit voorwoord is net de formatie rondgekomen. Met de door de vier partijen al aangekondigde beleidswijzigingen (m.n. minder internationale studenten, fikse bezuinigingen op onderwijs en wetenschap, langstudeerboetes en wat dies meer uit de hoed zal komen) moeten wij dan vrezen voor onze toekomst?! Het wordt door sommigen gezien als de bijl aan de stam van onze scholing, vorming en dus beschaving. Het staat in weerspraak met de in voorgaande paragraaf beschreven knelpunten en onze open economie! Persoonlijk zie ik niets in 'The Netherlands first' ideologie, gekopieerd naar vele slechte buitenlandse voorbeelden.

Om positief af te sluiten: in dit nummer introduceren wij ook onze nieuwe columnist Nicole van der Meulen, als opvolgster van Dimitri van Zantvliet. Zij hanteert volgens ons de juiste toonzetting en zal bij jullie, onze lezers, interesse opwekken. Wij wensen jullie een aangename kennismaking met haar.

Chris

IN DIT NUMMER

Auteur: Jordy van den Elshout MSc CISSP, de CISO van Kennisnet. Hij is bereikbaar via: j.vandenelshout@kennisnet.nl.

Eenduidige beveiliging van onderwijstoepassingen essentieel voor een digitaal veilig onderwijs

Elke leerling moet kunnen leren in een digitaal veilige schoolomgeving. Dat betekent dat ICT-toepassingen die docenten en leerlingen gebruiken, veilig moeten zijn. Zij mogen ervan uitgaan dat hun persoonsgegevens voldoende beschermd zijn. Maar wat is veilig genoeg? En is het beveiligingsniveau dat een leverancier biedt voldoende? Om deze vragen te beantwoorden is het Certificeringschema IBP ontwikkeld. Hierin is overeenstemming bereikt over het (basis)niveau van informatiebeveiliging en privacy van onderwijstoepassingen.

Net als in onze maatschappij speelt digitalisering een grote rol in het onderwijs. Al lange tijd worden ICT-toepassingen gebruikt, in plaats van enkel boeken. Ook toetsen worden steeds vaker via de computer afgenomen. Dat zie ik ook bij mijn dochters op de basisschool gebeuren. Deze verandering biedt voordelen, maar brengt ook risico's met zich mee. Het leidt tot vraagstukken rondom het verzamelen van gevoelige gegevens van kinderen. Uitlekken van deze gegevens kan namelijk grote gevolgen hebben. Daarnaast worden we steeds afhankelijker van digitale middelen, waardoor de beschikbaarheid van onderwijstoepassingen belangrijker wordt. Vooral op cruciale momenten. Bijvoorbeeld wanneer een toets gepland staat waar leerlingen zich lange tijd op voorbereid hebben. Wanneer de toets niet beschikbaar is door een verstoring, leidt dat tot vervelende situaties. En nog vervelender is het als de uitslagen voor de toets onjuist zijn omdat de integriteit van de toepassing onvoldoende geborgd is.

Om deze digitale onderwijstoepassingen adequaat en naar wens van het onderwijs te beveiligen, zijn afspraken nodig. Het belang van een toepassing voor het onderwijs kan namelijk het beste door het onderwijs zelf bepaald worden; de afnemer van de onderwijstoepassing. Daarom zijn er afspraken gemaakt over hoe dit belang bepaald moet worden en welk beveiligingsniveau daarbij hoort. Dit is uitgewerkt in het Toetsingskader van het Certificeringschema IBP.

> Het Certificeringschema IBP is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA) (1), een vastgestelde afspraak binnen Edustandaard. Edustandaard is het platform waar alle publieke en private partijen binnen het onderwijsveld bij elkaar komen om afspraken te maken, te beoordelen en vast te stellen. Vanuit Kennisnet begeleid ik de Werkgroep IBP (2) die het Certificeringschema IBP onderhoudt. Deze afspraak is opgesteld om ICT-toepassingen in het onderwijs te toetsen. In een apart document Toezicht wordt dit nader uiteengezet. Voor dit artikel beperk ik de toelichting tot de inhoud van het Certificeringsschema: het Toetsingskader.

Maatregelen

In het Toetsingskader is een eenduidig (basis)niveau van informatiebeveiliging en privacy bepaald. Het geeft beveiligingseisen

voor een onderwijstoepassing, verdeeld over drie categorieën: beschikbaarheid, integriteit en vertrouwelijkheid (BIV).
Op basis van de BIV-classificatie worden de minimale beveiligingsmaatregelen voorgeschreven, zodat de onderwijstoepassing afdoende wordt beveiligd volgens het belang voor de beschikbaarheid, integriteit en vertrouwelijkheid. Dit voorkomt onnodig zware beveiligingsmaatregelen, die ten koste gaan van het budget of van de gebruikersvriendelijkheid. Maar zorgt ook voor voldoende zware maatregelen als het onderwijsproces of de gebruikte gegevens dat vereisen. Hoe deze classificatie bepaald wordt, licht ik later toe.

Om een beeld te geven van een maatregel op basis van het BIV-niveau: wanneer de beschikbaarheid van een onderwijstoepassing minder van belang is en daardoor een laag niveau voor beschikbaarheid kent, mag deze bijvoorbeeld bestaan uit enkele applicatieonderdelen. Maar wanneer de toepassing een hoog beschikbaarheidsniveau kent, dan worden dubbele applicatieonderdelen voorschreven. Dit kan ingevuld worden met meerdere servers in combinatie met een 'load-balancer'.

Voor de vertrouwelijkheid geldt hetzelfde. Wanneer een onderwijstoepassing een laag vertrouwelijkheidsniveau kent, bijvoorbeeld het inzien van het schoolrooster, dan is geen tweefactorauthenticatie (2FA) vereist. Maar bij een onderwijstoepassing met gevoelige persoonsgegevens van leerlingen is toegang met 2FA wel verplicht.

Vaststellen juiste BIV-classificatie van belang

Afdoende beveiliging valt of staat met een goede inschatting van de BIV-classificatie. Wanneer deze niet juist wordt ingeschat, leidt dit tot te lichte of te zware maatregelen op het gebied van beschikbaarheid, integriteit of vertrouwelijkheid. Daarom is een classificatieschema onderdeel van het Toetsingskader, in de vorm van een vragenlijst. De vragenlijst geeft een objectieve indicatie voor de BIV-classificatie.

Voor de beschikbaarheid wordt bijvoorbeeld de volgende vraag gesteld: welke impact heeft uitval (de data, informatie of ICT-toepassing zijn niet beschikbaar)? Mogelijke antwoorden hierop zijn: a) geen; b) het proces wordt belemmerd maar kan wel doorgaan; of c) het proces kan in zijn geheel niet doorgaan. Op basis van meerdere antwoorden in de categorie beschikbaarheid wordt het niveau bepaald: laag, midden of hoog. Op dezelfde manier wordt het niveau bepaald voor integriteit en vertrouwelijkheid. Een van de vragen voor vertrouwelijkheid is: kunnen personen schade ondervinden als gevolg van het uitlekken van de gegevens?

Met deze vragen wordt een link gelegd met het proces en de benodigde informatie, waar het in informatiebeveiliging om te doen is. De applicatie wordt daarmee in de juiste context geplaatst. Door een link te leggen met het proces, kan je het belang van beschikbaarheid en integriteit bepalen. Op basis hiervan wordt ook de hersteltijd (Recovery Time Objective) en maximale dataverlies in uren (RPO) aangewezen. Door naar de gebruikte informatie te kijken, kan je de gevoeligheid ervan bepalen, ofwel de vertrouwelijkheid.

> Als vragen in het Classificatieschema verkeerd geïnterpreteerd en beantwoord worden, kan dat leiden tot een onjuiste BIV-classificatie. Daarom wordt door de Werkgroep IBP van Edustandaard ook gekeken naar een aanvullende afspraak: een koppeling met referentiearchitectuur in het onderwijs, waarin BIV-classificatie van soorten applicaties centraal vastgesteld worden. Dit leidt tot meer uniformiteit in de BIV-classificatie en verkleint de kans op discrepantie en discussie.

Complementair aan andere normenkaders

Het Toetsingskader is een (nadere) aanvulling op normenkaders voor informatiebeveiliging, zoals de ISO 27001/2 en NIST SP 800-53. Maar ook op de normenkaders voor informatiebeveiliging en privacy die in het onderwijs gehanteerd worden, die gebaseerd zijn op het NBA-volwassenheidsmodel (3). Al deze normen richten zich met name organisatiebreed en niet specifiek op een onderwijstoepassing, zoals het Toetsingskader van het Certificeringschema IBP ROSA dat wel doet. Hierdoor is het Toetsingskader complementair aan eerdergenoemde normenkaders.

Leveranciers van onderwijstoepassingen gebruiken vaak al een normenkader voor informatiebeveiliging. Zij kunnen het Toetsingskader als aanvulling gebruiken. Het classificatieschema kan gebruikt worden om de onderwijstoepassing te classificeren. Vervolgens kunnen per applicatie passende maatregelen genomen worden, zoals in het begin van dit artikel uitgelegd.

Bij Kennisnet gebruiken we het Toetsingskader ook als aanvulling op ons ISMS volgens ISO 27001. Aangezien wij voor de landelijke

Om de digitale onderwijstoepassingen adequaat en naar wens van het onderwijs te beveiligen, zijn afspraken nodig

ICT-basisinfastructuur voor het primair- en voortgezet onderwijs en het mbo een breed scala aan diensten leveren (4), hebben wij voor het overzicht al onze diensten en onderliggende applicaties vastgelegd in een administratiesysteem. De vragenlijst van het classificatieschema voor het vaststellen van de BIV is hier onderdeel van en wordt door dienstverantwoordelijken ingevuld. Op basis van de BIV-classificatie worden de juiste beveiligingseisen geselecteerd en kan per maatregel de status bijgehouden worden. Op deze wijze houden we grip op en inzicht in de beveiligingseisen die per dienst decentraal geborgd moeten worden.

Kennisnet is de publieke organisatie (5) voor ICT in het primair- en voorgezet onderwijs en voor specifieke thema's in het mbo. Kennisnet zorgt ervoor dat technologie wordt benut om de kwaliteit en toegankelijkheid van het onderwijs te verbeteren en veiligheids- en ICT-risico's te beheersen. Hiervoor neemt Kennisnet verschillende rollen aan:

i) **Expert en gids** voor scholen en besturen die keuzes moeten maken over inzet van ICT,
ii) **Ontwikkelaar en dienstverlener** van publieke ICT-voorzieningen, en
iii) **Keten- en sectorarchitect** van de (sectorale en bovensectorale) ICT-infrastructuur in het onderwijs.

Kennisnet geeft ook advies over toepassing van informatiebeveiliging en privacy (IBP). Hiervoor is o.a. de Aanpak IBP (6) ontwikkeld, waar ook het Normenkader IBP op beschikbaar is gesteld. Ook werkt Kennisnet samen met andere publieke partijen om IBP in het onderwijs op een hoger niveau te krijgen. Hiervoor is het Programma Digitaal Veilig Onderwijs (7) gestart, met ministerie van OCW als opdrachtgever.

Beveiliging van de toepassing zelf

Wanneer je meer zekerheid wilt over de toegepaste informatiebeveiliging, dan vraag je daar bewijs van op. Als een leverancier ISO 27001 gecertificeerd is, vraag je het certificaat op, inclusief de 'Verklaring van Toepasselijkheid' (VvT). Het certificaat maakt inzichtelijk of de processen voor informatiebeveiliging volgens de norm (ISO 27001) zijn ingericht en op welk deel van de organisatie ('scope').

In de VvT staat beschreven welke maatregelen wel of niet van toepassing zijn, en waarom. Hier kun je nog op doorvragen, bijvoorbeeld op welke wijze de maatregelen zijn ingevuld. Logischerwijs stel je de vragen op basis van een eigen risicoanalyse voor jouw situatie.

Op dat moment heb je meer zicht en zekerheid over de processen die op organisatieniveau georganiseerd zijn, echter zegt dit weinig over de beveiligingseigenschappen van de geleverde onderwijstoepassing zelf. Dat inzicht is wel wenselijk, vooral als een leverancier geen ISO 27001 certificering heeft. Het Toetsingskader kan dit inzicht leveren op basis van de gewenste BIV-classificatie.
De leverancier kan het Toetsingskader invullen voor een specifieke onderwijstoepassing die zij leveren. Hierin kunnen zij de vragen beantwoorden die leiden tot een BIV-classificatie voor beoogd gebruik. Vervolgens kan per maatregel aangegeven worden wat de status is, inclusief toelichting. De onafhankelijkheid wordt bepaald door de toetsvorm, ofwel door wie de toets is uitgevoerd. Binnen het Certificeringsschema onderkennen we vier toetsvormen:

1. Self-assessment (lage onafhankelijkheid)
2. Interne audit (gemiddelde onafhankelijkheid)
3. Peer review (gemiddelde onafhankelijkheid)
4. Externe audit (hoogste onafhankelijkheid)

Hiermee heb je inzicht in het beveiligingsniveau van de toepassing zelf en in hoeverre dit is toegepast. Mocht het niveau onvoldoende blijken voor het gebruik, dan kun je hier extra eisen

Maak gebruik van het Certificeringschema!
Het Certificeringschema ROSA IBP is ontwikkeld voor het onderwijs, maar ook zeker toepasbaar voor andere sectoren of binnen een organisatie zelf, zoals Kennisnet dat ook doet. Het is vrij te gebruiken (CC-BY) en te downloaden via de website van Edustandaard.

aanstellen. Mocht je meer zekerheid willen over de toepassing van de maatregelen, dan kun je de toets laten uitvoeren door een externe auditor.

Borgen van beveiligingseisen

Het Toetsingskader zorgt ook voor het specificeren van de adequate beveiligingseisen in een verwerkersovereenkomst. Deze omvat vaak een standaardlijst met beveiligingseisen, maar de AVG vereist dat er passende maatregelen worden genomen. Met de BIV-classificatie kun je aangeven wat gewenst en passend is. Op basis van het toetsingskader kunnen dan de specifieke beveiligingseisen voor dat niveau voorgeschreven worden in de beveiligingsbijlage. Tijdens een DPIA kan een ingevuld Toetsingskader opgevraagd worden, om toepassing van deze beveiligingseisen te controleren.

In de modelverwerkersovereenkomst (van het Privacy Convenant (8)) voor het primair- en voorgezet onderwijs en het mbo wordt het Toetsingskader daarvoor ook gebruikt. Het Toetsingskader (Excelsheet) heeft daar speciaal een rapportfunctie voor, dat een-op-een overgenomen kan worden in de beveiligingsbijlage van een verwerkersovereenkomst. Daarmee worden de beveiligingsmaatregelen ook contractueel geborgd.

Referenties

(1) https://rosa.wikixl.nl
(2) https://www.edustandaard.nl/standaard_werkgroepen/werkgroep-informatiebeveiliging-en-privacy-ibp
(3) https://www.nba.nl/tools-en-ondersteuning/publicaties/2019/handreiking-bij-volwassenheids-model-informatiebeveiliging/
(4) https://www.kennisnet.nl/diensten
(5) Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW)
(6) https://aanpakibp.kennisnet.nl/normenkader/
(7) https://www.digitaalveiligonderwijs.nl/
(8) https://www.privacyconvenant.nl/downloads/

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Privacybubbels

Al scrollend door een privacyforum stuitte ik op een post waarin iemand zocht naar een 'stomme' tv. Na de eerste lichte verbazing, viel al snel het kwartje. De persoon zocht een tv die niet smart was en wilde dus eigenlijk een kijkbuisvariant van een air gapped laptop. Geen verbinding met het internet en dus ook geen apps die allerhande data over kijkgedrag kunnen verzamelen. Het bleek zoeken naar een speld in een hooiberg.

Het wordt steeds lastiger om in een toenemende digitale wereld een offline variant van iets te vinden. En dat 'iets' moet je dan zo breed mogelijk opvatten. Het bijschrijven van mijn kind op mijn huisadres bleek bij voorkeur digitaal te moeten gebeuren – door mij via het onlinesysteem van de gemeente. Terwijl ik eigenlijk gewoon even langs wilde lopen om aan de balie een en ander af te doen, werd het letterlijk maken van een afspraak ontraden met een verwijzing naar het onlinesysteem. Dat dit helemaal niet kon via dat systeem, wist geen enkele ambtenaar.

Zo kwam ik na vier mislukte pogingen dus toch nog bij een mens van vlees en bloed uit. Waar ik – ironisch genoeg – naar huis gestuurd werd om een tien jaar oud papieren huurcontract op te halen, als bewijs dat ik daadwerkelijk op dat adres woonde, dat terwijl die informatie nu juist wel – al die tien jaar – gewoon in het door hen zeer makkelijk te consulteren onlinesysteem staat. Maar dat kon niet. Van computer says no naar ambtenaar says no in vier pogingen.

En zo navigeren we met elkaar door een wereld waar privacy maakbaar is, maar ook vaak allerhande schendingen ervan op de loer liggen. Die maakbaarheid zit dan vooral in het vooraf goed nadenken of iets op een andere manier kan en als dat niet zo is, er dan voor zorgen dat alle risico's zo veel mogelijk ingedamd worden. Dat valt lang niet altijd mee, zeker niet als de norm 'gedigitaliseerd' is of als je bijvoorbeeld te maken hebt met 'vendor lock-in' of onvoorspelbare neveneffecten die inbreuk kunnen maken op de privacy.

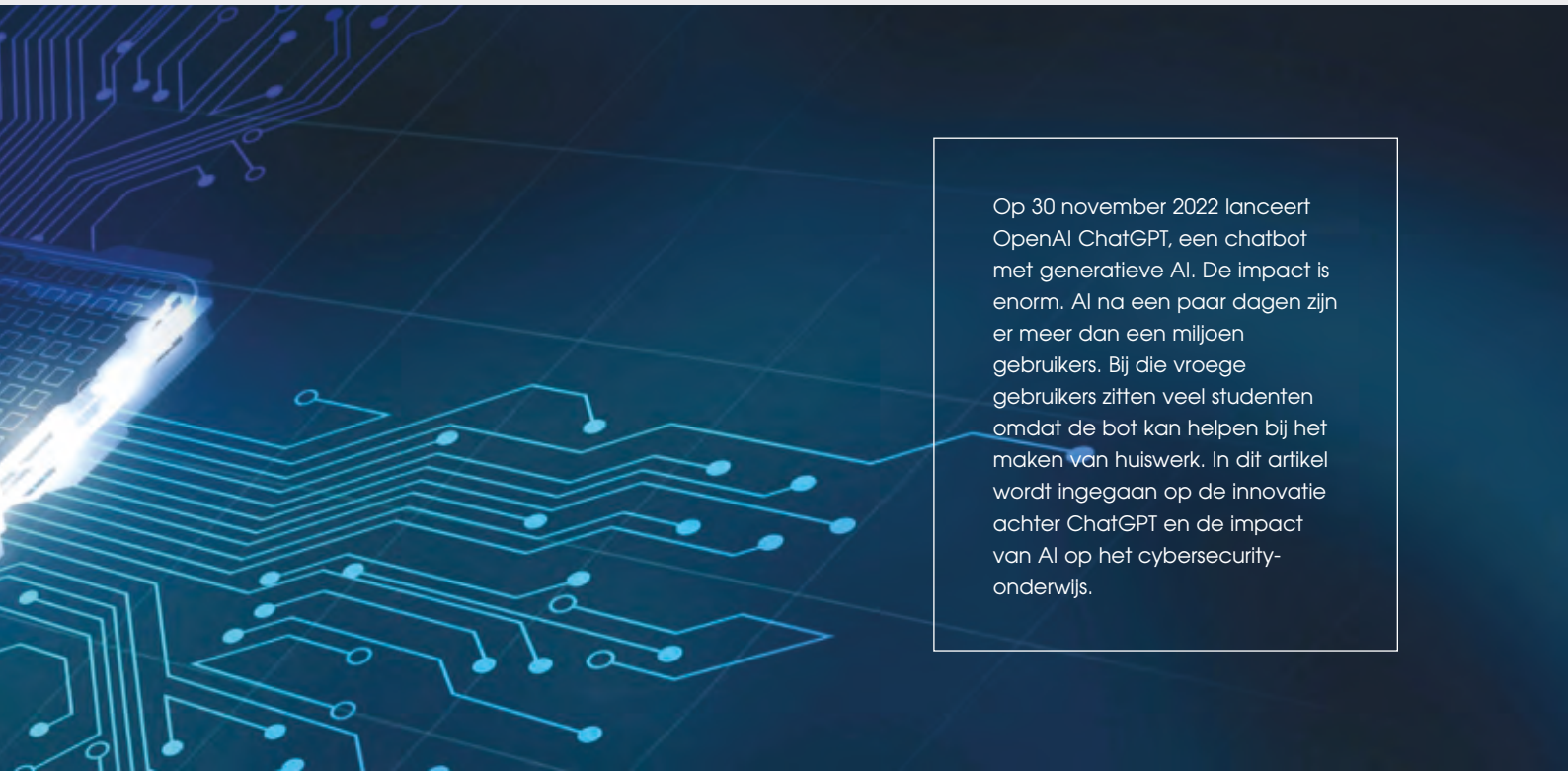
En soms vereist dat ook dat we smart doen om stom te kunnen creëren. Een van de mooiste, recenter voorbeelden daarvan vind ik het afplakken van de camera's van onze slimme telefoons. In de dance-scene is dat steeds vaker een voorwaarde om naar binnen te mogen gaan op een feest of in de club. Weigeren om het af te laten plakken, is het feest moeten missen. Onbevangen jezelf kunnen zijn, dansen en genieten zonder op het internet te belanden staat voorop. En, soms moet je ergens gewoon de stekker uittrekken – zo getuige het recente advies van de privacytoezichthouder aan de Nederlandse overheid om van Facebook af te gaan omdat er toch geen goede afspraken over privacy met het bedrijf te maken zijn. En hoe meer van dit soort kleine voorbeelden komen, hoe makkelijker het wellicht ook wordt om die speld in die hooiberg te vinden. En wie weet branden we die hooiberg dan samen stukje voor stukje af.

Rachel

Auteurs: Pieter Burghouwt, Emiel Kerpershoek en Marcel Spruit werken bij de Haagse Hogeschool en verzorgen cybersecurity-onderwijs zowel op bachelor- als masterniveau. Pieter Burghouwt e.a. zijn te bereiken via: P.Burghouwt@hhs.nl.

Kansen en bedreigingen van AI in het onderwijs

Bijna dagelijks is er berichtgeving over nieuwe AI-ontwikkelingen. Veel banen zijn ingrijpend aan het veranderen of gaan ingrijpend veranderen en bedrijven als OpenAI en NVIDIA groeien spectaculair, waarbij laatstgenoemde meer waard werd dan Google 's Alfabet (1). Het is meer dan alleen een hype; achter de soms overdreven verwachtingen liggen belangrijke technische ontwikkelingen, met name op het gebied generatieve AI.



Op 30 november 2022 lanceert OpenAI ChatGPT, een chatbot met generatieve AI. De impact is enorm. Al na een paar dagen zijn er meer dan een miljoen gebruikers. Bij die vroege gebruikers zitten veel studenten omdat de bot kan helpen bij het maken van huiswerk. In dit artikel wordt ingegaan op de innovatie achter ChatGPT en de impact van AI op het cybersecurity-onderwijs.

Cybersecurity en AI hebben belangrijke raakvlakken. Niet alleen wordt AI ingezet in het cybersecuritydomein voor bijvoorbeeld detectie van aanvallen; AI is zelf ook een IT-systeem en moet beschermd worden en veilig zijn.

Cybersecurityonderwijs en Machine Learning

Cybersecurity is een onderdeel of specialisatie van veel IT-opleidingen van het bacheloronderwijs, zoals bijvoorbeeld hbo-ICT en Computer Science. Daarnaast zijn er cybersecuritymasteropleidingen, die zowel vanuit hbo-instellingen als universiteiten worden aangeboden (2).

Al vele jaren introduceren de meer technisch-gerichte cybersecuritycurricula ML (Machine Learning) als middel om aanvallen, zoals intrusions, anomalies, spam en malware, te kunnen detecteren. De diepgang loopt daarbij sterk uiteen, afhankelijk van het opleidingsniveau en de focus van de studie. Uiteraard worden daarbij bekende ML-algoritmes geïntroduceerd, zoals bijvoorbeeld: neurale netwerken, beslisbomen en Naive Bayesian Filters maar er zijn wel verschillen:

- Op universiteiten wordt doorgaans een meer theoretische benadering gehanteerd, waarbij een sterke nadruk ligt op wiskundige fundamenten en theoretische aspecten van AI. Vaak is Machine Learning een onderdeel van datascience. Daarnaast heeft uiteraard de focus van onderzoeksgroepen invloed op de inhoud van het curriculum.
- Het onderwijs op hogescholen is meer gericht op praktische toepassingen en het gebruiken bij het oplossen van concrete problemen. De studenten maken bijvoorbeeld kennis met Naive Bayesian Classifier om op praktische wijze SPAM van normale e-mails te onderscheiden.

Voor projecten en practica met ML wordt vaak Python gebruikt, met name vanwege de toegankelijkheid en de uitgebreide ondersteuning voor machine learning bibliotheken. Studenten maken daarbij meestal gebruik van publiekelijk beschikbare datasets om modellen te trainen en te testen. Door de focus op detectie wordt ML vaak ingezet voor binaire classificatie (bijv. wel of geen intrusion). Ook bij digitale forensische analyse speelt ML een belangrijke rol, zoals predictive coding bij E-discovery.

Beperkingen van ML in cybersecurity-onderwijs

Bij het aanbieden van onderwijs op het gebied van ML spelen er twee belangrijke beperkingen:

1. Effectieve toepassing van ML-algoritmes vereist domeinspecifieke en wiskundige kennis. Dit is met name voor hogescholen een belangrijke beperking omdat studenten daar minder op getraind worden dan studenten van universiteiten. Het gebruik van ML-bibliotheken en GUI-gebaseerde

datascience-applicaties kunnen helpen, maar het blijft voor studenten lastig om te overzien welk algoritme het beste kan worden toegepast, welke features (input) gebruikt moeten worden en hoe training en testen het beste kunnen worden aangepakt.
2. Succesvolle toepassing van ML vereist gespecialiseerde grote datasets, die vaak nog gelabeld moeten zijn voor training. Het verkrijgen van dergelijke datasets is ingewikkeld en tijdrovend, wat de praktische mogelijkheden voor educatieve doeleinden beperkt.

Foundation modellen

AI tientallen jaren speelt ML een belangrijke rol in het AI-domein. In plaats van een machine te vullen met regels, leert de machine uit data om daarmee te kunnen voorspellen, classificeren of genereren.

Vanaf ongeveer 2010 gaat dit een stap verder door ontwikkelingen in Deep Learning (3). Met name bij beeldverwerking worden dan grote stappen gezet. De machine leert van ruwe data, zoals pixels, zonder 'handmatige' feature-engineering. Vanaf 2017 zijn er veel nieuwe ontwikkelingen op het gebied van generatieve AI. Met generatieve AI is het mogelijk om op basis van input tekst, beeld en geluid te genereren. Op zichzelf is dat niet nieuw, maar nieuwe architecturen, zoals met name transformers maken het mogelijk om AI te trainen op basis van zeer grote hoeveelheden data, door middel van self supervised learning (4). Hierdoor ontstaat een nieuw soort modellen, aangeduid als foundation modellen of GPAI (General Purpose AI) (5). Bekende voorbeelden van deze foundation modellen zijn GPT4, Gemini en Llama. Eén van de kenmerkende eigenschappen van foundation modellen is de hoge mate van 'transfer learning', waarbij het model ook problemen kan oplossen in domeinen waarvoor het niet of slechts minimaal getraind is.

Hierdoor is er sprake van een paradigma-shift in het ontwerpen van AI-systemen van smalle gespecialiseerde modellen, die gerealiseerd worden door intensieve training op een bepaalde taak, naar de meer universele pre-trained foundation modellen, die met beperkte aanpassingen op een nieuwe taak kunnen worden ingezet. Deze eigenschap droeg ook bij aan het succes van ChatGPT; de assistent die niet alleen welbespraakt is, maar ook zeer uiteenlopende taken kan uitvoeren, waaronder gespecialiseerde taken op basis van beperkte instructies en voorbeelden.

Generatieve AI in het cybersecurity-onderwijs

De komst van generatieve AI geeft in het cybersecuritydomein nieuwe mogelijkheden, zoals:

1. Het semantisch zoeken in documenten op basis van een vraag. Aan het AI-model wordt een vraag gesteld, waarbij een document(deel) wordt meegenomen. Door het meenemen van een document(deel) is het antwoord veel preciezer en terug te leiden naar de specifieke bron. Als gewerkt wordt met grote documenten of een hele bibliotheek, dan wordt door middel van speciale vectoren, 'embeddings', eerst het deel in de documentatie geselecteerd dat het meest relevant is. Men noemt deze techniek RAG (Retrieval Augmented Generation) (6).
2. Agents die bijvoorbeeld via API's, complexe applicaties, diensten of tools aanroepen. Hiermee kan op basis van een vraag een ingewikkelde handeling worden uitgevoerd. Het resultaat kan weer geïnterpreteerd en eenvoudig uitgelegd worden door het AI-systeem.
3. Het genereren van software en configuraties op basis van prompts. Zowel red teams als blue teams kunnen het ontwikkelen van speciale software of configuraties vereenvoudigen met GenAI. Github Copilot is een voorbeeld van een ontwikkeltool, die op basis van instructies in mensentaal, software kan schrijven, verbeteren en uitleggen (7).
4. Datascience op basis van een dataset met daarbij een vraag. Het AI-systeem voert automatisch data-analyse uit en gebruikt daarbij gegenereerde software voor analyses op de dataset. De uitvoer wordt vertaald naar resultaten in de vorm van een begrijpelijk antwoord (8).
5. Detectie van bijvoorbeeld threats en anomalies waarbij alleen finetuning nodig is in plaats van een volledige training (9).

De toepassingen zijn nog volop in ontwikkeling en het ligt voor de hand dat ze vaker teruggevonden gaan worden in de cybersecuritycurricula; waarschijnlijk eerst in projecten en later structureel in andere onderwijsvormen.

Een andere belangrijke ontwikkeling is dat kwaadwillenden steeds vaker AI zullen gebruiken om aanvallen te ondersteunen, bijvoorbeeld door te helpen met het programmeren van malware, het opstellen van geloofwaardige phishingmails of het genereren van deep fake beeld en geluid. Ook die kennis zal zijn weg moeten vinden in de cybersecuritycurricula (10).

Ten slotte vormen AI-systemen zelf ook een doelwit van cyberaanvallen (11). Voorbeelden hiervan zijn:

- Tijdens training het model beïnvloeden door aanpassing van training-data, pretraining-data, finetuning-data of modelparameters (poisoning)
- Tijdens gebruik het model misleiden door bepaalde features in de data aan te passen (evasion)

- De vertrouwelijkheid van het systeem aanvallen, bijvoorbeeld door middel van speciale input, die een preprompt-tekst laat zien (prompt injection)
- Aanvallen die te maken hebben met de implementatie, bijvoorbeeld een datalek via een AI-provider of ondersteunende software en bibliotheken met daarin Trojaanse paarden etc.

Ook dit zal aandacht moeten krijgen in de cybersecuritycurricula.

Ongeoorloofd gebruik AI

Sinds de komst van ChatGPT hebben studenten generatieve AI massaal omarmd. Schattingen over het gebruik van ChatGPT door studenten lopen uiteen. Uit onderzoek in het VK van oktober 2023 bleek dat 32% van de studenten meerdere keren per week gebruik maakt van ChatGPT maar bij informatica en technische studies lag dit op 66% (12). Het is natuurlijk zorgelijk wanneer generatieve AI door studenten ongecontroleerd wordt ingezet voor het maken van studieopdrachten. Bovendien worden in het hoger onderwijs de leerprestaties beoordeeld op basis van opdrachten die buiten het zicht van de docenten worden gemaakt. De validiteit en betrouwbaarheid van die beoordeling kan ernstig worden verstoord als onduidelijk is in hoeverre AI heeft geholpen bij het maken van een opdracht. Weliswaar zijn hiervoor verschillende detectietools ontwikkeld, maar ze blijken in de praktijk vaak foutgevoelig (13). Vaak is het gebruik van generatieve AI, zoals ChatGPT, zelfs zonder detectietools al duidelijk te herkennen. Zo zal de AI-applicatie in sommige gevallen literatuurreferenties verzinnen of een stuk hoogdravende tekst genereren zonder echte inhoud. Maar het gebruik van generatieve AI is niet altijd te bewijzen, zeker niet als generatieve AI verder evolueert.

In plaats van detectie is preventie van ongeoorloofd AI-gebruik in de studie een betere oplossing. Dat kan enerzijds door te werken in een gecontroleerde omgeving, die tijdens toetsing de toegang tot AI blokkeert. Anderzijds kan dat door het gebruik van AI juist te omarmen en zo veel mogelijk in te bedden in het onderwijs. In dat laatste geval moeten studenten bij gebruik goed de mogelijkheden en risico's weten en verantwoordelijkheid nemen. Belangrijke verantwoordelijkheden in deze context zijn:

1. Werken met toestemming (van de opdrachtgever en/of de school en binnen wet- en regelgeving)
2. Transparant AI-gebruik (door precies aan te geven waar en hoe AI gebruikt is)
3. Correctheid en aanvaardbaarheid van AI output (overgenomen AI-resultaten moeten correct en veilig zijn en mogen bijvoorbeeld dus niet gevaarlijk of beledigend zijn)
4. Geen hinder bij beoordeling leeruitkomsten (AI mag niet gebruikt worden voor zaken die de student zelf moet doen om de beoogde leeruitkomsten aan te tonen)

Dergelijke verantwoordelijkheden zijn alleen te nemen met voldoende kennis over hoe AI op de juiste manier gebruikt moet worden. Zaken als correctheid, ethiek, verklaarbaarheid en nieuwe regelgeving, zoals de AI-Act (14), spelen daarbij een belangrijke rol en horen dus ook in een modern cybersecuritycurriculum.

Ten slotte bieden de nieuwe mogelijkheden van AI ook allerlei didactische kansen in het onderwijs. Zo bieden OpenAI en Microsoft customizable AI-agents met aanvullende documenten, API-calls en prompting. Hiermee kan een docent een AI-applicatie maken die bijvoorbeeld de slides van een les uitlegt of oefenvragen stelt en die na beantwoording uitleg geeft of een inhoudelijke discussie aangaat met een student.

Kortom, we zitten in een zeer interessante periode, waarin AI flinke veranderingen brengt in het onderwijs en zeker ook in het cybersecurity-onderwijs.

Referenties

(1) https://www.forbes.com/sites/dereksaul/2024/02/12/nvidia-is-now-more-valuable-than-amazon-and-google/
(2) https://communities.surf.nl/cybersecurity/artikel/cybersecurity-opleidingen-bij-mbos-hogescholen-en-universiteiten-in-nederland
(3) https://www.nature.com/articles/nature14539
(4) https://proceedings.neurips.cc/paper_files/paper/2017/hash/3f5ee-243547dee91fbd053c1c4a845aa-Abstract.html
(5) https://arxiv.org/abs/2108.07258
(6) https://proceedings.neurips.cc/paper/2020/hash/-6b493230205f780e1bc26945df7481e5-Abstract.html
(7) https://docs.github.com/en/copilot
(8) https://platform.openai.com/docs/assistants/tools/code-interpreter
(9) https://sciendo.com/article/10.2478/kbo-2023-0072?content-tab=abstract
(10) https://ieeexplore.ieee.org/abstract/document/10198233
(11) https://csrc.nist.gov/pubs/ai/100/2/e2023/final
(12) https://www.thehrdirector.com/business-news/ai/chatgpt-32-university-students-admit-using-weekly/
(13) https://hai.stanford.edu/news/ai-detectors-biased-against-non-native-english-writers?ref=gptzero.ghost.io
(14) https://artificialintelligenceact.eu/the-act/

Auteur: Dr. Els de Busser is universitair docent cyber security governance bij het Institute of Security and Global Affairs van Universiteit Leiden. Els is bereikbaar via: e.de.busser@fgga.leidenuniv.nl.

Cybersecurity by integrated design: veiligheid voorbij technologie

Storingen in het functioneren van digitale technologie en de gevolgen van hacks of datalekken worden vaak pas aangepakt wanneer er effectief schade is veroorzaakt. We denken in dergelijke gevallen dan voornamelijk aan financiële of materiële schade. Het is van groot belang de aanpak van zulke problemen te verschuiven naar de vroegste ontwikkelingsfase. De toeslagenaffaire liet op pijnlijke wijze zien hoe fouten in de ontwikkeling van digitale technologie tot meer dan enkel financiële of materiële schade kunnen leiden (1).

Het door NWO gefinancierde onderzoeksproject Cybersecurity by Integrated Design – kortweg het C-SIDE project – heeft als ambitie richtlijnen op te stellen voor softwareontwikkeling. Deze richtlijnen houden rekening met zowel technologische als niet-technologische aspecten. Het doel is om al in de beginfasen van softwareontwikkeling meer veiligheid in te bouwen, zodat dit later resulteert in veiligere technologie.

Een interdisciplinair team van wetenschappers van de Universiteit Leiden en de Haagse Hogeschool bestudeert verschillende elementen van dit proces. Hun doel is om een set richtlijnen te creëren die sleutelfiguren in het softwareontwikkelingsproces helpt. Deze richtlijnen zullen hen ondersteunen bij het integreren van relevante organisatie-gerelateerde aspecten, mensenrechten en het voorkomen en detecteren van kwetsbaarheden in softwaredesign. Bovendien omvat het project een studie naar het meten van veiligheid en kwetsbaarheden in technologie. Om het gebruik van zulke richtlijnen te ondersteunen, wordt ook een studie uitgevoerd naar het institutionele design van de Nederlandse overheid.

Waarom digitale veiligheid door geïntegreerd design?

By-design denken is op zichzelf niet nieuw. Privacy-by-design en security-by-design zijn veelvoorkomende begrippen in de wereld van digitale technologie en veiligheid. Wat wel nieuw is, is om het by-design denken uit te breiden naar meer dan enkel de technologische aspecten. De holistische en interdisciplinaire aanpak van het C-SIDE project past daar uitstekend bij. Door expertises uit verschillende disciplines bij elkaar te brengen zoals de computerwetenschappen, sociale wetenschappen, politieke wetenschappen en organisatiestudies, krijgen we een breder beeld van wat nu precies nodig is om software niet alleen op technologisch vlak beter en veiliger te ontwikkelen, maar ook hoe de organisatie rondom de softwareontwikkelaar optimaler en veiliger kan werken. We hebben het dan zowel over de organisatie van het ontwikkelende bedrijf, als over hoe de overheid zich organiseert. Vanuit wetenschappelijk standpunt is het project innovatief, omdat het onderzoekers van diverse disciplines samenbrengt om gezamenlijk iets nieuws te creëren. Een grote uitdaging voor de projectleiding is om vier promovendi hun eigen onderzoek te laten doen. Tegelijkertijd moeten zij in teamverband de richtlijnen ontwikkelen, zodat het geheel meer waarde heeft dan de som der delen.

Veiligheid voorbij technologie

Security-by-design mag dan wel een veelgebruikt begrip zijn in de ontwikkeling van technologie, uit een systematisch onderzoek naar de wetenschappelijke literatuur over security-by-design blijkt echter dat er vooral onduidelijkheid heerst over wat dit nu precies betekent (2). Een discipline-overstijgend onderzoek geeft aan dat er geen eensgezindheid bestaat over het begrip. In tegenstelling tot privacy-by-design dat door slechts één auteur uitvoerig werd bestudeerd en beschreven, is security-by-design door een groot aantal auteurs geanalyseerd, met een brede variatie aan definities tot gevolg. Auteurs zijn het oneens over wat nu precies beschermd wordt – toestellen, systemen, of privacy – en wat nu precies vermeden wordt door security-by-design toe te passen – kwetsbaarheden, aanvallen of dreigingen. Ook de manier waarop, en op welk moment in de software lifecycle security-by-design wordt ingezet, is niet geharmoniseerd. Wat wel duidelijk is, is dat er een onmiskenbare gelegenheid bestaat om security-by-design concreteer te maken door een eenduidige definitie en bruikbare richtlijnen aan te bieden. Dit is wat het C-SIDE project beoogt.

Digitale veiligheid wordt vaak beperkt ingevuld op basis van de traditionele triade: vertrouwelijkheid, integriteit en beschikbaarheid, ook wel bekend als de 'CIA'. Wanneer deze klassieke blik echter verder wordt geopend, en ook fysieke en sociale veiligheid worden meegenomen in het denken over security-by-design, kan dit resulteren in een verhoogde aandacht voor de impact die technologie op mensen kan hebben, bijvoorbeeld door algoritmes te ontwerpen die niet discriminerend werken. Een andere manier om security-by-design breder in te vullen is door te kijken naar de waarden die een softwareontwikkelingsbedrijf vooropstelt, zoals privacy, inclusie, en duurzaamheid. Deze waarden vloeien namelijk door in de geldende regels, processen, en uiteindelijk de producten die het bedrijf op de markt brengt. Een bedrijfscultuur is ook gebaseerd op deze waarden en heeft volgens wetenschappelijk onderzoek (3) een effect op de veiligheid in het bedrijf. Dit betekent dat wanneer werknemers van een bedrijf zich veiliger gaan gedragen en veiligheid een rode draad vormt door de besluitvormingsprocessen heen, en de praktijk in alle lagen, dat betere resultaten oplevert dan wanneer enkel wordt gefocust op het naleven van de geldende wet- en regelgeving. Wanneer bijvoorbeeld de sociale veiligheid sterk is in een organisatie, en werknemers voldoende vertrouwen hebben om op ondeugdelijkheden in softwareontwikkeling te wijzen zonder negatieve gevolgen, dan leidt dit tot veiligere technologie.

Een (overdreven) focus op het naleven van geldende wet- en regelgeving kennen we als compliance. Vaak wordt echter de denkfout gemaakt dat compliance automatisch tot veiligheid leidt (4). Mensen zullen fouten blijven maken, ongevallen zullen

Digitale veiligheid wordt vaak beperkt ingevuld op basis van de traditionele triade: vertrouwelijkheid, integriteit en beschikbaarheid, ook wel bekend als de 'CIA'

blijven gebeuren en ook een hacker zal er niet bij stilstaan of een bedrijf een perfecte compliance-score heeft.

Het C-SIDE project bouwt verder op deze visie en breidt ook hier het concept van veiligheid uit. Het uitbreiden van veiligheid met fysieke en sociale veiligheid werd tot op zekere hoogte bevestigd door een steekproef van softwareontwikkelaars (5). Op de vraag wat we precies van hen mogen verwachten als het gaat om het inschatten van de impact van de software die zij ontwikkelen, kan daar onmogelijk een algemeen antwoord op gegeven worden. Dit kan enkel op basis van concrete omstandigheden. Een mogelijk criterium dat hierbij kan helpen is de 'redelijkerwijs te verwachten impact', rekening houdend met de technologische en maatschappelijke ontwikkelingen van dat moment, om een juiste inschatting te kunnen maken.

Een belangrijke technologische tak van het C-SIDE project is het meten van veiligheid. Naast het veelgebruikte meten van het aantal kwetsbaarheden, is het vernieuwende van het project dat ook de kritische inzichten van de betrokken personen worden meegenomen in het meten van veiligheid (6). Dit zorgt voor een meer geïntegreerde aanpak. In het meten van veiligheid, door middel van het nagaan van het aantal kwetsbaarheden in software, wordt vaak vertrouwd op zogenaamde bibliotheken van bekende kwetsbaarheden. Een tweede technologische tak van het C-SIDE project betreft daarom een analyse van de kwaliteit en kwantiteit van dergelijke bibliotheken, en wat de mogelijkheden voor het verbeteren van deze bibliotheken zijn om uiteindelijk tot veiligere software te komen.

De combinatie van technologie en governance in het project doet ook de vraag rijzen hoe de Nederlandse overheid een passende ondersteuning kan bieden van een geïntegreerde aanpak van digitale veiligheid. Om deze vraag te beantwoorden werd in een eerste fase van het project het Nederlandse overheidslandschap van digitale veiligheid in kaart gebracht. In een tweede – nog lopende fase – wordt bestudeerd in hoeverre dit landschap gefragmenteerd is, en of dit problematisch is. Een belangrijk onderdeel van deze studie is hoe de academische literatuur en de beschikbare beleidsdocumenten schrijven over fragmentatie.

De C-SIDE richtlijnen

Nu het onderzoeksproject inmiddels halverwege is, neemt het eindproduct duidelijkere vormen aan. De richtlijnen die na vier jaar wetenschappelijk onderzoek worden gepubliceerd, zijn onderverdeeld op basis van de verschillende belanghebbenden over digitale veiligheid: de Nederlandse overheid, softwareontwikkelaars, en de bedrijven waarvan ze deel uitmaken. Door deze belanghebbenden heldere richtlijnen aan te reiken die een organisatorische, technologische, ethische, en beleidsmatige inbedding van veiligheid mogelijk maken, is het doel van het C-SIDE project, een geïntegreerde en interdisciplinaire aanpak van digitale veiligheid na te streven, een stap dichterbij.

Referenties

(1) Prins, C. (2021), Discriminerende algoritmes, Nederlands Juristenblad: https://www.njb.nl/blogs/discriminerende-algoritmes/

(2) Del Real, C.; De Busser, E. en Van den Berg, B. (2024). Shielding Software Systems: A Comparison of Security by Design and Privacy by Design Based on a Systematic Literature Review, Computer Law and Security Review, Vol. 52, 105933.

(3) Schein, E.H. (1990). Organizational culture. Am. Psychol., Organizational Psychology 45, 109–119; Van Niekerk, J.F. en Von Solms, R. (2010). Information security culture: A management perspective. Computer Law and Security Review, Vol. 29, 476–486.

(4) Boeken, J. (2024). From Compliance to Security, Responsibility beyond Law, Computer Law and Security Review, Vol. 52, 105926.

(5) Del-Real, C., en De Busser. (2023). Defining security by design: A stakeholders perspective. Cyber Security by Integrated Design. December 2023: https://www.projectcside.nl/research-and-publications

(6) Kudriavtseva, A. (2024). A Software Security Evaluation Framework. In2024 IEEE/ACM 46th International Conference on Software Engineering: Companion Proceedings (ICSE-Companion '24), April 14–20, 2024, Lisbon, Portugal. ACM, New York, NY, USA (in druk)

COLUMN NICOLE

Quantum is coming: tijd om te ontwaken

Terwijl iedereen over elkaar heen struikelt om de laatste ontwikkelingen op het gebied van AI bij te benen, doet zich in de coulissen de volgende technologische doorbraak voor: quantum computing. Quantumcomputing maakt gebruik van de principes van de kwantummechanica om informatie te verwerken op een fundamenteel andere manier dan klassieke computers. Tien jaar geleden waarschuwde de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) al voor de mogelijke impact van quantum computing op onze huidige vormen van encryptie. Blijkbaar is er nog steeds onvoldoende aandacht voor dit onderwerp op beleidsniveau, in ieder geval bij de Europese Commissie (EC). Deze conclusie trek ik op basis van een brief die in maart werd gepubliceerd door twintig Europarlementariërs. Hierin doen zij een oproep aan de EC om organisaties te stimuleren zich voor te bereiden op een overgang naar quantum proof encryptie.

Het gegeven dat juist de EC deze wake-upcall nodig heeft, is opmerkelijk. Ongeveer zeven jaar geleden gaf zij opdracht aan Europol en Eurojust om te werken aan een Observatory Function on Encryption. De EC wil tijdig op de hoogte zijn van relevante ontwikkelingen om het beleid daarop te kunnen aanpassen. Als projectleider en medeauteur van de rapporten van deze Observatory Function kan ik u verzekeren dat wij destijds ook al wezen op de mogelijke gevolgen van quantumcomputing. Natuurlijk is er onzekerheid en onduidelijkheid over wanneer quantumcomputing werkelijkheid zal worden; schattingen variëren van vijf tot vijfentwintig jaar, of soms nog langer. Ergens tussen Generatie Bèta (2025–2039) en Generatie Gamma (2040–2054) dus. Met de huidige klimaatcrisis, meerdere oorlogen en deepfakeporno, kan ik mij voorstellen dat het blussen van de branden van vandaag meer aandacht krijgt dan het uitblazen van een nog niet bestaande vlam in de toekomst.

En toch zeg ik: quantum is coming. Ik beschouw de komst van de quantum computer als een gegeven; we moeten ons erop voorbereiden. Dit zal, ben ik bang, niet snel en ook niet vrijwillig gebeuren. Organisaties nemen doorgaans pas cybersecuritymaatregelen onder dwang van de overheid of nadat zij slachtoffer zijn geworden van een serieus incident. Ik begrijp dat ik generaliseer en dat er organisaties zijn die hun huiswerk wel hebben gedaan. Maar op het gebied van cybersecurity zijn zulke verstandige organisaties eerder uitzondering dan regel. Daar komt bij dat beleidsmakers doorgaans achter de feiten aan lopen. Veelal gebruiken zij het argument dat technologie zich zo snel ontwikkelt, of liever gezegd laat ontwikkelen, dat het beleidsproces daar niet met dezelfde snelheid op kan reageren. Quantumcomputing nodigt ons uit – zowel organisaties als beleidsmakers – om eindelijk vooruit te lopen op de technologie. Dat kan echter alleen als wij tijdig ontwaken uit onze winterslaap.

Dr. Nicole van der Meulen is expert op het gebied van cybersecurity en emerging technologies en werkzaam bij SURF als Cybersecurity Innovation Lead, ns.vandermeulen@gmail.com

Authors: Reinder Wolthuis, senior consultant/projectmanager cybersecurity at TNO reinder.wolthuis@tno.nl. Gert van der Lee, senior innovator/researcher cybersecurity at TNO, gert.vanderlee@tno.nl. Richard Kerkdijk, senior security consultant at TNO, richard.kerkdijk@tno.nl. Natalia Kadenko, researcher at NCSC, n.i.kadenko@minjenv.nl.

SOC of the future

Security monitoring and incident response will face major challenges in the coming years, not least because the complexity of infrastructures, threats and regulation will increase drastically. SOC managers and governmental agencies need to rethink their strategies, policies and the organization of SOCs to be prepared for these challenges. This article describes a conceptual blueprint for future SOCs that can assist the NCSC, SOC managers and CISOs in creating long term SOC roadmaps.

Cyber-attacks are developing at a rapid pace and becoming increasingly sophisticated and complex. To elevate their cyber defences, many organisations have complemented traditional (preventive) security controls with security monitoring and incident response operations. Capabilities maintained to this end are often united in a so-called Security Operations Centre (SOC). Smaller organisations that cannot maintain such provisions in-house typically outsource them to (the SOC of) a Managed Security Service Provider (MSSP). The environment, in which such SOCs operate, however, is undergoing significant changes. A prominent example is the transformation of infrastructures that SOCs are tasked to protect, which are increasingly incorporating cloud services, OT (Operational Technology) and IoT (Internet of Things) devices. Meanwhile new regulation such as NIS2, the Cyber Security Act and Cyber Shield will impose new requirements SOCs, for instance concerning their collaboration and information exchange. Security Operations Centres and government bodies such as the National Cyber Security Centre (NCSC) will need to evolve with these changes in order to stay relevant and effective.

This article presents a conceptual blueprint for the SOC by the year 2030. It reflects predicted changes in technology, organisational structures, the market for security solutions and in national and European legislation, with specific attention towards the role of government bodies at the national and European level. The article is based on a study that TNO performed in collaboration with the Dutch NCSC (SOC2030). The study consisted of literature review and interviews with various stakeholders in industry.

Current state of the SOC

Organisations can implement security monitoring, detection and response capabilities in a variety of ways and to a varying level of maturity. They usually include event - and incident management, but may also cover threat intelligence, vulnerability management and a plethora of other operational security responsibilities. These capabilities can be either maintained in-house or (partially) outsourced to service providers, such as MSSPs, and may be consolidated in one organisational entity or spread out over more. A typical example of the latter is the separation between monitoring and detection capabilities (provided by a SOC) and response capabilities (provided by a CERT or CSIRT).

The last few years have already seen a rapidly changing SOC landscape, characterized by a growing SOC-market, regulations that increasingly address security operations, a wider adoption of best practices and more, mostly sector-based, collaboration. On the whole, these developments have led to a growing overall maturity of SOCs.

Relevant developments in the coming years

Regardless of way, shape or form, the challenge for SOCs in the coming years will be - not only to monitor an increasingly complex, distributed and diverse collection of endpoints, applications and data, but - to do that facing adversaries that are constantly increasing the effectiveness of their operations through adoption of innovative technologies. On top of that, the contribution of state-sponsored actors to the threat landscape will grow significantly under the influence of geopolitical dynamics, resulting in an overall increase in complexity and impact of cyberattacks.

Technological improvements revolving around automation will enable SOCs to face that challenge and to focus more on these complex, high impact attacks. These improvements include wider adoption of SOAR solutions for security workflow automation and AI for advanced detection and analytics. And although AI's capabilities will have limitations, most experts agree that it should be able to completely replace first tier analysts by 2030.

These technological developments will also change SOC staffing requirements. They allow SOC personnel to focus more on tactical and strategic duties and on the challenges that emerging technologies and changing regulatory requirements introduce. They also allow SOC personnel to focus more on prevention, threat hunting, prediction and other proactive capabilities instead of on detection and response.

In turn, this may invite switching from a classic SOC tier-based model to a model with collaborating expert groups or cross-functional teams, consisting of threat intelligence analysts, business risk analysts, security engineers, crisis managers and data analysts. It could also trigger new core capabilities for SOCs, such as adversary emulation and impact analysis.

However, all of these developments will come at a considerable price. The cost of maintaining a proper functioning SOC will increase dramatically as a result of adopting the required technological innovations. This will force companies with in-house SOC facilities to start outsourcing some or all of their SOC capabilities to specialised service providers. It will also drive collaboration between SOCs and promote initiatives for joint SOC services in industries such as energy and water.

And finally, legislation will continue to be a driving force for cybersecurity in general and for SOC maturity in particular. IT security governance will become more mature as government institutions increase supervision and enforcement of rules and policies. Moreover, experts stress that government involvement should not be limited to legislative and supervisory roles, but should also encompass advisory work and maybe even operational assistance to essential entities and sectors.

Vision on the SOC in 2030

The blueprint for Security Operations Centres in 2030 is a thought experiment that paints a picture of the SOC-world in 2030.

Please note that the blueprint is described in a somewhat provocative form, assuming that currently foreseen trends play out to their extreme. The underlying idea is that this will likely stimulate the most valuable discussion. Also, it is conceivable that unforeseen, disruptive technologies (similar to the internet, AI and quantum computing in the past) will emerge between now and 2030 that could drastically alter the cyber landscape and consequently affect the blueprint on specific aspects.

Foreseen developments in the SOC landscape are schematically visualised in the figure below. For reference, the figure incorporates two particular variants of SOC/CSIRT instalment in an end user organisation. Here organisation A maintains in-house SOC and CSIRT operations to protect a hybrid (on-premise and cloud) technical infrastructure, whereas organisation B relies solely on cloud infrastructure and outsourced most of its security operations to a third party MSSP.

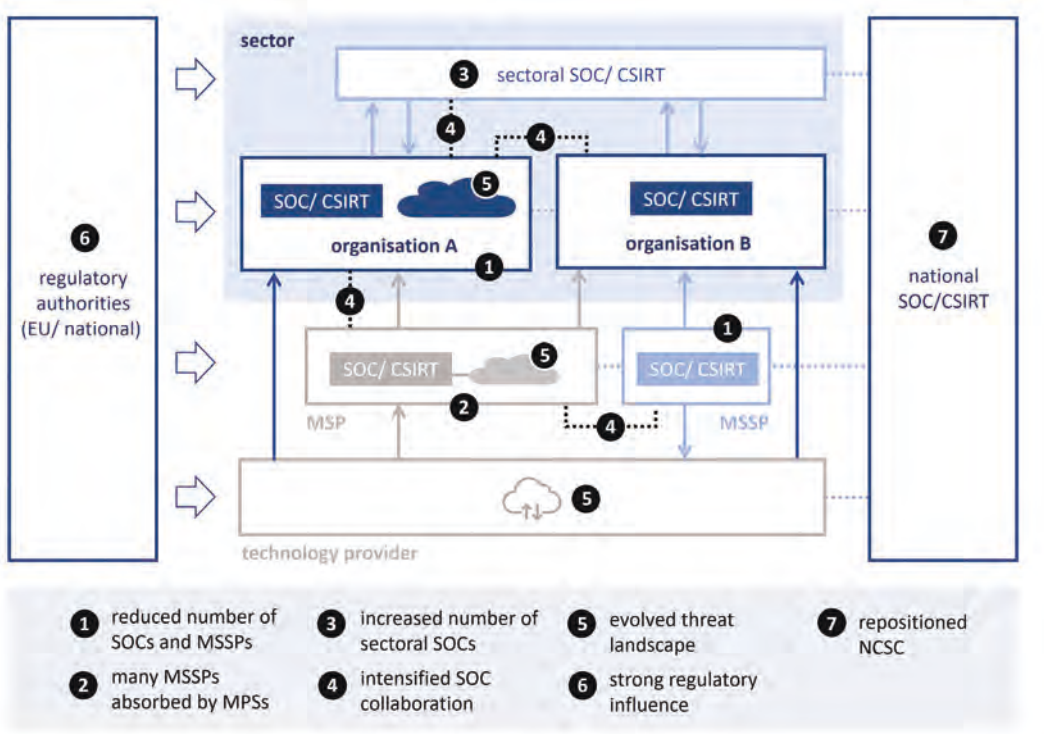


Figure 1: The SOC-landscape.

In practice, the landscape will obviously encompass a more elaborate range of deployment structures.

As shown in the figure, the authors foresee a total of 7 key changes in the SOC-landscape by the year 2030:

1. **The number of SOCs and MSSPs offering SOC services has decreased drastically.** Far fewer end-user organisations maintain their own SOC. Instead, most of them make use of the high-quality services provided by Managed Security Service Providers (MSSPs, e.g. KPN Security, Fox-IT, Pinewood) or even Managed (IT) Service Providers (MSPs, e.g. Akamai, Forescout). Consequently, the overall number of SOCs has decreased. The cost of keeping a mature SOC in operation and keeping it up-to-date is simply too high, due to the specific expertise and high degree of automation that this requires. Only a few large end-user organisations and end-user organisations that maintain specific infrastructure (such as OT infrastructure) or specific risks are able to justify an in-house SOC.
2. **MSPs have taken over much of the MSSP market.** For most of the market, the security services offered by large MSPs sufficiently fill the security monitoring needs of end-user organisations. But there will still be a role for the MSSP that has more insight in the specific context in which an end-user organisation operates. Consequently, there are new forms of collaboration between MSPs and MSSPs that offer their combined services to the end-user organisation.
3. **Every NIS3 (successor of NIS2) sector has a sectoral SOC, used for threat information exchange, and to provide collaborative monitoring, detection and response.** All the sectors to which the (fictitious) NIS3 applies have a sectoral SOC. The principal task of these sectoral SOCs is to facilitate (threat) information exchange within the sector. Many of these sectoral SOCs also offer collaborative monitoring, detection and response services to their members, although in most cases outsourced to a MSSP.
4. **A SOC and MSSP cannot operate without intense collaboration and information sharing with other stakeholders.** Information exchange between all the entities in the SOC landscape is a key element for SOCs in preventing and detecting threats. National SOCs mutually exchange information that is relevant for critical sectors and the role of

Information Sharing and Analyses Centres (ISACs) has been taken over by sectoral SOCs. Where relevant, national SOCs relay threat information to sectoral SOCs, end-user SOCs, MSSPs and MSPs within their respective countries. Besides national sharing and distribution, information is also shared bilaterally across borders, mainly by sectoral SOCs.

5. **The primary focus of SOCs and MSSPs will be on highly automated threats coming from skilled threat actors such as criminal organisations and nation states.** Threat actors at the level of script kiddies are managed in a 'business as usual' way of working and require little attention from the SOC. Attacks launched by such low-level threat actors are detected and mitigated automatically or handled as part of normal IT operations. Most attacks on end-user organisations, however, come from criminal organisations (for profit) and in some cases they are state-sponsored, (e.g. oriented at destabilizing society or stealing information). Such attacks are typically AI-assisted and mostly targeting a specific end-user organisation, which makes them hard to detect and mitigate.
6. **Most organisations make use of formally accredited SOC services, due to EU and national regulation.** NIS3 has become the essential EU regulation on cyber security. This has led to national cyber security regulations that mandate the use of SOC services for every critical sector. These SOC services need to be certified according to a defined minimum maturity level, depending on the criticality of the sector. A few widely adopted SOC maturity models drive the use of certified SOC services.
7. **The NCSC is the national SOC/CSIRT according to NIS3, the primary point for national threat information sharing and in the lead during national cyber crises.** The NCSC acts as national SOC/CSIRT (NIS3). In that role, the NCSC exchanges information that is relevant for critical sectors with other national SOCs. The NCSC has a coordinating and advisory role in the information exchange. The NCSC is in close contact with large technology providers that supply threat information. The NCSC relays relevant information to sectoral SOCs, end-user SOCs, MSSPs and MSPs where appropriate. When an incident with societal impact occurs at an end-user organisation in a critical sector or at several end-user organisations simultaneously, the NCSC coordinates the mitigating actions across all organisations involved on a national level.

In parallel to the above, the authors also foresee particular changes within the SOC and its direct environment:

The SOC focus is largely on proactive and predictive activities. Most common security incidents and vulnerabilities get detected automatically and mitigation is largely standardized and automated, for instance implemented with support of security playbooks and Security Orchestration, Automation and Response (SOAR) tools. But new and/or sophisticated attacks still require manual intervention, supported by automated (AI based) tooling for first-time incident detection and response. The focus of most SOCs is on optimizing situational awareness and predictive and proactive activities: monitoring the threat landscape and assessing threat intelligence.

Many SOC activities are automated and do not need human intervention. The detection, assessment and response to security events is highly automated with support of AI and SOAR tooling. Automation solutions have replaced first- and second tier security analysts in all but a very few (specialized) SOCs; highly sophisticated attacks also require involvement of security analysts, supported by the automated tools. The shift to cloud services offers particular potential for automated response. SOC personnel are able to focus on predictive and pro-active activities, business risk and situational awareness supported by a data lake that is filled by a multitude of internal and external data and information sources, maintained by data engineers.

Business processes such as Zero Trust decision making, benefit from the wealth of information that is available at the SOC. To do its job well, a SOC gathers an enormous amount of current information and data from all infrastructure and applications of an end-user organisation. Other business processes also profit from this information. For instance, the 'continuous decision making' (e.g. to change access rights) in Zero Trust will highly benefit from the up-to-date information sources available at the SOC.

Highly standardized technology, tooling and way-of-working enables efficient and effective performance and information exchange. SOCs and MSSPs make elaborate use of widely available standards e.g. for incident data and information exchange formats. Because of the use of these standardized formats and interfaces, the way of working is efficient and tools are interchangeable.

This paper has looked into the current state and the possible future of SOCs in the rapidly changing security landscape

Most of the infrastructure that is monitored by SOCs and MSSPs will be cloud-based. The IT-services industry has successfully transitioned to a "cloud unless" approach, leaving only classified systems, highly vulnerable intellectual property and OT as remaining on-premise infrastructure. Also 'cloud edge' solutions are broadly used. This refers to setups in which cloud technology is used on location, for example in combination with OT. This cloud focus allows SOCs to work in a highly standardized and automated way, making optimal use of the security capabilities that are built in by cloud service providers. This also makes it easier for MSSPs to standardize and automate activities across multiple customers.

A majority of SOC staff will consist of risk -, data -, threat analysts and crisis managers; only very few 'traditional' SOC analysts have remained. Virtually all traditional tier 1 and tier 2 SOC analysts' roles have disappeared, and the majority of SOC staff consists of highly skilled experts in risk analysis, CTI analysis or data analysis. These analysts operate on a tactical level and provide a new generation of core SOC services, such as collecting and processing high quality threat information, establishing situational awareness and conducting predictive analysis. With this shift to threats instead of incidents, response staff consists mostly of security engineers and crisis managers rather than traditional (security) incident responders. A challenge is to find and/or educate the few SOC analysts that are still needed, considering that the traditional career path from tier 1 to tier 2 to SOC analyst expert has disappeared.

All SOCs have abandoned the traditional tier-based SOC model in favour of flat organisational structures with staff collaborating in interdisciplinary teams. Instead of being organized in distinct tiers, SOC staff is organized in a skill- or role-based manner. This allows for a more flexible and targeted deployment of skills as cyber threats are addressed. SOCs have the mandate for making pre-emptive changes to the IT environment. A business impact threshold is agreed upon above which additional authorization (for SOC or MSSP) needs to be sought from decision makers.

Closing words

This paper has looked into the current state and the possible future of SOCs in the rapidly changing security landscape. Based on literature analysis and expert input, a number of conclusions and recommendations can be provided. First, collaboration and information-sharing will play an increasingly important role in how efficiently SOCs will be able to operate. It is therefore important to further examine the existing mechanisms and conduct research into the so far underutilized ways of collaboration. Second, most experts would encourage additional guidance and enforcement from the governmental institutions, believing that there is room for such a role. The NCSC in particular was mentioned as an institution ideally suited to play a central role in facilitating collaboration. Finally, each organization should re-examine its SOC strategy based on its needs and resources, as well as the anticipated shift from reactive to pro-active SOC.

Reference

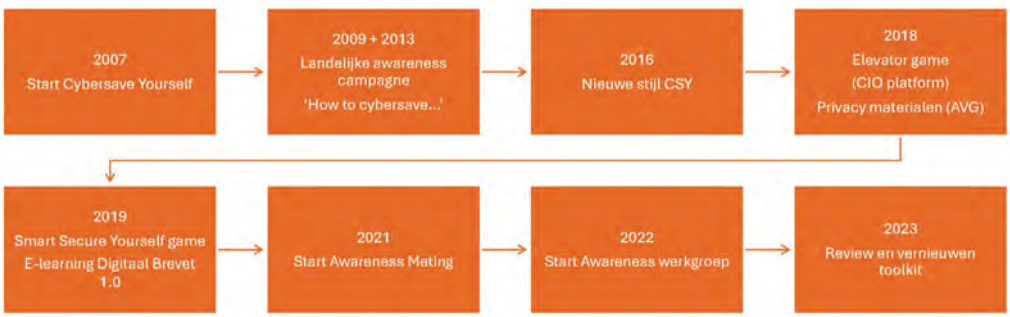
(SOC2030) Blueprint for a Security Operations Center in 2030 – SOC of the Future, Reinder Wolthuis, Gert van der Lee, unclassified, February 27 2024, report number TNO 2023 R11803, https://publications.tno.nl/publication/34642162/x0DJXn/TNO-2023-R11803.pdf

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 onderzoeksinstellingen 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 onderzoeksinstellingen waarin de leden hun krachten bundelen. Binnen SURF werken universiteiten, hogescholen, mbo-instellingen, UMC's (Universitair Medische Centra) en onderzoeksinstellingen 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.

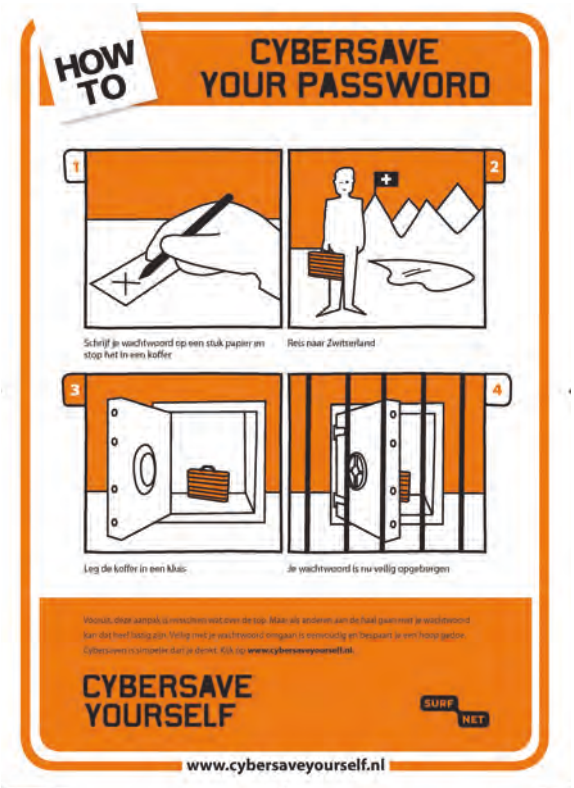
Na het besluit in 2007 om samen aan awareness te werken kwam in 2009 een grote, landelijke campagne uit, gericht op studenten en medewerkers. Deze campagne bevatte een breed scala aan materialen. Instellingen konden de bestanden uit de toolkit gebruiken om zelf materiaal te drukken zoals flyers, crime 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, grootschalige 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: j.j.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 afhangt 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 omscholingstraject voor cybersecurity. Make IT Work is opgericht in 2015 als omscholingstraject vanuit de Hogeschool van Amsterdam en heeft geen commercieël 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 bachelor-opleidingen (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.

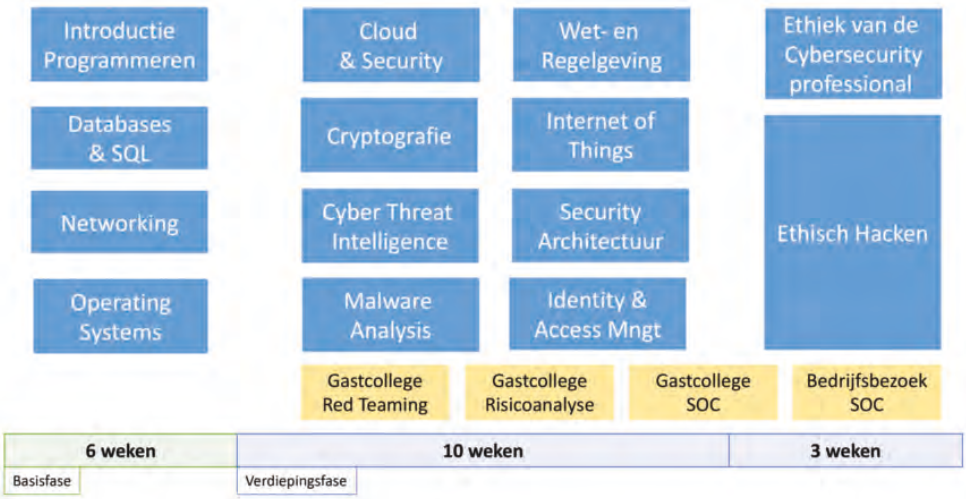
Kandidaten met een intentieverklaring beginnen met een fulltime opleiding van vijf maanden op de Make IT Work campus in Hilversum, gevolgd door zes maanden fulltime werken bij de werkgever. Na succesvolle afronding van het programma ontvangen ze het Make IT Work-certificaat op hbo-niveau en stromen direct 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 voorbereidt 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 fundamenten van cybersecurity worden gelegd met de vakken programmeren, databases, operating systems en netwerken. De basisfase wordt gevolgd door een verdiepingsfase 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 geverifieerd 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 compliancy). AI 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/gastsprekers 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 bassisopleiding, 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 aangemoedigd 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/kennis-centrum/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 onderzoeksdomein. 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 desastreus 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 rechercheur. 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 multidiscipline

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 analysetools 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 rechercheur 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 crucialer voor de digitaal rechercheur. 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-ontvangstsysteem. 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-muisspel; 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 rechercheur 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 instapniveau 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 domeinoverleg (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 verschillende 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 studiejaren 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.

COLUMN MARTIJN

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 Teszelszky is hoger onderwijsmanager I-Doctoraat bij I-Partnerschap, hij is te bereiken via: Kees.Teszelszky@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 terechtkomen 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 kennistoepassing, 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 dienstverlening. 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

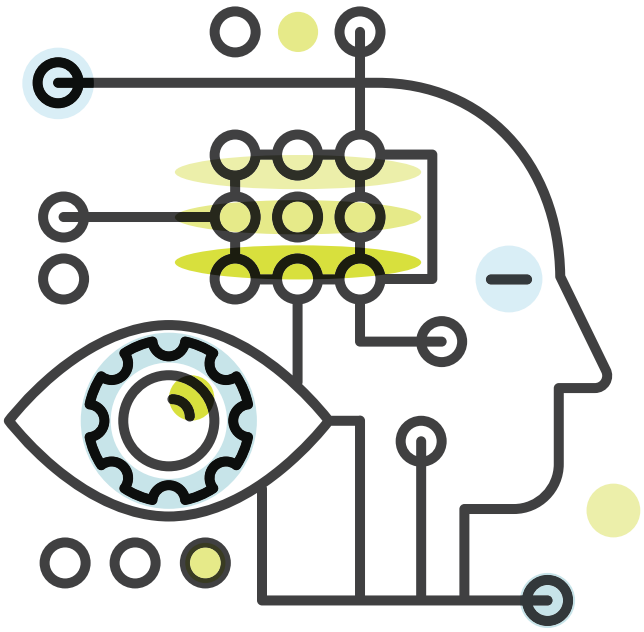
I-Partnerschap helpt die vraagstukken te vertalen naar concrete onderzoeksvragen en -trajecten. Vaak begint dit met een letterlijke vertaling; bij veel instellingen is Engels de formele voertaal van wetenschappers en onderzoekers. Na de vertaling van onderzoeksresultaten naar het Nederlands volgt nog 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 acade-



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.werkenvoornederland.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 groepsopdracht, 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.

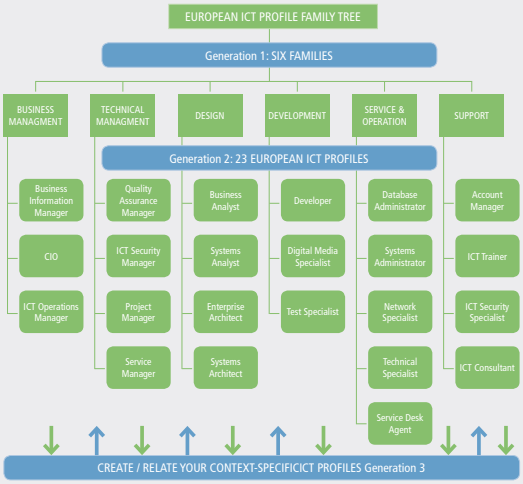
Referenties

(1) https://www.pianoo.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

COLUMN LEX

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.



European ICT profile family tree

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 informatie-beveiliging 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

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:

- het aantal buitenlande studenten aan de technische opleidingen van TU-Eindhoven en TU-Delft bedraagt gemiddeld bijna 50%
- ongeveer 25% van de buitenlandse studenten blijft nog minstens vijf jaar in Nederland werken
- 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 PvIB, 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 PvIB 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 verdedigingslinies tegen globale bedreigingen versterken en ons land veilig en concurrerend houden in het digitale tijdperk.

Organisaties, zoals het PvIB, 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 0de 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 buren 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. Parafraserend: 'Vive l'Europe!'.

PvIB
Platform voor InformatieBeveiliging

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

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.

DNV

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
C|CISO - 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