



Fred van Noord is kwartiermaker cybersecurity hoger onderwijs bij dcypher.
Fred is te bereiken via: f.vannoord@dcypher.nl



Jan Piet Barthel is directeur van dcypher en programmamanager cybersecurity onderzoek bij NWO. Jan Piet is bereikbaar via j.barthel@nwo.nl

Inventarisatie van erkende cybersecurity-opleidingen in Nederland



De afgelopen jaren is in onderzoek bevestigd waar de beroepspraktijk zich al jaren van bewust is: er is een toenemende krapte op de arbeidsmarkt van cybersecurityspecialisten en een tekort aan cybersecuritydocenten om die specialisten op te leiden. Om meer inzicht te krijgen in deze problematiek heeft dcypher in 2018 een inventarisatie uitgevoerd van cybersecurity-opleidingen in het hoger onderwijs.

Het doel voor de korte termijn is het identificeren en beschrijven van erkende opleidingen met een focus op cybersecurity. Het doel voor de langere termijn is het formuleren van aanbevelingen op basis van een verschillenanalyse van de vraag naar goed opgeleide experts en het aanbod van cybersecurity-opleidingen.

Werkwijze

Een klankbordgroep - bestaande uit professionals uit het bedrijfsleven, de overheid en het hoger onderwijs - heeft een sjabloon opgesteld met onderwerpen die relevant zijn voor cybersecurity. Van elk onderwerp kan daarin de onderwijsinspanning (studielast) worden aangegeven. Dit sjabloon is uitgezet in het hoger onderwijs.

De onderwerpen waren onderverdeeld in drie categorieën:

- Organisatie - zoals governance, risicomanagement en informatiebeveiliging, wet- en regelgeving en compliance, business continuity management, review en audit;
- Mens en gedrag - zoals awareness, cybercrime, ethiek;
- Techniek - zoals ICT (computersystemen, netwerken, software, data), ICT-beveiliging, malware-/fraude-/hacking-techniek, cryptografie, monitoring en analyse.

Daarnaast is in het sjabloon de studielast van stage en afstuderen, de keuzeruimte (zoals minoren) en de basiscompetenties (zoals presenteren, vergaderen, onderzoeken, ondernemen enzovoort) ingevuld.

Uitgangspunten bij het in kaart brengen van de opleidingen waren:

- de opleiding is voor een groot deel gericht op cybersecurity;
- de opleiding is opgenomen in het CROHO (1);

- de opleiding leidt op voor de graad Associate degree (2), bachelor of master;
- het totaal van de studielast aan cybersecurity-onderwerpen in de opleiding is minstens 60 ECTS (3).

De volgende opleidingen kwamen in aanmerking:

- opleidingen van het bekostigde hoger onderwijs (hogescholen en universiteiten);
- niet-bekostigde hbo-opleidingen (deze zijn op geen enkele manier door de rijksoverheid gefinancierd);
- niet-bekostigde post-initiële masteropleidingen (4).

In dit onderzoek zijn alleen de opleidingen meegenomen die daaraan hun medewerking hebben verleend. Onderwijsinstellingen die niet konden meedoen, zijn uitgenodigd hun gegevens alsnog aan te leveren om te worden opgenomen in het online overzicht.

Resultaten

Er worden twintig cybersecurity-opleidingen aangeboden door achttien onderwijsinstellingen. Vijftien hiervan zijn voltijd (vijf master, tien bachelor) en vijf deeltijd (drie master, twee bachelor). Drie van de vijf voltijd masteropleidingen zijn tweejarig (120 ECTS) en twee zijn éénjarig (60 ECTS). Bacheloropleidingen worden grotendeels door hogescholen aangeboden (11 van de 12).

	Master	Bachelor	totaal
Voltijd	5	10	15
Deeltijd	3	2	5
totaal	8	12	20

Tabel 1 - Verdeling van voltijd en deeltijd cybersecurity master- en bacheloropleidingen

Om opleidingen te kunnen typeren, is gekeken hoe in het curriculum de verhouding ligt tussen de categorieën:

Organisatie, Mens en gedrag en Techniek. Als één van de deze categorieën een hoger aandeel heeft dan 60% dan is de opleiding in het onderstaande overzicht aangegeven met een kleurmarkering (oker: Organisatie, oranje: Mens en gedrag, blauw: Techniek). Als de studielast grotendeels verdeeld is over twee dan wel drie categorieën dan is deze niet gekleurd.

Techniek	Organisatie	Mens en Gedrag	Combinatie
----------	-------------	----------------	------------

In onderstaande tabellen staan de resultaten per master- en bacheloroopleiding voor voltijd en deeltijd.

Master – Voltijd

Instelling	Opleiding	Organisatie (%)	Mens & Gedrag (%)	Techniek (%)
Vrije Universiteit (VU)	Computer Systems Security	3	-	97
TRU/e (Radboud/TUe)	Cyber Security	14	5	81
Univ. van Amsterdam	Security & Network Engineering	15	13	72
4TU (TU Delft/TU Twente)	Cyber security	16	16	68
Radboud Universiteit	Security & Privacy	67	11	22

Bachelor – Voltijd

Instelling	Opleiding	Organisatie (%)	Mens & Gedrag (%)	Techniek (%)
Hogeschool Amsterdam	Cyber Security	9	-	91
Radboud Universiteit	Cyber Security	6	4	90
Fontys Hogescholen	ICT & Cyber Security	5	5	90
Hogeschool Leiden	Forensische ICT	5	7	87
De Haagse Hogeschool	Cybersecurity Technology	12	2	86
Hogeschool Rotterdam	Technische Informatica	15	7	78
Arnhem & Nijmegen	Infrastructuur en Security Mgt	37	-	63
NHL Stenden	Cybersafety	34	66	-
Fontys Hogescholen	ICT & Management and Security	26	26	47
De Haagse Hogeschool	Information Security Management	56	24	20

Master – Deeltijd

Instelling	Opleiding	Organisatie (%)	Mens & Gedrag (%)	Techniek (%)
De Haagse Hogeschool (CSA)	Cyber Security	12	2	85
Hogeschool (CSA)	Engineering	-	-	-
Univ. Amsterdam	Security & Network Engineering	15	13	72
Univ. Leiden (CSA)	Executive Cyber Security	33	33	33

Bachelor – Deeltijd

Instelling	Opleiding	Organisatie (%)	Mens & Gedrag (%)	Techniek (%)
Fontys Hogescholen	ICT & Management and Security	26	26	47
NOVI	Cyber Security	52	-	48

Tabel 2 - Typering van master- en bacheloroopleidingen in voltijd of deeltijd

In onderstaande tabel staat per typering (Techniek, Organisatie en Mens en gedrag) de totalen naar voltijd versus deeltijd en master versus bachelor.

	Voltijd		Deeltijd		totaal
	master	bachelor	master	bachelor	
Techniek	4	7	2	-	13
Organisatie	1	-	-	-	1
Mens en Gedrag	-	1	-	-	1
Combinatie	-	2	1	2	5
totaal	5	10	3	2	20

Tabel 3 - Het aantal master- en bacheloroopleidingen, onderverdeeld naar typering en voltijd en deeltijd

Dertien opleidingen zijn gericht op Techniek, één opleiding richt zich vooral op Organisatie en één opleiding heeft de focus op Mens en gedrag. Vijf opleidingen bieden een mix van Techniek, Mens en gedrag en/of Organisatie.

Minoren en keuzevakken die zijn genoemd, zijn onder andere: pentesting/hacking, Internet of Things (IoT), big data, vulnerability research, sensor technology, mobile development, cybersecurity technology en cybersafety. Het gedetailleerde en geactualiseerde overzicht is te vinden op de website van dcypher: www.dcypher.nl.

Aantallen afstudeerders

In 2018 hebben bijna 400 studenten hun cybersecurity-opleiding afgesloten met een diploma (165 master, 229 bachelor). Het merendeel hiervan (307 studenten) heeft een technische cybersecurity-opleiding gevolgd (130 master, 177 bachelor). Het werkelijke aantal afgestudeerden is hoger, omdat een enkele opleiding niet in het overzicht staat en een paar opleidingen die wel in het overzicht staan geen uitstroombeggevens hebben aangeleverd. Overigens zal de komende jaren het jaarlijkse aantal afstudeerders naar verwachting verder groeien, omdat er dan nieuwe opleidingen bij zijn gekomen.

Docententekort

Aan opleiders is gevraagd naar het huidige of te verwachten docententekort bij hun opleiding. Ook is er gevraagd om welke specifieke expertise het daarbij gaat. Negen opleidingen geven aan dat het vinden van goede docenten niet eenvoudig is. Reacties variëren van 'enigszins moeilijk' tot 'heel moeilijk' / 'uiterst gecompliceerd'. De expertise waarnaar wordt

“Nederland beschikt over voldoende cybersecuritykennis en -kunde”

gezocht is ‘echte IT’er met kennis en ervaring op netwerk/pentesting/security-vlak en ethical hacking’. Vijf opleiders gaven aan geen problemen te hebben met het vinden van docenten.

Hybride docenten

Een ontwikkeling die verbetering kan brengen ten aanzien van het docententekort, is het hybride docentschap (5). Het geeft voordelen aan onderwijsinstellingen, professionals, studenten én werkgevers:

- het docententekort wordt opgelost;
- professionals kunnen met hun up-to-date inzichten en praktijkervaring bijdragen aan de innovatie van het onderwijs;
- professionals krijgen een afwisselende werkweek met de voldoening van het opleiden van jong talent;
- opleidingen worden aantrekkelijker voor (potentiële) studenten, omdat zij les krijgen van ervaren professionals die de praktijk goed kennen en de verhalen uit de praktijk doorgeven;
- werkgevers krijgen meer gemotiveerde medewerkers, vanwege de voldoening van het leveren van een bijdrage aan het urgente maatschappelijke vraagstuk van digitale veiligheid;
- werkgevers komen via hun medewerkers in een vroeg stadium in aanraking met jong talent.

Hoe verder?

1. Het hierboven geschetste beeld is een momentopname. Veranderingen hierin kunnen vele oorzaken hebben: opleidingen worden toegevoegd, vakken worden toegevoegd, vakken worden ingewisseld voor andere vakken enzovoort. Daarom wordt het beeld door dcypher online aangevuld en geactualiseerd. Geïnteresseerden in de meest recente informatie over een opleiding, wordt aangeraden om het online overzicht te bekijken en daarnaast de websites van opleidingen te raadplegen.

2. PvIB publiceert beroepsprofielen (6) die generieke cybersecurityberoepen beschrijven waarnaar op de arbeidsmarkt veel vraag naar is. Deze beroepsprofielen kunnen de basis zijn voor het ontwikkelen van cybersecurity-opleidingen. De beroepsprofielen kunnen bovendien gebruikt worden in een nog te implementeren certificatiestelsel (7).

Het Dutch cybersecurity platform higher education & research werd in 2016 opgericht. Hiermee hebben vier ministeries (EZK, OCW, J&V en Defensie) samen met NWO (Nederlandse organisatie voor Wetenschappelijk Onderzoek) het initiatief genomen invulling te geven aan één van de doelstellingen in de Nationale Cyber Security Strategie: “Nederland beschikt over voldoende cybersecuritykennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te halen.”

Referenties

- (1) Het Centraal Register Opleidingen Hoger Onderwijs (CROHO) bevat de lijst van alle in Nederland georganiseerde opleidingen voor hoger onderwijs die door het Ministerie van Onderwijs, Cultuur en Wetenschap worden erkend.
- (2) Een associate degree is een tweejarig programma binnen een HBO-bacheloropleiding met een eigen wettelijke graad (Ad). In 2018 bestonden, voor zover bekend, nog geen associate degree (Ad) opleidingen in cybersecurity. De haalbaarheid voor het starten van een Ad-opleiding werd onderzocht door de Hogeschool van Amsterdam en de Hogeschool van Rotterdam.
- (3) European Credit Transfer System; 1 ECTS = 28 uur studiebelasting.
- (4) Een post-initiële masteropleiding is een opleiding voor personen met een hbo- of universitaire diploma en/of met de nodige werkervaring in de beroepspraktijk.
- (5) Een combinatie van een baan voor de klas met een andere baan Zie www.hybridedocent.nl
- (6) www.pvib.nl
- (7) <https://www.pvib.nl/veelgestelde-vragen/certificering>