Marcel Spruit is lector Cyber Security & Safety aan de Haagse Hogeschool.
Hij is te bereiken via m.e.m.spruit@hhs.nl.

Masteropleiding Technische Cybersecurity gebaseerd op PvIB-beroepsprofiel

Er is wereldwijd een toenemend tekort aan goed opgeleide en ervaren informatiebeveiligers. Om daarop te anticiperen zijn voor informatiebeveiliging meer volwaardige opleidingsmogelijkheden nodig. Bovendien is meer harmonisatie van bestaande en nieuwe informatiebeveiligingsopleidingen gewenst om beter door te kunnen stromen naar vervolgopleidingen en deelopleidingen aan andere opleidingsinstellingen te kunnen volgen. In dit artikel delen we de ervaringen met het opzetten van een geaccrediteerde masterstudie in de informatiebeveiliging, gebaseerd op een gestandaardiseerd PvIB-beroepsprofiel en het onderliggende Europese e-Competence Framework.

Organisaties verwerken steeds meer digitale gegevens en zijn daar de afgelopen decennia steeds afhankelijker van geworden. Deze gegevens moeten dan ook goed beschermd worden en dat vraagt om voldoende goed opgeleide en ervaren informatiebeveiligers (1)(2). Daar is echter een toenemend tekort aan (3)(4). Blijkbaar worden er minder informatiebeveiligers opgeleid dan er nodig zijn.

Er zijn veel opleidingsmogelijkheden op het gebied van informatiebeveiliging, maar het betreft vooral relatief korte cursussen. Er zijn beduidend minder mogelijkheden om in het middelbaar of hoger onderwijs een volwaardige studie op het gebied van informatiebeveiliging te volgen. In het hoger onderwijs in Nederland waren er in 2018 slechts twintig studies, deels deeltijd, deels voltijd (5). Bovendien is er weinig consensus over welke competenties informatiebeveiligers zouden moeten bezitten (6). Met name door dat laatste zijn de bestaande opleidingen onderling slecht vergelijkbaar en kost het doorstromen, of het volgen van deelopleidingen aan andere opleidingsinstellingen, grote moeite. Bovendien is het werkgevers niet duidelijk welke afgestudeerden het beste op hun vacatures passen, terwijl afgestudeerden moeilijk kunnen aangeven op welk niveau ze zitten.

In reactie hierop heeft het PvIB, samen met een groep bekende organisaties, gestandaardiseerde beroepsprofielen op het gebied van informatiebeveiliging opgesteld (7)(8). Deze profielen specificeren de competenties die een informatiebeveiliger zou moeten bezitten. Voor het uitwerken daarvan wordt gebruik gemaakt van het Europese e-Competence Framework (9).

Het is de vraag in hoeverre het mogelijk en haalbaar is om een geharmoniseerde opleiding op het gebied van informatiebeveiliging te ontwikkelen, op basis van een gestandaardiseerd PvIB-beroepsprofiel en met gebruikmaking van het onderliggende Europese e-Competence Framework (e-CF).

Beroepsprofielen

Om meer helderheid te krijgen over de eisen die organisaties stellen aan de informatiebeveiligers die ze aan willen nemen, heeft het PvIB, samen met een groep bekende organisaties, het project Qualification of Information Security (QIS) opgezet. Dit project heeft gewerkt aan het formuleren van een beperkt aantal generieke beroepen binnen het domein informatiebeveiliging. Ieder van deze generieke beroepen is beschreven in een gestandaardiseerd beroepsprofiel (8). Een beroepsprofiel beschrijft de competenties die een informatiebeveiliger zou moeten bezitten. Een competentie is het vermogen om bepaalde kennis en vaardigheden toe te passen om taken en functies succesvol uit te voeren in een bepaalde rol of positie (9)(10)(11)(12). Een competentie kan uitgewerkt worden in kennis- en vaardigheidselementen. De e-competenties zijn uitgewerkt in e-CF, versie 3.0 (9). De algemene competenties heeft de PvIB-werkgroep Kwalificatie van informatiebeveiligers uitgewerkt in kennis- en vaardigheidselementen.

Competenties, alsook de kennis- en vaardigheidselementen, kunnen op een competentieniveau, lopend van 1 tot 5, beheerst worden. De niveaus zijn door het PvIB beschreven (8). Kort door de bocht kunnen we stellen dat de niveaus globaal overeenkomen met een bepaald denk- en werkniveau, te weten:

1. basisniveau;
2. mbo-niveau;
3. hbo-niveau;
4. masterniveau;
5. phD-niveau.

Door de betrokkenheid van een groot aantal vertegenwoordigers van allerlei sectoren en geledingen en uitgebreide reviewrondes kunnen de PvIB-beroepsprofielen rekenen op een breed draagvlak bij informatiebeveiligers, werkgevers in de publieke en private sector en onderwijsinstellingen. De beroepsprofielen kunnen gebruikt worden voor een nog te realiseren systeem voor certificatie en registratie van informatiebeveiligers.

Masteropleiding

De hiervoor genoemde gestandaardiseerde beroepsprofielen bevatten competenties die verder zijn uitgewerkt in kennis- en vaardigheidselementen. Elke beoefenaar van een in een beroepsprofiel gespecificeerd beroep moet de in het profiel genoemde competenties beheersen voor het uitoefenen van zijn of haar werk. Dit betekent dat de betreffende persoon de vereiste competenties moet kunnen verwerven, bijvoorbeeld door het volgen van een daarop gerichte opleiding.

Een informatiebeveiligingsopleiding kan worden ontworpen op basis van de competenties die in een informatiebeveiligingsprofiel worden vermeld. De daarin genoemde e-competenties zijn in het e-CF uitgewerkt in kennis- en

vaardigheidselementen. De algemene competenties heeft de PvIB-werkgroep Kwalificatie van informatiebeveiligers uitgewerkt in kennis- en vaardigheidselementen. Het detailniveau van de kennis- en vaardigheidselementen is een compromis tussen de nauwkeurigheid die vereist is voor standaardisatie en de flexibiliteit die in opleidingen voor de betreffende kennis en vaardigheden nodig is.

De kennis- en vaardigheidselementen die zo zijn bepaald, kunnen direct worden gebruikt als leerdoelen voor een opleiding. Op basis van de gespecificeerde kennis- en vaardigheidselementen kunnen docenten hun lesmateriaal ontwikkelen.

Dat deze aanpak werkt, konden we aantonen met de ontwikkeling van een technisch georiënteerde Master of Science-opleiding op het gebied van informatiebeveiliging. Deze masteropleiding werd ontwikkeld voor de Cyber Security Academy en de Haagse Hogeschool. Beide instellingen ontvangen al geruime tijd signalen dat een technisch georiënteerde masteropleiding op het gebied van informatiebeveiliging c.q. cybersecurity in de Haagse regio zeer welkom zou zijn. De nieuwe opleiding is tweejarig en parttime (60 ECTS) en is Master Cyber Security Engineering gedoopt. De opleiding is in 2018 door de NVAO geaccrediteerd en is 1 februari 2019 gestart. Als toelatingseis geldt een bachelor in informatica, informatiebeveiliging of cybersecurity, plus minimaal twee jaar relevante werkervaring.

Voor het ontwikkelen van de opleiding hebben we eerst het meest relevante beroepsprofiel gekozen, namelijk ICT-security specialist 3 (8). De volgende competenties zijn in dit profiel gespecificeerd:

- A7: volgen van technologische ontwikkelingen, competentieniveau 4;
- B4: oplossingen implementeren, competentieniveau 4;
- E3: risicomanagement, competentieniveau 3;
- E8: informatiebeveiligingsmanagement, competentieniveau 3;
- G3: communicatie en overtuigingskracht, competentieniveau 2;
- G4: onderzoek, competentieniveau 4;
- G7: analytisch vermogen, competentieniveau 4;
- G8: integriteit, competentieniveau 2.

Dat de competentie 'integriteit' op niveau 2 staat, betekent niet dat de beroepsbeoefenaar beperkt integer hoeft te zijn, maar dat deze 'slechts' de uitgangspunten en regels voor integer gedrag kent en kan verklaren en daarnaar kan handelen.

Elk van de gespecificeerde competenties is verder uitgewerkt in kennis- en vaardigheidselementen. De e-competenties zijn met behulp van het e-CF uitgewerkt in kennis- en vaardigheidselementen. We gebruikten hiervoor versie 3.0. Deze versie hebben we inhoudelijk enigszins aan moeten passen, omdat we inconsistenties en onvolledigheden tegenkwamen en deze vervolgens als voorschrijvende standaard gebruikt. De algemene competenties zijn met behulp van de uitwerking van de PvIB-werkgroep Kwalificatie van informatiebeveiligers uitgewerkt in kennis- en vaardigheidselementen. Deze uitwerking kon onverkort gebruikt worden.

De kennis- en vaardigheidselementen zijn vervolgens gedefinieerd als de leerdoelen. Dit resulteerde in een complete lijst met leerdoelen voor de opleiding. Vanzelfsprekend staat het elke opleidingsinstelling vrij om extra leerdoelen toe te voegen of bepaalde kennis en vaardigheden verder uit te diepen dan nodig is volgens het beroepsprofiel. Zo hebben we in deze opleiding bijvoorbeeld de onderzoekscomponent extra zwaar ingevuld en extra tijd ingeruimd voor het toepassen van kennis en vaardigheden op het gebied van cybersecuritytechniek in specifieke typen organisaties.

De tweede stap was het ontwerpen van een opleidingsstructuur. Daarbij is gekozen voor een indeling in drie semesters met ieder drie modules, en een vierde en laatste semester voor het thesisonderzoek. In elke module loopt een individueel project of een groepsproject, zodat er voldoende ruimte is om aan vaardigheden te werken. De inhoud van de semesters is in het kort:

1. Conceptualisatie van cyberbeveiliging. Dit semester is een beknopte inleiding in allerlei relevante aspecten, zoals menselijke factor, management, wetgeving en ethiek. Bovendien worden de onderdelen ICT en ICT-beveiliging opgefrist en op masterniveau gebracht.
2. Bouwstenen voor cyberbeveiliging. In dit semester duiken de studenten diep in de techniek van de ICT-beveiliging.
3. Cyberbeveiliging in sectoren en trends. In dit semester wordt de kennis uit de vorige semesters toegepast op specifieke typen organisaties. Verder worden de nieuwste technische trends op het gebied van ICT-beveiliging behandeld.

Op het gebied van informatiebeveiliging zijn meer volwaardige geharmoniseerde opleidingsmogelijkheden nodig

4. Onderzoek. Elke student moet individueel een wetenschappelijk onderzoeksproject doen en een masterscriptie schrijven.

De derde stap was het verdelen van de leerdoelen over de modules, zodanig dat alle modules (behalve de thesismodule) ongeveer dezelfde omvang zouden hebben en iedere module een logisch en samenhangend geheel zou vormen.

Ten slotte konden voor iedere module de docenten op basis van de aan hun toegewezen leerdoelen hun lesmateriaal ontwikkelen.

De op deze manier ontwikkelde opleiding voldoet qua competenties (kennis en vaardigheden) volledig aan het onderliggende PvIB-beroepsprofiel. Ook andere onderwijsinstellingen kunnen de PvIB-beroepsprofielen gebruiken om nieuwe opleidingen te ontwikkelen of bestaande opleidingen aan te passen. We zijn niet bang voor een `eenheidsworst', omdat opleidingsinstellingen binnen de opleiding voldoende ruimte hebben om leerdoelen toe te voegen, binnen de leerdoelen accenten te plaatsen en te werken met verschillende onderwijsvormen. Maar dankzij de gemeenschappelijke basis zijn verschillende opleidingen op basis van hetzelfde beroepsprofiel gelijkwaardig en kunnen ze effectiever worden geaccrediteerd. Bovendien kunnen vervolgopleidingen makkelijker aansluitend worden gemaakt en zijn deelopleidingen van andere opleidingsinstellingen (bijvoorbeeld minoren) makkelijker in te passen.

Conclusie

Op het gebied van informatiebeveiliging zijn meer volwaardige geharmoniseerde opleidingsmogelijkheden nodig. In dit artikel hebben we aan de hand van de ontwikkeling van de Master Cyber Security Engineering, op basis van het beroepsprofiel ICT-securityspecialist 3, laten zien dat het mogelijk en haalbaar is om een geaccrediteerde informatiebeveiligingsopleiding te ontwikkelen op basis van een PvIB-beroepsprofiel. Dit resulteert in een opleiding die qua competenties volledig voldoet aan het onderliggende beroepsprofiel en daarmee geharmoniseerd is met andere opleidingen die op hetzelfde beroepsprofiel gebaseerd zijn.

We hebben geconstateerd dat standaard competentieuitwerkingen zoals het e-CF, zij het inhoudelijk enigszins aangepast en als voorschrijvende standaard gebruikt, en de uitwerking van de PvIB-werkgroep Kwalificatie van informatiebeveiligers goed bruikbaar zijn voor het uitwerken van competenties tot leerdoelen.

Referenties

(1) Munnichs, G., Kouw, M. & Kool, L. (2017). Een nooit gelopen race. Rathenau Instituut.
(2) Smith, S.S. (2017). Internet Crime Report. FBI.
(3) Van Lakerveld, J.A., e.a. (2014). Arbeidsmarkt voor Cyber Security Professionals. PLATO.
(4) Morgan, S. (2017). Cybersecurity Job Reports, 2017 Edition. Herjavec.
(5) Van Noord, F. & Barthel, J.P. (2019). Inventarisatie van erkende cybersecurityopleidingen in Nederland. Informatiebeveiliging, 3.
(6) Spruit, M. & Van Noord, F. (2011). Onderzoek naar kwalificatie en certificatie van informatiebeveiligers. CPNI.NL.
(7) Van Noord, F. & Spruit, M. (2014). Informatiebeveiligers definiëren hun kwalificatiestelsel op basis van e-CF. Informatiebeveiliging, 4, 24-26.
(8) Spruit M. & Van Noord, F. (2017). Beroepsprofielen Informatiebeveiliging 2.0. PvIB.
(9) CEN (2014). CEN Workshop Agreement CWA 16234:2014 Part 1, European e-Competence Framework 3.0 - Part 1: A common European Framework for ICT Professionals in all industry sectors. CEN.
(10) Delamare Le Deist, F. & Winterton, J. (2005). What is competence? Human Resource Development International, 1, 27-46.
(11) M. Mulder, T. Weigel & K. Collins, "The concept of competence concept in the development of vocational education and training in selected EU member states. A critical analysis", Journal of Vocational Education and Training, nr. 1, 2006, pag. 65-85.
(12) Winterton, J., Delamare Le Deist, F. & Stringfellow, E. (2006). Typology of knowledge, skills and competences: clarification of the concept and prototype, Office for Official Publications of the European Communities.