BACHELOR IN DE CYBERSECURITY

HOGESCHOOL WEST-VLAANDEREN

TOETS NIEUWE OPLEIDING OP MAAT VAN DE EIGEN REGIE • BEOORDELINGSRAPPORT

23 APRIL 2024

RAYMONDA VERDYCK (VOORZITTER) • ERIK POLL, MOSSHIN ASSABAN, ROAN MERENS (COMMISSIELEDEN) • TINE SWAENEPOEL (SECRETARIS) • ILS AERTS (PROCESCOÖRDINATOR)

Inhoud

1 Abstract

De beoordelingscommissie onderzocht de potentiële kwaliteit van de bachelor in cybersecurity aan Hogeschool West-Vlaanderen (Howest) en beoordeelde die als voldoende. Het advies van de beoordelingscommissie aan de NVAO is dan ook positief.

Deze bacheloropleiding van 180 studiepunten maakt deel uit van de opleidingcluster IT (Information Technology). Andere opleidingen in die cluster zijn de bacheloropleiding Toegepaste Informatica (met een keuzetraject Development & Security), de graduaatsopleidingen Programmeren en Systeem- en Netwerkbeheer, en de postgraduaatsopleidingen Data Protection Officer, Advanced Cybersecurity en Industrial Security.

De commissie baseerde dit oordeel op het dossier van de opleiding en op gesprekken met de opleiding.

Op basis van het dossier stelde de commissie heel wat sterke punten vast. De nood aan een aparte bachelor in de cybersecurity is duidelijk en de bachelor komt tegemoet aan de noden van het werkveld. De aandacht voor heroriëntering van studenten door de link te houden met de opleiding toegepaste informatica met specialisatie in de cybersecurity is positief. Er is voldoende expertise in huis om de opleiding te dragen en de contacten met het werkveld laten toe dit aan te vullen met gastcolleges. De commissie voelde ook een grote gedrevenheid en passie bij de opleidingsverstrekkers, die met recht trots zijn op de aanwezige infrastructuur. Er is een duidelijke betrokkenheid van het veld, dat input geeft vanuit verschillende hoeken.

Over een aantal punten ging de beoordelingscommissie met de opleiding in gesprek, o.a. de verhouding van de bachelor in de cybersecurity tot de bachelor toegepaste informatica met specialisatie cybersecurity, de concrete uitwerking van het programma, de personeelsinzet, de infrastructuur en de toetsing van het eindniveau. De gesprekken hierover waren verhelderend voor de commissieleden.

De commissieleden formuleerden een aantal aanbevelingen voor de nieuwe opleiding.

- De leerresultaten zijn erg uitgebreid en versnipperd. Breng ze duidelijker en eenvoudiger in kaart door ze te clusteren, in functie van studeerbaarheid en helderheid voor studenten en docenten.
- Heb voldoende aandacht voor ondersteuning van en feedback aan studenten, zeker met het oog op de voorziene groei van het aantal studenten.
- Werk een plan uit om in de toekomst voldoende docenten te kunnen aantrekken om de voorziene groei op te vangen en de studenten goed te kunnen ondersteunen.
- Heb aandacht voor de continue professionalisering van de huidige docenten.
- Zorg dat ook voor het werkveld voldoende duidelijk is welke leerresultaten tijdens een stage aan bod moeten komen.
- Stem voor de toetsing van het eindniveau de stage duidelijk af op het securityproject.

2 Rapportage van het onderzoek van de commissie

2.1 Inhoudelijke verkenning: de eerste indrukken van de commissie

De leden van de beoordelingscommissie lazen met aandacht het dossier “Bachelor in de Cybersecurity – Aanvraag Toets Nieuwe Opleiding” van Howest. Elk lid noteerde individueel de sterke punten van de opleiding en enkele aandachtspunten en vragen. Deze eerste indrukken vormden het uitgangspunt voor een online voorbereidend overleg op donderdag 7 december 2023. Dit gesprek werd live verdergezet op maandag 11 december 2023. De structuur van het dossier diende hierbij als leidraad. Tussen 22 maart en 16 april 2024 heeft de commissie een bijkomend oefening gedaan om te kijken of de in tussentijd gevalideerde domeinspecifieke leerresultaten (DLR) geen fundamentele aanpassingen vereisen van het curriculum en leerdoelen die voor deze procedure door de opleiding werden gebruikt.

De commissie heeft na analyse vastgesteld dat de domeinen en technieken die beschreven zijn in het opleidingsprogramma gangbaar en relevant zijn en de vooropgestelde leerdoelen van de opleiding aan de gevalideerde DLR beantwoorden. Dit rapport blijft daarom valabel voor de beoordeling van de opleiding.

2.1.1 De sterke punten van de opleiding

Een van de sterke punten van de opleiding is dat die inspeelt op een **maatschappelijke nood** en tot stand kwam **in samenwerking met het werkveld**. Die samenwerking situeert zich zowel in de voorbereiding van het dossier als in de opleiding zelf, waar bv. gastdocenten een plaats krijgen en waar veel nadruk ligt op praktijkgericht leren. De opleiding lijkt daardoor nauw afgestemd te zijn op de behoeften van de sector.

De commissieleden appreciëren ook de aandacht voor **referentiekaders** uit het werkveld om de opleiding vorm te geven.

De commissieleden zien een **gevarieerd programma** met **verschillende vormen van didactische aanpak** en een balans tussen theorie en praktijk. Het programma werkt meer en meer toe naar verdieping en er is volgtijdelijkheid ingebouwd. De band met het werkveld is zichtbaar in het hele programma.

Er is aandacht voor de **studeerbaarheid** van de opleiding. De benadering is studentgericht, waarbij rekening gehouden wordt met onderwijsbehoeften en de mogelijkheid geboden wordt om faciliteiten te vragen. De opleiding houdt ook rekening met de beginkenmerken van de diverse instroom.

2.1.2 De onderzoeksvragen

Na het doornemen van het dossier en de voorbereidende overlegmomenten formuleerden de commissieleden een aantal onderzoeksvragen. Dat zijn elementen uit het dossier die voor hen onvoldoende duidelijk waren en die zij in dialoog met de instelling wilden uitklaren.

Onderzoeksvraag 1: de verhouding van de bachelor in de cybersecurity tot de bachelor toegepaste informatica met specialisatie cybersecurity
De commissieleden zien dat de opleiding inspeelt op een maatschappelijke nood en een vraag vanuit het werkveld. Maar waar liggen de verschillen met de bachelor toegepaste informatica met specialisatie cybersecurity? Beantwoordt dit aan de noden van (toekomstige) studenten? Hoe ziet men de wisselwerking tussen deze nieuwe bacheloropleiding en toegepaste informatica met specialisatie?

Onderzoeksvraag 2: de concrete uitwerking van het programma
De commissieleden waarderen de verschillende vormen van didactische aanpak, de heldere opbouw die naar verdieping toewerkt, de balans tussen theorie en praktijk. Ook de aandacht voor interdisciplinariteit en verschillende referentiekaders ervaren zij als positief.

De commissieleden zouden graag meer inzicht krijgen in de concrete uitwerking van de opleidingsonderdelen: hoe verhouden die zich tot de OLR, hoe worden de werkvormen concreet ingevuld, hoe vertaalt zich dit naar een toetsbeleid? De commissieleden vragen zich ook af hoe de opleiding om zal gaan met de verschillende achtergronden van de studenten die instromen en hoe de studeerbaarheid bewaakt wordt.

Onderzoeksvraag 3: de personeelsinzet
De commissieleden zien een duidelijke structuur voor personeelsinzet, met heldere rollen en aandacht voor een verscheidenheid aan competenties, professionalisering en diversiteit. Dat neemt niet weg dat de commissieleden zich afvragen hoe de opleiding van plan is de vele mensen die nodig zijn voor deze opleiding aan te trekken, gelet op de krappe arbeidsmarkt en de voorziene studentenaantallen? Is daar een plan van aanpak voor? En hoe zal men ervoor zorgen dat de docenten de snelle evoluties binnen de cybersecurity blijven volgen? Hoe bereidt men gastdocenten uit het werkveld voor op lesgeven in een bacheloropleiding?

Onderzoeksvraag 4: de infrastructuur
Een effectieve opleiding cybersecurity vraagt labo's en simulatieomgevingen om studenten voor te bereiden op real-life scenario's. Dat biedt studenten de mogelijkheid om hun vaardigheden in een realistische maar gecontroleerde setting te oefenen en te verfijnen. In welke mate kan de opleiding hierover beschikken? Welke soorten labo's en simulatieomgevingen zijn er? Zijn de nieuwste technologieën en softwaretools beschikbaar? Is deze infrastructuur toegankelijk voor studenten, ook als de groep groter wordt?

Onderzoeksvraag 5: de beoordeling van het eindniveau
De commissieleden lazen in het dossier dat vier opleidingsonderdelen (OLOD's) samen het eindniveau van een student beoordelen. Het OLOD internship is een blokstage die loopt over het volledige zesde semester. De commissieleden zouden graag meer inzicht krijgen in hoe die stage georganiseerd wordt. Hoe kiest een student een stageplaats? Hoe weten de stagementoren welke leerdoelen aan bod moeten komen? Hoe gebeurt de beoordeling van een stage? Hoe zorgt de opleiding ervoor dat over de OLOD's heen alle leerdoelen getoetst worden?

2.2 Dialoog met de instelling over de onderzoeksvragen van de commissie

2.2.1 Onderzoeksvraag 1: de verhouding van de bachelor in de cybersecurity tot de bachelor toegepaste informatica met specialisatie cybersecurity

De commissieleden zien heel duidelijk dat er in het werkveld nood is aan opgeleide professionals in de cybersecurity. Ze vragen zich evenwel af hoe de opleiding de verhouding tussen deze nieuwe bacheloropleiding en de bachelor in de toegepaste informatica met specialisatie cybersecurity ziet en welke wisselwerking mogelijk is tussen beide opleidingen.

Uit het gesprek met het instellingsbestuur blijkt dat de opleiding oordeelt dat de 60 studiepunten die besteed kunnen worden aan een keuzetraject niet meer volstaan om de professionals af te leveren die het werkveld nodig heeft.

Voor cybersecurity is de breedte van de technologische basis belangrijk, maar er moet voldoende verdiept kunnen worden richting cybersecurity en 60 studiepunten is daarvoor te weinig. In het keuzetraject is bv. threat intelligence een hoofdstuk binnen een opleidingsonderdeel, terwijl het in de nieuwe bachelor een volledig opleidingsonderdeel wordt. Er is echt nood aan meer uitdieping. De expertise daarvoor is er, door de stevig uitgebouwde onderzoekspoot cybersecurity.

Men stelt ook vast dat de afgestudeerden uit het keuzetraject beperkt inzetbaar zijn op de arbeidsmarkt. Die arbeidsmarkt is sterk geëvolueerd, er zijn meer rollen in het veld dan waar de afstudeerrichting op kan voorbereiden. De werkveldpartners geven aan dat cybersecurity over meer gaat dan enkel pentesting.

Een bachelor in de cybersecurity moet volgens de werkveldpartners een aantal begrippen kennen, weten waarvoor ze dienen, weten hoe je dingen kan en moet schrijven. Hij/zij moet het systeem kennen, kunnen nadenken over security en begrijpen wat cybersecurity operations inhoudt. Dit is aan bod gekomen tijdens de werkveldcommissies. Door de evoluties in de cybersecurity is het niet meer haalbaar voldoende breed inzetbare professionals af te leveren op basis van een keuzetraject van 60 studiepunten, al blijft dat keuzetraject wel waardevol.

Wie in het werkveld terechtkomt, moet een basisnotie hebben van heel veel verschillende aspecten van cybersecurity en zich op de werkvloer verder specialiseren, vanuit de brede context. Dat geldt in het algemeen voor alles wat informatica betreft. De werkveldpartners zijn ervan overtuigd dat de inwerktijd korter zal zijn bij afgestudeerde bachelors in de cybersecurity.

Sowieso is levenslang leren belangrijk. Ook wie afgestudeerd is moet voortdurend bij willen en kunnen leren. Daarom worden studenten toegeleid naar zelfregulerend en zelfsturend gedrag. Studenten moeten, vertrekkend van de kennis vanuit de opleiding, weten hoe ze de kennis die ze nodig hebben kunnen verwerven en verdiepen.

De opleiding heeft ook bij studenten in het eerste jaar toegepaste informatica en bij studiekiezers de nood aan een aparte opleiding cybersecurity bevraagd. Daaruit blijkt dat er twee groepen zijn: studenten die specifiek interesse hebben in een bachelor in de cybersecurity en studenten die interesse hebben in programmeren en software development, aangevuld met een luik cybersecurity.

Dit blijkt ook uit de gesprekken met studenten. Specifiek over cybersecurity verwoorden zij de nood om meer in de diepte te kunnen gaan. Het keuzetraject heeft een focus op red teaming, terwijl ook blue teaming aan bod zou moeten komen. De studenten vinden een basis van development belangrijk en zien ook de nood om alles rond informatica te leren, maar minder in de diepte, zodat meer aandacht besteed kan worden aan specifieke opleidingsonderdelen cybersecurity.

Door de opbouw van het programma wil de opleiding tegelijk inzetten op heroriëntering. Momenteel ziet men dat sommige studenten toegepaste informatica het goed doen in het keuzetraject cybersecurity, maar niet voldoende scoren voor programmeren. Die zou men kunnen toeleiden naar de nieuwe bachelor. Ook het omgekeerde is mogelijk. In de bachelor in de cybersecurity wordt o.a. een basis in het programmeren gegeven, waardoor heroriëntering naar de bachelor in de toegepaste informatica vanuit de bachelor in de cybersecurity haalbaar is.

Dit wordt vergemakkelijkt door de structuur, met een gezamenlijke opleidingsmanager aan het hoofd van een cluster met graduaatsopleidingen en bacheloropleidingen. Dit maakt uitwisseling en samenwerking mogelijk. Men wil de opleidingen helder positioneren ten opzichte van elkaar en de juiste student op de juiste plaats krijgen.

2.2.2 Onderzoeksvraag 2: de concrete uitwerking van het programma

De commissieleden waarderen de veelheid aan bekende referentiekaders, zoals NIST en CyBOK en de 12 rollen zoals gedefinieerd door ENISA. Ze vragen hoe die zich verhouden tot de OLR, het programma en de opleidingsonderdelen. Hoe gebeurde de mapping? De gesprekspartners lichten toe dat er voor elk opleidingsonderdeel een koppeling gemaakt is met de leerdoelen en de DLR. Ook de referentiekaders kregen in die mapping een plaats. Zo wilde men ervoor zorgen dat alles aan bod komt en dat niks zonder reden weggelaten wordt.

De commissieleden bevragen of dit duidelijk is voor de studenten. Hoe maakt men hen vertrouwd met de OLR? De gesprekspartners leggen uit dat sinds het dossier ingediend werd, de mappings nog aangepast zijn. Ook de studiefiches bevatten koppelingen met de

gedetailleerde leerresultaten. De studenten geven aan dat aan het begin van elk semester duidelijk gezegd wordt wat de inhoud van en verwachtingen voor elk vak zijn.

De commissieleden merken op dat mapping tussen leerresultaten, referentiekaders en opleidingsonderdelen heel erg gedetailleerd en uitgebreid is en daardoor versnipperd. Ze raden aan om dit duidelijker en eenvoudiger in kaart te brengen. Dit kan bv. door leerresultaten te clusteren. Dit is ook positief voor de studeerbaarheid en helderheid, zowel voor studenten als voor docenten. Het is ook belangrijk dat alles duidelijk weergegeven wordt in de studiefiches.

Om de diversiteit van de instromende studenten op te vangen, wordt geen voorkennis verondersteld en start men met de basis. In het eerste semester worden de fundamentals van programmeren en netwerken uitgelegd. De flow van de modules is logisch opgebouwd. Men heeft daar ervaring mee in de bachelor toegepaste informatica. Uit de gesprekken met de studenten blijkt dat zij het niet als een noodzaak ervaren een vooropleiding met informatica te hebben voor de bachelor in de toegepaste informatica. Er zijn instapcursussen en ze weten ook waar ze in de loop van het academiejaar kunnen aankloppen als er dingen niet duidelijk zijn.

Binnen Howest wordt steeds gewerkt op basis van leerlijnen. De leerdoelen sluiten daarbij aan en dit wordt vertaald in het programma. Er wordt toegewerkt naar afsluitende en geïntegreerde modules in de stages.

Een heterogene instroom laat ook toe dat studenten leren van elkaar. Sommigen zijn communicatief sterker, anderen hebben een stevigere technische basis. Dit sluit ook aan bij de noden van het werkveld, waar in team kunnen werken erg belangrijk is.

De gesprekspartners geven aan dat studeerbaarheid algemeen binnen Howest een aandachtpunt is. De docenten kunnen hier een opleiding voor volgen. Daarnaast wordt alles duidelijk aangegeven in de studiefiches, van leerdoelen tot cursusmateriaal en manier van toetsen. De hogeschool ontwikkelde een kader voor toetsbeleid en een toetsscan. Dat laat lectoren toe om na te gaan of hun toetsmateriaal transparant, betrouwbaar, valide, authentiek en gericht op het autonoom handelen is. Verder wordt elke opdracht ter evaluatie van studenten steeds ook bekeken door collega's die geen deel uitmaken van het OLOD-team. Dat meerogenprincipe wordt ook in de bachelor toegepaste informatica gehanteerd en blijkt een meerwaarde.

De studenten merken op dat feedback krijgen op bv. ingediende taken niet altijd vlot verloopt. Punten op labo's worden soms pas laat gegeven, als het over grote opdrachten gaat soms pas samen met de punten van een examen. Soms is de feedback nodig om verder te kunnen gaan met een project. De commissieleden vinden dit een aandachtspunt. Het is belangrijk dat studenten voldoende snel feedback krijgen. Ze raden de opleiding aan hiermee aan de slag te gaan, zeker gelet op de beoogde toename van het aantal studenten.

Een ander aspect van studeerbaarheid is de combineerbaarheid van specifieke OLOD's. Dat wordt globaal bekeken. De gesprekspartners zijn ook van mening dat de verzelfstandiging van het traject cybersecurity in deze bacheloropleiding de studeerbaarheid ten goede zal komen voor studenten die specifiek voor cybersecurity kiezen. Zij kunnen meer verdiepen en krijgen een basis van bv. developmentvakken waar ze misschien minder aanleg voor hebben.

Verder lichten de gesprekspartners toe dat studeerbaarheid ook gaat over de student die het eigen studieproces in handen kan nemen. De studiecoach legt bij eerstejaarsstudenten de focus op de overstap van het secundair naar het hoger onderwijs. Ook deeltijdse evaluaties worden met de studenten besproken. Als die slecht waren, bekijkt men hoe een student zich voorbereidde en wat anders aangepakt kan worden.

Het programma is zo opgebouwd dat er een evolutie is van geleid werken in semester 1, met zeer concrete instructies, richting meer zelfsturing en autonomie. Dit gaat samen met een veranderende rol van de docent die in het begin de student dichtbij houdt en evolueert naar een coachende rol. Dit komt aan bod in het professionaliseringstraject voor docenten, in bv. een workshop rond feedback geven aan studenten. Verder worden zeker in het eerste jaar monitoraten gegeven door de docenten.

2.2.3 Onderzoeksvraag 3: de personeelsinzet

De commissieleden verwijzen naar de uitdagingen als het gaat over personeelsinzet: heeft de opleiding een plan van aanpak om op een krappe arbeidsmarkt de juiste profielen aan te trekken om de bachelor in de cybersecurity uit te kunnen bouwen. De opleiding zet bovendien sterk in op begeleiding van de studenten. Daar is capaciteit voor nodig.

De gesprekspartners geven aan dat dit inderdaad een uitdaging is. Zowel in het veld IT als in het onderwijs in het algemeen is er een war on talent. Het eerste jaar van de nieuwe opleiding is haalbaar met de huidige bezetting. Zowel doordat het keuzetraject bestaat als door de lopende onderzoeksprojecten in de cybersecurity, is er al heel veel expertise en ervaring in huis.

Voor de verdere uitrol van de nieuwe bachelor is er dus nog tijd om goede profielen aan te trekken, in verschillende functies, bv. voltijds docent of gastlector. Zeker het betrekken van het werkveld is een deel van de oplossing. Ook in de afstudeerrichting cybersecurity binnen de bachelor in de toegepaste informatica kan men een beroep doen op gastlectoren. Om hen te ondersteunen is door de dienst onderwijs een OLOD ontwikkeld, die gastlectoren een basis geeft in didactiek voor het hoger onderwijs. Uit de gesprekken met de studenten blijkt dat zij deze gastlectoren uit het werkveld als een meerwaarde ervaren.

De gesprekspartners merken op dat in het programma zoals dat uitgetekend is, er geen enkel opleidingsonderdeel niet gerealiseerd kan worden met de huidige staf. Uiteraard is men zich ervan bewust dat als een van de huidige docenten ingezet wordt binnen de nieuwe opleiding, er een leemte ontstaat bij een andere opleiding. Maar doordat men de personeelsinzet bekijkt op het niveau van de cluster, verbreedt men de profielen die kunnen instromen.

De gesprekspartners geven aan dat ook enkele docenten in voorbereiding op deze nieuwe bachelor zelf een master in de cybersecurity aan het volgen zijn. Dit heeft aan de ene kant als doel om het personeel te kunnen behouden en aan de andere kant om zeker ook de onderwijskundige kennis te verankeren.

De leden van de commissie vragen of het de bedoeling is om blijvend een beroep te doen op externen. Dat is zeker niet de expliciete keuze binnen de opleiding, reageren de gesprekspartners. Sowieso zijn aan elk OLOD docenten in huis gekoppeld. Sommigen geven al een vergelijkbaar OLOD in de bachelor in de toegepaste informatica, anderen bereiden zich voor op de nieuwe opdracht. In die context wil men externen betrekken, zonder zich voor een module volledig afhankelijk te maken van externen. Dat vinden de gesprekspartners vanuit de opleiding een te groot risico. Ze willen voor bv. examens of de opvolging van het leerplatform liever een beroep doen op de eigen docenten.

De commissieleden zien duidelijk dat er voldoende mensen aan boord zijn om het eerste jaar vorm te kunnen geven, maar raden aan om een plan uit te werken om in de toekomst voldoende docenten te kunnen aantrekken, dat ook rekening houdt met de voorziene groei. Het blijft belangrijk de studenten goed op te vangen en te ondersteunen en daar zijn voldoende mensen voor nodig. Uit de gesprekken met studenten bleek dat het niet altijd lukt om voldoende snel feedback te geven over o.a. opdrachten en labo's.

De commissieleden vragen op welke manier men de docenten in staat kan stellen de snelle evoluties in de cybersecurity te blijven volgen.

De gesprekspartners geven aan dat er een onderzoeksgroep Security en Privacy is. Deze onderzoekers nemen een stuk lesopdracht op en brengen zo de inzichten uit het onderzoek binnen in de opleiding. De docenten doen ook mee aan workshops om de vinger aan de pols te houden, zoals bv. een NATO-oefening. Verder zal men voor bepaalde OLOD's extern ontwikkeld studiemateriaal gebruiken, dat is ook een manier om nieuwe trends binnen te halen.

Sowieso is professionalisering van de docenten belangrijk. Nieuwe docenten krijgen tijd om in hun rol te groeien. Ze draaien vaak eerst mee als coach, pas na even aan boord te zijn krijgen ze eindverantwoordelijkheid voor opleidingsonderdelen. Dit laat hen toe eigen accenten te leggen. Bij de selectie van nieuwe collega's kijkt men ook sterk naar matchende personal skills, niet enkel naar inhoudelijke kennis.

Structureel voorziet men ruimte in de roosters van docenten voor interne professionalisering. Voor de weging van een OLOD binnen de opdracht houdt men rekening met het aantal contacturen, de voorbereidingstijd die nodig is (gaat het over een vakinhoud die snel evolueert? bestaat er al cursusmateriaal of moet dat ontwikkeld worden?) en de nazorgtijd (de kwetsbaarheid van de groep studenten).

De commissieleden vinden het belangrijk dat er voldoende aandacht blijft voor de continue professionalisering van de docenten.

2.2.4 Onderzoeksvraag 4: de infrastructuur

De commissieleden lazen in het dossier dat een geïntegreerd Cybersecurity Operatiecenter (ISOC) uitgebouwd wordt, dat studenten van de opleiding cybersecurity de mogelijkheid zal geven om in een gesimuleerde realistische omgeving te werken in het kader van verschillende OLOD's. Labo's en simulatieomgevingen zijn inderdaad erg nodig om studenten voor te bereiden op real-life scenario's. De commissieleden zouden graag meer zicht krijgen op de soorten labo's en simulatieomgevingen waarover de opleidingen kan beschikken. Ze vragen zich af of de nieuwste technologieën en softwaretools aanwezig zijn. En of deze infrastructuur voldoende toegankelijk is voor de studenten, ook met het oog op de verwachte toename van de instroom.

Tijdens het bezoek van de commissieleden werd tijd voorzien voor een rondleiding en showcase op de campus. Binnen de IT-cluster wordt rond verschillende topics aan onderzoek gedaan. In projecten raken die topics elkaar soms. Het onderzoek is altijd toegepast en gekoppeld aan dienstverlening. Elk project moet een van de volgende vier zaken realiseren: technologie door-ontwikkelen, technologie toepassen, onderwijs optimaliseren of professionaliseren. De aanwezigheid van een onderzoeksgroep Security en Privacy zorgt voor een goede wisselwerking met de afstudeerrichting cybersecurity en dat zal ook het geval zijn voor de nieuwe bachelor in de cybersecurity.

De gesprekspartners leggen uit dat projecten vaak tot stand komen vanuit het werkveld. Zo gaat men op basis van open source software zaken uitbouwen voor kleine bedrijven die geen grote budgetten hebben voor cybersecurity. Een voorbeeld van een project is futurogram, dat via blokchain toelaat om videoboodschappen achter te laten voor familie als iemand overlijdt.

De zaken die in het kader van onderzoek en projecten ontwikkeld worden, kunnen ook ingezet worden in de opleiding. Een voorbeeld daarvan is een fictieve productiehal met controle-units. Dit gaat over industriële security. Het wordt nu gebruikt in de bachelor in de toegepaste informatica om bewustzijn te creëren bij studenten dat als je iets verandert aan software, dit een risico kan inhouden voor bv. een productielijn in een fabriek. Ook fysieke beveiliging komt op die manier aan bod.

Het geïntegreerd Cybersecurity Operatiecenter dat uitgebouwd wordt, is gebaseerd op open source software waarvoor men eigen rules schrijft. Opleidingbreed komen alle gegeven daar

toe. Analisten werken ermee en zien snel eventuele pogingen om te hacken. Er zijn ook teams die offensief en teams die defensief werken.

De financiering is deels intern. Daarnaast gaat men zo veel mogelijk op zoek naar externe funding, bv. via het programma TETRA van VLAIO. Die middelen laten tegelijk toe het nodige materiaal te voorzien. Zo zijn er servers aangekocht met voldoende sterke grafische kaarten om AI te kunnen gebruiken. De huidige capaciteit is voldoende voor de hele opleiding.

Het is een bewuste keuze om de projecten in handen te geven van eigen medewerkers en niet enkel aan (tijdelijke) projectmedewerkers, zo geven de gesprekspartners aan. Men stelt liefst dus het eigen personeel vrij voor onderzoek en de middelen worden dan gebruikt voor een vervangend docent. Op die manier vloeit de expertise beter door naar het onderwijs, afhankelijk natuurlijk van de aard van een project. Er is ook een excellentietraject voor studenten. Zij kunnen hun stage binnen een van de projecten doen samen met de onderzoekers. Het is ook de ambitie van de nieuwe opleiding in de cybersecurity om studenten te houden of te laten terugkomen.

De opleiding heeft ook een labo ter beschikking voor network system pentesting. Studenten krijgen dan de opdracht om in de omgeving binnen te geraken (ethical hacking) en bv. tot bij rapporten in de omgeving te gaan. Enkele studenten geven hier een demo van.

De commissieleden zijn onder de indruk van de beschikbare infrastructuur, in het bijzonder van het ISOC. Niet alle opleidingen hebben zo'n omgeving ter beschikking. De commissieleden zijn ervan overtuigd dat deze infrastructuur de student in staat stelt de technische vaardigheden aan te leren. De setting is zeker meer dan voldoende daarvoor.

2.2.5 Onderzoeksvraag 5: de beoordeling van het eindniveau

De commisieleden polsen naar de organisatie en beoordeling van de stage (OLOD internship). De gesprekspartners geven aan dat momenteel in de bachelor in de toegepaste informatica heel wat contacten gelegd zijn en er ook stages mogelijk zijn in cybersecurity. De basis is dus al gelegd en het aanbod is heel breed, zowel in bedrijven als bij politie en leger. Ook de systematiek wil men overnemen van de andere opleidingen in de cluster.

De matchmaking gebeurt via een stagemarkt. Via een stageplatform kunnen bedrijven en organisaties een concreet project indienen. De stagecoördinator beoordeelt de stageplaats: is er voldoende ruimte voor begeleiding, is er een goed leerklimaat, is er een structuur? Het is bijvoorbeeld niet de bedoeling dat een student de stage volledig van thuis uit doet. Het project dat een stagebedrijf voorstelt wordt beoordeeld op basis van de leerdoelen. Daarbij is de vraag of de verwachtingen overeenkomen met een niveau 6 (bachelor) en of er voldoende leerdoelen zijn die afgetoetst kunnen worden tijdens de stage.

Tijdens speeddatings met de studenten kunnen de bedrijven die projecten voor stages toelichten. Voorafgaand aan de effectieve matching zijn er nog vervolggesprekken. Voor de stagebedrijven heeft Howest een draaiboek ontwikkeld. Dat bevat ook een overzicht van alle leerresultaten.

Elke student krijgt een stagebegeleider, een van de lectoren van de opleiding. Die volgt het hele project. Voor de start van de stage is er een gesprek over de concrete invulling. Bij het begin van de stage gaat de stagebegeleider op stagebezoek, dan wordt ook het stagecontract getekend. Op die manier is er contact tussen stagebedrijf en stagebegeleider. Bij problemen of vragen kan het stagebedrijf de stagebegeleider dus contacteren. Ook de student kan bij de stagebegeleider terecht. Het gebeurt volgens de gesprekspartners zelden dat er een mismatch blijkt te zijn tussen student en stagebedrijf. De keren dat dat wel het geval is, wordt een andere stageplaats gezocht.

Bij elke stage is er een tussentijdse evaluatie, waarbij student, stagegever en stagebegeleider aanwezig zijn. Voor die tussentijdse evaluatie is er een evaluatieformulier, maar men

quoteert nog niet. Dat wordt pas op het einde van de stage gedaan, naar aanleiding van een soortgelijk overleg. De stagegever van het bedrijf scoort dan de verschillende leerresultaten en die scoring vormt de basis voor de punten.

De docenten ervaren dit contact met het werkveld ook als verrijkend. Een bijkomend resultaat is dat hier contacten gelegd worden voor gastcolleges.

Uit de gesprekken met de studenten blijkt dat zij al behoorlijk goed zicht hebben op wat hun stage zal inhouden. Ze vermelden de stagemarkt en de speeddating. Voor hen is de informatie over de mogelijkheden vooraf goed duidelijk. Ze geven aan dat er ook veel aandacht besteed wordt aan de sollicitatie op een stageplaats (speeddate).

De werkveldpartners geven aan dat er meestal een onderzoeksopdracht gegeven wordt tijdens een stage. Het is de bedoeling dat studenten individueel iets uitzoeken. De stagementor stuurt dat dan bij.

Algemeen vinden de werkveldpartners het vooral belangrijk dat een student tijdens de stage een goed project heeft en dingen kan leren die in een gesimuleerde context niet aan bod kunnen komen. Het is de bedoeling hen te helpen met het oog op later, als ze echt starten met werken. Ze vinden het belangrijk dat studenten kunnen bijleren.

De commissieleden vragen of het voor het werkveld voldoende duidelijk is wat de verwachtingen zijn van een stage. Niet alle werkveldpartners zijn even vertrouwd met het draaiboek en andere tools van Howest. Ze leggen ook niet allemaal de link met leerdoelen. De meeste stageprojecten zijn projectmatig, een student wordt dan beoordeeld op de vooraf geformuleerde outcome. Ze gaan er niet van uit dat een stage technische competenties moet toetsen.

De commissieleden denken dat het belangrijk is de stagebedrijven voldoende mee te nemen in het verhaal van de stage, door hen vertrouwd te maken met de tools (o.a. draaiboek) van Howest en door ook duidelijk afspraken te maken over de leerresultaten die tijdens een stage aan bod moeten komen.

De commissieleden vragen nog hoe men ervoor zorgt dat alle leerresultaten in de eindevaluatie aan bod komen. In welke mate zijn de vier OLOD's complementair en op elkaar afgestemd?

De gesprekspartners merken op dat het niet altijd mogelijk is in de stage alle leerdoelen sluitend af te toetsen. Dat is de reden waarom het security project gedaan wordt. Daar kan je wel aan alle leerdoelen een plaats geven. Het security project is draaiboekgericht, je kan er alles in onderbrengen.

De commissieleden bevelen aan om voor de toetsing van het eindniveau de stage nog duidelijker af te stemmen op dit security project, zodat zichtbaar is dat globaal alle leerdoelen aan bod komen.

3 Oordeel

De commissie benoemt een aantal sterke punten van de opleiding.

De commissie ervaart de duidelijke nood aan een bachelor in de cybersecurity en de heldere motivatie hiervoor als positief. Het is ook duidelijk dat deze tegemoetkomt aan de noden van het werkveld.

De commissie vindt de manier waarop de opleiding oog heeft voor de heroriëntering van studenten positief. Door het programma van de opleiding in de cybersecurity af te stemmen op dat van de bachelor in de toegepaste informatica, kunnen studenten hun keuze bijsturen.

De commissieleden zagen een team van opleidingsverstrekkers met veel gedrevenheid en passie, en met voldoende expertise om de opleiding te dragen. Bovendien worden ook gastcolleges opgezet met de steun van het werkveld.

De commissieleden zijn onder de indruk van de aanwezige infrastructuur, die tijdens een rondleiding uitgebreid gedemonstreerd werd.

Algemeen is er een duidelijke betrokkenheid van het werkveld, dat op verschillende momenten en vanuit verschillende hoeken input geeft.

Daarnaast formuleert de beoordelingscommissie enkele aanbevelingen:

- De leerresultaten zijn erg uitgebreid en versnipperd. Breng ze duidelijker en eenvoudiger in kaart door ze te clusteren, in functie van studeerbaarheid en helderheid voor studenten en docenten.
- Heb voldoende aandacht voor ondersteuning van en feedback aan studenten, zeker met het oog op de voorziene groei van het aantal studenten.
- Werk een plan uit om in de toekomst voldoende docenten te kunnen aantrekken om de voorziene groei op te vangen en de studenten goed te kunnen ondersteunen.
- Heb aandacht voor de continue professionalisering van de huidige docenten.
- Zorg dat ook voor het werkveld voldoende duidelijk is welke leerresultaten tijdens een stage aan bod moeten komen.
- Stem voor de toetsing van het eindniveau de stage duidelijk af op het security project.

De commissie gelooft dat er voldoende potentiële kwaliteit is voor de Bachelor in de cybersecurity en dat de aanbevelingen van de commissieleden opgenomen kunnen worden door het team dat de opleiding verder vorm zal geven.

Bijlage 1: Administratieve gegevens van de instelling en de opleiding

Instelling	Hogeschool West-Vlaanderen
Naam opleiding	Bachelor in de cybersecurity
Niveau en oriëntatie	VKS 6 - professioneel gerichte bachelor
(Bijkomende) titel	Geen
(Delen van) studiegebied(en)	Industriële wetenschappen en technologie
Afstudeerrichtingen	Niet van toepassing
Opleidingstrajecten voor werkstudenten, voltijds/deeltijds trajecten, dag-/avondonderwijs, onderscheiden vormen van diplomering	Voltijds dagonderwijs
De vestiging waar de opleiding wordt aangeboden	Brugge (campus Brugge Station)
Onderwijstaal	Nederlands
Studieomvang (in studiepunten)	180
Wanneer het om een graduaats- of bacheloropleiding gaat: de aansluitingsmogelijkheden en de mogelijke vervolgopleidingen; wanneer het om een masteropleiding gaat: de vereiste vooropleidingen en toelatingsvoorwaarden	Er zijn aansluitingsmogelijkheden en vervolgopleidingen zowel op bachelor- als op masterniveau. De lijst hieronder is niet exhaustief. Via verkorte opleidingen kunnen de studenten een tweede bachelordiploma behalen, bijvoorbeeld de bachelor Toegepaste informatica. Vervolgopleiding op masterniveau zijn de Master of Science in Cybersecurity (Université Libre de Bruxelles, Université Catholique de Louvain, Université de Namur, Ecole Royale Militaire, HELB, ESI Brussels) of Master in de Industriële wetenschappen – informatica of electronica-ICT.

Bijlage 2: Domeinspecifieke leerresultaten (DLR)

1. De bachelor in de cybersecurity analyseert de kritische bedrijfsprocessen, -data en -infrastructuur en doet een wezenlijke bijdrage tot cybersecurity by design en data protection by design door de identificatie, evaluatie en inperking van risico's en bedreigingen wat leidt tot een informatiebeveiligingsbeleid op, met inbegrip van strategische doelen, procedures, richtlijnen en policies.
2. De bachelor in de cybersecurity verzamelt, analyseert, structureert en deelt inzetbare informatie over threat intelligence die het gedrag, de motieven en het vermogen van cybercriminelen omvat, met inbegrip van phishing en ransomware.
3. De bachelor in de cybersecurity evalueert en verbetert in het volledige gamma van software, firmware en hardware technologieën de cybersecurity van (sub)systemen door opsporen, analyseren en afhandelen van bestaande aanvalsvectoren en kwetsbaarheden, dit door het inzetten van bestaande defensieve en offensieve beveiligingssoftware, inclusief het ontwikkelen van eigen scripts, penetration testing, reductie van de eigen digitale voetafdruk en participeren in red teaming oefeningen.
4. De bachelor in de cybersecurity selecteert en configureert de optimale technieken, met inbegrip van identificatie, authenticatie en autorisatie, en past deze toe binnen de gangbare omgevingen, inclusief fysieke en industriële omgevingen, voor elke fase van
5. De bachelor in de cybersecurity draagt bij tot structureren en optimaliseren van een secure development life cycle waarbij elke fase afdoende wordt beschermd door een gepaste combinatie van technische en organisatorische maatregelen, toegespitst op specifieke vereisten binnen relevante domeinen.
6. De bachelor in de cybersecurity versterkt cybersecurity awareness, ondersteunt de nodige veranderingsprocessen en levert organisatiegericht advies op het vlak van architectuur en onderhoud van de beveiliging van data- en bedrijfsprocessen.
7. De bachelor in de cybersecurity realiseert preventie, detectie, respons, herstel en opsporing van cyberdreigingen en -aanvallen door keuze, toepassing en interpretatie van de geschikte technieken.
8. De bachelor in de cybersecurity communiceert, rapporteert en overlegt, minstens in het Nederlands en het Engels, op een professionele manier en aangepast aan het doelpubliek over cybersecurity incidenten en actieplannen met verschillende stakeholders.
9. De bachelor in de cybersecurity handelt met een ethische verantwoordelijkheid in de domeinen van cybersecurity, intelligence, data protection, cyber crime, forensische opsporing en cyber warfare, rekening houdend met het wettelijk en deontologisch kader en met impact op personen, organisaties en maatschappij.
10. De bachelor in de cybersecurity initieert, implementeert, onderbouwt, documenteert cybersecurity projecten op maat van de organisatie, werkt hierbij teamgericht in een multidisciplinaire context, stelt de juiste prioriteiten en toont een goed timemanagement, probleemoplossend vermogen en zelfkritische ingesteldheid.
11. De bachelor in de cybersecurity stuurt de eigen professionele ontwikkeling vanuit de opvolging en raadpleging van relevante bronnen en vanuit praktijkgericht onderzoek naar (inter)nationale ontwikkelingen in de cybersecurity en de domeinen die dit beïnvloeden met het oog op levenslang leren.

Bijlage 3: Samenstelling van de commissie

De beoordeling is gebeurd door een commissie van deskundigen aangesteld door de NVAO. Deze is als volgt samengesteld:

Raymonda Verdyck *(voorzitter)*, Ex-afgevaardigd bestuurder van het GO!-onderwijs.

Erik Poll *(commissielid)*, Associate Professor in Digital Security at Radboud University Nijmegen (Netherlands).

Mohssin Assaban *(commissielid)*, International Business Professional cybersecurity.

Roan Merens *(student-commissielid)*, student IT Hogent.

De commissie werd bijgestaan door:

- **Ils Aerts** *(procescoördinator)* beleidsmedewerker NVAO.
- **Tine Swaenepoel** *(extern secretaris)* zaakvoerder Yelski.

Alle commissieleden hebben de deontologische code van de NVAO ondertekend.

Bijlage 4: Programma voor de dialoog met de opleiding

9.00u – 9.15u	15 min	Ontvangst en intern overleg commissie
9.15u – 9.30u	15 min	Gesprek met het instellingsbestuur
9.30u – 11.00u	1u 30 min	Gesprek met opleidingsverantwoordelijken en (beoogde) docenten
11.00u- 11.15u	15 min	Pauze en intern overleg commissie
11.15u – 12.00u	45 min	Gesprek met potentiële studenten
12.00u – 12.45u	45 min	Lunch en intern overleg commissie
12.45u - 13.30u	45 min	Rondleiding Showcase op de campus
13.30u – 14.00u	15 min	Intern overleg commissie
14.00u – 14.45u	45 min	Overleg met het werkveld
14.45u – 15.00u	15 min	Intern overleg commissie
15.00u – 15.30u	30 min	Vrij moment
15.30u – 16.00u	30 min	Intern overleg commissie
16.00u- 16.15u	15 min	Afsluitende dialoog met instellings- en opleidingsverantwoordelijken

Bijlage 5: Verantwoording

De beoordeling werd uitgevoerd aan de hand van het "*Beoordelingskader Toets Nieuwe Opleiding op maat van de eigen regie*" van juni 2020, zoals bekrachtigd door de Vlaamse regering op 27 november 2020.

Nadat de aanvraag ingediend door de instelling ontvankelijk werd verklaard, heeft de NVAO een commissie samengesteld. Deze commissie werd goedgekeurd door het dagelijks bestuur van de NVAO. De instelling tekende geen bezwaar aan tegen de commissie.

De commissie heeft zich aan de hand van de door de opleiding verstrekte documenten op de beoordeling voorbereid. Voorafgaand aan een voorbereidend overleg heeft elk commissielid de eerste indrukken opgemaakt en werden prioritaire vragen opgelijst.

Tijdens de voorbereidende werkzaamheden heeft de commissie verder alle verkregen informatie besproken en heeft zij tevens de dialoog met de instelling en de opleiding voorbereid.

Aan de hand van NVAO's Waarderende Aanpak heeft de commissie zich tijdens de dialoog verder verdiept in de context van de opleiding en op basis daarvan een onderzoek gevoerd naar de potentiële kwaliteit van de nieuwe opleiding.

Tijdens de afrondende werkzaamheden heeft de commissie alle verkregen informatie besproken en vertaald naar een holistisch oordeel. De commissie heeft deze conclusie in volledige onafhankelijkheid genomen.

Het totaal aan beschikbare gegevens is verwerkt tot een ontwerp van beoordelingsrapport. Eens alle commissieleden hadden ingestemd met de inhoud van het beoordelingsrapport, heeft de voorzitter van de commissie het beoordelingsrapport vastgesteld. Het door de voorzitter vastgestelde beoordelingsrapport werd aan de NVAO bezorgd.

Bijlage 6: Overzicht van het bestudeerde materiaal

Documentatie beschikbaar gesteld bij de aanvraag

- Informatiedossier Bachelor in Cybersecurity – Aanvraag Toets Nieuwe Opleiding – Howest – mei 2023
- Bijlagen:
    - **DLR bachelor in de CS, incl. de aftoetsing aan de descriptoren VKS6**
    - **Benchmark ba CS**
    - Vergelijking DLR Toegepaste informatica en Cyber Security
    - *Competentietrajecten per leerresultaat*
    - *Competentiematrix op niveau van de leerresultaten*
    - *Competentiematrix op niveau van de leerdoelen*
    - *Opleidingsprogramma*
    - **Studiefiches eerste opleidingsfase en afsluitende toetsen**
    - *Howest-kader inzake blended leren op opleidingsniveau*
    - Beschrijving personeel ba CS
    - Overzicht contacten werkveld
    - *Kwaliteitszorgcriteria Howest*

Documenten beschikbaar gesteld tijdens de dialoog

- Documenten opgehangen in het gesprekslokaal
    - Poster Bachelor cybersecurity internationalisering
    - Poster toegepast onderzoek en dienstverlening
    - Brief IBM
    - Poster attitudes en vaardigheden
    - Poster Cyber Security Mindsets
    - Poster profiel van de bachelor cybersecurity
    - Poster certificaten
    - Poster practice-based learning, project-based learning, problem-based learning
    - Poster studieprogramma cybersecurity
    - Poster onderzoeksleerlijn cybersecurity
- Documenten beschikbaar gesteld op laptop en bekeken door de commissieleden:
    - Cursus cybersecurity fundamentals
    - Nieuwe beschikbare studiefiches

Colofon

Bachelor in de cybersecurity
Hogeschool West-Vlaanderen • VL131193-23
Toets Nieuwe Opleiding op maat van de eigen regie •
Beoordelingsrapport
23 april 2024

Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 • 2514 JG Den Haag
P.O. Box 85498 • 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net