NVAO • NEDERLAND

TOETS NIEUWE OPLEIDING

ASSOCIATE DEGREE

AD CYBERSECURITY

Hogeschool Utrecht

BEKNOPT ADVIESRAPPORT

5 JULI 2023

1 Kwaliteitstoets

De toets nieuwe opleiding is een kwaliteitstoets. Een procedure toets nieuwe opleiding (TNO) is een *plan*beoordeling. Een panel van deskundigen toets de kwaliteit van de nieuwe opleiding tijdens een locatiebezoek aan de universiteit of hogeschool. Een discussie tussen 'peers' vormt de basis van de beoordeling en resulteert in een adviesrapport. De inhoud van de opleiding, de toetsing en de studeerbaarheid komen expliciet aan de orde.

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) neemt een accreditatiebesluit op basis van het paneladvies. Dit besluit kan positief, positief onder voorwaarden of negatief zijn. Als het besluit positief of positief onder voorwaarden is, mag de nieuwe opleiding starten. De instelling heeft daarmee het recht om een wettelijk erkend diploma af te geven aan studenten die de opleiding voltooien.

Dit beknopte adviesrapport bevat de belangrijkste uitkomsten van de toetsing door het panel. Een volledig adviesrapport met de bevindingen en overwegingen van het panel is ook beschikbaar. Op basis van het volledige rapport neemt de NVAO een accreditatiebesluit. De NVAO publiceert beide rapporten op haar website.[1]

Meer informatie over de NVAO-werkwijze en de (tijdelijke) TNO-procedure is te vinden op www.nvao.net.

2 Panel

Samenstelling

- Bart Preneel, *voorzitter,* gewoon hoogleraar en diensthoofd van de Computer Security & Industrial Cryptography (Cosic) onderzoeksgroep aan de Katholieke Universiteit Leuven;
- Martin Molema, *lid,* docent bij de Academie ICT & Creative bij NHL Stenden Hogeschool;
- Pim Sewuster, *lid,* Cybersecurity-expert bij ING;
- Suzet van Gaalen, *student-lid,* recent afgestudeerde van de opleiding Associate degree Commerciële Economie van Fontys Hogescholen en voormalig lid opleidingscommissie.

Ondersteuning

- Reinier Gerritzen, *secretaris*
- Laura Oosterveld, *NVAO-beleidsmedewerker en procescoördinator*

Locatiebezoek

24 mei 2023, Hogeschool Utrecht, locatie Amersfoort

[1] www.nvao.net

3 Oordeel

Het NVAO-panel oordeelt positief onder voorwaarden over de kwaliteit van de Associate degree Cybersecurity van de Hogeschool Utrecht.

De opleiding is er op basis van uitgebreid vooronderzoek in geslaagd een passend beroepsprofiel op te stellen. Daarbij heeft de Ad Cybersecurity zich mede gebaseerd op relevante (inter)nationale kaders en consulteerde zij meermalen een representatieve vertegenwoordiging van regionale werkveldpartners en andere onderwijsinstellingen. De gekozen competenties en leeruitkomsten passen goed bij het profiel en de opleiding heeft deze op het juiste Ad-niveau beschreven.

De Ad Cybersecurity richt een helder opgebouwd onderwijsprogramma in dat naarmate de studie vordert steeds praktijkgerichter wordt. De didactische aanpak is sterk en past goed bij de doelgroep van de Ad-student. Het bevlogen en didactisch bekwame docententeam is op haar taak toegerust. Het is de intentie van de instelling aan het team nog een docent met werkervaring in cybersecurity toe te voegen. Inhoudelijk maakt de opleiding vaak logische keuzes, al maakt zij niet altijd voldoende duidelijk hoe diepgaand zij de verschillende thema's aanbiedt en wat zij daarin van studenten verwacht. Het programma is verder zeker arbeidsmarktgericht, maar nog niet uitgesproken vernieuwend. Daar valt volgens het panel nog winst te behalen. De Ad Cybersecurity richt een toetssysteem in dat het leerproces van de studenten goed ondersteunt. De sterke examencommissie en toetscommissie zien actief toe op de kwaliteit van de toetsing. Wel behoeft de toetsdocumentatie op meerdere punten nog nadere schriftelijke uitwerking om de eisen voor studenten beter inzichtelijk te maken.

Hoewel de basis van de opleiding goed staat, signaleert het panel een essentieel verbeterpunt. Van het eerste jaar van het onderwijsprogramma is de eerste periode A veel gedetailleerder uitgewerkt dan de overige drie periodes. Het panel legt de Ad Cybersecurity daarom de volgende voorwaarde op: het team dient periode B, C en D verder uit te werken met uitgebreidere cursuswijzers, concrete opdrachten, passende beroepsproducten en onderwijsmateriaal voor docenten. Verder dient het team duidelijk te maken welke vakinhoud per periode centraal staat, inclusief de mate van diepgang en het verwachte niveau daarvan. Het panel wijst erop dat deze aanvullingen van het cursusmateriaal consequenties hebben voor de verschillende toetsmomenten en toetscriteria die het panel graag meegenomen ziet in de gedetailleerde uitwerking. De documentatie om aan deze voorwaarde te voldoen legt de opleiding uiterlijk acht weken voorafgaand aan de start van de opleiding (1 februari 2024) aan het panel voor.

Gezien de open en lerende houding die docenten in de gesprekken toonden en het ontwikkelproces tot nu toe, vertrouwt het panel erop dat de opleiding voorafgaand aan de start aan deze voorwaarde kan voldoen.

4 Sterke punten

Het panel constateert de onderstaande sterke punten:

1. Betrokken werkveld – In het uitgebreide vooronderzoek heeft de opleiding een breed scala aan organisaties uit het werkveld geraadpleegd om input te geven op het beroepsprofiel. Deze werkveldpartners geven aan dat zij veel kansen zien voor afgestudeerden van de Ad Cybersecurity.

2. Bevlogen docenten– Het docententeam is zeer gedreven en enthousiast. Zij tonen een grote betrokkenheid bij de nieuwe opleiding en een sterke interesse in het vakgebied van Cybersecurity.

3. Didactische aanpak – In deze opleiding werken studenten in leerteams en krijgen zij gevarieerde werkvormen aangeboden. De manier waarop de Ad Cybersecurity de onderwijsperiodes en onderwijsweken inricht, helpt studenten actief te studeren.

4. Programmatisch Toetsen – Het toetssysteem van de Ad Cybersecurity is zo vormgegeven dat studenten regelmatig tussentijdse producten opleveren waar zij feedback op krijgen. Daarmee ondersteunt de opleiding hun leerproces op goede wijze.

5. Examencommissie – De examencommissie en toetscommissie zijn actief betrokken bij de Ad Cybersecurity en houden goed toezicht op kwaliteit van de toetsing en op het Associatie degree-niveau van de opleiding.

5 Aanbevelingen

Met het oog op de verdere ontwikkeling van de opleiding doet het panel een aantal aanbevelingen. Deze aanbevelingen doen geen afbreuk aan het positieve oordeel over de kwaliteit van de opleiding.

1. Vakinhoud – Verhelder de Body of Knowledge & Skills (BoKS) voor het gehele onderwijsprogramma. Expliciteer wat een goede verhouding is tussen de verschillende cybersecuritythema's en operationaliseer per thema wat het verwachte niveau is dat studenten moeten bereiken. Werk tevens nader uit wat de benodigde vakinhoud is in het praktijkproject in het tweede leerjaar.

2. Toekomstgericht – Verrijk het onderwijsprogramma met meer innovatieve elementen. Betrek vooruitstrevende werkveldpartners en het lectoraat Cybersecurity van de HU daarbij.

3. Diverse inbreng werkveld – Zorg voor een werkveldcommissie met een evenwichtige verdeling tussen private en publieke organisaties. Voeg daar indien mogelijk vernieuwende cybersecurityorganisaties aan toe en overweeg leden te laten rouleren. Verduidelijk tevens de verwachte inbreng van de gastdocenten in het programma.

4. Toetsing – Werk verschillende aspecten van de toetsing nader schriftelijk uit om de eisen voor studenten duidelijker te maken.

5. Afstuderen – Formuleer nadere criteria voor het afstuderen en uniformeer het beslissingsformulier met die van de overige onderwijseenheden.

6 Hoe gaat het verder?

De NVAO neemt een accreditatiebesluit nieuwe opleiding op basis van het volledige adviesrapport van het panel. Dit besluit heeft een geldigheidsduur van zes jaar. Voor een accreditatiebesluit onder voorwaarden gelden andere bepalingen. Na accreditatie valt de nieuwe opleiding onder de gewone accreditatieprocedure voor bestaande opleidingen. De NVAO publiceert het besluit samen met het volledige rapport en deze beknopte versie ervan op haar website.[2]

Het interne systeem van kwaliteitszorg van de universiteit of hogeschool voorziet in passende vervolgacties die verzekeren dat de instelling de eigen visie op goed onderwijs realiseert. Een belangrijke bijdrage leveren de onderwijsvisitaties van opleidingen en diverse tussentijdse 'peer reviews'. Bij de volgende visitatie zal de opleiding terugkoppelen over wat zij met de aanbevelingen van het panel heeft gedaan. Deze verbeteracties krijgen ook een plek in het volgende adviesrapport. Meer informatie daarover op de website van de instelling.[3]

7 Summary

The outcome of the initial accreditation of the Associate degree (Ad) Cybersecurity of HU University of Applied Sciences is conditionally positive. The Accreditation Organisation of the Netherlands and Flanders (NVAO) organised a peer review and convened a panel of experts visiting the institution in Amersfoort on May 24, 2023.

Based on extensive preliminary research, the Ad Cybersecurity has succeeded in developing an appropriate professional profile that is based on relevant (inter)national frameworks. In this research the team also repeatedly

[2] https://www.nvao.net.nl/besluiten
[3] https: www.internationalhu.com/

consulted representative organisations from the Cybersecurity field. The chosen competencies and subsequent learning outcomes fit the profile and are described at the appropriate Associate degree level.

The Ad Cybersecurity has designed a well-structured educational programme that becomes more practice-oriented as the study progresses. The didactic approach is strong and suits Associate degree-students adequately. The enthusiastic and didactically competent teaching team is well-equipped for its task. The Cybersecurity topics that this programme offers fit the chosen profile. However, the extent or depth to which the several themes are addressed is not abundantly clear to the panel. Furthermore, there is still room for improvement when it comes to the innovative character of the programme. The Ad Cybersecurity sets up an assessment system that thoroughly supports the learning process of the students. The strong examination board actively monitors the quality of this system. However, the assessment documentation needs further written elaboration on several aspects to improve the clarity of the requirements for students.

Notwithstanding the adequate basis of the programme, the panel identifies an essential point for improvement for which it sets the following condition. The team must further develop periods B, C and D with more extensive course guides, clear assignments, appropriate professional products and educational material for teachers. Furthermore, the team must clarify which Cybersecurity topics are central per period, including the scope, depth and expected level of these topics. The panel points out that these additions to the course material may result in changes to the assessment criteria which the team needs to process in the documentation. The Ad Cybersecurity needs to meet this condition no later than eight weeks prior to the start of the programme in February 2024.

Further information about NVAO and the quality assurance system in the Netherlands can be found on www.nvao.net. For more information on HU University of Applied Sciences see the university's website.[4]

[4] https://www.internationalhu.com/

Het beknopte adviesrapport is tot stand gekomen in opdracht van de NVAO met het oog op de beperkte toetsing van de nieuwe opleiding Ad Cybersecurity van de Hogeschool Utrecht

Aanvraagnummer: AV-1759

NVAO

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