Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
T.a.v. Mw. Drs. A.C. van Huffelen
Postbus 20011
2500 EA Den Haag

Datum
15 december 2023

Onderwerp
Informerende brief van de Cyber Security Raad over onderwijsversterking en kennisontwikkeling

Excellentie,

Tijdens uw bezoek aan de Cyber Security Raad (hierna de raad) van 15 juni jl. spraken wij onder andere over het tekort aan cybersecurityspecialisten en de noodzaak om cybersecuritykennis in Nederland te behouden en verder te versterken. U heeft de raad gevraagd om duiding bij dit urgente onderwerp. In deze brief gaat de raad nader in op de verschillende oorzaken van het tekort, zoals onvoldoende aansluiting van vraag en aanbod op elkaar, nieuwe ontwikkelingen op het vakgebied, het groeiende docententekort, gebrek aan sturing en problemen met kennismigratie.

De raad benadrukt de noodzaak van gecoördineerde actie om de belangrijkste knelpunten aan te pakken, zoals omvorming van opleidingen en het tegengaan van de huidige *braindrain.* De raad doet in deze brief hiervoor een oproep aan alle direct betrokken ministeries, onderwijsinstellingen en het bedrijfsleven. Gezien de ernst en omvang van het probleem is centrale regie vanuit de overheid daarbij noodzakelijk.

Achtergrond

Nederland heeft een hoge digitaliseringsgraad. Dit draagt sterk bij aan ons economisch verdienmodel, maar brengt ook de nodige risico's met zich mee. Nederland heeft relatief gezien een uitgebreide (digitaal kwetsbare) infrastructuur, bijvoorbeeld in de transportsector. Daarnaast beschikken we over cruciale waterbouwwerken en is de Amsterdam Internet Exchange (AMS-IX) één van de grootste internetknooppunten ter wereld. Om dergelijke omgevingen goed te kunnen laten functioneren én te beveiligen is veel hoogwaardige expertise nodig.

Door de krapte over de volle breedte van de arbeidsmarkt komt de beschikbare cybersecurityexpertise steeds verder onder druk te staan. Nieuwe ontwikkelingen op het gebied van artificiële intelligentie (AI), internetsecurity en kwantumtechnologie, plus de intensivering van cybercriminaliteit en de dreiging vanuit statelijke actoren, drijven de behoefte aan diverse typen cybersecurityspecialisten verder op. Wereldwijd loopt het tekort volgens het Cybercrime Magazine tegen 2025 op tot 3,5 miljoen[1]. Tegelijkertijd zijn de risico's van mogelijke cyberaanvallen ongekend: de kosten van cybercriminaliteit kunnen in 2025 wereldwijd oplopen tot 10,5 biljoen dollar[2].

[1] Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025 (cybersecurityventures.com)
[2] Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)

Tekort aan specialisten

Al in 2015 agendeerde de raad het groeiende gebrek aan cybersecurityspecialisten, in het bijzonder met een oproep tot meer samenhang in de initiatieven rond cybersecurity in het onderwijs en het bedrijfsleven[3]. Ook onderzoeken en rapporten van andere toonaangevende instituten signaleerden al meerdere jaren geleden het tekort[4]. Intussen is de behoefte aan cybersecurityspecialisten explosief doorgegroeid, terwijl de doorontwikkeling van het Nederlandse cybersecurityonderwijs daarbij fors achterblijft.

De raad ziet een groeiende *cyber-skills gap*, dat intussen op zichzelf een veiligheidsrisico begint te vormen. Het aantal cybersecurityspecialisten in Nederland nam de laatste jaren in absolute aantallen weliswaar toe, maar blijft gelijk als percentage van de totale beroepsbevolking. Volgens de Cyber Workforce Study van de internationale cybersecurityorganisatie ISC2[5] wordt de *workforce gap* voor cybersecurity in Nederland over 2022 geschat op 21.5%. Daarmee scoort ons land slecht in vergelijking met landen als Frankrijk, Spanje, het Verenigd Koninkrijk en de Verenigde Staten.

Zoals in veel verschillende branches in Nederland is ook het tekort aan specialisten in het cybersecuritydomein uiterst zorgelijk. Zowel overheidsinstellingen als het bedrijfsleven voelen de tekorten, terwijl ons land grote ambities heeft op het gebied van (veilige) digitalisering. Hierdoor kan ook niet goed worden voldaan aan een belangrijke randvoorwaarde voor uitvoering van de verschillende overheidsstrategieën op dit vlak, waaronder de Nederlandse Cybersecuritystrategie (NLCS) en uw Werkagenda '*Waardengedreven* Digitaliseren'.

Oorzaken van het tekort

In Nederland is de afgelopen jaren al in verschillende fasen onderzoek gedaan naar (i) welke typen cybersecurityspecialisten bedrijven nodig hebben (rollen), (ii) welke competenties en skills bij deze rollen horen en (iii) wat de specifieke tekorten zijn. In de Nederlandse Cybersecuritystrategie (NLCS) is onder Pijler IV dan ook de nodige aandacht besteed aan de cybersecurityarbeidsmarkt.

Momenteel voert het Platform Talent voor Technologie in opdracht van het Ministerie van Economische Zaken en Klimaat een uitgebreid, aanvullend onderzoek uit. Dit moet een completer beeld geven van de actuele omvang van de tekorten, de verschillende typen expertise die nodig zijn en het zich ontwikkelend aanbod van cybersecurityonderwijs, zowel in de publieke als commerciële sector. Deze inzichten kunnen verder helpen bij de doorontwikkeling van het onderwijs. De resultaten van het onderzoek worden in het eerste kwartaal van 2024 verwacht. Vooruitlopend hierop constateert de raad dat de volgende oorzaken van het tekort (nog steeds) bestaan:

1. **Onvoldoende aansluiting van vraag en aanbod op elkaar**
   Dit blijft problematisch. Cybersecurity heeft zich in de afgelopen periode verder ontwikkeld van een technisch onderwerp tot een multidisciplinair en zelfs interdisciplinair vakgebied, dat veel verschillende skills en competenties vereist. De diverse profielen van specialisten[6] laten dit ook duidelijk zien, waarbij met name de senior medewerkers aan verschillende profielen moeten kunnen voldoen. Deze discipline-overstijgende kennis en kunde is veelal niet binnen één opleidingsinstituut aanwezig. Daarbij lijkt het

[3] CSR Advies 'Cybersecurity in onderwijs en bedrijfsleven' - Cyber Security Raad, november 2015 en CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' - Cyber Security Raad - april 2021
[4] 'Arbeidsmarkt voor Cyber Security Professionals', onderzoek in opdracht van het Wetenschappelijk Onderzoek- en Documentatie Centrum (WODC) Ministerie van veiligheid en Justitie., Platform Opleiding, Onderwijs en Organisatie B.V. (PLATO), Universiteit Leiden, december 2014
[5] Zie pagina 8 van Cyber Workforce Study, 2022, Cybersecurity Workforce Study (isc2.org)
[6] Zie voor een overzicht het European Cybersecurity Skills Framework – User Manual
European Cybersecurity Skills Framework (ECSF) - User Manual — ENISA (europa.eu)

snelgroeiende aanbod van commerciële partijen zeer divers en versnipperd en is de kwaliteit ervan onduidelijk.

2. **Ontwikkelingen in het vakgebied**
   Belangrijke praktische cybersecuritykennis ontwikkelt zich vooral in de private en publieke organisaties zelf, bijvoorbeeld op het gebied van risicomanagement, informatiedeling, incident response en nieuwe wetgeving. Deze kennis is niet vanzelfsprekend beschikbaar bij de opleidingsinstituten. De uitwisseling van nieuwe ervaringen en praktische kennis tussen bijvoorbeeld het bedrijfsleven, toezichthouders en universiteiten komt nog onvoldoende op gang, waardoor ook het onderwijsaanbod kwalitatief achterblijft. Dit geldt zowel voor het opleiden van nieuw cybersecuritytalent over de volle onderwijsbreedte (van mbo- en hbo-opleidingen tot universiteiten), als voor bijscholing van werknemers die al in het cybersecuritydomein actief zijn, of voor omscholing van werknemers die uit andere sectoren instromen.

3. **Docententekort**
   Er zijn niet genoeg geschikte opleiders om cybersecurityonderwijs te ontwikkelen en talent op te leiden. Specifiek zijn er te weinig hoogleraren die zich voldoende kunnen vrijmaken voor het geven en ontwikkelen van onderwijs, en het aantal lectoren groeit nauwelijks. Het bedrijfsleven leidt nu vaak zelf (pas afgestudeerde) nieuwe medewerkers op en schoolt ervaren personeel waar nodig zelf bij. Weliswaar is de private sector welwillend om met hun expertise bij te springen bij opleidingsinstituten, zoals eerder door de raad geadviseerd[3], maar ook dit leidt niet tot de vereiste volumes.

4. **Huidige sturing is onvoldoende**
   Verschillende *human capital agenda´s*, aanvalsplannen en een nationaal groeifondsvoorstel zijn inmiddels gelanceerd, vaak in publiek-private samenwerking. Deze zijn voornamelijk gericht op het tekort aan ICT´ers en werknemers in andere technische beroepen en richten zich bijvoorbeeld op het kweken van interesse voor bèta-opleidingen op middelbare scholen. Deze initiatieven zijn echter niet specifiek bedoeld om aan de toenemende vraag naar cybersecurityspecialisten te kunnen voldoen of zijn niet voldoende schaalbaar naar het nationale niveau. Bovendien kan het beoogde succes van initiatieven voor de technische/ICT-sector de potentie van meer werknemers voor cybersecurity verdringen. Tenslotte stuurt ook het ministerie van Onderwijs, Cultuur en Wetenschappen (OCW) niet specifiek op de ontwikkeling van cybersecurityonderwijs, maar richt het zich op generieke maatregelen voor bèta- en techniekopleidingen, in combinatie met het creëren van meer digitale geletterdheid.

5. **Problemen met kennismigratie**
   Als oplossing van de tekorten in technische/ICT-beroepen wordt vaak kennisimmigratie naar Nederland genoemd, of outsourcing van organisatieonderdelen naar het buitenland. Dergelijke bewegingen brengen extra risico´s met zich mee op het gebied van autonomie en kennisveiligheid. Hiervoor waarschuwde ook de Adviesraad voor Wetenschap, Technologie en Innovatie (AWTI) eerder dit jaar in een advies[7].

   Kennismigratie blijft desondanks hard nodig, maar zal ook geen sluitende oplossing kunnen bieden voor het tekort aan cybersecurityspecialisten. De raad ziet daarvoor drie belangrijke redenen:

[7] 'Kennis in conflict, veiligheid en vrijheid in balans', Adviesraad voor wetenschap, technologie en innovatie (AWTI), november 2022

- Nederlands talent wordt nu al herhaaldelijk weggekocht door de ons omringende landen, mede vanwege het wereldwijde tekort.
- In onderzoeksomgevingen maken het beperkte loopbaanperspectief, de hoge werkdruk en de gebrekkige financiering[8] het lastig om toponderzoekers uit het buitenland aan te stellen op Nederlandse universiteiten en hogescholen.
- Buitenlandse studenten, onderzoekers en andere cybersecurityspecialisten die wel naar Nederland komen, hebben vaak geen directe binding met ons land en de kans is groot dat ook zij na verloop van tijd weer emplooi zoeken in andere landen.

Opmerking: Er is sprake van om op universiteiten het Nederlands weer (gedeeltelijk) als primaire taal in te voeren. Voor het cybersecurityonderwijs zullen de problemen dan nog groter worden; het vakgebied heeft een internationale oriëntatie en is grotendeels Engelstalig. Veel van de bestaande docenten en onderzoekers hebben al een buitenlandse achtergrond, waarvoor geen Nederlandse vervangers te vinden zullen zijn.

Oplossingsrichtingen

Het tekort op de cybersecurityarbeidsmarkt zal in de komende periode een hardnekkig probleem blijven, dat niet met één enkele interventie te bestrijden is. Diverse raadsleden (publiek, privaat en wetenschap) zijn hierover met verschillende stakeholders in gesprek om de urgentie te benadrukken en oplossingsrichtingen te bespreken. De raad ziet daarbij de volgende mogelijkheden:

1. **Doorpakken op onderzoeksresultaten en bestaande onderwijsinitiatieven**
   De resultaten van de verschillende onderzoeken moeten leiden tot gerichte actie én investeringen. Alleen dan kan de toekomstige onderwijsontwikkeling in de benodigde vorm en omvang op gang komen en vraag en aanbod (oorzaak 1) beter op elkaar aansluiten. Centraal moet daarbij staan het multidisciplinaire karakter van cybersecurity, zowel voor opleiding van nieuw talent als voor omscholing en bijscholing. Bestaande, *bottom-up* initiatieven voor hoogwaardige cybersecurityopleidingen en trainingen moeten schaalbaar gemaakt worden. Voorbeelden hiervan zijn:

   - De succesvolle lancering van duale hbo-opleidingen, waar cybersecurityonderwijs en werken in het bedrijfsleven gecombineerd worden.
   - De nieuwe opzet van cybersecuritycursussen aan universiteiten. Deze richten zich op het bijscholen van al in het werkveld actief personeel, waarbij hooggeplaatste cybersecurityfunctionarissen vanuit overheid én bedrijfsleven doceren.
   - Het verzorgen van cybersecurityonderwijs voor studenten, door bedrijven gezamenlijk met universiteiten specifieke vakken te laten invullen.

2. **Omvorming van opleidingen**
   Onderwijsinstellingen moeten de inhoudelijke invulling van hun opleidingen beter afstemmen op de ontwikkelingen in het vakgebied (oorzaak 2). De huidige vorm van onderwijsontwikkeling is hiervoor doorgaans niet geschikt en van generieke onderwijsarchitecten kan dit ook niet worden verwacht. Het vergt specifieke expertise om dit onderwijs in samenwerking met bedrijven en overheden (waaronder ook toezichthouders) te ontwikkelen. Doelstelling hierbij is om onderwijsmodules te ontwikkelen, te testen in

[8] Deze factoren maken ook andere vormen van kennismigratie lastig. Er is bijvoorbeeld bij werknemers uit de industrie maar zeer beperkte interesse om later in hun loopbaan weer bij universiteiten en hogescholen in te stromen, terwijl dit juist andere oorzaken zoals de beperkte interactie met bedrijven zou kunnen terugdringen.

pilots en verder uit te rollen. Ook raden van bestuur (of raden van toezicht) van de betreffende instellingen zouden een dergelijke transformatie moeten stimuleren.

Om snel te kunnen reageren op veranderingen in het werkveld, kan gedacht worden aan *learning loops* om nieuwe *best practices* te ontwikkelen. Een andere mogelijkheid is om speciale *cybersecuritylabs* op te laten zetten door vertegenwoordigers uit het onderwijs, samen met specialisten uit het bedrijfsleven en de publieke sector, inclusief toezichthouders. Verschillende publiek-privaat gefinancierde regionale centra zijn hiervoor al in ontwikkeling.

3. **Specifieke aanstelling van docenten**
   De raad beveelt aan om specifieke lectoren en hoogleraren aan mbo´s, hbo's en universiteiten aan te stellen, die naast cybersecurityonderzoek ook naam willen maken met het ontwikkelen van succesvol cybersecurityonderwijs. Gezamenlijk krijgen zij daarbij de taak om - vanuit hun eigen vakgebied en onderzoeksdomein - het cybersecurityonderwijs te ontwikkelen en overkoepelend vorm te geven, met een bijbehorende financiële impuls.

   Hierdoor moet een nauwe samenwerking ontstaan over de verschillende vakgroepen heen en tussen de verschillende instituten. Deze docenten zouden door hun werkgever primair beoordeeld moeten worden op hun persoonlijke bijdrage aan de (instelling-overstijgende) onderwijsontwikkeling. Ook hierbij is het essentieel om private samenwerking op te zoeken, bijvoorbeeld via brancheorganisaties en op deze wijze ook extra docenten te werven (oorzaak 3). Deze docenten kunnen ook een belangrijke rol spelen in de onder punt 2 genoemde cybersecuritylabs.

4. **Gecoördineerde uitvoering van de acties**
   De tekorten zijn inmiddels zo groot dat geen enkele partij, sector of regio dit meer alleen kan oplossen. Er is niet alleen meer geld nodig; ook gecoördineerde sturing op bestaande initiatieven en gerichte acties voor het versterken van cybersecurityopleidingen (oorzaak 4) is nodig. In lijn met de doelstellingen van de NLCS op dit vlak, dienen de verschillende direct betrokken ministeries vanuit hun eigenaarschap de handen ineen te slaan met de onderwijsinstellingen en het bedrijfsleven, om de huidige situatie te doorbreken.

5. **Tegengaan van de *braindrain***
   Het is essentieel om de bestaande docenten van universiteiten en mbo- en hbo-opleidingen te blijven binden en boeien, ook in combinatie met het uitvoeren van hoogwaardig cybersecurityonderzoek en het leggen van de juiste connecties met het bedrijfsleven. Verbetering van het imago van onderwijs en onderzoek[9] zal daarvoor eveneens nodig zijn, los van meer aantrekkelijke arbeidsvoorwaarden. Alleen dan kan het vestigingsklimaat voor docenten en onderzoekers verbeteren en een verdere exodus naar het buitenland (of naar ons eigen bedrijfsleven) worden voorkomen (oorzaak 5).

   Dergelijke aanvullende maatregelen zijn ook noodzakelijk om kennismigratie te blijven bevorderen: het is hard nodig om buitenlandse docenten, onderzoekers én studenten die naar Nederland zijn gekomen te stimuleren om hier te blijven. Eén van de cruciale randvoorwaarden om dit te bewerkstelligen én de huidige toestroom niet verder te laten teruglopen, is het behoud van Engels als voertaal op universiteiten.

[9] Een gerelateerd imago-issue is dat veel bedrijven een beperkte toegevoegde waarde zien in het in huis hebben van promovendi, waardoor instroom in onderzoek en onderwijs voor pas afgestudeerden nog minder aantrekkelijk wordt.

Deze brief wordt ook gestuurd naar de minister van Onderwijs, Cultuur en Wetenschap, en in afschrift aan de ministers van Justitie en Veiligheid en Economische Zaken en Klimaat.

Hoogachtend,
Namens de Cyber Security Raad,

Pieter-Jaap Aalbersberg
Covoorzitter CSR

Theo Henrar
Waarnemend covoorzitter CSR