Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 **Informatie- en communicatietechnologie (ICT)**

29 544 **Arbeidsmarktbeleid**

Nr. 1164

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 maart 2024

Om de digitale weerbaarheid van Nederland te waarborgen is het kunnen beschikken over voldoende goed geschoolde cybersecurityprofessionals een essentiële voorwaarde. In de Nederlandse Cybersecuritystrategie 2022–2028[1] (NLCS) is als actiepunt opgenomen om in 2023 een verkennend onderzoek naar de kwalitatieve en kwantitatieve tekorten op de Nederlandse cybersecurity arbeidsmarkt uit te voeren, en met een voorstel te komen hoe deze tekorten op de cybersecurityarbeidsmarkt aangepakt kunnen worden. Om deze redenen heb ik op 19 juni 2023 Platform Talent voor Technologie (PTvT) de opdracht gegeven een onderzoek uit te voeren naar de kwalitatieve en kwantitatieve tekorten op de cybersecurityarbeidsmarkt. PTvT heeft het onderzoek in nauwe samenwerking met Dialogic uitgevoerd. Daarbij heb ik hen ook gevraagd om te komen met aanbevelingen hoe deze tekorten aangepakt zouden kunnen worden. Veel partijen uit het veld hebben meegewerkt aan de kwalitatieve dataverzameling en duiding van de resultaten. Met deze brief bied ik de onderzoeksresultaten en aanbevelingen aan en ga ik in op de eerste vervolgstappen die gezet zullen worden.

Belangrijkste uitkomsten van het onderzoek

Er is een groeiende vraag naar cybersecurity expertise te zien op de arbeidsmarkt.[2] De verwachting is dat deze vraag zal toenemen door o.a. Europese regelgeving. De groeiende vraag naar cybersecurity-specialisten richt zich met name op medior- en senior posities. Uit het uitgevoerde onderzoek is tevens gebleken dat er groeiende aandacht is voor cybersecurity in de mbo-, hbo-, en wo-opleidingen. Bij het mbo ligt de focus meer op het technische aspect van cybersecurity, terwijl de hbo- en wo-opleidingen een meer multidisciplinair karakter hebben. Tevens

[1] Kamerstuk 26 643, nr. 925

[2] Van circa 8.000 vacatures in 2018 naar 19.000 in 2022 (indicatief, zie bijlage 1: Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity, p. 36)

kst-26643-1164
ISSN 0921 - 7371
's-Gravenhage 2024

blijkt uit het onderzoek dat de afstemming tussen cybersecurity-opleidingen op verschillende onderwijsniveaus beperkt is, en er geen gezamenlijk beeld is over wat er wordt verstaan onder «cybersecurity-expertise». Dit bemoeilijkt de afstemming tussen de vraag aan personeel in de markt en het aanbod van professionals die worden opgeleid of getraind. Daarnaast laat het onderzoek zien dat er verschillende carrièrepaden zijn binnen het vakgebied en dat cybersecurity als domein constant in beweging is als gevolg van technologische en maatschappelijke ontwikkelingen. De cybersecurity vraagstukken van vandaag zijn anders dan die van tien jaar geleden. Dit betekent voor cybersecurityprofessionals dat zij zich een leven lang moeten blijven ontwikkelen.

Het totale ecosysteem van cybersecurity onderwijs en arbeidsmarkt is omvangrijk en divers. Zoals in het onderzoeksrapport staat beschreven gaat het op de arbeidsmarkt om verschillende typen expertise, een groot aantal verschillende (typen) organisaties en velerlei functieprofielen waarin cybersecurity-expertise geheel of gedeeltelijk een rol speelt. Door deze diversiteit is het essentieel om in de gehele onderwijsketen (primair onderwijs, voortgezet onderwijs, mbo, hbo, wo, Leven Lang Ontwikkelen (LLO)) meer aandacht te hebben voor cybersecurity. Al deze partijen samen vormen het ecosysteem van cybersecurity onderwijs en arbeidsmarkt, maar ervaren allen hun eigen uitdagingen en knelpunten.

Om deze uitdagingen het hoofd te bieden hebben PTvT en Dialogic twaalf aanbevelingen geformuleerd welke zijn gericht op het onderwijs, de arbeidsmarkt en het ecosysteem in zijn geheel:

1. Ontwikkel een gezamenlijke taal en gezamenlijk beeld met betrekking tot de «cybersecurity-expertise».
2. Breng gerichte coördinatie aan op de aansluiting tussen onderwijs- en arbeidsmarkt.
3. Spreek het volledige potentiële talent aan. Hierbij kan worden gedacht aan het potentieel van MBO-talent en bijvoorbeeld het beter aanspreken van diverse groepen zoals vrouwen.
4. Zoek de samenwerking op tussen en binnen regio's, sectoren en ketens.
5. Vergroot de zichtbaarheid en aantrekkelijkheid van «het beroep» van cybersecurityprofessional.
6. Stimuleer om-, bij- en nascholing ten behoeve van horizontale en verticale ontwikkeling.
7. Werk aan behoud van professionals met behulp van arbeidsmobiliteit binnen de sector.
8. Verbeter de startpositie van net afgestudeerden.
9. Vergroot de interesse voor studeren en werken in cybersecurity.
10. Versterk de kaders en het materiaal voor cybersecurity-onderwijs.
11. Betrek de arbeidsmarkt sterker in het onderwijs.
12. Versterken en vergroot de aantrekkelijkheid van het docentschap.

Vervolgstappen

Het onderzoek laat zien dat er een veelheid aan vraagstukken is die verspreid zijn over de gehele keten van onderwijs en arbeidsmarkt. Er zal dan ook geen one-size-fits-all-oplossing zijn die alle deelproblemen gaat oplossen. Daar is een nauwe samenwerking voor nodig tussen partijen uit het onderwijsveld, bedrijfsleven, maatschappelijk middenveld en overheid.
Daarnaast is cybersecurity niet uitsluitend een technisch vraagstuk. Naast de behoefte aan ICT-geschoold personeel zijn ook professionals nodig met kennis vanuit andere disciplines om bijvoorbeeld de vertaalslag te kunnen maken van de techniek naar de bestuurskamer en naar de samenleving. Tegelijkertijd hangt het tekort naar cybersecurityprofessionals samen met

de algehele krapte op de arbeidsmarkt voor andere beroepen. De nulmeting van de NLCS door het Wetenschappelijk Onderzoek en Documentatie Centrum (WODC) signaleert dit ook.[3]

Tevens wordt in het kader van de Human Capital Agenda ICT (HCA ICT)[4] gewerkt aan het aanpakken van arbeidsmarkttekorten in het gehele digitale domein. Desalniettemin laat het onderzoek van PTvT en Dialogic zien dat er specifiek ruimte is voor verbetering in het cybersecurity-domein.

Ik neem de aanbevelingen over en ga ermee aan de slag met het veld en met de betrokken ministeries zoals het Ministerie van Onderwijs Cultuur en Wetenschap (OCW), het Ministerie van Sociale Zaken en Werkgelegenheid (SZW), het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en het Ministerie van Justitie en Veiligheid (JenV). Op basis van de aanbevelingen zullen de volgende initiële vervolgstappen worden ingezet.

1. Opzetten programmalijn cybersecurity binnen de Human Capital Agenda ICT

Om uitvoering te geven aan de twaalf aanbevelingen uit het onderzoek wordt binnen de Human Capital Agenda ICT HCA ICT een meerjarige eigenstandige cybersecurity programmalijn opgezet. De HCA ICT, uitgevoerd door PTvT, is één van de drie netwerkverbanden die zijn verbonden aan het Actieplan Groene en Digitale Banen.[5] PTvT en dcypher (publiek-private samenwerkingsplatform cybersecurity kennis en innovatie)[6] krijgen de opdracht om invulling te geven aan- en regie te voeren op de uitvoering van deze cybersecurity programmalijn. De stakeholders in het cybersecurityveld zullen hierbij nauw worden betrokken. Door de cybersecurity programmalijn een plek te geven onder de vlag van de HCA ICT, die weer verbonden is met het Actieplan Groene en Digitale banen, benutten we het bestaande netwerk, expertise en ervaringen op onderwijs- en arbeidsmarktvraagstukken ook ten gunste van het cybersecuritydomein en ontstaat samenhang van beleid en synergie van acties. De partijen die zijn aangesloten bij de HCA ICT ondernemen vaak ook activiteiten op het gebied van cybersecurity en talent. Zo bouwen we voort op bestaand beleid, gaan we versnippering tegen en bundelen we de krachten om de tekorten op de arbeidsmarkt het hoofd te bieden. Middels deze aanpak wordt tevens invulling gegeven aan aan de ingezette koers op dit thema in het actieplan van de NLCS.

Parallel aan de bovengenoemde actie om de aanbevelingen gezamenlijk met het veld op te pakken en om te zetten in concrete vervolgacties, zal ik alvast starten met de volgende acties:

---

[3] Kamerstuk 26 643, nr. 1128

[4] Kamerstuk 29 544, nr. 1173

[5] Kamerstuk 29 544, nr. 1173. De overige twee netwerkverbanden zijn de Techniekpact en Taakgroep Arbeidsmarkt en Scholing. HCA ICT richt zich op het digitale banen domein van het Actieplan Groene en Digitale Banen.

[6] Het publiek-private samenwerkingsplatform dcypher faciliteert de verbinding tussen overheid, bedrijven en kennisinstellingen en draagt zorg voor de agendering en programmering van cybersecurity kennis- en innovatie projecten en werkprogramma's (bron: Nederlandse Cybersecuritystrategie 2022–2028, pijler II).

2. Het vergroten van inzicht in en overzicht van de cybersecurity arbeidsmarkt

Voor het onderzoek hebben PTvT en Dialogic veel relevante informatie en data verzameld over de huidige stand van het cybersecurityonderwijs en de arbeidsmarkt. Deze informatie zal online worden ontsloten en worden bijgehouden in de vorm van netwerkkaarten en dashboards. Inzicht in de vraag naar cybersecurityspecialisten is noodzakelijk voor het gerichter inzetten van bestaande activiteiten, en/of het initiëren van nieuwe activiteiten. Kennis van succesvolle initiatieven is wenselijk om van elkaar te kunnen leren en initiatieven op te schalen. Anderzijds kunnen hiaten worden gesignaleerd en nieuwe publiek-private samenwerkingen worden opgebouwd. Dit voldoet ook in een behoefte van meerdere partners die betrokken waren bij de uitvoering van het onderzoek en geeft ook invulling aan een actie uit het actieplan NLCS. Hiermee bevorderen wij een gezamenlijke informatiepositie over bijvoorbeeld welke cybersecurity-opleidingen er in Nederland beschikbaar zijn en ontsluiten we vacature-analyse data middels dashboards. Om versnippering tegen te gaan zal waar mogelijk worden aangesloten op bestaande netwerkkaarten of vacature-dashboards die verbonden zijn aan het Actieplan Groene en Digitale banen.[7]

3. NWO-call versterken samenwerking kennisinstellingen en bedrijfsleven

In afstemming met het veld zal via NWO (Regieorgaan SIA) een subsidiecall worden opgezet om via praktijkgericht onderzoek de samenwerking te stimuleren tussen kennisinstellingen (mbo, hbo, wo), het bedrijfsleven en overheidsorganisaties. Die samenwerking kan voordelen bieden, de arbeidsmarkt kan namelijk een belangrijke rol spelen in het bieden van expertise die binnen de opleidingen benodigd is om studenten adequaat op te leiden en tegelijkertijd komt de arbeidsmarkt hiermee direct in aanraking met jong talent. De call draagt tevens bij aan actuele onderwijsvorming en de samenwerking tussen kennisinstellingen onderling. Tevens zal dit bijdragen aan de verbetering van de startpositie van net afgestudeerd talent. Daarmee kunnen alvast een aantal aanbevelingen uit het PTvT en Dialogic-onderzoek worden opgepakt, namelijk ten aanzien van1) de aansluiting tussen onderwijs- en arbeidsmarkt, 2) het verbeteren van de startpositie van net afgestudeerd talent en 3) het betrekken van arbeidsmarkt in onderwijsvorming. Deze actie draagt tevens bij aan pijler twee van het Actieplan Groene en Digitale banen dat zich richt op behoud en instroom van digitaal talent (in dit geval specifiek cybersecurity talent) op de Nederlandse arbeidsmarkt.[8] Dit instrument wordt momenteel nader vormgegeven in afstemming met het veld en zal naar verwachting eind 2024/begin 2025 open worden gesteld.

Tot slot

De bovengenoemde vervolgstappen zijn de éérste stappen in een traject van lange adem. Met de geschetste acties creëren we randvoorwaarden voor concrete activiteiten en initiatieven die leiden tot meetbare verbetering in de kwalitatieve en kwantitatieve tekorten op de cybersecurityarbeidsmarkt. Het gehele ecosysteem, bestaande uit het onderwijs, bedrijfsleven, maatschappelijk middenveld en de overheid, draagt een gezamenlijke verantwoordelijkheid voor het versterken van de cybersecurityarbeidsmarkt in Nederland. Het vraagstuk kan alleen samen worden opgelost. Ik doe daarom een oproep aan het ecosysteem om zich achter deze aanpak te scharen en gezamenlijk aan het vervolg te werken. Ik zet

[7] Kamerstuk 29 544, nr. 1173
[8] Kamerstuk 29 544, nr. 1173

mij samen met andere ministeries in om het veld bij elkaar te brengen om gezamenlijk acties en initiatieven op te zetten die leiden tot meer cybersecurityprofessionals, en daarmee een digitaal veiliger Nederland. U zult verder worden geïnformeerd over de voortgang van deze acties via de voortgangsbrieven van de Nederlandse Cybersecurity Strategie (NLCS) en de Strategie Digitale Economie.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens