

# Samenvatting

## ***Aanleiding en doel van het onderzoek***

Een tekort aan Cyber Security Professionals (CSP's) is een grote kwetsbaarheid voor de weerbaarheid van de vitale sectoren. In de "Nationale Cybersecurity Strategie 2 (NCSS2): Van bewust naar bekwaam" (2013) wordt benadrukt dat het Kabinet over voldoende cybersecuritykennis en -kunde wil beschikken. In dit kader is het van belang dat er op de korte en op de (middel)lange termijn evenwicht is tussen vraag en aanbod op de arbeidsmarkt voor CSP's binnen de publieke en private organisaties. Daarom wil de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) inzicht krijgen in de aard en omvang van een (eventueel) tekort aan deze professionals (zowel technisch als niet technisch) en oplossingsrichtingen identificeren om deze eventuele tekorten op korte en (middel)lange termijn te reduceren. In dit kader heeft PLATO BV van de Universiteit Leiden in samenwerking met Ockham IPS een arbeidsmarktonderzoek uitgevoerd naar vraag en aanbod van Cyber Security Professionals. Dit onderzoek is uitgevoerd in opdracht van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (WODC).

## ***Onderzoeksvragen***

In dit onderzoek staan de volgende onderzoeksvragen centraal:

- In hoeverre is er, nu en in de toekomst, een mogelijk kwalitatief en kwantitatief tekort aan Cyber Security Professionals op hoger en middelbaar niveau te verwachten?
- Hoe kunnen deze tekorten op de huidige en toekomstige arbeidsmarkt voor Cyber Security Professionals worden opgelost?

## ***Onderzoekopzet en –aanpak***

De arbeidsmarkt voor CSP's wordt in dit onderzoek benaderd als een domein waar de vraag naar en het aanbod van professionals op het terrein van cybersecurity samenkomen en elkaar (proberen te) vinden. Bij het verkrijgen van inzicht over de vraagkant ligt in dit onderzoek het accent op vacature-analyse. Wat betreft de aanbodkant spitst het onderzoek zich toe op het onderwijs- en opleidingsaanbod.

Om vanuit verschillende relevante invalshoeken en bronnen antwoord te krijgen op de onderzoeksvragen, zijn ook andere methoden gebruikt. Het onderzoek bestond uit de volgende (deels overlappende) componenten:

- Literatuuronderzoek naar cybersecurity, het werkveld, kenmerken en functieprofielen van CSP's. Dit betrof beleidsliteratuur en wetenschappelijke literatuur zowel Nederlandse als internationale literatuur.
- Analyse van de maatschappelijke context en ontwikkelingen (politiek, economisch, sociaal, technologisch en juridisch) die van invloed zijn op de vraag naar en het aanbod van CSP's.
- Vacature-onderzoek (met behulp van vacaturespider Jobfeed<sup>1</sup> van Textkernel).
- Inventarisatie en analyse van het onderwijs- en opleidingsaanbod en inventarisatie van aantallen studenten. In dit kader is internetresearch uitgevoerd en zijn 18 onderwijsaanbieders geraadpleegd (door middel van 18 interviews, deels face-to-face en deels telefonisch).
- Verkennende en verdiepende interviews (deels face-to-face en deels telefonisch) met werkgevers, werknemers in het private en publieke domein. Hierbij ging het in totaal om 34 interviews verspreid over 25 organisaties.
- Expertmeeting. Deze bijeenkomst werd gehouden in de afrondende fase van het onderzoek, met als doel de gevonden discrepanties tussen vraag en aanbod en

---

<sup>1</sup> <http://www.jobfeed.nl/>

oplossingsrichtingen te bespreken. Bij de expertmeeting waren 7 deelnemers uit deze verschillende organisaties betrokken.

### **Cybersecurity**

Cybersecurity is geen eenduidig begrip. Bij in de literatuur gevonden definities van cybersecurity ligt vaak een accent op informatiebeveiliging en ICT. Cybersecurity moet niet te beperkt worden opgevat. Het begrip cybersecurity refereert aan de kwetsbaarheid van bedrijven, burgers, overheid en de maatschappij als geheel. Aan deze kwetsbaarheden en het oplossen daarvan, zitten zowel technische ICT-aspecten als interactie-aspecten (mens-ICT). Dit maakt cybersecurity niet alleen een technisch ICT-vraagstuk, maar vooral ook een organisatievraagstuk.

*Conclusies 1: Cybersecurity is zowel een ICT- als een organisatievraagstuk. Cybersecurity moet vooral ook bekeken worden vanuit een breder organisatieperspectief waarin verschillende rollen en taken te vervullen zijn.*

### **Het werkveld van Cyber Security Professionals**

Het werkveld van de Cyber Security Professionals is sterk onderhevig aan veranderingen. De snel veranderende digitale wereld met daarbij komende dreigingen en noodzakelijke veiligheidscriteria stelt hoge eisen aan publieke en private organisaties om cybersecure te zijn of te worden. Zowel de frequentie van incidenten, als de impact daarvan, in termen van directe schade en indirecte schade (bijvoorbeeld imagoschade), neemt toe. Bedrijven en publieke organisaties worden zich meer en meer bewust van het feit dat cybersecurity niet alleen een ICT-issue is, maar een integraal thema. Cybersecurity is van een ICT-vraagstuk een 'boardroom issue' geworden, want het voortbestaan van het bedrijf kan in het geding komen. Toenemende beleidsaandacht voor cybersecurity, de noodzaak zich bewust te zijn van de risico's (aangezien internet zich op alle terreinen van het dagelijkse leven manifesteert) en veranderingen in wetgeving (op het gebied van privacy en dataprotectie) hebben een extra stuwend effect op de vraagontwikkeling.

*Conclusie 2: Twee factoren houden het werkveld van de Cyber Security Professional sterk in beweging. Enerzijds gaat het hierbij om maatschappelijke ontwikkelingen (op politiek, economisch, sociaal, technisch en juridisch terrein). Anderzijds vragen incidenten (afhankelijk van frequentie en impact) om aanpassingen in het werkveld.*

### **Functiegroepen**

In de literatuur komen drie dimensies naar voren waarmee functies van Cyber Security Professionals kunnen worden beschreven:

- Werkzaamheden kunnen als *technisch dominant* of als *niet technisch dominant* worden getypeerd. Technisch dominant wil zeggen dat de nadruk ligt op het ICT-perspectief. Bij niet technisch dominante functies staat het organisatieperspectief meer centraal.
- De functie kan *specifiek op cybersecurity gericht* zijn of *cybersecurity als onderdeel* hebben.
- De functie kan *operationeel-tactisch* of *tactisch-strategisch* georiënteerd zijn.

Op basis van deze dimensies en bestudering van vacatureteksten kunnen vier groepen van functies worden onderscheiden:

- 1) *Technisch dominante specialistische cybersecurityfuncties*. Deze functies zijn zeer specifiek op IT/informatiebeveiliging gericht en hebben een grote technische component. Voorbeelden van functies zijn: ethical hackers, penetratietesters, software testers en technical security-engineers.

- 2) *Niet technisch dominante specialistische cybersecurity functies.* Hierbij gaat het om cybersecurityspecialisten die meer vanuit een organisatieperspectief naar security kijken. Voorbeelden van functies zijn: IT security officers, IT security specialists, security officers, Information security officers, informatiebeveiligers.
- 3) *Technisch dominante functies waarbij cybersecurity een onderdeel is.* Deze beroepen zijn technisch van aard, maar niet gespecialiseerd in cybersecurity. Het betreft een brede groep beroepen waarvoor veelal een cybersecurity-gerelateerd certificaat vereist is of als pré wordt aangemerkt. Voorbeelden van functies zijn: systeembeheerders, softwareontwikkelaars en architecten.
- 4) *Niet technisch dominante functies waarbij cybersecurity een onderdeel is.* Dit is de minst afgebakende functiegroep. Hierin bevinden zich tal van functies zoals beleidsmedewerkers, juristen, directeuren, auditors. Bij deze functies kan cybersecurity onderwerp van de kernactiviteit zijn (bijvoorbeeld jurist in privacy-issues, beleidsmedewerker op het gebied van cybersecurity). Daarnaast gaat het om functies waarin cyber eerder als object van een ander domein wordt gezien (bijvoorbeeld object van beleid, rechtspraak) dan als kern van de werkzaamheden.

Het onderscheid operationeel-tactisch en tactisch-strategisch komt in alle vier de functiegroepen terug

*Conclusie 3: Op basis van de literatuur en bestudering van vacatureteksten, worden voor de Cyber Security Professional vier functieprofielen onderscheiden die in het kader van arbeidsmarktonderzoek gebruikt kunnen worden:*

- *technisch dominante specialistische cybersecurityfuncties;*
- *niet technisch dominante specialistische cybersecurityfuncties;*
- *technisch dominante functies waarbij cybersecurity een onderdeel is;*
- *niet technisch dominante functies waarbij cybersecurity een onderdeel is.*

### **De vraag naar en totale werkgelegenheid voor Cyber Security Professionals**

In de eerste drie kwartalen van 2014 zijn in totaal 916 vacatures gepubliceerd met betrekking tot het cybersecuritydomein. Op jaarbasis (gerekend over het laatste kwartaal van 2013 en de eerste drie kwartalen van 2014) gaat het om 1.158 gepubliceerde vacatures op het gebied van cybersecurity. De totale vraag zal groter zijn, omdat informele wervingskanalen en challenges<sup>2</sup> gericht op werving niet als vacatures tellen in de vacature-analyse.

Om een indruk te krijgen van de totale werkgelegenheid (het totaal aantal arbeidsplaatsen) op het gebied van cybersecurity maken we een vergelijking met de aantallen gepubliceerde vacatures en de werkgelegenheid in de brede ICT-sector. In de brede ICT-sector staat één vacature tot zes arbeidsplaatsen.<sup>3</sup> Passen we deze zelfde verhouding tussen vacatures en arbeidsplaatsen toe op het cybersecuritydomein, dan wordt op basis hiervan de totale werkgelegenheid binnen het cybersecuritydomein geschat op 7.000 arbeidsplaatsen.

Op basis van de omgevingsanalyse (het maatschappelijk belang en de rol van incidenten nemen toe, zie conclusie 2) wordt verwacht dat de vraag naar Cyber Security Professionals zal stijgen. Enerzijds neemt de urgentie van het inzetten van kennis en kunde op dit terrein toe. Anderzijds wordt het cybersecuritydomein steeds meer ook als een organisatievraagstuk gezien en breder opgevat (multidisciplinair).

<sup>2</sup> Een 'challenge' wordt in dit onderzoek omschreven als een uitdagende wervingsactiviteit met een *gaming* karakter, waarbij vraagstukken op het terrein van cybersecurity moeten worden opgelost.

<sup>3</sup> In 2013 was de totale werkgelegenheid in de ICT/automatisering ongeveer 300.000 (Panteia op basis van P-Direkt en Enquête beroepsbevolking, CBS). Het totaal aantal vacatures op jaarbasis is ongeveer 50.000 (Panteia/PLATO op basis van vacatureanalyse Jobfeed). De verhouding tussen het aantal vacatures en de totale werkgelegenheid is daarom 1 : 6.

De verwachte stijging van de vraag geldt voor alle vier de functiegroepen en ook voor aanpalende functies: Het cybersecuritydomein is een belangrijk deel van de leefwereld en daarom zijn verschillende aanpalende functies nodig waarin kennis van cybersecurity onontbeerlijk is.

Er moet onderscheid worden gemaakt in de vraag naar functies op MBO-, HBO- en WO-niveau. Door digitalisering en automatisering neemt de vraag naar MBO-opgeleiden binnen de ICT af, de vraag naar hoger opgeleiden neemt juist toe.

*Conclusie 4: Weliswaar is het aantal zichtbare vacatures momenteel nog bescheiden, echter er zijn indicaties (toename van de urgentie en bredere opvatting van het cybersecuritydomein) dat de vraag naar CSP's (in zijn totaliteit) in de toekomst zal toenemen. Deze stijging geldt vooral voor hoger opgeleiden en in mindere mate voor op MBO-niveau opgeleide professionals.*

De aard van de vraag naar de vier in dit onderzoek onderscheiden functiegroepen laat zich als volgt typeren:

- 1) *Technisch dominante specialistische cybersecurityfuncties.* De arbeidsmarkt voor dit profiel wordt, naast grote werkgevers (zowel banken, politie en defensie) gedomineerd door consultancybedrijven. Deze specialisten (hackers, pentesters) delen met cybercriminelen de rol van 'front-runner' in de ontwikkeling van cybersecurity. Om de verdere technologische ontwikkeling van cybercrime bij te benen, zal de vraag naar deze specialisten aanhoudend stijgen.
- 2) *Niet technisch dominante specialistische cybersecurityfuncties.* De arbeidsmarkt voor dit functieprofiel kent een gedifferentieerder palet aan vragende organisaties. Het aanstellen van dit type CSP is voor veel organisaties de eerste stap in het op orde brengen van de cybersecurity. In veel gevallen is één CSP voldoende om de security te organiseren. Specialistische taken worden via inhuur van derden uitgevoerd. Na een sterke groei in de eerste vijf jaar zal de vraag naar niet technische dominante cybersecurityfuncties licht dalen, doordat organisaties hun beveiliging in de organisaties hebben ingebed. Tegen die tijd zal echter de vervangingsvraag ook een rol gaan spelen omdat mensen met pensioen gaan. In vacatures met betrekking tot deze groep functies wordt om professionals met ervaring gevraagd.
- 3) *Technisch dominante functies waarbij cybersecurity een onderdeel is.* In de arbeidsmarkt voor dit functieprofiel wordt de grootste groei verwacht. Deze markt wordt bepaald door software-ontwikkelaars. Deze bedrijven zijn zich de laatste jaren gaan toeleggen op verbeterde beveiliging van hun software (secure by design) en vragen ICT'ers met ervaring op het terrein van security, securitycertificaten en/of -affiniteit. Aangezien meer en meer organisaties als softwarebedrijven gezien kunnen worden (ICT is de kern van veel bedrijven), neemt de vraag naar deze technici in de toekomst toe. De vraag naar veiligere systemen weerklinkt in de systeemontwikkeling en systeembeheersing.
- 4) *Niet technisch dominante functies waarbij cybersecurity een onderdeel is.* De arbeidsmarkt voor dit functieprofiel kent een veelheid aan verschillende functies, waarbij sommige professionals niet eens beseffen dat zij zich bezighouden met cybersecurity. In de toekomst zullen vaker en nadrukkelijker competenties ten aanzien van cybersecurity-gerelateerde taken worden gevraagd.

*Conclusie 5: Een stijging van de vraag geldt voor alle functiegroepen, maar de grootste groei wordt verwacht bij de technisch dominante functies waarbij cybersecurity een onderdeel is.*

### **Aanbod van Cyber Security Professionals vanuit onderwijs en opleiding**

Er zijn in dit onderzoek ruim tachtig soorten aanbod geïnventariseerd. Als het aantal

aanbiedingslocaties daarin wordt verwerkt, gaat het om vele honderden opleidingen en andere vormen van aanbod. Het opleidingsaanbod gerelateerd aan cybersecurity is zeer divers en omvangrijk. Er bestaan veel aanbiedingsvormen naast elkaar, zoals initiële opleidingen, post-initieel onderwijs, korte cursussen, masterclasses, workshops, seminars, on the job leren, afstandsonderwijs, en in-company training.

De opleidingen worden op talrijke locaties aangeboden. Er zijn initiële en post-initiële opleidingen van MBO- tot WO-niveau. Ook in de private sector is het aanbod groot. Hierbij ligt een accent op het up-to-date houden van kennis en vaardigheden van werkenden.

Ook voor wat betreft inhoud en diepgang is de range van het aanbod breed. Deze bestrijkt opleidingen met duidelijke technische en informatica-inhouden én opleidingen met duidelijke veiligheids-, juridische, of forensische inhouden. Ook zijn er opleidingen die deelnemers indirect, maar diepgaand scholen in voor cybersecurity relevante vakken en competenties. In die categorie vallen opleidingen die een sterke ICT-component hebben maar gericht zijn op andere dan technische- of veiligheidsgebieden, zoals kunstmatige intelligentie, studies methoden en technieken, medische informatiekunde, logistiek, meet- en regeltechniek, etc. Al met al is er een veel breder aantal opleidingen dat aan de kennis en kunde van studenten/deelnemers bijdraagt, dan alleen de direct op ICT-, of internet- en cybersecurity gerichte opleidingen.

De veelheid aan opleidingen, cursussen en aanbiedingsvormen leidt ook tot intransparantie van het aanbod. Informatie over onderwijs- en opleidingstrajecten is op zich wel te achterhalen, maar wat ontbreekt is één helder overzicht van de opleidingsmogelijkheden en -routes in relatie tot de competenties waarvoor deelnemers willen en/of moeten worden opgeleid.

*Conclusie 6: Het opleidingsaanbod gerelateerd aan cybersecurity is divers en omvangrijk. Opleidingen worden vaak op verschillende locaties aangeboden en er is veel variatie in aanbiedingsvormen. Tegelijkertijd is het aanbod weinig transparant.*

Wat betreft het aanbod van professionals vanuit onderwijs en opleiding, lijken er in 2014 ruim voldoende deelnemers in een relevante vooropleiding te zitten:

- een instroom van 6.880 deelnemers op MBO 4 niveau;
- een instroom van 73 deelnemers op HBO associate degree niveau;
- een instroom van 4.053 deelnemers op HBO niveau;
- een instroom van 292 deelnemers op Master niveau;
- een instroom van deelnemers aan post-academische- en post-executive masters van (zoals blijkt uit de interviews) zeker 200 personen.

Er is dus een groot potentieel aan mensen die in principe inzetbaar lijken. Zelfs als we rekening houden met een uitval van 50%, blijven de aantallen nog hoog in vergelijking met de beschikbare vacatures. Tegelijkertijd leiden deze aantallen maar zeer beperkt tot instroom in cybersecurity-gerelateerde functies. MBO'ers vervolgen hun opleiding vaak op HBO-niveau. Veel bredere HBO- en WO-opleidingen hebben cybersecurity maar beperkt in het programma ingebouwd en er zijn (nog) weinig specialistische cybersecurityopleidingen. Dit leidt ertoe dat studenten niet of pas relatief laat cybersecurity als optie meenemen in hun overwegingen ten aanzien van hun verdere studie of loopbaan.

*Conclusie 7: Het opleidingspotentieel is in principe toereikend om te voorzien in de vraag naar CSP's. Het is echter de vraag of deelnemers aan cybersecurity-gerelateerde opleidingen cybersecurity als loopbaanoptie zien.*

### ***Gevonden discrepanties tussen vraag en aanbod***

Gevonden discrepanties bij onderzoeksvraag 1: In hoeverre is er, nu en in de toekomst, een mogelijk kwalitatief en kwantitatief tekort aan Cyber Security Professionals op hoger en middelbaar niveau te verwachten?

In de relatie van de vraag naar en het aanbod van CSP's zijn eerder intransparanties en kwalitatieve discrepanties te constateren dan kwantitatieve discrepanties. De opgave lijkt niet zozeer te zijn om meer mensen op te leiden, maar veeleer om hen tijdens hun opleiding te interesseren voor cybersecurity en voor banen in die sector. De aansluitingsproblemen (discrepanties tussen vraag en aanbod) die organisaties ervaren, zijn eerder van kwalitatieve dan van kwantitatieve aard of te wijten aan intransparantie van de arbeidsmarkt. Samengevat komen de volgende discrepanties naar voren:

- Studenten worden weliswaar opgeleid in voor cybersecurity relevante studierichtingen, maar zij missen een specifieke gerichtheid op cybersecurity.
- Veel organisaties hebben onvoldoende kennis over wat zij eigenlijk nodig hebben, wie ze precies zoeken en waar ze die kunnen vinden.
- Er is voldoende aanbod, maar de professionals hebben nog niet het gewenste niveau: zij missen (afhankelijk van de functie en de taken) òf technische kennis òf kennis van de organisatie.
- Professionals hebben cybersecurity als deeltaak erbij gekregen, maar zijn niet specifiek opgeleid op dat terrein. Omdat zij veel andere taken hebben ligt snelle competentie-ontwikkeling op het terrein van cybersecurity ook niet altijd voor de hand.

*Conclusie 8: In kwantitatieve zin hoeft er geen sprake te zijn van tekorten. De aansluiting van de vraag naar CSP's en het aanbod van deze professionals wordt gehinderd door intransparanties en kwalitatieve discrepanties.*

### ***Oplossingsrichtingen bij de gevonden discrepanties***

Hierbij gaat het om de beantwoording van onderzoeksvraag 2: Hoe kunnen (eventueel) geconstateerde tekorten op de huidige en toekomstige arbeidsmarkt voor Cyber Security Professionals worden opgelost? Met andere woorden: Hoe kan de match tussen vraag en aanbod worden verbeterd? In het onderzoek komen de volgende (mede door experts op het terrein van cybersecurity benadrukte) oplossingsrichtingen naar voren:

#### *1. De mogelijkheden van het onderwijs benutten bij het oplossen van discrepanties.*

Het onderwijs kan een grote rol spelen bij het oplossen van discrepanties. Het gaat daarbij om het bevorderen van bewustzijn onder leerlingen en studenten in het algemeen, het motiveren tot voor cybersecurity relevante studiekeuzes bij een deel van de leerlingen en studenten en het gericht, zelfs specialistisch, opleiden van een nog specifiekere groep. Leren en professionaliseren in een zich snel ontwikkelend veld als de cybersecurity vereist bij uitstek een vorm van een leven lang leren. In het kader van een leven lang leren is het van belang, ook te zoeken naar efficiënte en effectieve manieren om in werksituaties de kennis verder te ontwikkelen, te delen en te vertalen in verbeteringen en innovaties. De werkomgeving strekt verder dan alleen de eigen organisatie.

Behalve professionalisering in de zin van persoonlijke ontwikkeling in het beroep, is er ook de noodzaak van ontwikkeling van het vak. Cybersecurity is een terrein waar op verschillende niveaus, veel werk wordt verricht in allerlei publieke en private organisaties (van klein tot groot) en industrieën. Ook de opleidingswereld draagt bij aan de ontwikkelingen in het cybersecuritydomein. Samenwerking van alle betrokken partijen is van vitaal belang voor het 'up to date' blijven van de cybersecuritysector en allen die daarin werkzaam zijn. We zien dit vertaald in actieve betrokkenheid van ICT-bedrijven in

opleidingen, in deelname van practici als docenten in hogere opleidingen, en in participatie van wetenschappers in het oplossen van praktische problemen.

*2. Veranderen van werkprocessen in organisaties en samenwerking tussen organisaties, om zodoende het niveau van cybersecurity op peil te brengen en te houden.*

In het onderzoek in zijn totaliteit komen op dit vlak de volgende mogelijkheden naar voren:

- gelegenheid creëren binnen en tussen organisaties om kennis te delen en van elkaar te leren;
- verbeteren van secundaire arbeidsvoorwaarden, wat het werk voor meer groepen zoals vrouwen, extra aantrekkelijk kan maken;
- efficiënter en gericht werven (ook binnen de eigen organisatie, door functionarissen opmerkzaam te maken op de mogelijkheden om door te groeien in een cyber cybersecurity-gerelateerde functie);
- inzet van een pool van professionals vanuit verschillende organisaties, outsourcing en inhuren van externe specialisten;
- zichtbaar maken van het werk van de CSP binnen de organisatie en het nut daarvan;
- hanteren van een minder hiërarchische organisatiestructuur (geldt voor grotere organisaties).

*3. Verhelderen van onderwijs- en opleidingsroutes.*

De relatie tussen opleidingstrajecten en -routes, te verwerven competenties, uit te oefenen functies en te bereiken posities op de arbeidsmarkt is diffuus. De trajecten die loopbaanontwikkeling in de cybersecurity ondersteunen zijn dat ook. Keuzes maken in het woud van mogelijkheden is niet altijd eenvoudig. Daar ondervinden zowel de mensen die het aangaat als de organisaties de nadelen van. Het betekent dat te vaak de juiste man of vrouw op de verkeerde plek belandt. Het leidt tot inefficiënte en ineffectieve leer- en loopbaanroutes. Het verhelderen van de onderwijs- en opleidingstrajecten en -routes, zal een positieve uitwerking hebben op de kwaliteit van het aanbod en de toeleiding van uitstromende deelnemers en studenten naar functies op het terrein van cybersecurity.

Deze oplossingsrichting verwijst ook naar een leven lang leren. Het werkveld van cybersecurity vraagt om permanente actualisering van kennis en het 'up to date' houden van vaardigheden. In dat kader groeit de noodzaak om gestalte te geven aan een systeem van onderhoud van kennis, actualisering van kennis en kennisontwikkeling.

*4. Monitoren van ontwikkelingen in de samenleving, het onderwijs en opleidingen en arbeidsmarkt. De hierdoor verkregen gegevens kunnen de aansluiting van de vraag naar en het aanbod van CSP's op de korte en (middel)lange termijn ten goede komen.*

In het verlengde van oplossingsrichting 3 kan dataverzameling en registratie over opleidingen en de vraag op de arbeidsmarkt een bruikbaar middel voor kwaliteitsverbetering zijn. Het onderzoek naar de arbeidsmarkt voor Cyber Security Professionals, zoals beschreven in dit rapport, biedt een stand van zaken. De samenleving in zijn totaliteit en het werkgebied van de CSP's zijn sterk in beweging. Een vorm van monitoring van ontwikkelingen in de samenleving, de arbeidsmarkt en de opleidingsmarkt kan de aansluiting van de vraag naar en het aanbod van CSP's op de kortere en langere termijn ten goede komen.

*5. Het imago van het cybersecuritywerkveld en de -functies sterker en uitdagender neerzetten.*

Cybersecurityfuncties worden nog al eens geassocieerd met een bepaald soort ethical hackers die volledig opgaan in hun vak (zwart T-shirt, paardenstaart etc.). Aan de andere kant worden cybersecurityfuncties in verband gebracht met 'moeilijkdoeners binnen de organisatie': immers door hun oriëntatie op alles wat er mis kan gaan, zijn zij in de ogen van anderen wel een beetje moeilijk. De uitdagende, vooruitstrevende, en complexe aspecten van het werk mogen meer op de voorgrond worden gebracht. Een andere kwestie is dat de sector vooral uit mannen bestaat. Op het terrein van cybersecurity zijn

verschillende functies te vervullen waarbij verschillende soorten competenties vereist zijn. Dat maakt het werkveld interessant voor mannen en vrouwen. Een positieve uitstraling van de mogelijkheden en uitdagingen maakt de vijver waaruit kan worden gevist groter. Voorlichting, scholing en eventueel publieksacties (bijvoorbeeld in de vorm van challenges) kunnen ook bijdragen aan verandering.

*6. Cybersecurity oppakken als een gezamenlijke verantwoordelijkheid van burgers, overheid, organisaties en onderwijs: gericht op bewustwording.*

Alle geraadpleegde organisaties en deskundigen zijn het erover eens: cybersecurity is een kwestie die het leven van vrijwel iedere burger beïnvloedt. Daarom is het belangrijk om gericht op de hele samenleving, te werken aan bewustwording. Het doel hiervan is dat iedereen zich bewust wordt van de risico's en de mogelijkheden zich daartegen teweer te stellen. Er ontstaat aldus een behoefte om deskundigen op te leiden en in te zetten, die die bredere groep van burgers weten te bereiken met de boodschap dat cybersecurity vraagt om alertheid, maatregelen en controles op het gebied van informatieveiligheid.

Dit houdt ook in dat cybersecurity meer gezien moet worden als iets wat altijd en overal een rol speelt waar mensen met ICT-systemen werken en interacteren. Hierin ligt ook een taak voor het funderend onderwijs (primair en secundair onderwijs). Hoe daaraan vorm te geven, zal in toekomstig onderzoek verder moeten worden uitgezocht.

*Conclusie 9: Oplossingsrichtingen voor discrepanties op de arbeidsmarkt voor CSP's hebben betrekking op:*

- 1. Benutten van de mogelijkheden van onderwijs en opleidingen op het vlak van (o.a.) bewustwording, studiekeuze, verduidelijken van opleidingsroutes en mogelijkheden voor een leven lang leren op het terrein van cybersecurity.*
- 2. Versterken en verbeteren van werkprocessen in organisaties en bevorderen van samenwerking tussen organisaties.*
- 3. Verhelderen van onderwijs- en opleidingsroutes.*
- 4. Monitoren van ontwikkelingen in relatie tot de arbeidsmarkt van CSP's.*
- 5. Verbeteren en versterken van het imago van het cybersecuritywerkveld en de CSP.*
- 6. Doorgaan op de ingeslagen weg om cybersecurity te benaderen als een gezamenlijke verantwoordelijkheid van burgers, overheid, organisaties, onderwijs en opleidingen: gericht op bewustwording.*