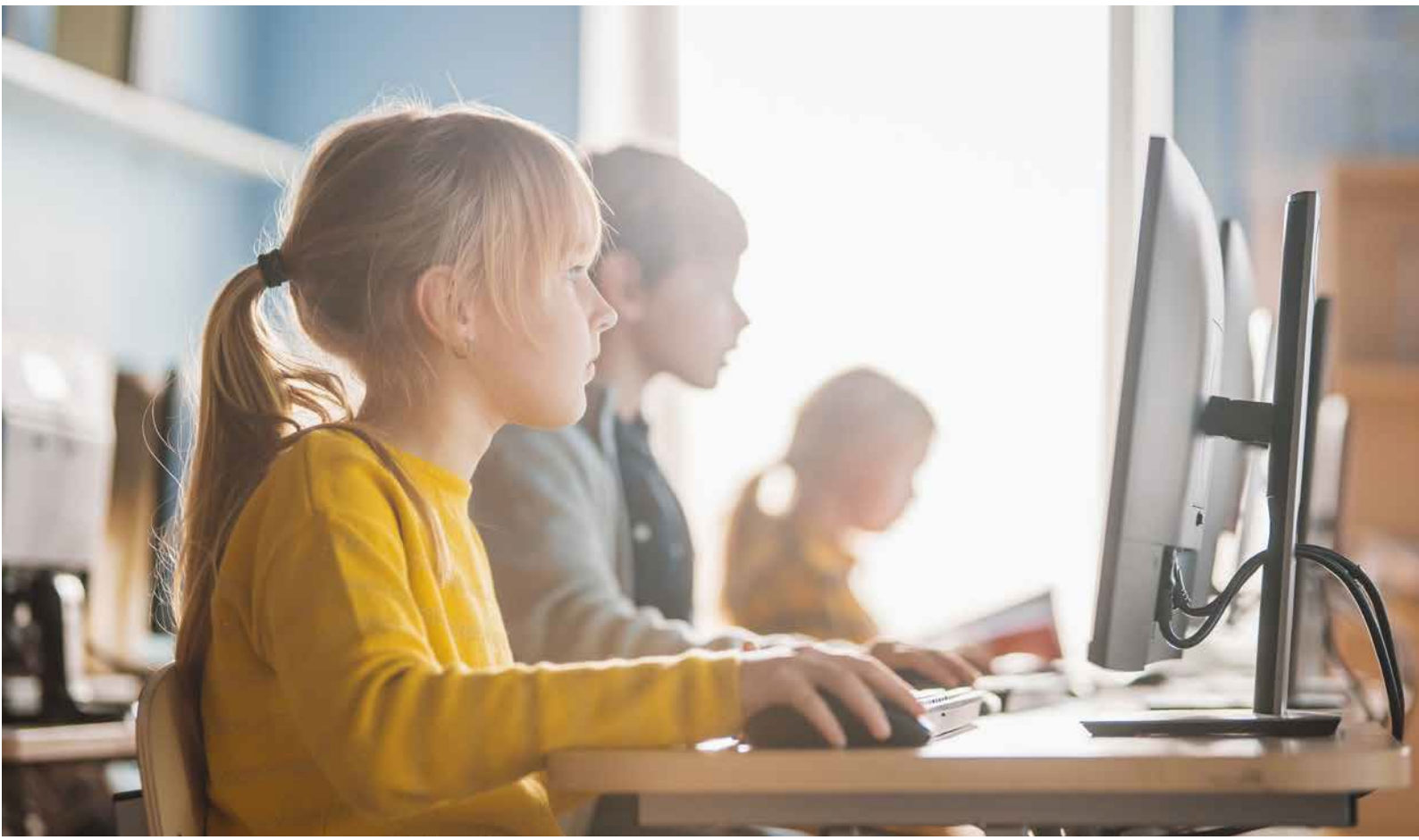
Bit by Bit

Samen voor digitaal veilig onderwijs

Arbeidsmarktanalyse personeel

invoering IBP normenkader

Beschikbaarheid IBP personeel voor Funderend Onderwijs



Ministerie van Onderwijs, Cultuur en Wetenschap

Kennisnet

SIVON

PO RAAD

VO RAAD

Inhoudsopgave

Inleiding

AANLEIDING

Vanuit het ministerie van OCW is de ambitie uitgesproken dat instellingen in het Funderend Onderwijs (FO) per 2027 digitaal veilig zijn. Dit betekent dat zowel leerlingen als medewerkers erop kunnen vertrouwen dat hun digitale gegevens optimaal beschermd zijn en dat er actieplannen klaarliggen voor die momenten waarop de digitale veiligheid in gevaar is. Om de digitale veiligheid te waarborgen heeft Kennisnet binnen het programma Digitaal Veilig Onderwijs (DVO)[1] een normenkader[2] ontwikkeld. Dit normenkader biedt een duidelijk handvat voor scholen om te kunnen voldoen aan digitale veiligheid. Om aan de ambitie van het ministerie van OCW – en daarmee aan de ambitie van het programma DVO – te voldoen, is afgesproken dat scholen in 2027 voldoen aan volwassenheidsniveau 3 van het normenkader. Om daar naartoe te groeien, hebben scholen nog veel werk te verrichten. Uit de nulmeting die in 2023[3] is uitgevoerd, komt namelijk naar voren dat geen van de ondervraagde scholen voldoet aan volwassenheidsniveau 3 van het normenkader IBP-FO.

Om te kunnen voldoen aan de eis tot digitale veiligheid hebben scholen expertise en capaciteit op het gebied van Informatiebeveiliging (IB) en Privacy (P) nodig. In het onderzoek 'Impactanalyse'[4] is een inschatting gemaakt hoeveel capaciteit per school nodig is. De aanvullende vraag in het huidige onderzoek is in hoeverre deze benodigde capaciteit ook daadwerkelijk beschikbaar is. Kan de arbeidsmarkt op korte en lange termijn voldoende bijdrage leveren in het voorzien van de nodige expertise en capaciteit. Een aanpalende vraag is tegen welke kostprijs deze capaciteit in te kopen is door scholen. Aangezien elke euro maar één keer kan worden besteed, geven scholen in principe de prioriteit aan zaken die direct nodig zijn om kwalitatief goed onderwijs te geven en worden voor onder andere beveiliging van informatie en privacy geen afzonderlijke financiën beschikbaar gesteld.

Om na te gaan in hoeverre voldoende personeel beschikbaar is op de arbeidsmarkt, willen we zicht krijgen op de arbeidsmarkt voor personeel dat uit de voeten kan met het implementeren van het normenkader IBP. Wanneer zicht is gekregen op de arbeidsmarkt, kan verder worden ingegaan op de kosten van de inhuur van personeel en expertise. Dit is uiteraard mede afhankelijk van de schaarste en beschikbaarheid hiervan. De bevindingen uit de impactanalyse worden in dit rapport eveneens meegenomen bij de vraag in hoeverre voldoende IBP-expertise beschikbaar is op de arbeidsmarkt.

DEFINITIE: IBP-EXPERTISE

Om de vraag over de beschikbaarheid van IBP-expertise te beantwoorden is het van belang dit begrip eerst goed te definiëren. IBP staat voor Informatiebeveiliging en Privacy en dit wordt binnen de onderwijssector vaak ook in één adem genoemd. De IBP'er, IBP-adviseur of IBP-coördinator zijn voorbeelden van rollen die je binnen de onderwijssector kunt aantreffen. De IBP'er in de onderwijssector is vaak een rol die een meer beleidsmatige invalshoek heeft en bij een staffunctionaris, maar bijvoorbeeld ook bij een onderwijzer of schoolleider kan zijn belegd. In andere sectoren kom je deze term IBP niet of nauwelijks tegen, dus ook niet in meer generieke arbeidsmarktonderzoeken. Wanneer we kijken of IBP-expertise beschikbaar is op de arbeidsmarkt, hanteren we een smallere, meer technische definitie en sluiten aan bij de term "cybersecurity". Dit betekent dat we uitgaan van 'cybersecurity-expertise, cybersecurity-ervaring, cybersecurity-specialist et cetera.

[1] Het programma DVO is een samenwerking van de volgende ketenpartners: het ministerie van OCW, Kennisnet, SIVON, de PO-raad en de VO-raad
[2] normenkaderibp.kennisnet.nl
[3] https://www.kennisnet.nl/app/uploads/Nulmeting-Normenkader-IBP-FO.pdf
[4] Nog niet gepubliceerd

ONDERZOEKSVRAGEN

De onderzoeksvragen die voorliggen, zijn de volgende:

- Hoe ziet de arbeidsmarkt voor ICT-expertise en –ervaring op korte én op lange termijn eruit?
- In welke mate is het haalbaar voor scholen in het funderend onderwijs om voldoende IBP-expertise te werven, gezien de vraag naar cybersecurity-personeel in andere sectoren?

AANPAK

Om deze vragen te beantwoorden is besloten om eerst een bronnenonderzoek uit te voeren waarin wordt nagegaan in hoeverre deze vragen reeds kunnen worden beantwoord door gebruik te maken van bestaande onderzoeksinformatie en -kennis. Zo heeft bijvoorbeeld het ministerie van Economische Zaken en Klimaat (EZK) onlangs een groot arbeidsmarktonderzoek laten uitvoeren naar de beschikbaarheid van cybersecurity-specialisten in Nederland[5] wat eveneens zeer bruikbaar is voor het vraagstuk omtrent beschikbaarheid van de bredere scope van IBP-specialisten in het funderend onderwijs. Ook geven de nulmeting en de impactanalyse (beide uitgevoerd in opdracht van DVO) al enkele antwoorden op deze onderzoeksvragen. In de huidige rapportage wordt dit bronnenonderzoek beschreven en zal antwoord worden gegeven op bovenstaande onderzoeksvragen die hiermee te beantwoorden zijn en zal advies worden gegeven voor het vervolg.

[5] Onderzoeksrapportage onderwijs en arbeidsmarkt cybersecurity (2024)

Bevindingen uit beschikbaar onderzoek

NULMETING NORMENKADER IBP VOOR HET FO (DVO)[6]

In de nulmeting is in 2023 op basis van de input van 15 schoolbesturen in het funderend onderwijs gekeken naar de stand van zaken op het vlak van informatiebeveiliging op basis van het Normenkader IBP FO. Aanvullend zijn de obstakels en uitdagingen in kaart gebracht om het normenkader te implementeren. Daaruit komt naar voren dat één van de redenen dat scholen nog niet voldoen aan de eisen van het normenkader voortkomt uit het tekort aan expertise en capaciteit binnen de scholen om de normen uit te voeren. Het betreft dan met name een tekort aan personeel met kennis van IBP. Dit tekort is volgens het onderzoek het meest nijpend bij kleinere en middelgrote instellingen. De capaciteit bij met name kleinere scholen wordt in eerste instantie primair beschikbaar gesteld aan onderwijs. Met name bij kleinere scholen worden IBP-taken meestal uitgevoerd door iemand die die taak aanvullend krijgt naast de overige werkzaamheden. De IBP-rol wordt dan uitgevoerd door iemand vanuit de ondersteuning of vanuit het onderwijzend personeel.

In dit onderzoek betrof het de capaciteit van de bredere groep personeel met IBP-expertise.

Relevante bevindingen uit de nulmeting voor de huidige onderzoeksvragen:

- In de steekproef voldeed nog geen enkel schoolbestuur aan volwassenheidsniveau 3 op alle normen van het normenkader.
- In de praktijk is de uitvoering van IBP afhankelijk van een kleine groep individuen. Omdat de werkprocessen vaak niet gedocumenteerd zijn, resulteert dit in de situatie dat uitval van één individu grote gevolgen kan hebben voor de continuïteit van de uitvoering.
- Op het vlak van bewustwording rondom IBP bij zowel bestuurders, als onderwijspersoneel dienen nog grote stappen gezet te worden. Dit gebrek aan awareness heeft op dit moment een negatief effect op de naleving van beheersmaatregelen. Extra inzet zal nodig zijn om de awareness te verhogen.
- Het gebrek aan expertise wordt door schoolbesturen vaak genoemd als een belangrijk obstakel bij de implementatie van het normenkader. Dit gaat om technische, juridische en beleidsmatige expertise. Het ontbreken van deze kennis speelt het sterkst bij schoolbesturen waarbij de IBP-rollen niet worden uitgevoerd door experts, maar door ‘regulier’ onderwijspersoneel.
- Het gebrek aan (interne en externe) capaciteit die beschikbaar is voor IBP vormt ook een belangrijk obstakel voor schoolbesturen bij de implementatie van het normenkader. Een tekort aan beschikbare capaciteit hangt in de praktijk vaak samen met de vrees dat het vrijmaken van capaciteit voor IBP conflicteert met de uitvoering van het reguliere onderwijs.

IMPACTANALYSE (DVO)[7]

Het doel van de impactanalyse in 2024 was inzicht te geven in de impact voor schoolorganisaties om de maatregelen van het Normenkader IBP-FO op volwassenheidsniveau 3 te implementeren en vervolgens structureel uit te blijven voeren. De focus van het onderzoek was dus niet de impact van het normenkader op digitale veiligheid, maar de impact van de vereisten uit het normenkader op de bedrijfsvoering van schoolbesturen om het normenkader succesvol te implementeren en uit te voeren.

Bij de resultaten is onderscheid gemaakt in de impact voor verschillende typen scholen. Daarbij is gebruik gemaakt van eerder gedefinieerde archetypes. Op basis van hun capaciteit, expertise en bewustzijn op het

[6] Uitgevoerd door Dialogic in opdracht van DVO. https://www.kennisnet.nl/app/uploads/Nulmeting-Normenkader-IBP-FO.pdf
[7] Uitgevoerd door Dialogic, O21 en Serendip in opdracht van DVO. Rapport nog niet openbaar gesteld.

gebied van IBP zijn scholen in een van de vier archetypes ingedeeld. De volgende archetypes zijn benoemd (a) de koplopers, (b) de uitvoerders, (c) de denkers en (d) de achterhoede.

In dit onderzoek betrof het eveneens de capaciteit van de bredere groep personeel met IBP-expertise.

Relevante bevindingen uit de impactanalyse voor de huidige onderzoeksvragen:

- Alle archetypen zullen zowel incidenteel als structureel een aanzienlijke tijdsinspanning moeten leveren om aan de vereisten van het normenkader te voldoen. Een inschatting is gegeven hoeveel capaciteit hiermee gemoeid is voor alle personen in de school die betrokken moeten zijn bij de invoering van het normenkader (dus niet alleen het ICT-personeel, maar alle betrokkenen bij het IBP-beleid). Over alle normen opgeteld wordt verwacht dat incidentele tijdsinspanning van 1.720-4.060 uur nodig is en een jaarlijkse tijdsinspanning van 310-670 uur per schoolbestuur nodig is om tot volwassenheidsniveau 3 te komen. Deze tijdsinspanning is op macroniveau geredeneerd vanuit het normenkader en houdt geen rekening met doorlooptijd als gevolg van overleg, besluitvormingsprocessen of kennisontwikkeling. De tijdsinspanningen moeten dus worden gelezen als de (minimale) impact in een 'ideale' situatie zonder schakelkosten, overlegmomenten of het activeren van collega's.
- De mate waarin een schoolbestuur dichter bij de ondergrens of de bovengrens van benodigde uren valt, is in belangrijke mate afhankelijk van de aanwezige expertise en mandaatvorming. Koplopers vallen vaker bij de ondergrens, terwijl de achterhoede bij de bovengrens vallen.
- Naast de impact op het personeel, heeft het normenkader impact op de kosten van software en hardware. De uitbreiding van Software as a Service-dienstverlening met extra licenties voor beveiliging is geen noodzakelijke voorwaarde om te voldoen aan het normenkader. Wel is het zeer waarschijnlijk dat schoolbesturen zullen moeten investeren in hun kritische informatiesystemen (afhankelijk van de uitkomst van hun eigen risicoanalyse). Op het vlak van hardware ligt het effect van het normenkader met name op het niveau van device management. De meerkosten hiervan zijn afhankelijk van de specifieke beheersmaatregelen van een schoolbestuur.
- Op basis van de huidige situatie en de huidige beschikbare ondersteuning wordt geconcludeerd dat Koplopers en Uitvoerders (in principe) over de rollen en expertise beschikken om binnen de geplande invoeringsperiode tot aan 2027 aan het normenkader te voldoen. Dit betekent echter wel dat de huidige werkzaamheden van personen met deze expertise geherprioriteerd moeten worden. Vanuit schoolbesturen wordt unaniem benoemd dat de aanwezige capaciteit reeds drukbezet is en er dus behoefte is aan meer capaciteit (in vast dienstverband). Dus ook bij deze scholen zal mogelijk extra capaciteit moeten worden ingehuurd. De Denkers en Achterhoede missen expertise en capaciteit, wat betekent dat hier per definitie extra expertise en capaciteit, in dienst of via inhuur, nodig is voor een tijdige implementatie van het normenkader.
- Schoolbesturen verwachten uitdagingen rondom werving van benodigde kennis en kunde, en hebben behoefte aan een regisseur om de behoefte aan schaarse expertise op sectorniveau in te vullen.
- Wanneer schoolbesturen met elkaar gaan concurreren om de werving van personeel, heeft dit een prijsopdrijvend effect.
- Er zitten onzekerheidsmarges aan de impact op het schoolbestuur. Zo moeten de tijdsinspanningen worden gelezen als de (minimale) impact in een 'ideale' situatie zonder schakelkosten, overlegmomenten of het activeren van collega's. Daarom is het ook niet goed mogelijk om de impact per school en archetype te vermenigvuldigen naar landelijke cijfers.
- De voorgaande opmerking geeft ook aan dat de kans groot is dat de impactanalyse een onderschatting geeft van de daadwerkelijke capaciteit en kosten die gemoeid zijn met de invoering van het normenkader IBP.

KENNISPROFIEL IBP (DVO)[8]

In 2024 heeft DVO een kennisprofiel IBP ontwikkeld waarin beschreven wordt welke kennis beschikbaar moet zijn voor een school om gebruik te kunnen maken van het ondersteuningsaanbod[9] dat binnen DVO wordt ontwikkeld

[8] Uitgevoerd door DVO (2024).
[9] Zie ook de website Aanpak IBP

om het normenkader te kunnen implementeren. Het doel van dit kennisprofiel is om een beschrijving te geven van het minimale kennisniveau. Hiermee worden schoolbesturen geholpen te bepalen of de benodigde kennis in de school en/of bij hun leverancier aanwezig is.

In dit onderzoek betrof het wederom de capaciteit van de bredere groep personeel met IBP-expertise.

Relevante opmerkingen uit het kennisprofiel IBP voor de huidige onderzoeksvragen:

- Uit beschikbare kennis en ervaring van experts blijkt dat de groep IBP'ers binnen het onderwijs niet homogeen is in kennisniveau, noch in de manier waarop de functie vorm krijgt binnen scholen en/of schoolbesturen. Zo heeft niet iedere school een IBP'er, maar hebben sommige scholen een ICT-coördinator. Ook wordt de functie niet altijd uitgevoerd door eigen personeel, maar wordt externe ondersteuning ingehuurd. In sommige gevallen is IBP vertegenwoordigd in het bestuur, in andere gevallen niet. Kortom, er is sprake van een zeer grote diversiteit.
- Bij de ontwikkeling van de hulpmiddelen binnen het ondersteuningsaanbod om scholen en schoolbesturen te helpen om aan de normen te voldoen wordt uitgegaan van een minimaal kennisniveau van IBP'ers. In de aanloop naar de implementatie van de Algemene Verordening Gegevensbescherming (AVG) is veel geïnvesteerd in kennis van privacy bij personeel. Kennis over informatiebeveiliging is echter op (veel) plekken achtergebleven. Hierdoor is de sector in de breedte niet voldoende geëquipeerd om het normenkader te implementeren.
- Informatiebeveiliging en privacy worden binnen de onderwijssector vaak in één adem genoemd. Dit zie je ook terug in de afkorting die binnen de onderwijssector overal gebezigd wordt: IBP (Informatiebeveiliging & Privacy), zoals in het netwerk IBP, IBP-coördinator of Aanpak IBP. Het zijn twee domeinen die dicht bij elkaar liggen en deels ook overlappen. Toch zijn er ook verschillen. Zo heeft privacy een goede wettelijke basis met de AVG. De AVG beschrijft wat je als organisatie moet doen en regelen op het gebied van privacy en veel organisaties zijn hier in aanloop naar en sinds de inwerkingtreding van de AVG dan ook mee aan de slag gegaan. Zo hebben zij bijvoorbeeld vaak, al dan niet intern, een functionaris gegevensbescherming benoemd van wie de taken ook vaststaan. Voor informatiebeveiliging bevat de AVG een bepaling dat 'passende maatregelen' dienen te worden genomen, waarbij definiëring van 'passend' achterwege is gebleven.
- In de praktijk is het verstandig als de IBP kennis niet bij één persoon zit om de afhankelijkheid van één persoon te minimaliseren. Het is dus goed denkbaar dat er meerdere functionarissen zijn die hun kennis kunnen bundelen en zo het hele kennisprofiel afdekken.

ONDERWIJS EN ARBEIDSMARKT CYBERSECURITY (EZK)[10]

Aangezien Nederland en de EU hard werken aan een digitaal veilige samenleving, heeft het Ministerie van Economische Zaken en Klimaat opdracht gegeven voor een onderzoek naar de huidige kwantitatieve en kwalitatieve tekorten op de arbeidsmarkt om aan deze digitaal veilige samenleving vorm te geven. Dit onderzoek, uitgevoerd door PVTV en Dialogic geeft zicht op de aanwas van nieuwe cybersecurityspecialisten vanuit relevante opleidingen en op de vraag naar cybersecurityspecialisten op de arbeidsmarkt. Deze vraag is voor de arbeidsmarktanalyse van IBP-specialisten in het onderwijs eveneens van groot belang. Zoals ook eerder beschreven vormt cybersecurity een onderdeel van IBP en informatie over de beschikbaarheid van specialisten op dit gebied geeft een indicatie voor het grotere geheel. Aanwas van nieuwe cybersecurity specialisten is nodig in alle branches waar gewerkt wordt aan digitale veiligheid. Anders dan een PABO – waar de meeste studenten expliciet worden opgeleid om in het basisonderwijs te gaan werken – hebben cybersecurityspecialisten een opleiding die ze in vele branches kunnen toepassen. Bij het nagaan van de arbeidsmarkt voor beschikbaar personeel ín het onderwijs, zal dus ook rekening gehouden moeten worden met de vraag naar cybersecurity-specialisten in de rest van Nederland en de EU. Het onderzoek van het ministerie van EZK is dan ook in grote mate relevant voor de onderzoeksvragen in het rapport dat nu voor u ligt.

[10] Uitgevoerd door PTVT en Dialogic in opdracht van het ministerie van EZK (2024). Onderzoeksrapportage onderwijs en arbeidsmarkt cybersecurity (2024)

Het ministerie van EZK verwoordt in het onderzoeksrapport dat de aanwezigheid van voldoende goed geschoolde cybersecurity professionals essentieel is. De huidige krapte op de totale arbeidsmarkt, nieuwe technologische ontwikkelingen en de intensivering van cybercriminaliteit zijn bepalend voor de steeds groter wordende behoefte aan diverse typen cybersecurityspecialisten. Op basis van de onderzoeksresultaten wil het Ministerie van EZK meer informatie over welke (beleids-)instrumenten op de korte en op de lange termijn ingezet kunnen worden om de cybersecurity arbeidsmarkt te versterken. Op basis van de onderzoeksresultaten wordt dan ook een actieplan opgesteld.

In dit onderzoek betrof het specifiek de capaciteit van cybersecurity-specialisten.

Relevante bevindingen uit het onderzoek onderwijs en arbeidsmarkt van EZK voor de huidige onderzoeksvragen:

- Door de variatie in de manier waarop de MBO ICT-opleidingen invulling geven aan het onderwijs, is niet mogelijk gebleken precies te achterhalen hoe groot het aandeel cybersecurity in de opleiding is. Navraag bij de opleidingsmanagers leert in ieder geval dat bij een aantal mbo-instellingen cybersecurity een standaard onderdeel van de ICT-opleiding is, terwijl anderen meer gebruik maken van de mogelijkheden die de keuzedelen bieden. Behalve bij de ICT-opleidingen is er bij de rest van de mbo-opleidingen nauwelijks of nog geen aandacht voor cybersecurity.
- Het totaal aantal studenten van deze betreffende MBO-opleidingen blijft ongeveer gelijk met rond de 23.000 studenten per jaar. Over de afgelopen jaren stroomden er jaarlijks gemiddeld 6.000 gediplomeerde ICT-studenten uit.
- Op hoger onderwijs niveau (hbo en wo) zijn er 10 studies geïdentificeerd die volledig in het teken staan van cybersecurity (5 hbo, 5 wo), 29 studies die een specialisatie-/ keuzerichting cybersecurity aanbieden (18 hbo, 11 wo) en 13 studies (6 hbo, 7 wo) die een verplicht onderdeel cybersecurity in hun programma hebben geïntegreerd. Tevens zijn er 9 hoger onderwijs- studies (8 hbo, 1 wo) aan het licht gekomen die nog in ontwikkelingsfase, accreditatiefase, of opstartfase zijn.
- De instroom van studenten met een relevant onderdeel cybersecurity in hun studie blijft de laatste drie jaren redelijk gelijk; rond de 3000 studenten jaarlijks. Het aantal afgestudeerde studenten neemt jaarlijks toe bij met name studies die volledig in het teken staan van cybersecurity, dan wel bij studenten die binnen hun studie een specialisatie-/ keuzerichting cybersecurity gekozen hebben.
- Binnen het Leven Lang Ontwikkelen-aanbod (LLO-aanbod) is uitgebreid niet-bekostigd onderwijsaanbod (dat wil zeggen, aanbod dat niet gesubsidieerd wordt door de ministeries van OCW en EZK. De kosten van de opleiding komen voor rekening van degene die de opleiding volgt, van de werkgever of van de uitkeringsinstantie opleidingen aan een particulier instituut, schriftelijke cursussen of bedrijfsopleidingen), waarvan ongeveer 20% gericht is op de meest gevraagde cybersecuritycertificaten op de arbeidsmarkt.
- Geschat wordt dat er circa 60.000-110.000 cybersecurity professionals op de arbeidsmarkt actief zijn, waarvan 17.000-33.000 professionals met een specialistisch cybersecurityprofiel.
- De vraag op de arbeidsmarkt is in kaart gebracht door de huidige vacatures te analyseren. De onderzoekers geven aan dat niet de gehele vraag zal hiermee in kaart zal zijn gebracht omdat de verwachting is dat posities ook zonder vacaturestelling vervuld worden. In de vacatureanalyse is een groeiende vraag naar cybersecurity-expertise te zien op de arbeidsmarkt: van circa 8.000 in 2018 tot circa 19.000 in 2022, voor zowel de specialistische cybersecurityprofielen als de bredere functieprofielen waar cybersecurity een onderdeel van uitmaakt. De vraag naar cybersecurity-expertise groeit dus en dit betreft zowel de specialistische cybersecurityprofielen als de bredere functieprofielen waar cybersecurity een onderdeel van uitmaakt.
- De vraag naar cybersecurity personeel is verschillend per provincie en kent een zwaartepunt op de vraag naar medior en senior functies waarvoor een hbo of wo-opleidingsniveau gevraagd wordt. De meeste vraag naar cybersecurity expertise komt van de overheid en de IT-sector. De vraag in de sector onderwijs staat op nummer 7 (zie onderstaande tabel).

4.3.4 Sector

De meeste vacatures zien we terug in de sectoren overheid, IT en zakelijke dienstverlening en advies. In figuur 18 is de top 10 weergegeven.

#	SBI-2	Sector_naam	2018	2019	2020	2021	2022	Totaal
1	84	Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen	857	1152	1503	1743	2570	7825
2	62	Dienstverlenende activiteiten op het gebied van informatietechnologie	927	1054	1409	1541	2196	7127
3	69	Rechtskundige dienstverlening, accountancy, belastingadvisering en administratie	550	621	544	1240	1658	4613
4	70	Holdings (geen financiële), concerndiensten binnen eigen concern en managementadvisering	795	792	593	973	1079	4232
5	46	Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)	425	490	732	1337	805	3789
6	64	Financiële instellingen (geen verzekeringen en pensioenfondsen)	489	628	513	776	1040	3446
7	85	Onderwijs	344	351	385	572	716	2368
8	80	Beveiliging en opsporing	197	327	372	524	463	1883
9	86	Gezondheidszorg	312	318	285	461	475	1851
10	78	Arbeidsbemiddeling, uitzendbureaus en personeelsbeheer	95	121	211	613	603	1643

Figuur 18: top 10 sectoren met cybervacatures. Bron: Jobdigger, bewerking Dialogic

- De populatie cybersecurity professionals kenmerkt zich als een relatief jonge populatie, waarvan tweederde man is en eenderde vrouw. Immigratie en arbeidsmigranten lijken belangrijk te zijn voor de sector: circa 5-10% van de instroom is toe te schrijven aan werknemers uit het buitenland die in Nederland komen werken.
- In 15% van de vacatures wordt expliciet gevraagd naar een cybersecuritycertificaat. De meest gevraagde certificaten zijn de CISSP, CISM, en CISA4. Binnen de specialistische cybersecurity profielen wordt vaak een certificaat gevraagd; zoals bijvoorbeeld de Chief Information Security Officers (CISO) of een Penetratietester, die computersystemen en apps test op kwetsbaarheden in de beveiliging.
- De komst van de NIS2 richtlijn (Network and Information Security), de Cyber Resilience Act (CRA) en de verdere ontwikkeling van AI zullen een grote rol gaan spelen op de cybersecurity arbeidsmarkt. De verwachting is dat de NIS2 de vraag naar cybersecurity professionals in de breedte zal doen toenemen, van de ECSF profielen Chief Information Security Officers (CISO) tot aan Implementers, Analisten, Auditors en Pentesters. Door de CRA zal de vraag naar cybersecurity professionals naar verwachting eveneens in de breedte toenemen.
- Door de verdere ontwikkeling en inzet van AI zal de vraag naar de uitvoering van bepaalde taken door mensen afnemen, maar tegelijkertijd zullen er ook nieuwe taken ontstaan en zullen nieuwe competenties benodigd zijn.
- Organisaties die marginaal met cybersecurity bezig zijn, waar cybersecurity een relatief kleine rol speelt, en die niet onder de NIS2 en/of CRA vallen zullen vermoedelijk blijven kiezen voor de ‘hybride’ functies in combinatie met externe inhuur/inkoop/organisatie van cybersecurity-expertise.
- De vervolgvraag is hoe die gevraagde expertise georganiseerd gaat worden binnen de economie. In welke mate gaan organisaties cybersecurity-expertise in huis halen of organiseren ze dat extern via inhuur en inkoop en/of via samenwerkingsverbanden? Men zou dit kunnen beschouwen als een ‘make-or-buy’ beslissing. We zien veel situaties waarin bijvoorbeeld één FG of CISO voor meerdere organisaties actief is of waar via gezamenlijke regelingen bij gemeenten zorggedragen wordt voor de invulling van specialistische functies die de maturiteit en behoeften van individuele organisaties soms nog overstijgt. In andere woorden: aangenomen dat er sprake is van een groeiende toekomstige vraag naar cybersecurity-expertise, is de vervolgvraag bij welke organisaties deze vraag zich op welke manier gaat manifesteren. Moet iedere organisatie zelf cybersecurity-expertise in huis hebben en zo ja, welke expertise dan precies? In generieke zin is binnen dit onderzoek naar voren gekomen dat deze organisaties allereerst wel bewust moeten zijn van wat de rol van cybersecurity is voor de organisatie in kwestie, en dat het aannemen van iemand die het overzicht heeft wel stap 1 is. Deze persoon kan vervolgens ook inschatten wat er extern ingehuurd/ingekocht moet worden en/of wat er intern moet gebeuren om aan de cybersecuritydoelen van de organisatie te voldoen.
- Een aanvullend onderdeel van deze wetgeving is dat het de vraag naar professionals vergroot die bezig zijn met compliance, toezicht en handhaving. Denk aan meer auditors en legal & compliancy-officers.
- Tenslotte: bedrijven die zich niet bewust zijn van de (toekomstige) risico’s, hebben momenteel nog geen vraag. Dit kan een grote latente vraag betekenen.

AANVALSPLANNEN BRANCHES EN EZK [11]

Het ministerie van Economische Zaken en Klimaat heeft een aanvalsplan ontwikkeld waarin een samenhangend pakket maatregelen is neergelegd om onder andere het tekort aan ICT-personeel aan te pakken. De branche-organisaties gaan hier in hun aanvalsplan getiteld *Chronisch Tekort ICT'ers* op in. Ook in deze aanvalsplannen wordt aangegeven dat er een groot tekort is aan ICT'ers. Cybersecurity is een deelaspect van ICT, namelijk de beveiliging van die ICT. In die zin hebben de aanvalsplannen betrekking op een bredere populatie dan die we voor ogen hebben voor het op orde krijgen van informatiebeveiliging en privacy binnen de funderend onderwijssector. Wij gaan er echter vanuit dat de mate waarin ICT'ers of cybersecurityspecialisten beschikbaar zijn op de arbeidsmarkt vergelijkbaar is.

Ook in deze aanvalsplannen betreft het de capaciteit van cybersecurity-specialisten.

Relevante opmerkingen uit de aanvalsplannen voor de huidige onderzoeksvragen:

- Het tekort aan ICT'ers werkt bij uitstek intersectoraal door. Van grote ICT bedrijven tot bedrijven wiens bedrijfsvoering in grote mate van ICT afhankelijk is, van zorg en onderwijs tot lokale overheid en rijksoverheid en van sportclub tot nationale ledenvereniging: iedereen heeft ICT'ers nodig om de digitale transformatie van Nederland vorm te geven.
- Nederland scoort al jaren goed op de ranglijsten van gedigitaliseerde landen. We zien dit terug in een constante groei van de arbeidsmarkt ICT en succesvolle bedrijvigheid. Tegelijk zien we ook dat de groei van het aanbod op de arbeidsmarkt de groei van de vraag naar digitalisering niet kan bijbenen. Nederland digitaliseerde snel en gestaag met een arbeidsmarkt die al jaren zeer krap is.
- Om de omvang van de krapte te begrijpen is het van belang te erkennen dat ICT'ers niet alleen werkzaam zijn in de ICT-sector. Vandaag de dag zijn twee op de drie ICT'ers niet werkzaam in de ICT-sector, maar in sectoren die in toenemende mate gebruikmaken van digitale technologie. Daarbij is het aantal ICT'ers in alle sectoren in 2021 in harde cijfers hoger dan ooit.

[11] https://www.nldigital.nl/wp-content/uploads/sites/3/2023/02/Aanvalsplan-Chronisch-Tekort-ICTers.pdf en https://open.overheid.nl/actieplan groene en digitale banen/pdf

Conclusies en aanbevelingen

Digitale veiligheid gaat over alle grenzen van sectoren en landen heen. De behoefte aan security specialisten en specialisten op het gebied van informatiebeveiliging (IB) en privacy (P) bestaat dan ook in elke sector en stijgt nog harder met de toename van de digitalisering en de komst van wetgeving zoals de NIS2 richtlijn (Network and Information Security) en de Cyber Resilience Act (CRA) en de verdere ontwikkeling van kunstmatige intelligentie (Artificial Intelligence (AI)).

Het onderwijs is in deze geen vreemde eend in de bijt: ook in het Funderend Onderwijs (FO) is een toename van IBP-experts nodig, aangezien het primair, secundair en speciaal onderwijs moeten gaan voldoen aan het normenkader voor digitaal veilig onderwijs[12]. Voor alle normen moet elke school voor 2027 beleid en uitvoering ontwikkelen. Uit een eerste nulmeting die is gehouden[13] blijkt dat geen enkel schoolbestuur nog voldoet aan volwassenheidsniveau 3 op alle gestelde normen en dat de uitvoering van IBP op scholen afhankelijk is van een kleine groep individuen. Schoolbesturen geven aan dat het gebrek aan interne en externe capaciteit die beschikbaar is voor IBP één van de obstakels vormt bij de implementatie van het normenkader.

Uit het onderzoek naar de impact die de invoering van het normenkader heeft op de financiële en personele bedrijfsvoering van scholen[14] blijkt dat alle scholen zowel incidenteel als structureel een aanzienlijke tijdsinspanning moeten leveren om aan de vereisten van het normenkader te voldoen. Afhankelijk van de vorderingen die scholen al gemaakt hebben, betreft dit een eenmalige inspanning van 1.720-4.060 uur per school en een structurele tijdsinspanning van 310-670 uur per school per jaar. Dit is een minimale inschatting van de tijdsinspanning aangezien is uitgegaan van een optimale situatie van invoering en waarbij geen rekening is gehouden met aanvullende tijdsinvesteringen als gevolg van overleg, besluitvormingsprocessen, kennisontwikkeling of het activeren van collega's. Naast de impact op het personeel, heeft het normenkader impact op de kosten van software en hardware.

In het hier gerapporteerde bronnenonderzoek naar de beschikbaarheid van cybersecurity-specialisten op de arbeidsmarkt is nagegaan of een aanwas van dergelijk personeel voor het onderwijs überhaupt beschikbaar is. Opgemerkt moet worden dat deze vraag nog los staat van de vraag of de kosten voor dit personeel gedragen kunnen worden door scholen. Op basis van beschikbare onderzoeken en aanvalsplannen die in dit rapport beschreven zijn, valt te concluderen dat er een tekort is op de arbeidsmarkt om te voldoen aan de vraag naar cybersecurity-specialisten in alle branches. Dit geldt dus ook voor de onderwijssector.

De vervolgvragen voor het onderwijs sluiten in dit geval exact aan bij de algemene vervolgvragen voor cybersecurity in Nederland en de EU (zie het citaat uit het onderzoek van het ministerie van EZK hieronder). Om te kunnen voldoen aan het normenkader zal er in het FO gezocht moeten worden naar creatieve oplossingen om met het schaarse personeel aan de grote opdracht van invoering van het normenkader op volwassenheidsniveau 3 te kunnen voldoen. Een groot voordeel van deze oplossingen is eveneens dat ze meerwaarde bieden bij de uitvoering van het normenkader en de kosten van cybersecurity personeel voor scholen kunnen drukken.

Enkele denkbare opties voor efficiency ter voorbeeld:

- De organisatie van IBP centraal bij het schoolbestuur beleggen en niet bij elke school afzonderlijk.
- Stimuleren van (regionale) samenwerking tussen scholen wat behalve personeelsbesparing ook leidt tot kosten-efficiëntie door deling van kennis.
- Versterken van de kennis van onderwijspersoneel dat betrokken is bij de uitvoering van IBP-beleid op scholen
- Meer centraal aanbod, onder andere door het bieden van landelijke formats en/of landelijke ondersteuning van scholen

[12] normenkaderibp.kennisnet.nl

[13] https://www.kennisnet.nl/app/uploads/Nulmeting-Normenkader-IBP-FO.pdf

[14] Rapport nog niet openbaar gesteld.

- Aanbod of specifieke dienstverlening op afzonderlijke elementen inzetten als dienst ‘as-a-service’.

We adviseren op basis van deze bevindingen dan ook om flink in te zetten op het efficiënt gebruik van cybersecurity personeel dat voor scholen beschikbaar is. Om dit te optimaliseren stellen we voor een vervolgonderzoek uit te zetten om na te gaan welke efficiëntieslagen reeds worden benut door scholen en in andere sectoren om dit mee te geven als best practices.

Uit: Onderzoeksrapportage onderwijs en arbeidsmarkt cybersecurity (2024) van EZK

De vervolgvraag is hoe die gevraagde expertise georganiseerd gaat worden binnen de economie. In welke mate gaan organisaties cybersecurity expertise in huis halen of organiseren ze dat extern via inhuur en inkoop en/of via samenwerkingsverbanden? We zien veel situaties waarin bijvoorbeeld één FG of CISO voor meerdere organisaties actief is of waar via gezamenlijke regelingen zorggedragen wordt voor de invulling van specialistische functies die de maturiteit en behoeften van individuele organisaties soms nog overstijgt. In andere woorden: aangenomen dat er sprake is van een groeiende toekomstige vraag naar cybersecurity-expertise, is de vervolgvraag bij welke organisaties deze vraag zich op welke manier gaat manifesteren. Moet iedere organisatie zelf cybersecurity expertise in huis hebben en zo ja, welke expertise dan precies? In generieke zin is binnen dit onderzoek naar voren gekomen dat deze organisaties allereerst wel bewust moeten zijn van wat de rol van cybersecurity is voor de organisatie in kwestie, en dat het aannemen van iemand die het overzicht heeft wel stap 1 is. Deze persoon kan vervolgens ook inschatten wat er extern ingehuurd/ingekocht moet worden en/of wat er intern moet gebeuren om aan de cybersecuritydoelen van de organisatie te voldoen.

Bit by Bit

Samen voor digitaal veilig onderwijs

Contactgegevens
Details