OP HET KRUISPUNT VAN

Kunstmatige intelligentie en cyberbeveiliging

ONDERZOEK NAAR DE DYNAMIEK VAN DEZE TWEE TECHNOLOGIEËN EN HUN IMPACT OP DE TEWERKSTELLING, OPLEIDING EN COMPETENTIES IN BRUSSEL

Digitalcity.brussels
Pool Opleiding Werk voor digitale beroepen

RAPPORT

2024

VOORWOORD

Tussen symbiose en modegril gaat dit verslag dieper in op de banden tussen kunstmatige intelligentie (ofte AI) en cyberbeveiliging, twee cruciale domeinen die ons huidige digitale landschap vormgeven. Aan de hand van de analyse in dit verslag onderzoeken we de wederzijdse impact van beide disciplines en hun invloed op IT-beroepen en -opleidingen in Brussel.

AI en cyberbeveiliging zijn nauw met elkaar verweven en versterken elkaar in een cyclus van continue innovatie. AI biedt veelbelovende hulpmiddelen voor het versterken van de beveiliging van IT-systemen, terwijl cyberbeveiliging de betrouwbaarheid en integriteit van AI-oplossingen waarborgt. Deze relatie is echter niet zonder uitdagingen.

In Brussel, Europees knooppunt van innovatie en technologie, zijn deze kwesties van bijzonder belang. Bedrijven en instellingen moeten zich snel aanpassen aan technologische veranderingen en over geschoold personeel beschikken dat deze complexe uitdagingen aankan.

Dit document belicht de voornaamste economische uitdagingen in verband met AI en cyberbeveiliging en benadrukt het cruciale belang van deze sectoren voor het concurrentievermogen en de veerkracht van bedrijven en infrastructuren in een steeds veranderende digitale omgeving.

Door samen te investeren in opleiding en innovatie te bevorderen kunnen we een toekomst creëren waarin digitale beroepen niet alleen bestand zijn tegen technologische uitdagingen, maar ook ongeziene kansen bieden voor zowel werkzoekenden als bedrijven. Digitalcity.brussels bevindt zich in het hart van deze transformatie en biedt een dynamische omgeving waarbinnen talent zich kan ontplooien en mee vorm kan geven aan een veelbelovende digitale toekomst voor Brussel en daarbuiten.

JEAN-PIERRE RUCCI
Directeur van Digitalcity.brussels

PIERRE MERVEILLE
Voorzitter van Digitalcity.brussels

WAT IS DIGITALCITY.BRUSSELS?

WIJ ZIJN

De vzw Pool Opleiding-Werk voor digitale beroepen, **Digitalcity.brussels**, is het resultaat van een publiek-private samenwerking tussen de sectorale sociale partners enerzijds en de Brusselse openbare dienst voor arbeidsbemiddeling (Actiris) en de Brusselse opleidingscentra (Bruxelles Formation en de VDAB) anderzijds. Digitalcity.brussels brengt een heuse dialoog op gang tussen bedrijven en de actoren van de Pool. Haar missies zijn haar bestaansreden. De Pool wist zich op te werpen als unieke en essentiële referentiepartner in Brussel voor opleiding en tewerkstelling in de digitale sector en voor digitale beroepen, en voor al onze doelgroepen: bedrijven, werknemers, onderwijscentra, studenten enz.

digitalcity.brussels

ONZE WAARDEN

Rond deze vijf kernwaarden is het ons te doen:

01 Samenwerking
Samenwerking die teamgeest en solidariteit met elkaar verbindt.

02 Continue verbetering
Continue verbetering waaruit moet blijken dat we in staat zijn om onszelf uit te dagen en met veranderingen om te gaan.

03 Tevredenheid
Tevredenheid van de Brusselse gebruikers en van het personeel van de Pool.

04 Oplossingsgericht
Oplossingsgericht aanpak die probleemoplossing pragmatisch benadert en gebruikmaakt van collectieve intelligentie.

05 Innovatie
Innovatie die verwijst naar een vindingrijke manier om met verandering om te gaan, nieuwe ideeën te genereren, processen te verbeteren en onze diensten te vernieuwen.

De medewerkers en partners van Digitalcity.brussels zijn vastberaden om deze waarden uit te dragen in hun dagelijkse werk door ze op te nemen in elk aspect van hun missies en verantwoordelijkheden.

INHOUDSOPGAVE

RAPPORT 2024

In de huidige digitale wereld vormt de combinatie van kunstmatige intelligentie (AI) en cyberbeveiliging een landschap waarin innovatie en veerkracht met elkaar zijn verweven. In Brussel, het bruisende Europese epicentrum van economische en ondernemersactiviteiten, roept deze convergentie cruciale vragen op en levert ze interessante debatten op. De toename van cyberbedreigingen en technologische vooruitgang brengen deze twee IT-sectoren op de voorgrond en roepen vragen op over hun reikwijdte, gebruik enzovoort. Met dit in het achterhoofd moeten we een aantal punten bekijken:

- Hoe zijn ze met elkaar verbonden?
- Wat is de impact van AI op cyberbeveiliging?
- Hoe kunnen we de veiligheid van snelgroeiende AI garanderen door vooringenomenheid en kwaadwillig gebruik te voorkomen?
- En vooral; welke impact zullen deze twee gebieden hebben op de ontwikkeling van IT-beroepen, de Brusselse arbeidsmarkt en het bestaande en toekomstige opleidingsaanbod?

In dit verslag onderzoeken we de kern van deze symbiose tegen de achtergrond van de strategische positionering van bedrijven, de evolutie van IT-profielen en de herformulering van het opleidingsaanbod.

AGENDA

In september 2023 organiseerden we rond dit thema kracht een webinar waarin vijf experts op het gebied van AI en cyberbeveiliging debatteerden over de synergiën tussen deze twee gebieden.

HUGUES BERSINI
AI-onderzoeker aan de ULB

GRÉGORIO MATIAS
CEO en medeoprichter van MCG

MARTIN FOCKEDEY
inspecteur bij CCB

ISSAM EL HADDIOUI
Security Engineering Manager bij Checkpoint

MICHEL HERQUET
Managing Partner bij B12

YouTube

Dit webinar kan opnieuw worden bekeken op het **YouTube-kanaal** van **Digitalcity.brussels**.

DOELSTELLINGEN & METHODOLOGIE VAN HET VERSLAG

01

DOELSTELLINGEN

Dit verslag onderzoekt de impact van AI op het gebied van cyberbeveiliging in België en omgekeerd, en focust op het ecosysteem van Brusselse bedrijven. Het verslag schetst een overzicht van de huidige situatie aan de hand van een marktanalyse, de bestaande oplossingen, de percepties van spelers in de sector, beroepsprofielen en uitdagingen rond aanwerving, evenals de beschikbare opleidingen. Het onderzoekt de toekomstige kansen voor AI in cyberbeveiliging in België, maar ook de vooruitzichten voor de AI-markt in Brussel, en legt daarbij de focus op de uitdagingen voor de beroepen en opleidingen.

Ons verslag is het resultaat van een nauwgezette analyse, gebaseerd op een groot aantal onderzoeken, rapporten van experts, gegevens van gerenommeerde onderzoeksinstellingen en van de overheid. Elke observatie wordt stevig onderbouwd door een gevarieerde en diepgaande kennisbasis, waardoor een uitgebreid en goed geïnformeerd perspectief wordt geboden op de onderwerpen die in dit verslag aan bod komen. Daarnaast hebben we een reeks interviews gehouden met experts en bedrijven om meer inzicht te krijgen in de realiteit van de markt. De volledige lijst van geïnterviewde experts staat achteraan in het verslag.

Ter afsluiting van ons onderzoek hebben we het initiatief genomen om onze conclusies niet alleen om te zetten in aanbevelingen, maar ook in concrete acties die aansluiten bij de doelstellingen van Digitalcity.brussels. Deze initiatieven richten zich specifiek op de uitdagingen voor digitale beroepen en opleidingen, met de ambitie om de drijvende kracht te worden achter het scheppen van eenheid in het digitale Brusselse landschap.

Ons hoofddoel is de uitdagingen aan te gaan die inherent zijn aan dit domein en concrete projecten te presenteren die de harmonisatie van inspanningen in de wereld van Brusselse IT-opleidingen zullen katalyseren. Deze initiatieven zijn ook bedoeld om het profiel van de IT-sector, het opleidingsaanbod en de diversiteit van loopbanen te vergroten gelet op het tekort aan gekwalificeerde professionals, vooral op het gebied van AI en cyberbeveiliging.

OMSCHRIJVING VAN HET ONDERZOEKSVELD

02

02 INLEIDING

Voor een goed begrip van het onderwerp is het belangrijk om een definitie te formuleren en uitleg te geven over deze twee domeinen die we in het vervolg van het verslag zullen analyseren.

Naast de definities worden deze thema's geassocieerd met een reeks specifieke kwesties die de complexiteit van de digitale wereld aantonen aan de hand van belangrijke punten zoals veiligheid, bewustmaking, gegevensbeheer en economische aantrekkelijkheid. In dit hoofdstuk worden deze kwesties bekeken door de lens van cyberbeveiliging en van kunstmatige intelligentie.

2.1 Cyberbeveiliging: definitie en uitdagingen

In de Cybersecurity Strategy België 2.0 wordt cyberbeveiliging gedefinieerd als het resultaat van een verzameling beveiligingsmaatregelen om het risico op verstoorde en ongeoorloofde toegang tot informatie- en communicatiesystemen (ICT) tot een minimum te beperken [1]. Met andere woorden; alle wetten, kaders, systemen en methoden om aan risicomanagement te doen om personen en activa (materieel en immaterieel) van overheden en organisaties te **beschermen**.

Gartner, het bekende Amerikaanse advies- en onderzoeksbureau dat bekend staat om zijn analyse van technologische trends, definieert cyberbeveiliging [2] als *het inzetten van mensen, beleid, procedures en technologieën om organisaties, hun kritieke systemen en gevoelige informatie te beschermen tegen digitale aanvallen*.

Bescherming is dus een sleutelbegrip in cyberbeveiliging. Met de voortschrijdende digitalisering van private, officiële en professionele gegevens wordt **het aanvalsterrein voor criminelen steeds ruimer**. Een van de belangrijkste uitdagingen voor de sector van de cyberbeveiliging is meer sensibilisering voor deze dreiging die zowel individuele burgers als grote en kleine bedrijven treft. **Sensibilisering** is van het grootste belang. Er is nog een lange weg te gaan gezien de snelle ontwikkelingen op het gebied van cyberbeveiliging. Om maar één actueel voorbeeld te noemen: er zijn recentelijk talloze aanvallen geweest op Europese ziekenhuizen die steeds vaker het doelwit zijn van gerichte aanvallen die hun infrastructuur ondermijnen. Het is van levensbelang dat landen, maar ook bedrijven en overheidsinstanties, weerbaar worden en cyberbeveiligingsmaatregelen nemen. **De bescherming van vitale instellingen, bedrijven en burgers is een van de cruciale elementen die deel uitmaken van de prioriteit van de cyberbeveiligingsstrategie in België en, de facto, in Europa.**

Cyberbeveiliging heeft ook sociaaleconomische gevolgen. Door deze grotere cyberdreiging ontstaan professionele beschermingsdiensten in België, Europa en in de rest van de wereld. In gespecialiseerde en andere bedrijven die hele afdelingen inzetten om het bedrijf en zijn klanten te beschermen, zien we een **heuse boom in vragen naar beveiliging**. Dit leidt wereldwijd tot een **tekort aan talent** dat volgens een onderzoek van ISC2 wordt geschat op **5,5 miljoen** mensen [3].

[1] CBB – Cybersecurity Strategy België 2.0 – 2021 -2025.

[2] Gartner – What is cybersecurity?

[3] ISC2 - How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce – 2023.

2.2 AI: definitie en uitdagingen

In haar voorstel voor een verordening in 2021 definieert de Europese Commissie kunstmatige intelligentie (AI) als "software... die voor een bepaalde reeks door mensen gedefinieerde doelstellingen ***output kan genereren****, zoals inhoud, voorspellingen, aanbevelingen of beslissingen die van invloed zijn op de omgeving waarmee wordt geïnterageerd*[4]*".* Het Europees Parlement maakt een onderscheid tussen twee soorten kunstmatige intelligentie[5]:

- **AI-software** zoals zoekmachines, virtuele assistenten, gezichts- en spraak-herkenningssystemen enzovoort.
- **AI *"belichaamd"*** in de vorm van robots, zelfrijdende auto's, het Internet der Dingen enzovoort.

We horen ook vaak spreken over Machine Learning (ML). Wat is ML? ***Machine Learning*** of automatisch leren is een subgenre van AI dat zich richt op **autonoom leren en autonome verbetering** van het systeem op basis van ervaring zonder expliciete programmatie. Leeralgoritmen worden gebruikt om AI-modellen te trainen.

Generatieve AI of GenAI is een vorm van AI die gegevens en inhoud (geschreven of visueel) genereert door de productie van nieuwe gegevens. GenAI kan worden onderscheiden van klassieke AI (**discriminatieve AI**) omdat klassieke AI zich richt op meer specifieke taken zoals classificatie, voorspelling en probleemoplossing op basis van reeds bestaande gegevens. ChatGPT of Midjourney zijn voorbeelden van GenAI.

AI [KUNSTMATIGE INTELLIGENTIE]

Als "software ... die voor een bepaalde reeks door mensen gedefinieerde doelstellingen output kan genereren, zoals inhoud, voorspellingen, aanbevelingen of beslissingen die van invloed zijn op de omgeving waarmee wordt geïnterageerd".

Grote taalmodellen (LLM's ofte *Large Language Models*) zijn GenAI-toepassingen die speciaal zijn ontworpen voor natuurlijke taalverwerking (NLP - Natural Language processing).

Een van de aan AI verbonden uitdagingen is **ethiek**. Dit wordt de meest complexe kwestie van de komende jaren aangezien AI-technieken voor instellingen steeds sneller gaan. **Hoe kunnen we een AI ontwikkelen die ethischer, veiliger en vrij van vooroordelen is?** Is de huidige AI een betrouwbare technologie? Tegen deze achtergrond is er vandaag wetgeving nodig om een kader te vormen voor de ontwikkeling van deze nieuwe technologie. Op Europees niveau is dit het doel van de **AI Act**.

Een andere kwestie is **de aantrekkelijkheid van AI** in de wereldeconomie. Hoe kan AI worden gebruikt om het concurrentievermogen te vergroten? Het is een krachtige technologie die op de arbeidsmarkt ten dienste kan staan van gezondheid, mobiliteit, ecologie, veiligheid en andere sectoren. Het kan zelfs de winstgevendheid, aantrekkelijkheid, concurrentiekracht en productiviteit van een bedrijf vergroten.

Het biedt een reëel economisch potentieel, maar dit moet worden omkaderd door gestructureerde wet- en regelgeving, met name op het gebied van gegevensbescherming. De kwestie wordt momenteel bestudeerd door de Europese instellingen, en de oplossingen die worden gevonden zijn voorwerp van de huidige en toekomstige uitdagingen.

[4] Toute l'Europe - Intelligence artificielle: que fait l'Union européenne? – 2024.

[5] Europees Parlement - Kunstmatige intelligentie: definitie en gebruik – 2021.

DE SECTOREN IN BELGIË

03

In 2022 voerde Agoria, de federatie van technologiebedrijven, een studie uit over de toestand van de sector van cyberbeveiliging in België [6].

3.1 De sector van cyberbeveiliging

Volgens de studie telt deze sector **441 Belgische bedrijven** die gespecialiseerd zijn in cyberbeveiliging. Deze bedrijven alleen al hebben **6405 VTE (voltijds equivalenten)** in dienst. Het zijn echter niet alleen cyberbeveiligingsbedrijven die experts aanwerven. Bepaalde sectoren, zoals het bank- en verzekeringswezen of de overheid, zijn ook op zoek naar een groot aantal cyberbeveiligingsprofielen.

Terecht, want de digitalisering van bedrijven, groot en klein, en de opslag van gegevens in de cloud breiden almaar verder uit. Dit brengt een verhoogd beveiligingsrisico mee aangezien hierdoor het speelveld voor criminele hackers ook groter wordt. Een StatBel-enquête over het gebruik van ICT in bedrijven [7] schat dat *"23,2% van de Belgische bedrijven al minstens één keer werd geconfronteerd met een ICT-gerelateerd beveiligingsincident"*. Dit kan ertoe leiden dat bepaalde diensten niet beschikbaar zijn of dat vertrouwelijke gegevens worden vernietigd, beschadigd of openbaar gemaakt. In die context zijn kmo's minder goed gewapend om nieuwe meer geavanceerde bedreigingen het hoofd te bieden.

Volgens een studie van Proximus [8] werden in 2022 meer grote bedrijven getroffen door cyberdreigingen dan kleine. **45% van de ondervraagde grote bedrijven gaf aan een of meer cyberincidenten te hebben meegemaakt, tegenover 25% van de kleine en middelgrote bedrijven**. Er werd geen rekening gehouden met het feit dat grote bedrijven heel wat beter zijn voorbereid op aanvallen. Ze beschikken immers over meer middelen (personeel, financieel en strategisch) om zichzelf te beschermen en hebben vaak een gevestigde digitale en beveiligingscultuur dankzij training, bewustwording en crisismanagementplannen. Het zijn dan ook de kleinste bedrijven die het ergst getroffen worden door dit soort incidenten.

Met de groeiende dreiging groeit ook de behoefte aan specialisten op het gebied van cyberbeveiliging en wordt het een maatschappelijk probleem. Het is een boomende sector. Er is nochtans een groot tekort aan talent in België en de rest van de wereld. Het Agoria-onderzoek wijst op **een tekort van meer dan 1.200 werknemers in de cyberbeveiligingssector, en zelfs meer dan 3.000 werknemers in alle sectoren samen** [9].

Een van de belangrijkste kwesties op het gebied van cyberbeveiliging is **sensibilisering** (zowel bij het grote publiek en jongeren als bij bedrijven). Volgens het Proximus-onderzoek is *"het bewustzijn nog niet wijdverspreid* [10]**" 22% van de werknemers in grote bedrijven zegt nog nooit een IT-beveiligingsbewustzijnstraining** (security awareness training) **te hebben gevolg, tegenover 46% bij kmo's**. Hoewel dit cijfer niemand verbaast, is het wel opvallend in het licht van de exponentiële toename van bedreigingen voor bedrijven.

[6] Agoria – First socio-economic study on the cyber security sector in Belgium, 2022.

[7] Statbel – Enquête over het gebruik van ICT en e-commerce in bedrijven, 2022.

[8] Proximus – Onderzoeksverslag: De impact van cyberbeveiliging op bedrijven in de Benelux, 2022.

[9] Agoria – 2022, First socio-economic study on the cyber security sector in Belgium.

[10] Proximus – Onderzoeksverslag: De impact van cyberbeveiliging op bedrijven in de Benelux, 2022.

45%

45% van de ondervraagde grote bedrijven gaf aan een of meer cyberincidenten te hebben meegemaakt, tegenover 25% van de kleine en middelgrote bedrijven.

6.405 VTE

Deze bedrijven alleen al hebben 6.405 VTE (voltijds equivalenten) in dienst.

441

Volgens de studie die AI4Belgium uitvoerde in 2020 zijn er in België 441 bedrijven die hun activiteiten baseren op AI-technologieën.

10%

Volgens de FOD Economie gebruikte in 2021 10% van de bedrijven in België minstens één AI-technologie [13].

3.2 De sector van de kunstmatige intelligentie

Op de portaalsite van het collectief AI4Belgium vinden we een raming van het ecosysteem van kunstmatige intelligentie in België. Volgens de studie die AI4Belgium uitvoerde in 2020 zijn er in België **441 bedrijven** die hun activiteiten baseren op AI-technologieën [11]. We zien meteen dat Vlaanderen met 233 bedrijven het grootste aantal bedrijven telt dat gespecialiseerd is in AI. Daarna volgt Wallonië met 106 bedrijven en ten slotte Brussel met 102 bedrijven. Dit ecosysteem omvat bedrijven die gespecialiseerd zijn in diensten, gezondheid en biotechnologie, maar ook in landbouw, financiële technologie, recht, industrie enz. In 2023 waren er 6.000 bedrijven met een AI-activiteit in Europa. Dit is flink wat minder dan in de Verenigde Staten, waar ongeveer 15.000 AI-gebaseerde bedrijven actief zijn [12]. Als we naar deze gegevens kijken en rekening houden met de vooruitzichten voor de ontwikkeling en democratisering van AI, is het aantal Belgische bedrijven zeker veranderd sinds de laatste telling in 2020.

Daarnaast zijn er nog de bedrijven die kunstmatige intelligentie gebruiken ten behoeve van hun bedrijf. Volgens de FOD Economie **gebruikte in 2021 10% van de bedrijven in België minstens één AI-technologie** [13]. Hoe groter het bedrijf, hoe meer kunstmatige intelligentie uiteraard wordt geïmplementeerd. 41% van de grote bedrijven gebruikt het, tegenover slechts 8% van de kleine bedrijven. We hebben geen relevante gegevens over de ontwikkeling van de AI-markt in België, maar op basis van wereldwijde voorspellingen kunnen we zeggen dat AI wijdverspreid is in onze samenleving en al een impact heeft binnen bedrijven. Volgens een voorspelling van de International Data Corporation (IDC) zal de wereldwijde waarde van AI-software exponentieel groeien, van naar schatting 64 miljard dollar in 2022 tot meer dan 250 miljard dollar in 2027 [14].

[11] AI4Belgium – Panorama van AI.

[12] Statista 2023 – Number of artificial intelligence (AI) companies in major economies worldwide in 2023.

[13] FOD Economie - 2022, Barometer van de informatiemaatschappij, geavanceerde digitale technologieën.

[14] Gartner Predicts AI Software Will Grow To $297 Billion By 2027.

[15] FOD Economie - 2022, Barometer van de informatiemaatschappij, geavanceerde digitale technologieën.

Interessant genoeg **wordt AI** volgens de studie van de FOD Economie [15] **in België in bedrijven vooral gebruikt voor ICT-beveiliging en in tweede instantie voor de organisatie van bedrijfsbeheerprocessen**. De cyberbeveiligingssector toont dan ook een reële interesse in de implementatie van kunstmatige intelligentie.

STRATEGIEËN EN WETTELIJKE OMKADERING

04

04 INLEIDING

Cyberbeveiliging en de ontwikkeling van kunstmatige intelligentie vormen beslissende strategische uitdagingen voor landen en Europa. Vandaag hebben zowel Europa als België strategische plannen ontwikkeld (zie hieronder) voor deze twee domeinen om het potentieel van deze technologieën te bepalen. Het is interessant om te zien dat er in deze plannen bruggen worden geslagen tussen deze twee technologiedomeinen.

4.1 Cyberbeveiliging in Europa en België

4.1.1 Europa: oprichting en mandaat van ENISA (2004)

In 2004 richtte het Europees Parlement *ENISA* op om de veerkracht van Europese infrastructuren te verbeteren en de digitale veiligheid van de samenleving en burgers te handhaven. De opdrachten van ENISA werden versterkt door de verordening van de Europese Unie over cyberbeveiliging in 2019 en in het bijzonder de **EU Cybersecurity Act**[16].

De opdrachten van ENISA zijn de volgende[17]:

1. Een kader voor Europese samenwerking te scheppen en deze strategische eenwording te dirigeren.
2. Een cyberbeveiligingsbeleid op te stellen.
3. Een doeltreffende Europese operationele samenwerking op te zetten.
4. Te investeren in vaardigheden en expertise op het gebied van cyberbeveiliging.
5. Het vertrouwen van de gebruikers in de digitale omgeving te vergroten.
6. Strategieën te ontwikkelen om de dreiging in te dammen en de veerkracht van Europa te vergroten.
7. Kennis te delen en verdiepen in het cyberbeveiligingsecosysteem van de EU.

[16] European Commission: The EU Cybersecurity Act.

[17] ENISA - EU-agentschap voor cyberbeveiliging.

4.1.2 Europa: de NIS-richtlijn (2016-2024)

De Europese **NIS**-richtlijn (**netwerk- en informatiebeveiliging**) is in 2016 in werking getreden. Dit is de eerste Europese tekst over cyberbeveiliging. In 2019 werd hij omgezet in Belgisch recht. Een van de doelstellingen is om lidstaten aan te moedigen om nationale strategieën voor cyberbeveiliging op te stellen.

Na herziening wordt deze eerste versie als onvolledig beschouwd (beperkingen in de duidelijkheid van de toepassingsgebieden en bevoegdheden, gebrek aan informatie-uitwisseling en een richtlijn die onvoldoende is afgestemd op de toenemende ontwikkeling van bedreigingen).

In 2021 stelt het Europees Parlement versie 2 NIS van de NIS-richtlijn voor. Op basis van deze nieuwe Europese versie zal België een wet inzake netwerk- en informatiebeveiliging moeten opstellen. De richtlijn wordt gepubliceerd op 14 december 2022 [18] en omgezet in Belgisch recht op 26 april 2024.

Voortbouwend op de resultaten van haar voorganger, breidt de NIS2-richtlijn de doelstellingen en het toepassingsgebied uit om de bescherming tegen steeds geraffineerdere kwaadwillende actoren te versterken. Hoewel AI nauwelijks wordt vermeldt, is deze uitbreiding ongekend in cyberregulering en markeert deze gebeurtenis een paradigmaverschuiving op Europees niveau.

Er zijn andere Europese richtlijnen en kaders die de beveiliging van infrastructuur en van gegevens regelen en de groei van AI beïnvloeden, zoals de *General Data Protection Reglementation (GDPR), de European Cyber Resilience Act (CRA), de Digital Operational Resilience Act* (DORA) en andere die een strategisch kader willen scheppen en beveiliging in Europa op alle niveaus regelen [19].

4.1.3 Cybersecurity strategie België 2.0 (2021-2025)

In 2012 nam België het eerste strategisch plan voor cyberbeveiliging [20] aan. In navolging van deze eerste strategie publiceerde België in 2021 een bijgewerkte strategie voor een versterkte beveiliging van cyberspace aan de hand van een aantal acties:

1. De digitale omgeving versterken en het vertrouwen vergroten.
2. Gebruikers en beheerders bewapenen.
3. Vitale organisaties beschermen tegen cyberbedreigingen.
4. Reageren op de cyberdreiging.
5. Verbeteren van publieke, private en universitaire samenwerkingsverbanden.
6. Internationale engagement.

Vergeleken met het plan van 2012 richt versie 2.0 zich op vitale sectoren; energie, financiën, mobiliteit, volksgezondheid, drinkwater, digitale dienstverleners en de overheid. Het wijst erop dat deze sectoren van vitaal belang zijn omdat ze een grotere bescherming vereisen en meer impact hebben dan andere economische sectoren. Tot slot is het **duidelijk dat samenwerking tussen de actoren in het domein van cyberbeveiliging (overheid, publieke sector, private sector, opleidingsinstanties enz.) cruciaal is**. In dit plan wordt echter weinig gezegd over de impact van kunstmatige intelligentie op cyberdefensie, ondanks het belang van deze technologie.

4.1.4 België: Cybersecurity Coalition (2015)

Op het gebied van samenwerking en het bundelen van krachten is de oprichting van de **Cybersecurity Coalition** een goed voorbeeld van het bundelen van middelen. Deze vzw werd opgericht in 2015 en is een samenwerking tussen de academische wereld, de overheid en de privésector. Deze groep helpt de veerkracht van België op het vlak van cyberbeveiliging versterken door een robuust ecosysteem uit te bouwen.

NIS

[NETWORK AND INFORMATION SECURITY]

*De Europese **NIS**-richtlijn (netwerk- en informatiebeveiliging) is in 2016 in werking getreden. Dit is de eerste Europese tekst over cyberbeveiliging. In 2019 werd hij omgezet in Belgisch recht. Een van de doelstellingen is om lidstaten aan te moedigen om nationale strategieën voor cyberbeveiliging op te stellen.*

[18] Eur-Lex - Directive (EU) 2022/2555 of the European Parliament & of the Council.

[19] European Cyber resilience Act – website.

[20] Belgium, Cybersecurity strategy, 2012.

[21] Nationaal convergentieplan voor de ontwikkeling van kunstmatige intelligentie – 2022.

4.2 Kunstmatige intelligentie in Europa en België

4.2.1 Europa: AI Act (2024)

De belangrijkste is de **AI Act** die in januari 2024 haar definitieve versie kreeg. Dit is de **eerste Europese verordening over kunstmatige intelligentie**. Ze toont de continue vooruitgang van kunstmatige intelligentie aan, maar ook dat gecoördineerde maatregelen nodig zijn om het gebruik ervan te reguleren, de grenzen ervan vast te leggen en gebruikers te beschermen tegen de mogelijke vooroordelen van deze technologie. De belangrijkste kwesties zijn gegevensbeveiliging en gebruikersbescherming.

Met regelgeving zoals de AI Act wil Europa de ontwikkeling van AI en de toepassing ervan zo veilig mogelijk maken.

4.2.2 België: oprichting van AI4Belgium (2019)

In 2019 werd het **collectief AI4Belgium** opgericht om private, publieke en academische spelers in Belgische AI-wereld samen te brengen. Deze coalitie is vastbesloten om België te positioneren in het Europese AI-landschap. Bij de oprichting van de coalitie werd een actieplan opgesteld met 4 hoofddoelen:

1. AI bovenaan de politieke agenda zetten.
2. Het publieke debat aanzwengelen door de implicaties van AI aan het publiek uit te leggen.
3. Mensgerichte AI aanmoedigen en inzetten.
4. Het ontwikkelen van een eerste versie van een Belgische AI-strategie die resulteert in het convergentieplan.

AI Act

De belangrijkste wettelijke omkadering is de AI Act die in januari 2024 haar definitieve versie kreeg. Dit is de eerste Europese verordening over kunstmatige intelligentie.

4.2.3 België: Convergentieplan voor de ontwikkeling van AI (2022)

In 2022 publiceerde de Belgische federale overheid een nationaal convergentieplan voor de ontwikkeling van AI met 9 strategische doelstellingen in haar eerste pijler [21]:

- Betrouwbare AI bevorderen.
- Cyberbeveiliging waarborgen.
- Het concurrentievermogen en de aantrekkingskracht van België versterken dankzij AI.
- Een gegevensgestuurde economie en een krachtige infrastructuur ontwikkelen.
- AI in het hart van de gezondheidszorg.
- Ten dienste van een duurzamere mobiliteit.
- Het milieu beschermen.
- Betere opleiding en levenslang leren.
- Burgers betere diensten en bescherming bieden.

De tweede pijler van het Convergentieplan richt zich op de relatie tussen AI en cyberbeveiliging; het verband tussen deze twee technologieën wordt erin belicht, alsook hun wederzijdse invloed.

KRUISBESTUIVING TUSSEN AI EN CYBERVEILIGING

05

5.1 AI voor veiligheid

De recente technologische vooruitgang op het gebied van kunstmatige intelligentie heeft een heel nieuwe wereld van mogelijkheden geopend voor het gebruik ervan in cyberbeveiliging.

Het gebruik van AI in het cyberdomein wordt vaak genoemd om verschillende redenen

1. **Automatisering** van bepaalde tijdrovende taken om responstijden te verbeteren en de werkdruk van analisten te verlagen.
2. **Machine Learning** om terugkerende patronen te identificeren.
3. **Redeneerfuncties** om de analyse van gegevens te verduidelijken, scenariomodel-lering te verbeteren en te anticiperen op aanvalsvectoren.

Bedrijven gebruiken met andere woorden AI ook om zichzelf te beschermen tegen cyberbedreigingen.

Het doel is om:

- **Zwakke plekken te ontdekken** in de infrastructuur voordat criminelen dat doen.
- **Aanvallen te detecteren:** aanvalspatronen en anomalieën analyseren (logboekanalyse).
- Malware te analyseren om **te anticiperen op toekomstige aanvallen** en **de respons te verbeteren** (snelheid, automatisering van een deel van de respons, betere monitoring).
- Crisismanagementoefeningen te genereren.

5.2 AI ten dienste van de misdaad

De groei van kunstmatige intelligentie is ook gunstig voor cybercriminelen die deze technologie gebruiken om hun impact en speelveld te vergroten. De democratisering van AI en de digitalisering van de bedrijfswerkplek in de cloud hebben het aanvalsgebied voor cybercriminelen duidelijk verruimd en de diversiteit van aanvallen vergroot.

Deep voice [22], deepfake [23] en geautomatiseerde aanvallen zorgen voor snellere aanvallen, betere voorbereiding van aanvallen, de mogelijkheid voor meer geavanceerde aanvallen, en natuurlijk een breder actieterrein.

AI wordt voornamelijk gebruikt voor social engineering-aanvallen [24]. In het verslag van Enisa wordt uitgelegd dat *"innovatie in social engineering voornamelijk wordt gedreven door kunstmatige intelligentie, vooral sinds de release van ChatGPT* [25] -aanvalstechnieken op drie verschillende manieren te verbeteren:

1. **AI gebruiken om overtuigende phishing-e-mails** [26] en **-berichten** te maken die legitieme bronnen natuurgetrouw nabootsen.
2. **Deepfake** om stemopnames te klonen (de zogenaamde deep voice).
3. AI-gebaseerde **datamining**.

Het is cruciaal om de belangstelling van criminelen voor AI-technologieën in de gaten te houden. In het Threat Landscape 2023-verslag van ENISA [27] wordt in de ranglijst van cyberbeveiligingsbedreigingen de nadruk gelegd op de impact van AI-chatbots en, meer in het algemeen, AI dat in staat is om informatie te manipuleren.

Toch blijft ransomware de meest-voorkomende bedreiging **(34%)**, gevolgd door **DDoS-aanvallen** [28] **(28%)** en **gegevensbedreigingen (18%)**. **AI is nog steeds vrij marginaal**. De meest bedreigde sectoren zijn de **openbare sector (19%), particulieren (11%), gezondheidszorg (8%) en ten slotte digitale infrastructuren** [29] **(7%)**.

[22] Deep voice: techniek waarbij AI de stem van een persoon reproduceert om het slachtoffer te manipuleren.

[23] Deepfake: een multimediasynthesetechniek waarbij AI wordt gebruikt om desinformatie te creëren.

[24] Social Engineering: strategie die cybercriminelen gebruiken om slachtoffers te manipuleren om persoonlijke of gevoelige gegevens te verkrijgen.

[25] ENISA – Enisa Threat Landscape 2023.

[26] Phishing: hierbij doet men zich voor als een vertrouwde derde partij om het slachtoffer te manipuleren en persoonlijke gegevens te stelen (zoals toegangscodes voor bankrekeningen).

[27] ENISA – Enisa Threat Landscape 2023.

[28] DDoS-aanval (Denial-of-service attack): aanval waarbij een website niet kan functioneren door een groot aantal aanvragen te verzenden om de netwerkcapaciteit te verzadigen.

[29] ENISA – Enisa Threat Landscape 2023.

BELANGRIJKSTE CIJFERS

de populairste bedreiging

% 34	Ransomware
% 28	DDoS-aanvallen
% 18	Gegevensbedreigingen

de meest bedreigde sectoren

% 19	Openbare sector
% 11	Particulieren
% 8	Gezondheidszorg

"Het gebruik van AI is nog relatief zeldzaam gezien de complexiteit van de technologie. Natuurlijk worden bij sommige aanvallen waarbij mensen betrokken zijn strategieën om het slachtoffer te manipuleren versterkt door overtuigende AI-gegenereerde deepfakes. Traditionele aanvallen die misbruik maken van eenvoudige beveiligingslekken zullen nog een hele tijd aanhouden, zonder dat daar per sé AI voor nodig is.

VINCENT DEFRENNE
Directeur Cyberstrategie bij cyberbeveiligingsbedrijf Nviso

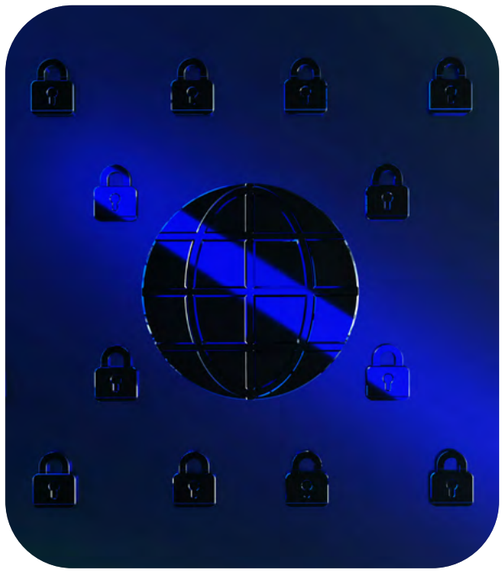
5.3 De veiligheid van AI

De grootste uitdaging van dit decennium betreft de razendsnelle ontwikkeling van AI en de problemen die dit meebrengt voor vertrouwelijkheid, integriteit en beschikbaarheid van diensten.

Zoals elke nieuwe technologie brengt AI nieuwe beveiligingsuitdagingen mee. In dit geval richten de aanvallen zich meestal op de corruptie van trainingsgegevens.

Om goed te functioneren en relevante antwoorden te geven heeft AI een grote hoeveelheid gegevens (trainingsgegevens) nodig. Een van de uitdagingen van deze technologie is de betrouwbaarheid en neutraliteit van deze gegevens. Dit is essentieel op elk niveau: gegevensverzameling, gegevensopslag en het delen van informatie.

Corruptie van deze trainingsgegevens kan leiden tot **bias of de invoer van vertekende gegevens**, ook gekend als ***data poisoning***; het wijzigen van trainingsdata om backdoors [30] te introduceren die fouten veroorzaken tijdens de productie.



Recente ontwikkelingen op het gebied van AI leiden tot controverses en roepen vragen op over gegevensbescherming. Het debat rond de integratie van AI in het domein van cyberbeveiliging en omgekeerd, is interessant en vereist bijzondere aandacht in het Belgische IT-ecosysteem.

Tot slot is een van de huidige kwesties waarrond veel te doen is in Europa de nood aan ethiek, met deze fundamentele vragen: Hoe moet bedrijfsinnovatie worden gereguleerd?, Hoe kunnen we bias [31] vermijden bij het gebruik van deze innovatieve digitale hulpmiddelen?

Om een oplossing te vinden op deze kwesties, met name bij overheidsdiensten, werd in 2024 op initiatief van de FOD een ethische commissie opgericht: BOSA [32]. De doelstellingen van dit comité van deskundigen zijn:

1. Openbare diensten en ambtenaren meer zin voor verantwoordelijkheid geven.
2. Ambtenaren bewuster maken van ethiek, onder andere in hun gebruik van gegevens en de gevolgen hiervan voor de rechten van burgers, inclusie en transparantie garanderen, en het respecteren van waarden.
3. Een voorbeeldrol zijn voor burgers als federale administraties digitale gegevens ethisch en innovatief verwerken.

[30] Backdoor: kwaadaardig computerprogramma dat toegang geeft tot een geïnfecteerde computer.

[31] Bias: wetenschappelijke vooringenomheid. Bias in AI betekent dat computers soms vooroordelen hebben omdat ze uit oneerlijke of onvolledige gegevens leren. Zo zal een "dokter" gemakkelijker mannelijk zijn dan vrouwelijk, enzovoort.

[32] FOD BOSA 2024 - Raadgevend Comité voor Ethiek inzake Data en Artificiële intelligentie voor de federale overheid - oproep tot kandidaat-leden.

Hoe krijg je een AI die je kunt vertrouwen?

Er zijn twee belangrijke factoren in de beveiling van kunstmatige intelligentie: AI beveiligen, omdat het een technologie is met nieuwe beveiligingsproblemen, én AI gebruiken voor beveiliging. Voor vertrouwen in deze systemen zal er een kwaliteits- en betrouwbaarheidslabel gecreëerd moeten worden.

NOEMIE HONORÉ
Associate Partner en Hoofd van Wavestone België

EEN OVER-ZICHT VAN DE BEROEPEN EN EEN WOORD OVER DE UITDA-GINGEN DOOR HET TEKORT AAN TALENT

06

06 INLEIDING

6.1 Beroepen in kaart brengen

IT-beroepen zijn divers en interdisciplinair; daarom is het een onbegonnen taak om ze op een concrete manier in te delen. In dit hoofdstuk kijken we naar een aantal beroepen die gerelateerd zijn aan cyberbeveiliging en kunstmatige intelligentie.

6.1.1 Beroepen die verband houden met cyberbeveiliging

Voor cyberbeveiliging baseren we ons op het document van ENISA dat een overzicht geeft van cyberbeveiliging-gerelateerde beroepen [33].

Dit document deelt deze beroepen in 12 categorieën in:

Chief Information Security Officer (CISO)
Verantwoordelijk voor de beveiliging van informatiediensten. Hij of zij implementeert strategieën om de gegevens en infrastructuur van een bedrijf te beschermen en beoordeelt de risico's. 01

Cyber Incident Responder (CIRT)
Expert die reageert op cyberbeveiligingsincidenten. Hij of zij identificeert kwetsbaarheden en corrigeert ze om een potentiële aanval te voorkomen, maar suggereert ook oplossingen voor verbetering na een incident. 02

Cyber Legal, Policy and Compliance Officer
Verantwoordelijke voor naleving van de lokale en internationale regelgeving door de onderneming. 03

[33] ENISA - European Cybersecurity Skills framework (ECSF) - User Manual, 2022.

Cyber Threat Intelligence Specialist (CTI)
Specialist die inlichtingen verzamelt over cyberbedreigingen en de modus operandi van tegenstanders. Hij of zij volgt de huidige trends in cyberbedreigingen en kwetsbaarheden.

04

Cybersecurity Architect
Specialist die beveiligingsoplossingen en architectuurmodellen bouwt voor de beveiliging van informatiesystemen.

05

Cybersecurity Auditor
Voert beveiligingsaudits uit en verzekert de naleving van de regelgeving. Hij of zij onderscheidt zich van de compliance officer door zich te richten op toezicht van de naleving.

06

Cybersecurity Educator
Professionele trainer in cyberbeveiliging.

07

Cybersecurity Implementer
Verantwoordelijk voor de ontwikkeling en implementatie van cyberbeveiligingsoplossingen.

08

Cybersecurity Researcher
Werkt aan onderzoek en innovatie op het gebied van cyberbeveiliging.

09

Cybersecurity Risk Manager
Beheert cyberbeveiligingsrisico's in functie van de bedrijfsstrategie.

10

Digital Forensics Investigator
Onderzoekt cybercriminaliteit om cybermisdrijven aan het licht te brengen.

11

Penetration Tester
Evalueert de doeltreffendheid van de beveiliging van een bedrijf door de grenzen van het systeem te testen en gaat de rol van cybercrimineel spelen.

12

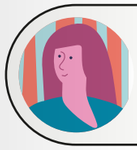
Deze **beroepen omvatten zowel technische** als meer **overkoepelende beroepen**, met een strategische en juridische focus.

De meest populaire en "representatieve" banen in cyberbeveiliging zijn de volgende: **CISO en *penetration tester* enz**. Zij tonen echter slechts één aspect van cyberbeveiliging. Zoals we hebben gezien zijn er in dit domein nog veel meer beroepen die bijdragen tot IT-beveiliging.

Er is steeds meer vraag naar meer juridische en strategische beroepen die te maken hebben met compliance als gevolg van de implementatie van Europese normen en regelgeving in ver-band met gegevensbescherming. **Het is dan ook belangrijk om de diversiteit aan cyberbe-veiligingsprofielen te belichten.**

6.1.2 AI-beroepen

Wat AI-beroepen betreft zijn er geen referentiekaders voor gespecialiseerde beroepen, maar de **volgende profielen duiken geregeld op in vacatures:**



Data Scientist
Ontwikkelt algoritmen om een dataset te importeren, classificeren, opschonen en analyseren; het gaat hier om zowel gestructureerde gegevens (vb. Excel-bestanden) als ongestructureerde gegevens (vb. vrije tekst of video's).

01

Machine Learning Engineer (ML Engineer)
Dit beroep is vergelijkbaar met dat van de Data Scientist; de ML Engineer richt zijn of haar analyse wel eerder op het produceren van voorspellingen met behulp van de gegevens.

02

Chief Data Officier ou Data Protection Officer
Iis direct gekoppeld aan de komst van de Europese GDPR-regelgeving. Deze officer zorgt ervoor dat het bedrijf voldoet aan de bestaande regelgeving voor het beheer van bedrijfsgegevens. Deze functie houdt niet rechtstreeks verband met AI (of IT), maar is wel essentieel en raakt aan dit technologiedomein.

03

Data Engineer
Richt zich op het beheer en de organisatie van gegevens, in tegenstelling tot de Data Scientist die focust op gegevensanalyse.

04

Data Analyst
In tegenstelling tot de Data Scientist vertrekt de Data Analyst vanuit bestaande gegevens voor de opmaak van analyserapporten.

05

AI-ontwikkelaar
Verwerkt AI-functionaliteit in softwareapplicaties gedurende de ontwikkeling ervan.

06

6.1.3 Profielen met dubbele competenties

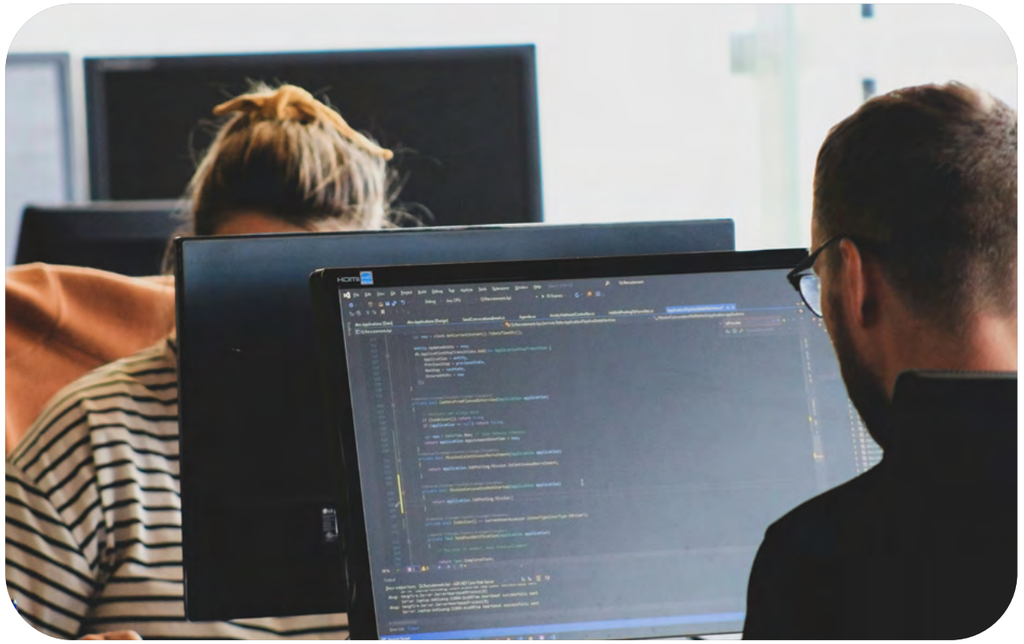
Men moet een onderscheid maken tussen de beroepen die betrokken zijn bij het ontwerpen van AI en beroepen die te maken hebben met het gebruik ervan. **De integratie van AI-oplossingen in een bedrijf vereist niet noodzakelijk experts en technische profielen.**

Dit rapport werpt twee fundamentele vragen op:

1. Is er vraag naar profielen met AI-competenties voor cyberbeveiliging?
2. Is er vraag naar specialisten met beveiligingsvaardigheden in de AI-sector?

We zien de laatste tijd vacatures opduiken in rekruteringsdatabases voor profielen met competenties in deze twee domeinen. Volgens de cyber security Workforce Study van ISC2 is er veel vraag naar AI-competenties, in het bijzonder naar Machine Learning. De vraag hiernaar is sinds 2022 met 28% gestegen [34]. Dit is wellicht toe te schrijven aan de snelle ontwikkeling van AI-technologieën sinds begin 2023.

> *Deze vaardigheid blijft echter relatief schaars op de arbeidsmarkt. De vraag ernaar is nog niet echt ingeburgerd.*
>
> —
>
> 
>
> VINCENT DEFRENNE
> Directeur Cyberstrategie
> bij cyberbeveiligingsbedrijf Nviso



[34] ISC2 – 2023 - How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce.

[35] AGORIA - First socio-economic study on the cyber security sector in Belgium, 2022.

[36] ISC2 – 2023 - How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce.

6.2 De uitdagingen van het tekort aan talent

Uit een studie van Agoria blijkt dat er op de Belgische markt een tekort is aan ruim 1.200 werknemers in de sector van cyberbeveiliging zelf, tot meer dan 3.000 werknemers in alle sectoren samen [35]. Wereldwijd loopt dit tekort op tot 4 miljoen.

Een van de factoren voor het tekort aan talent in cyberbeveiliging die de studie van ISC2 rond knelpuntberoepen in de cyberbeveiligingssector [36] aanvoert, is kostenverlaging in een onzekere economie die hoge kosten met zich meebrengt voor het bedrijf, evenals lagere lonen. Dit uit zich in een langere duur voor de implementatie van technologieën, de herstructurering of inkrimping van het beveiligingsteam en het schrappen van opleidingen in beveiliging. Dit draagt grotendeels bij tot het tekort aan talent in cyberbeveiligingsberoepen.

In zijn onderzoek wijst ISC2 erop dat het tekort aan competenties een grotere impact kan hebben dan het onvermogen om nieuwe cyberbeveiligingsprofielen aan te werven. Er is dus een verschil tussen een tekort aan vaardigheden en een tekort aan talent. Hier kan opleiding een rol spelen. **Het personeelstekort kan deels worden opgelost door werknemers voor te lichten over cyberbeveiliging**. In dit onderzoek oordelen de respondenten dat de volgende middelen het best zijn om het tekort aan cyberbeveiligingspersoneel te voorkomen en te beperken:

1. **Opleiding**
   72%
2. **Aanbieden van meer flexibele werkomstandigheden**
   69%
3. **Investering in diversiteit, kansengelijkheid en inclusiviteit**
   68%
4. **Investeren in certificering en aanwerven van nieuw personeel**
   67%

Daarnaast speelt het aanbod van financiële compensatie een belangrijke rol bij het aantrekken en binden van werknemers.

> **Ook softs skills spelen hier een belangrijke rol.**
>
> Volgens G. Alsteens is op het gebied van kunstmatige de ethiek het belangrijkste aspect bij aanwerving, en niet de technologie. Het is moeilijker om mensen met goede ethische competenties te vinden dan met technische vaardigheden.
>
> —
>
> 
>
> GEOFFROY ALSTEENS
> Cloud & AI Advisor bij Paradigm.brussels

> *De initiële en voortgezette opleiding kan worden gezien als de beste vorm van bescherming.*
>
> —
>
> 
>
> YVES ROGGEMAN
> Professor computerwetenschappen
> aan de ULB

OPLEIDING, EEN DOORSLAG-GEVENDE FACTOR

07

07 INLEIDING

Uit de ISC2 studie "*How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce* [37]" uit 2023 blijkt dat opleiding een geringere invloed heeft op aanwerving dan professionele ervaring en kwalificaties.

Opleiding zal het meeste effect hebben op het personeel van andere afdelingen. Dit doelpubliek heeft het meeste baat bij een introductie tot cyberbeveiliging.

Voor we onze gedachten over de uitdagingen van opleiding in deze context uiteenzetten, is het interessant om een overzicht te geven van het opleidings-aanbod in deze twee domeinen in Brussel.

7.1 Opleidingskaart voor Brussel

Wat hier volgt is een niet-limitatieve lijst van opleidingen AI en cyberbeveiliging in Brussel. Merk op dat geen van deze opleidingen ontworpen is om mensen op te leiden in zowel AI als cyberbeveiliging. Sommige opleidingen behandelen wel concepten uit een van de twee gebieden zonder er dieper op in te gaan.

[37] ISC2 – 2023 - How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce.

7.1.1 Op universitair niveau

ULB

MASTER — 2 JAAR

Master in cyberbeveiliging met focus op systeemontwerp en -analyse

(Samenwerking met de Koninklijke Militaire School, UCL, UNamur, Haute école Bruxelles Brabant, en de Hogeschool Ilya Prigogine)

De troeven:
Legal aspects of IT-security, ethiek, Machine Learning en datamining enz.

MASTER — 2 JAAR — START IN 2024

Master in cyberbeveiliging volgens Erasmus Mundus joint master in Cybersecurity

(CYBERUS)

De troeven:
Samenwerking met TalTech University (Tallinn, Estland) - ontwikkeling, coding en ontwerp), UL (Luxemburg – voor het financieel aspect) en UBS (Lorient, Frankrijk - Frans militair testcentrum, aanvalssimulatieruimte en forensisch onderzoek), en de ULB (cryptologieaspect).

MASTER — 1 JAAR

Specialisatiemaster in data science, Big Data

De troeven:
Huidige trends in Artificial intelligence enz.

VUB

MASTER — 2 JAAR HIERHIER

Master of Science in Applied Sciences and Engineering

De troeven:
Dit masterprogramma behandelt ook beveiliging en AI (met pijler ethiek).

MASTER — 1 JAAR

Aplied Informatics: Artificial Intelligence

De troeven:
Huidige trends in AI, cloud computing and Big Data processing enz.

SUMMER TRAINING – 2023, MOGELIJK OOK IN 2024?

Cybersecurity: law and practice

4 dagen voor werknemers en studenten.

De troeven:
Cybersecurity Law (EU-cybersecurity Laws, Nis2, Alact enz.), Cybersecurity Practice (firewalls, DNS & DNS Attacks enz.) enz.

7.1.2 Aan de hogescholen

LEONARDO DA VINCI COLLEGE

BACHELORSDIPLOMA — 3 JAAR

Bachelorsdiploma in informatica - applicatieontwikkeling

De troeven:
Optionele cursussen: Machine Learning, cyberbeveiliging en malware enz. (in het derde jaar)

BACHELORSDIPLOMA — 1 JAAR

Bachelier Bussiness Data Analysis

(Samenwerking met Ephec)

De troeven:
Statistiek, data (verzamelen, beheren en visualiseren), business (interpretatie van gegevens).

ERASMUS HOGESCHOOL BRUSSEL

MICROKREDIET OP ÉÉN TRIMESTER

Cybersecurity & ethical Hacking

De troeven:
Network security, Ethical hacking of software security, Ethical hacking.

1 JAAR POSTGRADUAAT

Toegepaste Kunstmatige intelligentie

De troeven:
Data Science, IoT and Big Data enz.

EPHEC

SOCIALE PROMOTIE – 1 JAAR

Korte cursus cyberbeveiliging

De troeven:
Host Security, Incident Response, Network Security, Software Security.

He2b

SPECIALIST — 1 JAAR

Specialist in cyberbeveiliging

De troeven:
Niveau van specialisatie in cyberbeveiliging.

ODISEE

SPECIALIST — 1 JAAR

Cybersecurity specialist

De troeven:
Security Operations, CCNA Cyberops Associate Certificate, Security And Automation enz.

7.1.3 Opleidingen voor volwassenen

DIGITALCITY.BRUSSELS MET BRUXELLES FORMATION

6 MAANDEN + 2 MAANDEN STAGE VOOR WERKZOEKENDEN

AI-ontwikkelaar

De troeven:
Python, R-taal voor AI, Power BI, AI-specifieke projectmethodologie (Agile en Scrum), ethiek en GDPR.

6 MAANDEN VOOR WERKZOEKENDEN

Cybersecurity Analyst

De troeven:
Cloud, Analyse en Penetratietests, Beveiligingsprotocollen en -tools, Netwerken, Wettelijk Kader en Methodologie (GDPR, ISO2700x-norm, crisisbeheer, enz.)

10 DAGEN VOOR WERKZOEKENDEN

Summer school: cybersec

De troeven:
Sensibilisering voor Cyberbeveiliging, Case Study van de Implementatie van een beveiligde Windows Server-infrastructuur, Security Gaming (poging tot aanvallen en verdedigingstechnieken).

BECODE

7 MAANDEN VOOR WERKZOEKENDEN

Data-experts

De troeven:
Initiatie Machine Learning, Deep Learning, Computer Vision, Kennismaking met de Cloud.

7 MAANDEN VOOR WERKZOEKENDEN

Cybersecurity analyst

De troeven:
System Administration, Networks, Programming, Analyst, Pentest, enz.

MOLENGEEK

7 MAANDEN VOOR WERKZOEKENDEN

Soc analyst

De troeven:
IT-beveiligingsarchitectuur, Opsporing van Verdachte Activiteiten, Beheer van Beveiligingsprojecten, Microsoft-Certificering.

7 MAANDEN VOOR WERKZOEKENDEN

Data analyst

De troeven:
Programmeren in Python, Machine Learning, Computer Vision enz.

LE WAGON

2 TOT 7 MAANDEN

Data engineer

De troeven:
De fundamenten van Data Engineering, Data Warehouse Management, Data voor Visualisatie, het Optimaliseren van Data Workloads enz.

2 TOT 7 MAANDEN

Data science and IA

De troeven:
Python, Machine Learning, Deep Learning, Ml Engineering, Generative Ai enz.

2 TOT 7 MAANDEN

Data analytics

De troeven:
Basis, SQL, Extraction, Data Visualization enz.

FARI (AI FOR THE COMMON GOOD)

De troeven:
De FARI AI Academy (voor managers, postdoctoraal, lesgevers), AI voor DPO's.

7.1.3 Opleidingen voor volwassenen

Voor onze zakelijke klanten is ons opleidingsaanbod voor AI en cyberbeveiliging beschikbaar in onze opleidingscatalogus. Hier zijn enkele interessante opleidingen: AI-technieken, Toepassingen en Ontwikkeling, Data Science, Machine Learning met Python, Cybersecurity Fundamentals, forensische analyse, hacken vermijden, Sensibilisering tot IT-beveiliging enz [38].

De Brusselse codeerscholen zijn ook op de innovatietrein gesprongen en bieden nu opleidingen aan in cyberbeveiliging en AI.

7.1.4 Opleiding in Brussel: de uitdagingen

AI en cyberbeveiliging zijn populaire thema's, vooral in de opleidingssector. **De echte uitdaging ligt in het voortdurend aanpassen van bestaande programma's aan de realiteit van de arbeidsmarkt.** Deze aanpassing vereist een interdisciplinaire aanpak met meerdere vaardigheden op het gebied van IT, statistiek, recht, strategie en natuurlijk specialisatie in cyberspace en AI.

Dat is echter niet alles. Om deze interdisciplinaire aanpak tot een logisch einde te brengen is het belangrijk om **nauwere banden** te smeden **tussen bedrijven en de academische wereld**. Deze banden moeten worden versterkt zodat opleidingsinstanties zich kunnen aanpassen aan de realiteit en de behoeften van bedrijven die personeel aanwerven.

> *"Het is noodzakelijk om banden te scheppen tussen bedrijven en opleidingsinstanties, ook al zijn er al een aantal initiatieven die hiermee rekening houden, zoals AI4belgium en de Cybersecurity Coalition.*
>
> —
>
> 
>
> AXEL LEGAY
> Professor aan de UCL

In deze context **moeten instellingen zoals Digitalcity.brussels als platform voor beroepen en opleidingen in Brussel een actieve rol spelen in het smeden van die banden. We moeten fungeren als een solide, betrouwbare brug tussen deze twee werelden**. We moeten bedrijfsleiders sensibiliseren voor de rekruteringsproblematiek en samenwerken met bedrijven om ons aanbod aan te passen zodat het beter beantwoordt aan hun rekruteringsuitdagingen en -behoeften.

Ondanks het groeiende tekort in de cyberbeveiligingssector zijn er nog steeds te veel bedrijven die onnodig op zoek zijn naar overgekwalificeerde profielen. Hooggekwalificeerde profielen met diepgaande vaardigheden in AI of cyber zijn natuurlijk essentieel in hoogtechnologische domeinen. In de meeste gevallen volstaan echter minder gekwalificeerde maar bekwame profielen.

Daarom is het van cruciaal belang om **prioriteit te geven aan de flexibiliteit van de programma's en de complementariteit van het opleidingsaanbod in Brussel**. Onze regio heeft een erg gevarieerd aanbod van digitale opleidingen die aangepast kunnen worden aan alle leerprofielen. Dit is wat Brussel zo sterk maakt, maar het is essentieel om **de middelen te bundelen en zodoende een aanbod te creëren dat zoveel mogelijk profielen dekt**.

Gezien de wervingsbehoeften van bedrijven ligt een andere uitdaging in de **ontwikkeling en uitbreiding van AI- en cyberbeveiligingsopleidingen**. In Brussel is het aanbod van dergelijke opleidingen de voorbije jaren weliswaar toegenomen, maar er is **nog steeds te weinig aanbod om aan de behoeften van de markt te voldoen**. Dit is des te meer het geval omdat bijvoorbeeld op de universiteit "te weinig studenten zich inschrijven voor technische opleidingen en hun aantal elk jaar daalt", aldus Yves Roggeman, professor computerwetenschappen aan de ULB. Hoe kunnen we het fenomeen van mensen die hun opleiding voortijdig afbreken verklaren? Is dit toe te schrijven aan een imagoprobleem van de sector, de vertegenwoordiging van de beroepen, een probleem van basisvaardigheden? Bij Digitalcity.brussels besteden we hier bijzondere aandacht aan. In het licht van haar missies als Pool Opleiding-Werk voor digitale beroepen zou Digitalcity.brussels moeten kunnen helpen bij het vinden van antwoorden op deze vragen. Waarom zetten deze studenten hun studie voortijdig stop? Hoe kan men op betrouwbare wijze de reden(en) voor deze verandering achterhalen?

[38] U vindt al deze en andere opleidingen vinden in onze opleidingscatalogus voor bedrijven op onze website: Digitalcity.brussels.

CONCLUSIE

08

08 INLEIDING

AI en cyberbeveiliging zijn de twee belangrijkste technologische trends vandaag.

Sinds de komst van ChatGPT en vergelijkbare programma's blijft kunstmatige intelligentie exponentieel groeien met aanzienlijke economische invloed. Op het gebied van cyberbeveiliging nemen de bedreigingen in alarmerend tempo toe en steeds meer bedrijven zijn kwetsbaar voor deze aanvallen.

Het gebruik van AI op het gebied van cyberbeveiliging is enerzijds ingeburgerd omdat verschillende cyberbeveiligingssystemen (van niet Belgische makelij) het al verwerkt hebben, maar anderzijds nog niet wijdverspreid als competentie in België. Er bestaat echter een onderlinge verwevenheid tussen beide domeinen. Elk bedrijf dat cyberbeveiligingsdiensten aanbiedt, onderzoekt de mogelijkheid om AI te integreren om de effectiviteit ervan te beoordelen. De tijd zal ons leren hoe dit evolueert.

Bij cybercriminelen blijft het gebruik van AI vooralsnog marginaal omwille van een toename van traditionele zwendelpraktijken waarvoor minder expertise nodig is. Het is daarom voorbarig om te zeggen dat AI een grote invloed zal hebben op cybercriminaliteit.

Zeker is dat steeds meer bedrijven buiten de sector van cyberbeveiliging AI integreren in hun beheerprocessen om hun activiteiten te optimaliseren. Voor bedrijven rust de uitdaging van deze onderlinge verwevenheid tussen AI en cyberbeveiliging zich vooral daar. Er zijn immers zwakke plekken in de beveiliging van AI. AI-gerelateerde beveiliging in het bijzonder roept veel vragen op. Omdat AI een opkomende technologie is, onderstreept democratisering ervan het belang van een snelle structurering van gegevensbeveiliging.

Met de formalisering van de AI-wet is het duidelijk dat Europese overheden een robuuste strategie moeten ontwikkelen die zich richt op gegevensbeveiliging, waaronder trainingsgegevens, bias-kwesties, gegevensbronnen, beheer van persoonlijke en vertrouwelijke gegevens enz.

Tegen deze achtergrond neemt de vraag naar AI- en cyberbeveiligingsprofielen toe. Profielen die beide expertises combineren zijn echter nog zeldzaam en eerder gericht op onderzoek en innovatie.

Het opleidingsaanbod voor deze twee domeinen is de voorbije jaren in Brussel uitgebreid. Er blijven niettemin een aantal belangrijke uitdagingen:

1. Ondanks de ontwikkelingen die hebben plaatsgevonden, is er nog steeds een **dringende behoefte om het aantal beschikbare opleidingsprogramma's uit te breiden** om te voldoen aan de groeiende vraag in deze specifieke domeinen.
2. Er moeten nog heel wat inspanningen worden geleverd voor **bewustmaking onder jongeren**, vooral onder degenen die op het punt staan om een beroepskeuze te maken.
3. Een derde cruciaal aspect is de **promotie van ruime opleidingsmogelijkheden** in Brussel.

Digitalcity.brussels houdt in de hoedanigheid van de Pool Opleiding-Werk van het Brussels Hoofdstedelijk Gewest deze drie uitdagingen nauwlettend in het oog bij het uitbouwen van zijn opleidings- en sensibiliseringsaanbod.

In het Brusselse opleidingslandschap is er geen specifieke behoefte aan opleidingen die zowel AI als cyberbeveiliging behandelen. Hoewel het relatief gesproken over een "niche" gaat, laten heel wat AI- en cyberbeveiligingsexperts en -bedrijven van zich horen. Het is dan ook om belangrijk om de ontwikkelingen op dit terrein te volgen in het licht van nieuwe behoeften.

DE PROJECTEN VAN DIGITALCITY.BRUSSELS

09

09 CONCLUSIE

Digitalcity.brussels heeft ten slotte concrete acties gepland naar aanleiding van de specifieke bevindingen in dit verslag. Deze acties maken deel uit van haar missies in verband met opleiding, werkgelegenheid en bewustmaking.

Met deze projecten hoopt Digitalcity.brussels werkzoekenden en jongeren warm te maken voor de domeinen van AI en cyberbeveiliging. De POW (Pool Opleiding-Werk) wil ook inzicht krijgen in de werkgelegenheids- en opleidings-problematiek bij bedrijven die in deze twee sectoren investeren en een actieve rol spelen bij het oplossen van deze problematiek.

Dit zijn de acties die vanaf 2024-2025 zullen worden gevoerd:

connection

9.1 De behoeften BEGRIJPEN

Om gelijke tred te houden met de realiteit van de arbeidsmarkt zal Digitalcity.brussels voor bedrijven die op zoek zijn naar IT-profielen een **enquête opzetten om de evolutie van hun beroeps- en opleidingsbehoeften in kaart te brengen**. Deze bedrijven zullen ook worden uitgenodigd om in de vorm van een adviescommissie van deskundigen actief samen te werken met Digitalcity.brussels om het aanbod aan te passen aan de realiteit van de Brusselse IT-arbeidsmarkt.

Lancering van een behoeftenonderzoek bij Brusselse bedrijven

1. **Doelstellingen:** nieuwe behoeften identificeren in de evolutie van beroepen en opleidingen bij bedrijven in Brussel. Dit project sluit aan bij de bevindingen van het vorige monitoringverslag van Digitalcity.brussels: Digitalisering van Brusselse kmo's [39].
2. **Publiek:** Brusselse bedrijven.
3. **Kalender:** start van het eerste onderzoek in 2025 - tweejaarlijks.

Oprichting van een comité van experts voor monitoring

1. **Doelstellingen:** de relatie tussen Digitalcity.brussels en Brusselse IT-bedrijven versterken rond beroepen en opleidingen. Met mogelijkheden voor win-winpartnerschappen (opleidingen aanpassen aan de behoeften van bedrijven in het kader van het traject Opleiding-Werk, sponsoring van evenementen van Digitalcity.brussels, zichtbaarheid in de communicatie van Digitalcity.brussels).
2. **Doelgroepen:** bedrijven en experts
3. **Hoe het werkt:** oprichting van het comité en verschillende raadplegingen als onderdeel van projecten en discussies over jaarlijkse thema's.
4. **Kalender:**
   2024. Oprichting van het comité en opstellen van de methodologie.
   2025 : début des consultations.

[39] Digitalcity.brussels – publicaties: Brusselse kmo's digitaliseren: ga de uitdaging aan samen met Digitalcity.brussels!

9.2 OPLEIDEN en aanpassen van de opleiding

Digitalcity.brussels wil als Pool Opleiding-Werk voor digitale beroepen werkzoekenden en bedrijven opleidingen aanbieden die aansluiten bij de realiteit van de IT-sector. In dit licht hebben we ons aanbod in de loop van de jaren ontwikkeld in de twee snel veranderende domeinen van AI en cyberbeveiliging.

Opleidingen en opmaak van jaarlijkse catalogus

1. **Doelstellingen:** in deze context willen we blijven nadenken over de organisatie van opleidingen die zijn afgestemd op de behoeften omtrent AI en cyberbeveiliging, maar ook rond innovatieve en aan de doelgroepen aangepaste lesmethoden. Tijdens deze denkoefening is het belangrijk om één ding in gedachten te houden: Brussel telt voornamelijk kmo's. Heel wat kmo's gebruiken technologie om hun productiviteit en winstgevendheid te verbeteren. Daarom werken we vooral samen met kleine bedrijven in Brussel die niet noodzakelijkerwijs op de hoogte zijn van cyberbeveiliging en AI. Digitalcity.brussels zal haar aanbod aan sensibiliserings-/initiatiecursussen voor medewerkers versterken en promoten.
   → Bijvoorbeeld: Cybersecurity Fundamentals, Hacking vermijden en Prompt Engineering.
2. **Publiek:** werkzoekenden, bedrijven inclusief kmo's.

9.3 SENSIBILISEREN en informeren

Naast een voortdurend evoluerend aanbod aan opleidingen en een analyse van de behoeften van bedrijven is bewustmaking een essentieel onderdeel van de opdracht van Digitalcity.brussels.

Evenement: AI en cyberworkshopst

1. **Doelstellingen:** synergie tussen opleidingsinstellingen en bedrijven in de AI- en cybersector om perspectieven en beroepen te bieden in de digitale beroepen van de toekomst. Meer bekendheid geven aan loopbanen in AI en cyberbeveiliging.
2. **Doelgroep:** jonge werkzoekenden, studenten, mensen die geïnteresseerd zijn in deze thema's en meer willen weten over de diversiteit van de betrokken beroepen.
3. **Kalender:** 15 oktober 2024
4. **Details evenement:** inleidende workshops in cyberbeveiliging en kunstmatige intelligentie. Workshops gericht op nieuwkomers die aarzelen om in dit beroep te starten, evenals stagiairs die een inleidende opleiding in deze domeinen volgen. Deze workshops worden aangevuld met getuigenissen en demonstraties die inzicht geven in de relevante beroepen.

Informatiesessie: focus op het tekort aan beroepen in cyberspace en AI

1. **Doelstellingen:**
   IT-beroepen toelichten en de diversiteit aan beroepen en competenties in de technische beroepen promoten. Digitalcity.brussels en haar missies presenteren. Medewerkers van werkwinkels helpen met hun advies.
2. **Doelgroep:** werkzoekenden en medewerkers van tewerkstellings- en opleidingsinstellingen.
3. **Kalender:**
   2024: informatiesessie voor tewerkstellings- en opleidingsinstellingen. Frequentie: 2 per jaar.

ONZE EXPERTS

Voor het opstellen van dit verslag vroegen we deskundigen ter zake om deel te nemen aan individuele interviews voor hun advies over de onderwerpen die in de analyse aan bod kwamen. We willen hen bedanken voor hun bijdrage en tijd.

- **NATHANAEL ACKERMAN**
  Chief Evangelist Officer - IA4Belgium
- **GEOFFROY ALSTEENS**
  Cloud and AI Advisor - Paradigm.brussels
- **GEORGES ATAYA**
  Professor - Solvay Brussels School
- **GUNTHRAM CORNERLIS**
  Program Manager Digital Business - Sirris
- **VINCENT DEFRENNE**
  Director Cyber Strategy & Architecture - Nviso
- **ALICE DEMARET**
  AI impact Advisor - ULB
- **FRANCK DUMORTIER**
  Onderzoeker - VUB
- **NOÉMIE HONORÉ**
  Partner en Manager
  Wavestone België
- **JEAN KERVYN**
  Projectmanager - CCB
- **AXEL LEGAY**
  Professor en oprichter van Cyberwal
  by Digital Wallonia – UCL / CyberWal
- **YVES ROGGEMAN**
  Professor Computerwetenschappen - ULB
- **ERIC VAN CANGH**
  Senior Business Group Leader Digital - Agoria

Digitalcity.brussels

Pool Opleiding Werk voor digitale beroepen

Digitalcity Brussels
6 Jules Cockxstraat
1160 Brussel
02 475 20 00
info@digitalcity.brussels
www.digitalcity.brussels

COPYRIGHT EN WETTELIJKE VERMELDINGEN

VERANTWOORDELIJKE UITGEVER
Jean-Pierre Rucci
jp.rucci@digitalcity.brussels

REDACTEUR
Christina Galouzis
christina.galouzis@digitalcity.brussels

DESIGN & COMMUNICATIE
Noémie Valcauda
noemie.valcauda@digitalcity.brussels

VERTALING
Luc Huygh
luc.huygh@digitalcity.brussels

POSTPRODUCTIE
Noémie Valcauda - Luc Huygh

FOTOCREDITS
Unsplash.com

ONTWERP & LAY-OUT
PointRelay
vincent@pointrelay.be

Is een initiatief van

actiris.brussels
BRUXELLES FORMATION former pour l'emploi
VDAB
AGORIA
Beci
SETCa-BBTK FGTB-ABVV
CNE L'avenir a son syndicat
CGSLB ACLVB

Met de steun van

RÉGION DE BRUXELLES-CAPITALE
BRUSSELS HOOFDSTEDELIJK GEWEST
Francophones Bruxelles
beliris POUR BRUXELLES VOOR BRUSSEL
Avec le soutien du Fonds social européen
Met de steun van het Europees sociaal fonds