Vlaamse Regering

DE VLAAMSE MINISTER VAN WERK, ECONOMIE, WETENSCHAP, INNOVATIE, EN SPORT

QUATERNOTA AAN DE VLAAMSE REGERING

Betreft: Vlaams Beleidsplan Cybersecurity

1. SITUERING

1.1 Wat is cybersecurity (CS)?

Cybersecurity is van cruciaal belang voor onze welvaart en onze veiligheid. Naarmate ons dagelijks leven en onze economieën meer vervlochten raken met digitale technologieën, worden we kwetsbaarder.

Cybersecurity is doorheen de jaren uitgegroeid tot een belangrijke wetenschappelijke discipline gelieerd aan de computer- en ingenieurswetenschappen. Concreet definieert PwC (benchmarkingstudie, 2018) cybersecurity op basis van de Rolay Hollaway University of London als *"alle aspecten van beveiliging die weerslag hebben op de cyberspace. Het heeft betrekking tot de technische aspecten zoals cryptografie en access control die gebruikt worden om data te beschermen, maar ook tot de operationele en managementmechanismen die gebruikt worden om digitale systemen te besturen en te onderhouden."*

De voornaamste inbreuken als gevolg van tekortkomingen in cybersecurity zijn volgens PwC onder andere phishing, malware, menselijke fouten, diefstal of verlies van gegevens. Bovendien worden cyberincidenten steeds diverser, waarbij soms geopolitieke strategieën meespelen. Kwaadwillige cyberactiviteiten vormen op die manier niet alleen een bedreiging voor onze economieën en de ontwikkeling van de digitale eengemaakte markt, maar ook voor onze democratieën, onze vrijheden en onze waarden. Een op vertrouwen gebaseerde digitale economie waarbij data en artificiële intelligentie alsmaar aan belang winnen, kan daarom niet anders dan gelijktijdig een strategie en investeringsimpuls rond cybersecurity te voorzien.

1.2 Internationale omgevingsanalyse: een sterke Vlaamse uitgangspositie

Tegen 2021 stelt PwC dat het budget voor cybersecurity wereldwijd meer dan één triljoen dollar zal bedragen. De Global Security Index (GCI) van de Verenigde Naties rankt Singapore, De Verenigde Staten, Maleisië, Oman, Estland, Mauritus, Australië, Georgië, Frankrijk en Canada als de tien landen die zich het meest inzetten voor cybersecurity. België bevindt zich in deze ranking op een 30ste plaats, waarbij cybersecurity wordt gemeten op 5 aspecten: juridisch, technisch aspect, organisatie, samenwerking en capaciteitsopbouw.

Gezien de omvang van de budgetten, de bestaande schaalvoordelen en het sterke digitale ecosysteem van onderzoek, take-up van het bedrijfsleven, onderwijs et cetera kan de Verenigde Staten zich wereldwijd leider noemen in het gebied van cybersecurity. Al moet gezegd dat China aan een inhaalbeweging bezig is.

Hoewel Europa niet over dezelfde schaalvoordelen beschikt, beschikken landen als Estland en Frankrijk over sterke posities waar Europa op kan verder bouwen. Ook België en in het bijzonder Vlaanderen hebben een goede reputatie, zeker op het vlak van onderzoek met wereldwijd vermaarde en geïmplementeerde (Leuvense) cryptografie (zie infra).

Tot slot komt vaak het belang en de wisselwerking tussen cybersecurity en militaire veiligheidsaspecten naar boven, wat ook de sterke internationale positie van Israël mee helpt verklaren.

1.3 Europese beleidsagenda

Cybersecurity vormt al langer een belangrijk onderdeel van de Europese beleidsagenda, met het Europees agentschap voor informatie- en netwerkbeveiliging (ENISA) als expertisecentrum dat lidstaten en private sectoren bijstaat met advies en oplossingen.

De groeiende uitdagingen leidden in 2013 tot een Cybersecurity Strategie met als doelstelling om een betrouwbaar, veilig en open cyberecosysteem te bevorderen. Een belangrijke stap hiertoe is de zogenaamde 'network and information systems directive', vaak afgekort als NIS Directieve uit 2016. Dit is de eerste Europese wetgevende actie rond cybersecurity die als doelstelling heeft de nationale cyberrisico's beter te stroomlijnen en de awareness te vergroten. Hiertoe werden nationale contactpunten aangeduid die moeten instaan als aanspreekpunt. In België is dit het Centrum voor Cyberbeveiliging (CCB, zie infra).

Door de snelle evoluties in het digitale landschap en bijhorende risico's heeft de Europese Commissie in 2017 een communicatie naar het Parlement en de Raad gebracht met als titel *"weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU".* Deze communicatie, voortbouwend op vorige initiatieven, zet een aantal potentiële maatregelen uit zoals het versterken van ENISA, het creëren van een vrijwillig unie-wijde cybersecurity certificatiekader, coördinerende antwoorden op grote incidenten en werd erkend dat

"it is also in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services."

De communicatie overweegt bovendien de mogelijkheid om de cybersecurity-capaciteit van de Unie te versterken via een netwerk van cyberbeveiligingscompetentiecentra met een Europees Cybersecurity Competence Center als kern, als aanvulling op bestaande zaken om op deze manier de capaciteit in Europa rond cybersecurity fundamenteel te versterken.

Deze plannen worden momenteel binnen de verschillende overlegstructuren besproken, en zullen vanaf het nieuw meerjarig financieel kader (MFK) in nauw verband staan met het 'Digitaal Europa Programma' (DEP) en Horizon Europe. Waar Horizon Europe mogelijk cybersecurity-onderzoek zal financieren, is DEP een nieuw programma gericht op disseminatie en capaciteitsversterking in nieuwe, aan elkaar gelinkte technologiedomeinen zoals AI, cybersecurity en high performance computing.

1.4 Vlaamse opportuniteiten

De hierboven geschetste technologische en internationale ontwikkelingen maken dat indien Vlaanderen een weerbare digitale economie wil uitbouwen, investeringen in cybersecurity noodzakelijk zullen zijn. Vlaanderen kan hiervoor voortbouwen op bestaande sterktes.

De sterkte van Vlaanderen ligt in de eerste plaats in haar wereldwijd vermaard onderzoek. Miljarden toepassingen dragen Vlaamse cryptografie in zich. Hoewel diverse universiteiten sterk staan in het domein van cybersecurity, zijn het voornamelijk de Leuvense onderzoeksgroepen COSIC en DistriNet die de Vlaamse onderzoekswereld wereldwijde bekendheid bezorgen, waarvan de *Advanced Encryption Standard* (AES, ook wel "Rijndael" genoemd naar de betrokken professoren) het uithangbord is. Met evoluties zoals high performance/quantum computing en de steeds meer digitale leefwereld blijft het een opportuniteit om dit onderzoek in Vlaanderen verder te ondersteunen.

Dit onderzoek vertalen in concrete toepassingen en ingang doen vinden in de Vlaamse bedrijfscontext is misschien wel de grootste opportuniteit. In het verleden werd cybersecurity te vaak als een 'burden' gezien, zonder te beseffen dat het een essentieel onderdeel is van een betrouwbare, duurzame digitale keten. Dit inzicht is aan het veranderen door de vele internationale evoluties en moet aangegrepen worden om de Vlaamse burgers en bedrijven te ondersteunen om cybersecurity-toepassingen in hun processen en leefwereld doordacht te laten implementeren. Dit sluit aan bij een steeds grotere interesse vanuit klassieke industriële takken om hun productieprocessen aan de 4^{e} industriële revolutie aan te passen. Een goed werkend ecosysteem kan bovendien een hefboom creëren voor deze industriële adoptie. Een samenspel van sterke Vlaamse sectorfederaties, clusters, acceleratoren, universiteiten en kennisinstellingen is samen best geplaatst om de specifieke adoptie van cybersecurity naar hun doelgroep te initiëren, faciliteren, versnellen en maximaal te ondersteunen. Ook de overheden hebben een proactieve rol te spelen heeft, onder meer door zelf het goede voorbeeld te geven.

1.5 Nood aan een Vlaams geïntegreerde beleidsagenda in drie luiken

We kunnen stellen dat we vandaag in Vlaanderen een sterke, hoogkwalitatieve basis hebben. Gelet op de snelle evolutie van het cybersecurity-domein en de initiatieven in de ons omringende landen, is het echter noodzakelijk deze kritische massa significant te versterken en te vergroten. Nadruk hierbij moet liggen op de impact op het economisch weefsel, het behoud en versterken van excellentie, meer en sneller lokaal valoriseren van beschikbare technologieën, en tevens een drastische toename van de talentbasis gelet op de noden die op de arbeidsmarkt voor dit domein zullen ontstaan.

Een coherente beleidsagenda vertrekt daarom van een geïntegreerde benaderingen van de gehele kennisketen van onderzoek tot absorptie in het economisch en maatschappelijk weefsel.

Daarom dient de Vlaamse beleidsagenda te bestaan uit drie luiken:

- (1) *Investeren in top strategisch basisonderzoek* gericht op het ontwikkelen van nieuwe kennis, wetenschappelijke doorbraken en talent op wereldniveau daar waar Vlaanderen reeds excellent presteert én waar de synergie kan bekomen worden met de vraaggedreven implementatie-agenda van het Vlaamse bedrijfsleven.

- (2) *Een centrale focus op de implementatie van cybersecurity-toepassingen in het bedrijfsleven*. Een vraaggedreven agenda vanuit het bedrijfsleven moet via open, goed georganiseerde kanalen en netwerken gebracht worden tot bestaande overheidsinstrumenten (van voornamelijk het Vlaams Agentschap Innoveren en Ondernemen, VLAIO) en relevante instellingen.

- *(3) Een sterk flankerend beleid waarin naast op de significante opleidingsnoden voor de arbeidsmarkt ook op het vlak van juridische en ethische aspecten van cybersecurity wordt gewerkt.* En waarbij de centrale focus ligt op een correcte doch ambitieuze *outreach* naar de bevolking zodat cybersecurity niet enkel als een *burden* wordt gezien maar als een noodzakelijke bouwsteen voor bedrijven en samenlevingen in een digitale omgeving.

2. VOORGESCHIEDENIS VAN DE TOTSTANDKOMING VAN HET VLAAMS BELEIDSPLAN CYBERSECURITY

2.1. Benchmarkstudie uitgevoerd door PwC in het voorjaar 2018

In haar rol van beleidsvoorbereiding heeft het Departement EWI in het voorjaar van 2018 een benchmarking uitgevoerd via een overheidsopdracht uitgevoerd door het consultancybureau PwC met een drieledige opdracht:

- De huidige ontwikkelingen in Vlaanderen op het gebied van cybersecurity in kaart brengen;
- De positie van Vlaanderen vergelijken met een aantal landen, zowel binnen als buiten Europa;
- Aanbevelingen formuleren als basis voor het uitwerken van beleidsinitiatieven en overheidsinterventies om de ontwikkelingen op het vlak van cybersecurity in Vlaanderen verder te ondersteunen.

Door bevragingen en bureauonderzoek heeft deze studie ons een actueel beeld gegeven van het Vlaamse en internationale landschap. Dit gebeurde voor elke component van het cybersecurity-ecosysteem: onderwijs, onderzoek, bedrijven, beleidsinitiatieven en beveiligingsbewustzijn.

2.2. Stakeholderdag op 3 juli 2018

Deze benchmarkingstudie vormde een eerste omgevingsanalyse die daarbij de basis vormde om het betrokken werkveld in Vlaanderen samen te brengen op een stakeholdersdag georganiseerd door het Departement EWI in samenspraak met Agoria, als relevante sectorfederatie.

De stakeholdersdag vond plaats op 2 juli 2018 en bracht, in lijn met de triple-helix constellatie, alle relevante actoren samen vanuit de overheid, universiteiten en kennisinstellingen en het bedrijfsleven en hun vertegenwoordigers. De benchmarkingstudie van PwC en de voorbereiding van de stakeholdersdag op 2 juli maakte duidelijk dat Vlaanderen over diverse actoren beschikt met een goede uitgangspositie om Vlaanderen te versterken op het vlak van cybersecurity. Zij maken samen deel uit van het bestaande Vlaamse ecosysteem. In opvolging van de benchmark studie ging de Vlaamse overheid in interactie met het werkveld om relevante, onderbouwde beleidsopportuniteiten verder te identificeren. Te meer een transversale technologie als cybersecurity ook transversaal moet aangepakt worden doorheen de kennisketen met de actieve spelers in Vlaanderen.

3. VLAAMS BELEIDSPLAN CYBERSECURITY

3.1. Een geïntegreerd CS-plan in drie luiken, kaderend in de Vlaamse digitaliseringsstrategie

Vlaanderen zet op dit ogenblik breed in op de digitalisering van de samenleving. De digitalisering van de overheid wordt onder meer ondersteund via het Programma Innovatieve Overheidsopdrachten en de werking van het Agentschap Informatie Vlaanderen (AIV). De digitalisering van de gemeenten wordt ondersteund met de werking Smart Flanders, de oproep Smart Cities van VLAIO en de city of things proeftuin. Inzake de digitalisering van het bedrijfsleven speelt VLAIO vandaag al een belangrijke rol via haar gehele instrumentarium, en zeker ook via het trekkerschap van de transitie Industrie 4.0. Met dit beleidsplan cybersecurity wil de Vlaamse regering een bijkomende impuls geven aan de digitalisering van het Vlaamse bedrijfsleven en aan de adoptie van cybersecurity technologie in het bijzonder.

Het plan Cybersecurity bestaat zelf uit drie delen:

1. versterken top CS-onderzoek in Vlaanderen
2. implementatie in het Vlaamse bedrijfsleven
3. flankerend beleid gericht op bewustmaking, opleiding en ethische omkadering

Ten eerste is er het top basisonderzoek. Enerzijds leidt strategisch onderzoek dat aansluit bij de industriële vragen en noden tot nieuwe en differentiërende mogelijkheden voor de Vlaamse industrie. Anderzijds worden de internationale sterktes van het cybersecurityonderzoek in Vlaanderen verder uitgebouwd; wat onze regio in staat stelt toponderzoekers (bv. internationale doctoraatsstudenten en postdoctorale onderzoekers) aan te trekken die later doorstromen naar het cybersecurity human capital in Vlaanderen.

Ten tweede is er de ondersteuning van het industriële landschap bij innovatie op het vlak van cybersecurity. Dit implementatieluik beoogt in eerste instantie het delen van cruciale kennis op de meest toegankelijke, laagdrempelige wijze. Het programma beoogt in tweede instantie het begeleiden van bedrijven bij een verbeteringstraject op het vlak van cybersecurity. Complementaire elementen bij het implementeren van cybersecurityinnovatie zijn piloot- en demonstratieprojecten voor grotere groepen van bedrijven met een gemeenschappelijke noemer (enkele voorbeelden: een sector zoals de financiële sector, gebruikers van een type platform zoals hybride cloud-omgevingen of organisaties met een gelijkaardige cybersecuritymaturiteit). Tot slot zijn er onderzoeksprojecten zoals o.a. toegepast onderzoek binnen bedrijven en ICON-projecten (collaboratief onderzoek).

Ten derde is er de training en opleiding voor de industrie. Het programma ontwikkelt en levert industrieopleidingen op het vlak van cybersecurity (zoals aangegeven gericht op een ruim en gevarieerd doelpubliek. Het aanbod is gestoeld op sterke bestaande componenten (internationaal, academisch, en technologisch). Het wordt zo efficiënt mogelijk uitgerold, met MOOC's (online) waar mogelijk en met een sterke regionale aanwezigheid, dicht bij de bedrijven. Naast bovenstaande opleiding is er ook een ruime disseminatie van nieuwe cybersecuritytrends en actuele informatie, enerzijds met het oog op een groeiende awareness en sensibilisatie, maar ook als wegwijzer voor de meer geavanceerde spelers.

Deze drie delen worden hieronder meer in detail toegelicht. Maar eerst wordt de governance kort geschetst.

3.2. Governance van het cybersecurity beleidsplan

Bij de uitwerking van het CS-beleidsplan staan een aantal principes voorop:

1. Er worden geen nieuwe juridische structuren opgericht: het programma loopt dwars door een aantal bestaande (overheids)organisaties heen en wordt gecoördineerd aangestuurd en uitgevoerd vanuit een triple helix filosofie in samenwerking tussen overheid, kennisinstellingen en bedrijven;

2. Het programma staat voor de uitvoering en deelname open en is toegankelijk voor elke relevante stakeholder, die dus expertise, knowhow of toegang tot een doelgroep heeft;

.

3. Er wordt gewerkt met zowel de open indiening via de bestaande steunkanalen als met open calls/aanbestedingen om de meeste assen van het programma in te vullen, en daarbij wordt maximaal een beroep gedaan op de bestaande instrumenten van de Vlaamse overheid en bouwend op de sterktes van het bestaande Vlaamse ecosysteem;

4. Voor het luik "top strategisch basisonderzoek" wordt gewerkt met een programmatorische aanpak, met deels gerichte calls naar projecten, die strategisch gestuurd worden en regelmatig extern gevalideerd op vlak van lokale Vlaamse relevantie en internationale excellentie;

5. Er wordt systematisch ingezet op samenwerkingen tussen verschillende actoren.

6. De calls / topics / strategische onderzoeksthema's / gebruikte instrumenten / … evolueren over de tijd in functie van de behoefte in de markt en worden bepaald via een grondig roadmapping proces met regelmatige validatie vanuit de industriële vraagzijde;

7. Projecten/thema's worden steeds extern objectief, neutraal geëvalueerd en internationaal getoetst;

3.2.1. Stuurgroep CS-programma

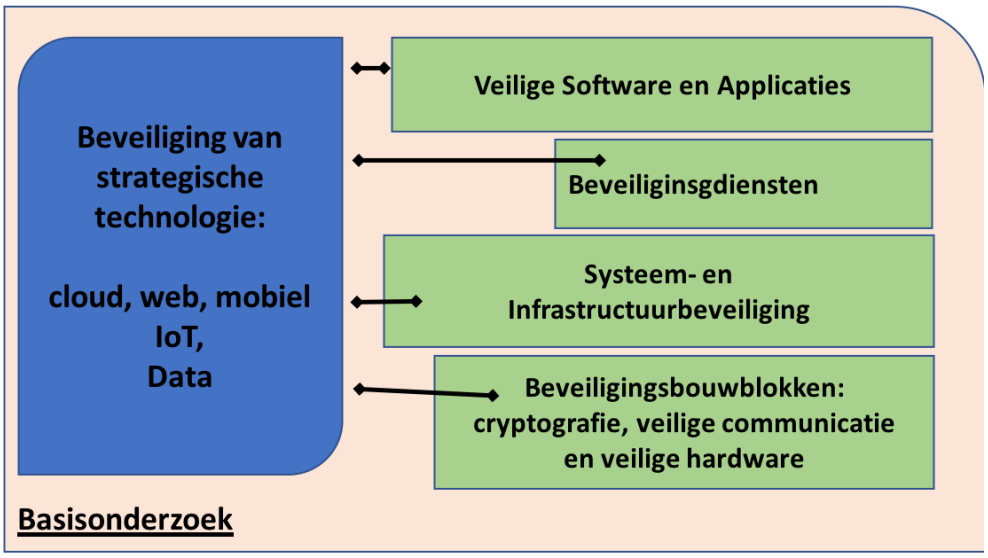
Het globale programma wordt opgevolgd door een stuurgroep die opgezet wordt onder leiding van Vlaio en het departement EWI met een vertegenwoordiging van de relevante stakeholders uit het bedrijfsleven en het onderzoeksveld. Om deze stuurgroep slagkrachtig te laten beslissen telt zij maximaal 12 leden, waarbij de verschillende stakeholders werken via het principe van vertegenwoordiging uit hun bestaande overlegstructuren. Op deze stuurgroep wordt de werking en impact van het programma geëvalueerd en waar nodig bijgestuurd. Er wordt in het bijzonder aandacht besteed aan de industriële relevantie van het programma door het betrekken van relevante bedrijven als klankbord voor de implementatie en de wetenschappelijke relevantie door het programma op gezette tijden extern te laten benchmarken op zijn wetenschappelijke impact op internationale schaal door internationale experts, teneinde de focus te behouden op die onderzoeksdomeinen waar Vlaanderen het verschil kan maken.

De samenstelling van de stuurgroep zal voorwerp uitmaken van een afzonderlijke beslissing van de Vlaamse Regering. Wanneer in het programma zich in het onderzoek of implementatieluik een vraag inzake dual-use met militaire toepassingen voordoet zal dit voorgelegd worden aan het ethisch en strategisch comité in het kader van dual use O&O zoals dit binnen Vlaio is opgezet.

3.3. Luik 1: het versterken van top strategisch basisonderzoek CS in Vlaanderen

Het basisonderzoek volgt vier lange termijn trajecten: (1) Veilige Software en veilige applicaties, (2) beveiligingsdiensten (in de zin van kritische beveiligingscomponenten die men bijna altijd moet integreren in applicaties en platformen), (3) systeem en infrastructuurbeveiliging en (4) basisbouwblokken waaronder veilige hardware, communicatie en cryptografische algoritmen en protocollen. Deze onderzoekslijnen vormen een stabiel kader op lange termijn, waarbinnen uiteraard regelmatig nieuwe thema's aan bod kunnen komen.

Onderstaande figuur illustreert meteen ook dat de vier voorgestelde onderzoekslijnen bijdragen tot cybersecurityoplossingen die kunnen ingezet worden in de belangrijke strategische ICT trends en technologieën waarmee de digitale economie geconfronteerd wordt. De KU Leuven neemt de coördinatie op van dit luik.



(A) Onderzoekslijn 1: Software- en Applicatiebeveiliging

Voor een grote fractie van de veiligheids-incidenten is de uitbuiting van een of andere software-zwakheid een sleutelelement. Dit bevestigt de nood aan basisonderzoek over de kwaliteit van beveiligingssoftware en applicatielogica en de betrouwbare koppeling tussen beide. Er wordt ingezet op drie belangrijke uitdagingen: (1) het ondersteunen van een beveiligingsmethodiek die toepasbaar is in de volledige levenscyclus van software en applicaties; (2) het ontwikkelen van verificatietechnologie die harde garanties kan leveren voor belangrijke (beveiliging)kritische eigenschappen van software en (3) kerntechnologie die toekomstige softwareontwikkelingen inherent veiliger kan maken.

(II) SDLC, beveiliging gedurende de levenscyclus van softwareapplicaties

De creatie, ontwikkeling en ondersteuning van veilige softwareapplicaties en diensten vormt een inherent grote uitdaging. Er werd al heel wat vooruitgang geboekt op dit terrein: op het vlak van (1) het modelleren van kwetsbaarheden, aanvalsscenario's en misbruiken, (2) het modelleren van beveiligde oplossingen (Security by Design en Privacy by Design, o.a. met beveiligingspatronen) en (3) het aanleveren van veilige code en het ontwikkelen van systematische beveiligingstesten.

Verdere verbeteringen zijn noodzakelijk, samen met de georkestreerde toepassing van deze technieken in de context van een volledige levenscyclus waarin ook andere ontwikkelingsactiviteiten aan bod komen die deels los staan van beveiliging. Hierbij moeten een aantal best of breed technieken gecombineerd worden. In functie van de maturiteit van de organisatie die het interne beveiligingsproces wil verbeteren kan dit leiden tot lichtvoetige (agile) beveiliging of tot intensieve processen met uitgebreide testprocedures en certificatie.

(III) Programmaverificatie

Statische programma-analyses leiden informatie over het gedrag van een applicatie volautomatisch af uit diens broncode en laten toe om zwakheden of ongewenst gedrag te detecteren. Het is een belangrijke uitdaging om de precisie en schaalbaarheid van een analyse te garanderen voor applicaties met inherent niet-determinisme en om statische analyse geschikt te maken om garanties te bieden bij verplichte kwaliteitscontroles (reviews) en om ze bij updates te laten schalen in functie van de grootte van de verandering aan de broncode. Voor de meest beveiligingsgevoelige componenten in software of voor kritische software is er nood aan schaalbare programma-verificatie, die ontwikkelaars toelaat om (met minimale inspanning) op een formele manier de afwezigheid van klassen van beveiligingsproblemen en implementatiefouten te bewijzen.

Dynamische programma-analyses zijn complementair aan statische analyses: zij voeren een applicatie uit om het gedrag ervan te observeren of om over datzelfde gedrag controle uit te oefenen en het te wapenen tegen zwakheden. De belangrijkste uitdagingen zijn het combineren van transparantie (geen beïnvloeding van het gedrag), volledigheid en het omgaan met dynamische applicaties, waarbij componenten van derden geïntegreerd worden tijdens de uitvoering (bv. de cliëntzijde van webapplicaties).

(IIII) Veilige programmeertalen en veilige compilatie

Veel aanvallen tegen software zijn gebaseerd op het uitbuiten van implementatie-details van de software of de onderliggende infrastructuur. Heel bekende klassieke voorbeelden zijn de geheugenbeheer-zwakheden zoals buffer overflows, of injectie-aanvallen zoals SQL injection of script injection. Nieuwere voorbeelden zijn de recente micro-architecturale zijkanaal-aanvallen zoals Spectre, Meltdown en Foreshadow.

Er is onderzoek nodig naar een automatische bescherming tegen deze klasse van problemen die kan ingebouwd worden in raamwerken, compilers en systeemsoftware. Een bijzondere uitdaging vormen de logische zwakheden, fouten in de softwarelogica die minder verband houden met de onderliggende infrastructuur en meer met de toepassing zelf. Er zal onderzocht worden in welke mate programmeertalen meer ondersteuning kunnen bieden voor het uitdrukken en afdwingen van toepassingspecifieke veiligheidsvereisten. Dit kan via statische type-systemen (bv om via typering aan te geven welke informatie confidentieel is) of via programmeertaalontwerp (bv door

via een capability-safe ontwerp van de taal, sterke garanties te geven over de isolatie van minder vertrouwde code).

Voor software die niet op één computer draait, maar op een gedistribueerd systeem, kan deze ondersteuning worden ingebouwd in programmeertalen of raamwerken die op een geschikte manier abstractie maken van details rond deployment, coördinatie en communicatie. Door deze abstracties vervolgens te voorzien van de nodige parametrisaties, kunnen veiligheidsaspecten op een samenstelbare wijze worden uitgedrukt. Dat laatste is cruciaal nu software bijna per definitie gedistribueerd is en opgebouwd is uit componenten die in verschillende programmeer-paradigma's en talen werden geschreven, en meestal ook ontwikkeld worden door verschillende teams.

Er is een sterke synergie tussen veilige programmeertalen en veilige compilatie in de zin dat eens toepassingspecifieke veiligheidsvereisten expliciet gemaakt worden in de broncode, het ook mogelijk is voor compilers en systeemsoftware om die vereisten af te dwingen tegen krachtige aanvallers die niet enkel de applicatie-logica maar ook implementatiedetails van de onderliggende infrastructuur trachten uit te buiten. Een belangrijke uitdaging hierbij is het aanbieden van sterke garanties over de veiligheid van dergelijke compilers en systeemsoftware, bijvoorbeeld door te werken met computer-verifieerbare veiligheidsbewijzen.

(B) Onderzoekslijn 2: Kritische beveiligingsdiensten voor diverse platformen

Een groot aantal beveiligingsoplossingen steunt op de controle van gebruikers, op basis van hun identiteit of toegekende rechten en persmissies, en op de evaluatie of de gebruiker in kwestie de toelating heeft om functionaliteit uit te voeren, toegang te krijgen tot informatie, enz. Deze beveiligingsfunctionaliteit wordt geleverd door kritische beveiligingsdiensten die gebaseerd zijn op authenticatie, autorisatie en audit. Dit onderzoeksdomein evolueert zeer snel en wordt bovendien uitgebreider, aangezien het verregaand gebruik van diverse databronnen de complexiteit van deze uitdaging aanzienlijk heeft verhoogd.

(I) Identiteitsbeheer en Authenticatie

De creatie van authenticatiesystemen die op naadloze wijze kunnen samenwerken met een groeiend palet van applicaties en platformen vormt een belangrijke uitdaging. De kosten die gepaard gaan met het betrouwbaar beheren van gebruikers, identiteit en de daaraan gekoppelde platformen voor toegangscontrole is zeer hoog, zowel voor de gebruikers als voor de partijen die onlinediensten en applicaties aanbieden. Het vereiste onderzoek streeft dan ook naar oplossingen die enerzijds beveiliging, transparantie en privacy verhogen, en tegelijk de drempel en lasten (friction) voor de gebruiker beperken. Een belangrijk onderzoeksthema in deze context is het benutten van een groot aantal sensoren die meer en meer aanwezig zijn in slimme apparaten en omgevingen: deze maken het mogelijk oplossingen te bouwen die het gedrag van de gebruiker nauwkeurig herkennen (gedragsgebaseerde biometrie). Uiteraard volgt hieruit een grote en bijkomende uitdaging om de beveiliging (authenticatie) in kwestie te beschermen tegen nieuwe aanvallen en misbruik. Het wordt belangrijk de robuustheid van diverse oplossingen te verhogen en meteen ook een antwoord te bieden voor de belangrijke vereisten op het vlak van privacy.

(II) Autorisatie en Audit

Autorisatie en audit vormen samen met authenticatie de zogenaamde AAA-diensten: wanneer een gebruiker correct herkend werd door middel van authenticatie, dan dient een digitaal platform

vervolgens na te gaan of de gebruiker in kwestie wel degelijk de toestemming krijgt om bepaalde acties en operaties uit te voeren. Dit gebeurt in principe door middel van autorisatie. Het is een bijzondere uitdaging autorisatie aan te leveren die gelijktijdig veilig en performant is, robuust in een omgeving met aanvallers en bovendien duidelijk voor alle belangrijke actoren: eindgebruikers, beheerder van de platformen en eigenaars (exploitanten) van digitale applicaties. Precies omwille van efficiëntiecriteria worden in de praktijk vaak operaties toegestaan zonder dat een volledige en volwaardige controle uitgevoerd werd. Op basis van een grondige analyse van de historiek vult een auditproces de autorisatiediensten dan aan door post factum de relevante informatie verder te analyseren.

Het belang van auditoplossingen gaat uiteraard verder dan dat. Het gaat in principe om een groeiend aantal vereisten op het vlak van cybersecurity. Hierbij biedt het grondig registreren van het gekozen beleid, de historiek van de applicatie en de acties van gebruikers en beheerders etc. ondersteuning aan derde partijen die op basis van een controlespoor (audit trail) een oordeel vellen over de exploitatie van een digitale dienst en diens beveiliging. Dergelijke technologie zal uiteraard bijdragen tot het lange termijn doel waarbij heel wat facetten van belangrijke digitale diensten gecertifieerd kunnen worden op basis van een betrouwbare audit. Hierbij is automatisering en efficiëntie van groot belang.

(IIII) Toegangscontrole voor Data en Dataprotectie

In een wereld waar de toegang tot data alsmaar belangrijker wordt spreekt het voor zich dat de klassieke beveiligingsvereisten op het vlak van authenticatie en autorisatie nieuwe oplossingen vergen voor een dataspecifieke context. Zo zijn klassieke technieken bijvoorbeeld onvoldoende schaalbaar om toe te passen telkens er een element een dataset opgevraagd wordt; evenmin is het toelaatbaar grootschalige zoek of selectieoperaties toe te laten op een dataset waarvan een aantal elementen mogelijk niet toegankelijk (mogen) zijn voor de aanvrager van de operatie. Daarom is er een belangrijke nood aan basisonderzoek dat zich specifiek richt op toegang tot de data.

Een strategie die snel aan belang wint is veilige en betrouwbare dataverwerking waarbij de gegevens beschermd blijven tijdens de verwerking, ofwel omdat ze opgeslagen blijven op meerdere beveiligde servers of verwerkt worden in een geëncrypteerd formaat; dit kan op basis van geavanceerde technologieën zoals Multi-Party Computation (MPC) en (Somewhat) Fully Homomorphic Encryption ((S)FHE). Voor specifieke toepassingen kan gebruik gemaakt worden voor speciale oplossingen zoals Functional Encryption, Private Information Retrieval en Private Set Intersection. Al deze technieken bieden een optimale veiligheid, maar door hun hogere kost (vereiste rekenkracht en/of communicatie) zijn ze niet altijd schaalbaar. Daarom worden ze aangevuld met data access middleware, die op basis van de rechten van de gebruiker en het beveiligingsbeleid van de eigenaar van de data, ervoor zorgt dat de zichtbare dataelementen correct geselecteerd worden. Ook hier is er nood aan onderzoek om voldoende krachtige en efficiënte technieken beschikbaar te stellen.

Ten slotte is er een belangrijke, bijkomende nood aan anonimisering van data, in het bijzonder in het licht van de huidige regelgeving omtrent privacy. Een zeer belangrijk deel van de hier onderzochte technieken is gebaseerd op geavanceerde toepassingen van cryptografie. Dit omvat ook technieken die het mogelijk maken om statistische analyses uit te voeren en informatie af te leiden over groepen, zonder informatie over individuele gebruikers prijs te geven (zoals pseudonimisering, sanitizatie, aggregatie en het verstoren van gegevens met ruis op basis van differentiële privacy).

(C) Onderzoekslijn 3: Systeem- en infrastructuurbeveiliging

Deze onderzoekslijn bevat naast de voor de hand liggende systeem- en infrasctuctuurdimensie ook een activiteit die de beveiligingsbeheer en –operaties ondersteunt, en een multidisciplinair luik dat de nodige aandacht geeft aan policy en regelgeving.

(I) Systeembeveiliging

Elk systeem, gaande van diensten in de cloud tot kleinschalige embedded sensoren, vergt een combinatie van hard- en software om correct te functioneren. Systeembeveiliging wordt geadresseerd op twee vlakken: schaalbare basistechnieken en ondersteuning voor gedecentraliseerde beveiliging.

Schaalbare basistechnieken. Systeembeveiliging wordt gekenmerkt door een voortdurende wedloop tussen aanvals- en verdedigingstechnieken.

Dit vereist verregaand basisonderzoek waarbij noodzakelijke beveiligingseigenschappen nagestreefd worden: mogelijkheid tot fijnkorrelige isolatie, run-time attestatie en garanties omtrent de integriteit van software, data en control flow. Ook het in kaart brengen van de beschikbare en meest waarschijnlijk geëxploiteerde aanvalsvectoren vereist continu onderzoek. Oplossingen voor systeembeveiliging vertrekken van hard- en software co-design en moeten schaalbare mechanismen opleveren, bijvoorbeeld op basis van beperkte uitbreidingen van de instructieset, of door het toevoegen van processormodi of nieuwe componenten in het run-time systeem, etc. Het gebruik van de ontwikkelde oplossingen dient zoveel mogelijk geautomatiseerd en moet voldoen aan niet-functionele beveiligingsvereisten die aangepakt worden met de nodige tools (o.a. compilers). Indien voorgestelde oplossingen immers teveel manuele interventies vereisen door ontwikkelaars, dan is de kans op fouten te groot en het praktisch gebruik te duur en te omslachtig.

Gedecentraliseerde beveiliging. Een tweede onderzoeksactiviteit in dit luik adresseert gedecentraliseerde beveiliging. Dit thema vormt een essentiële vereiste voor het beheren en opereren van autonome systemen. Hierbij wordt er onderzoek geleverd op het vlak van gedecentraliseerde detectie van bedreigingen en gedecentraliseerde respons.

(II) Netwerkbeveiliging

Kerntechnologie van het moderne Internet werd in de 70er jaren geïntroduceerd. Vandaag zijn de bouwstenen waarmee gewerkt wordt zoals bv. routering met BGP en adressering met DNS relatief bekend. Daarbij zijn er ook een aantal securitybeperkingen zeer zichtbaar en vaak te gemakkelijk exploiteerbaar door aanvallers. Vergelijkbare observaties kunnen gemaakt worden voor een aantal andere infrastructuurcomponenten zoals PKI (public key infrastructure) die essentieel is voor het web en voor heel wat mobiele ecosystemen. In een aantal gevallen zijn beveiligingsoplossingen bekend maar duur qua exploitatie. Daarnaast stellen draadloze en mobiele protocollen unieke beveiliginsguitdagingen, zoals bv. recent geïllustreerd met de KRACK attack die een beperking in het WPA2 protocol aantoonde.

Dit alles is ongetwijfeld van groot en voortdurend belang voor netwerkoperatoren en service providers (ISPs). Deze korte schets motiveert zonder twijfel de nood aan een doorgedreven onderzoeksinspanning op het vlak van de beveiliging en robuuste exploitatie van huidige en toekomstige netwerken, en voor de ontwikkeling van nieuwe oplossingen die alle elementen van

de netwerkprotocolstapel adresseren. De toepassing van geavanceerde cryptografie vormt een belangrijk element in de oplossingen die verder onderzocht moeten worden.

(IIII) Monitoring en Management

Het beveiligen van systemen, netwerken en kritische infrastructuur gaat gepaard met een beheeraspect. Hoe robuust het initieel geïnstalleerd systeem ook is, de evolutie van software, diensten en systemen, de voortschrijdende inzichten van aanvallers en de inherente beperkingen die gepaard gaan met eender welke beveiligingsoplossing, vergen in principe een actieve bewaking en mogelijk verdediging van heel wat omgevingen. Een belangrijk doel van onderzoek in deze context is het ontwikkelen van middelen die de verzameling, opslag, en representatieve monitoring van informatie mogelijk maken. Hierbij is de bruikbaarheid van deze informatie, in het bijzonder voor de beveiligingsanalyse en digitale bewaking, van groot belang.

Een ander belangrijk aspect is de hernieuwbaarheid en aanpasbaarheid van software binnen bestaande vereisten van de levenscyclus van die software. Het vlot kunnen updaten van software in het veld, inclusief de erin gebruikte verdedigingstechnieken om tegemoet te komen aan nieuw opduikende aanvalsvectoren, is cruciaal maar verre van triviaal. Het beheer van een geïnstalleerde basis in een context met een spatiale en temporele softwarediversiteit vereist belangrijk onderzoek op het vlak van beveiligingsbeheer.

(IV) Policy, regelgeving en economische aspecten

Het is een welbekend gegeven dat de relatief late ingebruikname van cybersecurityoplossingen een gevolg zijn van marktfalen. Het is nl. inherent moeilijk voor gebruikers, klanten en aankopers om duidelijk te evalueren welke producten en diensten een relatief betere beveiliging en privacy bieden. Er is mede daardoor (en door een gebrek aan algemeen bewustzijn en basiskennis omtrent cybersecurity) weinig motivatie om voor beveiliging te betalen. Bovendien wil niemand graag het voortouw nemen om te investeren in een gemeenschappelijke omgeving die degelijk beveiligd is, als de directe opbrengst voor de eigen organisatie beperkt is, en de verantwoordelijkheid en aansprakelijkheid (liability) onduidelijk. Een grondige en doorgedreven studie van deze mechanismen is belangrijk, om de kloof tussen technische oplossingen en hun feitelijke gebruik beter te begrijpen, en om vervolgens ook na te gaan hoe hieraan verholpen kan worden door bij te dragen aan adequate regelgeving. Verder moet er in technische oplossingen ondersteuning geboden worden om de naleving van policies (regelgeving) te beoordelen en te meten. Dit luik van het onderzoeksprogramma is een belangrijke hefboom om alle maatschappelijke actoren mee te laten evolueren met de snelle technologieontwikkeling binnen cybersecurity.

(D) Lijn 4: Technologische bouwblokken: veilige hardware, cryptografie en veilige communicatie

Beveiligingstechnologie steunt op een aantal kernbouwblokken, die in deze onderzoekslijn bestudeerd en ontwikkeld worden: veilige hardware, cryptografische algoritmen en protocollen (met inbegrip van de veilige implementatie ervan) en oplossingen voor veilige communicatie.

(I) Veilige Hardware

Halfgeleidertechnologieën ondergaan een sterke evolutie: naast het schalen volgens de wet van Moore zijn er ook andere belangrijke trends ("More than Moore"); het onderzoek bestudeert hoe procesvariaties en halfgeleiderruisbronnen kunnen aangewend worden voor beveiligingsdoeleinden zoals Physical Unclonable Functions (PUFs) en nieuwe True Random

Number Generators (TRNG's). Daarnaast worden de beveiligingseigenschappen van toekomstige geheugentechnologieën bestudeerd zoals Magnetoresistive Random Access Memory (MRAM) en Resistive Random Access Memory (ReRAM). Belangrijke onderzoeksproblemen zijn veilige opslag van cryptografische sleutels, maar ook veilige berekeningen direct in het geheugen. Het samenspel van toekomstige logica en beveiliging is een ander cruciaal onderzoeksgebied dat kan leiden tot nieuwe vormen van logica of een betere bescherming tegen fysieke aanvallen. Daarnaast wordt er onderzoek gepland naar nieuwe hardware-gebaseerde aanvalsvectoren door middel van kwaadwillige manipulatie van de toekomstige hardware, zoals bijvoorbeeld Trojaanse paarden op laag niveau. Een laatste onderzoeksgebied zijn beveiligde hardware-ontwerpstromen die onderzoeken hoe beveiligings- en privacy-functionaliteit geïntegreerd kan worden in de ontwerpmethodologie.

(III) Cryptografische algoritmen en protocollen

Cryptografie bestudeert wiskundige technieken om gegevens te beschermen tijdens communicatie, opslag en tijdens de verwerking ervan; het vormt de kern van de bescherming van digitale gegevens en processen.

Uitdagingen op het gebied van symmetrische cryptografie omvatten (1) het verbeteren van de wisselwerking tussen beveiliging, kosten en prestaties en in het bijzonder lange-termijn beveiliging, (2) cryptografische primitieven voor low-end processoren en knopen met strikte beperkingen op beschikbare energie en (3) nieuwe constructies die geschikt zijn voor white-box cryptografie, Multi-Party Computation (MPC) en post-kwantum digitale handtekeningen, dat wil zeggen, digitale handtekeningen die aanvallen op kwantumcomputers kunnen weerstaan.

Voor publieke sleutel cryptografie wordt er onderzoek gevoerd naar de ontwikkeling en evaluatie van post-kwantumprimitieven op basis van roosters, isogenieën en kwadratische systemen in meerdere veranderlijken (Multivariate Quadratic systems).

Een derde aspect is de ontwikkeling van efficiënte cryptografische software en hardware-bibliotheken met ingebouwde beveiliging tegen fysische aanvallen zoals aanvallen gebaseerd op nevenkanalen en op foutinjectie.

Voor elk van deze onderzoeksonderwerpen wordt er gesteund op wiskundig onderzoek naar harde problemen om de beveiliging op te baseren. Er worden beveiligingshulpmiddelen ontwikkeld voor de evaluatie van de veiligheid die zowel statistisch, logisch als algebraïsch kunnen zijn en die kunnen gecombineerd worden met formele verificatiemethoden.

(IIII) Veilige communicatie

Het veilig verbinden van twee of meer knopen is een essentieel bouwblok om een veilig ecosysteem op te bouwen. Hierbij wordt onderzoek gedaan naar cryptografische protocollen op de netwerklaag, datalinklaag en fysische laag om na te gaan welke knopen dichtbij liggen, om een veilige verbinding op te zetten met nieuwe knopen, om sessiesleutels overeen te komen en te updaten en om gecompromitteerde knopen te herroepen. Voor het eerste doel kunnen gesofisticeerde protocollen voor distance bounding gebruikt worden, die cryptografie vermengen met fysische eigenschappen. Voor al deze problemen vormt het beperken van de vertraging een belangrijke onderzoekuitdaging. Daarnaast is het essentieel dat het protocol robuust is, d.w.z. voorwaartse veiligheid biedt als een of meer knopen gecompromitteerd worden en dat het gebruikte algoritme op een veilige manier kan onderhandeld worden. Daarnaast is het ook zeer belangrijk om de veiligheid van implementaties te analyseren. Naast het voorstellen van nieuwe protocollen zal de veiligheid van belangrijke relevante standaardprotocollen zoals Bluetooth Low Energy (BLE), SSH en TLS bestudeerd worden. Een belangrijk aspect is het beschermen van de metadata op elk niveau van de communicatie. Hierbij wordt bestudeerd hoe metadata lekt op verschillende manieren en worden technieken ontwikkeld om metadata op een efficiënte en effectieve manier te beveiligen op alle relevante niveaus (vb. mix netwerken).

Toepassing van het basisonderzoek in strategische technologieplatformen

De vier onderzoekslijnen die hierboven werden samengevat leiden tot onderzoeksresultaten die toepasbaar zijn in diverse omgevingen. Het programma zal systematisch investeren in prototypes die aantonen in welke concrete, strategische technologieomgevingen de resultaten snel toegevoegde waarde kunnen leveren. Hierbij zal er ook regelmatig synergie gerealiseerd worden tussen bijdragen uit de verschillende lijnen.

Gegeven de huidige stand van zaken in het onderzoek, lijkt het relatief voor de hand liggend dat de nadruk zal liggen op (1) cloudomgevingen met mobiele en webgebaseerde cliënten, (2) IoTplatformen waarop complexe gedistribueerde toepassingen worden uitgerold, en (3) data-gedreven platformen waar gegevensbescherming en naleving van regelgeving cruciaal is. DIt laatste domein kent vandaag veel strategische trends, waaronder blockchain.

3.4. Luik 2: implementatie in het Vlaams bedrijfsleven

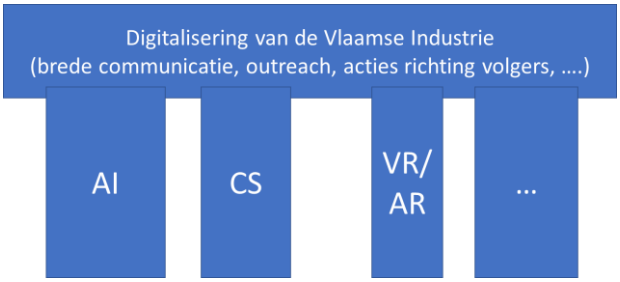
VLAIO zal fungeren als trekker van het luik implementatie. Hiertoe zal VLAIO zich intern organiseren zodat er voldoende afstemming en coördinatie ontstaat tussen de beleidsagenda's inzake AI, Cybersecurity, gepersonaliseerde geneeskunde, maar ook de bestaande werkingen inzake industrie 4.0, smart cities, de digitaliseringsagenda binnen de overheid via het programma innovatieve overheidsopdrachten, etc.

De doelstelling is om voor al deze beleidsagenda's te komen tot een heldere gecoördineerde inzet van het VLAIO-instrumentarium in overleg met de stakeholders (zie 'governance') gebaseerd op een heldere visie op de rol van elk instrument. Een eerste belangrijke opdracht zal zijn om KPI's te formuleren, niet enkel qua bereik, maar de bereik-KPI's in te zetten vanuit doelstellingen op langere termijn qua maturiteit van het bedrijfsleven inzake digitalisering en cybersecurity. VLAIO, in samenwerking met de stakeholders betrokken bij het programma, krijgt de opdracht dergelijke maturiteitsindex en bijhorende KPI's tot stand te laten komen, mogelijk door het uitschrijven van een opdracht hiervoor.

3.4.1. Basisvisie inzet instrumentarium

In voorliggende nota wordt het kader gegeven voor inzet van de binnen VLAIO beschikbare instrumenten op de doelstellingen van het actieplan, zodat de middelen naar de relevante begrotingsrubrieken binnen het Hermesfonds kunnen herschikt worden.

Een belangrijk principe is dat naast de verschillende voorliggende beleidsagenda's (AI, cybersecurity, gepersonaliseerde geneeskunde, virtual reality, smart cities, industrie 4.0, …) ook werkt gemaakt wordt van acties die generiek inzetten op de digitalisering van de Vlaamse economie. Onderstaand schema geeft dit weer.



De digitalisering van de Vlaamse economie wordt nu al gestimuleerd via verschillende acties, waaronder de activiteiten binnen de transitie naar Industrie 4.0 en de activiteiten van de speerpuntclusters. Om de doorzichtigheid voor ondernemers te garanderen en efficiëntie te bereiken, is het nodig dat de impulsprogramma's rond AI en CS in een globalere context worden geplaatst.

3.4.2. Generieke ondersteuning rond digitalisering van bedrijven

Eerst en vooral vertrekt de vraagstelling vanuit de bedrijven dikwijls vanuit een meer algemene problematiek rond digitale transformatie en de impact daarvan op de processen, de producten en het businessmodel. Het is aangewezen bedrijven vanuit de hele economie (maakindustrie, diensten, …) dan ook vanuit die generieke invalshoek te benaderen (welke invloed heeft digitalisering op mijn bedrijf, hoe kan ik mijn manier van werken aanpassen, hoe begin ik daaraan) en niet in verspreide slagorde met (deel)oplossingen. Dit geldt zeker als het gaat om bedrijven die op het vlak van digitalisering minder verder staan.

Anderzijds is de toepassing van CS enkel mogelijk als de onderneming een geschikte veiligheidsstructuur heeft en moet er een voldoende niveau van digitale geletterdheid bereikt zijn.

Op deze horizontale sokkel moeten de verschillende technologie-gedreven programma's uitgebouwd worden. Daarin wordt competentie opgebouwd binnen die specifieke domeinen en van daaruit kan gespecialiseerde ondersteuning geleverd worden.

Deze redenering volgend, wordt een horizontale eerstelijnsbenadering uitgebouwd waarbij gewerkt wordt aan de 'digital readiness' en de digitale geletterdheid van ondernemers en ondernemingen. Dat houdt in dat de stakeholders worden ingezet om te sensibiliseren, informeren en eerste ondersteuning geven voor een brede aanpak van de uitdagingen van digitalisering. De actielijnen daar zijn:

- een gedeeld plan dat het overzicht houdt over de verschillende programma's en acties en in het bijzonder de complementariteit en de buikbaarheid/toegankelijkheid voor de ondernemingen bewaakt;
- een gemeenschappelijke website waar de initiatieven rond digitalisering worden samen gebracht;
- generieke eerstelijnsdienstverlening om ondernemingen in hun aanpak van digitalisering te ondersteunen, vertrekkende vanuit hun (nieuw) businessmodel (assessments, maturiteitsbeoordelingen, algemene coaching,…);
- doorverwijsfunctie in een verder gespecialiseerd netwerk;
- binnen het bestaande horizontaal instrumentarium eventuele accenten leggen die toelaten de behandelde digitale thema's correct aan bod te laten komen, en die doortrekken naar alle projecten die bijdragen tot digital readiness en digitale geletterdheid;
- geïntegreerde aanpak voor specifieke platformen, waar oplossingen ontwikkeld worden voor gelijklopende noden voor een (deel)sector.

Verder moet bekeken worden in welke mate een gedeelde aanpak kan gevolgd worden in activiteiten naar het bredere publiek (outreach), STEM en opleidingsinitiatieven rond digital skills.

3.4.3. Vier basisacties inzake cybersecurity implementatie

Het implementatieluik van CyberSecurity voor Vlaanderen is erop gericht overheid en industrie maximaal te ondersteunen in de verbetering van kennis en vaardigheden op het vlak van

cybersecurity. Door samenwerking wordt er gezorgd voor een maximaal effect en zo groot mogelijk impact van de geleverde inspanningen.

Hierbij worden er vier belangrijke activiteiten ontwikkeld:

1. Kennisopbouw en deling m.b.t. markt, technologie en bruikbare ervaringen
2. Creatie van modellen en processen om maturiteit te beoordelen en te verbeteren aan de hand van *proven approaches,* en ondersteuning van bedrijven in de uitvoering van dergelijke *assessments* en verbeteringstrajecten
3. Collaboratief onderzoek met de nadruk op cybersecurity (groepen van bedrijven)
4. Innovatieprojecten in de cybersecuritysector, en in de beveiliging van producten en diensten in de digitale economie (individuele bedrijven)

Aan deze vier grote acties wordt dan het instrumentarium van VLAIO gekoppeld en kunnen kwalitatieve KPI's voorzien worden, die uiteindelijk uitgedrukt worden in bereik bij bedrijven.

3.4.4. Inzet van instrumentarium: van generiek naar specifiek

Naar inzet van instrumentarium vanuit VLAIO wil dat zeggen dat voor de verschillende voorliggende actieplannen telkens een deel middelen zal ingezet worden op meer algemene inspirerende, sensibiliserende, bewustmakende acties en bredere coaching en advies, in parallel met acties die meer domeinspecifiek zijn.

Een specifiek aandachtspunt is de toegankelijkheid voor de zorgsector binnen dit werkingsmodel. Na goedkeuring van de programma's zullen de personeelsleden van de vzw team bedrijfstrajecten gespecialiseerd in de zorg en/of CS een dialoog opstarten met de zorgsector om de toegang tot de acties voorzien in deze beleidsagenda's voor de zorgsector specifiek te faciliteren. De innovatiegerichte maatregelen van VLAIO, evenals de kennisdiffusiemaatregelen voorzien bij Hogescholen en ook het (nieuwe) contract ondernemerschap staan open voor actoren uit de zorgsector georganiseerd in vzw-vorm. Belangrijk aandachtspunt is de economische rationale achter het ingediende project en in een aantal gevallen het vrijmaken van de noodzakelijke co-financiering. Om de actoren uit de zorgsector maximaal te faciliteren gebruik te maken van de kennis die ontwikkeld zal worden binnen de beleidsagenda's zal de vzw team bedrijfstrajecten in samenspraak met het beleidsdomein Welzijn de verschillende acties die genomen worden communiceren met de sector. Er zal onderzocht worden of er drempels zijn voor VZW's om te participeren in het COOCK programma, desgevallend zal het HBC bekijken hoe deze weggewerkt kunnen worden.

Onderstaand schema geeft dit weer:

1.	2.	3.	4.	5.
INSPIREREN, SENSIBILISEREN, BEWUSTMAKING	COACHING, ADVIES, BEGELEIDING	INDIVIDUELE EN COLLECTIEVE STEUNVERLENING VOOR KENNISDIFFUSIE	INDIVIDUELE EN COLLECTIEVE STEUNVERLENING VOOR KENNISOPBOUW	STEUN VOOR IMPLEMENTATIE OP BEDRIJFSNIVEAU

De filosofie van de inzet van het instrumentarium vanuit VLAIO is dan een trechtermodel, waarbij breed gesensibiliseerd wordt met de bedoeling om individuele ondernemingen aan te zetten om actie te ondernemen. De actie kan afhankelijk van de onderneming het opstarten van een implementatietraject zijn, tot het opstarten van onderzoek.

De inzetbare instrumenten en besluiten voor steuntoekenning binnen dit trechtermodel worden hieronder beknopt beschreven. De doelstelling is om het instrumentarium flexibel in te zetten doorheen de tijd. Gezien de middelen recurrent worden toegewezen, wil dat zeggen dat de omvang van de inzet van instrumenten doorheen de tijd kan wijzigen volgens de noden van het programma. Op basis van onderstaande redenering wordt een eerste voorstel voor herverdeling van kredieten naar de strategische prioriteiten binnen hermes gedaan. Door de jaren heen kan deze eerste toewijzing via krediethertschikkingen nog wijzigen.

1. *Inspireren, sensibiliseren, bewustmaken*
   - Contract ondernemerschap. Opname van het breed naar de bevolking en ondernemingen toe inspireren, sensibiliseren, bewustmaken in de vernieuwing van het contract ondernemerschap. Aan de dienstverleners binnen het lopende contract ondernemerschap zal VLAIO de opdracht geven binnen de mogelijkheden van het lopende contract, zonder budgetverhoging, activiteiten te plannen in het najaar 2019 en voorjaar 2020. Voor deze acties zullen de dienstverleners moeten samenwerken met neutrale organisaties (zoals hogescholen en andere kennisinstellingen) die over de nodige knowhow beschikken. VLAIO zal de van de dienstverleners ontvangen programma's meedelen tijdens de voortgangsrapportage.
     - Startevent
     - Roadshows
     - Events, inclusief actieve matchmaking bedrijven/organisaties/instrumenten
     - Doorwerking naar bestaande events met andere finaliteit (Open Bedrijvendag, dag van de klant, womed award, …)
   - STEM-acties (ook naar onderwijs)/STEM-academies…

2. *Individuele en collectieve steunverlening voor kennisdiffusie*
   - Voorzien van een brede laagdrempelige, sensibiliserende begeleiding via COOCK, TETRA, SPC, IBN,….
     - vb. hub/kenniscentrum als opstap, later verankering via kmo-portefeuille
     - een scan, eerste laagdrempelig advies wat cybersecurity als impact zou kunnen hebben op de bedrijfsvoering of hoe het business model in de toekomst zou kunnen geaffecteerd worden door toenemende aandacht voor cyberveiligheid in de samenleving

    - middelen innovatieversneller: via begeleidingstrajecten in groepsverband bedrijven aanzetten tot de implementatie van reeds bewezen innovaties/technologieën
- Versterking van de capaciteit van team bedrijfstrajecten en de clusters om doorwerking in specifieke domeinen en sectoren te verzekeren
- Opzetten van een netwerk om internationale trends inzake cybersecurity implementaties te identificeren in de verschillende sectoren van de Vlaamse industrie (Chemie, voeding, Bouw, …): samenwerking met partners met internationaal netwerk om kennis te detecteren (via oproep)
- Sensibilisering en disseminatie van (internationale) kennis en best practices naar het Vlaamse bedrijfsleven (via Vlaio partner netwerk): samenwerking met speerpuntclusters, sectorfederaties, werkgeversorganisaties, … *Individuele en collectieve steunverlening voor kennisdiffusie*

- Kmo-portefeuille en kmo-groeisubsidie om diepgaandere screening en invoeren CS in bedrijfsvoering te stimuleren. Mogelijke ondersteunende acties hierbij kunnen zijn: met consultants gespecialiseerd in VS een groepswerking opzetten en opleidingen voorzien ter begeleiding van hun kwaliteit van dienstverlening
- NCP-werking als toeleiding naar Europese middelen en informatieverschaffing over de Europese kanalen en beleidslijnen
- COOCK: collectieve kennisopbouw- en kennisdiffusie met individuele implementatietrajecten
- TETRA
- EFRO of proeftuinen: voorzien van demo-installaties e.d., aanvullend op wat al bestaat

3. *Individuele en collectieve steunverlening voor kennisopbouw*
    - ICON-call om resultaten van het onderzoeksluik naar het bedrijfsleven door te vertalen. De ICON-projecten zijn een belangrijk instrument voor de vertaling van onderzoek naar oplossingen voor bedrijven. We kiezen er voor om de oproepen voor de verschillende impulsprogramma's (AI, CS, PM) binnen afzonderlijke enveloppes uit te voeren, maar wel gelijktijdig, mogelijk pas vanaf jaar 2 om praktische redenen, zodat projecten op de raakvlakken best kunnen gepositioneerd worden en in tweede orde eventuele overschotten en tekorten kunnen weggewerkt worden. Dit vereist een centrale selectieprocedure voor deze projecten, die door VLAIO wordt uitgevoerd.
    - Baekeland en innovatiemandaten, zodat onderzoek effectief in de bedrijven zelf uitgevoerd wordt
    - Ontwikkelings- en onderzoeksprojecten op bedrijfsniveau

4. *Steun voor implementatie op bedrijfsniveau*
    - Kmo-groeisubsidie
    - Strategische transformatiesteun (investeringen en opleidingen)
    - Ontwikkelingsprojecten

3.4.5. Aanzet van KPI's vanuit de stakeholders

Onderstaand voorstel van KPI's werd opgemaakt door de betrokken stakeholders. Bij de verdere verfijning van inzet van instrumenten kunnen deze KPI's nog wijzigen. Ze worden ter illustratie mee opgenomen, maar zijn niet definitief, wel onderbouwd. Na de herverdeling van middelen die in deze nota voorgesteld wordt, zal de inzet van specifieke instrumenten verder uitgeklaard worden en zal onderstaande tabel verder vorm krijgen.

Prioriteit Hermesfonds	Voorstel actieplan	Mogelijk instrument VLAIO	Budget					Aantallen projecten				
			'19	'20	'21	'22	'23	'19	'20	'21	'22	'23
Ondernemerschap	doelgroepspecifieke coaching en begeleiding	TBD	2000	2000	2000	2000	2000	6	6	4	4	4
Innovatiesteun		COOCK, TETRA, SPC, IBN, ...	7000	7000	7000	7000	7000	10	15	20	20	20
		Baekeland	-	250 (P.M.)	250 (P.M.)	250 (P.M.)	500 (P.M.)	-	1	1	1	2
		Industriële onderzoeksprojecten	1000 (P.M.)	1.250 (P.M.)	1.500 (P.M.)	1.750 (P.M.)	1.750 (P.M.)	2	5	6	7	7
		Industriële ontwikkelingsprojecten	1125 (P.M.)	375 (P.M.)	625 (P.M.)	750 (P.M.)	750 (P.M.)	1	3	5	6	6
		Icon	-	4.500	4.500	4.500	4.500	-	3	3	3	3
TBD	**Portal, review icon, governance stakeholders, ...**											

Een belangrijk werkpunt is de brede vraagactiverende werking naar het bedrijfsleven toe via '*communities*', zoals bijvoorbeeld in de gezondheidszorg. In samenspraak met de stuurgroep en in dialoog met het Hermes beslissingscomité zal VLAIO deze vraagactiverende werking vorm geven door inzet van een mix van bestaande instrumenten. Via het reguliere instrumentarium (COOCK, Tetra, activeren van het potentieel van de bestaande speerpuntclusters en mogelijk IBN's, …) zullen projecten met CS-finaliteit ondersteund worden, waardoor via bestaande en nieuwe communities een extra impuls kan gegeven worden aan het experimenteren en ook daadwerkelijk implementeren van CS binnen een bepaald domein of groep van bedrijven. Door gerichte inzet van het contract ondernemerschap in het kader van (1) acties in het kader van digital readiness – perceel 2 en (2) lerende netwerken gericht op het versnellen van de implementatie van innovaties – perceel 4 zullen eveneens voor *communities* een begeleidingsmogelijkheid ontstaan in het verlengde van het bredere innovatiegerichte instrumentarium van VLAIO (zie bovenstaand trechtermodel). Slechts indien na hanteren van bovenstaand model blijkt dat er vanuit de beleidsagenda's nog niet ingevulde noden zijn, zal een afzonderlijke oproep inzake community-werking rond CS overwogen worden.

Naast de bovenvermelde aspecten zullen in beperkte mate middelen uitgetrokken worden om het programmamanagement te vergoeden, een portaalwebsite uit te bouwen, een aanbesteding te doen ter ondersteuning van de review van de icon's, etc..

Conclusie: op basis van de huidige uitwerking van het programma zal de herverdeling van middelen gebeuren vanuit de provisie naar de begrotingsrubrieken van waaruit de verschillende acties opgestart kunnen worden. De instrumentspecifieke inzet binnen het programma kan dan verder uitgewerkt worden naar het niveau van concrete calls met verder te verfijnen KPI's. Voor elk in te zetten instrument zal de geëigende beslissingsprocedure gevolgd worden. Dat wil zeggen dat nog verdere beslissingen volgen van de Vlaamse Regering, de bevoegde minister(s) en het Hermes Beslissingscomité of Comité van Toezicht bij EFRO. De globale hierboven beschreven aanpak zal daarbij gehanteerd worden.

Om een globaal overzicht mogelijk te maken zal jaarlijks de globale uitvoering van het actieplan, luik implementatie, gerapporteerd worden aan het Hermes Beslissingscomité met de vraag om er een advies bij te formuleren.

3.5. Luik 3: flankerend beleid: sensibilisering, opleidingsaanbod, security & privacy by design

De hoofddoelstelling van het implementatiebeleid en het flankerend beleid is het vergroten van de brede bewustwording bij het Vlaamse bedrijfsleven inzake de verschillende vormen van cybercriminaliteit en hoe deze te herkennen en te voorkomen. Waar veel media aandacht gaat naar de denial-of-service (DNS) en randsome-ware gebaseerde cybercriminaliteit (het blokkeren van bedrijfskritische accounts zoals mail of ERP systemen die vervolgens vrijgegeven worden tegen betaling) of phishing, is data integriteit en economische spionage een sterk toenemende bedreiging inzake cybersecurity. Voor Vlaanderen als kenniseconomie is het afschermen van bedrijfskritische data zoals onderzoeksresultaten of gebruikersdata van levensbelang. Door een gebrek aan kennis inzake integriteitstesten voor systemen kan een data lek vaak reeds lang gebeurd zijn voordat het bedrijf het ontdekt of worden veel gegevensdiefstallen simpelweg nooit ontdekt. Het bewerkstelligen van een shift in mindset naar "security & privacy by design" waarbij bedrijven in het organiseren van hun bedrijfsvoering het minimaliseren van cybersecurity risico's als uitgangspunt meenemen eerder dan iets wat achteraf wordt toegevoegd als "nice to have" is hierbij een essentiële stap. Veilige (digitale) producten zijn een essentiële differentiator op de

globale markt en Vlaanderen wil hierin met dit programma de lead nemen door Vlaamse producten als cybersecure te kunnen positioneren.

Het uitbouwen van een laagdrempelig opleidingsaanbod en bijhorende sensibiliseringscampagne moeten zorgen voor het verhogen van de bewustwording inzake de verschillende security uitdagingen waar elk Vlaams bedrijf, van KMO tot multinational, incl. de zorgsector, in de hypergeconnecteerde economie voor staat. Ook het verhogen van het bewustzijn inzake data privacy en cybersecurity in de privé context bij de brede bevolking is hier één van de hoofddoelstellingen. Hierbij zal ook een gepast aanbod uitgewerkt worden naar het secundair onderwijs in afstemming met het Beleidsdomein Onderwijs en Vorming.

Om in te spelen op de noden van de industrie & en de brede bevolking wordt door Vlaio en EWI en het beleidsdomein Onderwijs en Vorming in samenwerking met de VDAB, syntra, de hoger onderwijsinstellingen (hogescholen en universiteiten) en andere betrokken stakeholders een overzicht gemaakt van het huidige aanbod aan cybersecurity opleidingen in Vlaanderen. Welke gebreken zijn er in het aanbod, zowel qua duurtijd, qua niveau als qua vormingsdoel (theoretisch versus toegepast) en hoe kunnen deze op een efficiënte manier ingevuld worden en kan bovendien ook het bestaande aanbod gerichter bekendgemaakt worden.

4. WEERSLAG VAN HET VOORSTEL OP DE BEGROTING VAN DE VLAAMSE GEMEENSCHAP

De beslissing behelst de herverdeling van de middelen voorzien op begrotingsartikel 1EBG2AH-PR, basisallocatie 1EE104 0100 (provisie). Hier werd naar aanleiding van de begrotingsopmaak 60 miljoen euro voorzien voor de actieplannen Artificiële Intelligentie, Cybersecurity en gepersonaliseerde geneeskunde.

20 miljoen euro hiervan zijn voorzien voor het voorliggende actieplan Cybersecurity. Deze middelen omvatten zowel de delen onderzoek, implementatie als opleiding. Om de verdere vormgeving van het actieplan mogelijk te maken en om de uitvoering van het actieplan aan te vatten is een herverdeling van de middelen nodig naar de relevante begrotingsrubrieken.

Het bijgevoegde besluit van de Vlaamse Regering organiseert de herverdeling naar het Hermesfonds, hieronder wordt meer detail gegeven.

Volgende verdeling van middelen wordt voorgesteld:

1. Top CS-onderzoek:
    a. 8.000.000 euro te voorzien op begrotingsrubrieken onder het beheer van het departement EWI
2. Indicatieve verdeling implementatie: 9.000.000 euro te voorzien op begrotingsrubrieken binnen het Hermesfonds. Meer bepaald wordt volgende subverdeling voorgesteld, rekening houdende met die onderdelen van het programma waar de regulier beschikbare middelen, na o.a. de opstap die Innovatie in 2019 geniet, onvoldoende zijn
    a. Strategische doelstelling ondernemerschap (via contract)
        i. Doelgroepspecifieke coaching en begeleiding,…: 2.000.000 euro
    b. Strategische doelstelling Kennisdiffusie en Innovatiesteun

i. Rubriek O&O&I beleidsagenda CS: Versterking projectgenese van specifieke communities of snellere opstart icon's, inclusief versterking vzw bedrijfstrajecten met 1 VTE: : 7.000.000 euro

ii. Versterking ontwikkelingsprojecten en onderzoeksprojecten CS

iii. Versterking icon: p.m. pas vanaf jaar 2

iv. Proeftuinen: p.m. pas vanaf jaar 2

3. flankerend beleid gericht op bewustmaking, opleiding en ethische omkadering:

    a. 1.500.000 euro te voorzien op begrotingsrubrieken onder het beheer van het departement EWI ter versterking van de opleidingsmodules ingericht door hoge scholen en universiteiten met bijzondere aandacht voor permanente vorming

    b. 1.500.000 euro te voorzien op begrotingsrubrieken onder het beheer van VLAIO, contract ondernemerschap, ter versterking van de bredere sensibilisering, coaching en opleiding van bedrijven en onderwijs inzake omgaan met thema's gerelateerd aan Cybersecurity en gepaste opleidingen voor ondernemers en hun kernpersoneel. Voor wat betreft onderwijs kunnen de hier voorziene middelen (ca. 666.000 euro) gepoold worden met deze voor AI)

Dat geeft onderstaande tabel tot herverdeling. Deze middelen worden voortaan recurrent op deze wijze voorzien op de begroting voorzien. Ze staan binnen het Hermesfonds uiteraard open voor kredietherschikking conform de reguliere werkwijze binnen het Hermesfonds. met uitzondering van de als O&O&I-gelabelde middelen onder rubriek 2.c.. Deze kunnen niet herverdeeld worden naar rubrieken binnen het Hermesfonds die niet onder de O&O&I-doelstelling vallen. VLAIO zal jaarlijks binnen de governancestructuren van het CS-plan afspraken maken en rapporteren over de aanwending van de middelen. Eveneens zal deze rapportage jaarlijks voor advies voorgelegd worden aan het Hermes Beslissingscomité.

Het bestek van alle onderdelen in voorliggend programma die via de overheidsopdracht mbt. het contract ondernemerschap uitgevoerd worden zal ter informatie voorgelegd worden.

Bij de begrotingsopmaak zal telkens gekeken worden hoe de middelen moeten gealloceerd worden. Zo staat het bijvoorbeeld al vast dat de middelen gericht op ondernemerschap over de jaren zullen afnemen ten voordele van de middelen innovatiesteun en met name icon-oproepen.

Uit de reguliere middelen zal geput worden voor onderzoeks- en ontwikkelingsprojecten, collectieve projecten, Baekelandmandaten, etc.

(in duizend EUR)

begrotingsartikel	basisallocatie	Krediet-soort	van		naar	
			VAK	VEK	VAK	VEK
EB0-1EBG2AH-PR	EB0 1EE104	VAK/VEK	20.000	9.500		
ECH-1ECG5CA-WT	ECH 1EC361	VAK			2100	
ECH1EFG5NA-WT	ECH 1EF3BV	VAK			8400	
EB0-1EEG2JA-WT	EB0 1EC102	VAK/VEK			9.500	9.500
Totaal			20.000	9.500	20.000	9.500

Het gunstig advies van de Inspectie van Financiën werd verleend op …

Het begrotingsakkoord werd verleend op …

5. WEERSLAG VAN HET VOORSTEL OP DE LOKALE BESTUREN

1 personeel: het voorstel heeft geen weerslag op gebied van personeelsinzet door de lokale besturen.

2. werkingsuitgaven: het voorstel heeft geen weerslag op de lopende uitgaven van de lokale besturen;

3 investeringen en schulden: het voorstel heeft geen investeringen als gevolg;

4 ontvangsten: het voorstel resulteert niet in bijkomende financiële middelen voor de lokale besturen;

5 conclusie: het voorstel heeft geen weerslag op de lokale besturen.

6. WEERSLAG VAN HET VOORSTEL OP HET PERSONEELSBESTAND EN DE PERSONEELSBUDGETTEN

Het voorstel heeft geen weerslag op het personeelsbestand en op het personeelsbudget, zodat het akkoord van de Vlaamse minister, bevoegd voor het algemeen beleid inzake personeel en organisatieontwikkeling, niet vereist is.

7. KWALITEIT VAN DE REGELGEVING

NVT

8. VOORSTEL VAN BESLISSING

De Vlaamse Regering beslist:

1° haar goedkeuring te hechten aan het Vlaams Beleidsplan Cybersecurity zoals beschreven in deze nota;

2° haar goedkeuring te hechten aan het ontwerpbesluit van de Vlaamse Regering houdende de herverdeling van begrotingsartikelen van de algemene uitgavenbegroting van de Vlaamse Gemeenschap voor het begrotingsjaar 2019 in het kader van het Vlaams beleidsplan Cybersecurity ;

3° De minister bevoegd voor het economisch beleid en de technologische innovatie te gelasten de uitvoering van het actieplan aan te vatten. De minister bevoegd voor het economisch beleid en de technologische innovatie zal een voortgangsrapportage aan de Vlaamse Regering meedelen uiterlijk 1 januari 2020, na advies over de voortgang door het Hermes Beslissingscomité

4° De minister bevoegd voor het economisch beleid en de technologische innovatie te gelasten een voorstel van samenstelling van stuurgroep voor te leggen aan de Vlaamse Regering

5° de minister bevoegd voor het economisch beleid en de technologische innovatie te gelasten de voorziene werking richting het onderwijs uit te werken in overleg met de minister bevoegd voor het onderwijs;

De Vlaamse minister van Werk, Economie, Innovatie en Sport
Philippe MUYTERS

Bijlagen:

- ontwerpbesluit van de Vlaamse Regering houdende de herverdeling van begrotingsartikelen van de algemene uitgavenbegroting van de Vlaamse Gemeenschap voor het begrotingsjaar 2019 in het kader van het Vlaams beleidsplan Cybersecurity;
- het Advies Inspectie van Financiën dd. 19/02/2019;
- het begrotingsakkoord dd. 04/03/2019.