Vlaamse Regering

DE MINISTER-PRESIDENT VAN DE VLAAMSE REGERING EN VLAAMS MINISTER VAN BUITENLANDSE ZAKEN, CULTUUR, DIGITALISERING EN FACILITAIR MANAGEMENT

NOTA AAN DE VLAAMSE REGERING

Betreft: relanceproject VV065: "Cybersecurity en uitrol SIEM"

Met deze nota wordt aan de Vlaamse regering goedkeuring gevraagd voor de invulling van het relanceproject 'Cybersecurity en uitrol SIEM' (VV065) en bijhorende middelen.

1. SITUERING

A. BELEIDSVELD/BELEIDSDOELSTELLING

Beleidsveld digitalisering

B. VORIGE BESLISSINGEN EN ADVIEZEN

Deze nota geeft invulling aan het project 'cybersecurity en uitrol SIEM' (VV065) zoals bepaald in het relanceplan 'Vlaamse Veerkracht' als beslissing van de Vlaamse regering van 26 september 2020.

2. INHOUD

A. CONTEXT VAN HET PROJECT

Met het relanceplan "Vlaamse Veerkracht" wil de Vlaamse regering Vlaanderen digitaal transformeren. Eén van de drie horizontale basispijlers van deze digitale transformatie ambitie richt zich op de overheidsdienstverlening waarbij ook versneld wordt geïnvesteerd in de achterliggende systemen en processen, als cruciale bouwsteen, om de gemeenschappelijke dienstverlening te faciliteren.

De websites, internettoepassingen en interne werkplek van de Vlaamse overheid krijgen steeds meer af te rekenen met misbruik en niet-geautoriseerde toegang tot informatie en informatie verwerkende systemen. Om de klant steeds meer centraal te zetten en een uiterst klantvriendelijke dienstverlening te realiseren die op elk ogenblik en vanop elke plek toegankelijk is, moet Digitaal Vlaanderen deze achterliggende systemen en processen beschermen, rekening houdend met de evoluerende bedreigingen en technologische vernieuwingen. Het is daarom noodzakelijk een aantal cruciale initiatieven en verbeteringen door te voeren op vlak van informatieveiligheid.

Dit specifieke relanceproject is een belangrijk onderdeel van het strategisch plan Stuurorgaan Vlaams informatie -en ICT-beleid. Het voorziet o.m. in verschillende bijkomende gerichte flankerende initiatieven en investeringen op vlak van informatieveiligheid om de digitale transformatie veilig en in lijn met de GDPR & privacy regelgeving te versnellen. Dit relanceproject is dan ook van essentieel

belang om de digitaliseringsdoelstellingen van de Vlaamse overheid te verwezenlijken. De voorziene acties vormen een directe katalysator voor andere digitale transformatieprojecten in het relanceplan.

B. PROJECTDOELSTELLINGEN

De Vlaamse overheid wil in de eerste plaats het vertrouwen genieten van de burger, onderneming en/of vereniging, de persoonlijke levenssfeer van de burger beschermen en de reputatie hooghouden van de Vlaamse overheid als betrouwbare partner.

Een aantal doelstellingen van dit initiatief zijn daarnaast van bijzonder belang voor het succes van de verdere relanceplannen van de Vlaamse overheid:

- **Snelle time-to-market:** De context waarbinnen de overheid opereert vereist snelheid en wendbaarheid. Digitaal Vlaanderen ondersteunt dit door het aanbieden van een uniform informatieveiligheidsbeleid met kant-en-klare mitigerende maatregelen en ondersteunende tools. Industrialisatie van gestandaardiseerde veiligheidscomponenten zorgen voor ontzorging en faciliteren volume en snelheid voor de individuele entiteiten. Het laat hen toe zich te focussen op eigen kerntaken en specialisaties.

- **Flexibiliteit:** IT-afdelingen willen applicaties bouwen die beter en sneller kunnen inspelen op de vragen vanuit de business, op veranderingen in de bedrijfscontext of in het beleid. Het informatieveiligheidsbeleid biedt hieraan ondersteuning door de veiligheidsmaatregelen af te stemmen op het kritieke en privacygevoelige karakter van de onderhavige informatiesystemen.

- **Beveiliging:** De Vlaamse overheid dient te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). We ambiëren een zeer hoge beveiligingsgraad met focus op operationele opvolging en onafhankelijk toezicht, die aangetoond wordt door onafhankelijke audits.

- **Verzekeren van bedrijfscontinuïteit:** door het voeren van een adequaat informatieveiligheidsbeleid worden bedreigingen snel geïdentificeerd en laat de Vlaamse overheid toe snel in te grijpen en ernstige incidenten af te wenden en eventuele gevolgen in te perken. Dit draagt aanzienlijk bij aan de robuustheid van de informatiesystemen, wat op haar beurt de bedrijfscontinuïteit en het vertrouwen in onze overheid positief beïnvloedt.

Om de doelstelling van de Vlaamse regering inzake digitalisering te versnellen is het van cruciaal belang dat een veilige digitale dienstverlening kan gerealiseerd worden met een zo klein mogelijke impact op de werking en budgetten. Digitaal Vlaanderen kan dit project centraal aansturen om de coherentie en de snelheid van uitvoering te verhogen om de Vlaamse overheid maximaal te digitaliseren. Op die manier laten we hen toe zo snel mogelijk de ambities te realiseren inzake relance ten behoeve van burgers, bedrijven en organisaties.

C. RESULTATEN

Dit project focust op volgende resultaatgebieden:

1. VO-brede aanpak van informatieveiligheid

De VO-brede strategie voor informatieveiligheid zal een duidelijk kader, governance en verantwoordelijkheden vastleggen voor een gedragen aanpak voor informatieveiligheid.

De bekrachtiging door de Vlaamse Regering van het informatieveiligheidsbeleid van de Vlaamse Overheid zal worden voorgelegd in een aparte nota 'Strategie voor informatieveiligheid' en zal, overeenkomstig art. 3 laatste lid van het decreet van 26 december 2016 houdende de oprichting van het stuurorgaan Vlaams Informatie- en ICT-beleid, voorstellen het mandaat te geven aan het Stuurorgaan, om samen met de werkgroep Informatieveiligheid en het agentschap Digitaal Vlaanderen dit informatieveiligheidsbeleid concreet vorm te geven en op te volgen.

Binnen deze strategie wordt het reeds bestaande raamwerk voor informatieclassificatie gebruikt als beleidskader binnen de Vlaamse overheid rond het beheersen van risico's op het vlak van informatieveiligheid, met inbegrip van bescherming van persoonsgegevens. Binnen dit project voorzien we een verdere uitwerking en communicatie van dit raamwerk.

Daarnaast willen we betere en geïnformeerde beslissingen door een duidelijk begrip van de risicoblootstelling van de Vlaamse overheid op het vlak van informatieveiligheid en veiligheid van persoonsgegevens. Entiteiten kunnen door self-assessment of een conformiteitstoetsing hun maturiteit meten. Op het niveau van het stuurorgaan wordt een centraal dashboard uitgewerkt dat inzicht geeft in de overkoepelende veiligheidsrisico's

Op basis van een periodieke rapportering van hoge kwaliteit moet het voor beslissingsnemers en beleidvoerders mogelijk zijn om de juiste beleid- en investeringsbeslissingen te nemen. Een duidelijk kader en zicht op de risico's leiden tot een consistente aanpak die onnodige complexiteit en tegenstrijdige adviezen vermijdt binnen dezelfde overheid. Deze aanpak zal de beheersbaarheid én de betaalbaarheid van het informatieveiligheidsbeleid verhogen.

Het relanceproject Cyber security en uitrol SIEM (VV065) beoogt volgende resultaten op te leveren:

Nr.	Omschrijving	Voorziene datum
VV065.01.01	Opbouw standaardrapportering en centraal dashboard voor veiligheidsrisico's	31/12/2021
VV065.01.02	Verdere uitbouw van informatieclassificatie-raamwerk	31/12/2022
VV.065.01.03	Ontwikkeling instrument voor self-assessment	31/05/2022
VV.065.01.04	Ontwikkeling proces en tooling voor conformiteitstoetsing	31/05/2022

2. Verhogen van digitale competenties

Een gebrek aan kennis en expertise met betrekking tot informatieveiligheid leidt tot een situatie waar we niet in staat zijn in te schatten wat de risico's van onze informatieverwerking zijn en ons niet adequaat kunnen beschermen. Op die manier is het onmogelijk onze beoogde doelstellingen te halen. Dit resultaat mitigeert deze risico's en zorgt ervoor dat niet iedere entiteit afzonderlijk deze kennis individueel moet verwerven door volgende acties:

- Minder blootstelling aan risico's met betrekking tot informatieveiligheid door opleiden en bewustmaken van de werknemers van de Vlaamse overheid en de lokale besturen. Dit gebeurt concreet aan de hand van een reeks opleidingen binnen de Vlaamse overheid en lokalen besturen met betrekking tot informatieveiligheid. Daarnaast zal er een phishing test campagne worden georganiseerd om de personeelsleden bewust te maken van de gevaren van valse e-mails en het bewustzijn rond informatieveiligheid duurzaam te versterken.

- Interne competentie -en kennisopbouw verhogen door het uitbouwen van de dienstverlening binnen Digitaal Vlaanderen waarbij een pool aan specialisten met brede inzetbaarheid aan

klanten kan worden aangeboden, specifiek voor Data Protection Officers en veiligheidscoördinatoren.

Het relanceproject Cyber security en uitrol SIEM (VV065) beoogt volgende resultaten op te leveren:

Nr.	Omschrijving	Voorziene datum
VV065.02.01	Communicatie -en bewustmaking campagne met betrekking tot informatieveiligheid	31/12/2021

3. Weerbare digitale processen en robuuste infrastructuur uitbouwen

Dit resultaat heeft als doelstelling om het veiligheidsniveau van de informatieverwerking op operationeel niveau te verhogen door de juiste processen en veiligheidsbouwstenen te voorzien.

Elke entiteit staat binnen de eigen organisatie in voor het correct implementeren van maatregelen en controles zoals gedefinieerd in de Vo informatieclassificatie van de Vlaamse overheid. Het is echter logischer en efficiënter om een aantal diensten op een Vo-breed basisaanbod te baseren. Dit zijn onder meer het overkoepelend monitoren en opvolgen van informatieveiligheidsincidenten (operationeel) en het optimaal inrichten van dienstverlening en bouwstenen met betrekking tot informatieveiligheid (organisatorisch en technologisch).

Dit kadert binnen de regierol die Digitaal Vlaanderen binnen het kader van de nieuwe raamcontracten zal opnemen op een aantal cruciale ICT-domeinen (o.a. informatieveiligheid) op het vlak van gemeenschappelijke dienstverlening. We willen hiermee volgende doelen bereiken:

- Verhogen van de maturiteit van onze veiligheidsorganisatie door ondersteuning met betrekking tot veiligheidsdienstverlening & tools
- Geïntegreerde dienstverlening met betrekking tot het beheersen van risico's van onze gemeenschappelijke ICT-systemen
- Verhogen van het operationele veiligheidsniveau door Vo veiligheidsbouwstenen verder uit te bouwen
- Tijdige detectie van informatieveiligheidsincidenten
- Versterkte slagkracht met betrekking tot ernstige informatieveiligheidsincidenten

Volgende concrete investeringen zullen aanleiding geven tot een verbetering van de weerbaarheid van onze ICT-dienstverlening en de robuustheid van de onderliggende infrastructuur:

3.1 De verdere uitbouw van het centraal systeem van veiligheidsbouwstenen en het beheer van veiligheidsevenementen en –informatie (SIEM)

Als informatieveiligheidsincidenten niet tijdig worden gedetecteerd en zich over de hele overheid verspreiden, kan dit een belangrijke impact hebben op onze bedrijfscontinuïteit en het vertrouwen in onze dienstverlening van zowel burgers, bedrijven en overheden op de verschillende beleidsniveaus. Een reactie in verspreide slagorde kan belangrijke imago-schade opleveren in de pers als we niet helder communiceren en gecoördineerd optreden.

Informatieveiligheidsincidenten en afwijkend gedrag binnen onze ICT-infrastructuur moeten tijdig worden gedetecteerd, verzameld, gecorreleerd en geanalyseerd. Deze activiteiten moeten berusten op een hoog beschikbaar 'Security Operations Center' (SOC) dat de klok rond de diensten kan garanderen, zodat de Vlaamse entiteiten minder veiligheidspersoneel moeten aanwerven, continu opleiden en hun interne aanwezigheid moet garanderen om zich te beschermen tegen cybercriminaliteit.

Deze SOC biedt gecentraliseerde dienstverlening voor het beheer en opvolging van bedreigingen, kwetsbaarheden en veiligheidsincidenten, waaronder monitoring, opsporing, waarschuwing, respons en rapportering. De dienstverlening bestaat uit diensten voor het beheer van de beveiligingsbouwstenen, toezicht op de waarneembare activiteit, analyse van de gecollecteerde data en eerste interventie bij incidenten. Deze dienstverlening omvat de uitbating van een centraal systeem voor het beheer van veiligheidsevenementen en -informatie (SIEM).

a. Uitbreiden van centraal systeem met kritieke infrastructuur -en applicatiecomponenten

Actueel verzamelt systeem voor het beheer van veiligheidsevenementen en -informatie (SIEM) hoofdzakelijk data afkomstig van kritieke netwerkcomponenten. Door eveneens bedrijfstoepassingen te monitoren, verhoogt de effectiviteit van de bescherming fundamenteel: er is een beter en overkoepelend inzicht in bedreigingen, kwetsbaarheden en veiligheidsincidenten waardoor hieraan een snellere en accurater antwoord kan worden geboden. Deze uitbreiding vormt de kern van dit projectonderdeel.

b. Uitbreiden van het centraal systeem voor het beheer van veiligheidsevenementen en –informatie (SIEM) met log analytics en artificiële intelligentie.

Aanvallen op digitale systemen en bedrijfstoepassingen worden steeds gesofisticeerder en moeilijker te identificeren. Krachtige tools om de logs van de verschillende systemen en bedrijfstoepassingen te analyseren zijn onontbeerlijk om bepaalde patronen en correlaties naar boven te brengen. Via artificiële intelligentie wordt het opsporen van anomalieën geautomatiseerd en geoptimaliseerd via de “self learning” capaciteiten vervat in het systeem.

Het centrale SIEM wordt uitgebreid met de mogelijkheden van log analytics functionaliteiten. Verder wordt gefocust op het activeren, trainen en optimaliseren van de motor voor artificiële intelligentie.

3.2 We versterken het centrale aanbod veiligheidsbouwstenen

We verhogen de maturiteit van de entiteiten van de Vlaamse Overheid en betrokken partners inzake informatieveiligheid door maximaal in te zetten op het hergebruik van een centraal aanbod veiligheidsbouwstenen. We maken maximaal hergebruik van de veiligheidsbouwstenen door deze te koppelen aan het plan van aanpak op maat van de klant (via self-assessment/maturiteitsmeting). Door deze aanpak mitigeren we de risico’s en kwetsbaarheden pro-actiever en zorgen we ervoor dat het aanbod afgestemd is op de noden van elke klant.

We voorzien functionele uitbreidingen op verschillende bouwstenen. Het gaat over volgende componenten:

- Een adequaat systeem om de auditlogs die systemen genereren (bv. rond toegang tot persoonsgegevens) te archiveren en te bewaren. Deze nood stelt zich bij alle systemen van de Vlaamse overheid (Log management). Voorziene uitbreidingen zijn het automatisch retentiebeheer en doorzoekbaarheid voorzien ikv audit-vereisten en wetgeving, vereisten ikv legal logging verder uitbouwen, integratie met SIEM en monitoringtools, verdere integratie voorzien met toegangs- en gebruikersbeheer van Digitaal Vlaanderen. Daarnaast verbeteren en standaardiseren we het onboardingproces voor afnemende klanten.

- Het beheer van encryptie en bijhorende sleutel om de vertrouwelijkheid van gegevens (onder meer in cloud-omgevingen) te garanderen (encryptiebouwstenen). Voorziene uitbreidingen zijn het bijkomend ondersteunen van sleutel- en encryptiebeheer voor zowel lokale als cloud omgevingen. Zowel het ondersteunen van “Bring your own key” als “Manage your own key”,

volgens regels ikv informatieveiligheid en AVG/GDPR. Verdere optimalisatie van onboarding proces, zodat klanten standaard kunnen aansluiten, via API-ondersteuning en self-service beheer. Verdere uitbouw van self-service portaal en aansluitingsmogelijkheden voor klanten ikv service delivery optimalisatie.

- De beveiligingscomponenten (bv. firewalls) die het netwerk en werkplek beschermen tegen ongeoorloofde toegang en bedreigingen (bv. DDOS aanvallen, cf. Belnet) tijdens hun interactie met netwerken die niet onder de controle vallen van de centrale dienstverlening, ingericht voor de Vlaamse overheid (oa. internet).

- Een systeem voor Privileged Access Management (PAM) dat een gecontroleerde toegang verschaft voor (externe) beheerders van infrastructuur (vereiste in kader van AVG). Dit systeem voorkomt niet geautoriseerde, ongeoorloofde en ongecontroleerde beheer toegang tot systemen van de Vlaamse overheid. Privileged Access Management (PAM). Voorziene uitbreidingen zijn het automatiseren van de interactie tussen PAM en gebruikersbeheer via geautomatiseerde webservices. Verdere onderzoek van secret-management functionaliteiten o.b.v. concrete use cases van klanten. Verdere uitbreiding en automatisatie van onboarding procedure voor klanten, via API-interface en self-service portaal.

- Het beheer van digitale certificaten van de Vlaamse overheid nodig voor versleutelde communicatie en tekenen bij digitale informatie uitwisseling: Certificatenbeheer (VoPKI, VoDCB. Voorziene uitbreidingen zijn API-driven, automatische onboarding en deboarding via ACME.

- Penetratietesten en audits informatieveiligheid om een oordeel of advies gegeven over de kwaliteit en veiligheid van de inrichting van de informatieverwerking. Een audit informatieveiligheid kan eng of breed opgevat worden, zich beperken tot diagnose of ook geïmplementeerde oplossingen omvatten en kan een veelheid aan domeinen omvatten: beleid en organisatie, bewustzijn in de organisatie, technisch beheer, logisch toegangsbeheer, incidentenbeheer, bedrijfscontinuïteit, enzovoort; Pentesten en audits informatieveiligheid. Deze pentesten en audits worden aangeboden binnen de dienstverlening van de raamcontracten van Digitaal Vlaanderen.

- Binnen Digitaal Vlaanderen bieden we met onze veiligheidsbouwstenen een aantal oplossingen aan voor gebruikers die aanmelden in een toepassing van een Vlaamse entiteit of lokaal bestuur. Steeds meer klanten investeren echter in RPA-technologie (Robotic Process Automation), waarbij softwarerobots de handelingen van menselijke gebruikers emuleren (zij het dan veel sneller en efficiënter). Deze RPA-technologie brengt een aantal aandachtspunten met zich mee op het vlak van veiligheid. Voorziene uitbreidingen zijn het volledige E2E lifecycle management van virtuele identiteiten via gebruikersbeheer. Het ondersteunen van sterke authenticatie voor RPA-identiteiten. Het veilig beheren, monitoren van de toegang voor RPA-identiteiten via PAMaaS

Het relanceproject Cyber security en uitrol SIEM (VV065) beoogt volgende resultaten op te leveren:

Nr.	Omschrijving	Voorziene datum
VV065.03.01	Uitrol SIEM: koppeling met bedrijfsapplicaties en kritieke infrastructuurcomponenten	31/12/2022
VV.065.03.02	Uitrol SIEM: Activeren, trainen en optimalisatie van de motor voor artificiële intelligentie via log analytics	31/12/2022

VV.065.03.03	Verdere optimalisatie en inrichting van centraal log management conform vereisten i.k.v wetgeving en informatieveiligheid.	31/05/2022
VV.065.03.04	Verdere uitbouw van encryptiebouwstenen zodat de vertrouwelijkheid van gegevens gegarandeerd blijft.	31/12/2022
VV.065.03.05	Verdere integratie en uitbouw van PAM zodat er steeds controle is op beheerderstoegangen voor zowel infrastructuur als toepassingen, api's.	31/12/2022
VV.065.03.06	Verdere uitbouw Certificatenbeheer	31/05/2022
VV.065.03.07	Uitvoering penetratietesten en het koppelen van de veiligheidsbouwstenen aan geidentificeerde risico's	31/12/2022
VV.065.03.08	Self-service portaal voor klanten: self-assessment, maturiteitsscan, onboarding, opvolging en beheer van risicomaatregelen afgestemd op self-assessment en maturiteitsscan	31/12/2022
VV.065.03.09	Levenscyclusbeheer van RPA identiteiten via de veiligheidsbouwstenen.	31/12/2022

D. PROJECTBEHEER

Over de algemene voortgang van het relanceproject zal op regelmatige basis worden gerapporteerd aan het Stuurorgaan Vlaams Informatie- en ICT-beleid en het directiecomité van het relanceplan Vlaamse Veerkracht.

De operationele uitvoering van het programma wordt verzekerd door de strategische stuurgroep van de gemeenschappelijke dienstverlening van het agentschap. Er zijn eveneens middelen voorzien voor de opvolging van dit programma. Deze opvolging zal worden opgenomen door een extern profiel dat tijdelijk via het USG-contract zal worden aangetrokken.

De noden en behoeften van de verschillende belanghebbenden bij de respectieve deelprojecten worden bevraagd via bestaande klantenfora van het agentschap Digitaal Vlaanderen waaronder het ICT-klantenforum.

Waar nodig worden aanvullend specifieke projectstuurgroepen, werkgroepen en eventuele klankbordgroepen opgericht om maximaal te garanderen dat de opgeleverde resultaten beantwoorden aan concrete noden en behoeften van de beoogde doelgroepen.

Binnen de Vlaamse overheid werden voor elke entiteit bedrijfsveranderingsmanagers aangeduid die het veranderingsbeheer bij de entiteit begeleiden.

3. BESTUURLIJKE IMPACT

A. BUDGETTAIRE IMPACT VOOR DE VLAAMSE OVERHEID

De investeringsmiddelen voorzien in het relanceplan Vlaamse Veerkracht worden belast ten belope van € 2.500.000 VAK in 2021 en 2022. Onderstaande tabel biedt meer details.

Nr.	Transitie dienstverlening	VAK 2021	VEK 2021	VAK 2022	VEK 2022
VV.065.01	VO-brede aanpak van informatieveiligheid			**€ 200.000**	**€ 200.000**
	Verdere uitbouw van informatieclassificatie-raamwerk			€ 90.000	€ 90.000
	Ontwikkeling instrument voor self-assessment			€20.000	€ 20.000
	Opbouw standaardrapportering & centraal dashboard			€ 50.000	€ 50.000
	Ontwikkeling proces en tooling voor conformiteitstoetsing			€ 40.000	€ 40.000
VV.065.02	Verhogen digitale competenties			**€ 55.000**	**€ 55.000**
	Communicatie -en bewustmaking campagne m.b.t. informatieveiligheid			€ 55.000	€ 55.000
VV.065.03	Weerbare digitale processen en robuuste infrastructuur uitbouwen	**€ 560.700**	**€ 460.700**	**€ 1.484.067**	**€ 1.584.067**
	Uitrol SIEM: onboarding van bedrijfsapplicaties en kritische componenten			€ 350.000	€ 350.000
	Uitrol SIEM: Activeren, trainen en optimalisatie van de motor voor artificiële intelligentie via log analytics			€ 80.000	€ 80.000
	Optimalisatie en inrichting van centraal log management	€ 60.000	€ 60.000	€ 154.000	€ 154.000
	Uitbouw encryptiebouwstenen			€ 91.467	€ 91.467
	Integratie en uitbouw PAM	€ 150.700	€ 150.700	€ 145.000	€ 145.000
	Verdere uitbouw Certificatenbeheer	€ 350.000	€ 250.000	€ 100.000	€ 200.000
	Uitvoeren pentesten en het koppelen van de veiligheidsbouwstenen aan geïdentificeerde risico's			€ 163.600	€ 163.600
	Integratie self-service portaal voor klanten			€ 150.000	€ 150.000
	Verdere uitbouw RPA functionaliteiten			€ 250.000	€ 250.000
VV.065.04	Overkoepelend programma management	**€ 78.498**	**€ 78.498**	**€ 121.735**	**€ 121.735**
	Totaal	**€ 639.198**	**€ 539.198**	**€ 1.860.802**	**€ 1.960.802**

RECURRENTE MIDDELEN

Om de doelstelling van de Vlaamse regering inzake digitalisering te versnellen is het van cruciaal belang dat een veilige digitale dienstverlening kan gerealiseerd worden met een recurrente financiering zodat deze functie informatieveiligheid centraal aangestuurd wordt om de coherentie en de snelheid van uitvoering te verhogen om de Vlaamse overheid maximaal te digitaliseren.

Digitaal Vlaanderen heeft, gelet op de aard van haar kernopdrachten, te maken met verschillende kostendrijvers die aangedreven worden door het toenemend gebruik of externe factoren. De belangrijkste **kostendrijvers** zijn:

- Het aantal toestellen en netwerklocaties onder beheer (+ 250)
- Het toenemend gebruik van onze centrale veiligheidsbouwstenen
- Bijkomende maatregelen opgelegd door wetgeving (GDPR, INSPIRE, …)

We voorzien met dit recurrent budget de centrale exploitatiekosten van verschillende bouwstenen op te vangen. Het gaat over volgende componenten:

- De detectie van informatieveiligheidsincidenten en afwijkend gedrag binnen onze ICT-infrastructuur berusten op een hoog beschikbaar 'Security Operations Center' (SOC) dat de klok rond de diensten kan garanderen, zodat de Vlaamse entiteiten minder veiligheidspersoneel moeten aanwerven, continu opleiden en hun interne aanwezigheid moet garanderen om zich te beschermen tegen cybercriminaliteit

- Een adequaat systeem om de auditlogs die systemen genereren (bv. rond toegang tot persoonsgegevens) te archiveren en te bewaren. Deze nood stelt zich bij alle systemen van de Vlaamse overheid (Log management)

- De extra beveiligingscomponenten (bv. firewalls, proxies) die het netwerk en werkplek beschermen tegen ongeoorloofde toegang en bedreigingen in cloud-context (bv. DDOS aanvallen, cf. Belnet) tijdens hun interactie met netwerken die niet onder de controle vallen van de centrale dienstverlening, ingericht voor de Vlaamse overheid (oa. internet)

	Recurrente middelen
SIEM - Security Operations Center	€ 850.000
Exploitatie log management	€ 225.000
Extra beveiligingscomponenten netwerk	€ 350.000
Totaal	**€ 1425.000**

B. ESR-TOETS

Niet van toepassing.

C. IMPACT OP HET PERSONEEL VAN DE VLAAMSE OVERHEID

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

D. IMPACT OP DE LOKALE EN PROVINCIALE BESTUREN

Het voorstel van beslissing heeft geen directe weerslag op de werking of werkingsuitgaven van de lokale en provinciale besturen. De raamovereenkomsten staan wel voor hen ter beschikking om in te zetten in de digitale transformatie van hun beleidsvoering en dienstverlening aan burgers, ondernemers en verenigingen.

5. VOORSTEL VAN BESLISSING

De Vlaamse Regering beslist:

(1) Haar goedkeuring te hechten aan de invulling van het relanceproject 'Cybersecurity & uitrol SIEM' (VV065) en bijhorende eenmalige middelen voor de uitvoeringsperiode 2021-2022 en recurrente middelen vanaf 2022.

De minister-president van de Vlaamse Regering en Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management,

Jan JAMBON