Vlaamse Regering

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

DE VLAAMSE MINISTER VAN BINNENLANDS BESTUUR, BESTUURSZAKEN, INBURGERING EN GELIJKE KANSEN

NOTA AAN DE VLAAMSE REGERING

Betreft: Maatregelen n.a.v. verhoogde dreiging op vlak van informatieveiligheid, opstart van een coördinerend Cyber Response Team voor de lokale overheden en versnelde investeringen m.b.t. VO-strategie informatieveiligheid

Samenvatting

<u>Een eerste pijler van deze nota Vlaamse regering gaat over de oprichting van een 'Cyber Response Team':</u>

De recente cyberincidenten in Zwijndrecht, Antwerpen en Diest hebben ons nogmaals duidelijk gemaakt dat cyberdreigingen in toenemende mate een risico vormen voor overheden op alle niveaus. Sinds enkele weken zien overheden in Vlaanderen het aantal aanvallen op hun ICT-infrastructuur sterk stijgen. Zo'n aanval kan leiden tot de onbeschikbaarheid van ICT-systemen en het verlies van data waaronder ook persoonsgegevens. Er zijn bovendien signalen vanuit het Centrum voor Cybersecurity België (CCB) en de Veiligheid van de Staat dat er mogelijks nog andere centrumsteden de komende weken geviseerd kunnen worden.

Naar aanleiding van deze incidenten wordt een Cyber Response Team (CRT) opgericht. Dit Cyber Response Team zal (1) lokale overheden actief ondersteunen als er zich een incident voordoet en (2) preventief advies geven om een incident te vermijden:

1. **Vandaag ontbreekt deze actieve begeleiding van de getroffen overheidsdienst met betrekking tot wat er precies moet gebeuren, zowel bij een incident als preventief. Het op te richten Cyber Reponse Team zal deze rol opnemen en besturen reactief en preventief bijstaan (bv.: door middel van reeds bestaande draaiboeken). Er wordt gezorgd dat er naar lokale besturen die het slachtoffer zijn geworden van een cyberaanval, de nodige kwalitatieve ondersteuning wordt geboden teneinde de aanval te kunnen remediëren ('response'). Concreet zal er in dat geval steeds een team van experten uit het CRT gestuurd worden naar het geïmpacteerd lokaal bestuur, die zullen zorgen voor een eerste contactname, coördinatie en begeleiding. Daarnaast zal het CRT desgevallend ook ondersteuning geven bij het melden van datalekken, enzovoort.**

2. **Daarnaast zal het CRT de expertise tussen de bevoegde Vlaamse en federale overheidsdiensten bundelen en ervoor zorgen dat er een gecoördineerde dienstverlening en communicatie naar de lokale besturen toe verzorgd zal worden. Digitaal Vlaanderen zal verzekeren dat de informatiedoorstroming vanuit het CRT richting de VO wordt opgenomen.**

Het CRT zal opereren in nauwe samenwerking met onder andere het CCB en de politiediensten. Het CERT en de politie zijn en blijven verantwoordelijk voor het digitaal forensisch onderzoek en het vatten van de daders.

<u>Een tweede pijler van deze nota gaat over versnelde investeringen m.b.t. de strategie informatieveiligheid binnen de Vlaamse overheid:</u>

Een weerbare ICT-infrastructuur is dus noodzakelijker dan ooit, zeker omdat onze samenleving en haar overheid steeds sneller digitaliseert. Naar aanleiding van de Coronacrisis, werden reeds een aantal investeringen gedaan om de continuïteit van de dienstverlening van de Vlaamse overheid te kunnen garanderen, en de digitale werkplek op hetzelfde niveau te brengen als de fysieke werkplek, zowel wat beschikbaarheid, functionaliteit als veiligheid betreft. Om het beveiligingsniveau van de Vlaamse overheid zelf naar een hoger niveau te brengen, dringen zich een aantal investeringen op om de uitvoering van de strategie informatieveiligheid te verhogen.

1. SITUERING

A. BELEIDSVELD/BELEIDSDOELSTELLING

BELEIDSDOMEIN: Kanselarij en Bestuur

BELEIDSVELD: Binnenlands Bestuur en stedenbeleid / Brussel / Vlaamse Rand / Gelijke Kansen en Integratie en Inburgering / Digitalisering

B. VORIGE BESLISSINGEN EN ADVIEZEN

Door de toegenomen digitalisering lopen Vlaamse bedrijven meer dan ooit het risico om slachtoffer te worden van cybercriminelen. Het kan elk bedrijf overkomen. Zowel kleine kmo's als grote multinationals, in om het even welke sector. Voor de Vlaamse Regering is cyberveiligheid dan ook een topprioriteit.

<u>Beleidsplan Cybersecurity</u>

De Vlaamse Regering keurde op 22 maart 2019 het Beleidsplan Cybersecurity goed om die ambitie te ondersteunen. Onder de noemer Cybersecurity Vlaanderen voorziet het een jaarlijkse investering van € 20 miljoen. Het plan bestaat uit 3 luiken die elkaar aanvullen en versterken.

<u>Informatie en veiligheidsstrategie (VR 2021 1510 DOC.1151/1)</u>

Deze strategie werd goedgekeurd door Vlaamse Regering op 15/10/2021. VR 2021 1510 DOC.1151/1

De Vlaamse overheid wil met deze strategie volgende doelstellingen bereiken:

- Bedrijfscontinuïteit garanderen tijdens en na een ernstig incident.
- De persoonlijke levenssfeer van de burger beschermen.
- Het vertrouwen genieten van de burger, onderneming en/of vereniging.
- De reputatie hooghouden van de overheid als betrouwbare partner.

Actieplan cyberveilige steden en gemeenten (VR 2020 3004)

In het kader van dit actieplan is het project cyberveilige steden en gemeenten opgestart i.s.m. de VVSG. Het project omvat 3 sporen:

- Het ontwikkelen en onderhouden van een digitale toolkit met handleidingen, leidraden, checklists en sjablonen om de steden en gemeenten te informeren en ondersteunen bij de interne organisatie.
- Het organiseren van het traject ethisch hacken i.s.m. Howest, waarbij ethische hackers de informatiesystemen van lokale besturen doorlichten.
- Sensibiliserings- en vormingsinitatieven voor verschillende doelgroepen binnen lokale besturen, nl. het management en beleid of ICT-medewerkers.

Cofinanciering van ICT-veiligheidsaudits voor lokale besturen (VR 2020 3004)

Verder kunnen lokale besturen een professionele ICT-veiligheidsaudit laten uitvoeren met cofinanciering. De basisaudit omvat een meerdaagse analyse van kwetsbaarheden van ICT-systemen en een dag begeleiding om de remediëring van de meest prioritaire kwetsbaarheden op te starten. Verder kan een bestuur ook aanvullende auditwerkzaamheden bestellen naast de basisaudit. Lokale besturen kunnen rekenen op cofinanciering voor de basisaudit en de aanvullende audit.

Aanbod Lokaal Digitaal (VR 2022 1507)

Digitaal Vlaanderen werkt via Lokaal Digitaal een vraaggestuurd aanbod 'Lokaal Digitaal' voor alle lokale besturen uit vertrekkende vanuit de bestaande structuren en expertise van de Vlaamse Overheid. Lokale besturen kunnen de vele digitale uitdagingen niet langer individueel aan of zijn naast elkaar gelijkaardige oplossingen aan het onderzoeken, uitwerken, aanbesteden en implementeren, waardoor heel wat tijd, middelen, energie en expertise verloren gaan. Zeker rond de uitbouw van performante cyberveilige IT-infrastructuur en open geïntegreerde oplossingen (die gegevens kunnen delen met andere toepassingen) is een gezamenlijke aanpak aangewezen. Lokaal Digitaal tracht een antwoord te bieden op deze uitdagingen.

2. INHOUD

A. NOODZAAK VAN EEN CYBER RESPONSE TEAM

Digitale instrumenten zullen nu en in de toekomst meer dan ooit het verschil maken in de lokale besturen. Dat vereist een sterke cyber- en informatieveiligheid.

Naar aanleiding van de informatieveiligheidsincidenten bij de lokale besturen Zwijndrecht, Antwerpen en Diest is gebleken dat lokale besturen kwetsbaar zijn voor hacking. Bij deze verschillende incidenten is de dienstverlening aan de burger door het betrokken lokaal bestuur gedurende enkele dagen tot enkele weken in belangrijke mate onderbroken en/of verstoord. Wanneer een lokaal bestuur geconfronteerd wordt met een cyberaanval of ander IT-gerelateerd incident, dienen op korte termijn diverse maatregelen genomen te worden om de situatie onder controle te krijgen en terug te keren naar de gewone werking. Proactief nadenken over de te nemen stappen faciliteert het crisisbeheer bij grootschalige incidenten.

Het bestrijden van cyberveiligheidsincidenten is jammer genoeg geen rechtlijnig proces, maar een complexe oefening waarbij diverse acties door elkaar lopen, gaande van het detecteren van een incident, tot het inperken van schade, het herstellen van de dienstverlening, melden aan de bevoegde instanties, rapporteren aan regulatoren en slotbeschouwing. Er is een belangrijke rol weggelegd voor ICT, maar al even belangrijk zijn de organisatorische inrichting en de uitvoering van het afsprakenkader die interne en externe communicatie en organisatiebeheersing faciliteren. Om lokale besturen hierin te ondersteunen, is in het kader van het actieplan cyberveilige steden en gemeenten een toolkit cyberveiligheid ontwikkeld door de VVSG met sjablonen, richtlijnen en checklists. Hiermee worden de nodige handvaten aangereikt aan lokale besturen om zich preventief voor te bereiden op eventuele cyberincidenten.

Gezien de complexiteit van deze materie is het voor vele lokale besturen niet haalbaar om zich hier tijdig op te organiseren en om alle nodige gespecialiseerde expertise aan boord te hebben. De kans is reeël dat een lokaal bestuur externe expertise zal moeten inroepen om het incident zo vlot en efficiënt als mogelijk aan te pakken. Bovendien gebeurt het niet elke dag dat cybercriminelen je dienstverlening en werking volledig dreigen plat te leggen. Daarnaast is een gecoördineerde kennisdeling tussen alle betrokken partijen een must.

De oprichting van een op Vlaams niveau aangestuurd Cyber Response Team (CRT) zorgt voor de nodige synergie en efficiënte inzet van middelen. Digitaal Vlaanderen en het Agentschap Binnenlands Bestuur zullen de krachten bundelen en hun expertise inzetten om de lokale besturen optimaal te ondersteunen.

Via de Smart Region Board wordt het Agentschap Innoveren en Ondernemen en het Vlaams Departement Economie, Wetenschap en Innovatie op de hoogte gehouden van de werkzaamheden van het CRT.

B. ONDERSTEUNING CYBER RESPONSE TEAM VAN DE VLAAMSE OVERHEID

Het Cyber Response team biedt een centrale ondersteuning vanuit de Vlaamse overheid ter ondersteuning van de lokale besturen. Deze ondersteuning is gefocust op de preventie van cyberincidenten als op remediëring en herstel. Het is van belang dat deze ondersteuning in het geval van een incident, kan leiden tot een concreet incidentresponseplan, dat rekening houdt met de context, aanwezige middelen, capaciteit en rollen binnen het lokaal bestuur.

Het CRT zet hiervoor de nodige beheerssystemen en rapportering op (gebaseerd op de bestaande tooling binnen Digitaal Vlaanderen) zodat een vlotte, professionele dienstverlening gegarandeerd wordt, deze dienstverlening opgevolgd wordt en waar nodig bijgestuurd.

Deze aanpak voorziet een flexibele opschaling of afbouw van de activiteiten in functie van het dreigingsniveau, de actuele situatie van de incidenten. Dit voorstel vormt de basis voor een korte-termijn respons op de recente gebeurtenissen en vormen de basis van meer structurele maatregelen op langere termijn.

Het CRT-team bestaat uit volgende rollen en verantwoordelijkheden:

Coördinator (Expert / Part time)

- Verzekeren dat de juiste functies de nodige rollen vervullen.

- Verzekeren dat alle acties tijdig worden uitgevoerd door de verschillende rollen.

Mailbox Analyst (Junior / Part time)

- Monitoren van de centrale mailbox.
- Documenteren / centraliseren van de vragen van lokale besturen.
- Toewijzen van de vragen aan de relevante rollen.

IT / Cyber Expert (Expert, Junior / Part time)

- Behandelen van technische vragen (bv. best practices rond patch management, vulnerability tools, …).
- Verzamelen en verwerken van verslagen om geleerde lessen te trekken en te delen met lokale besturen, zoals o.a.:
- Lessons learned rapporten van voorbije incidenten bij lokale besturen.
- Audit findings ihkv Cyber Veilige Gemeenten (Audit Vlaanderen).

Communicatie Expert (Expert, Junior / Part time)

- Behandelen van vragen rond communicatie.
- Voorbereiden van communicaties voor externe stakeholders (e.g., CCVO, lokale besturen, …)
- Opvolgen van (sociale) media rond lopende / nieuwe cyberincidenten bij lokale besturen.

Juridisch Expert (Expert / Part time)

- Behandelen van juridische vragen (bv. meldingsplicht, …).

Toolkit Analyst (Junior / Part time)

- Verzamelen en centraliseren van toolkits die lokale besturen toelaten om cyberincidenten te beheersen (bv. toolkit van CCVO, VVSG, CCB, …).

Liaison met overheden, overheidsdiensten en gerechtelijke instanties (Expert / part time)

- Monitoren en uitvoeren van acties waarbij interactie met overheden, overheidsdiensten en/of gerechtelijke instanties vereist is.

Dit team zal worden besteld op het raamcontract van Audit Vlaanderen m.b.t. ICT-audits. Volgende prijszetting wordt gehanteerd.

Profiel	Senioriteit	Profiel raamcontract	Dagprijs (ex BTW)
Coordinator & Comms	Senior Manager	Profiel D	€ 2.621,94
IT Cyber Expert (analyse)	Exp. SR Consultant	Profiel C	€ 1.038,29
Juridisch expert	Senior Consultant	Profiel B	€ 812,80
Toolkit Analyst	Junior	Profiel A	€ 686,95
Mailbox analyst	Junior	Profiel A	€ 686,95
Communicatie	Junior	Profiel A	€ 686,95

De capaciteit is flexibel en zal variabel zijn in functie van de werklast. We herevalueren de samenstelling van het team in functie van de doelstelling, in het bijzonder omtrent het gepaste profiel voor de rol van coördinator.

Remediëring en herstel

Het CRT biedt ondersteuning bij de opstart van een cyber response plan. Dit cyber response plan bestaat uit een stappenplan en een kader die de geïmpacteerde partij onmiddellijk kan toepassen zodat de business continuïteit zo snel mogelijk hersteld kan worden. Dit plan is gebaseerd op beste praktijken in dit domein en in overeenstemming met de procedures en richtlijnen van toepassing binnen de Vlaamse overheid.

Het team bundelt alle beschikbare informatie vanuit de verschillende partners binnen zowel de federale (CCB) als Vlaamse Overheid (Digitaal Vlaanderen en het Agentschap Binnenlands Bestuur). Daarnaast worden ook verschillende externe partijen betrokken (VVSG, V-ICT-OR, ICT-dienstenleveranciers en andere ledenorganisaties), de vragen ontvangen van de lokale besturen, de bevindingen van Audit Vlaanderen en de input vanuit threat intelligence (specifieke case info en advies van het Centrum voor Cybersecurity België (CCB), de geheime diensten en Cyber Threat Intelligence van commerciële partijen).

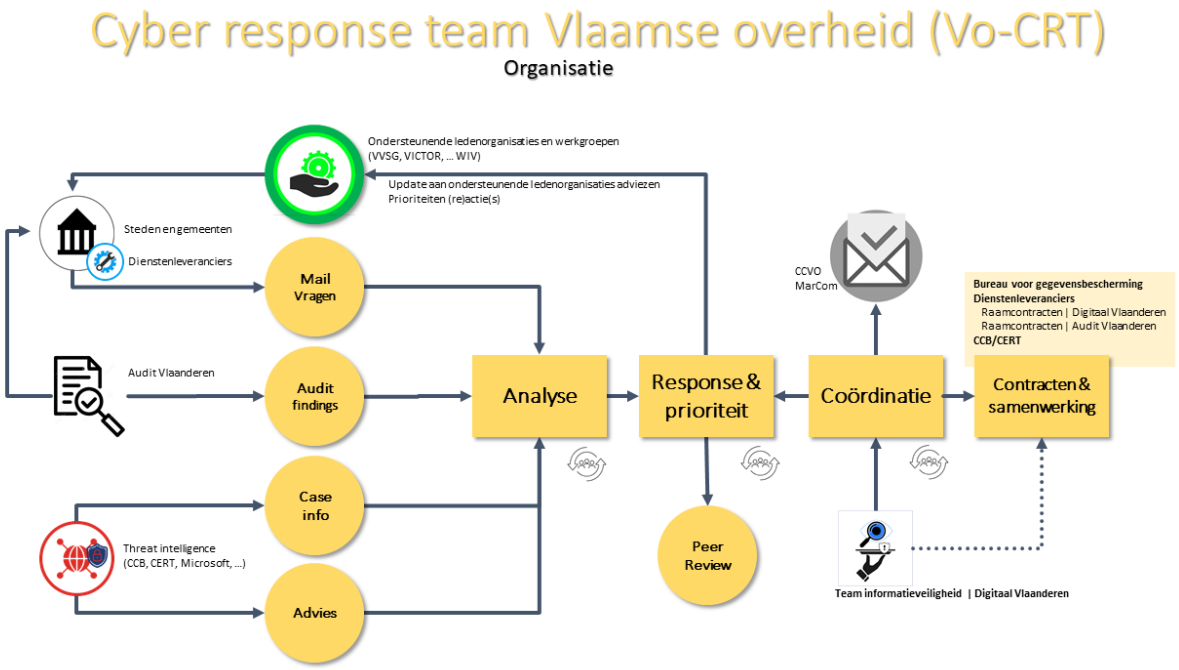
Het team analyseert de verzamelde informatie en bepaalt op basis daarvan de correcte response en prioriteit en dit na afstemming met de VVSG en V-ICT-OR. Op basis van deze informatie kan ook het bestaande ondersteuningsaanbod voor lokale besturen (bv. cyberveilige steden en gemeenten) verder worden uitgewerkt.

Verder coördineert het team de interne en externe communicatie naar alle belanghebbenden: geïmpacteerde partijen, leidend ambtenaren en de media.

Het team voert ook een analyse van de impact op de Vlaamse overheid uit (b.v. noodzaak van nooddecreten m.b.t. Omgevingsvergunningen). Nadien coördineert het team ook de nodige acties i.k.v de impact op de Vlaamse overheid.

Tenslotte zorgt het team voor de juridische begeleiding bij de te ondernemen stappen waaronder: informeren van de Gegevensbeschermingsautoriteit, het Bureau voor Gegevensbescherming van Digitaal Vlaanderen en de federale diensten.

Onderstaande figuur vat de taken en interacties van het CRT samen.



Preventief

Om nieuwe informatieveiligheidsincidenten te voorkomen, verzamelt het CRT de beschikbare informatie (actuele cases, informatie van het Centre for Cyber Security Belgium (CCB), de geheime diensten en Cyber Threat Intelligence van commerciële partijen) en verwerkt deze informatie in nieuwe adviezen, dit in nauwe samenwerking met de ondersteunende ledenorganisaties.

Het team verspreidt deze adviezen naar de Vlaamse administratie en via de VVSG en andere ledenorganisaties (V-ICT-OR, VERA, ...) naar de lokale besturen.

Het team capteert ook de noden van lokale besturen om extra dienstverlening en tools te ontwikkelen om de adviezen ook daadwerkelijk te implementeren.

We bieden snelle communicatie, kant-en-klare overeenkomsten, processen en procesbegeleiding aan met zowel gespecialiseerde cyber defense organisatie als de dienstverlening en expertise van Digitaal Vlaanderen: Bureau voor Gegevensbescherming en Team Informatieveiligheid.

Lokale ondersteuningsteam

Het CRT zorgt voor eerste contactname, begeleiding en ondersteuning. Op die manier zal het CRT het getroffen lokaal bestuur vlot laten kennisnemen van bestaande draaiboeken en van het aanbod van CRT voor zover nog niet gekend. Het CRT zal opereren in nauwe samenwerking met onder andere het CCB en de politiediensten. Hun diensten zullen complementair zijn aan de diensten die worden aangeboden door het CCB
Het CRT zal een adviserende rol opnemen en zal het lokaal bestuur leiden naar het bestaande ondersteuningsaanbod.

Dit eerste luik wordt voor 100% gefinancierd door de Vlaamse Overheid.

Het CRT voorziet ook in een 'vliegend team' dat naar een lokaal bestuur dat getroffen is door een cyberaanval ter plaatse kan worden gestuurd. Indien externe expertise nodig is om de crisis in goede banen te leiden, kan het CRT advies verlenen en aangeven welke ondersteuning het lokaal bestuur bijkomend kan gebruiken. Op basis daarvan kan het lokaal bestuur vervolgens een geschikte leverancier aanstellen, al dan niet via het raamcontract van Audit Vlaanderen. De uitvoering gebeurt in nauwe afstemming met het CRT, zodat maximaal hergebruik en standaardisatie wordt bereikt. Dit luik wordt voor 100% gefinancierd door de lokale besturen.

Onderstaande figuur vat dit samen:

C. VERSNELDE INVESTERINGEN M.B.T. DE STRATEGIE INFORMATIEVEILIGHEID BINNEN DE VLAAMSE OVERHEID

De strategie m.b.t. informatie-veiligheidsstrategie werd goedgekeurd door Vlaamse Regering op 15/10/2021. Deze nota wil een versnelling in de uitvoering van deze strategie bewerkstelligen via structurele maatregelen die de organisatie en beheersing van risico's versterkt en bovendien de beveiliging van het netwerk, de cloud -en datacenterinfrastructuur en bijhorende beveiliging (firewall, VPN, etc.) verhogen. Daarmee gaan we verder op het elan van de investeringen naar aanleiding van de Coronacrisis, om de continuïteit van de dienstverlening van de Vlaamse overheid te kunnen garanderen, en de digitale werkplek op hetzelfde niveau te brengen als de fysieke werkplek, zowel wat beschikbaarheid, functionaliteit als veiligheid betreft.

Het is belangrijk op te merken dat de Vlaamse overheid voor heel wat (digitale) dienstverlening de backbone levert voor de lokale besturen en het daarom minstens even belangrijk is dat we de VO-cyberveiligheid garanderen. Het is ook veel moeilijker om op regionaal niveau naar een 'offline' dienstverlening te evolueren zoals lokale besturen dit in sommige noodgevallen hebben gedaan. Dat maakt de impact van een cyberincident potentieel nog veel groter.

De verschillende veiligheidsteams hebben in de afgelopen weken eveneens verhoogde activiteit vastgesteld op o.m. de netwerkinfrastructuur (DDOS-aanvallen), Mijn Burgerprofiel (DDOS) en toepassingen gerelateerd aan lokale dienstverlening (de toepassing 'maatschappelijke oriëntatie ' van AGII).

De strategie focust zich rond een aantal pijlers.

Een VO-brede aanpak van informatieveiligheid en digitale competenties

Door een duidelijk kader, governance en verantwoordelijkheden vast te leggen kunnen we tot een VO-gedragen aanpak voor informatieveiligheid evolueren.

In het geval van een cyberincident is bijvoorbeeld een gestructureerde en goed afgelijnde communicatie en samenwerking cruciaal zijn om de werking en het herstel van de Vlaamse overheid te garanderen. De gebruiker heeft niet alleen nood aan het delen van documenten maar evolueert naar een geïntegreerde communicatie die verschillende kanalen samenbrengt. Daarvoor is het ook noodzakelijk dat de interne processen binnen de gemeenschappelijke ICT-dienstverlening over alle bouwstenen heen uniform worden gemaakt (bv. MAGDA, MijnBurgerprofiel, ICT-raamcontracten). Een ISO-cerficatie kan in belangrijke mate bijdragen aan de maturiteit en continue verbetering van de security-organisatie.

Concreet gaat het om volgende investeringen in 2023:

VO-brede aanpak van informatieveiligheid		**800.000 €**
Cyberweerbaarheid	Cyber security & response team VO	350.000 €
	Coördinatie m.b.t. ISO27001 certificering Digitaal Vlaanderen	250.000 €
SIAM Digitaal Vlaanderen	Stroomlijnen interne (security) processen (MAGDA, MBP) op service-integratie management (SIAM, P1) tooling	200.000 €

Deze budgetten rond cyber response teams zijn gebaseerd op een kostinschatting op basis van bovenstaande tarieven. Er wordt eveneens gebruik gemaakt van het raamcontract van Audit Vlaanderen Aangezien er reeds een bestaande informatieveiligheidsorganisatie is, wordt de noodzakelijke capaciteit kleiner ingeschat dan voor lokale besturen.

De coördinatie m.b.t. ISO27001 en SIAM Digitaal zijn projecten om de efficiënte van de bouwstenen van Digitaal Vlaanderen te verhogen in geval van een cyberincident en zullen concreet bestaan uit 2 VTE die via USG en perceel 1 van de raamcontracten zullen worden gecontracteerd.

De recurrente kost bestaat uit het noodzakelijke werkingsbudget om de opgerichte teams verder te zetten. Deze kosten zijn dus gebaseerd op de initiële tijdsinschatting aan de tarieven van de resp. raamovereenkomst. Niettegenstaande aan kennisopbouw en documentatie zal worden gedaan tijdens de initieel voorzien periode, is het noodzakelijk dit te verduurzamen zodat de weerbaarheid wordt verhoogd binnen de Vlaamse overheid. De trend naar meer cyberdreigingen en mogelijke impact op onze werking maken deze continuïteit absoluut noodzakelijk.

Weerbare infrastructuur

Deze prioriteit heeft als doelstelling om het veiligheidsniveau van de informatieverwerking op operationeel niveau te verhogen door de juiste organisatie en veiligheidsbouwstenen te voorzien.

Met deze prioriteit willen we het volgende resultaten bereiken:

1. Verhogen van de maturiteit van onze veiligheidsorganisatie door ondersteuning met betrekking tot veiligheidsdienstverlening & tools;
2. Geïntegreerde dienstverlening met betrekking tot het beheersen van risico's van onze gemeenschappelijke ICT-systemen;
3. Verhogen van het operationele veiligheidsniveau door veiligheidsbouwstenen van de Vlaamse Overheid verder uit te bouwen;
4. Tijdige detectie van informatieveiligheidsincidenten;
5. Versterkte slagkracht met betrekking tot ernstige informatieveiligheidsincidenten.

Concreet gaat het om volgende investeringen in 2023:

Weerbare infrastructuur		**1.215.000 €**
Architectuur & weerbaarheid van de datacenter -en netwerkinfrastructuur versterken	Finaliseren uitrol software-defined netwerk (netwerksegmentatie)	200.000 €
	Verhogen van de redundantie van het netwerk	20.000 €
	Implementatie zero-trust security concept (incl. IoT monitoring)	200.000 €
	DNS Sec integratie met SIEM	40.000 €
	Datacenter: versterking van toegang voor beheerders	55.000 €
	Betere monitoring op werkplekken (bv. versleuteling, ransomware, …)	100.000 €
Veiligheidsbouwstenen	Versterking toegangsbeheer (risico op ongeoorloofde toegang verkleinen voor +1000 toepassingen)	250.000 €
Vermindering van veiligheidsrisico's door uitfasering legacy-infrastructuur	Netwerk: EOSL vervanging/phaseout decentrale fortinets FW's	150.000 €
	API Management Consolidatie & Security monitoring	200.000 €

Deze budgetten zijn gebaseerd op een kostinschatting door de verschillende teams. Er is geen hardware -en softwarekost voorzien, m.u.z. 20K euro ter verhoging van de reduntatie, aangezien het voornamelijk om integratie en configuratie van verschillende infrastructuurcomponenten betreft. De kosten zijn voornamelijk gebaseerd op mensuren die binnen de ICT-raamcontracten (percelen 1, 2, 3 en 4) zullen worden gepresteerd aan de standaardtarieven. De totale inschatting bedraagt 1.493MD over de verschillende trajecten.

3. BESTUURLIJKE IMPACT

A. BUDGETTAIRE IMPACT VOOR DE VLAAMSE OVERHEID

Voor de opstart van het Cyber Response Team en de operationele werking 2022-2023 is een budget nodig van in totaal 1.000.000 EUR opgedeeld zoals hieronder aangegeven. Na 6 maanden wordt de werking, samenstelling en financiering van het Cyber Reponse Team geëvalueerd.

Deze kost wordt in 2023 belast:

- ten belope van €500.000 VAK op het krediet bestemd voor het Gemeente zonder Gemeentehuisproject en in de begroting is ingeschreven op het artikel SJ0-1SMC2GD-WT;
- en ten belope van €500.000 VAK op het krediet bestemd voor e-inclusieprojecten en in de begroting is ingeschreven op het artikel SJ0-1SFC2CA-WT.

Omwille van die reden kan de recurrente kost voor dit team die vanaf 2024 zal bestaan, momenteel nog niet worden begroot.

Activiteit	2022	2023
Opstart ondersteunende tooling: Service Management		80.000€
Curatieve en preventieve ondersteuning (1 maand in 2022)	120.000 €	
Curatieve en preventieve ondersteuning		700.000 €
Coördinatie		100.000 €
Totaal	**€120.000**	**€880.000**

Voor de investeringen in 2023 om de VO-strategie informatieveiligheid te versnellen is een budget nodig van 2.015.000 EUR. Bij begrotingsaanpassing 2023 zal het budget voor deze investeringen worden verschoven naar Digitaal Vlaanderen vanuit de enveloppe Wonen. Dit wordt gecompenseerd door de verdeling van de klimaatmiddelen naar de enveloppe van Wonen voor hetzelfde bedrag.

De verduurzaming van deze strategie (m.a.w. de recurrente kost vanaf 2024), zal op een later moment worden geëvalueerd. Er loopt momenteel een nulmeting die de cyberveiligheid bij zowel de Vlaamse overheid als lokale besturen in kaart brengt. Op basis van de bijhorende risico-analyse, kan een meer onderbouwde inschatting gemaakt worden van de recurrente behoeften. Dit zal in een latere fase aan de Vlaamse Regering worden voorgelegd.

Activiteit	2023
Investeringen Vo-brede aanpak informatieveiligheid	800.000 €
weerbare infrastructuur	1.215.000 €
Totaal	**€2.015.000**

Het advies van de Inspectie van Financiën werd op 21/12/2022 verleend (GDR/2022005574).
Het begrotingsakkoord werd aangevraagd.

In haar advies heeft de Inspectie van financiën een aantal bemerkingen geformuleerd welke hieronder worden toegelicht:

- *In de nota wordt aangeven dat een gecoördineerde kennisdeling tussen alle betrokken partijen een must is. In welke mate komt dit al niet gedeeltelijk reeds aan bod in het kader van bovenvermelde initiatieven? Was het bijvoorbeeld ook niet één van de doelstellingen om in het kader van de ICT-veiligheidsaudits aan kennisdeling te doen?*

Binnen het kader van bovenvermelde initiatieven wordt inderdaad al aan kennisdeling gedaan. Globale audit-bevindingen worden gedeeld via infosessies. Binnen het project cyberveilige gemeenten wordt de opgebouwde kennis via een kennisbibliotheek ter beschikking gesteld.

Beide bronnen dienen als input voor het cyber response team. Op zijn beurt zal het team ook bovenvermelde bronnen kunnen aanvullen met nieuwe informatie. We bouwen dus verder op bestaande informatie en kennis.

In beide gevallen gaat het vandaag echter om high-level en algemene informatie dat niet wordt toegepast binnen de specifieke context van een bepaald cyberincident of binnen een lokaal bestuur. Er is m.a.w. geen kennisdeling uit concrete incidenten en kwetsbaarheiden. Dat is de taak van het cyber response team.

We zien dat lokale besturen in de praktijk onvoldoende gebruik kunnen maken van de opgebouwde kennis wegens beperkte competenties binnen de organisatie. Het CRT zal de vertaling kunnen maken naar het terrein.

- *Het CRT voorziet in een 'vliegend team' dat naar een lokaal bestuur dat getroffen is door een cyberaanval ter plaatse kan worden gestuurd. Tot hoever gaat deze ondersteuning? Wat dient lokaal bestuur minimaal zelf op te nemen? Een duidelijke afbakening is noodzakelijk in wat de ondersteuning precies bestaat zodat de verwachtingen eveneens duidelijk zijn.*

De tekst wordt aangepast om verdere verduidelijking te geven bij de scope van het 'vliegend team'. Het lokaal bestuur kan beroep doen op deze ondersteuning voor een brede waaier activiteiten binnen de context van het cyberincidenten. Deze afbakening zal case per case worden gedaan voorafgaand aan de start van de opdracht, zodat de verwachtingen ten alle tijden duidelijk zijn.

- *De Inspectie van Financiën moet vaststellen dat voor recurrente taken externen worden ingeschakeld zodat er een risico is van weinig tot geen kennisopbouw. Mogelijks moet er ook wisselend personeel worden ingezet ook voor de recurrente taken. Dergelijke opdracht in zijn totaliteit laten uitvoeren door een derde is af te raden.*

De overweging maakt deel uit van de geplande evaluatie. Op dat moment kan de piste worden bekeken om interne mankracht in te schakelen en de kennis te verduurzamen. Gezien de hoogdringendheid is dat bij het begin van het traject echter geen mogelijkheid.

- *Inzake het Cyber security & response team VO wordt enkel verwezen naar bestaande tarieven maar er is verder geen enkele informatie over de samenstelling van dit team met bijvoorbeeld een opdeling tussen opstartkosten en recurrente kosten. De IF kan dit dus niet beoordelen. De coördinatie m.b.t. ISO27001 en SIAM Digitaal zijn projecten om de efficiënte van de bouwstenen van Digitaal Vlaanderen te verhogen in geval van een cyberincident en zullen concreet bestaan uit 2 VTE die via USG en perceel 1 van de raamcontracten zullen worden gecontracteerd. Er wordt verder geen duiding geven over de duurtijd van het project, het soort profielen en de motivering waarom specifiek op de raamcontacten beroep wordt gedaan. Op basis van deze informatie kan de IF het voorstel niet evalueren.*

De tekst is aangepast in die zin. De recurrente kost bestaat uit het noodzakelijke werkingsbudget om de opgerichte teams verder te zetten. Deze kosten zijn dus gebaseerd op de initiële tijdsinschatting aan de tarieven van de respectievelijke raamovereenkomsten. Niettegenstaande

aan kennisopbouw en documentatie zal worden gedaan tijdens de initieel voorzien periode, is het noodzakelijk dit te verduurzamen zodat de weerbaarheid wordt verhoogd binnen de Vlaamse overheid.
De keuze van de raamcontracten komt voort uit de situatie van hoogdringendheid. Er was niet voldoende tijd om zelf mensen aan te werven. Waar een link is met de huidige operationele dienstverlening wordt gebruik gemaakt van de ICT-raamcontracten. Indien niet, wordt het raamcontract van Audit Vlaanderen en/of USG gebruikt, in functie van de aard van de profielen.

- *Weerbare infrastructuur. In totaal wordt voor 1.250.000 euro aan investeringen voorzien (projecten, zie blz. 10 nota aan de VR). Sommige van deze projecten zijn logisch zoals versterking toegangsbeheer. Voor andere projecten is het niet duidelijk waarom juist deze keuze wordt gemaakt. Welke afweging werd gemaakt? De totale inschatting bedraagt 1.493MD over de verschillende trajecten. Een detail wordt niet gegeven.*

De afweging voor de investeringen is gemaakt op basis van een risico-inschatting en expertise van de verschillende domeinexperten die binnen de ICT-raamcontracten actief zijn. Er werd hoofdzakelijk beoordeeld welke risico's en bedreigingen die we globaal zien gebeuren, binnen de huidige dienstverlening additioneel konden gemitigeerd worden. De grootorde van de budgetten is indicatief voor de verdeling van het aantal mandagen over alle investeringen.

- *Voor de opstart van het Cyber Response Team en de operationele werking 2022-2023 wordt het benodigde budget geraamd op in totaal 2.670.000 EUR. De Inspectie van Financiën kan deze raming niet beoordelen. Hoeveel VTE worden concreet ingezet. Waarom nog een kost van 120 KEUR in 2022? Wat zijn de verdere uitgangspunten bijvoorbeeld inzake de inzet van vliegende teams? Rekening houdend met de verschillende profielen en de dagprijs van deze profielen, de voltijdse en halftijdse inzet van deze profielen zoals werd vermeld in de nota aan de Vlaamse Regering en uitgaande van 220 werkdagen wijkt de kost toch aanzienlijk*

Omwille van budgettaire redenen wordt de scope van het Cyber Response Team bijgesteld, waardoor het te begroten bedrag ook naar beneden zal worden bijgesteld. Het benodigde budget wordt op die manier niet meer op 2.670.000 EUR geraamd, maar op 1.000.000 EUR.
Er worden in totaliteit tijdens de eerste 6 maanden gemiddeld 50 mandagen per maand ingezet over 8 profielen. We voorzien een eerste rationalisatie en evaluatie van de noodzakelijke inzet na 6 maanden. Er is geen kost voorzien voor de vliegende teams. De nota werd in die zin verduidelijkt.

De reden voor de kost in 2022 is omdat de activiteiten n.a.v. de recente incidenten reeds is opgestart vanwege de hoogdringendheid.

- *De Inspectie van Financiën wijst erop dat de uitgaven waarschijnlijk 100% in VEK dienen te worden aangerekend in 2023 zodat compensatie op de onderbenutting 2022 niet mogelijk is. Tevens kunnen geen vastleggingen 2022 op niveau DV worden genomen want de IF begrijpt dat er nog geen offertes zijn (welke profielen juist zullen worden ingezet voor welke periode is immers onduidelijk). De Inspectie van Financiën is niet akkoord met de stelling dat er geen budgettaire impact is.*

De nota werd na het advies van de Inspectie van Financiën bijgesteld waardoor de VAK-impact van het project niet in 2022, maar in 2023 zal komen te liggen. Het Agentschap Binnenlands Bestuur zal de kosten die gemaakt zijn in 2022 door het Agentschap Digitaal Vlaanderen omwille van hoogdringendheid, vergoeden.

- *Bijkomende middelen worden gevraagd om de VO-strategie informatieveiligheid te versnellen. Wat zou bijvoorbeeld de impact zijn op andere projecten indien deze versnelling moet opgevangen worden binnen de bestaande referte kredieten? Welke projecten stelt men dan voor te verschuiven? De IF wijst erop dat dat men tevens al de goedkeuring vraagt van de recurrente benodigde middelen hoewel deze nog niet kunnen worden ingeschat. M.a.w. het dossier wordt eigenlijk te vroeg ingediend.*

M.b.t. de recurrente middelen is de nota aangepast. M.u.v. concrete projectbudget (bv. VRD2) is er momenteel geen ruimte binnen de bestaande referte krediet voor andere projecten. De uitvoering van de gevraagde versnelling is dus afhankelijk van de goedgekeuring van deze nota.

- *De lokale besturen kunnen op termijn beroep doen op het aanbod van het CRT. Wanneer concreet de vliegende teams kunnen worden ingezet is niet duidelijk. Uit het voorstel blijkt immers dat nog verschillende elementen dienen te worden uitgewerkt waarbij wel wordt aangegeven dat veel materiaal zal worden gerecupereerd.*

De inzet van de vliegende teams dient case-per-case worden beoordeeld i.f.v. gevraagde capaciteit. In principe kunnen de vliegende teams ingezet worden vanaf januari 2023.

B. ESR-TOETS

Niet van toepassing

C. IMPACT OP HET PERSONEEL VAN DE VLAAMSE OVERHEID

Geen impact op het personeelsbestand noch op de personeelsbudgetten.

D. IMPACT OP DE LOKALE EN PROVINCIALE BESTUREN

Geen weerslag van het voorstel op de lokale en provinciale besturen.

4. VOORSTEL VAN BESLISSING

De Vlaamse regering beslist:

1. Haar goedkeuring te hechten aan de oprichting van het Cyber Response Team en bijhorende eenmalige middelen voor de uitvoeringsperiode 2022-2023;

2. Haar goedkeuring te hechten aan het voorstel om de VO-strategie rond informatieveiligheid te versnellen en de nodige investeringen vrij te maken en toe te voegen aan de begroting van het Eigen Vermogen Digitaal Vlaanderen.

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

//

JAN JAMBON

De Vlaamse minister van Binnenlands Bestuur, Bestuurszaken, Inburgering en Gelijke Kansen

BART SOMERS