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: Aanvullende ondersteuning voor lokale besturen in 2024 inzake informatieveiligheid door het Cyber Response Team

Samenvatting:

Naar aanleiding van o.a. de cyberaanval op stad Antwerpen heeft de Vlaamse Regering beslist op 13/01/2023 om een Cyber Response Team (CRT) voor lokale besturen op te richten. Het CRT is een kennisorganisatie dat kennis en expertise bundelt en lokale besturen ondersteunt bij cyberincidenten. De ondersteuning van het CRT is tweeledig:

- Preventieve ondersteuning
- Reactieve ondersteuning

Ondanks het huidige ondersteuningsaanbod blijken lokale besturen nog onvoldoende voorbereid op cyberincidenten. De huidige ondersteuning vanuit de Vlaamse overheid maken kwetsbaarheden bij lokale besturen inzichtelijk (bv. via ICT-veiligheidsaudits) en bieden de nodige houvast (bv. de toolkit cyberveiligheid), maar toch is er een duidelijke nood aan meer **proactieve ondersteuning**.

Omwille van het aanhoudende belang van informatieveiligheid voor lokale besturen, willen het Agentschap Binnenlands Bestuur en Digitaal Vlaanderen daarom inzetten op een meer hands-on begeleiding van steden en gemeenten in samenwerking met het Cyber Response Team. Er wordt voorgesteld om een aanvullende opdracht toe te kennen aan het Cyber Response Team, ter ondersteuning van lokale besturen. De opbracht behelst twee sporen:

- Begeleiding van lokale besturen bij het opmaken van een Business Continuïteitsplan
- Begeleiding van lokale besturen bij de implementatie van Vlaamse bouwstenen m.b.t. Toegangs- en Gebruikersbeheer

1. SITUERING

A. BELEIDSVELD/BELEIDSDOELSTELLING

BELEIDSDOMEIN: Kanselarij en Bestuur

B. VORIGE BESLISSINGEN EN ADVIEZEN

Door de toegenomen digitalisering lopen Vlaamse lokale besturen meer dan ooit het risico om slachtoffer te worden van cyberincidenten. De afgelopen jaren leerden ons dat het elke stad of gemeente kan overkomen. Voor de Vlaamse Regering is cyberveiligheid dan ook een topprioriteit.

Beleidsplan Cybersecurity

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.

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 te 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 vormingsinitiatieven 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.

Cyber Response Team voor lokale besturen (VR 2023 1301)

Naar aanleiding van o.a. de cyberaanval op de stad Antwerpen heeft de Vlaamse Regering beslist op 13/01/2023 om een Cyber Response Team (CRT) voor lokale besturen op te richten. Het CRT is een kennisorganisatie dat kennis en expertise bundelt en lokale besturen ondersteunt bij cyberincidenten.

2. INHOUD

A. NOODZAAK VAN AANVULLENDE ONDERSTEUNING DOOR HET CYBER RESPONSE TEAM

Naar aanleiding van o.a. de cyberaanval op de stad Antwerpen heeft de Vlaamse Regering beslist op 13/01/2023 om een Cyber Response Team (CRT) voor lokale besturen op te richten. Het CRT is een kennisorganisatie dat kennis en expertise bundelt en lokale besturen ondersteunt bij cyberincidenten. De ondersteuning van het CRT is tweeledig:

- **Preventieve ondersteuning**: Om nieuwe cyberincidenten te voorkomen, verzamelt het CRT alle beschikbare informatie en verwerkt de informatie in gerichte adviezen en kennisartikelen, die o.a. via ledenorganisaties worden verspreid. Verder capteert en beantwoordt het CRT vragen van lokale besturen.
- **Reactieve ondersteuning**: In het geval een cyberincident zich voordoet, ondersteunt het CRT lokale besturen bij het opstarten van een Cyber Response Plan, de coördinatie van activiteiten en communicatie. Verder ondersteunt het CRT bij het verzamelen van alle nodige informatie en informeren van Vlaamse en federale diensten zoals de Gegevensbeschermingsautoriteit (GBA).

Met de oprichting van het CRT hebben lokale besturen een centraal aanspreekpunt, waar ze terecht kunnen met al hun vragen. Ook wanneer lokale besturen getroffen zijn door een cyberaanval, staat het CRT klaar voor ondersteuning. Het CRT, dat op Vlaams niveau, wordt aangestuurd zorgt voor de nodige synergie en efficiënte inzet van middelen. Digitaal Vlaanderen en het Agentschap Binnenlands Bestuur bundelen de krachten en zetten hun expertise in om de lokale besturen optimaal te ondersteunen.

Echter, uit de resultaten van onder andere de ICT-veiligheidsaudits met cofinanciering en het traject ethisch hacken i.s.m. VVSG blijkt dat er steeds verschillende organisatorische en technische kwetsbaarheden zijn bij lokale besturen. Ondanks het huidige ondersteuningsaanbod blijken lokale besturen nog onvoldoende voorbereid op cyberincidenten. De huidige ondersteuning vanuit de Vlaamse overheid maken kwetsbaarheden bij lokale besturen inzichtelijk (bv. via ICT-veiligheidsaudits) en bieden de nodige houvast (bv. de toolkit cyberveiligheid), maar toch is er een duidelijke nood aan meer **proactieve ondersteuning**.

Omwille van het aanhoudende belang van informatieveiligheid voor lokale besturen, willen het Agentschap Binnenlands Bestuur en Digitaal Vlaanderen daarom inzetten op een meer hands-on begeleiding van steden en gemeenten in samenwerking met het Cyber Response Team. Hiervoor worden bestaande instrumenten, zoals de toolkit cyberveiligheid, zo veel als mogelijk hergebruikt. Omwille van het huidige takenpakket van het CRT en haar positie in het landschap, is het CRT de aangewezen partij om de verdere ondersteuning en begeleiding van lokale besturen op zich te nemen. Het CRT zal op die manier meer inzetten op netwerkontwikkeling en -verruiming, in samenwerking met bestaande partnerorganisaties zoals VVSG of V-ICT-OR. Hiermee beoogt ABB de zichtbaarheid van het CRT te verhogen en haar rol en positie in het landschap te consolideren.

Hiervoor worden, boven op de voorziene middelen voor de opstart en operationele werking van het CRT, bijkomende middelen voorzien.

B. AANVULLENDE OPDRACHT CYBER RESPONSE TEAM VOOR LOKALE BESTUREN

De aanvullende ondersteuning voor lokale besturen door het Cyber Response Team omvat twee sporen. Enerzijds worden lokale besturen begeleid om de nodige voorbereidingen te treffen om snel te kunnen reageren wanneer een cyberaanval zich voordoet, anderzijds wordt ingezet op de beveiliging van de digitale infrastructuur. Hieronder worden beide sporen meer in detail toegelicht.

Spoor 1: Begeleiding van lokale besturen bij het opmaken van een Business Continuïteitsplan

Wanneer een lokaal bestuur slachtoffer wordt van een cyberincident, heeft dit grote gevolgen voor de dienstverlening aan de burger. Naargelang de impact en reikwijdte van het incident, kan de dienstverlening van het lokaal bestuur gedurende enkele dagen tot weken in belangrijke mate worden onderbroken en/of verstoord. Een lokaal bestuur dat geconfronteerd wordt met een cyberincident moet daarom snel en gepast actie ondernemen om de situatie zo snel mogelijk onder controle te krijgen en terug te keren naar de reguliere werking. Het CRT ondersteunt hier reeds in, maar toch is het belangrijk dat al proactief is nagedacht over welke stappen genomen moeten worden bij het crisisbeheer bij grootschalige incidenten en dat lokale besturen beschikken over een kwalitatief business continuïteitsplan (BCP).

Uit de resultaten van de ICT-veiligheidsaudits en het traject ethisch hacken blijkt echter dat een bruikbaar BCP vaak nog ontbreekt bij lokale besturen. Een gedegen Business Continuity Management (BCM) wordt echter almaar belangrijker voor lokale besturen om de continuïteit van hun dienstverlening aan burgers te kunnen waarborgen. Deze nood wordt zichtbaar wanneer incidenten met betrekking tot informatieveiligheid de toegang tot of het vertrouwen in diensten onmogelijk maken. Daarom is het van cruciaal belang dat lokale besturen zich effectief voorbereiden, onder meer via het opstellen van een Business Continuity Plan (BCP).

In nauw overleg met het Agentschap Binnenlands Bestuur (ABB) zal het VO-CRT lokale besturen ondersteunen bij deze uitdaging. Het eerste spoor binnen de opdracht beoogt dan ook om lokale besturen verder te informeren, sensibiliseren en responsabiliseren en hen te begeleiden bij het opmaken van hun eigen continuïteitsplan met een mix van individuele en peer-to-peer begeleiding. Het doel van het eerste spoor is om via een reeks van workshops lokale besturen bij te staan in het opmaken van een BCP. Hiervoor wordt gebruik gemaakt van de reeds ontwikkelde instrumenten uit de toolkit cyberveiligheid.

In totaal krijgen 50 lokale besturen intensieve begeleiding bij het opmaken van een BCP. In 2024 worden twee golven georganiseerd, met telkens 25 lokale besturen. Voor iedere golf worden er vijf workshops georganiseerd. Elke workshop wordt dus tweemaal georganiseerd. Die workshops behandelen verschillende aspecten van het BCP. Eerst wordt toegelicht wat een BCP is, waarom het relevant is en hoe je ermee aan de slag gaat. Daarbij wordt aan de hand van een zelfevaluatie nagegaan waar het lokaal bestuur staat. Vervolgens wordt dieper ingegaan op de impact van een incident op de continuïteit in dienstverlening en worden kritieke processen geïdentificeerd, als voorbereiding van het BCP. Op basis van een grondige impactanalyse, krijgen de lokale besturen de nodige ondersteuning om de BCP's op te maken en te verankeren in de eigen organisatie. Tot slot wordt toegelicht hoe lokale besturen verder aan de slag kunnen gaan, om hun BCP zelf actueel te houden.

De workshops worden over een periode van 8 à 9 maanden gespreid, opdat deelnemende lokale besturen voldoende tijd hebben om de nodige informatie te verzamelen, contacten te leggen en de nodige voorbereidingen te treffen. Doorheen het proces worden experten ter beschikking gesteld om feedback te geven op tussentijdse resultaten en inzichten te capteren. Die inzichten en geleerde lessen worden vertaald in beleidsaanbevelingen.

De ondersteuning wordt 80% gefinancierd door de Vlaamse overheid. Lokale besturen zullen kunnen intekenen op dit aanbod, mits een formele engagementsverklaring waarbij ze zich ertoe verbinden de nodige personeelsinzet te voorzien om het volledige traject te doorlopen en op het einde van het traject een BCP te kunnen afleveren en mits een co-financiering van 20%.

De opdracht wordt als volgt opgezet:

Voorbereiding en plannen van de workshops

In een eerste fase worden de reeds bestaande BCM-gerelateerde informatie van het VO-CRT en de VVSG geconsulteerd (zoals bijv. de richtlijnen van het VVSG voor het opstellen van BCP's en de aangeboden templates). Daarnaast worden de lokale besturen geïdentificeerd met de nodige ervaring die later in de workshops kunnen worden betrokken als goede praktijk om geleerde lessen te delen. Tot slot wordt de aanpak zoals hieronder beschreven verfijnd en wordt de inhoud/voorbereiding van iedere workshop door ABB gevalideerd.

Workshop 1: Theoretisch kader BCM en zelfevaluatie

In de eerste workshop zal een antwoord worden geboden op volgende vragen:

- Wat is een BCP en waarom is het nodig? Waarom is het relevant en hoe wordt het beheerd (binnen een lokaal bestuur)?
- Waarom is een BCP relevant op vlak van informatieveiligheid?
- Welke referentiedocumenten bestaan er binnen de VO en in het algemeen?
- Waar staat mijn lokaal bestuur vandaag? Middels een zelfevaluatie aan de hand van '10 vragen'.

Daarnaast wordt de inleiding naar de volgende sessie gegeven, waar verder wordt toegelicht hoe een BCP tot stand komt.

Tussen workshop 1 en 2 wordt aan de deelnemers gevraagd om relevante informatie te verzamelen en door te nemen zowel met betrekking tot het algemeen kader als voor het eigen lokaal bestuur.

Workshop 2: Identificatie kritieke processen – Business Impact Analyse (BIA)

In de tweede workshop wordt dieper ingegaan op de impact van een incident op de continuïteit in dienstverlening en het identificeren van kritieke processen, als voorbereiding op het uitwerken van een BCP. Tijdens de workshops komen volgende vragen aan bod:

- Hoe bepaal je de kritieke processen? Wie betrek je in dergelijke oefening?
- Welke lessen kunnen we trekken uit eerdere trajecten bij lokale besturen?

Tijdens de workshop worden bruikbare sjablonen ter beschikking gesteld voor de effectieve uitwerking van een business impact analyse ter beschikking gesteld.

OPDRACHT: Na workshop 2 worden deelnemers gevraagd om hun eigen BIA te maken en door te sturen.

Workshop 3: Hoe maak ik mijn BCP?

In de derde workshop krijgen deelnemers algemene feedback die relevant is voor groep met betrekking tot de nazicht van de BIA's. Verder zal de workshop zich toespitsen op de opmaak van een BCP en komen volgende vragen aan bod:

- Welke 'strategische keuzes' moet ik maken?
- Welke bouwstenen heeft het BCP, gelinkt aan het instrumentarium van het VO-CRT?

- Wat moet zeker aan bod komen met informatieveiligheid in het achterhoofd?
- Hoe kan ik dienstverleners betrekken?

Tot slot worden tijdens deze workshop sjablonen ter beschikking gesteld voor de effectieve uitwerking van een BCP.

OPDRACHT: Na workshop 3 worden deelnemers gevraagd om hun eigen BCP op te maken en door te sturen naar het projectteam.

Workshop 4: Hoe ziet mijn BCP er uit en hoe veranker ik dit in de organisatie?

Tijdens de vierde workshop krijgen deelnemers algemene feedback die relevant is voor de groep met betrekking tot nazicht BCP's. Er wordt gefaciliteerde terugkoppeling geboden. De deelnemers krijgen de kans om over hun eigen ervaringen en uitdagingen/struikelblokken te spreken zodat ze instant feedback kunnen krijgen van de groep en van het CRT. De terugkoppeling wordt in specifieke thema's opgedeeld in functie van de resultaten van het nazicht van de BCP's.

Verder voorziet de workshop duidelijkheid rond de rollen en verantwoordelijkheden rond goedkeuring, onderhoud en verankering van BCP binnen het lokale bestuur. Tijdens deze workshop worden ook oefeningen gegeven rond de aanpak en periodiciteit van BCP's.
Tot slot voorziet de workshop experten die voor terugkoppeling zorgen bij vragen van de deelnemers met betrekking tot de BCP.

OPDRACHT: Na workshop 4 worden deelnemers gevraagd om een update van het eigen BCP door te sturen naar het projectteam.

Workshop 5: Geleerde lessen voor de toekomst en verdere verankering

Tijdens de laatste workshop krijgen deelnemers algemene feedback die relevant is voor de groep met betrekking tot de gecontroleerde BCP's. Experten worden ingezet om bij terugkoppeling vragen van deelnemers met betrekking tot BCP en mogelijke volgende stappen te beantwoorden. De workshop biedt een samenvatting van de geleerde lessen doorheen het hele traject. Daarbij wordt ook de feedback van de deelnemers over het traject gecapteerd en worden geleerde lessen gevalideerd. Daarbij wordt ruimte voorzien om aanbevelingen te doen voor toekomstige workshops.

Individuele feedback

Tussen verschillende workshops wordt feedback voorzien op de resultaten van tussentijdse opdrachten bij het opmaken van een BIA of BCP. Deelnemende lokale besturen kunnen hun resultaten bezorgen en krijgen feedback in de vorm van vragen of opmerkingen op de aangeleverde elementen. Waar nodig wordt mondeling verduidelijkt. Doorheen iedere golf worden drie individuele feedbackrondes voorzien.

Rapportering rond geleerde lessen

Het CRT rapporteert over de geleerde lessen doorheen het traject, met specifieke focus op het belang van informatieveiligheid en de verankering van BCM binnen de lokale besturen. De geleerde lessen worden vertaald in een tastbaar instrument voor lokale besturen om zelf, zonder begeleiding, mee aan de slag te gaan. Het instrument wordt ter beschikking gesteld via de kanalen van het Cyber Response Team.

Spoor 2: (Piloot-)begeleiding van lokale besturen bij de implementatie van Vlaamse bouwstenen m.b.t. Toegangs- en Gebruikersbeheer

Uit de resultaten van de ICT-veiligheidsaudits blijkt eveneens dat naast organisatorische maatregelen, ook verschillende technische beveiligingsmaatregelen nog onvoldoende worden voorzien, in het bijzonder met betrekking tot toegangs- en gebruikersbeheer. Slechts een beperkt aantal lokale besturen beschikt op dit moment over multifactor authenticatie (MFA). Lokale besturen hebben onvoldoende expertise om technische beveiligingsmaatregelen te implementeren of de reeds bestaande Vlaamse bouwstenen m.b.t. Toegangs- en Gebruikersbeheer (ACM/IDM) te integreren.

Daarom wordt binnen de opdracht een tweede (piloot) begeleidings- en leertraject opgestart om een aantal lokale besturen te ondersteunen bij de volledige implementatie of aankoppeling van Vlaamse veiligheidsbouwstenen inzake ACM/IDM. Het doel van dit spoor is tweeledig; (1) de effectieve integratie van Vlaamse bouwstenen realiseren bij lokale besturen en (2) meer inzicht krijgen in de lokale uitdagingen en noden van lokale besturen met betrekking tot implementatie van Vlaamse bouwstenen. Die inzichten moeten Digitaal Vlaanderen in staat stellen om bestaande oplossingen beter af te stemmen op de noden van lokale besturen en opschaling en brede implementatie te faciliteren.

Dit project moet worden gepercipieerd als een proefproject, op basis waarvan de dienstverlening van Digitaal Vlaanderen verder op punt kan gesteld worden voor lokale besturen. De voortschrijdende inzichten van dit proefproject kunnen vertaald worden in bijsturing van bestaande roadmap. Met dit proefproject wordt inzicht verkregen in volgende vragen: 'Met welke uitdagingen worden Lokale Besturen geconfronteerd? Met welke obstakels wordt men – naargelang maturiteitsniveau – op lokaal niveau geconfronteerd?'

Het CRT zal voor daarom een team analisten ter beschikking stellen om bij 30 lokale besturen de integratie van Vlaamse bouwstenen m.b.t. toegangsbeheer van A tot Z te ondersteunen. Daarbij worden alle noden en gebruikersvereisten maar ook obstakels gecapteerd. Deze vereisten kunnen zowel op operationeel als op technisch niveau situeren. Het CRT verzamelt voor elk lokaal bestuur in een gedetailleerd rapport, dat wordt voorgelegd aan de Toepassingseigenaar van het Toegangs- en Gebruikersbeheer van Digitaal Vlaanderen. Naast integratie zullen lokale besturen ook worden geïnformeerd over het organiseren van en het communiceren over veranderingen binnen de organisatie. Binnen het begeleidingsproject wordt daarom een cursus voorzien om vertrouwd te geraken met het gebruik van de veiligheidsbouwstenen.

Na afloop van het piloot begeleidingstraject wordt een evaluatie voorzien. Daar worden de impact van de begeleiding en individuele inzichten gebundeld en vertaald naar beleidsaanbevelingen. In een latere fase kan worden bekeken of een soortgelijke dienstverlening zinvol kan zijn bij het integreren van andere bouwstenen of het aansluiten op Cloudops voor lokale besturen.

De ondersteuning wordt 80% gefinancierd door de Vlaamse overheid. Er wordt een co-financiering van 20% gevraagd aan de geselecteerde lokale besturen. De selectie van de lokale besturen zal gebeuren op basis van vooraf bepaalde criteria. Daarbij gaat bijzondere aandacht naar de verschillende grootte, maturiteit en geografische spreiding van lokale besturen en de deelname aan eerdere ondersteuningsinitiatieven, zoals de ICT-veiligheidsaudits met cofinanciering of het traject ethisch hacken i.s.m. VVSG.

Introductie

Digitaal Vlaanderen engageert zich om middels een breed-gecommuniceerde infosessie het proefproject voor te stellen aan de Vlaamse Lokale Besturen. Deze sessie wordt opgenomen en nadien

gedeeld met de besturen die door omstandigheden niet present konden tekenen. Deze infosessie wordt georganiseerd door Veiligheidsbouwstenen in samenwerking en nauwe afstemming met het Cyber Response Team van Digitaal Vlaanderen.

Gedurende een grace period van een aantal weken krijgen de lokale besturen de kans om in te tekenen op het proefproject. Agentschap Binnenlands Bestuur benoemt op basis van de input begrepen in deze nota, het aantal besturen dat deel kan nemen aan het project. Indien dit aantal overschreden wordt – i.e. indien meer dan het voorziene aantal lokale besturen wenst deel te nemen – zal in samenspraak met de stuurgroep van het CRT een selectie worden gemaakt. Indien dit aantal niet gehaald wordt, zal middels een tweede infosessie opnieuw uitgereikt worden naar de Vlaamse Lokale Besturen.

Intake

De 30 Lokale Besturen worden verdeeld in 5 groepen van telkens 6 besturen op basis van geografische nabijheid (gouwen / provincies). In onderling overleg wordt er een locatie bepaald waar de intake met de besturen die deel uitmaken van dezelfde groep, zal plaatsvinden.

Een vliegende ploeg van Digitaal Vlaanderen begeeft zich naar deze locatie. Aldaar geeft de ploeg een uitgebreide presentatie omtrent het Veiligheidsbouwstenen-aanbod van Digitaal Vlaanderen. De klemtoon kan daarbij op verzoek gelegd worden op het Toegangs- en Gebruikersbeheer.

Deze vliegende ploeg zal bestaan uit twee analisten die zich doorheen het traject beschikbaar maken voor advies en ondersteuning, en zich flexibel ter beschikking stellen voor vergaderingen – virtueel of op locatie.

Integratiedossier

Het integratiedossier vormt de ruggengraat van een integratietraject. Hierin worden alle noodzakelijke gegevens gecapteerd om een succesvolle integratie met het Toegangs- en Gebruiksbeheer op te zetten, zoals doelpubliek van de applicatie, detail omtrent het integratie-protocol, detail omtrent het rechtenmodel.
Het integratiedossier wordt op locatie aangevuld door de analisten, in samenspraak met de contacten van het lokaal bestuur.

Ondersteuning tijdens het integratietraject

De vliegende ploeg gaat actief ondersteunen bij het opzetten van de integratie. Indien er een gebrek aan protocol-specifieke kennis aanwezig is langs de kant van het bestuur, treedt de vliegende ploeg bij – alsook als er vragen zijn bij de bouwstenen zelf. Concreet zal de vliegende ploeg tijdens de testfase samen met het bestuur een geijkt testplan doorlopen, en handvaten aanreiken om onsuccesvolle testen en problemen het hoofd te bieden.

De 'hands on'-begeleiding wordt, binnen dit project, bovenop de standaarddienstverlening van Digitaal Vlaanderen aangeboden. Onder deze 'hands on'-begeleiding valt protocol-specifieke ondersteuning bij het opmaken van de SAML-metadata, het opmaken van OIDC of OAuth-requests en het opzetten van de federatie. Alsook de mapping naar rechten-en rollenmodellen op maat en troubleshooting-sessie(s). Tot slot behoren ook test-sessies tot de scope van de ondersteuning tijdens het integratieproces.

Ondersteuning na het integratietraject

De vliegende ploeg voorziet, na een succesvol integratietraject, desgewenst in de nodige monitoring en rapporteringsfunctionaliteit in het Gebruikersbeheer- en/of het Beheersportaal van het Toegangsbeheer.

Indien er volgend op een succesvol integratietraject door het bestuur gesignaleerd wordt dat één of meerdere bulk-upload of default entitlement scanners dienen ingeregeld te worden in het Gebruiksbeheer, zal de vliegende ploeg daarvoor de administratie en planning voor haar rekening nemen.

De vliegende ploeg zal, eenmaal de integratie met succes in productie gesteld is, tezamen met het participerende bestuur een evaluatie maken van het verloop en de resultaten van het traject, alsook van de tevredenheid ten aanzien van de aangeboden ondersteuning en de gretigheid om in de toekomst in een gelijkaardige context andere toepassingen te integreren met de Veiligheidsbouwstenen.

Bovenop de gerichte ondersteuning tijdens en na de integratietrajecten, zal de vliegende ploeg ook op volgende niveaus ageren en ondersteunen.

Cursus Toegangs- en Gebruikersbeheer

De vliegende ploeg kan de besturen die deel uitmaken van eenzelfde groep (cf. supra) desgewenst een cursus Toegangs- en Gebruikersbeheer geven. Met de cursus moeten lokale besturen vertrouwd geraken met het eigenlijke gebruik van de veiligheidsbouwstenen. Een dergelijke begeleiding kan ook ingeregeld worden richting de gebruikers van de toepassingen van deze lokale besturen.

Actief opmeten van de vragen, obstakels en feature request er leven bij de lokale besturen

De vliegende ploeg verzamelt actief vragen, obstakels en feature request die leven bij de lokale besturen die deelnemen aan het project. Deze vereisten kunnen zowel op operationeel als op technisch niveau situeren. De vliegende ploeg verzamelt deze vragen en vereisten voor elk lokaal bestuur in een gedetailleerd rapport. Dit rapport wordt voorgelegd aan de Toepassingseigenaar van het Toegangs- en Gebruikersbeheer.

Rapport en feedback

De Toepassingseigenaar bespreekt het rapport en de daaraan gekoppelde feedback en eventuele beleidsmaatregelen rechtsreeks met het lokaal bestuur.

3. BESTUURLIJKE IMPACT

A. BUDGETTAIRE IMPACT VOOR DE VLAAMSE OVERHEID

Voor de aanvullende ondersteuning door het Cyber Response Team in 2023-2024 is een budget voorzien van in totaal 640.000 EUR op het krediet bestemd voor ondersteuning naar duurzame en creatieve steden en in de begroting ingeschreven op het artikel SJ0-1SMC2HA-WT.

Onderstaande tabel betreft de indicatieve verdeling van het budget en de kosten door Digitaal Vlaanderen op basis van de vereisten die werden weergegeven in deze nota. De verdeling kan tijdens

de duur van de samenwerkingsovereenkomst worden bijgestuurd op aangeven van de stuurgroep van het Cyber Response Team.

Activiteit	2023
Spoor 1: Begeleiding van lokale besturen bij het opmaken van een Business Continuïteitsplan	300.000€
Spoor 2: (Piloot-)begeleiding van lokale besturen bij de implementatie van Vlaamse bouwstenen m.b.t. Toegangs- en Gebruikersbeheer	340.000€
Totaal	640.000€

Voor het uitwerken van spoor 1: begeleiding van lokale besturen bij het opmaken van een Business Continuïteitsplan', kan externe ondersteuning worden besteld op het raamcontract met referentie 2019/HFB/52630. Volgende prijszetting wordt gehanteerd.

	Prijs/dag (excl. BTW)	Prijs/dag (incl. BTW)
Profiel A	€746,02	€902,68
Profiel B	€882,69	€1.068,05
Profiel C	€1.127,57	€1.364,36
Profiel D	€2.847,39	€3.445,34

Voor het uitwerken van spoor 2: (Piloot-)begeleiding van lokale besturen bij de implementatie van Vlaamse bouwstenen m.b.t. toegangsbeheer (ACM/IDM), kan externe ondersteuning worden besteld op het raamcontract met referentie 2020/HFB/MPMO/63249.

De vliegende ploeg zal bestaan uit twee profielen:

- 1 medium-level business analist / project manager. Dit profiel is bezwaard met de ondersteuning, begeleiding en rapportering op het niveau van elke groep van lokale besturen. Per groep van lokale besturen worden 10 mandagen voorzien. De 30 deelnemende besturen worden verdeeld in 5 groepen van telkens 6 besturen op basis van geografische nabijheid.
- 1 medium-level functioneel analist. Dit profiel is bezwaard met de ondersteuning, begeleiding en rapportering op het niveau van elke individuele integratie. Per lokaal bestuur worden 10 mandagen voorzien. In totaal zullen 30 lokale besturen kunnen deelnemen aan het project.

Volgende prijszetting wordt gehanteerd.

	Prijs/dag (excl. BTW)	Prijs/dag (incl. BTW)
Medium-level Business analist project manager	€ 792,00	€958,32
Medium-level functioneel analist	€795,52	€962,57

Digitaal Vlaanderen en het EV DV worden aangemerkt als niet-belastingplichtige publiekrechtelijke lichamen in de zin van artikel 6, eerste lid, van het BTW-wetboek en zijn bijgevolg niet onderworpen aan de BTW.

Het advies van de Inspectie van Financiën werd op 1/12/2023 verleend.
In haar gunstig advies heeft de Inspectie van financiën een aantal bemerkingen geformuleerd welke hieronder worden toegelicht:

- *De criteria voor de oproep moet op voorhand bekend gemaakt worden.*

  De stuurgroep van het Cyber Response Team, met vertegenwoordiging van o.a. het Agentschap Binnenlands Bestuur en Digitaal Vlaanderen, houdt rekening met de opmerking van de IF bij de verdere uitwerking van beide sporen.

- *De bestelling inclusief offertes moet nog worden voorgelegd in het kader van de administratieve begrotingscontrole. De vastlegging kan pas nadat offertes zijn ontvangen.*

  De opmerking van de IF zijn bezorgd aan Digitaal Vlaanderen, die instaat voor de uitvoering van de bovenvermelde opdracht. Digitaal Vlaanderen zal dit verder opvolgen en ziet toe op de correcte naleving van de procedure. Het advies van de Inspectie van financiën zal eveneens als bijlage worden toegevoegd aan de voorziene samenwerkingsovereenkomst en maakt daarmee integraal deel uit van de opdracht van het Cyber Response Team.

- *Voor spoor 1 moet het budget verder worden uitgewerkt, zodat duidelijk is welke middelen zullen worden besteed aan de verschillende sporen. Per spoor kan eveneens de budgettaire impact transparanter worden weergegeven in de nota aan de Vlaamse regering i.p.v. enkel in de samenwerkingsovereenkomst als bijlage.*

  De detailbeschrijving, zoals initieel voorzien in de samenwerkingsovereenkomst, is integraal opgenomen onder '2. INHOUD' van de nota aan de Vlaamse regering. Op die manier wordt per spoor een uitgebreide beschrijving van de geplande activiteiten voorzien. Onder '3. BESTUURLIJKE IMPACT' is eveneens een meer gedetailleerde beschrijving voorzien van de vliegende ploeg en de verwachte effort per profiel.

- *Voor beide sporen adviseert de IF eveneens een bedrag aan te rekenen aan de lokale besturen gelet op het direct voordeel dat de lokale besturen hebben waarbij voor het eerste spoor lokale besturen die hebben nagelaten hun organisatiebeheersing voldoende uit te werken nu worden beloond ook voor aspecten die ruimer zijn dan ICT gerelateerde elementen.*

  De stuurgroep van het Cyber Response Team houdt rekening met het advies van de IF bij de verdere uitwerking van beide sporen.

De Vlaamse minister, bevoegd voor het budgettair beleid, heeft zijn akkoord gegeven op 18/12/2023, mits rekening wordt gehouden met:

- *Een co-financiering van minstens 20% ten laste van de deelnemende lokale besturen zowel in spoor 1 als spoor 2.*

  De ondersteuning wordt 80% gefinancierd door de Vlaamse overheid. Er wordt een co-financiering van 20% gevraagd aan de geselecteerde lokale besturen in een niet-geïnstitutionaliseerd horizontale samenwerking met de opmaak van een BCP als voorwerp. De selectie van de lokale besturen zal gebeuren op basis van vooraf bepaalde criteria. Daarbij gaat bijzondere aandacht naar de verschillende maturiteit, geografische spreiding en grootte van lokale besturen en de deelname aan eerdere ondersteuningsinitiatieven, zoals de ICT-veiligheidsaudits met cofinanciering of het traject ethisch hacken i.s.m. VVSG. De vorderingen met betrekking tot de horizontale samenwerking zal verlopen via het Fonds voor interbestuurlijke digitalisering lokale overheden en worden in het beheer van ABB opgesteld. Concrete afspraken rond dit ondersteuningsaanbod worden vastgelegd in een samenwerkingsovereenkomst, ondertekend door ABB, Digitaal Vlaanderen en het lokaal bestuur.

- *Het op voorhand bekend maken van de criteria voor de oproep/selectie van de lokale besturen*

  Lokale besturen die wensen deel te nemen aan dit traject zullen een aanvraag moeten indienen waarin hun maturiteit en visie rond cyberveiligheid wordt duidelijk gemaakt. In eerste instantie wordt een objectieve en kwalitatieve selectie gemaakt op deze visie en argumentatie van de maturiteit. Daarna worden deelnemers geselecteerd op basis van geografische spreiding, grootte en eerdere deelname aan andere ondersteuningsinitiatieven.

  Om een objectieve selectie te kunnen maken wordt eerst gekeken naar de maturiteit van de kandidaat. Het is belangrijk dat een lokaal bestuur alvorens de deelname aan het traject blijk geeft van een goede voorbereiding en motivatie. In hun aanvraag moeten als eerste de interne processen in kaart worden gebracht. De voorkeur zal hierbij gaan naar lokale besturen die de processen reeds (gedeeltelijk) in kaart hebben gebracht. Lokale besturen die deze beschrijving niet hebben, worden bij voorkeur niet meegenomen in het traject. Als tweede wordt gekeken naar de mate waarin het lokaal bestuur risicoanalyses uitvoert. Alvorens deel te nemen aan dit traject, is het belangrijk dat het lokaal bestuur zijn risico's heeft geïdentificeerd en geëvalueerd. Daarnaast zal het lokaal bestuur in zijn aanvraag ook moeten concretiseren binnen welke dienst het traject zal worden opgevolgd en wie de verantwoordelijkheid zal dragen tijdens dit begeleidingstraject. Ook de aanduiding van (meerdere) SPOC's is gewenst.

  In tweede instantie is het belangrijk om representatief te zijn en de lokale besturen zo goed mogelijk te vertegenwoordigen tijdens dit traject. Daarom zal in de tweede selectieronde, indien van toepassing door voldoende aanvragen, worden gekeken naar de geografische spreiding en de grootte van het lokaal bestuur.

  Indien van toepassing, wordt een derde selectie gemaakt op basis van eerdere deelname aan ander ondersteuningsaanbod vanuit Vlaanderen. Om lokale besturen die nog niet hebben deelgenomen aan bijvoorbeeld de co-financiering van ICT-audits of het traject ethisch hacken ook de kans te geven om te werken aan hun cyberveiligheid, wordt aan hen voorrang verleend.

- *Het voorleggen aan de Inspectie van Financiën van de bestellingen inclusief offertes in het kader van de administratieve en begrotingscontrole, en de vastlegging pas gebeurt nadat offertes werden ontvangen*.

  De opmerking van de IF zijn bezorgd aan Digitaal Vlaanderen, die instaat voor de uitvoering van de bovenvermelde opdracht. Digitaal Vlaanderen zal dit verder opvolgen en ziet toe op de correcte naleving van de procedure. Het advies van de Inspectie van financiën zal eveneens als bijlage worden toegevoegd aan de voorziene samenwerkingsovereenkomst en maakt daarmee integraal deel uit van de opdracht van het Cyber Response Team.

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. VERDER TRAJECT

5. VOORSTEL VAN BESLISSING

De Vlaamse regering beslist:

1. Haar goedkeuring te hechten aan de aanvullende ondersteuning voor lokale besturen door het Cyber Response Team en bijhorende eenmalige middelen voor de uitvoeringsperiode 2023-2024;

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

JAN JAMBON

De viceminister-president van de Vlaamse Regering en
Vlaamse minister van Binnenlands Bestuur, Bestuurszaken, Inburgering en Gelijke Kansen,

GWENDOLYN RUTTEN