Cybercase

Lokaal Digitaal traject

Webinar VVSG

12/06/2023

Onze opdracht

1. Toelichting Lokaal Digitaal

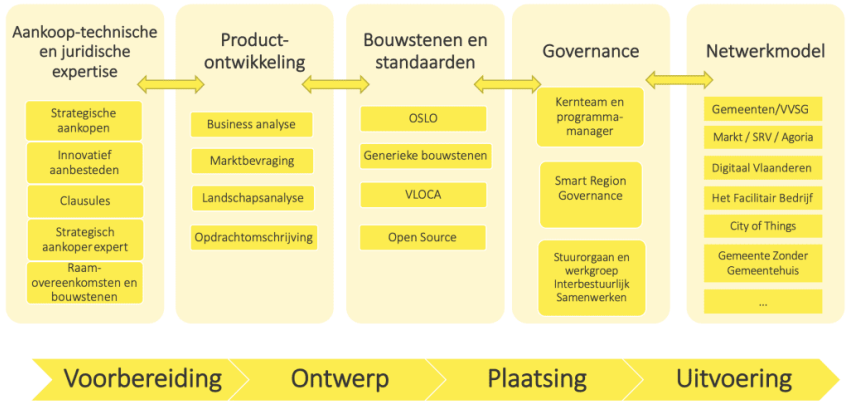
WAT

Het Lokaal Digitaal programma werd vanuit de **Smart Region Office** (SRO) in het leven geroepen met het oog op het **realiseren van concrete digitale oplossingen** die voor een **zo groot mogelijk aantal lokale besturen** het verschil maken door een **vraaggestuurd ondersteuningsaanbod** in het leven te roepen.

HOE

- **1ste luik**: **Opschaling** van een aantal **digitaliseringsprojecten** gericht op alle Vlaamse lokale besturen.
- **2de luik**: Organiseren van een **nieuwe organisatiestructuur** die de lokale besturen collectief kan ondersteunen in hun digitale transformatie.

De fundamenten van Lokaal Digitaal (fase 1)



WIE

- Het **Smart Region Office** coördineert alle initiatieven, standaarden en goede praktijken in samenwerking met Vlaamse entiteiten, lokale besturen, kennisinstellingen en bedrijven.
- Het programma Lokaal Digitaal wordt geleid door **programmamanager Simon Vander Elst** (Agentschap Digitaal Vlaanderen).
- **Digitaal Vlaanderen** voert het programma uit in nauwe samenwerking met de **Smart Region Office** (SRO), **Het Facilitair Bedrijf** en de **VVSG** onder het **Stuurorgaan Vlaams ICT en informatiebeleid** en binnen de **Smart Region Board** (SRB).

2. Context van deze opdracht

Context

Huidige situatie bij lokale besturen

- Lokale besturen vormen het **eerste aanspreekpunt** voor burgers, waardoor zij voortdurend in aanraking komen met **persoonsgevoelige data,** opgeslagen in een **diversiteit** aan **applicaties** en **toepassingen**
- Er zijn ruime **maturiteitswinsten** te boeken inzake **Cyberveiligheid** bij lokale besturen (cfr. audits & analyses van o.a. VVSG, CCB & V-ICT-OR)

Uitdagingen voor lokale besturen

- **Struikelblokken** zoals verouderde technologieën, versnelde digitale transformatie, verhoogde mobiliteit van data, gebrek aan controle op toeleveranciers, ...
- **Onbeheerste risico's** (cfr. audits) zoals bv. beveiligingssoftware, versleuteling, netwerksegmentatie, testen en opsporen van kwetsbaarheden van de IT-omgeving, voorzien van basiscontinuïteit, ...

Opdracht

1. Inzetten op een **gemeenschappelijk traject** dat moet resulteren in een **maturiteitsgroei inzake cyberveiligheid op lokaal niveau;**

2. **Onderzoeken van een gemeenschappelijk en eenvoudig afneembaar aanbod aan één of meerdere cybertools & diensten** (gebundeld in een **'catalogus**'), dat steden en gemeenten moet toelaten om **risico's maximaal te beheersen** en **kwetsbaarheden** zoveel mogelijk te **neutraliseren**.

3. Plan van aanpak - Overzicht

Deze indicatieve planning wordt doorheen de looptijd van het project en in functie van de beschikbaarheden van de verschillende stakeholders continu opgevolgd en waar nodig aangepast.

	15/mei	22/mei	29/mei	5/jun	12/jun	19/jun	26/jun	3/jul	10/jul	17/jul	24/jul	31/jul	7/aug	14/aug	21/aug	…
1. Projectopstart																
1.1 Kick-off vergadering	☆															
1.2 Projectlancering				☆												
2. Behoefteanalyse																
2.1. Stakeholderanalyse					☆											
2.2. Stakeholderbevraging						☆☆										
2.3. Opmaak overzicht toekomstige requirements							☆									
2.4 Analyse van bestaande landschap								☆								
2.5 Inschatting Vlaamsbrede behoefte									☆							
2.6. Tussentijdse rapportage richting de stuurgroep										☆						
2.7. Stuurgroep										☆☆						
3. Marktverkenning (optioneel)																
3.1. Opmaken informatiebundel																
3.2. Uitwerken plan van aanpak													☆			
3.3. Uitwerken besluitvormingskader																
3.4. Finale rapportage richting de stuurgroep														☆		
3.5. Stuurgroep														☆	☆	
3.6. Open marktconsultatie - verdere begeleiding																…

Legende

- ☆ Kick-off vergadering
- ☆ Projectlancering
- ☆ Interviews
- ☆ Werksessie/focusgroep
- ☆ Tussentijds/finaal rapport
- ☆ Survey
- ☆ Terugkoppeling
- ☆ Stuurgroepvergadering

3. Plan van aanpak

1. Projectopstart | **2. Behoefteanalyse** | 3. Marktverkenning

Doelstelling van deze fase

- Zicht krijgen op de **huidige toestand** bij lokale besturen en hun **verwachtingen en noden** in kaart brengen
- Opmaken **overzicht technische en functionele requirements** en een Security product- en dienstencatalogus

Uit te voeren werkzaamheden

Stap 2.1. Stakeholderanalyse: Identificatie van de te betrekken key stakeholders via werksessie van 2 – 3 uur met lokale besturen.

Stap 2.2. Stakeholderbevraging: Inzicht verkrijgen in de huidige toestand inzake cyber security en mogelijke conceptuele architectuur van de oplossing, rekening houdend met de eventuele variatie tussen gemeenten, d.m.v.:

- Individuele interviews
- Bredere focusgroepen (met o.a. politie & brandweer)

Stap 2.3. Opmaak overzicht toekomstige requirements: Opmaak eerste geprioriteerd overzicht van technische en functionele requirements

Stap 2.4. Analyse van bestaande landschap: High-level screening van de verschillende bestaande security oplossingen en diensten

Stap 2.5. Inschatting van de Vlaamsbrede behoefte:

- (Max) 8 bijkomende interviews
- Vlaamsbrede behoefte in kaart te brengen

Verwacht resultaat

- Inzicht in bestaande en cruciale processen & ICT-toepassingen rond cyber security bij lokale besturen en hun verwachtingen en noden
- Gevalideerd overzicht van de technische en functionele requirements
- Gevalideerde Security product- en dienstencatalogus

KPMG

3. Plan van aanpak

Zoom-in: stakeholderbevraging via interviews

2. Behoefteanalyse
2.1. Stakeholderanalyse
2.2. Stakeholderbevraging
2.3. Opmaak overzicht toekomstige requirements
2.4 Analyse van bestaande landschap
2.5 Inschatting Vlaamsbrede behoefte
2.6. Tussentijdse rapportage richting de stuurgroep
2.7. Stuurgroep

Doel

- In kaart brengen van de **actuele stand** van zaken inzake cyber security
- In kaart brengen van **de toekomstige gebruikerseisen** voor het aanbod van diensten, tools en oplossingen

Wat & hoe

- Interviews van **2-3 uur** gemeente / stad met een **IT-profiel**
- Initiële bevraging van **behoeften & noden**

Vragen

- Huidige stand van zaken:
  - Al dan niet aanwezigheid van bestaande tools & applicaties, aangeboden door huidige dienstverlener
  - Huidige governance van de eigen IT-organisatie
- Toekomstige noden:
  - Belangrijkste technische & functionele vereisten
  - Prioritaire noden m.b.t. services & solutions

3. Plan van aanpak

Zoom-in: stakeholderbevraging via focusgroepen

2. Behoefteanalyse
2.1. Stakeholderanalyse
2.2. Stakeholderbevraging
2.3. Opmaak overzicht toekomstige requirements
2.4 Analyse van bestaande landschap
2.5 Inschatting Vlaamsbrede behoefte
2.6. Tussentijdse rapportage richting de stuurgroep
2.7. Stuurgroep

Doel

- In kaart brengen van de **actuele stand** van zaken inzake cyber security
- In kaart brengen van **de toekomstige gebruikerseisen** voor het aanbod van diensten, tools en oplossingen

Wat & hoe

- Bredere focusgroepen van **2-3 uur** met **interne diensten**, betrokken **politie- en evt. brandweerzones**, …
- Komen tot **prioritering** van de **belangrijkste behoeften & noden**

Vragen

- Huidige stand van zaken:
  - Al dan niet aanwezigheid van bestaande tools & applicaties, aangeboden door huidige dienstverlener
  - Huidige governance van de eigen IT-organisatie
- Toekomstige noden:
  - Belangrijkste technische & functionele vereisten
  - Prioritaire noden m.b.t. services & solutions

3. Plan van aanpak

Doelstelling van deze fase

- Uitgewerkt plan van aanpak voor de marktconsultatie
- Opmaken van een besluitvormingskader

Uit te voeren werkzaamheden

Stap 3.1. Opstellen product- en dienstencatalogus: Opmaken informatiebundel om potentiele leveranciers te bevrage.

Stap 3.2. Uitwerken plan van aanpak: Opmaken maatgericht plan van aanpak voor de marktconsultatie.

Stap 3.3. Uitwerken besluitvormingskader: Uitwerken van een besluitvormingskader ter facilitering keuzeproces en selectie gunningscriteria.

Verwacht resultaat

- Gevalideerd plan van aanpak voor de marktconsultatie
- Gevalideerd besluitvormingskader

3. Plan van aanpak

Security Operations

End-to-end toezicht op incidenten en kwetsbaarheden

Vulnerability Management	Security Monitoring	Security incident Response	Business Context	Threat Management
• Beoordeling van de technische kwetsbaarheid • Herstel van de technische kwetsbaarheid • Toezicht op naleving van het beleid	• Incident detectie • Triage en onderzoek van incidenten	• Coördinatie van de reactie op incidenten • Reactie op incidenten	• Content management • Bedrijfs-operationele context • Bedrijfs-technologische context	• Dreigings-informatie • Opsporen van bedreigingen • Trendanalyse • Monitoren van merksentiment

Beveiligingsrapportering

Rapportering over risico's en de opvolging
Beheer van informatieverzoeken

4. Timing

	15/mei	22/mei	29/mei	5/jun	12/jun	19/jun	26/jun	3/jul	10/jul	17/jul	24/jul	31/jul	7/aug	14/aug	21/aug	…
2. Behoefteanalyse																
2.1. Stakeholderanalyse																
2.2. Stakeholderbevraging																
2.3. Opmaak overzicht toekomstige requirements																
2.4 Analyse van bestaande landschap																
2.5 Inschatting Vlaamsbrede behoefte																
2.6. Tussentijdse rapportage richting de stuurgroep																
2.7. Stuurgroep																

Interactiemomenten	Beoogde deelnemende belanghebbenden	Verwachte tijdsinspanning belanghebbenden (indicatief)
2.1. Stakeholderanalyse - Werksessie	• Deelnemende lokale besturen • Vertegenwoordiging politie, brandweer, ...	• 2u
2.2. Stakeholderbevraging - Individuele interviews	• Deelnemende lokale besturen (IT-profielen)	• 2u
2.2. Stakeholderbevraging - Focusgroepen	• Deelnemende lokale besturen, incl. betrokken interne diensten, politiezones, brandweer, ...	• 3u
2.3. Opmaak overzicht toekomstige requirements – Werksessie	• Deelnemende lokale besturen, incl. betrokken politiezones, brandweer, ...	• 2u
2.5. Analyse bestaande landschap – brede bevraging	• Overige Vlaamse lokale besturen	• 30 minuten
2.7. Klankbordgroep	• Programmamanager LD • Leden KBG	• Doornemen van het tussentijds/eindrapport (2u) • Deelname vergadering (2u)
Terugkoppeling na klankbordgroep	• Programmamanager LD • Leden KBG	• Deelname vergadering (1u)

kpmg.com/socialmedia

Document Classification: KPMG Public