Project Cyberveilige Gemeenten

Draaiboek crisisoefening cybercrime

vvsg

Draaiboek crisisoefening cybercrime

Datum	November 2023
Status	Versie november 2023
Opdrachtgever	VVSG
Auteurs	David Matthys (Hulpverleningszone Meetjesland), Desender Jens (Gemeente Evergem), Monballyu Sarah (Gemeente Evergem), Rik Geerts (C-smart), Thaïs De Vuyst (VVSG), Charlotte De Mullier (VVSG) en Jolien Schoonooghe (VVSG)
Review	Bert De Rycke (Gemeente Wielsbeke), Tijl Demeulemeester (Stad Oudenaarde), Eve Heremans (Gemeente Nijlen), Kenny Gribbe (Stad Dendermonde)

Inleiding

Welkom bij het draaiboek crisisoefening cybercrime voor lokale besturen. Dit draaiboek kadert binnen **het project Cyberveilige Gemeenten**, een samenwerking tussen de VVSG, het kabinet van Vlaams minister van Binnenlands Bestuur, Bestuurszaken, Inburgering en Gelijke Kansen, Agentschap Binnenlands Bestuur, Audit Vlaanderen en Digitaal Vlaanderen, om lokale besturen te **ondersteunen bij het organiseren van een crisisoefening op het gebied van cyberveiligheid**. Dit document biedt een overzicht aan materialen en informatie waarmee lokale besturen zelfstandig aan de slag kunnen gaan om de cyberveiligheidsbekwaamheid van hun organisatie te versterken.

Dit draaiboek beoogt flexibiliteit en aanpasbaarheid. Er zijn twee verschillende scenario's, elk met een andere moeilijkheidsgraad, om de oefening af te stemmen op de specifieke behoeften en capaciteiten van een lokaal bestuur. Dit draaiboek biedt de nodige hulpmiddelen om in elk lokaal bestuur een crisisoefening cybercrime succesvol te organiseren.

Een succesvolle crisisoefening vereist **de betrokkenheid van verschillende belanghebbenden binnen het lokaal bestuur**. Het draaiboek biedt gedetailleerde informatie over de rollen en verantwoordelijkheden van de verschillende sleutelfiguren.

Dit draaiboek helpt een lokaal bestuur om een geslaagde crisisoefening cybercrime te organiseren en de interne organisatie beter **voor te bereiden op de uitdagingen van cyberdreigingen**. Maak gebruik van de materialen en informatie in dit draaiboek en deel **ervaringen en inzichten te delen** met andere lokale besturen.

Combineer de oefening met de opmaak of het gebruik van een Business Continuity Plan (BCP).

Heb je **vragen, opmerkingen of suggesties** over dit draaiboek? Stuur ze naar **cyberveiligheid@vvsg.be**

Meer informatie over het project Cyberveilige Gemeenten kan je vinden op **de projectpagina cyberveiligheid**.

Inhoud

1. Over het project Cyberveilige Gemeenten

1. Over het project Cyberveilige Gemeenten

Het project Cyberveilige Gemeenten is een samenwerking tussen de VVSG en het kabinet van Vlaams minister van Binnenlands Bestuur, Bestuurszaken, Inburgering en Gelijke Kansen, Agentschap Binnenlands Bestuur, Audit Vlaanderen en Digitaal Vlaanderen. Het project is een initiatief met als ambitie **de cyberveiligheid van lokale besturen in Vlaanderen te versterken**.

Met de steeds toenemende cyberdreigingen is het van essentieel belang dat steden en gemeenten zich bewust zijn van de risico's en de nodige maatregelen nemen om zich te beschermen tegen cyberaanvallen.

Het project Cyberveilige Gemeenten biedt lokale besturen **ondersteuning** bij het implementeren van effectieve cyberveiligheidsmaatregelen. Het omvat een uitgebreid aanbod aan acties, waaronder **een toolkit cyberveiligheid**, **een samenwerking met ethische hackers van Howest** en **inspirerende webinars en infosessies**. Lokale besturen worden zo bewust van de risico's, ontwikkelen een cyberveiligheidsstrategie en kunnen beroep doen op de nodige tools en kennis om cyberaanvallen te voorkomen, te detecteren en te beheersen.

Het project moedigt ook de **samenwerking en kennisuitwisseling aan tussen lokale besturen**, zodat zij van elkaars ervaringen kunnen leren en gezamenlijk sterker staan in de strijd tegen cybercriminaliteit. Door middel van verschillende werkgroepen kunnen lokale besturen elkaar ondersteunen en expertise opbouwen op het gebied van cyberveiligheid.

Het project Cyberveilige Gemeenten benadrukt het belang van een integrale aanpak van cyberveiligheid, waarbij niet alleen **technische maatregelen** worden genomen, maar ook aandacht wordt besteed aan **bewustwording, training van medewerkers en het opstellen van beleidsrichtlijnen**. De doelstelling is om lokale besturen veerkrachtig en weerbaar te maken tegen de voortdurend evoluerende cyberdreigingen.

Meer informatie over het project Cyberveilige Gemeenten vind je op de projectpagina cyberveiligheid.

2. Waarom een crisisoefening cybercrime organiseren?

2. Waarom een crisisoefening cybercrime organiseren?

Het organiseren van een crisisoefening cybercrime binnen jouw lokaal bestuur is van cruciaal belang in de moderne digitale wereld waarin we leven. Hieronder sommen wij enkele redenen op waarom lokale besturen een dergelijke oefening moeten organiseren:

Betrek de noodplanningscoördinator en/of preventieadviseur en neem de oefening op in de jaarlijkse planning, net zoals de noodplanningsoefening, brandoefening of andere standaard oefeningen.

- **Bewustwording**

Een lokaal bestuur wordt zich na de crisisoefening bewust van de reële dreigingen en risico's waarmee het geconfronteerd kan worden op het gebied van cyberveiligheid. Het biedt een realistische omgeving om te begrijpen hoe cyberaanvallen kunnen plaatsvinden en welke impact ze kunnen hebben op de dagelijkse werking.

- **Voorbereiding**

Een crisisoefening betekent een verbetering van responsplannen en testen van procedures. De oefening identificeert kwetsbaarheden in de bestaande processen, waardoor een lokaal bestuur proactief maatregelen kan nemen om zich beter voor te bereiden op toekomstige cyberincidenten. Door de crisisoefening wordt een lokaal bestuur getraind om snel en effectief te reageren in geval van een cyberaanval.

2. Waarom een crisisoefening cybercrime organiseren?

- **Samenwerking**

Een crisisoefening brengt profielen samen en bevordert de samenwerking tussen verschillende diensten. De uitvoering creëert een gelegenheid voor multidisciplinaire samenwerking en communicatie, zodat medewerkers leren hoe ze efficiënt kunnen samenwerken in een crisissituatie. De oefening beoordeelt ook de samenwerking met externe partners, zoals leveranciers, op vlak van veerkracht en responsmogelijkheden..

- **Risicobeheersing**

Door regelmatig een crisisoefening cyberveiligheid te organiseren, evalueert en verbetert een lokaal bestuur de risicobeheersingsmaatregelen. Ze neemt proactieve maatregelen om kwetsbaarheden te verminderen en de weerbaarheid tegen cyberdreigingen te vergroten. Dit helpt om de impact van een daadwerkelijke cyberaanval te minimaliseren en de continuïteit van de dienstverlening te waarborgen.

- **Vertrouwen en reputatie**

Het organiseren van een crisisoefening cybercrime toont aan dat een lokaal bestuur de bescherming van persoonsgegevens en de veiligheid van digitale systemen serieus neemt. Het vergroot het vertrouwen van medewerkers, inwoners, stakeholders en partners in de veerkracht en capaciteiten van eenlokaal bestuur. Het draagt bij aan een positieve reputatie en positioneert het bestuur als proactief en bekwaam op het gebied van cyberveiligheid.

Kortom, het organiseren van een crisisoefening cybercrime is een essentiële stap voor jouw lokaal bestuur om zich voor te bereiden en te reageren op cyberdreigingen.

3. Starten aan een crisisoefening cybercrime

3. Starten aan een crisisoefening cybercrime

Aangezien digitale dreigingen en cyberaanvallen steeds vaker bij lokale besturen voorkomen, heeft een lokaal bestuur de verantwoordelijkheid om de cyberveiligheid van de interne werking te waarborgen. Daarom is het ook een goeie zet om een crisisoefening cyberveiligheid te organiseren.

De twee oefenscenario's zijn een voorbereiding op mogelijke cyberaanvallen en testen de responsmogelijkheden. De organisatie van de crisisoefening zet in op

- het beschermen van gevoelige informatie
- het waarborgen van de continuïteit van diensten
- het opbouwen van veerkracht tegen cyberbedreigingen.

Het draaiboek crisisoefening cybercrime bevat **twee verschillende scenario's**: een tijdelijke uitval van een onderdeel van de digitale dienstverlening zonder een lek van persoonsgegevens en een totale uitval van de dienstverlening met een lek van persoonsgegevens. De oefening daagt het crisisteam uit om snel en effectief te reageren, de situatie te beoordelen, de impact te minimaliseren en herstelmaatregelen te treffen.

De crisisoefening cyberveiligheid traint de medewerkers van het lokaal bestuur, vergroot het bewustzijn en scherpt de reactieprocedures aan. Zwakke punten in het beleid, de processen en de technische infrastructuur worden geïdentificeerd en later aangepakt.

Organiseer en evalueer een crisisoefening cybercrime door de volgende zes stappen te volgen.

3. Starten aan een crisisoefening cybercrime

- Stap 1: Een crisisoefening cybercrime organiseren
  - Deel 1: De oefenbegeleider
  - Deel 2: De observator(en)
  - Deel 3: Oefenscenario kiezen
  - Deel 4: Het crisisteam
- Stap 2: Een crisisoefening cybercrime uitvoeren
- Stap 3: Een crisisoefening cybercrime evalueren

Stap 1: Een crisisoefening cybercrime organiseren

Deel 1: De oefenbegeleider
Deel 2: De observator(en)
Deel 3: Oefenscenario kiezen
Deel 4: Het crisisteam

Vereniging van
Vlaamse Steden
en Gemeenten

Deel 1: De oefenbegeleider

Deel 1: De oefenbegeleider

Een oefenbegeleider is een essentiële rol bij het **opzetten en begeleiden** van een crisisoefening cybercrime binnen een lokaal bestuur. Als ervaren deskundige, creëert de oefenbegeleider een realistische en leerzame simulatie.

De oefenbegeleider **kiest een oefenscenario**, rekening houdend met de specifieke behoeften en doelstellingen van het lokaal bestuur. Eveneens zorgt hij of zij voor alle praktische elementen die nodig zijn om een crisisoefening cybercrime uit te voeren.

Tijdens de oefening fungeert de oefenbegeleider als **begeleider en facilitator**. Hij of zij leidt het crisisteam door de verschillende situaties en uitdagingen die zich voordoen tijdens het gesimuleerde cyberincident. De oefenbegeleider zorgt voor een vlotte en realistische uitvoering van de oefening en stimuleert deelnemers om actief te reageren.

De oefenbegeleider is daarnaast verantwoordelijk voor het **monitoren van de voortgang** en fungeert hij of zij als timekeeper. Indien nodig, kan de oefenbegeleider ingrijpen om de oefening op schema te houden en de deelnemers te ondersteunen bij het vinden van oplossingen.

Na afloop van de oefening is de oefenbegeleider samen met de observatoren betrokken bij **de evaluatie van de oefening en het verzamelen van feedback van het crisisteam**. Het lokaal bestuur gebruikt vervolgens deze waardevolle input om inzicht te verwerven, sterkte punten te benadrukken en verbeterpunten te identificeren voor de verdere versterking van de cyberveiligheid.

De volgende lijst somt taken op van de oefenbegeleider.

Pas het overzicht van taken aan naargelang de noden en behoeften van jouw lokaal bestuur.

Takenlijst voor de organisatie van de crisisoefening 2/2

- ❑ Verzamel alle noodzakelijke ondersteuning: het draaiboek, de checklist voor de oefenbegeleider en observatoren, presentatie van het scenario, de checklist voor de evaluatie

- ❑ Nodig alle betrokken diensten uit

  Elke betrokken dienst vaardigt iemand af als vertegenwoordiger. Zorg ervoor dat alle cruciale functies zijn vertegenwoordigd in het team. De oefening start vanaf het moment dat de oefenbegeleider een seintje geeft, maar het crisisteam verzamelt zich pas op het juiste moment in de oefening.

- ❑ Duid 1 of 2 observatoren aan die het crisisteam tijdens de oefening zullen observeren en nodig hen uit. Bezorg hen de checklist voor observatoren en leg de taak uit.

  De observatoren kunnen zowel interne medewerkers zijn als externen. Zorg voor observatoren die de oefening kunnen bijwonen en feedback kunnen geven aan het crisisteam. Plan ook een debriefingssessie na de oefening om leerpunten en verbeterpunten te identificeren.

Deel geen extra informatie met deelnemers om de crisisoefening zo realistisch mogelijk te maken.

Takenlijst voor de organisatie van de crisisoefening 1/2

- ❑ Bepaal het doel en de scope van de crisisoefening in overleg met jouw lokaal bestuur

  Stel duidelijke doelstellingen op voor de oefening. Wat wil je bereiken? Bijvoorbeeld testen van respons op een cyberaanval, verbeteren van samenwerking tussen afdelingen, versterken van communicatievaardigheden

  Zorg ervoor dat het MAT akkoord is met het uitvoeren van een crisisoefening cyberveiligheid. Leden van het MAT nemen ook deel aan de oefening, dus de oefenbegeleider deelt alleen praktische informatie over de oefening.

- ❑ Kies een oefenscenario

  Kies een realistisch oefenscenario dat past bij de cyberveiligheidsrisico's van de stad of gemeente. Zorg ervoor dat het scenario uitdagend, maar haalbaar is.

- ❑ Stel een planning op voor de crisisoefening, inclusief de datum, tijd en locatie

- ❑ Zorg voor de benodigde faciliteiten: een oefenruimte, apparatuur en eventuele andere benodigdheden

  Controleer en zorg ervoor dat alle technologische aspecten die nodig zijn voor de oefening goed functioneren, inclusief de IT-infrastructuur en simulatieomgeving.

Tip: zorg voor een whiteboard waarop je een overzicht kan maken van feiten, acties en noden (FAN-bord). Denk ook aan fysieke contactlijsten van leveranciers en pers.

Takenlijst tijdens het uitvoeren van de crisisoefening

- ❑ Onthaal de leden van het crisisteam op de vermelde locatie.

  Tip: laat deelnemers pas spreken vanaf het moment in de oefening dat ze er bijgehaald zijn.

- ❑ Begeleid de oefening en zorg dat alle geplande gebeurtenissen plaatsvinden tijdens de oefening.
- ❑ Houd de tijd en voortgang van de oefening in de gaten en stuur indien nodig bij om de oefening op schema te houden.
- ❑ Faciliteer de communicatie tussen de deelnemers en stimuleer een actieve deelname en betrokkenheid van het crisisteam.

Takenlijst na het uitvoeren van een crisisoefening

- ❑ Evalueer de oefening met het crisisteam en de observatoren, met het oog op prestaties en leerpunten.
- ❑ Verzamel de feedback van de deelnemers over de oefening en identificeer mogelijke verbeteringen.
- ❑ Schrijf een evaluatierapport met een samenvatting van de oefening, de behaalde doelen en aanbevelingen voor toekomstige oefeningen.
- ❑ Deel het evaluatierapport en de bevindingen met het lokaal bestuur en andere relevante partijen. Zorg ervoor dat alle betrokken collega's de juiste procedure onder de knie krijgen.
- ❑ Bespreek de resultaten van de oefening en mogelijke verbeteringen met het crisisteam om lessen te trekken voor de toekomst.
- ❑ Bereid eventuele vervolgoefeningen voor op basis van de leerpunten en bevindingen van de huidige oefening.

Pas het scenario bij elke oefening aan of focus op een belangrijk deelproces. Tip: kies als scenario eens voor een uitzonderlijk moment, bijvoorbeeld de aanloop naar verkiezingen.

Vereniging van
Vlaamse Steden
en Gemeenten

Deel 2: De observatoren

Deel 2: De observatoren

Naast de oefenbegeleider, zijn observatoren van essentieel belang tijdens een crisisoefening cyberveiligheid binnen een lokaal bestuur. Hun taak is om onpartijdig

- **toezicht te houden op de oefening**
- **de deelnemers te observeren**
- **waardevolle feedback te verzamelen voor een grondige evaluatie achteraf**

Als neutrale waarnemers kunnen observatoren objectieve inzichten bieden en helpen bij het identificeren van sterke punten en verbeterpunten in de respons op een cyberincident.

Takenlijst

- ❑ Observeer tijdens de oefening

  Volg aandachtig de crisisoefening, let op hoe de deelnemers omgaan met de gebeurtenissen en uitdagingen die zich voordoen tijdens de crisisoefening.

- ❑ Noteer de observaties

  Documenteer waarnemingen en opmerkingen zorgvuldig, zowel positieve aspecten als mogelijke verbeterpunten.

- ❑ Focus op specifieke doelstellingen

  Evalueer of het crisisteam de doelstellingen heeft bereikt en hoe efficiënt en effectief de reacties waren.

- ❑ Identificeer de leerpunten

  Dit kan variëren van communicatieproblemen en coördinatiekwesties tot technische uitdagingen en besluitvormingsprocessen.

- ❑ Werk samen met de oefenbegeleider

  Zorg dat de observaties en de feedback geïntegreerd zijn in de evaluatie.

vvsg

Vereniging van
Vlaamse Steden
en Gemeenten

Deel 3: Oefenscenario kiezen

Oefenscenario 1

Context

“Op een normale werkdag merkt een medewerker van de IT-afdeling van de gemeente verdachte activiteiten op in het netwerk. Al snel wordt duidelijk dat de gemeentelijke website en gemeentelijke applicaties niet meer toegankelijk zijn voor zowel interne medewerkers als externe gebruikers. Na een initiële analyse wordt vastgesteld dat er sprake is geweest van ongeoorloofde toegang tot het systeem door een kwaadaardige hacker.”

De gebeurteniskaarten voor deze oefening vind je bij het referentiemateriaal.

Oefenscenario 2

Context

“Op een normale werkdag ontdekt een medewerker van de IT-afdeling van jouw lokaal bestuur verdachte activiteiten in het netwerk. Na een initiële analyse wordt vastgesteld dat er sprake is geweest van een succesvolle aanval door kwaadwillige hackers, waarbij de volledige digitale dienstverlening uitviel en er gevoelige informatie en persoonsgegevens zijn gelekt.”

De gebeurteniskaarten voor deze oefening vind je bij het referentiemateriaal.

Vereniging van
Vlaamse Steden
en Gemeenten

Deel 4: Het crisisteam

Deel 4: Het crisisteam - verplicht

Het crisisteam cybercrime bestaat uit een groep diverse personen, met elk een specifieke rol en verantwoordelijkheid tijdens een cybercrisis. Samen vormen ze een goed geoliede machine die snel en doeltreffend kan reageren op de uitdagingen tijdens een cyberincident.

Welke profielen behoren MINIMAAL tot het crisisteam?

1. **Een crisismanager** staat aan het hoofd van het crisisteam en is verantwoordelijk voor het leiden van de respons op de cyberaanval. Hij of zij coördineert de inspanningen van het team en neemt cruciale beslissingen in overleg met andere leden. De crisismanager is stressbestendig en kan snel schakelen om de situatie onder controle te houden.

2. **Een notulist** heeft een belangrijke rol in het vastleggen van alle gebeurtenissen, beslissingen en acties tijdens de oefening. Het zorgvuldig bijhouden van de genomen stappen en de tijdsduur van elke actie is waardevol voor de latere evaluatie van de oefening.

3. **Een communicatieverantwoordelijke** verzorgt de interne en externe communicatie tijdens de crisisoefening. Hij of zij zorgt ervoor dat alle betrokkenen goed geïnformeerd worden met heldere en consistente verwoording.

4. **ICT-verantwoordelijke** is de expert op het gebied van cyberveiligheid en neemt de technische leiding tijdens de oefening. Hij of zij evalueert de cyberaanval, bepaalt de juiste technische maatregelen en coördineert de herstelwerkzaamheden.

5. **De noodplanningscoördinator** is vertrouwd met methodieken van een crisiswerking. Hij of zij zal zeker worden betrokken bij mogelijke incidenten veroorzaakt door een cyberaanval, bijv. evacuatie van een woonzorgcentrum of het verstoren van de openbare orde door relschoppers.

Deel 4: Het crisisteam - facultatief

Welke profielen behoren OPTIONEEL tot het crisisteam?

1. **De functionaris gegevensbescherming** begeleidt de organisatie om zich zo goed mogelijk te conformeren aan de bepalingen van de GDPR. Hij of zij focust zich vooral op het opsporen van mogelijke datalekken en het inlichten van de toezichthouder(s) (VTC en GBA). Personeel met juridische achtergrond en/of een advocatenkantoor kan bijstand verlenen, bijv. om aansprakelijkheid in te schatten of zich voor te bereiden op schadeclaims.

2. **De HR-verantwoordelijke** kent de organisatiestructuur en zet de beschikbare medewerkers optimaal in. Hij of zij neemt eventueel de interne communicatie over van de communicatieverantwoordelijke. Hij of zij mobiliseert de eigen procesexperten in het kader van de bedrijfscontinuïteit, om te bepalen in welke volgorde de bedrijfsprocessen (en dus de bijhorende systemen) bij voorkeur herop gestart worden. Hij of zij staat in voor de planning van de medewerkers tijdens de crisis.

3. **De financieel verantwoordelijke** controleert of er nog bestellingen geplaatst kunnen worden, facturen betaald kunnen worden of andere financiële stromen blijven werken, gelet op het feit dat de afhandeling van een cyberaanval lang kan duren. Bijkomend kan hij of zij opdracht geven tot het ramen van de opgelopen financiële schade.

4. **De facilitair verantwoordelijke** staat mee in voor het inrichten van een crisisruimte, zeker wanneer er behoefte is aan noodstroom via generatoren. Hij of zij neemt ook de verdere coördinatie van de logistieke ondersteuning op zich en werkt samen met de technische dienst van het lokaal bestuur.

Draaiboek crisisoefening cybercrime

Stap 2: Een crisisoefening cybercrime uitvoeren

Stap 2: Een crisisoefening cybercrime uitvoeren

De oefenbegeleider heeft een centrale rol bij het uitvoeren van een crisisoefening cyberveiligheid en het gebruik van de gebeurteniskaarten. Een stapsgewijze uitleg:

1. **Doelbepaling:** Begin met het vaststellen van het specifieke doel van de oefening. Wat wil je bereiken met de crisisoefening?

2. **Scenariokeuze:** Kies een geschikt oefenscenario dat past bij jouw lokaal bestuur.

3. **Timing en coördinatie:** Bij het gebruik van de gebeurteniskaarten, hou je best rekening met de timing van elke gebeurtenis. Een goede coördinatie is essentieel om ervoor te zorgen dat de oefening soepel verloopt.

4. **Real-time aanpassingen:** Als oefenbegeleider kan je tijdens de oefening real-time aanpassingen maken op basis van de reacties van het crisisteam. Als bepaalde gebeurtenissen te makkelijk of te moeilijk lijken, kan je de oefening aanpassen om een optimale leerervaring te bieden.

5. **Observatie en feedback:** Zorg ervoor dat de observatoren de oefening kunnen bijwonen en feedback kunnen geven over de prestaties van het crisisteam. Deze feedback is waardevol voor het identificeren van sterke punten en verbetergebieden.

6. **Evaluatie:** Na de oefening hou je een uitgebreide evaluatiesessie waarin de gebeurtenissen worden besproken en de leermogelijkheden worden geïdentificeerd. Zorg ervoor dat het crisisteam begrijpt wat goed ging en wat er kan worden verbeterd.

7. **Rapportage:** Evalueer het succes van de oefening aan de hand van het vooraf bepaalde doel en maak een rapport met aanbevelingen voor toekomstige oefeningen en verbeteringen in de cyberveiligheidsrespons.

Als oefenbegeleider is het belangrijk om flexibel te zijn en goed voorbereid te zijn op onverwachte wendingen. Door de gebeurteniskaarten effectief te gebruiken en de oefening goed te coördineren, zul je het crisisteam uitdagen en voorbereiden op echte cyberdreigingen.

Stap 3: Een crisisoefening cybercrime evalueren

Stap 6: Crisisoefening cybercime evalueren

De evaluatie van de crisisoefening cybercrime binnen een lokaal bestuur is een essentiële stap om inzicht te krijgen in de effectiviteit van de oefening en om waardevolle lessen te trekken voor de toekomst. Identificeer sterke punten en zoek verbeteringen om de cyberveiligheid van het lokaal bestuur te versterken.

Het belang van de evaluatie

De evaluatie van een crisisoefening cyberveiligheid biedt meerdere voordelen voor een lokaal bestuur:

1. **Identificatie van sterke punten:** effectieve besluitvorming, communicatie en coördinatie tussen het crisisteam en andere belanghebbenden.

2. **Verbetering van de respons**: aanpassen van technische maatregelen tot het verfijnen van protocollen en procedures.

3. **Ontwikkeling van lessen voor de toekomst**: om de cyberveiligheidsplannen- en procedures van het lokaal bestuur te versterken bij toekomstige incidenten.

4. **Teamcohesie en samenwerking**: het belang van teamreflectie en samenwerking binnen het crisisteam en met andere betrokken diensten.

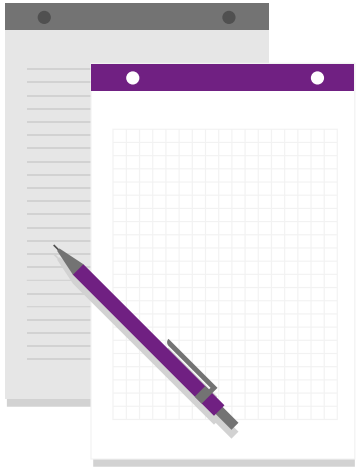
Stap 6: Crisisoefening cybercrime evalueren

Het evaluatieproces bestaat uit de volgende stappen:

1. **Verzamelen van feedback**: door middel van enquêtes, interviews of feedbackformulieren.
2. **Analyse van de prestaties:** beoordeel hoe goed de gestelde doelen zijn bereikt en of de acties adequaat waren.
3. **Identificatie van sterke punten:** denk aan effectieve besluitvorming, snelle reacties, goede communicatie, ...
4. **Identificatie van verbeterpunten:** technische aspecten, maar ook communicatieproblemen, coördinatie of besluitvormingsprocessen.
5. **Leerpunten en aanbevelingen:** zorg ervoor dat deze punten duidelijk en haalbaar zijn.
6. **Bespreking met het crisisteam:** moedig discussie aan over de prestaties en mogelijke verbeteringen.
7. **Implementatie van verbeteringen: i**mplementeer de leerpunten en aanbevelingen in het cyberveiligheidsplan en bijbehorende procedures. Zorg ervoor dat verbeteringen worden doorgevoerd voor toekomstige oefeningen en reële incidenten.
8. **Monitoring en follow-up:** controleer de effectiviteit van de genomen maatregelen en blijf waar nodig aanpassingen maken.

Stap 6: Crisisoefening cybercrime evalueren

Voor de evaluatie van de crisisoefening cyberveiligheid gebruik je de checklist voor oefenbegeleider en observatoren. Deze documenten vormen al een basis voor de evaluatie van een crisisoefening, vul dit document steeds verder aan naar gelang de noden en behoeften van jouw lokaal bestuur.



4. Referentiemateriaal

4. Referentiemateriaal

Gebeurteniskaarten oefenscenario 1

Tijdelijke uitval van een element van de digitale dienstverlening, zonder datalek.

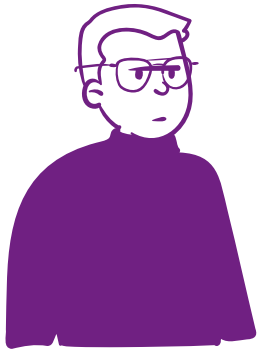
Noot: deze gebeurteniskaarten zijn een basis voor dit oefenscenario. Pas als oefenbegeleider gebeurte nissen aan naargelang de noden en behoeften van jouw lokaal bestuur.

vvsg

Gebeurteniskaart

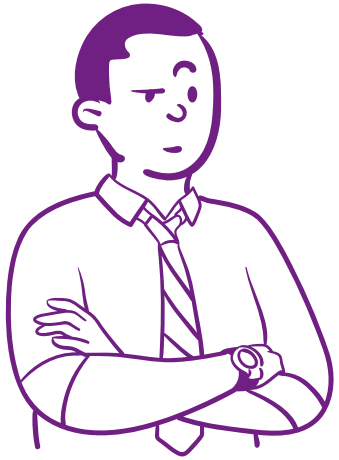
Een medewerker binnen de interne organisatie van het lokaal bestuur meldt dat zij hinder ondervindt wanneer ze naar de website van het lokaal bestuur surft en wil inloggen in één van de bijbehorende toepassingen verbonden aan de website.

Gebeurteniskaart



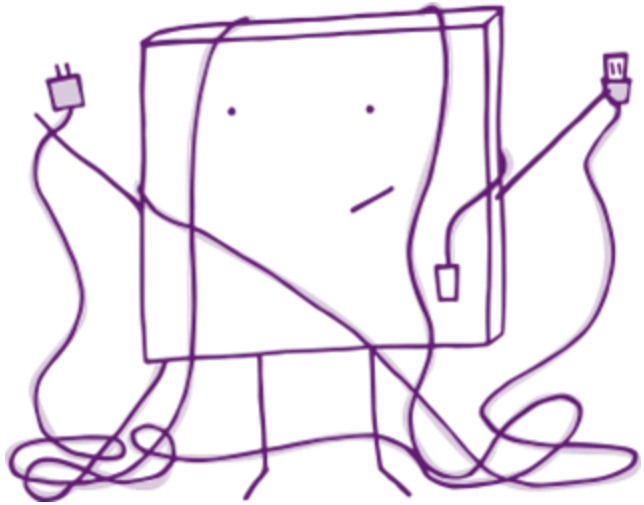
De onthaalmedewerker van het lokaal bestuur kreeg een aantal telefoontjes van boze burgers, met de boodschap dat ze de website van het lokaal bestuur niet kunnen consulteren. Inloggen op de toepassingen verbonden aan de website, zoals het e-loket, lukt ook niet.

Gebeurteniskaart



Er heerst ongerustheid en verwarring bij de medewerkers van het lokaal bestuur.

Gebeurteniskaart



De website van het lokaal bestuur en de verbonden toepassingen zijn offline.

Gebeurteniskaart

Op sociale media verschijnen er berichten over de verstoring binnen het lokaal bestuur. Verschillende theorieën steken de kop op.

Gebeurteniskaart

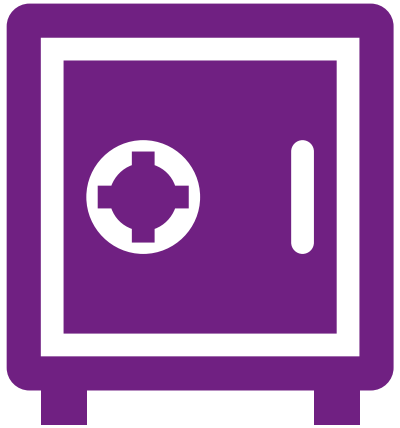
De berichten op sociale media werden ook door de lokale pers opgemerkt. In een mum van tijd verschijnen er verschillende berichtgevingen. Het algemeen telefoonnummer van het lokaal bestuur wordt overspoeld met telefoontjes van journalisten.

Gebeurteniskaart

Gebeurteniskaart

De helpdesk van de ICT-leverancier is niet bereikbaar.

Gebeurteniskaart



De kwaadwillige hacker kon zich geen toegang verschaffen tot gevoelige informatie en persoonsgegevens.

Gebeurteniskaart

Het lokaal bestuur is erin geslaagd om de toegang van de kwaadwillige hacker te blokkeren.

Gebeurteniskaart

De website en gekoppelde toepassingen zijn terug operationeel.

4. Referentiemateriaal

Gebeurteniskaarten oefenscenario 2

Volledige uitval van de digitale dienstverlening, met datalek.

Noot: deze gebeurteniskaarten zijn een basis voor dit oefenscenario. Pas als oefenbegeleider geb eurtenissen aan naargelang de noden en behoeften van jouw lokaal bestuur.

vvsg

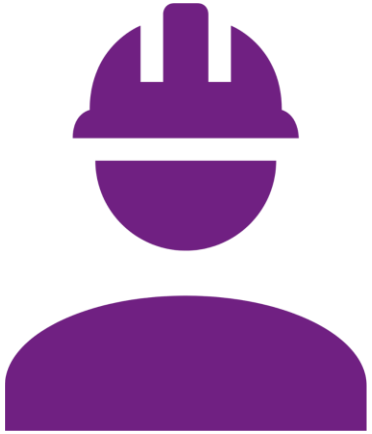
Gebeurteniskaart

Een medewerker van de lokale bibliotheek meldt dat bezoekers sinds een kwartier een foutmelding krijgen wanneer ze hun boeken inscannen om te ontlenen en in te leveren. Ze hebben ondertussen verschillende toestellen geprobeerd, maar op elk toestel verschijnt dezelfde foutmelding.

Gebeurteniskaart

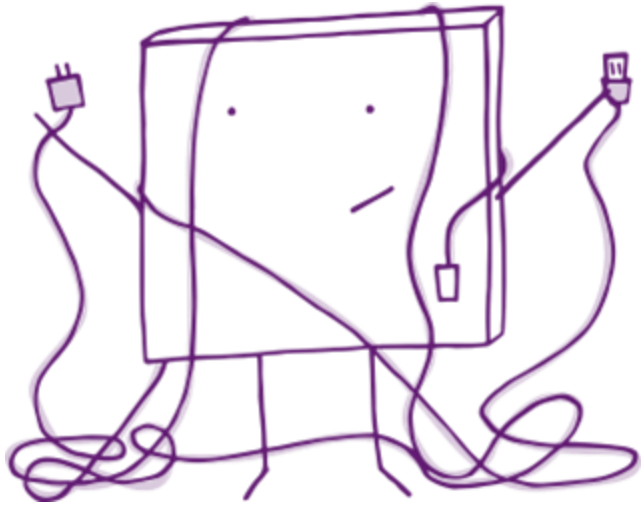
De onthaalmedewerker van het lokaal bestuur meldt aan de dienst ICT dat er plots geen oproepen meer binnenkomen en verstuurd kunnen worden via de helpdeskapplicatie.

Gebeurteniskaart



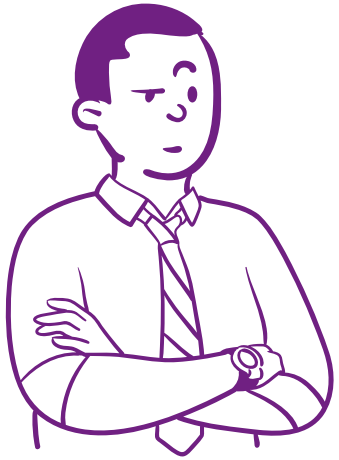
De technische dienst van het lokaal bestuur meldt dat ze hun planning voor vandaag niet meer kunnen consulteren via de gebruikelijke applicatie.

Gebeurteniskaart



De website en bijbehorende toepassingen van het lokaal bestuur zijn offline gehaald.
Zowel inwoners als personeel kunnen niet meer inloggen.

Gebeurteniskaart



Er heerst ongerustheid en verwarring bij de medewerkers van het lokaal bestuur.

Gebeurteniskaart

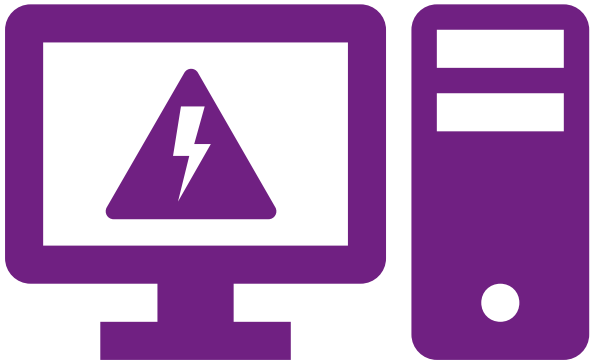
Het lokaal bestuur is momenteel onbereikbaar voor inwoners. Op sociale media verschijnen talloze berichten van ongeruste inwoners.

Gebeurteniskaart

De berichten op sociale media werden ook door de lokale pers opgemerkt. In een mum van tijd verschijnen er verschillende berichtgevingen.

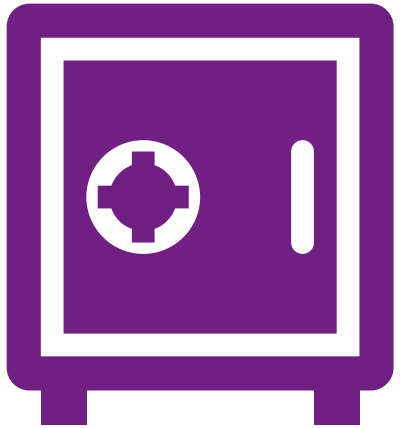
Gebeurteniskaart

Gebeurteniskaart



¾ van de werktoestellen verbonden op het interne netwerk van het okaal bestuur blijkt geïnfecteerd te zijn door de cyberaanval.

Gebeurteniskaart



De kwaadwillige hacker kon zich toegang verschaffen tot gevoelige informatie en persoonsgegevens.

Gebeurteniskaart

“Ik ontving vandaag een e-mail met de melding dat ik mijn milieubelastingen nog niet zou hebben betaald…”

- Marie, 40 jaar, is vorige maand komen wonen in jouw lokaal bestuur.

“Ik kreeg vandaag een SMS dat ik mijn bankgegevens online moest aanpassen om mijn leefloon nog verder te ontvangen…”

- Ludo, 67 jaar, woont alleen en heeft beperkte computervaardigheden.

Gebeurteniskaart

Ook de lokale media is op de hoogte van het datalek binnen het lokaal bestuur.

Gebeurteniskaart

De helpdesk van de ICT-leverancier is niet bereikbaar.

Gebeurteniskaart

Een dichtstbijzijnde politie- of brandweerzone reageert op de vraag om hulp en biedt een aantal veilige pc's aan. Ze willen ook de ICT-dienst van het lokaal bestuur ondersteunen.

Gebeurteniskaart

Het lokaal bestuur is erin geslaagd om vanuit een veilige back-up bepaalde elementen van de digitale ICT-infrastructuur terug op te starten.

Gebeurteniskaart

Het lokaal bestuur is erin geslaagd om de toegang van de kwaadwillige hacker te blokkeren.

Gebeurteniskaart

Een lokaal bestuur uit de buurt biedt hulp aan. De inwoners kunnen voor bepaalde zaken bij hun dienstverlening terecht, aangezien dit lokaal bestuur met dezelfde toepassingen werkt.

Gebeurteniskaart

Het lokaal bestuur is erin geslaagd om een deel van de dienstverlening terug operationeel te krijgen.

4. Referentiemateriaal

Extra gebeurteniskaarten

Noot: Deze gebeurteniskaarten zijn een basis voor dit oefenscenario. Je mag als oefenbegeleider ook zelf gebeurtenissen veranderen, toevoegen of weglaten naargelang de noden en behoeften van jouw lokaal bestuur.

vvsg

Gebeurteniskaart

Er kunnen geen mails meer verstuurd en/of ontvangen worden.

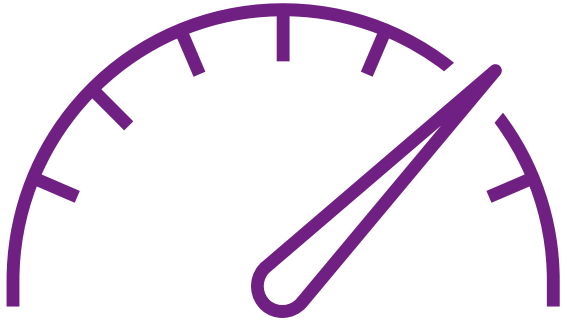
Gebeurteniskaart

Inkomende en uitgaande oproepen via de vaste telefoon zijn niet meer mogelijk.

Gebeurteniskaart

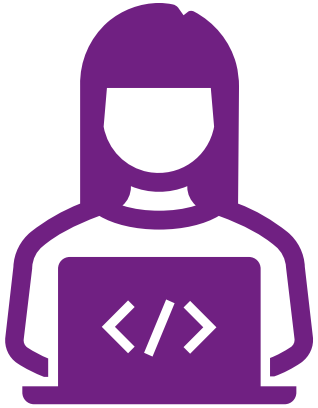
Bezoekers op diverse locaties melden dat het gastennetwerk niet meer functioneert.

Gebeurteniskaart



Het lukt niet meer om de klimaatregeling (heating, ventilation, air purifying) in bepaalde gebouwen aan te sturen.

Gebeurteniskaart



Collega's die van thuis uit werken raken niet meer ingelogd op de ICT-omgeving ("Toegang is geweigerd").

Gebeurteniskaart

De dienst ICT vraagt aan iedereen om met spoed uit te loggen uit ALLE werkcomputers.

Gebeurteniskaart

Sommige printers beginnen uit zichzelf documenten af te drukken.

Gebeurteniskaart

De tijdsregistratie (prikklokken) zijn niet langer operationeel.

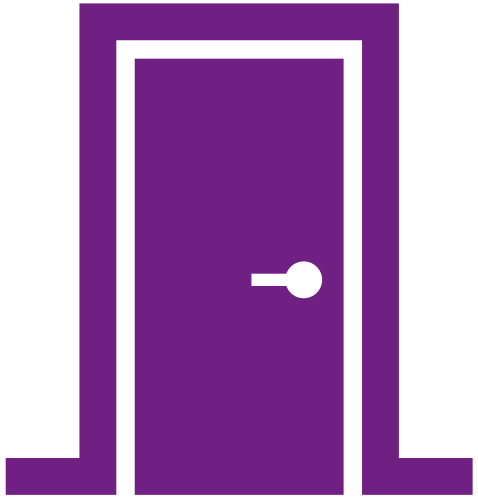
Gebeurteniskaart

De monitoren voor camerabewaking zijn op meerdere sites op “zwart” gegaan.

Gebeurteniskaart

De monitoren voor camerabewaking zijn op meerdere sites op “zwart” gegaan.

Gebeurteniskaart



De toegangscontrole is buiten dienst, er is een sleutel nodig om in sommige gebouwen binnen te geraken.

4. Referentiemateriaal

Takenlijst observator

vvsg

Voor de oefening

- ❑ Zorg ervoor dat je het oefenscenario en de doelstellingen ervan begrijpt.
- ❑ Je bent op de hoogte welke rollen en functies de deelnemers zullen hebben tijdens de oefening.
- ❑ Neem alvast **het observatieplan** door dat aangeeft op welke specifieke aspecten je moet letten tijdens de oefening.

Takenlijst observator

Tijdens de oefening

- ❑ Let op de communicatie binnen het crisisteam.
- ❑ Beoordeel de effectiviteit van de besluitvorming en de snelheid van de respons.
- ❑ Controleer of het crisisteam de juiste procedures volgen.
- ❑ Beoordeel de coördinatie en de samenwerking tussen de verschillende leden van het crisisteam.
- ❑ Noteer eventuele uitdagingen, problemen of obstakels die zich voordoen tijdens de oefening.
- ❑ Let op de technische respons op de cyberaanval en het verloop van het herstelproces.
- ❑ Controleer de naleving van het cyberveiligheidsbeleid en de procedures van het lokaal bestuur.
- ❑ Noteer hoe goed het crisisteam omgaat met de gebeurtenissen op de gebeurteniskaarten.

Na de oefening

- ❑ Bespreek de observaties en bevindingen met het crisisteam en de oefenbegeleider.
- ❑ Identificeer sterke punten en gebieden die verbeterd kunnen worden.
- ❑ Formuleer leerpunten en aanbevelingen.
- ❑ Samen met de oefenbegeleider zorg je ervoor dat de observaties worden opgenomen in het evaluatierapport van de oefening.
- ❑ Optioneel: Samen met de oefenbegeleider deel je de observaties en aanbevelingen met het management en andere belanghebbenden.

Is er iets niet duidelijk of heb je vragen? Spreek dan zeker de oefenbegeleider aan!

Observatiepunten voor de observator tijdens een crisisoefening cyberveiligheid

- ✓ **Communicatie**
  - Hoe wordt er gecommuniceerd binnen het crisisteam?
  - Is de communicatie duidelijk, tijdig en effectief?
  - Worden de juiste communicatiemiddelen gebruikt?

- ✓ **Besluitvorming**
  - Hoe worden beslissingen genomen binnen het crisisteam?
  - Wordt er snel en doordacht gehandeld bij het nemen van beslissingen?
  - Worden beslissingen goed gemotiveerd en gecommuniceerd?

- ✓ **Samenwerking en coördinatie**
  - Hoe verloopt de samenwerking tussen de verschillende leden van het crisisteam?

- ✓ **Technische respons**
  - Hoe snel reageert het crisisteam op de cyberaanval?
  - Hoe adequaat zijn de technische maatregelen om de aanval te stoppen en het systeem te herstellen?
  - Worden er juiste procedures gevolgd bij het omgaan met de technische aspecten van de aanval?

- ✓ **Herstelproces**
  - Hoe efficiënt verloopt het herstelproces na de aanval?
  - Worden de juiste stappen genomen om de website en de bijbehorende toepassingen weer online te krijgen?

4. Referentiemateriaal

Observatiepunten voor de observator tijdens een crisisoefening cyberveiligheid

vvsg

Observatiepunten voor de observator tijdens een crisisoefening cyberveiligheid

- ✓ **Naleving van de procedures**
  - Worden de cyberveiligheidsprocedures van het lokaal bestuur gevolgd?
  - Hoe goed zijn de deelnemers op de hoogte van de procedures en weten ze hoe ze moeten handelen?

- ✓ **Stressbestendigheid**
  - Hoe gaan de deelnemers om met de stress van een crisis?
  - Wordt de situatie goed beheerd en blijft iedereen kalm en gefocust?

- ✓ **Reactietijd**
  - Hoe snel reageert het crisisteam op de verschillende gebeurtenissen?
  - Worden er tijdige acties ondernomen om de aanval te stoppen en de gevolgen te beperken?

- ✓ **Evaluatie van gebeurtenissen**
  - Worden de gebeurtenissen grondig geëvalueerd voordat er actie wordt ondernomen?
  - Wordt er voldoende informatie verzameld om weloverwogen beslissingen te nemen?

- ✓ **Teamcohesie**
  - Hoe goed werkt het crisisteam samen als een geheel?
  - Wordt er onderlinge steun geboden en vertrouwen opgebouwd?

4. Referentiemateriaal

Toolkit cyberveiligheid

Deze toolkit bevat diverse tools om binnen jouw lokaal bestuur aan de slag te gaan met cyberveiligheid.

De toolkit cyberveiligheid werd door de VVSG en een taskforce van lokale experten samengesteld.

vvsg

Extra referentiemateriaal

Samen met een taskforce van lokale experten werkte de VVSG **de toolkit cyberveiligheid** uit met diverse sjablonen, richtlijnen en documentatie om lokale besturen te begeleiden naar een cyberveilige digitale dienstverlening en organisatiestructuur.

- Cyber Response Team van de Vlaamse Overheid
- Eerste hulp bij een cyberaanval - CERT
- Leidraad Crisiscommunicatie

Toolkit cyberveiligheid

Samen met een taskforce van lokale experten werkte de VVSG **de toolkit cyberveiligheid** uit met diverse sjablonen, richtlijnen en documentatie om lokale besturen te begeleiden naar een cyberveilige digitale dienstverlening en organisatiestructuur.

- Draaiboek cybercrime
- Business continuïteitsplan
- Crisiscommunicatieplan
- Checklist crisisbeheer
- Beleid voor responsible disclosure
- Register voor cyberincidenten
- Procedure melding cyberincidenten
- Interne en externe contactlijsten
- Richtlijnen Secure Software Development
- Veiligheids- en opvolgingsplan
- Richtlijnen organisatiebeheersing
- Cybertips en –tricks
- Richtlijnen beveiliging camerasystemen
- Nuttige freeware cyberveiligheid
- Initiatieven en vormingen

5. Bronnen

5. Bronnen

- **Interactieve cyberoefening Vereniging van Nederlandse Gemeenten (VNG)**
  - Interactieve Cyberoefening | VNG. (z.d.). VNG. https://vng.nl/artikelen/interactieve-cyberoefening
- **Cyberoefenpakket VNG: oefenscenario's digitale incidenten**
  - https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vng-oefenscenarios-digitale-incidenten/
- **Rapport cyberaanval gemeente Willebroek**
  - Rapport cyberaanval gemeente Willebroek (z.d.). https://www.vvsg.be/kennisitem/vvsg/rapport-cyberaanval-gemeente-willebroek
- **Rapport cyberaanval Universiteit Maastricht**
  - Ministerie van Onderwijs, Cultuur en Wetenschap. (2021, October 20). Rapport Cyberaanval Universiteit Maastricht. Kamerstuk | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/kamerstukken/2020/06/12/definitief-rapport-cyberaanval-universiteit-maastricht-21pj-docx

Over de VVSG

De Vereniging van Vlaamse Steden en Gemeenten vzw is het steunpunt, de belangenbehartiger en de beweging van het lokale bestuur.

Alle 300 gemeenten en OCMW's in Vlaanderen zijn lid, naast vele politiezones en intergemeentelijke samenwerkingsverbanden. Een huis van vertrouwen dat haar leden advies en begeleiding verleent, informatie geeft op maat, zorgt voor opleiding en vorming, ontmoetingsdagen organiseert en andere ondersteunende diensten biedt.

Meer dan 10.000 politici of ambtenaren volgen elk jaar een studiedag of een opleiding bij de VVSG.

Meer informatie vind je op **het VVSG-kennisnetwerk**.

Slotwoord

Met het doornemen van dit draaiboek heb je een belangrijke stap gezet in het versterken van de cyberveiligheid en paraatheid binnen jouw lokale bestuur. Cyberdreigingen vormen een toenemende uitdaging en proactieve maatregelen zoals deze oefeningen zijn van vitaal belang zijn om de gemeenschap te beschermen.

Cyberveiligheid is een voortdurende inspanning en een gedeelde verantwoordelijkheid. Deel de opgedane kennis en ervaring delen met collega's en herhaal de oefeningen regelmatig om mee te zijn met de evoluerende cyberdreigingen.

Onze dank gaat uit naar alle betrokkenen die hebben bijgedragen aan de totstandkoming van dit draaiboek en aan de versterking van cyberveiligheid binnen lokale besturen.

Mail naar cyberveiligheid@vvsg.be voor vragen, behoefte aan verdere assistentie of het delen van feedback.

Draaiboek crisisoefening cyberveiligheid

AGENTSCHAP BINNENLANDS BESTUUR
Vlaamse overheid

AUDIT VLAANDEREN
Vlaamse overheid

DIGITAAL VLAANDEREN
Vlaamse overheid

vvsg