****

Checklist Crisisbeheer

Dit sjabloon kadert binnen het Project Cyberveilige Gemeenten,

een samenwerking tussen:

****



*Wanneer een lokaal bestuur geconfronteerd wordt met een cyberaanval of ander IT-gerelateerd incident, dienen op korte termijn diverse maatregelen genomen te worden om terug controle over de IT-omgeving te krijgen en mogelijke financiële- en reputatieschade in te perken. Door de veelheid aan keuzes die gemaakt dienen te worden en de snelheid waarmee alles moet gebeuren, is het niet altijd even eenvoudig om het overzicht te behouden.*

*Deze checklist op basis van de ervaringen van Belgische en Nederlandse lokale besturen en algemene aanbevelingen tracht een overzicht te geven van de te doorlopen stappen, en kan gebruikt worden als een beknopte, richtinggevende gids of een inspiratiebron voor een breder draaiboek voor cybercriminaliteit. Natuurlijk is elke organisatie en elk lokaal bestuur anders en het is dan ook aangeraden om de stappen aan te passen aan de werking, organisatie en richtlijnen binnen je lokaal bestuur. De checklist kan niet gezien worden als een zuiver chronologisch proces aangezien vele stappen tegelijkertijd moeten plaatsvinden en de chronologie sterk bepaald wordt door het incident zelf. Desalniettemin zorgt een goede voorbereiding en incident response strategie ervoor dat je tijdens crisissituaties beroep kan doen op een houvast. Door proactief na te denken over de stappen die je binnen je lokaal dient te zetten bij een echte crisissituatie kunnen heel wat kopzorgen en nodeloos tijdverlies vermeden worden.*

**1.Identificatie en melding**

In eerste instantie moet gecontroleerd worden of er daadwerkelijk een incident heeft plaatsgevonden en wat de reikwijdte is van het voorval. Deze activiteit omvat in meeste gevallen de systeembeheerder en eindgebruiker - zoals een medewerker van het OCMW, een burger die geen toegang krijgt tot de website of ander platform, een toeleverancier, … - maar kan ook het gevolg zijn van proactieve detectie van incidenten door de ICT-beveiliging of het systeembeheer. Indien wordt vastgesteld dat het inderdaad een incident is, moet de meldingsprocedure in gang gezet worden en moeten de nodige voorbereidingen getroffen worden in kader van het beperken van de blootstelling en sporenonderzoek.

|  |  |  |  |
| --- | --- | --- | --- |
| Gedaan | Taakomschrijving | Uitvoerend | Verantwoordelijk |
| Badge Tick1 met effen opvulling | Een ICT-gerelateerd probleem wordt vastgesteld door een medewerker of inwoner, zoals problemen bij het inloggen, vertraagde werking van systemen of andere storingen met merkbare impact. Bij vermoeden van een grotere problematiek of onduidelijkheden hierrond wordt de melding volgens de interne richtlijnen **geëscaleerd naar de ICT-dienst, DPO, CISO, … voor verder onderzoek**. | Interne medewerker of externe | Diensthoofd of onthaal |
|  | **Beperk indien nodig onmiddellijk de blootstelling**. Wanneer het probleem een elektronisch apparaat betreft houdt dit bijvoorbeeld in dat men niet inlogt of het apparaat wijzigt, dat men het apparaat niet uitschakelt en dat men het apparaat van de netwerkverbindingen haalt, zonder de voedingskabel te verwijderen. |  |  |
|  | Noteer hoe het probleem werd ontdekt en welke acties al ondernomen werden. **Zorg voor een zo concreet mogelijke beschrijving met data, tijden, de gecompromitteerde apparaten, applicaties, websites en andere.** |  |  |
|  | De ICT-dienst, DPO of CISO maakt een **voorlopige beoordeling** van het type incident en de urgentie. Gaat het over een geïsoleerd technisch probleem of zijn er sporen van besmetting, onrechtmatige toegangen of andere tekenen die kunnen wijzen op cybercriminaliteit? Deze snelle analyse kan resulteren in twee uitkomsten:   1. De melding blijkt een technische storing die verholpen kan worden binnen een redelijke termijn om daarna terug over te gaan naar de normale werking. 2. Er blijkt meer aan de hand: Op een bepaald moment vermoedt de IT-dienst dat de werking van de organisatie risico loopt, omdat het oplossen van het probleem van lange duur zal zijn of die duur op dit moment moeilijk of onmogelijk ingeschat kan worden. |  |  |
|  | De ICT-dienst, DPO of CISO stelt, afhankelijk van de interne meldingsprocedure, het **diensthoofd**, de **algemeen directeur of een ander leidend ambtenaar** **op de hoogte** zodra er een vermoeden is dat het daadwerkelijk gaat over cybercriminaliteit. Het gaat hier idealiter over iemand die 24/7 bereikbaar is. |  |  |
|  | Het diensthoofd, de algemeen directeur of een ander leidend ambtenaar stelt de burgemeester of leidinggevende op de hoogte en vraagt bij hoge urgentie goedkeuring om het **incident te melden aan de lokale politiezone en het CERT**. Zorg voor een vaste contactpersoon, idealiter een IT-profiel indien voldoende capaciteit. |  |  |
|  | **Start het forensisch onderzoek:** ga de logfiles (bv. Systeemlogs, firewall-logs) na om te kijken of data gestolen werd en breng in kaart of er sprake is van een onbeschikbaarheid of manipulatie van data of intrusie. Ga op zoek naar de oorzaak indien mogelijk - besmette link in mail, geïnstalleerd virus, … - en kijk wat de reikwijdte van de infectie is en welke systemen in de IT-omgeving getroffen zijn. |  |  |
|  | **Contacteer de lokale politie vooraf aan je verklaring** zodat zij al voorbereidingen kunnen treffen.  Verzamel in kader van de aangifte zoveel mogelijk relevante info, zoals het tijdstip van het incident, het detectietijdstip, de vermoedelijke oorsprong en oorzaak, het type data dat geïmpacteerd is, de acties die ondernomen werden, het getroffen besturingssysteem of software, de naam van het virus of netwerk indien gekend, … Het kan ook nuttig zijn om logbestanden en screenshots toe te voegen. |  |  |
|  | **Waarschuw iedereen die IT-systemen beheert over de infectie** - denk hierbij zeker ook aan toeleveranciers - zodat alle aangetaste computers, systemen en applicaties van het netwerk losgekoppeld kunnen worden. |  |  |
|  | Blijf na het bundelen van de initieel beschikbare informatie **fysiek en digitaal bewijs vergaren** dat een duidelijk overzicht geeft van het incident en de impact op data en dienstverlening, zoals afbeeldingen van harddisks, netwerkverkeergegevens van en naar gecompromitteerde systemen en toepassingen, applicatielogs, toegangslogs en foto’s van de omgeving van het incident. Maak een inventarisatielijst van al het beschikbare bewijsmateriaal en houdt bij wie, wanneer, wat gedaan heeft met het bewijsmateriaal. |  |  |

**2.Schadebestrijding**

In deze fase is het van belang dat de organisatie de omslag naar crisisbeheer maakt, met een Gemeentelijk Coördinatiecomité of Crisis Management Team, afhankelijk van de grootorde en interne processen. Het team dat zich ontfermt over het crisisbeheer is belast met het grondig beoordelen van de aard en omvang van het incident en het inperken van verdere schade. Dit omvat zowel IT-technische maatregelen om terug controle te krijgen over systemen en toepassingen als crisiscommunicatie naar interne en externe stakeholders.

|  |  |  |  |
| --- | --- | --- | --- |
| Gedaan | Taakomschrijving | Uitvoerend | Verantwoordelijk |
| Badge Tick1 met effen opvulling | **De burgemeester of leidinggevende brengt de noodplanningscoördinator (NPC) op de hoogte**, die op zijn of haar beurt andere relevante actoren in kennis stelt, zoals de Federale Diensten van de Gouverneur en de gemeentelijke communicatie-ambtenaar. | Burgemeester | Algemeen directeur |
|  | Bepaal in overleg met de noodplanningsambtenaar of **opgeschaald dient te worden naar de gemeentelijk fase**, op basis van relevante indicatoren. Denk hierbij aan afwegingen als ...     1. De mate waarin de impact op inwoners en andere specifieke doelgroepen direct merkbaar is 2. De mate waarin men kan inschatten hoelang het incident kan duren 3. De waarschijnlijkheid dat gevoelige gegevens gecompromitteerd zijn 4. De nood aan een duidelijk afgestemde crisiscommunicatie waarbij alle diensten en disciplines nauw betrokken zijn |  |  |
|  | **Duid een secretaris of notulist aan** en hou alle handelingen bij in een logboek.   1. Indien gemeentelijke fase ANIP afgekondigd: ICMS (opstart via NC112). 2. Indien geen gemeentelijke fase: maak gebruik van een alternatief, al dan niet zelf-ontwikkeld, logboek waarin gebeurtenissen bijgehouden kunnen worden. |  |  |
|  | Zorg ervoor dat het **Gemeentelijk Coördinatiecomité (GCC) of Crisis Management Team klaarstaat** en afdoende geïnformeerd is voor de opstart van de crisiswerking. Binnen een minimale samenstelling kan gekozen worden voor volgende vertegenwoordigers:    1. Crisismanager (voorzitter van de vergadering) 2. Secretaris/notulist (logboek) 3. Diensthoofd IT 4. Diensthoofd Communicatie 5. Coördinator Noodplanning 6. Diensthoofd HR (overzicht van aantal en kwalificaties medewerkers in organisatie) 7. Preventieadviseur   Waar nodig - of gebruikelijk - kan aangevuld worden met bijkomende profielen. Denk aan:   1. Coördinator Logistiek, Facilitair beheer, Technische dienst (gebouwen, voorraden) 2. Een deskundige met juridische vorming of achtergrond, in kader van schadeclaims en strafonderzoek. 3. Coördinator Financiën, in kader van contracten, facturen, uitkeringen, verzekering, ... 4. Coördinator voor specifiek zwaar getroffen of vitale diensten: OCMW, RVT,… |  |  |
|  | **Leg de frequentie vast waarbinnen het Gemeentelijke Coördinatiecomité (GCC) of Crisis Management Team samenkomt**, op dag 1 van de crisis kunnen meerdere overleggen aangewezen zijn. Een goede informatiedoorstroom vanuit de diensthoofden is hierbij cruciaal, maar men kan ook overwegen om het volledige MAT actief binnen het GCC te betrekken. |  |  |
|  | **Verhoog de beschikbare menselijke capaciteit** en schakel bij incidenten met hoge urgentie **externe expertise** in. Dit kan zowel voor het stoppen van de cyberaanval, het onderzoek naar de oorsprong of de heropstart van de IT-omgeving. Het kan hierbij gaan over externe toeleveranciers met ervaring op vlak van incident response of bestaande partnerschappen met andere lokale besturen. Het betrekken van externe expertise is geen falen van de IT-dienst, maar een blijk van een correcte inschatting van de complexiteit van het incident. |  |  |
|  | **Neem volgend op het initieel forensisch onderzoek maatregelen om de scope en impact van het incident onder controle te houden, bijvoorbeeld:**   1. Verander mogelijk gecompromitteerde wachtwoorden 2. Staak de exploitatie van een gecompromitteerde applicatie of server 3. Gebruik een virus- of spywarescanner om kwaadaardige bestanden en services te verwijderen 4. Werk handtekeningen bij 5. Schakel aangetaste gebruikersaccounts uit 6. Identificeer en verhelp aanwezige kwetsbaarheden 7. Verwijder de actieve en opgeslagen inhoud en verzoek om verwijdering van de gecachte of in proxy opgeslagen webpagina‘s, die geïndexeerd zijn door zoekmachine bedrijven en andere Internet-archief bedrijven. Denk hierbij aan incidenten waarbij gevoelige gegevens onjuist geplaatst werden op publiek toegankelijke websites. |  |  |
|  | **Bepaal of je systemen al dan niet afschakelt tijdens het incident.** Door systemen niet meteen los te koppelen of uit te schakelen kan in een latere fase informatie uit het geheugen gehaald worden voor verder onderzoek. Dit kan echter ook de deur openen voor bijkomende schade. Deze beslissing kan genomen worden op basis van volgende criteria:   1. Wat kan er gebeuren als het incident niet onder controle raakt? 2. Brengt de aanval of inbreuk onmiddellijke, zware schade toe? 3. Is er (mogelijke) schade aan en/of diefstal van activa? 4. Is het nodig om bewijzen bij te houden? Zo ja, welke bronnen van bewijsmateriaal moet de organisatie verzamelen? Waar worden deze opgeslagen? Hoe lang moet het bewijsmateriaal worden bewaard? 5. Is het nuttig dat de hacker voorlopig niet weet dat hij gedetecteerd werd? 6. Is de beschikbaarheid van diensten essentieel of is het aanvaardbaar om het systeem offline te brengen. |  |  |
|  | **Bepaal of je de server(s) zolang mogelijk aan laat staan of dat je overgaat tot uitschakelen en loskoppelen.** Het is aanbevolen om uitschakeling en loskoppeling maximaal uit te stellen, aangezien cruciaal bewijsmateriaal verloren kan gaan of de hacker gealarmeerd kan worden.  Indien op een gegeven moment desalniettemin beslist wordt om af te schakelen, is dit een mogelijke volgorde voor een virtueel lokaal bestuur dat grotendeels on-premise werkt:   1. Back-upservers: deze zijn cruciaal voor de herstelfase en het is dan ook essentieel om deze te vrijwaren voor (verdere) schade 2. Citrix-servers voor virtuele desktops 3. Applicatieservers voor verschillende toepassingen 4. Emailservers 5. File-en-printservers 6. Domeinservers (gebruikersbeheer): dit vereist wel dat de IT-dienst nog lokale accounts ter beschikking heeft, die niet gekoppeld zijn aan een domein   Er zijn echter evenzeer servers die je voorlopig online kan laten, omdat ze kunnen helpen om de besmetting op te sporen en te monitoren of omdat het over vitale functies gaat. Denk aan:   1. Firewallservers 2. Anti-virusservers 3. Monitoringservers 4. Telefonieservers (VOIP) |  |  |
|  | **Laat eindgebruikers hun toestellen uitschakelen.** Zowel op desktops, als laptops, tablets en andere toestellen dienen gebruikers hun sessie af te melden en de apparatuur volledig uit te schakelen. Dit kan gecommuniceerd worden via het regulier crisiscommunicatiekanaal, zoals een interne Whatsappgroep, instructiefiches, … |  |  |
|  | **Focus op de verschillende netwerken en netwerksegmenten.** Schakel de draadloze netwerken zoveel mogelijk uit en installeer tools - eventueel in samenwerking met externe experten - die diepgaand de verkeerstromen monitoren. Vertrek in eerste instantie van een whitelist waardoor enkel gekend en noodzakelijk verkeer mag bewegen tussen adressen en poorten. |  |  |
|  | **Richt een snel, veilig en bruikbaar communicatiekanaal op** of maak gebruik van een gepast bestaand kanaal voor communicatie naar alle interne diensten en stakeholders, zoals een Whatsappgroep voor belangrijke mededelingen. |  |  |
|  | Zorg ervoor dat de **interne medewerkers binnen de gangbare communicatiestructuren als eerste geïnformeerd worden** over de crisissituatie en zorg er doorheen het volledige proces voor dat medewerkers steeds als eerste informatie krijgen over nieuwe ontwikkelingen, om zo het draagvlag hoog te houden. |  |  |
|  | Nadat interne medewerkers op de hoogte werden gebracht is het aangeraden om **zelf over de crisis te communiceren naar de buitenwereld**. Door deze ‘stealing thunder’ strategie toe te passen behoud je controle over de perceptie en kan je voorkomen dat foutieve interpretaties of veronderstellingen een eigen leven gaan leiden. In eerste instantie zal de communicatie zich hoogstwaarschijnlijk tot algemene procesinformatie beperken. |  |  |
|  | **Voor de communicatiestrategie wordt best gewerkt op basis van een** [**bestaand crisiscommunicatieplan**](https://www.vvsg.be/kennisitem/vvsg/sjabloon-crisiscommunicatieplan), met een bijhorende contactenlijst, overzicht van de beschikbare communicatiekanalen en leidraden die helpen om snel tot de juiste boodschap te komen. Indien nog geen plan voorhanden is, kan men zich baseren op de aanpak bij eerdere crisissituaties. |  |  |
|  | **Spreek een aanspreekpunt binnen de IT-dienst af voor interne en externe communicatie gedurende de crisissituatie.** Kijk hierbij naar een diensthoofd of ervaren medewerker die moeilijke technische zaken behapbaar kan uitleggen. |  |  |
|  | **Werk duidelijke interne communicatielijnen uit** waarbij medewerkers - idealiter via hun respectievelijk diensthoofd - vragen kunnen richten aan management, die op hun beurt zorgen voor een triage van vragen en deze voorleggen aan de correctie dienst of werkcel. |  |  |
|  | **Zorg in overleg met de IT-dienst voor instructiefiches naar personeel** om nieuwe aanvallen of bijkomende schade te vermijden, denk hierbij aan het niet meebrengen van eigen hardware. |  |  |
|  | **Leg een lijst met Frequently Asked Questions aan** waarbij antwoorden uitgeschreven worden voor veelgestelde vragen, om te vermijden dat het aantal interne en externe ad-hoc vragen te hoog oploopt. |  |  |

**3.Remediëring en herstel**

Na de opstart van het crisisbeheer dient de oorzaak van het incident geblokkeerd of verwijderd te worden, en moeten de nodige stappen gezet worden om de impact op de dienstverlening of veiligheid van gevoelige gegevens in te dammen. Daarnaast moet gekeken worden hoe bedrijfsprocessen veilig herstart kunnen worden indien deze gestopt werden en op welke wijze verdere risico’s en escalaties gemitigeerd kunnen worden. Bedrijfscontinuïteit en heropstart staan centraal in deze fase.

|  |  |  |  |
| --- | --- | --- | --- |
| Gedaan | Taakomschrijving | Uitvoerend | Verantwoordelijk |
| Badge Tick1 met effen opvulling | **Tracht de beschikbaar menselijke capaciteit zoveel mogelijk op te schakelen.** Doe indien mogelijk beroep op expertise en bijstand van naburige lokale, provinciale en federale overheden, private partners, … Dit geldt voor het IT-technische luik, maar evenzeer voor communicatiegerelateerde, organisatiegerichte en juridische aspecten. | Diensthoofden | MAT |
|  | **Definieer impactclusters met de afdelingshoofden.** Door impactclusters te definiëren kan je een structuur voor crisisbeheer uitwerken waarbinnen diensten en stakeholders gericht kunnen werken, prioriteiten bepaald kunnen worden en **werkcellen opgericht kunnen worden** die zich ontfermen over hun respectievelijke impactcluster(s).  Deze clustering kan gebeuren op basis van een bestaande afdelingsstructuur, maar ook andere clusters zijn mogelijk indien dit het toewijzen van verantwoordelijkheden faciliteert. In gemeente Willebroek koos men bijvoorbeeld voor de clusters sociaal (omvat o.a. het woonzorgcentrum en de OCMW-werking), diensten (omvat technische en administratieve dienstverlening als de onthaalbalie, burgerzaken en vergunningen), vrije tijd (omvat o.a. de bibliotheek en evenementen) en externen (omvat o.a. externe organisaties als VDAB en CAW). |  |  |
|  | **Prioriteer tussen de gehanteerde impactclusters** op basis van de aanwezigheid van kritische processen, termijn-gebonden diensten en producten en de nood aan een duidelijk platform binnen het crisisbeheer. Een reeds bestaande [business impact analyse](https://overheid.vlaanderen.be/toolbox/toolbox-bedrijfscontinu%C3%AFteitsmanagement-bcm/stappenplan/stap/2) of [business continuïteitsplan](https://www.vvsg.be/kennisitem/vvsg/sjabloon-business-continuiteitsplan) kan dit proces faciliteren. |  |  |
|  | **Lijst per werkcel de kritieke instellingen of diensten** **op** (zoals de medicatiegegevens bij de woonzorgcentra of de betaling van leeflonen door het OCMW) **en de kritieke processen** (zoals betalingen, stockbeheer en vergunningen) voor de verschillende impactclusters. Wijs daarnaast concrete taken toe aan de werkcellen voor hun respectievelijke impactcluster. |  |  |
|  | **Focus binnen de werkcellen op remediëring op korte termijn**, maar werk daarnaast ook op problemen die op lange(re) termijn zouden kunnen opduiken. |  |  |
|  | **Upgrade het GCC of Crisis Management Team** **en medewerkers die instaan voor kritische dienstverlening**. Tot dusver hebben zij enkel gewerkt met pen en papier omdat alle computers als verdacht worden beschouwd tot het tegendeel blijkt. Nu is het zaak hen bv. van laptops met 4G-verbinding (per toestel of via routers) te voorzien of printers ter beschikking te stellen (met USB-kabels). Informatie kan worden opgevraagd via USB-sticks en USB-harde schijven - die na elke update van informatie telkens volledig werden gescand - en/of via cloudopslag met strenge beveiliging (bv. OO-drive, TresorIT). |  |  |
|  | **Activeer een reeks emailadressen op een emaildomein voor basis werkgerelateerd mailverkeer** die gebruikt kunnen worden door medewerkers die instaan voor kritische dienstverlening. |  |  |
|  | **Zorg ervoor dat de netwerkomgeving onder controle is en onder verscherpt toezicht staat.** Alle gecapteerde informatie dient weggeleid te worden naar een beveiligde locatie voor latere analyse. |  |  |
|  | **Onderzoek de noden voor een gedeeltelijke heropstart van de dienstverlening binnen het GCC, Crisis Management Team of de werkcellen.** Kijk bijvoorbeeld of niet-geïmpacteerde laptops aangeschaft of ingezet kunnen worden en luister naar medewerkers om bijkomende noden te identificeren. |  |  |
|  | **Definieer** binnen de werkcellen op basis van een aanwezige producentencatalogus of andere beschikbare documentatie met diensten en producten, zoals een [business continuïteitsplan](https://www.vvsg.be/kennisitem/vvsg/sjabloon-business-continuiteitsplan), **welke diensten nog aangeboden kunnen worden in reguliere of licht gewijzigde vorm.**  Kijk op basis van de continuïteitsoefening welke diensten of medewerkers momenteel hun taken niet kunnen uitvoeren en schakel hen waar mogelijk in op andere diensten waar continuïteit van dienstverlening prioritair is. |  |  |
|  | **Werk voor prioritaire diensten alternatieve processen of methodieken uit.** Denk hierbij aan doorverwijzing naar partners voor de opmaak van bepaalde documenten en attesten of dienstverlening binnen een uitwijklocatie die reeds vastgelegd werd bij het opmaken van [bestaande draaiboeken](https://www.vvsg.be/kennisitem/vvsg/draaiboek-cybercrime) of noodplannen. |  |  |
|  | **Tracht de situatie en vooruitgang binnen het lokaal bestuur in kaart te brengen via een gekende methodiek** als een Feiten-Acties-Noden-bord (FAN) of een andere visuele uitwerking die het mogelijk maakt om overzicht te houden. |  |  |
|  | **Maak werk van een gefaseerde heropstart van servers, één voor één.** Gebruik hierbij bijvoorbeeld de omgekeerde volgorde van die in kader van de afschakeling. Volg daarbij een vast stramien:    1. Neem eerst een snapshot van de “oude” (vermoedelijk geïnfecteerde) machine. 2. Start de server op. Neem controle als administrator van de computer. 3. Gebruik detectietools om sporen van infectie terug te vinden. Inventariseer deze met het oog op bewijsgaring. Heb bijzondere aandacht voor indicatoren die kunnen wijzen op gegevensverlies of datalekken. Werk hiervoor samen met de DPO, politie, andere (interne) experten, … 4. Gebruik opschoonsoftware om na akkoord de server te reinigen. Indien niet zeker of alles gewist is, dan wel of het niet lukt, overweeg om een eerdere back-up terug te zetten. 5. Verklaar de machine terug in dienst, met de een melding of deze 100% operationeel is, of er bijzonderheden zijn (zoals dataverlies). |  |  |
|  | **Aanvullend op de gefaseerde heropstart van servers kan ingegaan worden op het gebruikersbeheer via domeincontrollers:**   1. Zet eerst alle gebruikers, behalve de IT-administratoren, uit. 2. Vooraleer een gebruiker terug mag aanmelden in het domein moet het wachtwoord gereset worden. Geef indien nodig een éénmalige code die bij eerste inlogpoging meteen gewijzigd dient te worden. 3. Breng de gebruikers gefaseerd terug in dienst. Eerst IT-administratoren, dan leden van het Crisis Management Team, medewerkers die instaan voor kritische dienstverlening, …, in functie van hun belang voor de crisisbestrijding en het continuïteitsherstel. |  |  |
|  | **Zorg voor een goede wisselwerking tussen het herstel van de schade en het opschonen enerzijds, en het heropstarten van de kritische werking** (continuïteit) anderzijds. Ingeval er conflicten zijn of zich voordoen, worden deze aangekaart door het diensthoofd binnen het GCC of Crisis Management Team. |  |  |
|  | **Controleer bestaande niet AD-gelinkte toegangen**, zodat gekeken kan worden of de hackers via deze weg nog toegang hebben tot systemen en toepassingen. Zorg ervoor dat de wachtwoorden vernieuwd worden of maak nieuw accounts aan indien nodig. Dit geldt zeker wanneer wachtwoorden gelekt of achterhaald werden. |  |  |
|  | **Werk een protocol uit voor toestellen voor eindgebruikers die terug in dienst worden gesteld**, met stappen als een controle door antivirus- en antimalware. Indien nodig of gewenst kan een volledige herformattering hieraan voorafgaan. |  |  |
|  | De kans is reëel dat reguliere mailadressen niet langer beschikbaar zijn gedurende de crisissituatie. Waar nodig kunnen voor het waarborgen van dienstverlening in specifieke diensten **nieuwe mailadressen uitgewerkt worden om basis werkgerelateerd mailverkeer mogelijk te maken** tussen de diensten onderling en met relevante externe partners. |  |  |
|  | **Leg vast wanneer de afschaling van de crisisfase kan gebeuren**, door deze te koppelen aan specifieke modaliteiten, zoals 100% kans dat geen verdere escalaties kunnen voorkomen. |  |  |

**4.Kennisgeving**

Bepaal welke gevoelige gegevens mogelijk zijn blootgesteld door het incident en zorg ervoor dat de getroffenen hiervan op de hoogte zijn. Kennisgeving kan ook aan de orde zijn indien kritieke dienstverlening naar burgers toe in het gedrang komt ten gevolge van het incident. Snelheid is aan de orde indien er persoonsgegevens verloren zijn gegaan of bekend geworden zijn bij niet rechthebbenden. Dit houdt in dat de Vlaamse Toezichtscommissie (VTC) en Gegevensbeschermingsautoriteit (GBA) op de hoogte gebracht dienen te worden indien aan de bijhorende voorwaarden voldaan is. Snelheid is ook belangrijk vanuit een PR-oogpunt, om mogelijke reputatieschade in te perken.

|  |  |  |  |
| --- | --- | --- | --- |
| Gedaan | Taakomschrijving | Uitvoerend | Verantwoordelijk |
| Badge Tick1 met effen opvulling | **Neem beslissingen rond het informeren van getroffenen** op basis van de bevindingen van het Crisis Management Team, de IT-dienst, functionaris gegevensbescherming en/of veiligheidsconsulent.Is het risico op blootstelling zo groot dat informeren noodzakelijk is? Gaat het over een incident met betrekking tot persoonsgegevens waarbij een aanzienlijke kans bestaat op ernstige nadelige gevolgen voor de betrokkenen? | DPO | Algemeen directeur |
|  | **Verzamel de naam en adresgegevens van getroffenen**, denk hierbij aan slachtoffers van een datalek en inwoners waarvoor geen of slechts beperkte dienstverlening mogelijk is, en zorg ervoor dat zij zo snel mogelijk verwittigd worden. Zorg er tevens voor dat de verzamelde data veilig wordt behandeld, verstuurd en opgeslagen. |  |  |
|  | **Maak melding bij de Vlaamse Toezichtcommissie (VTC) en de Gegevens Beschermingsautoriteit (GBA)** indien het incident gepaard gaat met een datalek dat een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Dit geldt ook indien data niet gelekt werd, maar wel tijdelijk onbeschikbaar was. Wanneer het incident een datalek inhoudt ben je wettelijk verplicht om hiervan aangifte te doen bij de bevoegde instanties. Verstuur de melding zo snel mogelijk na detectie en uiterlijk 72 uur na kennisname. |  |  |
|  | **Kies een geschikt communicatiemiddel voor het informeren van getroffenen.** Kijk hierbij naar de hoeveelheid te informeren personen, de grootorde van het risico en de mate waarin informatie gecompromitteerd is. Bij een datalek met een groot aantal getroffenen, waarbij vele slachtoffers niet gekend zijn, kan het nuttig zijn om te kijken naar minde fijnmazige communicatiemiddelen, zoals een toegespitste website of -pagina. |  |  |
|  | **Win juridisch advies** in over de positie en aansprakelijkheid van de gemeente en de gekozen communicatiestrategie voor het informeren van getroffenen. |  |  |
|  | **Bereid de schriftelijke informatieverstrekking voor**, in samenspraak met management, de functionaris gegevensbescherming of veiligheidsconsulent en een juridisch expert. |  |  |
|  | **Bekijk intern** met alle betrokken diensten - directie, communicatie, DPO of CISO, ICT, … - **of de nodige meldingen gedaan werden** naar de VTC, GBA, politie, CERT en andere relevante instanties of organisaties. Verzamel alle beschikbare informatie over de verschillende meldingen, zodat deze makkelijk opgehaald kunnen worden in geval van vragen. |  |  |

**5.Evaluatie en rapportering**

Het is belangrijk bij crisissituaties om de cirkel rond te maken en lessen te trekken uit het incident en de bijhorende aanpak. Dit houdt in dat het incident besproken wordt met het team en andere relevante betrokkenen, maar ook dat in de nodige rapportering wordt voorzien en dat mogelijke verbeteringen aan de crisisaanpak doorgevoerd worden op basis van de recente crisissituatie.

|  |  |  |  |
| --- | --- | --- | --- |
| Gedaan | Taakomschrijving | Uitvoerend | Verantwoordelijk |
| Badge Tick1 met effen opvulling | **Verzamel gegevens met betrekking tot de werkzaamheden van het personeel dat heeft meegewerkt aan het crisisbeheer.** De totale kosten kunnen mogelijk van belang zijn indien er een rechtszaak komt tegen een verdachte, omdat deze dan mogelijk verhaald kunnen worden. De gegevens kunnen bovendien relevant bronmateriaal zijn voor geleerde lessen. | Personeelsdienst | Personeelsdienst |
|  | **Plan een vergadering ongeveer 2 tot 6 weken na het incident** om een evaluatie uit te voeren over de aanpak van het incident, dit kan met het Gemeentelijk Coördinatiecomité of Crisis Management Team, maar het kan ook relevant zijn om de bredere organisatie fysiek of digitaal te bevragen. Deze evaluatie wordt best gestructureerd aan de hand van enkele vragen, zoals:   1. Werden de aanpak en de procedures voor cyberveiligheidsincidenten gevolgd? Waren die geschikt? Moet bestaande plannen aangepast worden? 2. Was de informatie op tijd beschikbaar? Zo nee, zou het mogelijk zijn geweest om die sneller te hebben, en hoe? 3. Hebben de ondernomen stappen het herstel mogelijk verhinderd op de een of andere manier? 4. Kan het delen van informatie met andere organisaties verbeterd worden? 5. Welke oplossingen en maatregelen kunnen soortgelijke incidenten in de toekomst voorkomen? 6. Zijn er voortekens of indicatoren die men kan monitoren om soortgelijke incidenten in de toekomst gemakkelijker te detecteren? 7. Welke extra middelen zijn nodig om toekomstige cyberveiligheidsincidenten te detecteren, analyseren en beperken in impact? 8. Beschikt het lokaal bestuur over de nodige capaciteit en expertise om te reageren op cyberveiligheidsincidenten of moet gekeken worden naar een externe partner of nieuwe aanwervingen? |  |  |
|  | **Onderzoek oplossingen en beveiligingsmaatregelen om een herhaling van het incident te voorkomen** in de toekomst en hoe snel deze geïntegreerd kunnen worden. Giet de oplossingen in het [Veiligheids- en Opvolgingsplan](https://www.vvsg.be/kennisitem/vvsg/sjabloon-veiligheids-en-opvolgingsplan) om zo te verzekeren dat de maatregelen tijdig en correct geïmplementeerd worden. Bij het onderzoek dienen enkele vragen gesteld te worden, zoals:   1. Wat was de concrete aanleiding van het incident en hoe kon dit gebeuren? 2. Had het lokaal bestuur meer kunnen doen om de inbraak of intrusie te voorkomen? 3. Neemt het lokaal bestuur voldoende maatregelen om herhaling te voorkomen? 4. Krijgt cyberveiligheid voldoende aandacht binnen de strategie en budgettering van het lokaal bestuur? |  |  |
|  | **Het is belangrijk om elk incident en alle ondernomen acties in kader van het crisisbeheer te documenteren en de vergaarde informatie bij te houden.** Soortgelijke incidenten kunnen opnieuw plaatsvinden en vereisen mogelijk dezelfde processen, of een klein incident kan een onderdeel blijken van een groter incident dat later ontdekt wordt. Indien het incident samengaat met een inbreuk op de bescherming van persoonsgegevens, is het cruciaal dat hiervan een overzicht bijgehouden wordt. |  |  |
|  | **Werk op basis van de notulen en nabespreking een verslag uit van het incident**, dat als naslagwerk kan dienen voor het eigen lokaal bestuur, maar ook voor andere externe instanties die kunnen leren uit de crisisaanpak. |  |  |
|  | **Zorg ervoor dat het incident aan bod komt in het jaarverslag** van de functionarisgegevensbescherming en andere processen die de incidenten binnen het lokaal bestuur in kaart brengen en bespreekbaar maken. Zo kan ook op termijn gekeken worden of de geplande acties naar aanleiding van het incident daadwerkelijk geïmplementeerd werden. |  |  |

**6.Bronvermelding**

* **Cyber Security Coalition en Centre for Cyber Security Belgium**, *Cyberveiligheid, gids voor incidentenbeheer*, 2016 | Geraadpleegd via <https://www.cybersecuritycoalition.be/nl/resource/incident-management-guide/>
* **Gemeente Willebroek**, *Rapport Cyberaanval Willebroek*, 2020 | Geraadpleegd via <https://www.vvsg.be/kennisitem/vvsg/rapport-cyberaanval-gemeente-willebroek>
* **Verbond van Belgische Ondernemingen**, *Crisis Management, een praktische leidraad voor een doeltreffend crisisbeheer*, 2015 | Geraadpleegd via <https://www.vbo-feb.be/globalassets/publicaties/crisismanagement--praktische-leidraad-voor-een-doeltreffend-crisisbeheer/crisismanagement_nl.pdf>
* **Vereniging van Nederlandse Gemeenten en Informatiebeveiligingsdienst voor gemeenten**, licentie onder: CC BY-NC-SA 4.0., *Voorbeeld Incidentmanagement en Response Beleid*, 2019 | Geraadpleegd via <https://www.informatiebeveiligingsdienst.nl/product/voorbeeld-incidentmanagement-en-response-beleid-2/>