

Handreiking Incident- en response management

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

Colofon

### Naam document

Incident en response management

### Versienummer

2.2

### Versiedatum

September 2021

### Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).



Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD) (2018)

Tenzij anders vermeld, is dit werk verstrekt onder een Creative Commons Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal licentie. Dit houdt in dat het materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden: Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. De IBD wordt als bron vermeld;
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de IBD en / of de Vereniging van Nederlandse Gemeenten;
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer dit werk wordt gebruikt, hanteer dan de volgende methode van naamsvermelding: “Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten”, licentie onder: CC BY-NC-SA 4.0.

Bezoek <http://creativecommons.org/licenses/by-nc-sa/4.0> voor meer informatie over de licentie.

### Rechten en vrijwaring

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

### Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

### Wijzigingshistorie

|  |  |  |
| --- | --- | --- |
| Versie | Datum | Wijziging / Actie |
| 1 | Juli 2013 | Initiële versie |
| 1.01 | Augustus 2015 | Kleine tekstuele wijzigingen |
| 1.1 | December 2015 | Aanpassing i.v.m. WBP |
| 1.1.1 | Augustus 2016 | Taskforce BID verwijderd |
| 2.0 | December 2018 | BIO Update, AVG update |
| 2.2 | September 2021 | Update n.a.v. GGI-veilig, GRN, incidenten en andere ontwikkelingen |

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

**Doel**

Het doel van dit document is om een handreiking te zijn voor het inrichten van het incident en response management proces.

**Doelgroep**

Dit document is van belang voor de CISO, de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

**Relatie met overige producten**

* Baseline Informatiebeveiliging Overheid (BIO)
* Verhogen Digitale Weerbaarheid[[1]](#footnote-1)
* Informatiebeveiligingsbeleid van de gemeente
* Handreiking patchmanagement voor gemeenten
* Handreiking proces wijzigingsbeheer
* Handreiking proces configuratiebeheer
* Handreiking patchmanagement voor gemeenten
* Factsheet Incident management
* Bedrijfscontinuïteitbeheer[[2]](#footnote-2)
* Coordinated Vulnerability Disclosure
* Factsheet: gehackt en nu verder

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

6.1.1.1 Verantwoordelijkheden zijn vastgelegd door leiding van de organisatie

7.1.2.1 Alle medewerkers zijn gewezen op hun verantwoordelijkheid omtrent informatiebeveiliging

7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid om bedrijfsinformatie te beschermen en kennen de regels en verplichtingen

9.4.4.2 Het gebruik van systeemhulpmiddelen wordt gelogd

11.1.2.1 Waarschuwingen van concrete beveiligingsrisico’s worden gedeeld met relevante collega’s

12.3.1.2 Risicoafweging voor maximale dataverlies en maximale hersteltijd

12.4.2 Bescherming van informatie in logbestanden

12.4.2.2 Risicoafweging voor bewaarperiode van logging

12.6.1 Beheer van technische kwetsbaarheden

15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

H16 Beheer van informatiebeveiligingsincidenten

Managementsamenvatting

Deze handreiking beschrijft de uitgangspunten en bijhorende processtappen voor het incident management- en respons proces. Omdat 100% informatieveiligheid niet bestaat zullen incidenten plaatsvinden. Het hebben van een goed incident management- en respons proces kan de impact daarvan verkleinen, omdat adequaat gereageerd kan worden en de schade en impact hierdoor minimaal kunnen blijven. Daarnaast leidt het proces ertoe dat lering wordt getrokken van incidenten, waardoor de kans op herhaling ook wordt verkleind. Alle medewerkers zijn verantwoordelijk voor informatiebeveiliging en dienen een incident te kunnen herkennen en weten waar ze dat moeten melden.

Gemeenten zijn zelf verantwoordelijk voor het goed inrichten van het incidentmanagementproces en kunnen bij incidenten om advies vragen bij de IBD. Ook kan in sommige gevallen de IBD (online) aansluiten bij het crisisteam en ook ondersteuning leveren op het gebied van woordvoering. De IBD kan voor tijdelijke ondersteuning van een getroffen gemeente in de warme fase hulp inroepen van andere gemeenten via het Gemeentelijk Response netwerk (GRN) op basis van bijvoorbeeld een zoekprofiel. De IBD is 24/7 bereikbaar voor gemeenten bij spoed als gevolg van een incident.

Er zijn verschillende type incidenten die allemaal een prioritering dienen te krijgen, de impact en de urgentie van het incident bepaalt welke prioritering toegekend wordt. Het eerste uur na ontdekking van een incident is cruciaal. Er moet zo min mogelijk impact zijn van het incident zonder dat er informatie over het incident verloren gaat. Dit is namelijk nodig om later een goed onderzoek te kunnen doen naar de oorzaak van het incident.

Binnen het incidentmanagementproces wordt gewerkt met protocollering en besluitvorming volgens een vaste aanpak die afgeleide is van de BOB-aanpak van de veiligheidsregio’s. De besluitvorming aanpak is gebaseerd op en de gebruikte notatiewijze is BOBOC. Dit staat voor Beeldvorming, Opties, Besluit, Opdracht en Controle.

Incident management wordt binnen veel disciplines uitgevoerd, maar kent altijd een bepaalde vergelijkbare aanpak langs stappen die doorlopen moeten worden, de incident response actie. Andere disciplines zijn bijvoorbeeld cybergevolg bestrijding (G4), de Good practice guide for incident management, de CSIRT maturity toolkit. Naast deze meer op cyber gerichte aanpakken kan het zijn dat een incident uitmondt in een calamiteit met uitstraling naar de fysieke ruimte, in dat geval kan besloten worden om op te schalen naar een GRIP situatie maar ook om op basis van een GRIP aanpak het gemeentelijk crisisteam te laten bijstaan of ondersteunen door specialisten van de veiligheidsregio in een GBT-achtige structuur.

Een incident response-actie bestaat uit de volgende stappen:

* Detectie
* Initiatie
* Analyse
* Inperken / indammen schade (insluiting en beperking)
* Oplossen
* Herstel
* Remediatie
* Afsluiten incident
* Evaluatie en rapportage

Inhoudsopgave

[1. Inleiding 7](#_Toc82647472)

[1.1. Doelstelling incident management 7](#_Toc82647473)

[1.2. De indeling van het document is als volgt: 7](#_Toc82647474)

[2. Incidentmanagement 8](#_Toc82647475)

[2.1. Wat is het 8](#_Toc82647476)

[2.2. Waarom doen we dit 8](#_Toc82647477)

[2.3. Voorkomen is beter dan genezen 8](#_Toc82647478)

[2.4. Belang van incident management 8](#_Toc82647479)

[3. Het opzetten van incident management 9](#_Toc82647480)

[3.1. Incident management en respons beleid van de gemeente 9](#_Toc82647481)

[3.2. Incident management en respons proces 9](#_Toc82647482)

[3.3. Hoe te gebruiken 14](#_Toc82647483)

[4. Aandachtspunten 15](#_Toc82647484)

[4.1. Hoe begin ik? 15](#_Toc82647485)

[4.2. Metrieken / KPI’s 15](#_Toc82647486)

[4.3. GGI-Veilig 15](#_Toc82647487)

[4.4. Externe leveranciers 16](#_Toc82647488)

[4.5. Logging 16](#_Toc82647489)

[4.6. Personeel 16](#_Toc82647490)

[4.7. Voorbereiding 16](#_Toc82647491)

[4.8. Gouden uur 17](#_Toc82647492)

[4.9. De 7 gouden regels van incident management 17](#_Toc82647493)

[5. Incident Impact Leidraad 18](#_Toc82647494)

[5.1. Incident Impact bepaling 18](#_Toc82647495)

[5.2. Teamsamenstelling crisisteam 19](#_Toc82647496)

[5.3. Agenda voorbeeld 20](#_Toc82647497)

[Bijlage 1: Incident management en response stappenplan en sjabloon 21](#_Toc82647498)

[Bijlage 2: Incidentenprocedure informatiebeveiliging 36](#_Toc82647499)

[Bijlage 3: Incidenten en meldingsniveau matrix 37](#_Toc82647500)

[Bijlage 4: Definities 40](#_Toc82647501)

[Bijlage 5: Incident management en response beleid gemeente <gemeente> 43](#_Toc82647502)

# Inleiding

Incident management is een proces dat een belangrijk instrument is bij het indammen van schade en voorkomen van erger als er informatiebeveiligingsincidenten optreden. Het hebben van een goed lopend incidentmanagementproces is cruciaal om schade voor de gemeentelijke bedrijfsprocessen te beperken. Het proces bestaat uit het tijdig identificeren en oplossen, en het achteraf leren van een incident, zodat de impact laag en kans op herhaling minimaal is. Het gaat bij informatiebeveiliging om informatiebeveiligingsincidenten die betrekking hebben op de informatievoorziening. Men spreekt men ook wel over Computer Security Incident management of cyber security incident management. Waar in dit document gesproken wordt over Computer Security Incident management of cyber security incident management bedoelen we hetzelfde als incident management en response of in het kort incident management. Het primaire doel is de ontwikkeling van een goed begrepen en voorspelbare reactie op schadelijke gebeurtenissen in de meest brede zin van het woord.

Gemeenten moeten zich bewustzijn van hun verantwoordelijkheden als het gaat om het verwerken van, en het beschermen van deze informatie ten behoeve van hun burgers en ketenpartners. Deze verantwoordelijkheid strekt zich uit tot het hebben van een draaiboek voor ‘wat te doen, als er iets misgaat’. Dit kunnen ook draaiboeken zijn voor soorten incidenten die een bepaalde standaard aanpak vergen of die vaker voorkomen.

## Doelstelling incident management

Incident management is belangrijk omdat 100% beveiligen niet bestaat, niet alle incidenten zijn te voorkomen. Het is niet de vraag óf er iets gaat gebeuren maar wanneer. De belangrijkste te verwachte incidenten kunnen van tevoren bedacht worden en de bijpassende reactie en escalatieprocedure kan dus ook van tevoren uitgewerkt worden in een draaiboek en geoefend worden. Het incident managementproces heeft dan ook als doel om verstoringen zo snel mogelijk te verhelpen en nieuwe verstoringen in de toekomst te voorkomen. Als er sprake is van uitbesteding dan dienen er goede contractuele afspraken gemaakt te worden omdat de leverancier op basis van prioriteit kwetsbaarheden snel moet oplossen.

Het inrichten van incident management in het kader van informatiebeveiliging is een verplichting vanuit de BIO (hoofdstuk 16). Incident management is een essentieel proces voor een snelle reactie op, en verhelpen van informatiebeveiligingsincidenten.

Incidenten staan vaak niet op zichzelf en kunnen een uitwerking hebben naar andere processen of ketenpartners. Sommige incidenten doen zich niet bij één gemeente voor maar bij meerdere. Een incident moet behalve intern opgelost soms ook extern geëscaleerd worden zodat anderen gewaarschuwd kunnen worden en waardoor de impact van het incident zo klein als mogelijk gehouden kan worden. Extern escaleren gebeurt naar de IBD, zij hebben het overzicht, de contacten en de middelen om andere (keten)partners en gemeenten snel te kunnen waarschuwen en ook hebben zij een directe ingang bij het Nationaal Cyber Security Centrum (NCSC).

## De indeling van het document is als volgt:

Hoofdstuk 2 gaat over het incident management- en response proces waarin is toegelicht dat het proces bestaat uit: detectie, initiatie, analyse, indamming, oplossen, herstel, remediatie, afsluiten, evaluatie en rapportage. Hoofdstuk 2 volgt ook zoveel als mogelijk deze processtappen, die ook te vinden zijn in bijlage 1. Hoofdstuk 3 beschrijft verschillende aspecten die bij dit proces komen kijken zoals logging en het gouden uur. Hoofdstuk 4 gaat in op de verschillende prioriteringen die bij incidenten komen kijken. Afhankelijk van de urgentie en impact dient een incident als hoog of juist lager te worden geprioriteerd. Verder zijn in dit document een aantal bijlagen toegevoegd: een stappenplan/sjabloon, een procedurebeschrijving, een incidenten meldingsniveau matrix, definities en voorbeeld incident en response beleid.

# Incidentmanagement

## Wat is het

Een incident, in het kader van incident management, is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incident management is het geheel van organisatorische maatregelen dat ervoor moet zorgen dat een incident adequaat gedetecteerd, gemeld en behandeld wordt om daarmee de kans op uitval van bedrijfsvoering processen of schade ontstaan als gevolg van het incident te minimaliseren, dan wel te voorkomen. In dit document lijkt het alsof incident management voor beveiligingsincidenten iets nieuws is, maar dat is maar ten dele waar. Vaak is binnen een organisatie al incident management gericht op IT ingericht of bijvoorbeeld voor calamiteiten in de openbare ruimte, probeer daarop mee te liften in plaats van iets nieuws op te tuigen. Dit hoofdstuk volgt de stappen uit bijlage 1 en bevat daarnaast veel achtergrondinformatie passend bij de stappen van het incident managementproces. In hoofdstuk 3 is alle achtergrondinformatie opgenomen die niet direct met het proces te maken hebben, maar die wel van belang zijn om te weten als het proces ingericht wordt.

## Waarom doen we dit

Een succesvolle incident en response reactie bestaat uit een aantal te doorlopen stappen. Deze stappen zijn voor ieder incident gelijk.

De volgende informatie is bedoeld als een algemene checklist en een stappenplan die een gemeente kunnen helpen in de voorbereiding en het inrichten van een incidentmanagementproces. Er bestaan andere checklists en deze kunnen ook al in gebruik zijn. Dit document kan nuttig zijn voor iedereen, als een herziening van paraatheid of als een routekaart voor ontwikkeling. De eigenaar van het incident management en response proces is de incidentmanager. De rol van incidentmanager kan door verschillende personen worden uitgevoerd. De helpdesk heeft een nadrukkelijke rol bij het ontwikkelen van incident response reacties en bij de voorbereiding daarop.

Belangrijk is dat incidenten en uitgevoerde activiteiten worden vastgelegd voor latere evaluatie, woordvoering, bewijslast en dergelijke.

## Voorkomen is beter dan genezen

Uit onderzoek blijkt dat incidenten altijd zullen optreden en veel incidenten worden veroorzaakt door gebruikers- en bedien fouten. De kans dat incidenten optreden kan worden verkleind door een aantal maatregelen, hiervan hebben het opzetten van een bewustwording traject en opleidingen de grootste impact in het terugdringen van gebruiks- en bedien fouten. Daarnaast is het hebben van goede documentatie die ook onderhouden en gebruikt worden een belangrijk instrument.

## Belang van incident management

De IBD heeft in het kader van Verhogen Digitale Veiligheid 1 (VDW1) een tweetal mindmaps gepubliceerd. In de mindmap processen zijn de verschillende basismaatregelen uitgewerkt voor een aantal basisprocessen, waaronder ook voor het incidentmanagement proces.[[3]](#footnote-3) Deze mindmaps en gerelateerde documenten zijn te vinden op onze website en kunnen naast dit document gebruikt worden.

Het belangrijkste is:

* dat het incident management proces wordt ingebed in de gemeentelijke praktijk. Sluit zoveel als mogelijk aan bij bestaande ITIL procedures en laat incidenten altijd binnenkomen op het helpdesksysteem;
* voor incident management moeten procedures worden uitgewerkt en er moet rekening gehouden worden met onbeschikbaarheid van systemen en ICT middelen, zorg er dus voor dat procedures en telefoonlijsten ook offline beschikbaar zijn;
* zorg voor een logboek dat ook offline beschikbaar is en documenteer nauwkeurig de uitgevoerde acties en verder alles wat relevant is;
* richt een chatgroup in met deelnemers die direct geïnformeerd moeten worden bij een incident;
* leer van beveiligingsincidenten;
* zorg voor een actueel en gepubliceerde Coordinated Vulnerability Disclosure procedure (CVD).[[4]](#footnote-4)

De IBD is dag en nacht bereikbaar voor advies, maar bedenk dat incidenten op ieder moment van de dag kunnen plaatsvinden of opgemerkt worden. Richt dus ook bereikbaarheid buiten kantooruren in.

# Het opzetten van incident management

Incidentmanagement moet binnen de organisatie worden opgezet, het hebben van beleidsuitgangspunten en aansluitende processen en procedures zorgen ervoor dat voor iedereen duidelijk kan zijn hoe de gemeente omgaat met incident management. Vaak is binnen de gemeente incident management al aanwezig als ITIL-proces, in dat geval dient onderzocht te worden in hoeverre dat proces is aan te passen zodat ook beveiligingsincidenten worden geregistreerd en afgehandeld.

## Incident management en respons beleid van de gemeente

De hoeksteen van incident management en respons is het hebben van beleidsuitgangspunten, de volgende punten zijn hier van belang:

* Het incidentmanagementproces sluit zoveel als mogelijk aan bij bestaande ICT-beheer processen.
* De verantwoordelijkheden zijn vastgesteld.
* Incidenten worden ingedeeld naar ernst en impact en afhankelijk daarvan is er een aangepaste crisisteam samenstelling.
* Er zijn incident management procedures opgesteld.
* Incidenten worden regelmatig geoefend en hierover wordt gerapporteerd aan de directie.
* Het incident managementproces wordt gemeten.
* Incidenten worden gemeld bij de IBD.

In bijlage 5 is een voorbeeld tekst opgenomen voor dit beleid.

## Incident management en respons proces

### Opzetten van het proces en de documentatie

De procestappen van het incidentmanagementproces

Incident management doorloopt een aantal stappen die al of niet gecombineerd kunnen zijn. Onderstaand worden deze stappen uitgelegd. Stap 1 in het incidentmanagementproces is detectie, echter het incident is dan al gaande. Afhankelijk van de detectie bron en het soort incident kan er dus al langere tijd verlopen zijn tussen het incident en de detectie. Een voorbeeld hiervan is dat als je een APT hebt (niet een hackergroep) maar een Advanced Persistent Threat, dan kan deze tijd ook een jaar of meer zijn.

De volgende informatie is bedoeld als een algemene checklist en een stappenplan die een gemeente kunnen helpen in de voorbereiding en het inrichten van een incidentmanagementproces. Er bestaan andere checklists en deze kunnen ook al in gebruik zijn. Dit document kan nuttig zijn voor iedereen, als een herziening van paraatheid of als een routekaart voor ontwikkeling. De eigenaar van het incident management en response proces is de incidentmanager. De rol van incidentmanager kan door verschillende personen worden uitgevoerd. De helpdesk heeft een nadrukkelijke rol bij het ontwikkelen van incident response reacties en bij de voorbereiding daarop.

Belangrijk is dat incidenten en uitgevoerde activiteiten worden vastgelegd voor latere evaluatie, woordvoering, bewijslast en dergelijke.

Een incident response-reactie bestaat uit de volgende stappen:

* Detectie
* Initiatie
* Analyse
* Inperken / indammen schade (insluiting en beperking)
* Oplossen
* Herstel
* Remediatie
* Afsluiten incident
* Evaluatie en rapportage

Zie voor de checklist die binnen dit proces te gebruiken is bijlage 1.

### Detectie

Een incident kan verschillende risicobronnen hebben, dat wil zeggen dat incidenten kunnen ontstaan op verschillende plekken binnen de organisatie en daarmee is er ook een veelvoud aan bronnen waardoor de organisatie kan opmerken of er een incident is. De verschillende bronnen kunnen zijn:

* Applicatie, computer of netwerk vertraging.
* Een alert van een inbraakdetectiesysteem (IDS) of van het inbraak preventie systeem (IPS).
* Signalen van een data loss prevention system (DLP).
* Signalen van File Integrity Monitoring (FIM) systemen.
* Webfilters.
* Cloud access security broker (CASB).
* Signalen vanuit een SIEM/SOC systeem.
* Meldingen van gebruikers of partners.
* Tips.
* Aanwijzingen van een derde partij (CTI – Cyber threat intelligence)
* In de pers.
* Meldingen aan de servicedesk afkomstig van personeel

Deze signalen kunnen dus het incidentmanagementproces triggeren en komen doorgaans op een punt de organisatie binnen bij servicedesk of iets vergelijkbaars. Doorgaans liggen de eerste verdere stappen van het proces ook bij de servicedesk / helpdesk binnen ICT

### Initiatie

Vanaf het moment dat het er een vermoedelijk incident gemeld is die mogelijk ook nog aan de gang is dienen de eerste stappen te worden gezet. De eerste stap is erkennen dat er een beveiligingsincident is gebeurd of gaande is. Afhankelijk van het soort incident moeten bepaalde functionarissen een melding krijgen. In ieder geval is dat de IT-manager en mogelijk de CISO en het Incident Respons Team. Er kan hier in het proces ook een Incident Respons Manager of Incidentmanager worden aangewezen, een Incidentmanager is een persoon die de noodzakelijke stappen zet om het incident op te kunnen lossen, communicatie op te zetten en het incident responsteam aan te sturen. Dit kan dus iemand anders zijn dan servicedesk personeel, de IT-manager of de CISO.

Het is raadzaam om in deze fase het incident aan te melden bij de IBD, dit omdat ook andere gemeenten gewaarschuwd zouden moeten worden en ook omdat de IBD incidenten registreert voor het landelijke beeld van opgetreden incidenten. In ieder geval moet de IBD gebeld worden bij incidenten met grote impact op de dienstverlening van de gemeente. Dit is ook het moment waar de IBD actief de getroffen gemeente kan ondersteunen door bijvoorbeeld (online) deel te nemen in het crisisteam van de gemeente of door het geven van (woordvoerings-)advies.

In deze fase wordt ook gestart met het vastleggen van de genomen stappen in een logboek.

### Analyse

De analyse fase in het incidentmanagementproces is ervoor beschikbare informatie te onderzoeken om vast te stellen met wat voor soort incident men te maken heeft.

Op het moment dat een (digitaal) informatiebeveiligingsincident wordt opgemerkt moeten er keuzes gemaakt worden op basis van urgentie en impact. Om het triage proces te ondersteunen kan bij een beginnend incident eventueel gebruik gemaakt worden van triage ondersteuning door een externe partij, in het begin van het incident management proces kan triage helpen dat de juiste dingen gedaan worden om verdere schade te voorkomen en bewijsmateriaal veilig te stellen.

Uit de triage kan blijken dat later forensisch onderzoek nodig is en hiervoor is een goede opdrachtverstrekking noodzakelijk.

Een incident dat snel escaleert of ervoor zorgt dat de primaire organisatietaken hinder ondervinden en bijvoorbeeld de dienstverlening aan inwoners en bedrijven in gevaar komt en mogelijk voor langere tijd minder of niet beschikbaar is moet escaleren naar het business Continuity Management Proces (BCM). Voor meer informatie over BCM heeft de IBD de VDW module 4 beschikbaar.[[5]](#footnote-5)

Dit betekent dat de BCP-plannen (VDW4)[[6]](#footnote-6) uitgevoerd moeten gaan worden en dit gebeurt dan ook door een ander team dan het incident respons team.

De volgende stap is dat men, nadat er voldoende informatie verzameld is, een prioriteit bepalen van het incident.

Bepaal of het incident mogelijk persoonsgegevens betreft en dus een datalek is dat onder de AVG valt, en volg het datalekkenproces. Als bekend is dat het een datalek is, maar nog niet alle gegevens over het datalek bekend zijn, dan kan beslist worden een voormelding bij de AP te doen en later deze in te trekken of verder aan te vullen.

Ook kan later in deze fase gestart worden met digitaal forensisch onderzoek. Let wel op, het inschakelen van digitaal forensisch onderzoek kost tijd en geld. Tijd, omdat het onderzoek moet worden uitgevoerd en op dat moment kan men nog niet beginnen met herstel. (het oplossen van het incident gaat dus langer duren). Hierom, en omdat er geld mee gemoeid is, moet aan het men management goedkeuring vragen. Het uitvoeren van forensisch onderzoek is vaak tweeledig, enerzijds helpen bij incident oplossen maar ook het veiligstellen van digitaal bewijsmateriaal.

Vragen die de forensisch onderzoeker moet kunnen beantwoorden zijn:

* Wat is er gebeurd?
* Hoe kon dit gebeuren?
* Hoe lang is dit al aan de hand?
* Om welke systemen en applicaties gaat het?
* Welke persoonsgegevens zijn er geraakt?

### Inperken / indammen schade

Als de analyse is afgerond kan men beginnen met het wegnemen van de incident oorzaak. In de voorgaande stappen werd het incident proces gestart en de eerste stappen gezet naar analyse, nu is het zaak de oorzaak van het incident weg te nemen als randvoorwaarde voor de volgende stap, herstel.

### Oplossen

Nu de oorzaak van het incident is weggenomen kan aan herstel worden begonnen. Maak een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident en zorg ervoor dat risico’s die verband houden met dit incident worden gemitigeerd. In deze fase is het belangrijk om ook te blijven controleren of er sporen van eventuele buitgemaakte informatie te vinden is op het internet of Darkweb.

 pas als de gevolgen zijn ingedamd, dan kun je werken aan oplossen.

### herstel

Voor computer systemen zoals werkplekken en servers geldt dat ze mogelijk helemaal opnieuw moeten worden opgebouwd op “schone” apparatuur. In de meeste gevallen zal dit ook het geval zijn als een forensische partij naast het veiligstellen van gegevens voor onderzoek bepaalde systemen nog voor nadere analyse nodig heeft. Het komt steeds vaker voor dat gecompromitteerde systemen nooit meer helemaal vertrouwd kunnen worden en daarmee is het opnieuw opbouwen een noodzaak. Het herstellen van systemen is een tijdrovende en capaciteit kostende klus, hiervoor kan het noodzakelijk zijn om hulp in te roepen van extra capaciteit van andere gemeenten, de veiligheidsregio of leveranciers. De IBD kan voor tijdelijke ondersteuning van een getroffen gemeente in de warme fase hulp inroepen van andere gemeenten via het Gemeentelijk Response netwerk (GRN) op basis van bijvoorbeeld een functieprofiel. Op deze manier brengt de IBD gemeenten onderling in verbinding waarna zij verder kunnen afstemmen over de gewenste hulp / capaciteit. De IBD is 24/7 bereikbaar voor gemeenten bij spoed als gevolg van een incident.

Bepaal hier ook welke soort gegevens mogelijk zijn blootgesteld door het incident.

Als het geen persoonsgegevens betreft en herstel goed mogelijk is dan is geen verdere actie noodzakelijk, als het wel persoonsgegeven betreft moeten mogelijk betrokkenen in kennis worden gesteld. Dit is dus zaak voor overleg waar ook de FG betrokken moet worden.

Als eerder al ontdekt is dat er een datalek is en dat er een (voor) melding gedaan is aan de Autoriteit Persoonsgegevens (AP), dan moet melding bij de AP worden aangevuld en beslist worden of betrokkenen ook geïnformeerd moeten worden. Informeer indien noodzakelijk andere overheidsinstanties, zoals de IBD en/of de politie. Betrek voor deze melding eventueel een jurist van de gemeente (zie: meldingen). Snelheid is ook belangrijk vanuit een PR-oogpunt. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden. Let op, het is ook raadzaam om bij de woordvoering over een incident een jurist te betrekken, de aard en inhoud van de communicatie kan gevolgen hebben voor gemeentelijke aansprakelijkheid. Ook hier kan de IBD bij adviseren.

Herstel van informatie kan ook zodanig ingewikkeld zijn dat externe specialisten nodig zijn om hierbij te ondersteunen. Daarnaast is ook capaciteit van bijvoorbeeld functioneel/technisch beheerders nodig om te bepalen wat er aan informatie nog wel goed of niet goed meer is.

### Remediatie

Een belangrijke stap in de respons op incidenten is het verhelpen van eventuele kwetsbaarheden die tijdens het incident zijn uitgebuit. Dit omvat onder andere de technische kwetsbaarheden die het mogelijk hebben gemaakt dat malware-exploits werken. Daarnaast omvat dit ook alle ondersteunende technologieën, bedrijfsprocessen of personeelstraining die mogelijk zouden hebben geholpen om het incident te voorkomen als ze vóór het incident aanwezig waren geweest. Als er een kwetsbaarheid is uitgebuit bestaat de kans dat een aanvaller het weer opnieuw zal proberen, het is dus zaak om alle kwetsbaarheden en ondersteunende technologieën te verbeteren.

### Afsluiten incident

Nadat het incident is vastgesteld, onderzocht, opgelost en de oorzaken zijn weggenomen en alle getroffen systemen zijn hersteld, kan het incident worden gesloten. De gemeente kan dan weer terug naar normaal, er zijn echter nog wel enkele activiteiten die moeten plaatsvinden:

* Archiveren van forensisch bewijsmateriaal;
* Archiveren van incident informatie en communicatiegegevens;
* Notificeren van betrokkenen die ook in een eerder stadium zijn betrokken.
* Bij een datalek dat gemeld moet worden, alsnog de melding doen of de voormelding aanvullen bij de AP

### Evaluatie en rapportage

De doelstelling van evalueren in deze stap is tweeledig:

* Leren van het incident;
* Het incidentmanagementproces evalueren en aanscherpen (PDCA).

Identificeer lessen uit het incident en bespreek deze met het team, rapporteer over het incident, de genomen maatregelen en het algemeen verslag, pas het gevolgde draaiboek aan. Incidenten moeten goed worden beschreven, met de oplossing erbij, en bewaard zodat het incidentmanagementproces en eventueel andere processen worden verbeterd. Er kan lering worden getrokken uit het overzicht met het aantal incidenten en het type incidenten en hier kan vervolgens op worden geacteerd. Alle incidenten moeten daarnaast ook gemeld worden aan de IBD en daarvoor dient een speciale contactpersoon (VCIB) aangewezen worden. Zie hiervoor het aansluitdocument van de IBD.[[7]](#footnote-7) Incidenten melden bij de IBD geeft andere gemeenten ook de mogelijkheid om de kans en de eventuele impact van het incident te verkleinen. Mochten meerdere gemeenten last hebben.

Voor het delen van lessons learned van grotere incidenten aan andere gemeenten kan de IBD aan de gemeente vragen deel te nemen aan een aparte evaluatiesessie, de IBD kan ook aansluiten bij de evaluatie sessie binnen de gemeente.

## Hoe te gebruiken

Afhankelijk van de aard van het incident en de grootte van het Response team, kan het raadzaam en praktisch zijn om een aantal van de checklist stappen en sub-stappen parallel aan te pakken. Bijvoorbeeld: zodra de oorzaak van een incident wordt bepaald, remediatie van de oorzaak en het herstel van de functie kan worden gestart, terwijl documentatie activiteiten voor de evaluatie worden aangepakt.

Het is verstandig om de paraatheid van de gemeente op het gebied van ‘veiligheid incident response’ periodiek te oefenen op een manier vergelijkbaar met een noodsituatie planning. Geleerde lessen moeten zo nodig in de checklist, respons procedures en / of de toewijzing van hulpmiddelen worden opgenomen. Voor bewustwording en oefenen zijn verschillende producten te vinden op de website van de IBD.[[8]](#footnote-8)

De checklist/stappenplan in bijlage 1 bevat acties die nodig zijn om de meest ernstige veiligheidsincidenten aan te pakken, dat wil zeggen: de blootstelling van persoonlijk identificeerbare informatie beschermd door wetten, standaarden en / of contracten met partijen van buiten de gemeente. Het kan ook effectief worden gebruikt om andere veiligheidsincidenten aan te pakken, bijvoorbeeld: het beschadigen van openbare websites, ongeoorloofde toegang tot vertrouwelijke, maar niet wettelijk beschermde gegevens, of het verlies van vertrouwelijke papieren dossiers.

Gezien de trend naar meer gebruik van derden, met inbegrip van Cloud computing-leveranciers voor het leveren van diensten die gebruik maken van verzamelen, opslaan en/of verwerken van gemeentelijke gegevens, dienen de gemeenten rekening te houden met de gedeelde verantwoordelijkheid voor de incident response. Deze zijn vaak noodzakelijk door dergelijke overeenkomsten. Deze checklist biedt stappen die moeten gebeuren, ongeacht de locatie van een mogelijke inbreuk op de gegevensbeveiliging. Wie de verantwoordelijkheid moet nemen voor elk van deze stappen als een derde partij betrokken is, zal variëren afhankelijk van de aard van de externe dienst, evenals de beveiligingsgerelateerde termen van het contract tussen de gemeente en die partij.

# Aandachtspunten

Welke aspecten komen nog meer bij het incidentmanagementproces kijken? Hieronder staan enkele aspecten die belangrijk zijn voor het incident management proces.

## Hoe begin ik?

De IBD heeft in het kader van Verhogen Digitale Veiligheid 1 (VDW1) een tweetal mindmaps gepubliceerd. In de mindmap processen zijn de verschillende basismaatregelen uitgewerkt voor een aantal basisprocessen, waaronder ook voor het incidentmanagementproces.[[9]](#footnote-9) Deze mindmaps en gerelateerde documenten zijn te vinden op onze website en kunnen naast dit document gebruikt worden.

Het belangrijkste is:

* dat het incident management proces wordt ingebed in de gemeentelijke praktijk. Sluit zoveel als mogelijk aan bij bestaande ITIL-procedures en laat incidenten altijd binnenkomen op het helpdesksysteem;
* voor incident management moeten procedures worden uitgewerkt en er moet rekening gehouden worden met onbeschikbaarheid van systemen en ICT middelen, zorg er dus voor dat procedures en telefoonlijsten ook offline beschikbaar zijn;
* zorg voor een logboek dat ook offline beschikbaar is en documenteer nauwkeurig de uitgevoerde acties en verder alles wat relevant is;
* richt een chatgroup in met deelnemers die direct geïnformeerd moeten worden bij een incident;
* leer van beveiligingsincidenten;
* zorg voor een actueel en gepubliceerde Coordinated Vulnerability Disclosure procedure (CVD).[[10]](#footnote-10)
* De IBD is dag en nacht bereikbaar voor advies, maar bedenk dat incidenten op ieder moment van de dag kunnen plaatsvinden of opgemerkt worden. Richt dus ook bereikbaarheid buiten kantoor uren in.

## Metrieken / KPI’s

Over Incident en respons management moet ook kunnen worden gerapporteerd, daarnaast is het noodzakelijk om door middel van metrieken de effectiviteit van het incidentmanagementproces te kunnen beoordelen over langere tijd. Zaken die gemeten kunnen worden:

* Aantallen incidenten per categorie.
* Gemiddelde, minimale en maximale tijdsduur die nodig was van start van het incident totdat de organisatie er weet van had. (door een melding).
* Tijd besteed is vanaf melding tot follow up en oplossing per incident type.
* Tijd die besteed is tot indammen.
* Aantal incidenten die geleid hebben tot niet halen van SLA tijden/afspraken of het uitvoeren van publieksdiensten.
* Aantallen medewerkers die bewustwording cursus hebben gevolgd versus totaal aantal medewerkers die het hadden moeten volgen.
* Aantal Incidenten met impact op de burger.
* Aantal incidenten met privacy een component.

## GGI-Veilig

Voor deelnemende gemeenten aan GGI-veilig kunnen binnen verschillende percelen diensten afnemen om hulp te ontvangen bij incidenten en de response op incidenten. In alle stappen van het incident management proces zijn producten aanwezig binnen GGI-veilig.[[11]](#footnote-11)

Perceel 1: SIEM-SOC diensten

Perceel 2: Cloud Access Security Broker (CASB), Firewall, mailfiltering, Advanced Persistent Threat (APT) Protection, Anti-DDOS, Intrusion Detection & Prevention (IDS/IPS), Data Loss prevention (DLP) en anderen.

Perceel 3: Expert diensten zoals Compliancy checks, Pentesten, Computer Forensics.

## Externe leveranciers

Incidenten kunnen ook plaatsvinden bij externe leveranciers zoals bijvoorbeeld SaaS leveranciers. Ook in contracten en service level agreements (SLA’s) moeten (nadere) afspraken gemaakt worden om de belangen van de gemeente te waarborgen om het continuïteitsrisico bij incidenten en calamiteiten te beheersen.

## Logging

Bij het onderzoek naar mogelijke incidenten wordt veelvuldig gebruik gemaakt van de controle op logging uit systemen, netwerkapparatuur en programma’s. Dit zijn doorgaans dezelfde logbronnen die kunnen worden gebruikt door een monitoring en response[[12]](#footnote-12) dienst die detecteert of er kwetsbaarheden worden misbruikt of incidenten hebben plaatsgevonden. Los van de detectie, wordt logging ook veelvuldig achteraf gebruikt bij het reconstrueren van een incident of om te ontdekken welke systemen nog meer geraakt waren. Logs moeten bewaard worden volgens vaste regels en kennen per soort logging een bewaartermijn waarvan afgeweken kan worden (verlenging) als er een vermoeden is van een incident. Voor logging die betrokken was bij een beveiligingsincident geldt een bewaartermijn van 3 jaar. Als logging op de juiste wijze bewaard en behandeld wordt, kan logging ook dienen als bewijsmateriaal voor de wet als er aangifte wordt gedaan. Let hierbij wel op dat logging persoons gerelateerde of privacygevoelige informatie kan bevatten, en dat logging zodanig bewaard moet worden dat deze niet zomaar kan worden ingezien of worden gewijzigd. Zie hiervoor de ‘Aanwijzing Logging’ van de IBD .

## Personeel

Het incidentmanagementproces moet een eigenaar hebben en binnen het proces moet een vast aanspreekpunt zijn die eventueel ook zorgdraagt voor de externe communicatie. Het melden van incidenten is een taak van iedereen, in ieder geval moet altijd de servicedesk geïnformeerd worden. De beoordeling van de logging maar ook van gemelde incidenten behoort door een speciaal aangewezen functionaris te gebeuren afhankelijk van waarover de logging of de incidentmelding gaat. Onrechtmatigheden van een bepaalde categorie[[13]](#footnote-13) moeten gemeld worden aan de CISO. Bij een escalatie of een noodsituatie moet altijd rekening gehouden worden met woordvoering waarbij de IBD advies kan geven. Al het personeel dat betrokken is bij het incidentproces moet op de hoogte zijn van de procedures en de telefonische bereikbaarheid van belangrijke contactpersonen en teamleden. De IBD heeft ter ondersteuning om zicht te hebben op belangrijke nummers en stappen hiervoor een instrument ontwikkeld, het zogenaamde kaartje in de meterkast. Per soort incident kan het team een wisselende samenstelling hebben.

## Voorbereiding

Rond incidenten moeten voorbereidingen getroffen en geoefend worden. Voor incidenten met een mogelijke hoge impact is het wenselijk om dat regelmatig te doen. Voor incidenten met hoge impact kunnen zogenaamde cheat sheets [[14]](#footnote-14) of operational incident best practices worden voorbereid. Er kunnen voor bepaalde incidenten die vaker voorkomen standaard afhandeling instructies worden opgesteld, in vaktermen zijn dit playbooks. Een voorbeeld hiervan zijn de stappen die doorlopen moeten worden als bijvoorbeeld een apparaat is zoekgeraakt. Door te analyseren welke incidenten vaker voorkomen is het mogelijk om input te krijgen om deze playbooks voor standaard incident afhandeling te ontwikkelen.

Binnen de wereld van Computer Emergency Response zijn al veel cheat sheets en handreikingen ontwikkeld en deze zijn onder andere te vinden op:

<https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/>

<https://zeltser.com/security-incident-questionnaire-cheat-sheet/>

In deze sheets is steeds weer een bepaalde aanpak te herkennen die zeer goed toepasbaar is voor het ontwikkelen van eigen sheets.

In de voorbereiding is het ook belangrijk om iedereen die betrokken zal zijn bij het proces te informeren. Zorg voor overzichten met namen/functies en telefoonlijsten die ook offline beschikbaar zijn. Denk na over communicatie wanneer bijvoorbeeld het totale ICT-infrastructuur (óók VOIP) uitgevallen is of mobiele netwerken overbelast zijn vanwege grote drukte (bij calamiteiten). Het is raadzaam om voorbereid te zijn op uitval van ICT en dus moeten incident management procedures en telefoonlijsten ook offline beschikbaar zijn.

## Gouden uur

Het ‘gouden uur’ is het eerste uur na de ontdekking van het incident. Het is essentieel om het incident in te perken maar ook geen informatie verloren te laten gaan die nodig is voor het onderzoek of het onderzoek achteraf. In het geval van bijvoorbeeld een computerinbraak, het wissen van een schijf en de diefstal van data, kan het nodig zijn om een digitaal forensisch expert in te huren[[15]](#footnote-15). Deze kan alleen maar onderzoek doen als er zorgvuldig met bewijsmateriaal omgesprongen wordt. De handelingen uitgevoerd in het eerste uur zijn essentieel voor het welslagen van de reactie, maar ook op de bewijsvoering. Speciaal hiervoor heeft de IBD een factsheet: “Gehackt, hoe nu verder?”.[[16]](#footnote-16)

## De 7 gouden regels van incident management

1. Zet apparatuur niet uit die aanstaat
2. Verbreek de netwerk verbinding
3. Stel Back-ups veilig
4. Zet de automatische back-up uit
5. Stel logfiles veilig
6. Informeer de interne organisatie
7. Documenteer de genomen stappen

Tenslotte: Vraag bij twijfel advies van een digitaal forensisch expert of bel de Helpdesk van de IBD: 070 204 55 11.

# Incident Impact Leidraad

De Incident Impact Leidraad beschrijft de regels voor het beoordelen van de impact van een incident. Het bepalen van de impact van een incident is essentieel voor het activeren van de geschikte incident maatregelen, zoals onder andere de teamsamenstelling en opschaling. Waar in de voorgaande versies nog een algemene leidraad werd genoemd is in dit hoofdstuk de Incident impact meer toegeschreven op de gemeentelijke praktijk.

## Incident Impact bepaling

**LET OP: de tabel bevat slechts voorbeelden**.

Om de impact van een incident te bepalen, kiest u altijd uit de hoogste waarde van de desbetreffende categorie en de eindscore wordt bepaald door de hoogste score binnen alle categorieën. De incident classificatie wordt gedaan middels een impact inschatting langs de lijnen van MAPGOOD, aangevuld met een urgentie inschatting. Zie ook bijlage 3.

|  |  |  |  |
| --- | --- | --- | --- |
| Onderwerp  | Laag | Midden | Hoog |
| Aantal getroffen Mensen/medewerkers | <10 | <100 | >100 |
| Apparatuur werkt niet | Enkele apparaten uitgevallen. | Meerdere apparaten uitgevallen. | Meeste apparaten uitgevallen. |
|  | De apparatuur kan eenvoudig vervangen worden. | De apparatuur ondersteunt primaire processen en is moeilijk vervangbaar. | De dienstverlening van de gemeente komt voor langere tijd tot stilstand. |
| Programmatuur werkt niet | Software die de secundaire processen ondersteund is uitgevallen. | Software die de primaire processen ondersteunt is uitgevallen. | Software die de primaire processen ondersteunt is uitgevallen en kan langere tijd niet gebruikt worden. |
| Gegevens worden gekopieerd, versleuteld dan wel vernietigd | Gegevens die secundaire processen ondersteunen. | Gegevens die primaire processen ondersteunen. | Gegevens die organisatie overstijgend in ketens verwerkt worden. |
| Organisatieprocessen | Het incident blijft beperkt tot een enkele ondersteunende afdeling. | Het incident heeft impact op een primair proces, de publieksbalie moet gesloten worden. | Het incident overstijgt de organisatie (lokaal/regionaal) of er is impact op de buitenruimte. |
| Omgeving | Het incident beperkt zich tot een fysieke afdeling binnen het gemeentehuis. | Het incident treft meerdere afdelingen binnen een gemeentehuis. | Het incident breidt zich uit naar de buitenruimte en er ontstaat maatschappelijke onrust. |
| Diensten | Het incident beperkt zich tot lokale applicaties en systemen. | Het incident breidt zich uit naar of vindt plaats bij off-premise leveranciers en diensten. | Het incident breidt zich uit en keten afhankelijke diensten komen in gevaar. |
| Impact op betrokkenen | Het incident leidt niet tot enige schade voor betrokkenen. | Het incident leidt tot een klein risico voor betrokkenen. | De groep van betrokkenen is groot of het incident leidt tot een hoog risico voor betrokkenen. |
| Kans op reputatieschade | Geen kans op reputatieschade. | De reputatieschade beperkt zich tot lokale afdelingen en afdelingsmanagers.  | De reputatieschade is hoog met de kans dat het college valt.  |
| Financiële impact | De schade als gevolg van het incident is op te vangen binnen de begroting van een afdeling. | De schade als gevolg van het incident is op te vangen binnen de begroting van de organisatie. | De schade als gevolg van het incident is niet meer op te vangen binnen de begroting of getroffen voorzieningen. |
| Werk om te herstellen is arbeidsintensief | Het terugzetten van back-ups is voldoende om weer up en running te komen. | Back-ups hebben afhankelijkheden en deze moeten gecoördineerd en gecontroleerd worden. | De inspanning om te herstellen legt grote druk op de hele organisatie, externe ondersteuning is nodig. |
| Snelheid van toename incident | Het incident beperkt zich tot de getroffen apparaten en breid zich niet verder uit. | Het incident breidt zich uit naar andere apparaten en breid zich langzaam uit als er geen actie ondernomen wordt. | Het incident breidt zich snel verder uit en heeft in korte tijd de hele dienstverlening onmogelijk gemaakt. |
| Ketenafhankelijkheid | De geraakte processen zijn geïsoleerd en blijven binnen de afdeling waar het incident optreedt. | De geraakte processen beïnvloeden andere afdelingen binnen de organisatie. | Ketenafhankelijkheden zijn organisatie overstijgend regionaal en/of nationaal . |
| Beschikbaarheid bedrijfsprocessen | De geraakte productieprocessen ondervinden geen of zeer weinig hinder van het incident. | De dienstverlening van de primaire producten en diensten ondervindt hinder en loopt vertraging op. | De primaire producten en diensten zijn voor lange tijd niet beschikbaar en de dienstverlening aan inwoners en bedrijven stopt. |

*Tabel 1: Voorbeelden incident impact*

## Teamsamenstelling crisisteam

Ieder incident heeft zijn eigen dynamiek en dus ook een eigen samenstelling van het team. In 4.1 is een schema opgenomen om te bepalen hoe groot de impact van het incident is en afhankelijk van die classificatie wordt het team groter of worden er ook externe spelers uitgenodigd. De teamsamenstelling is essentieel voor een adequate reactie en om het incident zo klein als mogelijk te houden. Afhankelijk van de impact van het incident is er een andere teamsamenstelling te bedenken van het crisisteam. Door te oefenen kan beoordeeld worden of teamsamenstellingen juist zijn of dat er misschien aanpassingen nodig zijn. Oefenen in het kader van incident management is sowieso de manier om te ontdekken of de plannen aansluiten bij de praktijk of dat ze gewijzigd moeten worden.

De basis samenstelling van het crisisteam kan bestaan uit:

* Voorzitter
* Vastleggen acties / Notulen
* Technisch advies
* Beveiligingsadvies
* Privacy advies
* Communicatie / Woordvoering
* Aansturing ICT-intern
* Aansturing Leveranciers
* Juridisch advies
* Domeinadvies
* Externe capaciteit voor triage

Het team wijst iemand aan die protocolleert (logger)

In het vervolg schuift de politie aan in verband met het opsporingsaspect (OM)

Afhankelijk van de zwaarte van het incident en de impact op bedrijfsprocessen kunnen ook andere partijen nodig zijn, bijvoorbeeld:

* Burgemeester
* Portefeuille houder/Wethouder
* FG
* Crisismanager (OOV)
* Adviseur OOV
* Teammanager publieksdiensten
* Juridisch adviseur
* Leider forensisch onderzoeksteam
* Leveranciers (bijvoorbeeld ICT of MSSP)
* De IBD (online)

En indien er een escalatie plaatsvindt en/of impact gemeente overstijgend is:

* Veiligheidsregio:
	+ Operationeel leider
	+ AC Politie
	+ AC GHOR
	+ AC Brandweer
	+ CISO veiligheidsregio

## Agenda voorbeeld[[17]](#footnote-17)

In het document Handreiking Cybergevolgbestrijding G4-gemeenten – Deel 1 - warme fase[[18]](#footnote-18) Is uitgewerkt in paragraaf 1.4 hoe een typische agenda voor een crisisteam vergadering eruit zou kunnen zien.

# Bijlage 1: Incident management en response stappenplan en sjabloon

**Incident- en response management stappenplan**

Incident # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum ontdekking: \_\_\_\_\_\_\_\_\_\_\_\_ Datum gerapporteerd aan de CISO en het management: \_\_\_\_\_\_\_\_\_\_\_\_

Datum informatieverstrekking getroffenen: \_\_\_\_\_\_\_\_\_\_

*(Dit zou binnen een week na de ontdekking moeten zijn)*

*Incident met persoonsgegevens: JA / NEE*

**Type en scope van de gecompromitteerde data:**

**Incident team samenstelling:**

|  |
| --- |
| **STAP 0: Incident detectie** |
| **Dit is niet direct een formele stap, want incidenten gebeuren ongepland en onverwacht. Het wordt hier toch neergezet omdat het optreden van het incident en het moment van rapporteren of detecteren weten en bevestigen dat je een incident hebt wel een belangrijk gegeven is om later te willen weten. Men kan zo vaststellen hoeveel tijd verloren is gegaan tussen incident en acties/opvolging** |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | ***Het is van belang de start van het incident vast te stellen, dit is later nodig en helpt ook bij het bepalen hoelang het duurde vanaf het optreden van het incident tot de identificatie.***  |  |  |
|   | Noteer hoe het incident werd ontdekt en welke acties er tot nu toe genomen zijn. Geef een zo specifiek mogelijk antwoord, inclusief data, tijden, en welke apparaten gecompromitteerd zijn, applicaties, websites, et cetera. | Servicedesk |   |
|   | Noteer de gegevens van de melder | Servicedesk |   |
| **STAP 1: Initiatie** |
| **Controleer of een incident daadwerkelijk heeft plaatsgevonden. Deze activiteit omvat normaliter de systeembeheerder en eindgebruiker, 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, dan moeten de betreffende instanties gewaarschuwd worden.** |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 1.1   Onmiddellijk blootstelling beperken: | Afdeling |  |
|  | -        Als een elektronisch apparaat is gecompromitteerd: |   |  |
|  | o   Niet gebruiken (niet inloggen) of wijzigen van het apparaat |   |  |
|  | o   Zet het apparaat niet uit als het aan staat |   |  |
|  | o   Haal de netwerkverbindingen er af, maar NIET de voedingskabel |   |  |
|  |   |   |  |
|   |  1.2 Stel indien het incident daarom vraagt een incident manager aan | Servicedesk |   |
|  | 1.3   Waarschuw indien nodig de CISO  | Servicedesk |  |
|  | 1.4   Doe een melding bij de IBD | Servicedesk |  |
|  | *Handleiding: Voeg namen en telefoonnummers, e-mailadressen of indien mogelijk de link naar een online meldingsformulier toe.*  |   |  |
|  | 1.5   Indien het incident over elektronische apparaten gaat of als er media gestolen of verloren is, dan ook aangifte doen bij de politie. | Afdeling |  |
|  | *Handleiding: Deze stap alleen uitvoeren na overleg en op advies van de CISO of ICT- security afdeling.* |   |  |
|  | 1.6 Start met een logboek waarin gedurende het incident alle activiteiten op datum en tijd kunnen worden vastgelegd. | Servicedesk / incidentmanager |  |
| **STAP 2: Analyse** |
| **Controleer of een incident daadwerkelijk heeft plaatsgevonden. Deze activiteit omvat normaliter de systeembeheerder en eindgebruiker, 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, dan moeten de betreffende instanties gewaarschuwd worden.** |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 2.1   Voer een voorlopige beoordeling uit van het type en de scope van het incident en de impact. Als er potentieel gevoelige informatie blootgesteld is dan moet het management geïnformeerd worden en deze moet tijdens het verloop van het incident op de hoogte gehouden worden: | CISO of incidentmanager of -management (Incident Triage team) |  |
|  | *Voorbeelden:* |   |  |
|  | *a)     CIO* |   |  |
|  | *b)     Gemeentesecretaris* |   |  |
|  | *c)      Voorlichting* |   |  |
|  | *d)     IBD* |   |  |
|  | *e)     B&W*  |   |  |
|  | -        Indien het incident ook het lekken van persoonsgegevens betreft, leg dit dan nu vast. |   |  |
|  | -        Voor de beoordeling van de ernst van het incident kan mogelijk gebruik gemaakt worden van externe triage capaciteit via de partijen die voor forensics geselecteerd zijn binnen perceel 3 van GGI-veilig. Triage om te komen tot een goede forensische opdracht is zelf geen onderdeel van het perceel 3 en kan dus ook van andere marktpartijen worden afgenomen.  |   |  |
|  | -        De externe incident triage capaciteit kan worden ingezet om de ernst te beoordelen en ermee te helpen om een definitie te maken van de te onderzoeken getroffen ICT-objecten en logging om hiermee een gerichte opdracht te definiëren om een forensisch onderzoek partij in te schakelen via GGI-veilig.  |   |  |
|  | 2.2    Indien er sprake is van criminele activiteiten in verband met het incident moet bepaald worden of de politie mogelijk het onderzoek moet overnemen. Als dat gebeurt zal dit het vervolg van dit schema beïnvloeden. | Incidentmanager of -management |  |
|  | 2.3 afhankelijk van de zwaarte van het incident moet nu ook het incident responsteam worden samengesteld  | Incidentmanager of -management |  |
|  | *Handleiding: Zorg ervoor dat de vertegenwoordiger van de organisatie-eenheid waar het incident zich voordeed, deelneemt en dat deze persoon hoog genoeg in de organisatie zit om de nodige beslissingen te nemen.* |   |  |
|  | 2.4   Beoordeling Incident response proces en de verantwoordelijkheden met het Incident response team | De manager van het Incident response team |  |
|  | Verstrek ieder teamlid de huidige incident management Checklist. |   |  |
|  | Bespreek de communicatiestrategie. |   |  |
|  | Bespreek het belang van het goed in een tijdlijn documenteren en het voorkomen van het verloren raken van onderzoeksgegevens.  |   |  |
|  | *Handleiding: Aangaande het bespreken van de regels van de communicatie met het team in deze fase, is het vooral belangrijk om de nauwkeurigheid van de feiten te waarborgen tussen teamleden onderling en tussen het team en de juiste ambtenaren.* |   |  |
|  | *Voorbeelden:*  |   |  |
|  | *a)     Teamleden mogen niet praten met anderen buiten het team over het incident totdat er daarvoor toestemming is gegeven door het management of de CISO.* |   |  |
|  | *b)     Alle documentatie die door het team geschreven wordt moet op feiten gebaseerd zijn omdat het mogelijk in een strafrechtelijk onderzoek gebruikt kan worden.* |   |  |
|  | *c)      Er is dagelijks overleg tussen de teamleden.* |   |  |
|  | *d)     Het team moet bijhouden hoeveel tijd er besteed wordt en waaraan.* |   |  |
| ***STAP 3: Schade indamming en beoordeling van de blootstelling*** |
| ***Wijs een Incident response-teamleider aan en stel een bij het incident passend, ‘Incident response team’ samen. Dit team is belast met het beperken van verdere schade als gevolg van het incident. Start een grondige beoordeling van de aard en omvang van het incident en stel vast wat de schade is. Stel bewijsmateriaal veilig.*** |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 3.1   Beoordeel in overleg met het incident triage team of forensische ICT-capaciteit nodig is om digitaal bewijs te verzamelen voor opsporing, beoordeling van de schade en impact voor betrokkenen en organisatie. | Incident Triage team |  |
| Forensische ICT-capaciteit moet mogelijk worden ingekocht op basis van deelname aan GGI-Veilig. Het Incident Triage Team (1.4) (eventueel aangevuld met een externe partij voor directe ondersteuning en beoordeling van het incident) kan meehelpen om tot de juiste opdrachtverstrekking te komen aan de Forensische ICT partij.  |
|  | 3.2 Verzamelen en veiligstellen van bewijsmateriaal (bij zelf doen, zie anders 2.3) | Incident response team |  |
|   |
| *Handleiding: Verzamel fysiek en digitaal bewijs die tezamen een duidelijke, gedetailleerde beschrijving geven van hoe de data gecompromitteerd kon worden.* |
|  |
| *Voorbeelden:* |
| *a)     Images van de harddisk(en)* |
| *b)     Netwerkverkeersgegevens van en naar de gecompromitteerde apparatuur*  |
| *c)      Werkplek applicatie logs* |
| *d)     Toegangslogs* |
| *e)     Foto’s van de omgeving waar het incident plaatsvindt* |
|  | 3.3 Zorg voor, en onderhoud, al het bewijsmateriaal en houd bij waar het zich bevindt en wie er toegang toe heeft. | Incident response team |  |
|   |
| *Handleiding: Maak een inventarisatielijst van alle bewijsmateriaal en houdt bij wie, wanneer, wat gedaan heeft met het bewijsmateriaal.* |
| *Voorbeelden:* |
| *a)     Beschrijf wat exact het bewijsmateriaal is.* |
| *b)     Leg vast wie erbij moest en waarom.* |
| *c)      Leg vast waar en hoe het bewijsmateriaal opgeslagen is.* |
| *d)     Als apparatuur verplaatst moet worden zorg dan dat de ontvanger getekend heeft voor ontvangst en dat dit bewijs wordt toegevoegd aan de verzameling. Zorg dat de ontvanger weet welke verantwoordelijkheden er zijn.*  |
|  | 3.4 Neem maatregelen om de scope en de impact van het incident in te perken. | Incident response team |  |
|  |  |
|  | *Voorbeelden:* |
|  | - Indien het incident betrekking heeft op gevoelige gegevens die onjuist geplaatst zijn op publiek toegankelijke websites, verwijder dan 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, zoals bijvoorbeeld de Wayback Machine. |
|  |
|  | *- Staak de exploitatie van een gecompromitteerde applicatie of server.* |
|  | 3.5 Voer forensisch onderzoek uit en leg dit vast: | Incident response team |  |
| 1.     Analyseer bewijsmateriaal |
| 2.     Voer een reconstructie uit van het incident |
| 3.     Zorg voor gedetailleerde documentatie |
|  |
| *Handleiding: Bewaar origineel bewijsmateriaal en werk alleen op een kopie van de data. Zorg voor minimale verstoring van de bedrijfsvoering, zorg voor herleidbare en herhaalbare resultaten.* |
|  | 3.6 Maak de definitieve schatting af, en de documentatie over soort en afbakening van de blootgestelde data, evenals de beschikbaarheid en het soort van contactinformatie van de betrokken personen. | Incident response team |  |
|   | Geef mogelijk een voorwaarschuwing aan de Autoriteit Persoonsgegevens. | CISO of incidentmanager of –management of Privacy Functionaris |   |
|   |
| *Handleiding:* |
| *Als er een datalek is en deze valt onder de meldplicht datalekken van de AVG, dan moet er op basis van de beschikbare gegevens een voormelding gedaan worden bij de Autoriteit Persoonsgegevens.*  |
| **STAP 4: Remediatie en herstel** |
| **Neem maatregelen om de oorzaak van het incident te blokkeren of te verwijderen, verminder de impact door verdere blootstelling van de gevoelige gegevens te voorkomen, maak een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident en zorg ervoor dat risico’s die verband houden met dit incident worden gemitigeerd.** |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 4.1   Ga terug naar stap 3.2 en zoek naar aanvullende manieren om de blootstelling te beperken. | Incident response team |  |
|   |
| *Voorbeelden:* |
| *a)     Run periodiek web-query’s om u ervan te verzekeren dat de data niet verder is verspreid of gecached.* |
| *b)     Beoordeel de inventarisatie van getroffen hardware en systemen en wijzig verder waar nodig de wachtwoorden die mogelijk gecorrumpeerd zijn.* |
| c)      *Stop eventueel gecorrumpeerde diensten of applicaties en zorg voor work-arounds* |
|  | 4.2   Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico’s voor gevoelige dataopslag | Incident response team |  |
|   |
| *Voorbeelden:* |
| *a)     Run vulnerability scans op getroffen systemen;* |
| *b)     Beoordeel en bepaal waar de data zich bevindt en wijzig dit indien nodig om een hogere beschermingsgraad te verzekeren.* |
| *c)      Beperk de toegang tot systemen tot uitsluitend degenen die toegang nodig hebben.* |
| d)     *Gebruik software tools om gevoelige data te vinden, te verwijderen en te beschermen, bijvoorbeeld: Identity Finder.* |
|   | 4.3   Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze hersteld worden . | Hangt af van de getroffen systemen | *(dit lijkt een kleine stap, echter wanneer veel systemen getroffen zijn kan deze stap maanden in beslag nemen)* |
|  |
|  |
|  |
| **STAP 5: Kennisgeving** |  |
| **Bepaal welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffenen in kennis van het feit dat hun gegevens blootgesteld zijn. Snelheid is geboden indien er persoonsgegevens verloren zijn gegaan of bekend geworden zijn aan niet rechthebbenden. Informeer indien noodzakelijk andere overheidsinstanties, zoals de IBD en/of de politie. Bij sommige incidenten is het wettelijk verplicht een melding te doen naar andere instanties. Snelheid is ook belangrijk vanuit een PR-oogpunt. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden.** |  |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |  |
|  | 5.1   Neem beslissingen op basis van de bevindingen van het Incident response team  | Management |  |  |
|  | -    Geeft de mate van risico blootstelling de noodzaak tot het informeren van getroffenen? | *Bijvoorbeeld bij niet versleutelde persoonsgegevens die gelekt zijn.* |  |
|  | -    Zo ja, |  |  |
|  | ·       Indien van toepassing, is het de taak van rechtshandhaving om de betrokken partijen te infomeren? |  |  |
|  | ·       Wie gaat het schrijven uitgeven? |  |  |
|  | ·       Wie zal zich bezighouden met het beantwoorden van telefoon en e-mail op vragen van de betrokken personen? Rechtvaardigt het verwachte volume het opzetten of inzetten van een callcenter? |  |  |
|  | ·       Is het noodzakelijk om een officieel persbericht te plaatsen op de website van de gemeente? |  |  |
|  | -    Als er geen kans is geweest op blootstelling van informatie aan buitenstaanders, dan kan eventueel meteen doorgegaan worden naar stap 6. |  |  |
|  | 5.2   Indien het een incident betreft met persoonsgegevens waarbij een aanzienlijke kans bestaat op ernstige nadelige gevolgen voor de betrokkene dient de toezichthouder onverwijld in kennis gesteld te worden. | Management | *[3] Art 43a Wet meldplicht datalekken: De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.* |  |
|  | *Handleiding:* |  |  |
|  | *a)     Degenen die verantwoordelijk zijn voor het nemen van deze beslissingen zal variëren van gemeente tot gemeente, maar meestal is een deel van de ambtenaren geïnformeerd in Sub-stap 1.4. Beslissingen die genomen moeten worden, dienen in overeenstemming te zijn met eerdere beslissingen, tenzij eventuele afwijkingen volledig gerechtvaardigd zijn. Uiteraard moeten voor alle beslissingen de respectievelijke wetten, regelgeving en contractuele verplichtingen worden gevolgd.* |  |  |
|  | *b)     Er moet een geschikt communicatiemiddel gekozen worden, passend bij het incident, de hoeveelheid te informeren personen, de mate waarin risico gelopen is en/of informatie gecompromitteerd is.* |  |  |
|  | *c)      Er dient juridisch advies ingewonnen te worden over de positie en aansprakelijkheid van de gemeente bij bepaalde communicatie.* |  |  |
|  |   |   |  |  |
|  | 5.3   Verzamel de naam en adresgegevens van de getroffenen  | Afdeling, geadviseerd door de CISO of door het Incident response team |  |  |
|   |  |  |
| *Handleiding: Dit kan een moeilijk proces zijn als er mensen geraakt zijn waarvan de gemeente geen NAW-gegevens heeft.* |  |  |
|  |  |  |
| *Zorg ervoor dat de verzamelde data veilig wordt behandeld, verstuurd en opgeslagen en als de data niet langer benodigd is moet deze worden vernietigd.*  |  |  |
|   |  |  |
|  | 5.4   Zet telefoon en e-mail ondersteuning op in geval van vragen: | Afdeling, geadviseerd door de CISO of door het Incident response team |  |  |
| -        Stel een team samen. |  |  |
| -        Zorg voor voldoende infrastructuur, beoordeel of de lijn en e-mail capaciteit voldoende is. |  |  |
| -        Kies een geschikt telefoonnummer om te gebruiken. |  |  |
| -        Kies een geschikt e-mailadres om te gebruiken. |  |  |
| -        Bedenk van tevoren de reacties op de verwachte vragen. |  |  |
| -        Train het team. |  |  |
|   |  |  |
|  | 5.5   Als in stap 2 een website gekozen is om te communiceren: | Afdeling, geadviseerd door de CISO of door het Incident response team |  |  |
| -        Verzin een URL en website locatie. |  |
| -        Voorkom toegang totdat de website live mag gaan. |  |
| -        Bereid de inhoud voor. |  |
|   |  |
| *Handleiding:*  |  |
| *a)     Websites worden vooral gemaakt als het aantal getroffenen te groot is of omdat niet alle mensen bekend zijn.* |  |
| *b)     De website content moet goedgekeurd worden.* |  |
|   |  |
|  | 5.6   Voorbereiding schriftelijke informatieverstrekking aan getroffenen: | Afdeling, geadviseerd door de CISO of door het Incident response team |  |  |
| -    Bedenk het onderwerp en de huisstijl. |  |  |
| -    Schrijf een concepttekst. |  |  |
|  |  |  |
|  |  |  |
| *Handleiding:*  |  |  |
| *De inhoud van de brief moet zijn goedgekeurd door het management en door voorlichting.* |  |  |
|   |   |   |   |  |
| **STAP 6 : Afsluiten Incident** |  |
| **In deze stap wordt het incident afgesloten, de oorzaken zijn weggenomen, de systemen zijn hersteld. Bewijsmateriaal en incident gegevens worden gearchiveerd, de diverse partijen kunnen worden geïnformeerd**  |  |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |  |
|  | 6.1 archiveer al het verzamelde forensisch bewijsmateriaal | Incident manager |  |  |
|  | 6.2 Archiveer incident informatie en communicatiegegevens en het logboek | Incident manager |  |  |
|  | 6.3 Als er nog geen betrokkenen zijn genotificeerd en er zijn persoonsgegevens betrokken, ga terug naar de vorige stap | Afdeling, geadviseerd door de CISO of door het Incident response team |  |  |
|  | 6.4 Doe de benodigde meldingen |   |  |  |
|  | - Als er een noodzaak of een verplichting is, informeer de politie en doe aangifte. | Management |  |  |
|  | - Informeer de Informatie Beveiligingsdienst (IBD) | CISO of ACIB/VCIB |  |  |
|  |   |   |  |  |
|  | - Doe de definitieve melding aan de Autoriteit Persoonsgegevens (AP) als er bij Stap 2.1 een voor melding gedaan is. Doe een gemotiveerde melding aan de AP als er bij Stap 2.1 geen voormelding gedaan is en er toch meldplichtige persoonsgegevens gelekt zijn. (Gemotiveerd, omdat als bij een AP melding meer dan 72 uur vergaan zijn sinds de ontdekking van het datalek, je moet uitleggen waarom je pas na 72 uur een melding doet.) | Management of Privacy Functionaris |  |  |
|  | - Informeer derde partijen zoals serviceproviders als hiermee het risico van identiteitsdiefstal verkleind kan worden of als dat is vastgelegd in het respectievelijke contract. | Afdeling |  |  |
|  | - Als er bankgegevens blootgesteld zijn aan niet rechthebbenden, informeer dan de bank of creditcard firma’s. | Controller |  |  |
|  | - Coördineer de gelijktijdige communicatie-acties zodat de verschillende informatiestromen gelijktijdig plaatsvinden.  | Afdeling, Voorlichting |  |  |
| **STAP 7 : Rapportage en evaluatie** |  |
| **Identificeer lessen uit het incident en bespreek deze met het team, rapporteer over het incident, de genomen maatregelen en het algemeen verslag, rapporteer indien nodig intern en extern, pas het gevolgde draaiboek aan.** |  |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |  |
|  | 5.1   Verzamel alle tijdschrijfregels van het personeel dat heeft meegewerkt aan de Incident response-actie. De totale kosten kunnen mogelijk van belang zijn indien er een rechtszaak komt tegen een verdachte, omdat deze dan verhaald kunnen worden. | Iedereen die tijd geschreven heeft rapporteert aan het management |  |  |
|  |
|  | 5.2   Plan een vergadering ongeveer 2 tot 6 weken na het incident om een evaluatie uit te voeren over de aanpak van het incident. | Incident response team |  |  |
|  | 5.3   Onderzoek oplossingen om herhaling te voorkomen. | CISO |  |  |
| -        Indien nodig rapporteer hierover aan het management. |  |
| *Te beantwoorden vragen:* |  |
| *a)     Waarom was de data opgeslagen op een verkeerde plaats of niet veilige plaats?* |  |
| *b)     Wat hadden we meer kunnen doen om de inbraak te voorkomen?* |  |
| *c)      Neemt de afdeling voldoende maatregelen om herhaling te voorkomen?*  |  |
|  |  |
|  | 5.4 Onderzoek of het incidentmanagementproces effectief en efficiënt is uitgevoerd, zijn de juiste dingen gedaan? *(hier gaat het niet om inhoudelijk naar het incident te kijken zoals hierboven bij 5.3 maar om te onderzoeken of het proces goed gevolgd is of dat er verbeterpunten zijn aan het proces).* | CISO |  |  |
|  | 5.5   Plan oplossingsprojecten om de geleerde lessen effectief in te bedden in de organisatie. | Afdeling |  |  |
|  |
|  | 5.6   Sla alle Incident en response informatie veilig op, inclusief gesprekverslagen, aantekeningen en incident artefacten. In overeenstemming met wetgeving en intern beleid zal op enig moment (een deel van) de opgeslagen informatie vernietigd moeten worden.  | CISO |  |  |
| *Indien het een inbreuk betreft van de bescherming van persoonsgegevens moet altijd een overzicht hiervan worden bijgehouden.* |  |
|  |  |

# Bijlage 2: Incidentenprocedure informatiebeveiliging

### Melding van een informatiebeveiligingsincident

Elke medewerker dient alert te zijn op bedreigingen met betrekking tot informatiebeveiliging en is verplicht om alle incidenten die hij/zij ontdekt of vermoedt te melden aan de helpdesk.In gevalhet vertrouwelijke zaken of personen betreft, moet de melding ook rechtstreeks aan de CISO gedaan worden.

### Toewijzen en escaleren van een informatiebeveiligingsincident

Hieronder staat een lijst (twee tabellen) met mogelijke incidenten m.b.t. informatiebeveiliging. Deze lijst is niet uitputtend en zal dit ook nooit kunnen zijn: er zullen zich steeds nieuwe soorten beveiligingsincidenten voordoen. De lijst ondersteunt de helpdesk bij het herkennen van een beveiligingsincident en bij het inschatten van de impact. Het is aan te bevelen dat bij twijfel de helpdesk contact opneemt met de CISO of gelijkwaardig.

In veel gevallen zal de CISO niet als primaire behandelaar optreden, immers het technisch verhelpen van een dergelijk incident gebeurt niet door de CISO, maar door een technisch specialist. Het incident wordt dan door de helpdesk opgesplitst in deelincidenten, die naar de betrokken behandelaars worden gestuurd.

De CISO kan op twee manieren worden ingeschakeld:

1. De CISO moet direct een incident met hoge prioriteit oplossen, dan wel coördineren of adviseren. In dit geval neemt de helpdesk direct telefonisch contact op met de CISO (of vervanger).
2. De CISO moet op de hoogte worden gebracht dat een incident is gebeurd. Indien nodig is het incident ook naar een andere specialist gestuurd ter behandeling. De CISO raadpleegt de meldingsdatabase regelmatig (ongeveer 1 keer per week).

Er zijn twee invallers voor de Security Officer, in geval incidenten met hoge prioriteit behandeld moeten worden:

* Hoofd Facilitair Beheer, die ook de fysieke beveiliging in het takenpakket heeft.
* Hoofd afdeling Informatie en Beheer.

Acties Security Officer

* De CISO neemt direct maatregelen om bewijsmateriaal en andere gegevens die in dit stadium als relevant worden beschouwd, veilig te stellen.
* De CISO bepaalt hoeveel tijd en middelen nodig zijn voor afhandeling van het beveiligingsincident. Aan de hand hiervan en de impact van het incident bepaalt de CISO in overleg met het management de teamsamenstelling.

### Alarmeringsprocedure

Indien de CISO inschat dat de ernst van het incident dusdanig is óf acties nodig zijn die de handelingsbevoegdheid van de CISO te boven gaan, wordt de directe leidinggevende of de directie ingeschakeld.

# Bijlage 3: Incidenten en meldingsniveau matrix

| **GEBRUIKERS­INCIDENTEN** |  | **NIVEAU VAN MELDING \*)** |
| --- | --- | --- |
| **Incidenten categorie** | **Mogelijk incident** | **Helpdesk** | **CISO** | **Directie** |
| Onopzettelijk foutief handelen | Als gevolg van foutieve procedures | X |  |  |
|  | Als gevolg van foutgevoelige bediening | X |  |  |
|  | Onzorgvuldige omgang met password | X |  |  |
| Opzettelijk foutief handelen | Niet volgen van voorschriften | X | X | (X) |
|  | Fraude of diefstal | X | X | X |
|  | Ongeautoriseerde toegang door medewerker | X | X | X |
| Technisch falen van apparatuur | Storing in pc of randapparatuur | X |  |  |
| Technisch falen van apparatuur door externe invloeden | Wegvallen elektrische spanning | X | X |  |
| Menselijke omgang met apparatuur | Bedieningsfouten | X |  |  |
| Opzettelijke wijzigingen | X | X | (X) |
|  | Beschadiging of vernieling | X | X | X |
| Problemen met programmatuur | Fouten in programmatuur | X |  |  |
|  | Ongeautoriseerd gebruik | X | X |  |
|  | Wijziging door medewerker | X | X | X |
|  | Opzettelijk introduceren van een virus door medewerker | X | X | X |
|  | Inbrengen van virus door middel van niet gescreende programmatuur | X | X | X |
|  | Illegaal kopiëren  | X | X | X |
|  | Diefstal van programmatuur | X | X | X |
| Gegevens en gegevens­dragers | Zoekraken gegevensdragers | X | X | X |
|  | Diefstal van gegevensdragers | X | X | X |
|  | Beschadiging gegevensdragers | X |  |  |
|  | Onleesbaarheid van gegevensdragers | X |  |  |
|  | Fouten in gegevens door apparatuur | X |  |  |
|  | Fouten in gegevens door programmatuur | X |  |  |
|  | Opzettelijke invoer van foutieve gegevens | X | X | X |
|  | Onopzettelijke invoer van foutieve gegevens | X |  |  |
|  | Illegaal kopiëren van gegevens | X | X | X |
|  | Ongeoorloofd inzien van gegevens bijvoorbeeld bij invoer of printen | X | X | X |
|  | Onzorgvuldige vernietiging van gegevens | X | X | X |
| Omstandigheden op de werkplek | Uitval van elektriciteit | X |  |  |
| Wateroverlast door lekkage | X |  |  |
| (Faciliteiten) | Ongewenste trillingen | X |  |  |

| **BEHEER­INCIDENTEN** |  | **NIVEAU VAN MELDING \*)** |
| --- | --- | --- |
| **Incidenten categorie** | **Mogelijk incident** | **Helpdesk** | **CISO** | **Directie** |
| Identificatie en bevoegdheden van gebruikers | Geen eenduidige gebruiker bij een user-ID geconstateerd  | X | X |  |
|  | Ongeautoriseerde toegang door medewerker | X | X | X |
|  | Er komen gebruikers voor die niet meer bevoegd zijn (ex-medewerkers) | X | X |  |
|  | Vraagtekens bij bevoegdheden van bepaalde gebruikers of beheerders  | X | X |  |
| Onopzettelijk foutief handelen van gebruikers | Onzorgvuldige omgang met wachtwoorden door gebruikers | X | X |  |
| Opzettelijk foutief handelen van gebruikers | Kraken of omzeilen toegang door medewerkers of een buitenstaander  | X | X | X |
|  | Fraude of diefstal | X | X | X |
| Technisch falen van apparatuur | Storing in apparatuur | X | (X) |  |
| Technisch falen van apparatuur door externe invloeden | Wegvallen elektrische spanning of spanningsschommelingen | X | X | X |
|  | Wateroverlast | X | X | X |
|  | Uitval netwerkverbinding door aanval met grote hoeveelheden data | X | X | X |
| Omgang met apparatuur door gebruikers of derden | Beschadiging apparatuur | X | X | X |
| Diefstal van apparatuur | X | X | X |
|  | Apparatuur blijkt niet geregistreerd | X |  |  |
|  | Geregistreerde apparatuur blijkt niet aanwezig | X | X |  |
| Onopzettelijk foutief handelen | Fouten in handleiding | X |  |  |
| Problemen met programmatuur | Fouten in programmatuur | X | (X) |  |
|  | Ongeautoriseerde wijzigingen in programmatuur | X | X |  |
|  | Introductie van virussen via programmatuur | X | X | X |
|  | (On)opzettelijk ongeautoriseerd gebruik | X | X |  |
|  | Gebruik van ongeautoriseerde programmatuur | X | X |  |
| Gegevens en gegevensdragers | Ongeautoriseerde toegang tot gegevens | X | X | X |
|  | Zoekraken gegevensdragers | X | X | X |
|  | Diefstal van gegevensdragers | X | X | X |
|  | Beschadiging gegevensdragers | X |  |  |
|  | Onleesbaarheid van gegevensdragers | X |  |  |
|  | Fouten in gegevens door apparatuur | X |  |  |
|  | Fouten in gegevens door programmatuur | X |  |  |
|  | Opzettelijke invoer van foutieve gegevens | X | X | X |
|  | Onopzettelijke invoer van foutieve gegevens | X |  |  |
|  | Illegaal kopiëren van gegevens | X | X | X |
|  | Ongeoorloofd inzien van gegevens bijvoorbeeld bij invoer of printen | X | X | X |
|  | Onzorgvuldige vernietiging van gegevens | X | X | X |
| Facilitaire structuren en omgeving | Kortsluiting /stroomuitval | X | X | X |
| Wateroverlast door lekkage | X | X | X |
|  | Ongeoorloofde toegang tot computer­ruimte | X | X | X |
|  | Uitgifte sleutels aan ongeautoriseerde  | X | X | X |
| Diensten van derden | Cruciale diensten worden (tijdelijk) niet of onvoldoende geleverd | X | X |  |
|  | Niet gescreend personeel |  | X | X |
|  | Schending vertrouwelijkheid  | X | X | X |
|  | Misbruik van toevertrouwde middelen (gegevens, documentatie, en dergelijke) | X | X | X |
|  | Incidenten worden niet gemeld | X | X | X |
|  | Incidenten met informatie van de gemeente | X | X | X |

\*) Niveau van Melding:

* Helpdesk: Incidenten die door gebruiker en/of beheerder worden gemeld bij helpdesk.
* CISO: Incidenten die door helpdesk worden gemeld bij de CISO of andere Security Officer.
* Directie: Incidenten die door CISO worden gemeld bij directie.

# Bijlage 4: Definities

**Een gebeurtenis of event** is een waarneembare verandering in het normale gedrag van een systeem, omgeving, proces, workflow of persoon.

Er zijn drie basistypen van informatiebeveiligingsgebeurtenissen:

**Normaal** - een normale gebeurtenis heeft geen invloed op cruciale onderdelen van het systeem en zal ook niet eisen dat er extra controles moeten worden uitgevoerd. Normale gebeurtenissen vereisen geen interventie van hoger personeel of het management en er is geen melding van het event vereist.

**Escalatie** - een geëscaleerd event treft kritische productiesysteem of -systemen en vereist dat er maatregelen genomen moeten worden om mogelijke gevolgen in te perken en verdere schade, dan wel uitval, te voorkomen van dat systeem of deze systemen. Geëscaleerde gebeurtenissen vereisen de deelname van hoger personeel en het informeren van belanghebbenden zoals systeemeigenaren, leidinggevenden en het Response team.

**Emergency of noodsituatie** - een noodsituatie is een gebeurtenis die verregaande gevolgen zal hebben voor grote delen van de informatievoorziening en daarmee van de bedrijfsvoering van de gemeente, maar kan ook invloed hebben op de gezondheid of veiligheid van de mensen. Een noodsituatie vereist onmiddellijk handelen, maar niet nadat met zekerheid is vastgesteld wat er precies aan de hand is. Een noodsituatie kan alleen uitgeroepen worden door een incident coördinator na afstemming met het (lijn)management of de directie.

In alle gevallen moeten incidenten opgevolgd worden volgens een Computer Security Incident Response-plan op basis van de incident management en response checklist. Sommige incidenten kunnen voorspelt worden en dus kan er voor een aantal mogelijke incidenten van tevoren een Response-plan gemaakt worden.

**Incident Escalatie Regels**

Een set van regels waarin een hiërarchie voor escalatie Incidenten en triggers die leiden tot escalaties. Triggers zijn meestal gebaseerd op de ernst van incidenten en oplostijden.

**Incident management Rapport**

Een verslag leveren van Incident-gerelateerde informatie aan de andere managementprocessen.

**Incident Model of cheat sheet**

Een Incident-model bevat de vooraf gedefinieerde stappen die moeten worden genomen voor het omgaan met een bepaald type Incident. Dit is een manier om ervoor te zorgen dat regelmatig voorkomende incidenten daadwerkelijk en efficiënt worden afgehandeld. Zie ook bijvoorbeeld: <http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901?show=incident-handlers-handbook-33901&cat=incident>

**Incident Prioritering Leidraad**

De Incident Prioritering Leidraad beschrijft de regels voor het toekennen van prioriteiten aan incidenten, met inbegrip van de definitie van wat een Noodsituatie Incident. Omdat incident management escalatie regels meestal gebaseerd zijn op prioriteiten, is het toewijzen van de juiste prioriteit aan een incident essentieel voor het activeren van passende escalaties. Zie ook: Checklist Incident Prioritering Leidraad.

**Incident Record**

Een verzameling van gegevens met alle details van een incident, het documenteren van de geschiedenis van het incident van registratie tot sluiting. Elke gebeurtenis die mogelijk een risico kan gaan worden in de toekomst, is ook een incident (bijv. het uitvallen van een harde schijf van een reeks gespiegelde drives). Zie ook: Checklist Incident Record

**Incident Status Informatie**

Een bericht met de huidige status van een incident verzonden naar een gebruiker die eerder melding deed. Statusinformatie wordt doorgaans aan gebruikers op verschillende punten tijdens de levenscyclus van een incident.

MSSP staat voor Managed Security Services Provider

Dit kan ook uitgevraagd zijn via GGI veilig perceel 3.

**Proactieve gebruikersinformatie**

Een mededeling voor gebruikers van bestaande of dreigende incidenten of verstoringen, zelfs als de gebruikers zich nog niet bewust van de onderbrekingen, zodat gebruikers in staat zijn om zich voor te bereiden voor een periode van niet beschikbaarheid of verminderde van de dienst.

**Pers**

Pers woordvoering in verband met informatiebeveiligingsincidenten is een apart specialisme, besef dat goede woordvoering en goede communicatie een incident kunnen ondersteunen, maar ook dat verkeerde woordvoering voor een verdere escalatie kunnen zorgen.

**Support Aanvraag**

Een verzoek om een incident of probleem te ondersteunen, meestal uitgegeven door de Incident Manager wanneer verdere hulp nodig is van een derde partij zoals de IBD, maar ook het escaleren om daarmee anderen te kunnen waarschuwen.

**Gebruiker FAQ’s**

Zelf Help informatie voor gebruikers van de gemeente, meestal als onderdeel van de ondersteuningspagina's op het intranet.

**Aangifte**

Bij digitale inbraak moet altijd aangifte gedaan worden. Het maakt daarbij niet uit of de bedoeling achter inbraak per ongeluk of kwaadwillend was. Probeer zo mogelijk de aangifte te doen bij een digitaal rechercheur, dat vergemakkelijkt de aangifte.

**Triage expertise**

De gemeente kan gebruik maken van externe triage capaciteit voor het ondersteunen bij het uitvoeren van de triage en directe ondersteuning bij het oplossen van het incident.

**Forensische ICT**

Forensische ICT veelal aangeduid met 'IT Forensics' is een soort forensisch onderzoek dat zich richt op het vinden van juridisch bewijs in computers en digitale opslagmedia.

**Let op!** Indien de gemeente deelnemer is van GGI veilig dan moet Forensische ICT capaciteit worden afgenomen via GGI-Veilig. (zie: <https://www.scgemeenten.nl/project/ggi-veilig/>)

# Bijlage 5: Incident management en response beleid gemeente <gemeente>

Het incident management en response beleid van de gemeente geeft richting aan de wijze waarop de gemeente wenst om te gaan met alle incidenten en bijna incidenten op het gebied van informatiebeveiliging. De gemeente onderschrijft het belang van een adequate behandeling van incidenten en de response daarop om daarmee de gevolgen voor de bedrijfsvoering te minimaliseren. Incidenten dienen gestructureerd te worden behandeld en er moeten procedures worden vastgesteld om de reactie op incidenten doeltreffend en ordelijk te laten plaatsvinden. De gemeente wil leren van incidenten, en daarom moeten incidenten geëvalueerd worden. Dit beleid is van toepassing op de iedereen die werkzaam is bij de gemeente.

Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

De volgende uitgangspunten zijn vastgesteld voor de gemeente en deze zijn ontleend aan het gemeentelijk informatiebeveiligingsbeleid en de BIO:

1. Informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen worden zodanig kenbaar gemaakt dat de gemeente tijdig en adequaat corrigerende maatregelen kan nemen. Dit omvat ook het regelmatig beoordelen van loggegevens van informatiesystemen.
2. Informatiebeveiligingsgebeurtenissen moeten zo snel als mogelijk via de leidinggevende of de helpdesk of de CISO gerapporteerd worden.
3. Alle werknemers, ingehuurd personeel en externe gebruikers van gemeentelijke informatiesystemen en diensten moeten alle waargenomen of verdachte zwakke plekken melden volgens de procedure.
4. Informatiebeveiligingsincidenten moeten vastgelegd en beheerd worden en hiervoor zijn procedures gemaakt. Deze procedures moeten bekend zijn bij alle werknemers. In deze procedures moeten de verantwoordelijkheden belegd worden.
5. Informatiebeveiligingsmeldingen moeten periodiek beoordeeld worden met als doel de beheersmaatregelen te verbeteren.
6. Informatiebeveiligingsincidenten kennen soms een vervolgprocedure, daarom moet zoveel als mogelijk bewijsmateriaal verzameld worden in overeenstemming met de voorschriften.
7. Informatiebeveiligingsincidenten moeten geëvalueerd worden zodat de procedures kunnen worden bijgesteld en beheersmaatregelen kunnen worden verbeterd.
8. De CISO rapporteert periodiek een overzicht van de opgetreden beveiligingsincidenten en de impact op de bedrijfsvoering van de gemeente.



Nassaulaan 12

2514 JS Den Haag

CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)

CERT 24x7: Piketnummer (instructies via voicemail)

info@IBDGemeenten.nl / incident@IBDGemeenten.nl

Kijk voor meer informatie op:

www.informatiebeveiligingsdienst.nl

1. https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/ [↑](#footnote-ref-1)
2. <https://www.informatiebeveiligingsdienst.nl/product/handreiking-bedrijfscontinuiteitsbeheer/> [↑](#footnote-ref-2)
3. https://www.informatiebeveiligingsdienst.nl/product/vdw-module-1-mindmap-processen/ [↑](#footnote-ref-3)
4. https://www.informatiebeveiligingsdienst.nl/product/handreiking-coordinated-vulnerability-disclosure-bio/ [↑](#footnote-ref-4)
5. https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/ [↑](#footnote-ref-5)
6. https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/ [↑](#footnote-ref-6)
7. https://www.informatiebeveiligingsdienst.nl/aansluiten-bij-de-ibd/ [↑](#footnote-ref-7)
8. <https://www.informatiebeveiligingsdienst.nl/project/bewustwording/> [↑](#footnote-ref-8)
9. https://www.informatiebeveiligingsdienst.nl/product/vdw-module-1-mindmap-processen/ [↑](#footnote-ref-9)
10. https://www.informatiebeveiligingsdienst.nl/product/handreiking-coordinated-vulnerability-disclosure-bio/ [↑](#footnote-ref-10)
11. https://www.scgemeenten.nl/project/ggi-veilig/ [↑](#footnote-ref-11)
12. https://www.scgemeenten.nl/project/ggi-veilig/ [↑](#footnote-ref-12)
13. Zie Bijlage: Incident management en response stappenplan en sjabloon [↑](#footnote-ref-13)
14. Cheat sheets worden binnen het ICT-domein regelmatig gebruikt bij systeemontwikkeling en systeembeheer. [↑](#footnote-ref-14)
15. Zie hiervoor de [handreiking Digitaal Forensisch Onderzoek](https://www.informatiebeveiligingsdienst.nl/product/digitaal-forensisch-onderzoek/) [↑](#footnote-ref-15)
16. <https://www.informatiebeveiligingsdienst.nl/product/factsheet-gehackt-hoe-nu-verder/> [↑](#footnote-ref-16)
17. https://vng.nl/praktijkvoorbeelden/g4-ontwikkelt-handreiking-voor-bestrijding-gevolgen-cybercrises [↑](#footnote-ref-17)
18. https://assets.amsterdam.nl/publish/pages/946958/handreiking\_cybergevolgbestrijding\_g4\_-\_deel\_1\_warme\_fase.pdf [↑](#footnote-ref-18)