****

**Incident Response Plan**

Stappenplan aangeleverd door Lumen Group, ter ondersteuning in de naleving van de wettelijke verplichting uit de AVG (Artikel 32 AVG)

|  |  |
| --- | --- |
| **Versie** | V1.0 |
| **Auteur** | Lumen Group |
| **Opsteldatum** | 17 oktober 2022 |

Incident Response Stappenplan

**Versiebeheer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datum** | **Auteur** | **Versie** | **Status** | **Aanpassing** |
|  |  |  |  |  |

**Goedgekeurd**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Naam goedkeurder** | **Functie** | **Handtekening** |
|  |  |  |  |

[Creative Commons-Licentie](http://creativecommons.org/licenses/by-nc-sa/4.0/)  
Privacybeleid Werknemers Beleidsmodel aangeleverd door Lumen Group inclusief bijlagen ter ondersteuning in de naleving van de wettelijke verplichting uit artikelen 5, 24 en 32 AVG en ISO 18.1.4. van [Lumen Group](https://www.lumengroup.nl/) is in licentie gegeven volgens een [Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 4.0 Internationaal-licentie](http://creativecommons.org/licenses/by-nc-sa/4.0/).  
Toestemming met betrekking tot rechten die niet onder deze licentie vallen zijn beschikbaar via <https://www.lumengroup.nl/disclaimer/>.

De verantwoordelijkheid en aansprakelijkheid blijft bij de gebruiker voor: 1. Het bestuur en bedrijfsvoering van de organisatie. Hieronder valt onder andere de uitoefening van de bedrijfsactiviteiten in het kader van de verwante zakelijke aangelegenheden; en 2. De genomen beslissingen van de gebruiker die in een bepaalde mate gebaseerd zijn op de door Lumen Group geleverde adviezen, aanbevelingen of documenten.

**Inhoudsopgave**

[**1.** **Inleiding** 4](#_Toc115640250)

[**2.** **Stappenplan** 6](#_Toc115640251)

[**2.1** **Identificatie, detectie en initiatie** 6](#_Toc115640252)

[**2.2** **Analyse** 7](#_Toc115640255)

[**2.3** **Indammen van de schade** 8](#_Toc115640257)

[**2.4** **Herstel** 9](#_Toc115640258)

[**2.5** **Remediatie** 9](#_Toc115640259)

[**2.6** **Kennisgeving en communicatie** 10](#_Toc115640260)

[**2.7** **Evaluatie** 10](#_Toc115640261)

[**Bijlage A – Incident Response Teams Rollen en Verantwoordelijkheden** 11](#_Toc115640262)

[**Bijlage B - Incident Response Management Checklist** 13](#_Toc115640265)

# **Inleiding**

Dit Incident Response Plan bestaat uit een aantal te nemen stappen, bij een groot informatiebeveiligingsincident, zoals een cyberaanval. Dit betreft dus geen (reguliere) datalekken, waarbij persoonsgegevens zijn gelekt, maar (grootschalige) informatiebeveiligingsincidenten en -aanvallen waarbij de continuïteit van de bedrijfsvoering en de reputatie van de organisatie op het spel staan.

Formeer een Incident Response Team

Een goede voorbereiding is het halve werk. Formeer daarom een Incident Response Team en wijs een Incident Response Manager aan vóórdat de hierna genoemde stappen daadwerkelijk genomen worden. Formeer een crisisteam afhankelijk van de grootte van de organisatie en de mogelijke impact van het incident. Maak bij de keuze van de teamsamenstelling gebruik van de rollen en verantwoordelijken zoals genoemd in Bijlage A.

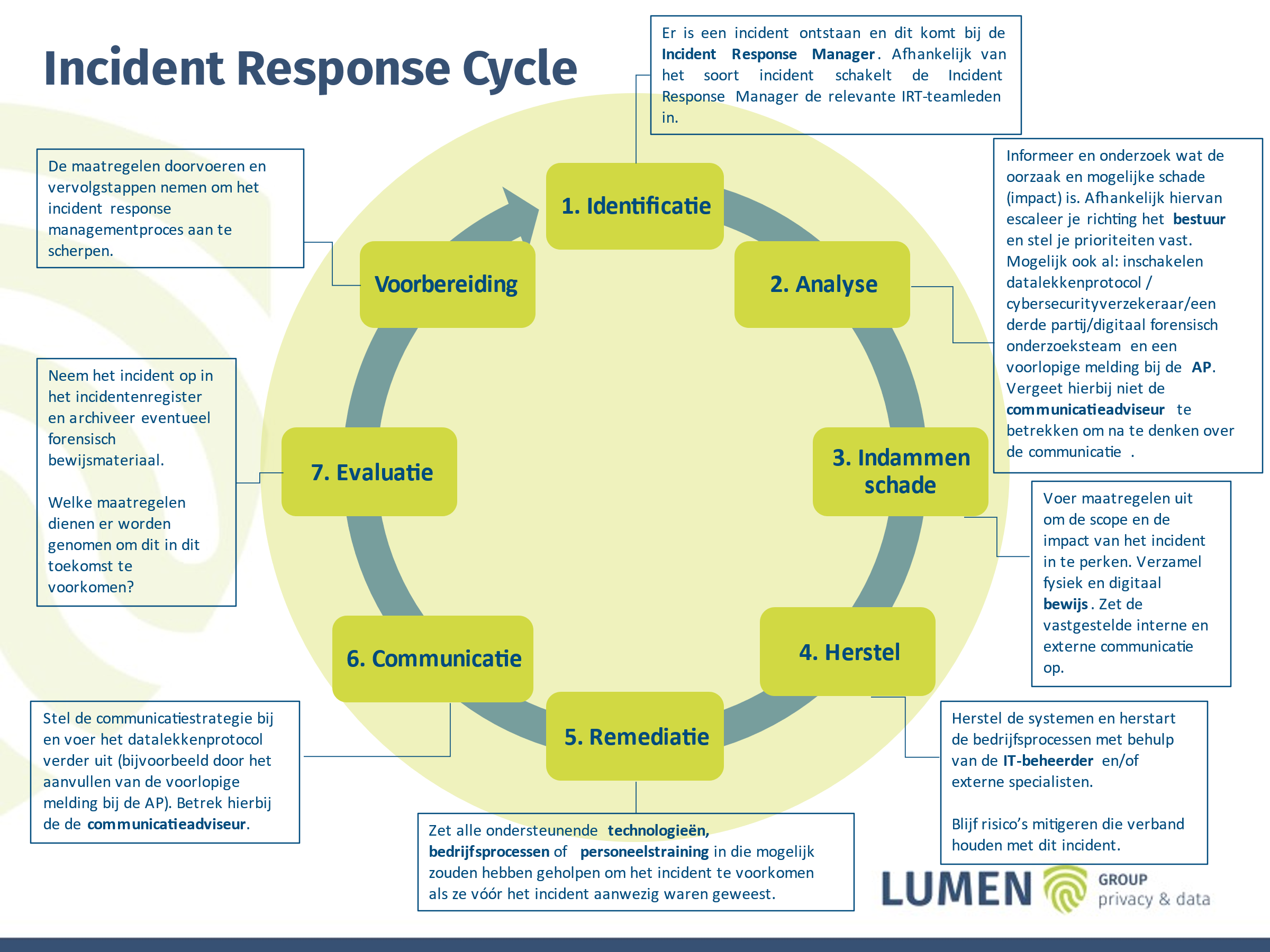
Stappenplan en response Checklist

In zeven stappen geeft dit Incident Response Plan aan wat te doen. Houd de ‘Incident Response Management Checklist’ (Bijlage B) erbij en vul deze zoveel als mogelijk in. In deze Checklist wordt specifiek per stap aangegeven welke actie(s) vereist is (of zijn).

De zeven stappen staan in Hoofdstuk 2 toegelicht. Afhankelijk van de situatie, kunnen sommige stappen parallel uitgevoerd worden. In het geval van een ransomware-aanval bijvoorbeeld, kan het nodig zijn om direct naar stap 3 of 4 over te gaan en deze stap(pen) parallel te doorlopen met de eerste stappen, om zo snel mogelijk de dienstverlening/bedrijfsvoering/werkzaamheden te kunnen hervatten. Hierbij in het kort een overzicht van de stappen:

1. De eerste stap is de ontdekking van het informatiebeveiligingsincident en afhankelijk van het soort beveiligingsincident schakelt de **Incident Response Manager** met de hiervoor vastgestelde **Incident Response Team-leden**.
2. Analyseer het beveiligingsincident tijdens de tweede stap en escaleer (indien nodig) richting het **bestuur** en schakel eventueel een digitaal forensisch onderzoeksteam in. De **communicatieadviseur** kan hier ook al een rol spelen. De schade als gevolg van het incident stel je vast en bewijsmateriaal stel je veilig.
3. Vervolgens probeer je de schade en de mogelijke impact van het beveiligingsincident zoveel als mogelijk in te dammen door maatregelen uit te voeren. Ook verzamel je bewijs en zet je de interne en externe communicatie op.
4. Herstel de systemen en herstart de bedrijfsprocessen met behulp van de **IT-beheerder**, eventuele extra capaciteit van leveranciers en/of externe specialisten. Mitigeer de risico’s die verband houden met dit incident.
5. Bij de vijfde stap zet je alle ondersteunende **technologieën, bedrijfsprocessen** of **personeelstraining** in die mogelijk zouden hebben geholpen om het incident te voorkomen als ze vóór het beveiligingsincident aanwezig waren geweest.
6. Vervolgens stel je de communicatiestrategie eventueel bij. Betrek hierbij de **communicatieadviseur**.
7. Tot slot: Leer van het beveiligingsincident door het te bespreken. Welke maatregelen dienen er worden genomen om dit in dit toekomst te voorkomen?

Deze maatregelen voer je door. Scherp het incidentmanagementproces met deze evaluatie aan (PDCA).[[1]](#footnote-2) Het incidentmanagement is hiermee een continu proces, zoals hieronder afgebeeld.



# **Stappenplan**

# **Stap 1 - Identificatie, detectie en initiatie**

Er is een incident ontstaan. Een signaal of een melding hiervan kan binnenkomen via verschillende kanalen of bronnen binnen ORGANISATIENAAM. Denk hierbij niet alleen aan interne meldingen, maar ook aan signalen vanuit organisaties waarmee wordt samengewerkt, de pers, of een ICT-systeem.

De eerste stap na het ontdekken van een beveiligingsincident dat heeft plaatsgevonden of nog gaande is, is het inschakelen van de Incident Response Manager. Afhankelijk van het soort incident betrekt de Incident Response Manager de hiervoor aangewezen leden van het Incident Response Team (IRT)[[2]](#footnote-3). In ieder geval is dat de IT-verantwoordelijke (CISO/Security Officer). Indien ORGANISATIENAAM een cybersecurityverzekering heeft afgesloten, neem dan contact op met de expert(s) van de verzekeraar en kijk voor de volgende stappen samen verder wat te doen.

Als een incident snel escaleert of ervoor zorgt dat de primaire organisatietaken hinder ondervinden en/of de dienstverlening van ORGANISATIENAAM in gevaar komt en mogelijk voor langere tijd minder of niet beschikbaar is, schakel dan het bestuur van ORGANISATIENAAM in.

Let op: bij grootschalige verstoringen van de (ICT)dienstverlening, bijvoorbeeld doordat bestandssystemen zijn versleuteld (in het geval van bijvoorbeeld een ransomware-aanval), ga direct door naar stap 3 of 4 om zo snel mogelijk de dienstverlening te kunnen hervatten. In overeenstemming met stap 3 (indammen van de schade) staak je bijvoorbeeld direct het gebruik van een gecompromitteerde applicatie of server en voer je in dat geval parallel de eerste stappen van dit Incident Response Plan uit.

In deze fase wordt door ieder lid van het IRT ook gestart met het bijhouden van de acties in de Checklist (Bijlage B) en het vastleggen van de genomen stappen in een logboek door het hiervoor aangestelde IRT-notulist.

Een veel voorkomend beveiligingsincident is bijvoorbeeld ransomware aanval.

Te herkennen aan:

* Ongebruikelijke facturen of andere zakelijke e-mails, mogelijk voorzien van malafide bijlagen of koppelingen;
* Ransomware berichten op het bestandssysteem;
* Ransomware meldingen op het beeldscherm;
* Ransomware berichten via e-mail;
* Medewerkers melden dat zij hun bestanden niet meer kunnen openen;
* Grote hoeveelheden bestanden worden (achtereenvolgens) aangepast op een (netwerk) bestandssysteem;
* Een ongebruikelijk(e) (grote) hoeveelheid data wordt weggesluisd;
* Systeemanalyse leidt tot identificatie van server-side versleuteling;
* Er worden aankondigingen gedaan van een geslaagde ransomware-aanval door bekende actoren op het darkweb.

Acties om beveiligingsincidenten te identificeren:

* In Windows onder computermanagement bij “Sessions” en bij “Open Files “; controleer op verbonden systemen/gebruikers;
* Eigendom van versleutelde bestanden; controleer het account dat deze bestanden wegschrijft;
* Zorg na de waarneming van een ransomware-aanval voor een actueel situationeel beeld (welke systemen zijn getroffen en wat is de functie van die systemen, wie is verantwoordelijk voor dat systeem) en een impactassessment zodat te nemen maatregelen daarop aansluiten.

# **Stap 2 - Analyse**

De analyse fase in het incidentmanagementproces is bedoeld om beschikbare informatie te onderzoeken om vast te stellen met wat voor soort incident men te maken heeft en wat de oorzaak van het incident is (geweest). De schade als gevolg van het incident wordt vastgesteld en bewijsmateriaal wordt veiliggesteld.

## Inschakelen externe partij(en)

Op het moment dat een (digitaal) informatiebeveiligingsincident wordt opgemerkt moeten er keuzes gemaakt worden op basis van urgentie en impact. In het begin van het incident managementproces kan ondersteuning door een externe partij helpen om de juiste maatregelen te nemen die verdere schade voorkomen en om bewijsmateriaal veilig te stellen. Maak daarom een melding van het incident bij het Computer Emergency Response Team (hierna: CERT) behorende bij de branche van ORGANISATIENAAM.

* Voor primair en voortgezet onderwijs wordt er door SIVON, Kennisnet, PO-Raad, VO-raad en het ministerie van OCW samen een CERT opgericht. Neem het alarmnummer hierin op zodra deze bekend is;
* Voor het hoger onderwijs is SURFcert 24/7 bereikbaar via Alarmnummer: +31 6 22 92 35 64;
* Organisaties in de zorg kunnen deelnemer worden van Z-CERT en als deelnemer incidenten mailen naar cert@z-cert.nl;
* Bij een (dreigend) incident waar een gemeente bij betrokken is, is het alarmnummer: +31 070 204 55 11.

## Digitaal forensisch onderzoeksteam

Schakel, indien gewenst of nodig (bijvoorbeeld als de cybersecurityverzekering dat vereist) een digitaal forensisch onderzoekteam in. Het uitvoeren van digitaal forensisch onderzoek helpt enerzijds bij het oplossen van het incident, anderzijds om digitaal bewijsmateriaal veilig te stellen.

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 men aan het management/bestuur van ORGANISATIENAAM goedkeuring vragen.

Vragen die de forensisch onderzoeker en andere externe partijen beantwoordt:

* Wat is er gebeurd?
* Hoe kon dit gebeuren?
* Hoe lang is dit al aan de hand?
* Is het incident nog bezig of al afgelopen?
* Wie/welke kwaadwillenden heeft/hebben toegang gehad (IP adres of inlog)?
* Om welke systemen en applicaties gaat het?
* Welke persoonsgegevens zijn er geraakt?

Verzamel zoveel als mogelijk (al dan niet samen met mogelijke externe partijen) fysiek en digitaal bewijs, wat een duidelijke gedetailleerde beschrijving geeft van hoe de data gecompromitteerd kon worden. Houd bij waar het bewijsmateriaal zich bevindt en wie er toegang toe heeft. Bijvoorbeeld door een inventarisatielijst van al het bewijsmateriaal te maken en bij te houden wie, wanneer, wat gedaan heeft hiermee.

Vervolgens bepaalt het IRT, nadat er voldoende informatie verzameld is, de prioriteiten voor het aanpakken van het incident. Zijn er mogelijk persoonsgegevens getroffen en is het dus (ook) een datalek dat onder de AVG valt, dan moet eveneens het Datalekkenprotocol opgestart worden. Als bekend is dat het een datalek is dat gemeld moet worden bij de Autoriteit Persoonsgegevens (hierna: AP), maar nog niet alle gegevens over het datalek bekend zijn, maak dan een voorlopige melding bij de AP. Later kan deze alsnog aangevuld of ingetrokken worden. Op die manier wordt ervoor gezorgd dat er in ieder geval binnen de wettelijke termijn van 72 uur een melding gemaakt wordt bij de AP.

Communicatie

Tegelijkertijd zal in relatie tot stap 6 (Kennisgeving en communicatie) nu al nagedacht moeten worden over de communicatie richting de medewerkers (intern), maar afhankelijk van de situatie ook extern met en het notificeren van externe stakeholders en mogelijke betrokkenen. Betrek de aangewezen communicatieadviseur van het IRT hierbij. Communicatie of bewust nog geen communicatie kan in dit stadium al een strategische overweging zijn om een calamiteit en/of crisis te managen.

* Intern communiceren om medewerkers helderheid te bieden om ruis en onrust op de werkvloer te voorkomen;
* Naar de buitenwereld communiceren om de reputatie van en het vertrouwen in de organisatie te beschermen en/of te herstellen. Dit vereist dat zo veel mogelijk onzekerheid wordt weggenomen door zorgvuldig informatie te verstrekken, een handelingsperspectief te bieden en duiding te geven aan wat er gebeurt. Maak hierbij een afweging om bij de communicatie naar buiten toe een splitsing te maken tussen/bij de betrokkenen en eventuele andere belanghebbenden. Iedereen is vooral gebaat bij open communicatie om vervolgschade te beperken.

# **Stap 3** **- Indammen van de schade**

Als de analyse is afgerond volgt het wegnemen van de oorzaak van het incident (als dat niet direct is gebeurd na ontdekking) en het indammen van de schade. Het wegnemen van de oorzaak van het incident en het indammen van de schade zijn randvoorwaarden voor de volgende stap, herstel. Denk hierbij bijvoorbeeld aan:

* Verhelp eventuele kwetsbaarheden die tijdens het incident zijn uitgebuit. Dit omvat onder andere de technische kwetsbaarheden die het mogelijk hebben gemaakt dat een hack-aanval of ander incident heeft plaatsgevonden. 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.
* Het verwijderen van de actieve en opgeslagen inhoud op publiek toegankelijke websites, als het incident betrekking heeft op gevoelige gegevens die onjuist geplaatst zijn. Verzoek om verwijdering van de gecachte of in proxy opgeslagen webpagina(‘s), die geïndexeerd zijn door zoekmachine bedrijven en andere Internet-archiefbedrijven, zoals bijvoorbeeld de Wayback Machine.
* Het preventief uitschakelen van (delen van) systemen of andere mitigerende maatregelen nemen.
* De vastgestelde interne en externe communicatiestrategie uitvoeren. Zorg dat de betrokken stakeholders (raad van bestuur, medewerkers, (keten)partners, klanten) tijdig en passend worden geïnformeerd. Schakel hiervoor met de aangewezen communicatieadviseur van het IRT.
* Bepaal hier ook welke soort gegevens mogelijk zijn blootgesteld door het beveiligingsincident. Als het geen persoonsgegevens betreft en herstel goed mogelijk is, dan is geen verdere actie noodzakelijk op dit vlak. Als het wel persoonsgegeven betreft, moeten betrokkenen mogelijk in kennis worden gesteld. Als eerder al ontdekt is dat er een datalek is en er een (voor)melding gedaan is aan de AP, vul dan de melding bij de AP verder aan. Volg het Datalekkenprotocol en raadpleeg de FG. Informeer indien noodzakelijk andere organisaties en overleg met de communicatieadviseur van het IRT.

# **Stap 4 - Herstel**

Na het wegnemen van de oorzaak en het indammen van de gevolgen, volgt de stap om de systemen te herstellen en de bedrijfsprocessen te herstarten als deze gestopt waren.

In deze fase is het belangrijk om ook te blijven controleren of er sporen van eventuele buitgemaakte informatie te vinden zijn op het internet of Darkweb. Schakel hiervoor desgewenst een bedrijf in dat hierin is gespecialiseerd. Mocht uit deze sporen blijken dat er persoonsgegevens zijn buitgemaakt, volg dan alsnog direct het Datalekkenprotocol.

Voor computersystemen op werkplekken en voor 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 leveranciers. 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 bruikbaar is.

# **Stap 5 -** **Remediatie**

Hoe kon dit gebeuren? Zet alle ondersteunende technologieën, bedrijfsprocessen en personeelstraining in die mogelijk zouden hebben geholpen om het incident te voorkomen als ze vóór het incident aanwezig waren geweest.

Check nogmaals of eventuele kwetsbaarheden die tijdens het incident zijn uitgebuit, wel echt zijn verholpen. Dit omvat onder andere de technische kwetsbaarheden die het mogelijk hebben gemaakt dat een hack-aanval of ander incident heeft plaatsgevonden. 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.

# **Stap 6 - Kennisgeving en communicatie**

Denk na over (mogelijk al in stap 2 gedane) communicatie met en het notificeren van externe stakeholders en betrokkenen. Neem beslissingen op basis van de bevindingen van het IRT en betrek altijd de aangewezen communicatieadviseur van het IRT hierbij.

* Wie zal zich bezighouden met het beantwoorden van telefoon en e-mail op vragen? Rechtvaardigt het verwachte volume het opzetten of inzetten van een callcenter?
* Is het noodzakelijk om een officieel persbericht uit te laten gaan en te plaatsen op de website van ORGANISATIENAAM?

# **Stap 7 - Evaluatie**

* Volg de taken op, zoals genoemd in de checklist (bijlage B);
* Neem het incident op in het incidentenregister. 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.
* Archiveer het forensisch bewijsmateriaal.
* Leer van het incident, door dit te bespreken met het team. Welke vervolgstappen en maatregelen worden er genomen om het incident in de toekomst te voorkomen? Hoe kan het incidentmanagementproces worden verbeterd?
* Scherp het incidentmanagementproces met deze evaluatie aan (PDCA). [[3]](#footnote-4)

# **Bijlage A – Incident Response Teams Rollen en Verantwoordelijkheden**

De teamsamenstelling is essentieel voor een adequate reactie om het incident zo klein als mogelijk te houden. Formeer een crisisteam afhankelijk van de impact van het incident. Beoordeel door te oefenen of teamsamenstellingen juist zijn, pas indien nodig aan en laat het team goedkeuren door het bestuur.

De basis samenstelling van het Incident Response Teams bestaat in ieder geval uit:

|  |  |
| --- | --- |
| **Rollen** | **Verantwoordelijkheden** |
| Een Incident Response Manager   * Bijvoorbeeld de privacy coördinator, de IT-manager of de CISO | * Deze zet de noodzakelijke stappen om het incident op te kunnen lossen; * Schakelt de noodzakelijke andere IRT’ers en (externe) partijen in; * Schakelt om communicatie op te zetten; * Stuurt het IRT aan. |
| De vertegenwoordiger van het management als voorzitter   * Bijvoorbeeld de Directeur | * Eindverantwoordelijk, ook naar buiten toe; |
| De vertegenwoordiger van de business/dienstverlening   * Bijvoorbeeld de Voorzitter College van Bestuur; | * Eindverantwoordelijk, ook naar buiten toe. |
| De Chief Information Security Officer (Hierna: CISO) | * Controleren en adviseren over de informatiebeveiligingsmaatregelen. |
| Security Officer | * Registreert en evalueert de incidentafhandeling. |
| Een technisch specialist / IT-beheerder | * Technisch aanspreekpunt voor IBP-incidenten. |
| Een communicatieadviseur | * Communicatie richting medewerkers; * Communicatie richting betrokkenen; * Eventueel communicatie richting externe stakeholders en/of de pers. |
| Een privacy coördinator | * Coördineren van privacyactiviteiten; * Eerste aanspreekpunt voor medewerkers voor vragen of opmerkingen; * Interne afhandeling van informatieverzoeken en andere rechten van betrokkenen; * Schakelpunt voor de FG; * Evalueren van het IBP-beleid en de genomen maatregelen. |
| De FG | * Houdt toezicht op naleving privacywetgeving en de verwerkingen van persoonsgegevens; * Informeert ORGANISATIE over verplichtingen die uit de AVG voortvloeien; * (Ongevraagd) Adviseren en aanbevelingen doen over privacy en informatiebeveiliging in het algemeen en de toepassing van de AVG. |
| Een notulist | * Vastleggen acties; * Zorgt voor de verslaglegging. |

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

* Burgemeester
* Portefeuille houder/Wethouder
* Crisismanager (Openbare Orde en Veiligheid (Hierna: OOV))
* Adviseur OOV
* Juridisch adviseur
* Leider forensisch onderzoeksteam
* Leveranciers (bijvoorbeeld ICT of MSSP)
* De Informatiebeveiligingsdienst (online)
* Politie
* Brandweer

# **Bijlage B - Incident Response Management Checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| **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. | Incident Response manager |  |
|  | Noteer de gegevens van de melder | Incident Response manager |  |
| **STAP 1: Identificatie en 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. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden.** | | | |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 1.1   Onmiddellijk blootstelling beperken: | De betrokken afdeling |  |
|  | Als een elektronisch apparaat is gecompromitteerd: |  |  |
|  | * Niet gebruiken (niet inloggen) of wijzigen van het apparaat; |  |  |
|  | * Zet het apparaat niet uit als het aan staat; |  |  |
|  | * Haal de netwerkverbindingen er af, maar NIET de voedingskabel |  |  |
|  |  |  |  |
|  | 1.2 Stel indien het incident daarom vraagt een incident manager aan | Incident Response manager |  |
|  | 1.3   Waarschuw indien nodig de CISO en/of IT-beheerder | Incident Response manager |  |
|  | 1.4   Schakel met de relevante IRT-leden   * *Voeg namen en telefoonnummers, e-mailadressen of indien mogelijk de link naar een online meldingsformulier toe.* | Incident Response manager |  |
|  | 1.5   Indien het incident over elektronische apparaten gaat of als er media gestolen of verloren is, dan ook aangifte doen bij de politie. | De betrokken afdeling |  |
|  | 1.6 Start met een logboek waarin gedurende het incident alle activiteiten op datum en tijd kunnen worden vastgelegd. | Incident Response manager |  |
| **STAP 2: Analyse** | | | |
| **Controleer of een incident daadwerkelijk heeft plaatsgevonden. Deze activiteit kan ook het gevolg zijn van proactieve detectie van incidenten door de ICT-beveiliging of het systeembeheer. Start een grondige beoordeling van de aard en omvang van het incident en stel vast wat de schade is. Indien wordt vastgesteld dat het inderdaad een incident is, dan moeten de medewerkers 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 hoogste management geïnformeerd worden en deze moet tijdens het verloop van het incident op de hoogte gehouden worden:   * Indien het incident ook het lekken van persoonsgegevens betreft, leg dit dan nu vast en stel het Datalekkenprotocol in werking. * Maak een melding van het incident bij het CERT en/of schakel de cybersecurityverzekeraar in (indien van toepassing). * Voor de beoordeling van de ernst van het incident moet mogelijk een forensisch onderzoeksteam ingeschakeld worden. Overleg hiervoor met het hoogste management. | IRT en Incident Response Manager |  |
|  | 2.2    Indien er sprake is van criminele activiteiten in verband met het incident moet bepaald worden of de politie het onderzoek moet overnemen. Als dat gebeurt zal dit het vervolg van dit schema beïnvloeden. | IRT en Incident Response Manager |  |
|  | 2.3 Afhankelijk van de zwaarte van het incident moet nu ook het IRT verder worden samengesteld met de juiste specialisten:   * Zorg ervoor dat de vertegenwoordiger van de afdeling 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 IRT:   * Verstrek ieder teamlid de incident response management Checklist. * Bespreek de communicatiestrategie. * Bespreek het belang van het goed in een tijdlijn documenteren en het voorkomen van het verloren raken van onderzoeksgegevens. * Verzamel zoveel als mogelijk (al dan niet samen met mogelijke externe partijen) fysiek en digitaal bewijs, wat een duidelijke gedetailleerde beschrijving geeft van hoe de data gecompromitteerd kon worden. Houd bij waar het bewijsmateriaal zich bevindt en wie er toegang toe heeft. Bijvoorbeeld door een inventarisatielijst van al het bewijsmateriaal te maken en bij te houden wie, wanneer, wat gedaan heeft hiermee. |  |  |
|  | *Let op: 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 externe partijen. Bijvoorbeeld:*   1. *Teamleden mogen niet praten met anderen buiten het team over het incident totdat er daarvoor toestemming is gegeven door het management of de CISO.* 2. *Alle documentatie die door het team geschreven wordt moet op feiten gebaseerd zijn omdat het mogelijk in een strafrechtelijk onderzoek gebruikt kan worden.* 3. *Er is dagelijks overleg tussen de teamleden.* 4. *Het team moet bijhouden hoeveel tijd er besteed wordt en waaraan.* |  |  |
|  | 2.5 Houd rekening met het Datalekkenprotocol, afhankelijk of er sprake is van een datalek is en deze valt onder de meldplicht datalekken van de AVG, dan moet er binnen 72 uur op basis van de beschikbare gegevens een (voorlopige) melding gedaan worden bij de AP. Raadpleeg hiervoor de FG. | Privacy-Coördinator en FG |  |
|  | 2.6 Communiceer indien nodig intern/extern: richting de medewerkers (intern), maar afhankelijk van de situatie ook extern met en het notificeren van externe stakeholders en mogelijke betrokkenen. | Communicatieadviseur |  |
| **STAP 3: Schade indamming en verdere beoordeling van de blootstelling** | | | |
| **Het bij het incident passend ‘Incident Response team’ is belast met het beperken van verdere schade als gevolg van het incident. 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. Verzamel en stel bewijsmateriaal veilig en voer de vastgestelde interne en/of externe communicatie uit.** | | | |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 3.1 Beoordeel in overleg met het IRT of forensische ICT-capaciteit nodig is om digitaal bewijs te verzamelen voor opsporing, beoordeling van de schade en impact voor betrokkenen en organisatie. | Incident Response Team |  |
| *3.2 Verzamel fysiek en digitaal bewijs die tezamen een duidelijke, gedetailleerde beschrijving geven van hoe de data gecompromitteerd kon worden, bijvoorbeeld:*  *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. Maak een inventarisatielijst van alle bewijsmateriaal en houdt bij wie, wanneer, wat gedaan heeft met het bewijsmateriaal. Bijvoorbeeld:  *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.*  *Beoordeel en bepaal waar de data zich bevindt en wijzig dit indien nodig om een hogere beschermingsgraad te verzekeren.* |
|  | 3.4 Neem maatregelen om de scope en de impact van het incident in te perken. Bijvoorbeeld:   * 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. * Wijzig verder waar nodig de wachtwoorden die mogelijk gecorrumpeerd zijn. * Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico’s voor gevoelige dataopslag. * Staak de exploitatie van een gecompromitteerde applicatie of server. |  |  |
|  | 3.5 Indien nodig, voer forensisch onderzoek uit en leg dit vast:   * Analyseer bewijsmateriaal; * Voer een reconstructie uit van het incident; * Zorg voor gedetailleerde documentatie.   *Tip: 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 inschatting van het incident af, en de documentatie over soort en afbakening van de blootgestelde data, evenals de beschikbaarheid en het soort van contactinformatie van de betrokken personen. |  |  |
|  | 3.7 Pas de communicatiestrategie naar aanleiding van nieuwe bevindingen en/of ontwikkelingen eventueel aan. | Communicatieadviseur |  |
| **STAP 4: Herstel** | | | |
| **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 Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze hersteld worden. | IT-beheerder | N.B. Wanneer veel systemen getroffen zijn kan deze stap maanden in beslag nemen |
| * Indien nodig overleg met het hoogste management in verband met hogere capaciteit leveranciers en/of de hiervoor ingeschakelde externe partij. |
|
|  | 4.2 Pas de communicatiestrategie aan:   * Overweeg opnieuw, als dat eerder nog niet vastgesteld kon worden, of er sprake is van een inbreuk op persoonsgegevens? Als er sprake is van een incident met persoonsgegevens waarbij een aanzienlijke kans bestaat op ernstige nadelige gevolgen voor de betrokkene(n), dient de AP onverwijld in kennis gesteld te worden. Stel alsnog het Datalekkenprotocol in werking. * Als eerder al ontdekt is dat er een datalek is en dat er een (voor) melding gedaan is aan de AP, dan moet melding bij de AP worden aangevuld indien mogelijk en beslist worden of betrokkenen ook geïnformeerd moeten worden. * Informeer indien noodzakelijk andere organisaties en overleg met de toegewezen communicatieadviseur. * Informeer en raadpleeg de FG. Meld ook aan de FG als het incident is opgelost. | FG en Communicatieadviseur |  |
| **STAP 5: Remediatie** | | | |
| **Zet alle ondersteunende technologieën, bedrijfsprocessen of personeelstraining in die mogelijk zouden hebben geholpen om het incident te voorkomen als ze vóór het incident aanwezig waren geweest.** | | | |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 5.1 Check nogmaals of eventuele kwetsbaarheden die tijdens het incident zijn uitgebuit, wel echt zijn verholpen. Ga terug naar stap 3 en zoek naar aanvullende manieren om de blootstelling te beperken. Mitigeer de risico’s die verband houden met dit incident:   * *Beoordeel bijvoorbeeld de inventarisatie van getroffen hardware en systemen en wijzig verder waar nodig de wachtwoorden die mogelijk gecorrumpeerd zijn.* * *Stop eventueel gecorrumpeerde diensten of applicaties en zorg voor work-arounds.* * Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico’s voor gevoelige dataopslag. |  |  |
|  | 5.2 Coördinatie van ondersteunende technologieën, bedrijfsprocessen of personeelstraining in die mogelijk zouden hebben geholpen om het incident te voorkomen als ze vóór het incident aanwezig waren geweest. |  |  |
|  | 5.3 *Beperk de toegang tot systemen tot uitsluitend degenen die toegang nodig hebben.*  *Tip: Gebruik software tools om gevoelige data te vinden, te verwijderen en te beschermen, bijvoorbeeld: Identity Finder.* | IT-beheerder |  |
| **STAP 6 : Communicatie** | | | |
| **Stel vast welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffenen in kennis van het feit dat hun gegevens blootgesteld zijn. Stel hierop de (eerder vastgestelde) communicatiestrategie verder af. Snelheid is geboden indien er persoonsgegevens verloren zijn gegaan of bekend geworden zijn aan niet rechthebbenden. Informeer indien noodzakelijk andere instanties en/of de politie. 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*** |
|  | 6.1 Neem beslissingen op basis van de bevindingen van het Incident response team:   * Geeft de mate van risico blootstelling de noodzaak tot het informeren van getroffenen? Zo ja: * 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 uit te laten gaan en te plaatsen op de website van ORGANISATIENAAM? | Communicatieadviseur |  |
|  | 6.2 Als dat nog niet eerder is gedaan, moet de reeds in stap 2 en/of 4 gedane voorlopige melding worden aangevuld bij de AP. Ook moet worden overwogen of en hoe in verband met de gelekte data de betrokkenen moeten worden geïnformeerd.   * Informeer en raadpleeg de FG. Meld ook aan de FG als het incident is opgelost. | Incident Response Manager en FG |  |
| **STAP 7 : 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 draaiboek aan.** | | | |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 7.1 Welke maatregelen dienen er worden genomen om dit in dit toekomst te voorkomen? Onderzoek oplossingen om herhaling te voorkomen. Indien nodig rapporteer hierover aan het management.  Beantwoord hierbij de volgende vragen:   1. Waarom was de data opgeslagen op een verkeerde plaats of niet veilige plaats? 2. Wat hadden we meer kunnen doen om de inbraak te voorkomen? 3. Neemt de afdeling voldoende maatregelen om herhaling te voorkomen? |  |  |
|
|  | 7.2 Leer van het incident door het te bespreken met het IRT:   * Plan een vergadering ongeveer 2 tot 6 weken na het incident om een evaluatie uit te voeren over de aanpak van het incident. * 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 maar om te onderzoeken of het proces goed gevolgd is of dat er verbeterpunten zijn aan het proces.)* * Pas eventueel de rollen en verantwoordelijkheden aan en plan oefensessies in om de werkbaarheid van het incident management te testen. | Incident response team |  |
|  | 7.3 Plan oplossingsprojecten om de geleerde lessen effectief in te bedden in de organisatie. | Incident Response Manager |  |
|  | 7.4 Neem het incident op in het incidentenregister.   * *Indien het een inbreuk betreft van de bescherming van persoonsgegevens moet altijd een overzicht hiervan worden bijgehouden.* | Privacy-Coördinator |  |
|  | 7.5 Verzamel alle tijdschrijfregels van het personeel dat heeft meegewerkt aan de Incident response-actie. De totale kosten kunnen mogelijk van belang zijn voor vergoeding door de cybersecurityverzekering en/of indien er een rechtszaak komt tegen een verdachte, omdat deze dan verhaald kunnen worden. | Iedereen die tijd geschreven heeft rapporteert aan het management |  |
|  | 7.6 Archiveer eventueel forensisch bewijsmateriaal.   * Sla alle Incident en response informatie veilig op, inclusief gesprekverslagen, aantekeningen en incident artefacten. In overeenstemming met wetgeving en het interne bewaar- en vernietigingsbeleid zal op enig moment (een deel van) de opgeslagen informatie vernietigd moeten worden. | Incident Response Manager |  |

1. Lumen Group heeft een ‘[Handreiking PDCA-cyclus](https://www.lumengroup.nl/knowledgebase/handreiking-pdca-cyclus-voor-privacy-en-informatiebeveiliging/)’ ontwikkeld waarin dit verder is uitgewerkt en wat als leidraad kan dienen voor de eigen organisatie. [↑](#footnote-ref-2)
2. Zie voor de teamsamenstelling, rollen en verantwoordelijkheden Bijlage A. [↑](#footnote-ref-3)
3. Lumen Group heeft een ‘[Handreiking PDCA-cyclus](https://www.lumengroup.nl/knowledgebase/handreiking-pdca-cyclus-voor-privacy-en-informatiebeveiliging/)’ ontwikkeld waarin dit verder is uitgewerkt en wat als leidraad kan dienen voor de eigen organisatie. [↑](#footnote-ref-4)