Handreiking crisisplan informatieveiligheid

Colofon

De tekst in deze handreiking is gebaseerd op het document Voorbeeld Incidentmanagement en responsebeleid v2.0, die door de Informatiebeveiligingsdienst (IBD) is opgesteld en beschikbaar gemaakt voor gemeenten. De teksten in deze handreiking zijn met toestemming van IBD aangepast en geschikt gemaakt voor de VVT door ActiZ.  Voor gebruik en delen van  het materiaal, verveelvoudiging, verspreiding en gebruik van dit materiaal verwijzen wij naar de Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD) als bronmateriaal van de inhoud.

Toelichting en leeswijzer

In deze handreiking staan beleidsuitgangspunten en processtappen voor het incidentmanagement- en responsbeleid. Omdat 100% informatieveiligheid niet bestaat zullen incidentenplaatsvinden. De verantwoordelijkheid van een zorgorganisatie voor informatieveiligheid strekt zich uit tot het hebben van een draaiboek voor ‘wat te doen, als er iets misgaat’. Daarnaast zorgt het proces ervoor dat lering wordt getrokken van incidenten, waardoor de kans op herhaling wordt verkleind. Dit document is een handreiking om een eigen crisisplan op te stellen die past bij je eigen organisatie. Zo is iedere organisatie verschillend, zijn zaken uitbesteed, en zijn functies en rollen anders ingevuld. Deze handreiking geeft een aanpak aan, die je kunt gebruiken om te vertalen naar de situatie van je eigen organisatie.

**Doelstelling incidentmanagement**

Incidentmanagement is zo belangrijk omdat 100% beveiligen niet bestaat en los daarvan: 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 te voren bedacht worden en de bijpassende reactie en escalatieprocedure kan dus ook van te voren uitgewerkt en geoefend worden. Het incidentmanagement proces heeft dan ook als doel om verstoringen zo snel mogelijk te verhelpen en te voorkomen in de toekomst. Ook als er ICT zaken zijn uitebesteed, zijn goede contractuele afspraken noodzakelijk zodat de leverancier op basis van prioriteit kwetsbaarheden snel oplost. Het eerste uur na ontdekking van een incident kan cruciaal zijn, er moet zo min mogelijk impact zijn van het incident zonder dat er informatie verloren gaat. Dit is namelijk nodig om later een goed onderzoek te kunnen doen naar de oorzaak van het incident.

Het doel van dit document is een handreiking voor VVT organisatie om een eigen crisisplan te maken voor incidentmanagement en response beleid gericht op informatieveiligheidscrises.

**Doelgroep**

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

**Leeswijzer**

Hoofdstuk 1 gaat over het incidentmanagement en responseproces. Daarnaast is er een stuk opgenomen over de meldingen en wie je wanneer moet inlichten. Hoofdstuk 2 beschrijft verschillende aspecten die bij dit proces komen kijken zoals logging en het gouden uur. Hoofdstuk 3 gaat in op de verschillende prioritering die bij incidenten komen kijken.

Over het algemeen wordt gesproken over de CISO als rol vanuit de informatiebeveiliging. Per organisatie zijn rollen en functies anders belegd en genoemd. Lees daarom de CISO als rol die van toepassing is in je eigen organisatie. Daarnaast hebben zorgorganisaties in meer of mindere mate hun ICT en beveiliging uitbesteed. Ook daarbij geldt dat in dit document de grote lijnen worden beschreven. Pas dit aan naar gelang de situatie en afspraken met leveranciers in je eigen organisatie.

Inhoudsopgave

[1. Incidentmanagement en response stappen 5](#_Toc74217209)

[1.1. Identificatie 5](#_Toc74217210)

[1.2. Schade indamming 5](#_Toc74217211)

[1.3. Remediatie en herstel 6](#_Toc74217212)

[1.4. Kennisgeving 6](#_Toc74217213)

[1.5. Rapportage en evaluatie 6](#_Toc74217214)

[2. Aandachtspunten 6](#_Toc74217215)

[2.1. Logging 6](#_Toc74217216)

[2.2. Betrokkenen bij incidentmanagement 6](#_Toc74217217)

[2.3. Voorbereiding 7](#_Toc74217218)

[2.4. Gouden uur 7](#_Toc74217219)

[2.5. Enkele tips 7](#_Toc74217220)

[3. Incident Prioritering Leidraad 7](#_Toc74217221)

[3.1. Incident urgentie (categorieën) 8](#_Toc74217222)

[3.2. Incident impact (categorieën) 8](#_Toc74217223)

[3.3. Incident Prioriteringsklassen 9](#_Toc74217224)

[Bijlage A: Incidentmanagement en response beleid stappenplan en sjabloon 11](#_Toc74217225)

[Bijlage B: Incidentenprocedure informatiebeveiliging 20](#_Toc74217226)

# Incidentmanagement en response stappen

Incidentmanagement bestaat uit een aantal te doorlopen stappen. Deze stappen zijn voor ieder incident gelijk, in de details zitten verschillen. Een incident response-actie bestaat uit de volgende stappen:

* identificatie
* schade indamming (insluiting en beperking)
* remediatie en herstel
* kennisgeving
* rapportage en evaluatie

Deze stappen staan in de volgende paragrafen kort uitgelegd en worden in detail beschreven in het stappenplan in bijlage A. De checklist in bijlage A bevat acties om de meest ernstige veiligheidsincidenten aan te pakken. Het kan ook effectief worden gebruikt om andere veiligheidsincidenten aan te pakken. Er is een 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 gegevens. Houd rekening 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 beveiligings-gerelateerde termen van het contract tussen de zorgorganisatie en die partij.

Het is verstandig om de paraatheid van de zorgorganisatie 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.

Hieronder eerst de korte uitleg per stap.

## Identificatie

Je controleert of er een kwetsbaarheid aanwezig is en/of een incident daadwerkelijk heeft plaatsgevonden. Deze activiteit omvat normaliter de systeembeheerder en eindgebruiker bij een melding. Het kan ook het gevolg zijn van proactieve detectie van incidenten door de ICT-beveiliging of het systeembeheer of doordat bij de controle van de logging iets naar boven komt. Als wordt vastgesteld dat er inderdaad een kwetsbaarheid of incident is, dan worden de betreffende instanties gewaarschuwd en de verdere stappen in werking gesteld.

## Schade indamming

Nadat het incident is opgemerkt en gemeld gaat de servicedesk ermee aan de slag. De incidentmanager (soms gewoon een helpdeskmedewerker) gaat handelen om de schade van het incident te beperken. De incidentmanager zal wanneer nodig opschalen. De CISO & FG of iemand anders met die rol wordt erbij betrokken en een team aangesteld om het incident te verhelpen. Bij grote informatiebeveiligingsincidenten zal de directeur bedrijfsvoering of andere portefeuillehouder een belangrijke rol spelen en zal de CISO in de meeste gevallen de teamleider worden. Dit team is belast met het beperken van verdere schade van het incident en kan een externe partij inschakelen voor advies. Start een grondige beoordeling van de aard en omvang van het incident, stel vast wat de schade is en stel bewijsmateriaal veilig. Bepaal of het datalek 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 Autoriteit Persoonsgegevens (AP) te doen en later deze in te trekken of verder aan te vullen.

## Remediatie en herstel

Je neemt maatregelen om de oorzaak van het incident te blokkeren of te verwijderen. Je vermindert de impact door verdere blootstelling van de gevoelige gegevens te voorkomen. Je maakt een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident. En je zorgt dat risico’s die verband houden met dit incident worden ingedamd. Voor de diensten die zijn uitbesteed is het noodzakelijk om goede afspraken te hebben met de leverancier om incidenten op te pakken.

## Kennisgeving

Je bepaalt welke gegevens mogelijk zijn blootgesteld door het incident en stelt de getroffenen in kennis. Maak een melding aan de Autoriteit Persoonsgegevens (AP) via de FG wanneer nodig. Bekijk welke verdere betrokkenen ook geïnformeerd moeten worden. Informeer indien noodzakelijk andere overheidsinstanties, zoals de IGJ en/of de politie. Betrek voor deze melding en ook communicatie eventueel een jurist in verband met aansprakelijkheid. Snelheid is ook belangrijk vanuit een PR-oogpunt.

## Rapportage en evaluatie

Identificeer lessen uit het incident en bespreek deze met het team en leveranciers. Rapporteer over het incident, de genomen maatregelen en het algemeen verslag zowel intern als extern en pas het gevolgde draaiboek aan waar nodig. Het is belangrijk om bij een incident alle uitgevoerde activiteiten vast te leggen voor latere analyse, evaluatie, woordvoering en bewijslast. Het is ook goed om de bschrijvingen met de oplossing van incidenten te bewaren om het incidentmanagement te verbeteren. Er kan lering worden getrokken uit het overzicht met het aantal incidenten en het type incidenten.

# Aandachtspunten

Welke aspecten komen nog meer bij het incidentmanagement proces kijken? Hieronder staan enkele aandachtspunten voor het incidentmanagement proces.

## Logging

Bij het onderzoek naar mogelijke incidenten wordt veelvuldig gebruik gemaakt van de controle op logging uit systemen, netwerkapparatuur en programma’s. Logbronnen worden gebruikt door een monitoring en response dienst die detecteert of er kwetsbaarheden 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 worden bewaard volgens vaste regels en kennen per soort logging een bewaartermijn waarvan afgeweken kan worden (verlenging) als er een vermoeden is van een incident. Als logging op de juiste wijze bewaard en behandeld wordt, kan logging ook dienen als bewijsmateriaal voor de wet. Let hierbij wel op dat logging persoonsgerelateerde of privacygevoelige informatie kan bevatten, en dat logging zodanig bewaard moet worden dat deze niet zomaar kan worden ingezien of worden gewijzigd. Voor de controle op logging is een voorbeeld cheat sheet te vinden op: <http://www.securitywarriorconsulting.com/security-incident-log-review-checklist.docx>

## Betrokkenen bij incidentmanagement

Het incidentmanagement proces heeft altijd een eigenaar en wijs binnen het proces een vast aanspreekpunt aan die eventueel ook zorgt voor de externe communicatie. Het melden van incidenten is een taak van iedereen. De beoordeling van de logging maar ook van gemelde incidenten gebeurt door een speciaal aangewezen functionaris afhankelijk van waarover de logging of de incidentmelding gaat. In ieder geval moet altijd de servicedesk geïnformeerd worden en meestal ook de CISO. Bij een escalatie of een noodsituatie moet altijd rekening gehouden worden met woordvoering. Al het personeel dat betrokken is bij het incident proces moet op de hoogte zijn van de procedures en de telefonische bereikbaarheid van belangrijke contactpersonen en teamleden. Per soort incident kan het team een wisselende samenstelling hebben.

## Voorbereiding

Rond incidenten kunnen voorbereidingen getroffen en geoefend worden. Voor incidenten met een mogelijk hoge impact is het wenselijk om dat regelmatig te doen. Voor incidenten met hoge impact kunnen zogenaamde cheat sheets of operational incident best practices dan wel standaard operationele digitale incident procedures gemaakt worden. ( Binnen de wereld van Computer Emergency Response zijn al veel cheat sheets ontwikkeld en op internet te vinden)

In de voorbereiding is het ook belangrijk om iedereen die betrokken wordt 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).

## Gouden uur

Het ‘gouden uur’ is het eerste uur na de ontdekking van het incident. Het uur waarin je het incident inperkt maar ook geen informatie verloren laat 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. 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.

## Enkele tips

1. Vraag bij twijfel advies van een digitaal forensisch expert.
2. Maak standaard procedures.
3. Zorg voor volledig inzicht in de juridische consequenties van het incident en tjouw betrokkenheid. Ga nooit verder dan je expertise toestaat.
4. Denk verder dan het apparaat in kwestie en let ook op de papieren documentatie die in de ruimte ligt en mogelijk ook moet worden beschermd om als mogelijk bewijs te dienen.
5. Documenteer nauwkeurig de uitgevoerde acties, deze moeten ook datum en tijd bevatten en gebruik genummerde pagina’s.
6. Isoleer bij het onderzoek de apparatuur vanuit elke netwerkverbinding (Bluetooth, bedraad of draadloos).
7. Schakel nooit een apparaat aan als het uit staat.
8. Als een apparaat is ingeschakeld en het lijkt actief bezig met het verwijderen van gegevens of onder externe controle te zijn, overweeg dan om het apparaat uit te schakelen door het snoer of de batterij weg te nemen. LET OP: niet uitzetten met de aan/uit knop, dan verdwijnen er mogelijk sporen. Win indien mogelijk deskundig advies in voordat je iets doet.
9. Maak eventueel foto’s van externe aansluitingen aan het apparaat, zoals printers of USB-drives en van scherm activiteiten die u kunt zien.

# Incident Prioritering Leidraad

Het bepalen van de juiste prioriteit van een incident is nodig om de geschikte maatregelen te nemen bij het incident. In dit hoofdstuk een korte uitleg hoe je die prioriteit bepaalt. De incident prioritering wordt afgeleid uit twee factoren: urgentie en impact.

**De prioriteit van een incident wordt meestal bepaald door de beoordeling van de impact en urgentie, waarbij:**

* Urgentie staat voor hoe snel de oplossing van het incident vereist is.
* Impact staat voor de omvang van het incident en van de mogelijke schade als gevolg van het incident voordat het kan worden opgelost.

## Incident urgentie (categorieën)

In deze paragraaf worden urgentie categorieën verder uitgewerkt. **LET OP: de tabel bevat slechts voorbeelden**.

Om de urgentie van een incident te bepalen, kies je altijd uit de hoogste waarde van de desbetreffende categorie:

|  |  |
| --- | --- |
| **Categorie Urgentie** | **Omschrijving** |
| **Hoog (H)** | * De schade veroorzaakt door het incident neemt snel toe.
* Werk dat moet worden hersteld door de medewerkers is zeer arbeidsintensief.
* Een groot incident kan worden voorkomen door bij een klein incident onmiddellijk te handelen.
* Het incident leidt tot aanzienlijke kans op ernstige gevolgen in het aglemeen of voor de bescherming van persoonsgegevens
 |
| **Medium (M)** | * De schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe.
* Er gaat werk verloren, maar dit is relatief snel te herstellen.
 |
| **Laag (L)** | * De schade veroorzaakt door het incident neemt in de tijd maar weinig toe.
* Het werk dat blijft liggen is niet tijdsintensief.
 |

*Tabel 1: Voorbeelden incident urgentie*

## Incident impact (categorieën)

In deze paragraaf worden de impact categorieën uitgewerkt, de tabel is slechts een voorbeeld.

Om de impact van het incident vast te stellen, kies je de hoogste desbetreffende categorie:

|  |  |
| --- | --- |
| **Categorie Impact** | **Omschrijving** |
| **Hoog (H)** | * Relatief veel medewerkers zijn geraakt door het incident en/of kunnen hun werk niet meer doen. Meerdere afdelingen zijn geraakt, de continuïteit van zorg komt in gevaar.
* Cliënten van een zorgorganisatie zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd.
* De financiële impact van het incident is (bijvoorbeeld) hoger dan €10.000,-.
* Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen voor bijv. bescherming van persoonsgegevens of continuïteit van zorg. Bij de beoordeling van de impact van het datalek zijn van belang:
	+ Gevaar voor welzijn en/of gezondheid.
	+ Gevolgen voor de persoonlijke levenssfeer van de getroffen personen.
	+ Aard en omvang van het datalek.
	+ Aard van de gelekte persoonsgegevens.
	+ De mate waarin technische beschermingsmaatregelen zijn getroffen.
	+ Er is reputatieschade, de krant wordt gehaald.
 |
| **Medium (M)** | * Enkele medewerkers zijn geraakt door het incident en/of kunnen hun werk niet meer doen, maar veiligheid van cliënten is niet meteen in gevaar.
* Enkele cliënten van een zorgorganisatie zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd.
* De financiële impact van het incident is (bijvoorbeeld) hoger dan €1.000,- en lager dan €10.000,-.
* Er is kans op reputatieschade.
 |
| **Laag (L)** | * Enkele medewekers zijn geraakt door het incident en/of kunnen niet meer hun werk doen maar de zorg komt niet in gevaar.
* Enkele cliënten van een zorgorganisatie zijn geraakt en/of lijden schade, maar dit is zeer minimaal. Persoonsgegevens zijn gecompromitteerd.
* De financiële impact van het incident is (bijvoorbeeld) lager dan €1.000,-
* Er is geen kans op reputatieschade.
 |

*Tabel 2: Voorbeelden incident impact*

## Incident Prioriteringsklassen

De Incident Prioriteit wordt verkregen door urgentie en impact tegen elkaar af te zetten.

**Incident Prioriteiten Matrix**

Als er klassen zijn gedefinieerd om urgentie en impact in te schalen, dan kan een Incident Prioriteit Matrix gebruikt worden om prioriteringsklassen te herleiden. In het onderstaande voorbeeld zijn de klassen uitgewerkt met een code en kleuren.

|  |  |
| --- | --- |
|  | **Impact** |
| Hoog | Midden | Laag |
| **Urgentie** | Hoog | 1 | 2 | 3 |
| Midden | 2 | 3 | 4 |
| Laag | 3 | 4 | 5 |

*Tabel 3: Incident prioriteringklassen*

|  |  |  |  |
| --- | --- | --- | --- |
| **Code/kleur** | **Omschrijving** | **Reactietijd**  | **Oplossingstijd** |
| **1** | Kritiek | Onmiddellijk | 1 uur |
| **2** | Hoog | 10 minuten | 4 uur |
| **3** | Medium | 1 uur | 8 uur |
| **4** | Laag | 4 uur | 24 uur |
| **5** | Zeer laag | 1 dag | 1 week |

*Tabel 4: Incidenten prioriteiten matrix*

### Groot incident identificeren

Grote incidenten hebben een ander soort Incident managementteam nodig en maken gebruik van een gescheiden proces dat speciaal is ingericht voor het behandelen van grote incidenten. Voor grote incidenten is het vaak nodig om aanvullende indicatoren vast te stellen voor het identificeren ervan. Voorbeelden van dergelijke indicatoren zijn:

1. Bepaalde (groepen van) bedrijfskritische diensten, toepassingen of onderdelen van de infrastructuur zijn niet beschikbaar en de geschatte tijd voor herstel is onbekend of extreem lang (nader te specificeren diensten, toepassingen of onderdelen van de infrastructuur).
2. Bepaalde (groepen van) vitale bedrijfsfuncties (bedrijfskritische processen) worden beïnvloed en de geschatte tijd voor het herstellen van deze processen tot volledige operationele status is onbekend of extreem lang (specificeren bedrijfskritische processen).

### Typering van kritische incidenten

Een kritisch incident kan ook worden omschreven als een ‘majeur incident’ of een ‘incident met hoge prioriteit’. Hoewel servicedeskmedewerkers vaak door ervaring een goed idee hebben over wat een kritisch incident is, blijft het moeilijk om een eenduidige definitie van dit begrip te geven. Daarom is het goed om de definitie zo ruim mogelijk te interpreteren. Een kritisch incident wordt meestal getypeerd door zijn impact. Vooral de impact op gebruikers speelt hierbij een belangrijke rol. Enkele voorbeelden:

* Een deel van de datacommunicatie van en naar de zorgorganisatie ligt plat door een storing in het netwerk.
* Een belangrijke database blijkt corrupt te zijn.
* Meerdere servers worden geïnfecteerd door een ‘worm’.
* Persoonsgegevens en vertrouwelijke informatie van cliënten worden per ongeluk publiek toegankelijk.

Enkele belangrijke gevolgen van kritische incidenten zijn:

* Een groot aantal medewerkers kunnen niet bij de cliëntgegevens in het ECD waardoor cliënten gevaar lopen.
* Een aantal systemen die belangrijk zijn voor de uitvoering van de zorg vallen uit of zijn niet benaderbaar.
* De kosten (inclusief gevolgschade) voor de zorgorganisatie zijn aanzienlijk of kunnen aanzienlijk worden.
* Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. De zorgorganisatie zou reputatieschade en verlies van vertrouwen van cliënten kunnen oplopen.

Bedenk ook dat alle rampen zoals onderkend in een continuïteitsplan kritische incidenten zijn en ook dat kleinere incidenten zich tot kritische incidenten kunnen ontwikkelen als er niet goed wordt ingegrepen.

En:

* De tijd en moeite die nodig zijn om het incident op te lossen zijn waarschijnlijk groot en het is zeer waarschijnlijk dat afspraken die zijn vastgelegd in de SLA niet kunnen worden nagekomen.

# Bijlage A: Incidentmanagement en response beleid stappenplan en sjabloon

**Incidentmanagement en response beleid 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 1: IdentificatieControleer 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. Als wordt vastgesteld dat het inderdaad een incident is, dan moeten de betreffende instanties gewaarschuwd worden.  |
| *Gedaan* | ***Taak*** | ***Eigenaar*** | *Notities* |
|  | 1. Onmiddellijk blootstelling beperken:
* Als een elektronisch apparaat is gecompromitteerd:
	+ Niet gebruiken (niet inloggen) of wijzigen van het apparaat
	+ Zet het apparaat niet uit
	+ Haal de netwerkverbindingen er af, maar NIET de voedingskabel
* 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.
 | Afdeling/team |  |
|  | 1. Waarschuw onmiddellijk de servicedesk (incidentmanager) en de CISO

*Handleiding: Voeg namen en telefoonnummers, e-mailadressen of de link naar een online meldingsformulier toe.*  | Afdeling/team |  |
|  | 1. Als het incident over elektronische apparaten gaat of als er media gestolen of verloren is, dan ook aangifte doen bij de politie.

*Handleiding: Deze stap alleen uitvoeren na overleg en op advies van de CISO of ICT/security afdeling.* | Afdeling/team |  |
|  | 1. Voer een voorlopige beoordeling uit van het type en de scope van het incident en de omvang van de blootstelling. Als er potentieel gevoelige informatie blootgesteld is dan moet het management geïnformeerd worden en tijdens het verloop van het incident op de hoogte gehouden worden:

*Voorbeelden:*1. *CIO of directeur*
2. *Communicatie*
3. *Bestuur*
	* Start met een logboek waarin gedurende het incident alle activiteiten op datum en tijd worden vastgelegd.
	* Indien het incident ook het lekken van persoonsgegevens betreft, leg dit dan nu vast en informeer de FG.
 | CISO of incidentmanager  |  |
|  | 1. Als 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.
 |  |  |
| *STAP 2: 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.* |
|  | 1. Stel het Incident response team samen

*Handleiding: Zorg ervoor dat de vertegenwoordiger deelneemt van de afdeling/team waar het incident zich voordeed en dat deze persoon hoog genoeg in de organisatie zit om de nodige beslissingen te nemen.* | Incidentmanager of -management |  |
|  | 1. Bespreek Incident response proces en de verantwoordelijkheden met het Incident response team
* Geef ieder teamlid de incidentmanagement checklist (deze of een aangepaste versie voor de eigen organisatie)
* Bespreek de communicatiestrategie.
* Bespreek het belang van het goed in een tijdlijn documenteren
* Bespreek hoe het verloren raken van onderzoeksgegevens te voorkomen.

*Handleiding: In deze fase is het vooral belangrijk om de communicatie-afspraken te besrpeken. En de nauwkeurigheid van de feiten te waarborgen tussen teamleden onderling en tussen het team en de juiste beleidsmedewerkers.**Voorbeelden:* 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.*
 | De teamleider van het Incident response team |  |
|  | 1. Verzamelen en veiligstellen van bewijsmateriaal

*Handleiding: Verzamel fysiek en digitaal bewijs die samen een duidelijke, gedetailleerde beschrijving geven van hoe de data gecompromitteerd kon worden.**Voorbeelden:*1. *Images van de harddisk(en)*
2. *Netwerkverkeersgegevens van en naar de gecompromitteerde apparatuur*
3. *Werkplek applicatie logs*
4. *Toegangslogs*
5. *Foto’s van de omgeving waar het incident plaatsvindt*
 | Incident response team |  |
|  | 1. Zorg voor al het bewijsmateriaal en houd bij waar het zich bevindt en wie er toegang toe heeft.

*Handleiding: Maak een inventarisatielijst van alle bewijsmateriaal en houd bij wie, wanneer, wat gedaan heeft met het bewijsmateriaal.**Voorbeelden:*1. *Beschrijf wat exact het bewijsmateriaal is.*
2. *Leg vast wie erbij moest en waarom.*
3. *Leg vast waar en hoe het bewijsmateriaal opgeslagen is.*
4. *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.*
 | Incident response team |  |
|  | 1. Neem maatregelen om de scope en de impact van het incident in te perken.

*Voorbeelden:*1. *Als het incident betrekking heeft op gevoelige gegevens die onjuist geplaatst zijn op publiek toegankelijke websites, verwijder dan de actieve en opgeslagen inhoud. 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)*
2. *Verander mogelijk gecompromitteerde wachtwoorden.*
3. *Staak de exploitatie van een gecompromitteerde applicatie of server.*
 | Incident response team |  |
|  | 1. Voer forensisch onderzoek uit en leg dit vast:
	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.*  | Incident response team |  |
|  | 1. 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 |  |
|  | 1. Geef mogelijk een voorwaarschuwing aan de Autoriteit Persoonsgegevens.

*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.*  | Functionaris Gegevensbescherming (FG) |  |
| STAP 3: Remediatie en herstelNeem 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 door het incident en zorg ervoor dat risico’s die verband houden met dit incident worden verminderd. |
|  | 1. Herhaal stappen 2.4 en 2.5 nu diepgaander en zoek naar aanvullende manieren om de blootstelling te beperken.

 *Voorbeelden:*1. *Run periodiek web-queries om u er van te verzekeren dat de data niet verder is verspreid of gecached.*
2. *Beoordeel de inventarisatie van getroffen hardware en systemen en wijzig verder waar nodig de wachtwoorden die mogelijk gecorrumpeerd zijn.*
3. *Stop eventueel gecorrumpeerde diensten of applicaties en zorg voor work-arounds*
 | Incident response team |  |
|  | 1. Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico’s voor gevoelige dataopslag

 *Voorbeelden:*1. *Run vulnerability scans op getroffen systemen;*
2. *Beoordeel en bepaal waar de data zich bevindt en wijzig dit indien nodig om een hogere beschermingsgraad te verzekeren.*
3. *Beperk de toegang tot systemen tot uitsluitend degenen die toegang nodig hebben.*
4. *Gebruik software tools om gevoelige data te vinden, te verwijderen en te beschermen, bijvoorbeeld: Identity Finder.*
 | Incident response team |  |
|  | 1. Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze weer in gebruik genomen worden.
 |  |  |
| STAP 4: KennisgevingBepaal welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffenen in kennis. Snelheid is geboden als er persoonsgegevens verloren zijn gegaan of bekend geworden zijn aan niet rechthebbenden. Informeer indien noodzakelijk andere overheidsinstanties, zoals de AP, de IGJ 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. |
|  | 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? (Bijvoorbeeld bij niet versleutelde persoonsgegevens die gelekt zijn)
* Zo ja,
* 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 call center?
* Is het noodzakelijk om een officieel persbericht te plaatsen op de website van de zorgorganisatie?
* Als er geen kans is geweest op blootstelling van informatie aan buitenstaanders, dan kan eventueel meteen doorgegaan worden naar stap 5.
1. Als het een incident is met persoonsgegevens waarbij een grote kans is op ernstige nadelige gevolgen voor de betrokkenen, moet de toezichthouder direct in kennis gesteld worden.

*Handleiding:*1. *Degenen die verantwoordelijk zijn voor het nemen van deze beslissingen zal variëren van zorgorganisatie tot zorgorganisatie, maar meestal is (een deel van) bestuur, directie en communicatie al geïnformeerd in eerdere stappen. Beslissingen die genomen moeten worden, zijn in overeenstemming met eerdere beslissingen, tenzij eventuele afwijkingen volledig gerechtvaardigd zijn. Uiteraard gelden voor alle beslissingen de respectievelijke wetten, regelgeving en contractuele verplichtingen.*
2. *Kies een geschikt communicatiemiddel, passend bij het incident, de hoeveelheid te informeren personen, de mate waarin risico gelopen is en/of informatie gecompromitteerd is.*
3. *Win eventueel juridisch advies in over de positie en aansprakelijkheid van de zorgorganisatie bij bepaalde communicatie.*
 | Management |  |
|  | 1. Verzamel de naam en adresgegevens van de getroffenen

*Handleiding: Zorg ervoor dat de verzamelde data veilig wordt behandeld, verstuurd en opgeslagen en als de data niet langer benodigd is moet deze worden vernietigd.*   | Afdeling/team, geadviseerd door de CISO of door het Incident response team |  |
|  | 1. Zet telefoon en e-mail ondersteuning op in geval van vragen:
	* 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 te voren de reacties op de verwachte vragen.
	* Train het team.
 | Locatieteam en communicatie, geadviseerd door de CISO of door het Incident response team |  |
|  | 1. Als in stap 4.1 een website gekozen is om te communiceren:
	* Bepaal de website locatie.
	* Voorkom toegang totdat de pagina live mag gaan.
	* Bereid de inhoud voor.

*Handleiding:* 1. *Websites worden vooral gebruikt als het aantal getroffenen groot is of omdat niet alle mensen bekend zijn.*
2. *De website content moet goedgekeurd worden door bestuur en CISO of Incident response team, en indien van toepassing overlegd met politie en andere ingeschakelde instanties en experts.*
 | Communicatie in overleg met de CISO of het Incident response team |  |
|  | 1. Voorbereiding schriftelijke informatieverstrekking aan getroffenen:
* Bepaal het onderwerp, stijl en vorm.
* Schrijf een concept tekst.

*Handleiding:* *De inhoud van de brief moet zijn goedgekeurd door het bestuur en door communicatie.* | Communicatie in overleg met afdeling/team en de CISO of het Incident response team |  |
|  | 1. Als er een noodzaak of een verplichting is, informeer de politie en doe aangifte als dit nog niet is gebeurd.

  | Management |  |
|  | 1. Doe de definitieve melding aan de Autoriteit Persoonsgegevens (AP) als er bij Stap 2.8 een voormelding gedaan is. Doe een gemotiveerde melding aan de AP als er bij Stap 2.8 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.)
 | FG in overleg met CISO en/of management |  |
|  | 1. Informeer derde partijen zoals service providers en applicatieleveranciers als risico’s als identiteitsdiefstal verkleind kan worden of als dat is vastgelegd in het respectievelijke contract.
 | Afdeling ICT |  |
|  | 1. Als er bankgegevens blootgesteld zijn aan niet rechthebbenden, informeer dan de bank of creditcard firma’s.
 | Controller |  |
|  | 1. Coördineer de gelijktijdige communicatie-acties zodat de verschillende informatiestromen gelijktijdig plaatsvinden.
 | Afdeling communicatie |  |
| STAP 5: Rapportage en evaluatieIdentificeer 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. |
|  | 1. Verzamel alle geïnvesteerde tijd van de medewerkers die hebben 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 besteed heeft rapporteert aan het management |  |
|  | 1. 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 |  |
|  | 1. Onderzoek oplossingen om herhaling te voorkomen.
	* Indien nodig rapporteer hierover aan het management.

*Voorbeelden van te beantwoorden 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?*
 | CISO |  |
|  | 1. Plan oplossingsprojecten om de geleerde lessen effectief in te bedden in de organisatie.
 | CISO en/of ICT en Afdeling/team |  |
|  | 1. 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. Indien het een inbreuk betreft van de bescherming van persoonsgegevens[[1]](#footnote-1) moet altijd een overzicht hiervan worden bijgehouden.
 | CISO |  |

# Bijlage B: Incidentenprocedure informatiebeveiliging

Elke medewerker moet alert zijn op bedreigingen van de informatiebeveiliging. Zij zijn vaak de eerste die een incident opmerken en melden. Elke organisatie maakt afspraken hoe en bij de melding te doen. Bij wie hoort de melding en wanneer wordt deze opgeschaald?

Als hulpmiddel staan twee tabellen met mogelijke incidenten. Deze lijst is niet uitputtend en zal dit ook nooit kunnen zijn: er zullen zich steeds nieuwe soorten beveiligingsincidenten voordoen en deze kan per zorginstelling verschillen. De lijst is een voorbeeld om voor de eigen helpdesk een hulpmiddel te maken voor het herkennen van een beveiligingsincident en het inschatten van de impact.

In veel gevallen zal de CISO niet als primaire behandelaar optreden, immers het technisch verhelpen van een dergelijk incident gebeurt niet door de Privacy Officer, 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.
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 als het goed is de meldingsdatabase regelmatig.

### 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 | 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 netwerk verbinding 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 zorgorganisatie | 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 bijv. Privacy Officer.
* Directie: Incidenten die door CISO of bijv. Privacy Officer worden gemeld bij directie.
1. [Zie AVG 33a lid 5.](https://wetten.overheid.nl/jci1.3%3Ac%3ABWBR0040940%26hoofdstuk%3D3%26paragraaf%3D3.2%26artikel%3D33%26z%3D2018-05-25%26g%3D2018-05-25) . [↑](#footnote-ref-1)