# Template (cyber)beveiligingsincident-stappenplan en -logboek

Versienummer: 1.0

Januari 2024

Dit template (cyber)beveiligingsincident-stappenplan en -logboek is zorgvuldig samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template (cyber)beveiligingsincident-stappenplan en -logboek is opgesteld door Kennisnet en verschijnt onder de licentie Creative Commons Naamsvermelding 4.0 Nederland.

<https://creativecommons.org/licenses/by/4.0/legalcode.nl>

Bij het samenstellen van dit template (cyber)beveiligingsincident-stappenplan en -logboek is gebruik gemaakt van de volgende bron:

Handreiking Incident- en response management, Vereniging van Nederlandse Gemeenten/ Informatiebeveiligingsdienst voor gemeenten, licentie onder: CC BY-NC-SA 4.0.

Gebruikswijzer van dit template (cyber)beveiligingsincident-stappenplan en -logboek

**Verwijder voor eigen gebruik van dit document deze en de voorgaande pagina.**

Deze gebruikswijzer is bedoeld als toelichting op het gebruik van dit template voor (cyber)beveiligingsincident-stappenplan en -logboek (en niet als leeswijzer voor het stappenplan zelf). Het (cyber)beveiligingsincident-stappenplan en -logboek helpen slechts als richtlijn voor IBP’ers om te komen tot een specifiek proces voor het eigen schoolbestuur. Met de zoek-en-vervangfunctie kun je bijvoorbeeld wel snel de naam van het schoolbestuur invullen, maar daarmee is het document nog niet geschikt om aan een bestuur voor te leggen. Vaak zal IBP bovenschools geregeld worden. <naam schoolbestuur> kun je dan vervangen door de naam van de overkoepelende instelling.

De invulling van het proces kan per schoolbestuur op onderdelen verschillen. Van invloed kunnen zijn:

* Grootte van het schoolbestuur (bijvoorbeeld niet voldoende personen om alle taken en rollen zuiver te scheiden).
* De politieke werkelijkheid binnen een schoolbestuur (een organisatieverandering is niet altijd wenselijk, of niet op dit moment; of er is een specifieke mandatenregeling die bepaalde verantwoordelijkheden anders belegt).
* Volwassenheid van IBP in het schoolbestuur (het beleid is bijvoorbeeld te veelomvattend als onderliggende taken, rollen en functies vooralsnog niet zijn ingevuld en niet snel kunnen worden ingevuld).
* Een schoolbestuur heeft meer of minder onderliggende documenten beschikbaar om aan te refereren.
* Vormgevingseisen.

Het schoolbestuur kan afhankelijk van bovenstaande situaties kiezen om:

* Elementen weg te laten (als er bijvoorbeeld geen procesmanager is, of geen CSIRT).
* Elementen naar een bijlage te verplaatsen of enkel te refereren aan een onderliggend document, of juist in plaats van een bijlage tekst in het hoofddocument op te nemen.
* Elementen verder uit te schrijven omdat er geen onderliggende documenten zijn.

Specifiek maken van dit document

|  |  |
| --- | --- |
| <tekst> | Vervang dit door tekst die passend is bij de eigen situatie, bijvoorbeeld <naam schoolbestuur> wordt ‘Schoolbestuur X’. |
|  |  |

# Template (cyber)beveiligingsincident-stappenplan en -logboek

## 

## 1. Documentgeschiedenis

### 1.1 Revisies

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Auteur | Review |
| **0.1** | 1 jan 2024 | <Voornaam Achternaam> | Eerste concept uitgewerkt |
|  |  |  |  |
|  |  |  |  |

### 1.2 Goedkeuring

Vastgesteld door <naam schoolbestuur>, hierna te noemen “de school”

|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Functie | Versie | Datum |
| <het schoolbestuur is eindverantwoordelijk en hier moet de hoogst verantwoordelijke in de instelling komen te staan> | <het schoolbestuur is eindverantwoordelijk en hier moet de hoogst verantwoordelijke in de instelling komen te staan> |  |  |

### 1.3 Document classificatie

|  |  |
| --- | --- |
| Classificatie | Beschrijving |
| **Openbaar** | Dit document mag zonder beperkingen worden gedeeld |
| **Vertrouwelijk** | Mag worden gedeeld met medewerkers van <naam schoolbestuur> (en evt. organisaties X,Y,Z) |
| **Geheim** | Dit document is exclusief bestemd voor de volgende personen: (bijv. leden MT) |

Inhoud

[Template (cyber)beveiligingsincident-stappenplan en -logboek 1](#_Toc2123395472)

[Template (cyber)beveiligingsincident-stappenplan en -logboek 2](#_Toc261896740)

[1. Documentgeschiedenis 3](#_Toc1846255844)

[1.1 Revisies 3](#_Toc1607251850)

[1.2 Goedkeuring 3](#_Toc882061367)

[1.3 Document classificatie 3](#_Toc1709928261)

[2. Inleiding 4](#_Toc1870600692)

[3. (cyber)beveiligingsincidentmanagement en response stappenplan en logboek 5](#_Toc941416738)

## 2. Inleiding

Bij (cyber)beveiligingsincidenten is het van belang dat er snel geschakeld wordt en dat, na het ontdekken van het incident, alle noodzakelijke stappen gevolgd worden. Snelle actie draagt eraan bij dat informatie beschikbaar blijft.

De template (cyber)beveiligingsincident-stappenplan en -logboek bevat acties die nodig zijn om de (cyber)beveiligingsincidenten waar persoonsgegevens bij betrokken zijn, aan te pakken en de uitgevoerde acties vast te leggen. De template kan ook effectief worden gebruikt om andere veiligheidsincidenten aan te pakken, zoals het beschadigen van openbare websites, ongeoorloofde toegang tot vertrouwelijke, maar niet wettelijk beschermde gegevens, en het verlies van vertrouwelijke papieren dossiers.

**Gebruikswijzer**

Maak na het registreren van een (cyber)beveiligingsincident een kopie van dit document en verwijder deze en voorgaande pagina. Verwijs in de servicemanagementtoepassing (bijvoorbeeld Topdesk) of het Excel-register van incidenten naar het document. De incidentmanager registreert in dit document de uitgevoerde stappen en legt alle relevante informatie over het incident vast.

## 3. (Cyber)beveiligingsincidentmanagement en response stappenplan en logboek

Incident- en responsemanagementstappenplan

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

Datum ontdekking: \_\_\_\_\_\_\_\_\_\_\_\_

Datum gerapporteerd aan de FG 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** | | | |
| **Incidenten gebeuren ongepland en onverwacht. Belangrijk is om direct te starten met vastlegging in het register. Door eenduidige en secure registratie kan je onder meer de juiste reactie bepalen, effectief de benodigde informatie vergaren en betrokkenen informeren, en achteraf vaststellen hoeveel tijd verstreken is 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 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 of IBP-verantwoordelijke |  |
|  | Noteer de gegevens van de melder | Servicedesk of IBP-verantwoordelijke |  |
| **STAP 1: Initiatie** | | | |
| **Deze activiteit ontstaat na een melding van de eindgebruiker of leverancier, maar kan ook volgen op proactieve detectie van incidenten door de ict-beveiliging of het systeembeheer. Indien wordt vastgesteld dat het inderdaad een incident is, dan moeten de juiste behandelaarsverantwoordelijken ingeschakeld worden.** | | | |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 1.1 Onmiddellijk blootstelling beperken:   * 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 | Eindgebruiker |  |
|  | 1.2 Stel indien het incident daarom vraagt een incidentmanager aan of stel een crisismanagementteam samen | Servicedesk/ bestuur |  |
|  | 1.3   Waarschuw indien nodig de IBP-verantwoordelijke | Servicedesk |  |
|  | 1.4   Indien het incident over gestolen elektronische apparaten gaat of als er media gestolen of verloren zijn, dan aangifte doen bij de politie. | Behandelaar |  |
|  | 1.5 Start met een logboek waarin gedurende het incident alle activiteiten op datum en tijd kunnen worden vastgelegd. | Servicedesk/ incidentmanager |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **STAP 2: Analyse** | | | |
| **De inspanningen van de analysefase vormen de basis voor de strategie die in de volgende fasen gehanteerd worden.**  **Gegevens en data uit de verschillende monitoring- en detectiesystemen worden geanalyseerd.** | | | |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 2.1 Voer een voorlopige beoordeling uit van het type en de scope van het incident en de impact. Is er potentieel gevoelige informatie blootgesteld is? Informeer dan het schoolbestuur en houdt het tijdens het verloop van het incident op de hoogte  Als het incident ook het lekken van persoonsgegevens betreft, leg dit dan vast. | IBP-verantwoordelijke  Incidentmanager |  |
|  | 2.2 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. | Bestuur |  |
|  | 2.3 Afhankelijk van de zwaarte van het incident wordt samen met de incidentmanager het proces crisismanagement geactiveerd [(Cybersecurity)crisis: hoe bereid je je voor?](https://www.kennisnet.nl/artikel/21437/cybersecuritycrisis-hoe-bereid-je-je-voor-oefen-met-de-bob-methode-2/) | Incidentmanager |  |
|  | 2.4 Vaststellen Incidentresponseproces en de verantwoordelijkheden met het Incidentresponseteam.   * Geef ieder teamlid deze checklist (cyber)beveiligingsincidentenmanagement. * Bespreek de communicatiestrategie. * Bespreek het belang van het goed in een tijdlijn documenteren en het voorkomen van verlies van onderzoeksgegevens.   *Handleiding: In deze fase is het belangrijk om de nauwkeurigheid van de feiten te waarborgen tussen teamleden onderling en tussen het team en de verantwoordelijken.*   * Voorbeelden: * Teamleden mogen niet praten met anderen buiten het team over het incident totdat daarvoor toestemming is gegeven door de IBP-verantwoordelijke of het schoolbestuur. * Alle documentatie die door het team geschreven wordt moet op feiten gebaseerd zijn omdat het mogelijk in een strafrechtelijk onderzoek gebruikt kan worden. * Er is dagelijks overleg tussen de teamleden. * Het team moet bijhouden hoeveel tijd er besteed wordt en waaraan. | Incidentmanager |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STAP 3: Schade-indamming en beoordeling van de blootstelling** | | | | | |
| **Wijs een Incidentresponseteamleider aan en stel een bij het incident passend, ‘Incidentresponseteam’ 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 of forensische ict-capaciteit nodig is om digitaal bewijs te verzamelen voor opsporing, beoordeling van de schade en impact voor betrokkenen en organisatie.  Forensische ict-capaciteit moet mogelijk worden ingehuurd.  < Het supportteam van Kennisnet kan ondersteuning leveren om tot de juiste opdrachtverstrekking te komen aan de forensische ict-partij. > | | Incidentmanager |  | |
|  | 3.2 Verzamelen en veiligstellen van bewijsmateriaal    *Handleiding: Verzamel fysiek en digitaal bewijs die tezamen een duidelijke, gedetailleerde beschrijving geven van hoe de data gecompromitteerd kon worden.*    Voorbeelden:   * Images van de harddisk(en) * Netwerkverkeersgegevens van en naar de gecompromitteerde apparatuur * Werkplek applicatie logs * Toegangslogs * Foto’s van de omgeving waar het incident plaatsvindt | | Incidentresponseteam |  | |
|  | 3.3 Zorg voor, en onderhoud, 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 het bewijsmateriaal. 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 voeg dit bewijs toe aan de verzameling. Zorg dat de ontvanger de verantwoordelijkheden kent. | | Incidentresponseteam |  | |
|  | 3.4 Neem maatregelen om de scope en de impact van het incident in te perken.  Voorbeelden:   1. Heeft het incident betrekking 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 zoekmachinebedrijven en andere Internet-archiefbedrijven, zoals de Wayback Machine. 2. Staak de exploitatie van een gecompromitteerde applicatie of server. | | Incidentresponseteam |  | |
|  | 3.5 Voer forensisch onderzoek uit en leg dit vast:   * Analyseer bewijsmateriaal * Voer een reconstructie uit van het incident * 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.* | Incidentresponseteam | | |  |
|  | 3.6 Voltooi de definitieve schatting en de documentatie over soort en afbakening van de blootgestelde data, evenals de beschikbaarheid en contactinformatie van de betrokken personen.  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.* | Incidentresponseteam  IBP-verantwoordelijke/FG | | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **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. Zijn er onderwijsprocessen of ondersteunende processen gestopt als gevolg van het incident? Herstart deze dan op een zorgvuldig gecontroleerde wijze en zorg ervoor dat risico’s die verband houden met dit incident weggenomen zijn.** | | | |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |
|  | 4.1 Ga terug naar stap 3.2 en zoek naar aanvullende manieren om de blootstelling te beperken.    Voorbeelden:   1. Run periodiek web-query’s om zeker te weten dat de data niet verder is verspreid of gecached. 2. Beoordeel de inventarisatie van getroffen hardware en systemen en wijzig waar nodig de wachtwoorden die mogelijk gecorrumpeerd zijn. 3. Stop eventueel gecorrumpeerde diensten of applicaties en zorg voor work-arounds | Incidentresponseteam |  |
|  | 4.2 Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatierisico’s voor gevoelige dataopslag    Voorbeelden:   1. Run vulnerabilityscans 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 softwaretools om gevoelige data te vinden, te verwijderen en te beschermen. | Incidentresponseteam |  |
|  | 4.3   Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is, kunnen de systemen 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 daarvan 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 IBD en de politie. Bij sommige incidenten is het wettelijk verplicht een melding te doen naar andere instanties. Snelheid is ook belangrijk vanuit PR-oogpunt. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden.** | | | | | |  |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | | | ***Notities*** |  |
|  | * 1. Neem beslissingen op basis van de bevindingen van het Incidentresponseteam * Maakt de risicoblootstelling het noodzakelijk getroffenen te informeren? Zo ja, bepaal vervolgens:   + Wie gaat communiceren?   + Wie gaat vragen van betrokken personen via telefoon en e-mail beantwoorden? 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 school? * Als er geen kans is geweest op blootstelling van informatie aan buitenstaanders, dan kun je eventueel meteen doorgaan naar stap 6. | Bestuur | | |  |  |
|  | 5.2 Zijn er persoonsgegevens betrokken bij het incident en is er mogelijke schade voor betrokkenen? Dan dient dit binnen 72 uur gemeld te worden bij de Autoriteit Persoonsgegevens. Zie hiervoor de Aanpak IBP beveiligingsincidenten en datalekken | IBP-verantwoordelijke/ FG | | |  |  |
|  | 5.3 Verzamel de naam- en adresgegevens van de getroffenen | Incidentresponseteam | | |  |  |
|  | 5.4 Zet telefoon- en e-mailondersteuning op in geval van vragen:   * Stel een team samen. * Zorg voor voldoende infrastructuur, beoordeel of de telefoon- en e-mailcapaciteit voldoende is. * Kies een geschikt telefoonnummer. * Kies een geschikt e-mailadres. * Bedenk van tevoren de reacties op de verwachte vragen. * Train het team. | Incidentresponseteam | | |  |  |
|  | 5.5 Als in stap 2 een website gekozen is om te communiceren:   * Verzin een URL en websitelocatie. * Voorkom toegang totdat de website live mag gaan. * Bereid de inhoud voor.   *Handleiding:*   1. *Websites worden vooral gemaakt als het aantal getroffenen te groot is of omdat niet alle mensen bekend zijn.* 2. *De websitecontent moet goedgekeurd worden.* | | Incidentresponseteam |  | |  |
|  | 5.6 Voorbereiding schriftelijke informatieverstrekking aan getroffenen:   * Bedenk het onderwerp en de huisstijl. * Schrijf een concepttekst.     *Handleiding:*  *De inhoud van de brief moet zijn goedgekeurd door het management en door voorlichting.* | | Incidentresponseteam |  | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STAP 6: Afsluiten Incident** | | | |  |
| **In deze stap wordt het incident afgesloten. De oorzaken zijn weggenomen, de systemen zijn hersteld. Bewijsmateriaal en incidentgegevens worden gearchiveerd, de diverse partijen kunnen worden geïnformeerd.** | | | |  |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |  |
|  | 6.1 Archiveer al het verzamelde forensisch bewijsmateriaal | Incidentmanager |  |  |
|  | 6.2 Archiveer incident informatie en communicatiegegevens en het logboek | Incidentmanager |  |  |
|  | 6.3 Als er nog geen betrokkenen zijn genotificeerd en er zijn persoonsgegevens betrokken, ga terug naar de vorige stap | Incidentresponseteam |  |  |
|  | 6.4 Doe de benodigde meldingen   * Als er een noodzaak of een verplichting is, informeer dan de politie en doe aangifte. * Doe de definitieve melding aan de Autoriteit Persoonsgegevens (AP) als er bij stap 2.1 een voormelding gedaan is. Doe een gemotiveerde melding aan de AP als er bij tap 2.1 geen voormelding gedaan is en er toch meldplichtige persoonsgegevens gelekt zijn. (Gemotiveerd, omdat als bij een AP-melding meer dan 72 uur verstreken zijn sinds de ontdekking van het datalek, je moet uitleggen waarom je pas na 72 uur een melding doet.) * Informeer derde partijen zoals serviceproviders als hiermee het risico van identiteitsdiefstal verkleind kan worden of als dat is vastgelegd in het contract. * Als er bankgegevens blootgesteld zijn aan niet-rechthebbenden, informeer dan de bank of creditcardfirma’s. * Coördineer de gelijktijdige communicatieacties zodat de verschillende informatiestromen gelijktijdig plaatsvinden. | IBP-verantwoordelijke/FG |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 en pas het gevolgde draaiboek aan.** | | | |  |
| ***Gedaan*** | ***Taak*** | ***Eigenaar*** | ***Notities*** |  |
|  | 7.1 Verzamel alle tijdschrijfregels van het personeel dat heeft meegewerkt aan de Incidentresponse-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 bestuur |  |  |
|  |
|  | 7.2 Plan een vergadering ongeveer 2 tot 6 weken na het incident om de aanpak van het incident te evalueren. | Incidentresponseteam |  |  |
|  | 7.3 Onderzoek oplossingen om herhaling te voorkomen.   * Indien nodig rapporteer hierover aan het management.   Te beantwoorden vragen:   1. Waarom was de data opgeslagen op een verkeerde of onveilige plaats? 2. Wat hadden we meer kunnen doen om de inbraak te voorkomen? 3. Neemt de afdeling voldoende maatregelen om herhaling te voorkomen? | IBP-verantwoordelijke /FG |  |  |
|  | 7.4 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 en of er verbeterpunten zijn aan het proces).* | IBP-verantwoordelijke /FG |  |  |
|  | 7.5 Plan oplossingsprojecten om de geleerde lessen effectief in te bedden in de organisatie. | Behandelaar |  |  |
|  |
|  | 7.6 Sla alle incident- en response-informatie veilig op, inclusief gesprekverslagen, aantekeningen en incidentartefacten. In overeenstemming met wetgeving en intern beleid zal op enig moment (een deel van) de opgeslagen informatie vernietigd moeten worden.  Als het gaat om een inbreuk van de bescherming van persoonsgegevens, moet hiervan altijd een overzicht worden bijgehouden. | IBP-verantwoordelijke/ FG |  |  |