Factsheet Incidentmanagement

Let op: nieuw telefoonnummer IBD
070 - 204 55 11

(Basis-) maatregelen kunnen risico's op informatiebeveiligingsincidenten sterk verminderen. Incidenten zijn echter nooit helemaal te voorkomen. Daarom is het van groot belang dat de gemeentelijke organisatie is voorbereid voor als het toch mis gaat. De schade bij een incident kan met goede voorbereiding worden beperkt. De IBD adviseert om het proces van incidentmanagement in te richten, te oefenen en regelmatig te actualiseren. Op hoofdlijnen zijn de verschillende aspecten van incidentmanagement op een rij gezet in deze factsheet. Daarbij is beschreven hoe u er zelf mee aan de slag kunt en in welke ondersteuningsproducten van de IBD u meer informatie kunt vinden over dit onderwerp. Incidentmanagement is één van de basisprocessen om de beveiliging op orde te krijgen. De IBD biedt hierop ondersteuning in het programma Verhogen Digitale Weerbaarheid.[1]

Waarom is incidentmanagement van belang

Er zijn verschillende soorten incidenten, van incidenten in de bedrijfsvoering tot fysieke gebeurtenissen zoals bijvoorbeeld brand. In deze factsheet ligt de focus op incidentmanagement als essentieel proces voor het zo snel mogelijk reageren op en verhelpen van informatiebeveiligingsincidenten. Die kunnen variëren van een kleine verstoring tot serieuze incidenten zoals een ransomware-aanval of datalekken. Incidenten kunnen grote financiële- en imagoschade voor de organisatie tot gevolg hebben, maar ook schade voor inwoners of bedrijven. Daarom is het inrichten van een incidentmanagementproces dan ook een verplichting vanuit de BIO (Hoofdstuk 16).[2]

Waar begin ik?

- Weet wie u nodig heeft bij het oplossen van een incident, denk aan leveranciers, dienstverleners en collega's. Zorg ook dat u deze mensen kent en dat u ze kunt bereiken, bijvoorbeeld in een appgroep.
- Zorg dat relevante stakeholders tijdig worden geïnformeerd. Dit zal in veel gevallen in ieder geval de Chief Information Security Officer (CISO) zijn. Denk bij grotere incidenten ook aan het management en bijvoorbeeld de gemeentesecretaris. Ook relevante functionarissen van de ICT-afdeling dienen tijdig betrokken te worden bij het afhandelen van het incident. Maak hierover duidelijke afspraken, dan weet men elkaar sneller te vinden als er daadwerkelijk sprake is van een incident met mogelijk hoge impact. Niet voor ieder incident hoeft het crisisteam bijeen te komen. Dit is afhankelijk van de impact. Wijs in ieder geval een incidentmanager of voorzitter van het crisisteam aan voor de coördinatie. Een crisisteam bestaat minimaal uit:
  - Vertegenwoordiger van de business/ gemeentesecretaris / dienstverleners
  - De CISO
  - Technisch specialist/ beheerder/ CIO
  - Communicatieadviseur
  - Privacy Officer (eventueel ook de Functionaris Gegevensbescherming).
- Bij incidenten is het van belang dat er snel geschakeld wordt na het ontdekken van een incident. Het eerste uur na de ontdekking en identificatie van een incident wordt ook wel het 'gouden uur' genoemd. Vlak na ontdekking is het dan ook van groot belang dat geen informatie verloren gaat voor onderzoek. Dit geldt zowel tijdens het oplossen van het incident als ook achteraf. Zo is het mogelijk het incident zo effectief mogelijk te verhelpen en kunnen bewijsstukken en een bijgehouden logboek achteraf helpen om de oorzaak en impact van het incident te achterhalen. Zie hiervoor ook de Factsheet 'Gehackt, hoe nu verder?' [3]
- Zorg ervoor dat er altijd melding wordt gedaan bij vermoeden van een informatiebeveiligingsincident. Dit kan in veel gevallen in eerste instantie bij de ICT-servicedesk en bij vermoedens van incidenten met een grote impact ook rechtstreeks bij de CISO. Belangrijk is dat voor iedere medewerker duidelijk is waar incidenten kunnen worden gemeld en dat er een open cultuur is om te melden. Tegelijkertijd moet de verantwoordelijkheid voor het afhandelen van de incidentmeldingen ook duidelijk worden belegd. Laat bij twijfel altijd iemand melden.
- Meld incidenten via de vertrouwde contactpersoon van de gemeente (VCIB) bij de IBD.[4] Eventueel kan dit ook iemand anders zijn als bijvoorbeeld de CISO. Daarbij kan de IBD-CERT (Computer Emergency Response Team) u direct voorzien van advies in het afhandelen van het incident en waar nodig escaleren naar andere gemeenten. Mochten meerdere gemeenten last hebben van hetzelfde incident dan kan de IBD optreden als contactpersoon richting de leverancier. Ook kan de IBD bij ernstige of complexe incidenten de hulp inroepen van andere gemeenten, andere (overheids)partijen en specialisten.
- Zijn er persoonsgegevens betrokken bij het incident en is er mogelijke schade voor betrokkenen dan dient dit ook binnen 72 uur gemeld te worden bij de Autoriteit Persoonsgegevens.[5]
- Bewaar gelogde en gerapporteerde informatie over (vermoedelijke) beveiligingsincidenten voor minimaal 3 jaar. Zo is het mogelijk om bepaalde patronen in incidenten te

ontdekken en relaties te leggen met onderkende risico's. Waar nodig kan dit leiden tot aanvullende maatregelen of melding hiervan aan relevante stakeholders. Deel ook analyses van beveiligingsincidenten met relevante partners als andere gemeenten en de IBD. Op deze manier kan er van elkaar geleerd worden en kunnen preventieve maatregelen worden genomen op incidenten die bij andere gemeenten al zijn voorgekomen.
- Gebruik een standaard locatie of template voor de logging en rapportage van incidenten. Dit kan bijvoorbeeld volgens het 'Incidentmanagement en response beleid stappenplan en sjabloon'.[6]

Hoe pak ik het aan?

- Maak handig gebruik van de Mindmap processen voor VDW module 1.[7] Hierin is voor de verschillende processen uitgewerkt wat de basismaatregelen zijn. Zo ook voor het incidentmanagementproces. Daarmee kan de basis op orde worden gebracht. Zodra hierin is voorzien kan verder worden doorgepakt op verdere professionalisering van het proces.
- Controleer ook aan de hand van hoofdstuk 16 van de BIO of het incident management aan de gestelde eisen voldoet. Dit is van belang omdat hier in de ENSIA-verantwoording naar wordt gevraagd. Maar dit moet vooral ook omdat het helpt om het incidentmanagementproces volwassen en volledig in te richten en in te passen in de organisatie. Zie hiervoor ook de bijbehorende handreiking van de IBD waarin dit voor incidentmanagement verder is uitgewerkt.[8]
- Richt de incident response (reactie) in volgens de volgende 5 stappen:
  - Identificatie: Heeft het incident daadwerkelijk plaatsgevonden en wat is er precies gebeurd? Meld het incident.
  - Indammen van de schade: Betrekken van vooraf gedefinieerde personen voor het indammen van het incident en beperken van de schade. De schade als gevolg van het incident wordt vastgesteld en bewijsmateriaal wordt veiliggesteld. Het beperken van de schade kan ook betekenen dat systemen preventief worden uitgeschakeld of dat andere mitigerende maatregelen worden genomen. In deze fase kan ook forensisch onderzoek worden gestart, hiervoor is toestemming nodig van het management. Verder in deze factsheet wordt hier nader op ingegaan.
  - Remediatie en herstel: Het nemen van maatregelen om de oorzaak van het incident te blokkeren of te verwijderen. Pas als de oorzaak van het incident is weggenomen kan een start gemaakt worden om systemen te herstellen en daarna de bedrijfsprocessen te herstarten als deze gestopt waren. Als het wegnemen van de oorzaak te lang gaat duren kun je niet verder met je bedrijfsprocessen, dit is ook het moment om te onderzoeken of aan de voorwaarden voldaan is voor het activeren van het BCM-plan. Als er diensten zijn uitbesteed is het noodzakelijk om goede afspraken te maken met de leverancier.
  - Kennisgeving: Denk na over communicatie met externe stakeholders. Betrek ook de communicatiemedewerker hierbij. Als er sprake is van een datalek kan vervolgens worden bepaald of een melding moet worden gemaakt bij de Autoriteit Persoonsgegevens (AP). Dit dient in ieder geval binnen 72 uur plaats te vinden. Ook moet worden overwogen of in verband met de gelekte data de betrokkenen moeten worden geïnformeerd. Meld ook aan de IBD als het incident is opgelost.
  - Rapportage en evaluatie: Leer van het incident in bespreking met het team en rapportage. Welke vervolgstappen en maatregelen dienen te worden genomen om het incident in de toekomst te voorkomen? Hoe kan het incidentmanagementproces worden verbeterd? Belangrijk is dat incidenten op een centrale plek worden gedocumenteerd.

Hoe pak ik het structureel op?

- Leg afspraken vast in een incidentmanagement en response beleid. De IBD heeft hiervoor een voorbeeld beschikbaar.[9] Hoe uitgebreid dit beleid zal zijn hangt mede af van de grote en complexiteit van de organisatie. Maak vooral handig gebruik van de onderdelen van het incidentmanagementproces die in dit voorbeeld zijn uitgewerkt. De versie voor de eigen gemeente kan zo verder worden afgestemd op de eigen organisatie. Leg alleen realistische afspraken vast die in de praktijk ook daadwerkelijk kunnen worden nageleefd. Maak ook afspraken met leveranciers. Maak afspraken met de proceseigenaren om gevoel te krijgen bij eisen voor beschikbaarheid.
- Classificeer incidenten op een logische en systematische wijze. Zo kan op basis van urgentie en impact direct worden bepaald welke prioritering het incident moet krijgen. Hiermee kan snel worden ingeschat of bijvoorbeeld moet worden opgeschaald, wie betrokken moeten worden bij de afhandeling van het incident en of het incident gemeld moet worden bij de IBD. De IBD heeft een leidraad opgesteld waarmee incidenten geclassificeerd kunnen worden aan de hand van bepaalde criteria. Pas deze criteria vooral aan naar wat voor de eigen organisatie werkbaar is. Leg ook de relatie met de relevante risico's voor de organisatie.
- Om te weten of u het incidentmanagementproces echt goed georganiseerd heeft, gaat er niets boven oefenen. Dit kan variëren van checklist reviews, table-top oefeningen, tot en met gesimuleerde- of volledige tests. Oefenen kan helpen in de bewustwording binnen de organisatie. Vanuit de oefening kan direct de vraag worden gesteld; hoe hebben wij dit zelf als organisatie op orde? De IBD en de VNG hebben verschillende oefenmogelijkheden en bewustwordingscampagnes beschikbaar gesteld. Soms ook van andere gemeenten.[10]
- Controleer minimaal jaarlijks of het incidentmanagementproces actueel en beschreven is en of verantwoordelijkheden juist zijn belegd. Ook dienen medewerkers voldoende getraind en opgeleid te zijn om toegewezen taken uit te kunnen voeren. Zo kunnen misverstanden worden voorkomen en kan waar nodig het proces geactualiseerd worden.

Wat is verder relevant?

- Controleer of het bedrijfscontinuïteitsbeheer (BCM) voor de organisatie actueel is. Dit is van groot belang voor het borgen

Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatiebeveiligingsdienst.nl. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 204 55 11 (instructies voor het piketnummer op de voicemail).

VNG Realisatie

Let op: nieuw telefoonnummer IBD 070 - 204 55 11

van de dienstverlening aan de inwoners en het voorkomen van informatieverlies. Daarmee heeft het belangrijke raakvlakken met incidentmanagement. Meer hierover is te lezen in de documenten van VDW-module 4: Bedrijfscontinuïteitsbeheer (BCM).[11]

- Gemeenten zijn zelf verantwoordelijk voor het goed inrichten van het incidentmanagementproces, maar bij zeer grote incidenten kunnen gemeenten het soms niet alleen aan. Om direct advies te kunnen geven kan de IBD indien nodig online aansluiten in het crisisteam van een gemeente Hierbij kan evt. ook geïnventariseerd worden op welke rollen en functies versterking gewenst is, om hulp van andere gemeenten uit te vragen. Dit wordt het Gemeentelijk Response Netwerk genoemd (GRN). Hierbij wordt op basis van een profiel door de IBD uitgevraagd of gemeenten (in de regio) hulp kunnen bieden met gerichte kennis en vaardigheden in de vorm van een tijdelijke samenwerking. Hiervoor hoeft een gemeente zich niet vooraf aan te melden. De IBD CERT vervult hierin een coördinerende rol.
- Afhankelijk van de classificatie van het incident kan het laten uitvoeren van digitaal forensisch onderzoek noodzakelijk zijn.[12] Dit start in de indamfase en is ook relevant voor de andere fases van de incident response. Het is daarbij om meerdere redenen belangrijk om vast te stellen wat er precies is gebeurd en wat de aanleiding is geweest. Als een incident te maken heeft met persoonsgegevens, is onderzoek zelfs wettelijk verplicht in het kader van de AVG. Forensisch onderzoek kan zelfs uitmonden in aangifte en strafrechtelijk onderzoek. De IBD CERT kan u hierbij adviseren, belangrijke vragen waar forensisch onderzoek antwoord op moeten geven zijn:
  - Wat is er gebeurd?
  - Hoe kon dit gebeuren?
  - Hoe lang is dit aan de hand geweest?
  - Om welke systemen en welke gegevens gaat het?

Tips uit de praktijk

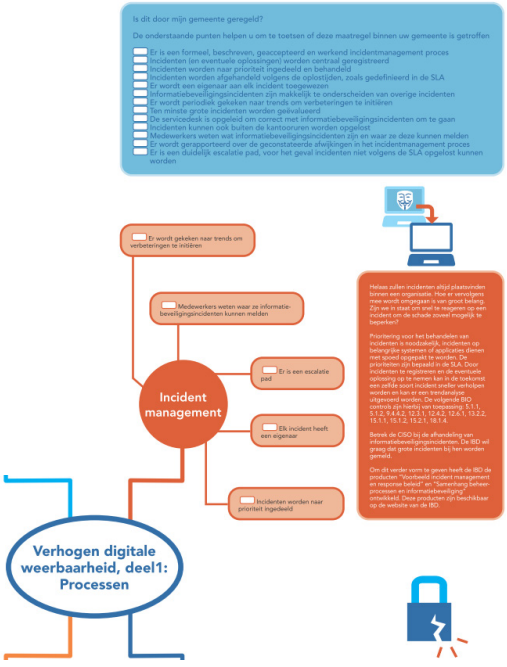
- Bel bij twijfel altijd de Helpdesk van de IBD-CERT voor advies op vervolgacties en woordvoering.[13]
- Documenteer nauwkeurig de uitgevoerde acties in een logboek, deze moeten ook datum en tijd bevatten. Zo kunt u precies nagaan wat precies wanneer heeft plaatsgevonden of is uitgevoerd.
- Incidenten kunnen ook buiten kantooruren plaatsvinden. Denk vooraf goed na over eventuele piket- en bereikbaarheidsdienst. Zorg ervoor dat incidenten ook buiten kantooruren kunnen worden gemeld en opgepakt.
- Richt binnen uw organisatie een chatgroep op waar de personen in zitten die direct op de hoogte moeten worden gesteld in het geval van een informatiebeveiligingsincident. Zo is er direct afstemming voor een risicoschatting, incident declaratie en het bepalen van vervolgacties.
- Leer van beveiligingsincidenten die al hebben plaatsgevonden. Goede voorbeelden hiervan bij gemeenten zijn de lessen van de hack bij de gemeente Lochem juni 2019, maar ook de Citrix-crisis januari 2020 en de hack bij de gemeente Hof van Twente. Van beide incidenten factsheets opgesteld met beschrijvingen en adviezen op deze incidenten. Maak handig gebruik van wat anderen al hebben geleerd.[14] [15] [16]
- Zorg voor een Coordinated Vulnerability Disclosure op de website van de gemeente. Zo kunnen eventuele ontdekte kwetsbaarheden op een verantwoorde wijze worden gemeld. Zie hiervoor ook de handreiking Coordinated Vulnerability Disclosure van de IBD.[17]
- Zorg voor inbedding van het incidentmanagementproces binnen het bestaande, op ITIL gebaseerde, ICT-beheer van de ICT-afdeling of het shared service center. Ga hierbij uit van gezamenlijke belangen en stem werkwijzen op elkaar af. Goede afstemming tussen bestuurlijke- en technische functionarissen bij de gemeente is hierbij van cruciaal belang.

Waar vind ik meer?

Ondersteuning van de IBD bij incidenten
https://www.informatiebeveiligingsdienst.nl/ondersteuning-bij-incidenten/
Verhogen Digitale Weerbaarheid Module 1
https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/
Voorbeeld Incidentmanagement en response beleid
https://www.informatiebeveiligingsdienst.nl/product/voorbeeld-incidentmanagement-en-response-beleid-2/
Factsheet Gehackt, hoe nu verder?
https://www.informatiebeveiligingsdienst.nl/product/factsheet-gehackt-hoe-nu-verder/
Handreiking Digitaal Forensisch Onderzoek
https://www.informatiebeveiligingsdienst.nl/product/digitaal-forensisch-onderzoek/
Baseline Informatiebeveiliging Overheid (BIO)
https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/
ITIL
https://nl.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
Kijk voor meer ook op de productenpagina van de IBD;
https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

Hulp nodig?

U kunt de IBD altijd om advies vragen. Dit kan telefonisch (070 204 55 11) of per mail (info@ibdgemeenten.nl / incident@ibdgemeenten.nl). Voor spoedgevallen is dit nummer zelfs 24/7 bereikbaar. Deel vooral ook uw successen! Ook andere gemeenten kunnen leren van datgene wat werkt.



Links in dit document

1 https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/
2 https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/
3 https://www.informatiebeveiligingsdienst.nl/product/factsheet-gehackt-hoe-nu-verder/
4 https://www.informatiebeveiligingsdienst.nl/ondersteuning-bij-incidenten/
5 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_kom_in_actie_bij_een_datalek.pdf
6 https://www.informatiebeveiligingsdienst.nl/product/voorbeeld-incidentmanagement-en-response-beleid-2/
7 https://www.informatiebeveiligingsdienst.nl/product/vdw-module-1-mindmap-processen/
8 https://www.informatiebeveiligingsdienst.nl/product/voorbeeld-incidentmanagement-en-response-beleid-2/
9 https://www.informatiebeveiligingsdienst.nl/product/voorbeeld-incidentmanagement-en-response-beleid-2/
10 https://www.informatiebeveiligingsdienst.nl/overzicht-bewustwordingscampagnes/
11 https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/
12 https://www.informatiebeveiligingsdienst.nl/product/digitaal-forensisch-onderzoek/
13 https://www.informatiebeveiligingsdienst.nl/ondersteuning-bij-incidenten/
14 https://www.informatiebeveiligingsdienst.nl/product/leren-van-lochem-lessen-uit-een-informatiebeveiligingsincident/
15 https://www.informatiebeveiligingsdienst.nl/product/kwetsbaarheden-in-citrix-lessen-voor-gemeenten-en-de-ibd/
16 https://www.informatiebeveiligingsdienst.nl/product/lessen-uit-de-hack-bij-hof-van-twente/
17 https://www.informatiebeveiligingsdienst.nl/product/handreiking-coordinated-vulnerability-disclosure-bio/