GEMEENTEBLAD
Officiële uitgave van gemeente Heemskerk

BM/2017/18799
12 juli 2017

Bekendmaking vaststelling beleid

Burgemeester en wethouders van Heemskerk maken bekend de beleidsregel Protocol beveiligingsincidenten en datalekken gemeente Heemskerk 2017 vast te stellen.

De nieuwe beleidsregel treedt in werking op 1 juli 2017. Deze regelgeving is vanaf de inwerkingtredingsdatum ook in te zien via www.heemskerk.nl/verordeningen. Nadere inlichtingen: bureau Facilitaire zaken, telefoonnummer 14 0251 of via deze website.

Geconsolideerde tekst van de regeling:

1 Inleiding

Het nemen van passende technische en organisatorische maatregelen om de persoonsgegevens van burgers te beveiligen is naast het creëren van bewustwording en het ervoor zorgen dat burgers hun rechten kunnen uitoefenen, één van de belangrijkste aandachtsgebieden die onder het gegevensbeschermingsbeleid Heemskerk valt. (Overkoepelend beleid Privacy & Gegevensbescherming Gemeente Heemskerk 2016; OD/2016/165423).
Het beheer van beveiligingsincidenten en datalekken is één van de maatregelen die moet zorgen voor de beveiliging van persoonsgegevens. Beveiligingsincidenten zijn helaas niet te voorkomen; 100% beveiliging is een utopie. De vraag is dan ook niet zozeer of er een beveiligingsincident met een hoge impact zal plaatsvinden, maar wanneer. Beveiligingsincidenten kunnen leiden tot onderbreking van werkzaamheden, reputatieschade en aanzienlijke financiële schade als gevolg van het bestrijden van een incident en het herstellen naar een normale situatie. Er kan sprake zijn van schadeclaims van burgers ingeval van nalatigheid of van een grote inbreuk op de beveiliging van persoonsgegevens. Indien de gemeente verzuimd regels te stellen of tekortschiet in de uitvoer hiervan dan loopt de gemeente ook nog eens kans op een aanzienlijke boete van de toezichthouder.

Als het gaat om inbreuk op de beveiliging van of verlies van persoonsgegevens is vanaf 2016 de Meldplicht datalekken van toepassing als toevoeging op de Wet bescherming persoonsgegevens (Wbp). Hiermee heeft de Nederlandse wetgever een voorsprong genomen op de Europese regels omtrent datalekken, welke zijn opgenomen in de Europese Algemene Verordening Gegevensbescherming (AVG), van kracht mei 2018. De meldplicht vereist dat de gemeente een ernstig datalek onverwijld meldt bij de Autoriteit Persoonsgegevens (AP) en aan de betrokkenen (lees: burger) wier persoonsgegevens het betreft.

Reden te meer om het beheer van informatiebeveiligingsincidenten structureel te borgen in de organisatie, rekening houdend met de eisen die gesteld worden aan de meldplicht datalekken. Dit document behandelt de organisatie en activiteiten die nodig zijn voor een goed werkend incidentenbeheer waarbij de nadruk ligt om snel, doeltreffend en efficiënt te reageren op het bestrijden en afhandelen van een beveiligingsincident of datalek.

2 Doel, afbakening en doelgroep

Incidentenbeheer is het geheel van organisatorische maatregelen dat ervoor moet zorgen dat een incident adequaat gedetecteerd, gemeld en behandeld wordt om daarmee de kans op uitval van de bedrijfsvoering of schade ontstaan als gevolg van het incident te minimaliseren dan wel te voorkomen. Een incident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden.

Incidentenbeheer gaat eveneens over het detecteren van incidenten. Dat vereist dat de organisatie voldoende maatregelen heeft getroffen om zoveel mogelijk incidenten in beeld te kunnen krijgen door onder meer gebruik te maken van logging en controle daarop, antivirussoftware en een actief werkend Intrusion detection systeem (IDS) op het data netwerkverkeer, maar ook meldingen van de Informatiebeveiligingsdienst (IBD) op mogelijke dreigingen zijn aan te merken als een (bijna) beveiligingsincident. Daarnaast; personeel behoort getraind te zijn op het herkennen van beveiligingsincidenten en te weten wat zij vervolgens moeten doen.

Het beheer van informatiebeveiligingsincidenten heeft betrekking op alle medewerkers en inhuurkrachten die werkzaam zijn bij de gemeente en op ketenpartners en bewerkers van persoonsgegevens waar uitwisseling van informatie plaatsvindt voor zover de verantwoordelijkheid voor het oplossen van een incident en herstel naar een normale situatie bij de gemeente ligt.

3 Organisatie incidentenbeheer

Incidentenbeheer dient structureel ingebed te worden in de interne organisatie van de gemeente Heemskerk. Naast het melden en afhandelen van beveiligingsincidenten is periodieke rapportage, als onderdeel van de P&C cyclus, over incidentenbeheer aan het management en bestuur van groot belang. Zo kunnen de nadelige gevolgen van incidenten en het ontstane inzicht als indicatie over de mate van gegevensbescherming bij de gemeente in kaart gebracht worden, hoewel niet alle beveiligingsincidenten veroorzaakt worden door nalatigheid of tekortkomingen in de beveiliging. Het helpt de organisatie in ieder geval het beveiligingsniveau waar nodig aan te passen en het biedt concrete voorbeelden voor het verhogen van bewustwording bij het personeel over gegevensbescherming.

De Chief Information Security Officer (CISO) is, namens de gemeentesecretaris, verantwoordelijk voor het periodiek verstrekken van informatie over beveiligingsincidenten en gebruikt hiervoor onder meer als input het incidentenregistratiesysteem van de servicedesk (Topdesk).

3.1 Servicedesk

Nu worden alle meldingen van de medewerkers in de organisatie, door bijvoorbeeld een e-mail te zenden, automatisch geregistreerd in de servicedesk van het team Automatisering en dit team of het team Facilitaire Dienst (FD) handelt deze meldingen in de meeste gevallen ook af. Ook gaan de meldingen die via de IBD bij de Vertrouwde Contactpersonen Informatiebeveiliging (VCIB) binnenkomen zo nodig het systeem van de servicedesk in.
Beveiligingsincidenten kunnen op diverse manieren worden gemeld. Hoe de toegang ook plaatsvind, de meldingen dienen te worden geregistreerd in de servicedesk. De voortgang kan worden bewaakt en de samenwerking tussen CISO en Automatisering wordt hiermee optimaal ingekleed. CISO en FG hebben

toegang tot de melding van het incident en dienen deze onder de eigen verantwoordelijkheid op te pakken en te behandelen.
Voor de aanmelding tot en met de afhandeling van een incident maakt het team Automatisering gebruik van een daarop afgestemde ITIL procedure (zie bijlage).

3.2 Computer Security Incident Response Team (CSIRT)

De gemeente Heemskerk heeft een Computer Security Incident Response Team (CSIRT) ingesteld om voorbereid te zijn om snel en adequaat te kunnen reageren op een beveiligingsincident die bijvoorbeeld buiten de scope van de servicedesk valt. Het gaat dan om beveiligingsincidenten met een hoog of kritische classificatie die directe mobilisering van het CSIRT vereist. Dit team bestaat uit een vaste kern medewerkers van de organisatie die afhankelijk van het incident gebruik maakt van andere noodzakelijke competenties/disciplines waaronder eventuele externe inhuur.

Het managementteam heeft de vaste kern van het CSIRT benoemd en deze bestaat uit de CISO, de CIO (Chief Information Officer) en de FG (Functionaris Gegevensbescherming). De CISO is team coördinator en verantwoordelijk voor een juiste procesmatige afhandeling van een incident dat via het CSIRT loopt. De CIO is verantwoordelijk voor het technisch bestrijden (ICT) van het incident en voor de technische herstelfase. De FG bepaalt de mate van inbreuk op de beveiliging van persoonsgegevens. Afhankelijk van de aard, omvang en impact van het incident kunnen de volgende teamleden dan wel disciplines worden toegevoegd:

- lijnmanager waarop het incident betrekking heeft en betrokken moet zijn bij de te volgen aanpak;
- gemeentesecretaris of de Algemeen Contactpersoon Informatiebeveiliging (ACIB), indien het incident bestuurlijke impact kan hebben;
- juridische bijstand om de gevolgen van een incident juridisch te toetsen. Denk aan aansprakelijkheid en boetes (Wbp/Avg);
- communicatie adviseur om mogelijke reputatieschade zoveel mogelijk in te dammen en direct te werken aan reputatieherstel;
- financieel specialist om de schadekosten in beeld te brengen en na te gaan in hoeverre de schade verzekeringstechnisch is afgedekt en de financiële claim afwikkelt;
- vertrouwensfunctionaris ingeval sprake is van verwijtbaar gedrag van een medewerker die een incident heeft veroorzaakt;
- externe inhuur indien bijzondere expertise nodig is zoals een ICT-specialist of een digitaal forensisch expert.

Deelname van inhuurkrachten aan het CSIRT vereist dat zij vooraf een integriteits- en geheimhoudingsverklaring hebben ondertekend. Het CSIRT is bevoegd om jaarlijks inhuur externen in te zetten tot een maximum van € 50.000 (exclusief btw) om escalatie van het incident direct te kunnen bestrijden.

Het CSIRT is bevoegd om in te grijpen om de schade als gevolg van een incident zo snel mogelijk in te dammen en de oorzaak te elimineren. Dit kan leiden tot tijdelijke uitval van de dienstverlening en/of tot dataverlies.

Het CSIRT onderhoudt een draaiboek om snel en adequaat te kunnen reageren op beveiligingsincidenten. Het draaiboek bevat van te voren bedachte reacties, checklists en escalatie procedures, sjablonen voor rapportages die periodiek uitgewerkt en geoefend worden.

Deelname aan het CSIRT vereist dat bij mobilisering het lopende werk van de teamleden tijdelijk wordt gestaakt, enigszins te vergelijken met het uitrukken van een brandweerteam. Het CSIRT is 24/7 bereikbaar omdat een incident met een kritische of hoge classificatie zich niet houdt aan werktijden. Voor de vaste kern van het CSIRT is uit dien hoofde voorzien in tijdelijke vervanging.

Er is een bereikbaarheidslijst van alle vaste (en potentiële) teamleden en een overzicht voor ‘piketdienst’ die de CISO onderhoudt.

4 Procedure

Een succesvolle security incident response bestaat uit een aantal te doorlopen processtappen die voor elk incident gelijk is. De verschillen zitten voornamelijk in de details (inhoud). Van belang is dat de organisatie beschikt over een security incident response draaiboek waarin diverse beveiligingsincident modellen (cheat sheets) zijn opgenomen om bepaalde type incidenten snel en efficiënt te kunnen afhandelen.

Elke medewerker van onze organisatie dient alert te zijn op bedreigingen met betrekking tot gegevensbescherming en is verplicht om elk beveiligingsincident die hij/zij ontdekt of vermoedt, te melden. Daarbij geldt uiteraard dat elke medewerker in staat moet zijn een beveiligingsincident te kunnen herkennen en weet hoe een melding dient te geschieden, hetzij aan de leidinggevende, de CISO of Servicedesk. De drempel voor het melden van een incident dient laag te zijn. De CISO zorgt ervoor dat informatie over het herkennen van beveiligingsincidenten (voorbeelden) en hoe gemeld behoort te worden beschikbaar is via daarvoor bestemde communicatiekanalen van de gemeente (denk aan intranet, werkoverleggen en introdagen nieuw personeel). Voorbeelden van beveiligingsincidenten zijn:

- Verlies of diefstal van waardepapier (paspoorten, rijbewijzen), dossier, usb-stick, tablet of andere gegevensdragers
- Niet naleven van beleid of richtlijnen
- Inbreuk op fysieke beveiligingsvoorzieningen
- Toegangsovertredingen
- Opzettelijk foutief handelen (fraude, diefstal)

Maar ook onzorgvuldig omgaan met persoonsgegevens door een bewerker en cyberaanvallen zoals een ddos, computerhacking of besmetting met ransomware, of het technische falen van apparatuur, stroomuitval, wateroverlast en dergelijke zijn aan te merken als incidenten.

De hieronder vermelde stappen hoeven niet volgtijdelijk plaats te vinden maar kunnen ook afhankelijk van de omvang van het CSIRT parallel geschieden.

4.1 Meld intern en prioriteer

De servicedesk is het aangewezen meldpunt en registreert alle incidentmeldingen. Een centraal meldingspunt is van belang om het proces zoveel mogelijk te standaardiseren, om versnippering van geregistreerde meldingen te voorkomen en om het totaaloverzicht te behouden (volledigheid en verantwoording). Meldingen die via de CISO of leidinggevenden binnenkomen worden eveneens geregistreerd in het incidentmeldingssysteem van de servicedesk.

Er zijn afspraken gemaakt met de medewerkers die de servicedesk beheren over de vertrouwelijkheid van de gemelde incidenten en het registratiesysteem is beveiligd tegen ongeautoriseerde toegang.

Alle incidentmeldingen zijn voorzien van een urgentie- en impactcode en gecategoriseerd voor rapportage doeleinden. Hiervoor zijn nadere instructies aanwezig die de CISO onderhoudt in samenwerking met de CIO. Zo is er een overzicht van voorkomende beveiligingsincidenten met vermelding van de urgentie en impact en periodiek wordt geactualiseerd door de CISO.

Servicedesk-medewerkers zijn geïnstrueerd over het direct doorgeven van incidenten aan de CISO en CIO die buiten hun scope vallen. Alle medewerkers van de servicedesk hebben een integriteits- en geheimhoudingsverklaring ondertekend. Vanuit Automatisering vindt toezicht plaats op de servicedesk en dagelijks controle op urgentie en impact van nieuwe meldingen.

4.2 Mobiliseer CSIRT

De vaste kern van het CSIRT wordt gemobiliseerd indien vanuit de servicedesk een incident is afgegeven met een hoge of kritische impact of indien een dergelijke melding rechtstreeks bij een van de vaste leden binnenkomt. De vaste kern van het CSIRT beoordeelt direct de aard en omvang van het incident en stelt vast of het incident ook daadwerkelijk heeft plaatsgevonden, bijvoorbeeld
door contact op te nemen met team Automatisering of de melder van het incident. Daarbij maakt de vaste kern van het CSIRT gebruik van een checklist om snel inzicht te krijgen in:

- de aard en omvang van het incident,
- welke teamleden aanvullend opgenomen moeten worden in het CSIRT en
- welke instanties geïnformeerd moeten worden over het incident (IBD, AP, etc).

Het CSIRT is belast met het beperken van verdere schade als gevolg van het incident, het blokkeren of verwijderen van de oorzaak, stelt de schade vast en zorgt voor het veiligstellen van bewijsmateriaal. Van elk incident dat via het CSIRT loopt vindt dossiervorming plaats. Het CSIRT maakt hierbij zoveel mogelijk gebruik van kennis en ervaring en voorbereidingen die zijn vastgelegd in een daarvoor opgesteld draaiboek.

Het CSIRT bepaalt welke acties noodzakelijk zijn en neemt bij twijfel contact op voor advies met de helpdesk van het IBD. Voor elk te behandelen incident via het CSIRT geldt dat teamleden niet mogen praten met anderen buiten het team totdat daarvoor toestemming is gegeven door de CISO. Dit om zoveel mogelijk ruis in de communicatie te voorkomen.

De CISO onderhoudt het contact met de gemeentesecretaris over de stand van zaken betreffende het incident. De gemeentesecretaris of de Algemeen Contactpersoon Informatiebeveiliging (ACIB) informeert indien nodig het bestuur.

4.3 Beperk schade en elimineer oorzaak

Er wordt zo snel mogelijk gestart met het indammen van de schade door het incident te blokkeren, te verwijderen en de impact voor verdere blootstelling te verminderen. Dit kunnen zowel activiteiten zijn vanuit de techniek als vanuit de organisatie. Vanuit de techniek is de CIO belast met het indammen van de schade en blokkeren of verwijderen van de oorzaak eventueel ondersteunt met externe expertise. Daarbij maakt het team waar nodig gebruik van vooraf opgestelde escalatieprocedures. Deze repressieve handelingen kunnen leiden tot tijdelijke uitval van onderdelen van het ICT-netwerk en/of verlies van data om verdere schade te voorkomen.

Het CSIRT bepaalt in samenspraak met de verantwoordelijke lijnmanager en de communicatie adviseur de (interne en externe) communicatiestrategie. Intern kan dit gericht zijn op het melden van het incident met bijbehorende instructies om bepaalde handelingen tijdelijk niet uit te voeren met eventueel een voorlopig spreekverbod om escalatie zoveel mogelijk te voorkomen. Extern is de communicatie gericht om zoveel mogelijk reputatieschade te voorkomen en direct te werken aan reputatieherstel. Externe communicatie geschiedt altijd in overleg met de gemeentesecretaris.

Indien sprake is van (mogelijke) inbreuk op de beveiliging van persoonsgegevens behoort een ernstige datalek onverwijld te worden gemeld bij het AP en eventueel aan betrokkenen. Dit traject loopt altijd via de FG. Zie hiervoor verder hoofdstuk 5. De CISO ziet er op toe dat dit traject conform de daarvoor geldende procedure wordt afgehandeld.

Het CSIRT adviseert de gemeentesecretaris aan de hand van de aard van het incident en in overleg met de juridische afdeling of aangifte bij de politie gedaan moet worden.

4.4 Herstel oude situatie

Na het indammen van de schade en het verwijderen van het incident is zo spoedig mogelijk herstel naar de oude situatie nodig. Bij bedrijfsprocessen die (deels) gestopt zijn als gevolg van een incident vindt op een gecontroleerde wijze een herstart plaats. Eventueel verlies van data wordt gereconstrueerd bijvoorbeeld aan de hand van een recovery procedure en/of brondocumenten. Het herstarten van een bedrijfsproces geschiedt in nauw overleg met de verantwoordelijke lijnmanager.
In overleg met de verantwoordelijke lijnmanager vindt communicatie naar de organisatie plaats over het herstel en eventuele gevolgen ervan.

Het bureau Planning, Control en Financiën (PCF) brengt de directe en indirecte kosten als gevolg van de schade zoveel mogelijk in beeld, rekening houdend met mogelijk ingediende schadeclaims van derden. Voorts wordt nagegaan in hoeverre deze kosten verhaald kunnen worden via de verzekering of derden dan wel voor eigen rekening zijn. Bureau PCF is eventueel in overleg met het team Juridische Zaken belast met de verdere financiële afwikkeling van het incident.

Ingeval een medewerker van de gemeente betrokken is bij de oorzaak van een beveiligingsincident door nalatig of kwaadwillend gedrag en daarvoor het nodige bewijsmateriaal is veiliggesteld, wordt de vertrouwensfunctionaris ingeschakeld en eventueel aangifte gedaan bij de politie. De gevolgen hiervan voor de betrokken medewerker kunnen leiden tot disciplinaire maatregelen, strafrechtelijk onderzoek en/of tot ontslag. Voor betrokkenheid van een externe medewerker geldt eenzelfde procedure met dien verstande dat

er geen vertrouwensfunctionaris betrokken is, maar wel dat het contract ontbonden kan worden. Schade kan worden verhaald op het bedrijf waar de externe in dienst is.

4.5 Informeer doelgroepen/betrokkenen

Van elk beveiligingsincident van enige omvang is een communicatiestrategie bepaald en uitgewerkt door team Communicatie en erop gericht op het zo veel mogelijk indammen van reputatieschade en op reputatieherstel. Intern gaat het dan om de gemeenteraad, bestuur, management en medewerkers en extern om betrokkenen, ketenpartners, media en andere belanghebbenden. Vooraf zijn hiervoor al de nodige standaard teksten in eigen huisstijl beschikbaar om geen tijd te verliezen waar snelheid geboden is.
Ingeval sprake is van een datalek wordt verwezen naar de meldplicht zoals opgenomen in hoofdstuk 5.
Indien nodig informeert de CISO de IBD over het beveiligingsincident met als doel om hieruit lering te trekken en dit geanonimiseerd door te communiceren naar andere gemeenten.

4.6 Evalueer, rapporteer en documenteer

Het CSIRT verzamelt van elk beveiligingsincident waarop dossiervorming van toepassing is alle documentatie die nodig is voor bewijsvoering ingeval sprake is van civiel of strafrechtelijk onderzoek, schadeclaims of toezicht vanuit het AP. Documentatie kan bestaan uit bespreekverslagen, ingevulde checklist, printscreens, emails, controle op loggings, bevindingen van ICT-specialisten of digitaal forensische experts, processen verbaal en de (uitwerking van de) communicatiestrategie.

Het CSIRT voert een evaluatie uit en legt dit vast in een rapportage inclusief advies, ter verbetering. Het rapport wordt voorgelegd aan de gemeentesecretaris en besproken. Waar nodig past de CISO het security incident response draaiboek aan.

Na afsluiting van het incident archiveert de CISO het incidentendossier. Vernietiging van het dossier vindt plaats nadat de daarvoor geldende wettelijke bewaartermijnen zijn verlopen. Het dossier is vertrouwelijk tenzij de CISO anders bepaalt.

5 Meldplicht datalekken

De meldplicht datalekken is opgenomen in de Wbp/Avg en brengt wettelijke verplichtingen met zich mee wanneer persoonsgegevens gevaar hebben gelopen. Het gaat dan om informatiebeveiligings-incidenten die de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens in gevaar brengen. Denk hierbij aan het verlies of ongeautoriseerde wijzigingen van persoonsgegevens of het kwijtraken van persoonsgegevens zonder een backup.

De wet vereist dat de gemeente ernstige datalekken onverwijld (binnen 72 uur) meldt aan het AP. Daarnaast geldt als eis dat alle betrokkenen worden geïnformeerd wanneer een datalek voor hem/haar waarschijnlijk ongunstige gevolgen heeft. Het is dus niet zo dat elk datalek moet worden gemeld maar daarvoor is wel een deugdelijke afweging nodig in de vorm van een privacy impactanalyse (PIA). Zo kan het dus gebeuren dat een datalek wel moet worden gemeld aan het AP, maar niet aan betrokkenen, omdat hun persoonsgegevens onbegrijpelijk (door versleuteling) of ontoegankelijk zijn voor degenen die geen recht hebben op inzage in deze gegevens.

Bij uitbesteding van taken aan bijvoorbeeld een salarisadministratiekantoor of gemeenschappelijke regeling waarbij sprake is van verwerking van persoonsgegevens door verwerkers blijft de gemeente aansprakelijk voor het melden van een datalek. Er zijn dan ook met alle verwerkers afspraken gemaakt over de gestelde eisen op het gebied van gegevensbescherming en over het onmiddellijk melden van beveiligingsproblemen aan de FG.

De FG stelt in samenwerking met de CISO een draaiboek op voor de afhandeling van informatiebeveiligingsincidenten die onder de meldplicht datalekken vallen. Daarin staan onder meer de criteria wat onder een datalek wordt verstaan en wanneer moet worden gemeld aan het AP en aan betrokkenen. De FG is eveneens belast met het periodiek onderhoud van het draaiboek.

Elk datalek volgt de procedure zoals beschreven in hoofdstuk 4. In hoofdstuk 5 komen alleen de specifieke eisen ten aanzien van de meldplicht datalekken ter sprake.

5.1 Analyseer impact datalek

Signalering van een datalek komt zoals elk ander incident centraal binnen bij de servicedesk en wordt via prioritering direct doorgesluisd naar de vaste leden van het CSIRT. Vanwege het gegeven dat een gemeente binnen 3 werkdagen behoort te melden aan het AP dient een privacy impactanalyse op het incident direct te worden opgepakt.

Gevolgen voor betrokkenen

In deze fase bepaalt de FG of de gemeente moet melden aan alleen het AP of aan het AP en betrokkenen. Indien nodig vraagt de FG advies bij het team Juridische Zaken of bij een externe adviseur die gespecialiseerd is in privacywetgeving. In essentie wordt bepaald of er op enige manier een risico is ontstaan voor de verwerking van persoonsgegevens. Op basis daarvan bepaalt de FG in overleg met het CSIRT of er wel of geen meldplicht is. In de kern gaat het hierbij om de volgende 3 vragen:

1. Is er sprake van een ernstig informatiebeveiligingsincident (ja/nee)?
2. Heeft het incident gevolgen voor betrokkenen (ja/nee)?
3. Zo ja, hoe groot zijn de gevolgen voor de betrokkenen (klein/middel/groot)?

De FG maakt hierbij gebruik van een standaard beoordelingsformulier voor het vastleggen van relevante informatie en bevindingen over het wel/niet melden. Bij de afweging om te melden aan betrokkenen kan gedacht worden aan de noodzaak om tijdig acties te ondernemen door betrokkenen om de gevolgen van een datalek te beperken of te herstellen en de emotionele impact op betrokkenen.
Het feit dat een melding aan betrokkenen kan leiden tot een relatief groot tijdbeslag en administratieve lasten is in beginsel geen zwaarwegende reden om niet aan betrokkenen te melden.
Het AP kan een gemeente na melding alsnog gelasten om melding te doen aan betrokkenen ondanks dat de gemeente aan het AP heeft aangegeven dit niet te doen.

Gevolgen voor eigen organisatie

In tweede instantie bepaalt de FG met andere leden van het CSIRT wat de gevolgen zijn voor de eigen organisatie waarmee bedoeld wordt welke vervolgacties noodzakelijk zijn om het datalek volgens de eisen van de meldplicht datalekken af te handelen. Een datalek kan leiden tot reputatieschade en mogelijke

schadeclaims indien het lek verwijtbaar is en betrokkenen schade hebben geleden. De gemeente is verplicht te melden aan betrokkenen en dit kan leiden tot lokale en mogelijk landelijke bekendheid.

De gemeente moet inzicht krijgen:

- of wel of niet gemeld moet worden aan alleen AP of AP en betrokkenen,
- in de juridische gevolgen voor schadeclaims of boetes,
- in de te verwachten kosten en dekking van deze kosten (denk aan verzekeringspolissen of indienen van schadeclaims indien een bewerker de schade heeft veroorzaakt).
- in de afhandeling (nazorg) van een datalek naar betrokkenen,
- In de communicatie-aanpak om reputatieschade zo beperkt mogelijk te houden.

Voor het dichten van het lek vindt aansluiting plaats met hoofdstuk 4. In het laatste geval gaat het dan om bijvoorbeeld herstel van gegevens of getroffen processen, maar ook indien van toepassing om disciplinaire maatregelen naar de medewerker die door nalatigheid het lek heeft veroorzaakt.

5.2 Meld datalek aan AP

De melding aan het AP verloopt via het digitale formulier van het AP. De FG is belast met de melding aan het AP. De melding kan eventueel naderhand worden aangevuld of ingetrokken. De ontvangstbevestiging via email wordt opgenomen in het dossier van het betreffende datalek.

5.3 Meld datalek aan betrokkenen

Voor het melden van een datalek aan betrokkenen geldt eveneens dat dit ‘onverwijld’ moet gebeuren. Er gelden hiervoor geen specifieke termijnen maar onnodige vertraging moet worden vermeden. De wijze waarop betrokkenen worden geïnformeerd, bepaalt de gemeente zelf. Een goed doordachte communicatiestrategie is dan ook van belang om reputatieschade zo beperkt mogelijk te houden. Het team Communicatie is hierbij nadrukkelijk betrokken evenals de gemeentesecretaris. De informatie die verstrekt moet worden, gaat minimaal in op de volgende vragen:

- Wat is er aan de hand en wat zijn de mogelijke gevolgen voor betrokkenen?
- Waar kan betrokkenen terecht met vragen?
- Wat kan betrokkenen zelf doen?

Indien adresgegevens van betrokkenen bekend zijn, kan melding plaatsvinden via een brief of via email met eventueel verwijzing naar een website met aanvullende informatie of meest gestelde vragen van betrokkenen (FAQ). De email of brief kan daardoor beknopt blijven. Vanuit de nazorg zorgt de gemeente ervoor dat betrokkenen de mogelijkheid hebben om vragen te kunnen stellen hetzij via een daarvoor ingericht emailadres of telefoonnummer.

5.4 Meld datalek aan overige partijen

Het gevaar is aanwezig dat de communicatie over een datalek wordt overgenomen door andere partijen/platforms zoals lokale, landelijke of sociale media, eigen medewerkers of ketenpartners waardoor als gevolg van ruis in de communicatie een datalek alsnog onnodig kan escaleren. Belangrijk is dat de gemeente de regie behoudt over de communicatie van een ernstig datalek dat gemeld is bij het AP en aan betrokkenen. Bij de uitwerking van de communicatiestrategie vindt afstemming plaats welke doelgroepen / overige partijen

worden geïnformeerd over het datalek en op welke wijze. Timing is hierbij ook van belang en zeker indien de melding al heeft plaatsgevonden aan betrokkenen.
Van belang is dat het management, bestuur en de gemeenteraad van de gemeente tijdig geïnformeerd zijn vanwege hun positie in de organisatie en contacten in de samenleving. Uiteraard behoren de medewerkers van de gemeente eveneens op de hoogte te worden gesteld om ruis in de communicatie te voorkomen en wellicht hen te voorzien van instructies hoe te reageren op vragen vanuit de samenleving en terughoudend te zijn met reacties op sociale media.

Via een persbericht stelt de gemeente de media op de hoogte, eventueel aanvullend met een persconferentie voor het stellen van vragen. Uiteraard behoort dit geheel afgestemd te zijn op de grootte van het datalek.

Een datalek kan een flinke knauw geven in het gestelde vertrouwen bij ketenpartners en aan de publieke sector als geheel. Ketenpartners kunnen zelfs last hebben indien sprake is van uitwisseling van informatie waarop het datalek betrekking heeft. Ketenpartners behoren dan ook geïnformeerd te worden over mogelijke nadelige gevolgen voor hun organisatie.

6 Prioritering informatiebeveiligingsincident

Om de geschikte incidentmaatregelen te activeren hanteert de gemeente een leidraad voor incidenten prioritering. Deze prioritering wordt herleid uit een tweetal factoren: urgentie en impact. De urgentie is de maat voor hoe snel de oplossing van een incident vereist is en de impact is de maat voor de omvang van het incident en van de mogelijke schade als gevolg van het incident voordat het kan worden opgelost.

De gemeente hanteert de volgende criteria :

Urgentie	***Omschrijving***
Hoog	- De schade, veroorzaakt door het incident neemt snel toe. - Werk dat moet worden hersteld door medewerkers is zeer arbeidsintensief. - Een groot incident kan worden voorkomen door bij een klein incident onmiddellijk te handelen.
Medium	- De schade, veroorzaakt door het incident neemt in de tijd aanzienlijk toe. - Er gaat werk verloren, maar dit is relatief snel te herstellen.
Laag	- De schade, veroorzaakt door het incident neemt in de tijd maar weinig toe. - Het werk dat blijft liggen is niet tijdsintensief.

Impact	***Omschrijving***
Hoog	- Relatief veel personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen. Meerdere afdelingen zijn geraakt, de publieksbalie moet gesloten worden. - Inwoners van een gemeente 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 hoger dan <€50.000,->.

	- Er is reputatieschade, de krant wordt gehaald.
Medium	- Enig personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen, bijvoorbeeld een afdeling. - Enkele inwoners van een gemeente 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 hoger dan <€10.000,-> en lager dan <€50.000,->. - Er is kans op reputatieschade.
Laag	- Enkele personeelsleden zijn geraakt door het incident en/of kunnen niet meer hun werk doen. - Enkele inwoners van een gemeente zijn geraakt en/of lijden schade. - De financiële impact van het incident is lager dan <€10.000,-> - Er is geen kans op reputatieschade.

De Incident Prioriteit wordt verkregen door urgentie en impact tegen elkaar af te zetten. De incident prioriteit matrix ziet er als volgt uit:

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

De kleurcodetabel leidt tot de volgende classificatie:

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

Het CSIRT wordt gemobiliseerd indien de classificatie kritiek of hoog is.

Deze indeling dient te worden vertaald naar een matrix waarin voorbeelden van mogelijke incidenten worden geclassificeerd iom Automatisering/Servicedesk.