gemeente
Het Hogeland

Informatiebeveiligings-rapportage 2018

Gemeente Het Hogeland

24-05-2019

Kenmerk:	Z.HHL.005689
Versie:	V1.1
Versiedatum:	24-05-2019
Gemaakt door:	G. Groot
Portefeuillehouder	Dhr. H.J. Bolding
Goedgekeurd door:	
Classificatie:	Openbaar

Versiebeheer

Versie	Datum	Auteur	Opmerkingen
0.5C	20-04-2019	Guido Groot	Opzet rapportage informatiebeveiliging 2018
0.6C	09-05-2019	Guido Groot	Opmerkingen verwerkt na de reviewronde door FG, Juridische Zaken, Concerncontroller, Strategisch adviseur informatiemanagement, Automatisering, Gegevenshuis, Adviseur informatiebeheer, Burgerzaken.
0.9C	17-05-2019	Guido Groot	Gereed voor afstemming met de gemeentesecretaris
V1.0	21-05-2019	Guido Groot	Opmerkingen verwerkt na afstemming gemeentesecretaris. Gereed voor afstemming met de portefeuillehouder college.
V1.1	24-05-2019	Guido Groot	Opmerkingen verwerkt na afstemming portefeuillehouder college.

Inhoudsopgave

1. Inleiding

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor gemeenten om hun processen uit te voeren. Gemeenten beschikken over een schat aan (zeer) vertrouwelijke informatie over zowel burgers als bedrijven en daarnaast zijn zij verantwoordelijk voor een betrouwbare en continue dienstverlening. Het is daarom belangrijk dat gemeenten op passende wijze hun informatie beveiligen.
Het begrip 'informatiebeveiliging' heeft betrekking op beschikbaarheid, integriteit (juistheid, volledigheid en tijdigheid) en vertrouwelijkheid van gegevens. Hoe waardevoller of gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. Gemeenten dienen bij hun informatiebeveiliging te voldoen aan wet- en regelgeving, zoals bijvoorbeeld voor privacy.
Met deze rapportage Informatiebeveiliging verantwoordt het college van de gemeente Het Hogeland zich aan de gemeenteraad over de status van informatiebeveiliging.

De gemeente dient jaarlijks verantwoording af te leggen over informatieveiligheid. Voorheen waren er aparte verantwoordingsprocedures voor de volgende registratiesystemen en systemen met privacygevoelige informatie:

- Basisregistratie Personen (BRP).
- Paspoort en Nederlandse Identiteitskaart (PNIK).
- Digitale persoonsidentificatie (DigiD).
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).
- Basisregistratie Adressen en Gebouwen (BAG).
- Basisregistratie Grootschalige Topografie (BGT).
- Basisregistratie Ondergrond (BRO).

Deze verantwoordingsprocedures bestaan nog steeds. Echter, sinds 2017 verantwoordt de gemeente zich ten aanzien van het informatiebeveiligingsgedeelte met behulp van een nieuwe systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid en is verplicht voor alle gemeenten. Met ENSIA leggen gemeenten in één keer verantwoording af aan toezichthouders over de informatiebeveiliging van bovenstaande systemen en over informatiebeveiligingsnormen, waaraan alle Nederlandse gemeenten zich dienen te houden (verticale verantwoording). Daarnaast dient het college zich ook naar de gemeenteraad toe te verantwoorden over informatiebeveiliging (horizontale verantwoording). Deze systematiek maakt de stand van zaken rondom informatieveiligheid meer inzichtelijk.

Omdat gemeente Het Hogeland per 1 januari 2019 een feit is hoeft de gemeente zich niet te verantwoorden over het jaar 2018 richting de raad. Omdat de gemeente informatiebeveiliging van groot belang vindt, wil de gemeente door middel van deze rapportage inzicht gegeven in de huidige stand van zaken en de resultaten over het jaar 2018 van de voormalig gemeenten Bedum, De Marne, Winsum en Eemsmond (BMWE - gemeenten).

In deze rapportage gaat het college verder in op:
- Het informatiebeveiligingsbeleid en doelstelling.
- Uitgevoerde acties in 2018.
- Resultaat informatiebeveiliging over 2018/2019
    - Per registratiesysteem;
    - Gemeentebreed.
- Beveiligingsincidenten en calamiteiten 2018.

- Het meerjarenperspectief.

2. Informatiebeveiligingsbeleid en doelstellingen

2.1 Informatiebeveiligingsbeleid

Een vastgesteld informatiebeveiligingsbeleid is het uitgangspunt voor de inrichting en borging van informatiebeveiliging in de gemeente. In 2013 is tijdens de Buitengewone Algemene Ledenvergadering van de VNG besloten dat iedere gemeente de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt voor haar informatiebeveiligingsbeleid hanteert. De BIG voldoet aan de internationaal geaccepteerde beveiligingsstandaarden ISO 27001/27002 en bevat een normenkader met beveiligingsmaatregelen die een goed basis-beveiligingsniveau voor gemeenten neerlegt.

Het huidige informatiebeveiligingsbeleid voor de gemeente Het Hogeland is in maart 2019 vastgesteld. Het informatiebeveiligingsbeleid hanteert de BIG als uitgangspunt en is in lijn met het algemene beleid en de relevante landelijke en Europese wet- en regelgeving. Het beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). De gemeente is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid.

Het informatiebeveiligingsbeleid gaat conform de BIG in op de volgende gebieden:

- Beveiligingsbeleid
- Organisatie van de informatiebeveiliging
- Beheer van bedrijfsmiddelen
- Personele beveiliging
- Fysieke beveiliging en beveiliging van de omgeving
- Beheer van communicatie- en bedieningsprocessen
- Toegangsbeveiliging
- Verwerving, ontwikkeling en onderhoud van informatiesystemen
- Beheer van informatiebeveiligingsincidenten
- Bedrijfscontinuïteitsbeheer
- Naleving

In het beleid staan concrete ontwikkeldoelen beschreven op het gebied van organisatorische, technische en fysieke beveiliging. Deze ontwikkeldoelen zijn verder uitgewerkt in het informatiebeveiligingsplan.

2.2 Doelstelling

De gemeente Het Hogeland stelt als doel om voor alle structurele processen in de organisatie, over 3 jaar tenminste op *volwassenheidsniveau 3* te opereren. Het volwassenheidsniveau bestaat uit 5 niveaus en geeft aan in hoeverre de organisatie in controle (niveau 5) is op het gebied van informatiebeveiliging. Volwassenheidsniveau 3 houdt in dat beheersmaatregelen zijn gedocumenteerd en op gestructureerde en geformaliseerde wijze worden uitgevoerd én aantoonbaar is. Hierbij ligt een focus op de informatiebeveiligingsprocessen bij I&A, facilitair, vastgoed, HRM en bij teams die met gevoelige informatie of (bijzondere) persoonsgegevens werken.

3. Uitgevoerde acties in 2018

3.1 Veiligheidsomissie

In 2017 hebben de BMWE - gemeenten besloten om informatieveiligheid op een hoger niveau te brengen, om het vervolgens structureel te borgen in de organisatie. Hiervoor is in 2017 de BMWE-veiligheidscommissie opgericht. In deze commissie zitten medewerkers van verscheidene vak afdelingen. De Veiligheidscommissie heeft op gemeentelijk niveau de status inzichtelijk gemaakt betreffende de zelfevaluatie informatiebeveiliging (ENSIA). Tevens heeft de Veiligheidscommissie maatregelen benoemd ter verbetering van informatiebeveiliging.

Vanaf 1 januari 2019 is de BMWE-veiligheidscommissie overgegaan naar de veiligheidscommissie Het Hogeland. De commissie houdt zich bezig met:

- Vraagstukken inzake informatiebeveiliging.
- Prioritering en planning van beveiligingsmaatregelen op basis van risicoanalyse.
- Het implementeren van beveiligingsmaatregelen.

De basis hiervoor zijn het informatiebeveiligingsbeleid, de BIG-normen en de informatiebeveiligingsaspecten van de audits en zelfevaluaties (waaronder ENSIA). Hierbij is rekening gehouden met de transformatie naar Het Hogeland. Op basis van risicoanalyse en aansluitend bij de huidige veranderingen beslist de gemeente welke verbeteracties in 2019 worden uitgevoerd. De prioriteiten voor 2019 zijn:

- Governance, rollen en verantwoordelijkheden
- Kennis, houding en gedrag ten aanzien van informatiebeveiliging
- Autorisatiemanagement
- Incidentmanagement
- Change management
- Leveranciersrelaties

3.2 AVG & ENSIA

De Algemene Verordening Gegevensbescherming (AVG), die per 25 mei 2018 door de Autoriteit Persoonsgegevens gehandhaafd wordt, en de komst van ENSIA hebben verschillende gevolgen. De BMWE - gemeenten zijn daarom in 2018 gestart om zowel privacy-activiteiten als informatiebeveiliging projectmatig op een hoger niveau te brengen en daarna structureel te borgen in de organisatie. Onder andere is de datalekprocedure vastgesteld en is er een start gemaakt met een verwerkingsregister.
Verder hebben de BMWE - gemeenten in 2017 een nulmeting uit laten voeren waarbij de kennis en het gedrag van medewerkers is gemeten ten aanzien van informatiebeveiliging. Dit heeft in 2018 geleid tot de uitvoering van workshops en onlinecursussen. Deze en andere bewustzijnsacties hadden tot doel de kennis, houding en gedrag van medewerkers ten aanzien van informatiebeveiliging te verbeteren.

4. Resultaat over 2018/2019

Zoals eerder vermeld, dient de gemeente zich te verantwoorden over BRP, PUN, DigiD, Suwinet, BAG, BGT en BRO. Dit kan met een zelfevaluatie (BRP, PNIK, BAG, BGT en BRO) of met een audit (DigiD en Suwinet). Verder toetst de gemeente haar informatieveiligheid in algemene zin via een zelfevaluatie. Om een compleet beeld te geven staan hieronder de resultaten en vervolgstappen beschreven van de BMWE - gemeenten over 2018 en de eerste 3 maanden van 2019 van gemeente Het Hogeland.

2018

4.1 Basisregistratie Personen (BRP) en Paspoort en Nederlandse Identiteitskaart (PNIK)

Bij deze zelfevaluaties worden de eigen handelingsprotocollen getoetst, waar de focus ligt op kwaliteit en daarmee integriteit (juistheid, volledigheid) en vertrouwelijkheid van informatie. Doordat de Rijksdienst voor Identiteitsgegevens (RVIG) de scores van de ENSIA niet heeft meegenomen in de BRP en PNIK-rapportage zijn hieronder de scores specifiek voor de BRP en PNIK-domeinen weergegeven. Uit de uitgevoerde zelfevaluatie hebben de BMWE - gemeenten de volgende score behaald: wat de score conform eigen protocllen handelen

Gemeente	**Score BRP** *vragenlijst per thema*	**Score PNIK**
Bedum	97,7%	100%
De Marne	97,7%	100%
Winsum	97,6%	100%
Eemsmond	95,9%	86,9%

De verbeteracties zijn bekend (variërend van procedurele tot technische acties) en zijn meegenomen in de jaarplanning van 2019.

4.2 Basisregistratie Adressen en Gebouwen (BAG)

Basisregistratie Adressen en Gebouwen (BAG) is onderdeel van het stelsel van basisregistraties in Nederland. Gemeenten zijn bronhouders van de BAG. Dat betekent dat de gemeente verantwoordelijk is voor het beheer en de kwaliteit van de gegevens van de adressen en gebouwen binnen de gemeentegrenzen. De focus ligt hier op de integriteit (juistheid, volledigheid en tijdigheid) van gegevens.
De BMWE - gemeenten heeft met een zelfevaluatie de borging van de processen, tijdigheid, volledigheid en juistheid getoetst. Vanuit het ministerie is de norm gesteld op 75% van de totaalscore. De score per gemeente is hieronder weergegeven.

Gemeente	**Score** *(norm 75%)*
Bedum	85%
De Marne	85%
Winsum	85%
Eemsmond	41%

Nadat de BAG-werkzaamheden van de gemeente Eemsmond bij het BAG-bureau van de DEAL-gemeenten waren beëindigd en zijn ondergebracht bij een extern bedrijf, zijn de processen niet goed beschreven, waardoor de opzet bestaan en werking niet getoetst konden worden. Dit heeft geresulteerd in de te lage score van de ENSIA-verantwoording.

4.3 Basisregistratie Grootschalige Topografie (BGT)

Basisregistratie Grootschalige Topografie (BGT) is een gedetailleerde digitale kaart van heel Nederland. Daarin staan onder andere gebouwen, wegen, water, spoorlijnen en groen. Door de gegevens in de BGT eenduidig op te slaan, zijn ze herbruikbaar voor alle overheidsorganisaties die deze gegevens nodig hebben. Gemeenten zijn bronhouder van deze basisregistratie en moeten er dus voor zorgen dat de gegevens van de BGT kloppen. Ook hier ligt de focus dus op de integriteit (juistheid, volledigheid en tijdigheid) van gegevens.
Ook voor de BGT hebben de voormalige BMWE - gemeenten een zelfevaluatie uitgevoerd op het gebied van borging van processen, tijdigheid, volledigheid en juistheid.
Vanuit het ministerie is de norm gesteld op 75% van de totaalscore. De score per gemeente is hieronder weergegeven.

Gemeente	**Score** *(norm 75%)*
Bedum	77%
De Marne	77%
Winsum	77%
Eemsmond	70%

In de gemeente Het Hogeland is het beheer van de BGT ondergebracht bij het team Gegevenshuis. Dit team zal zich onder meer toeleggen op het verwerken, beschikbaar stellen en bewaken van kwaliteit van basisregistratie gegevens.

Het beheer van de BGT is nog niet eerder, door de voormalige gemeenten, in eigen beheer uitgevoerd. 2019 worden benut om taken zelfstandig uit te gaan voeren en de kwaliteit van de gegevens en de bijbehorende processen op te werken naar het gewenste niveau.

4.4 Basisregistratie Ondergrond

De Basisregistratie Ondergrond (BRO) bevat gegevens over geologische en bodemkundige opbouw en, voor zover van belang voor het benutten van natuurlijke hulpbronnen in de ondergrond, ondergrondse constructies en gebruiksrechten. Het gebruik van geologische en bodemkundige gegevens vindt veelal plaats in de vorm van kaarten en profielen gebaseerd op geologische en bodemkundige modellen.

Over 2018 is het optioneel om als gemeente verantwoording af te leggen richting de toezichthouder Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Omdat de BRO relatief nieuw is en nog niet duidelijk belegd was/is in de organisatie(s), rekening houdend met drukke werkzaamheden rondom de herindeling en de keuze om wel of nog niet te verantwoorden, hebben de BMWE - gemeenten hebben ervoor gekozen zich over 2018 niet te verantwoorden over beheer van de BRO.

4.5 Betekenis uitkomsten zelfevaluaties BRP, BAG, BGT, BRO

Mede-bronhouders en andere gebruikers van basisregistraties mogen er op vertrouwen dat de gemeente haar rol in het stelsel van basisregistraties serieus oppakt. Het beoogd effect daarbij is:

- een overheid die niet naar de bekende weg vraagt;
- een overheid die klantgericht is;
- een overheid die zich niet voor de gek laat houden;
- een overheid die weet waarover ze het heeft;
- een overheid die haar zaken op orde heeft en niet meer kost dan nodig.

Op basis van de zelfevaluaties kan worden gesteld dat de gemeente nog niet op alle onderdelen op het gewenste kwaliteitsniveau zit. Dit geldt zowel voor de processen als de producten (de gegevens zelf). Zowel interne als externe gebruikers beschikken daarom nog

niet in alle gevallen over de juiste, volledige en actuele gegevens. En juiste deze kwaliteit wordt steeds belangrijker om processen, producten en diensten te ondersteunen. Daarbij worden burgers, bedrijven en instellingen ook steeds meer in stelling gebracht om zelf initiatieven te ontplooien of zelf zaken te regelen en daar voor moeten de gegevens op orde zijn.

De (maatschappelijke) impact lijkt hiermee aangetoond. Niet actuele, niet volledige of onjuiste basisregistratie gegevens kunnen leiden tot onjuiste of verkeerde besluiten. Dit geldt niet alleen voor de gemeente zelf, maar ook voor alle gebruikers van basisregistratiegegevens niet zijnde gemeente.

Voor gemeente Het Hogeland is het Team Gegevenshuis opgericht. Dit team zal zich toeleggen op het beheer van basisregistraties en richt zich onder meer op het verwerken, beschikbaar stellen en bewaken van kwaliteit van de basisregistraties gegevens. Door het beheer van basisregistraties te centraliseren en dit te zien als specialisme beoogd de gemeente de kwaliteit van de gegevens en daarmee de kwaliteit van de dienstverlening en bedrijfsvoering te verbeteren

De verbeterpunten die naar voren zijn gekomen uit de zelfevaluaties, worden meegenomen in het jaarplan van het Team Gegevenshuis en opgepakt in samenwerking met andere teams. 2019 zal dan ook in het teken staan van het opwerken naar een gewenst niveau. Om het doel te bereiken wordt in 2019 de volgende acties genomen: het op orde brengen van de basisregistraties, de bijbehorende werkprocessen en datadistributie naar interne en externe afnemers, waarover het college en de raad in 2020 wordt geïnformeerd

4.6 Informatieveiligheid gemeentebreed - Baseline Informatiebeveiliging Gemeenten (BIG)

Informatiebeveiliging is van belang voor meer dan alleen de voorgaande specifieke registraties en systemen. Dit geldt ook voor andere processen in de gemeente, vandaar dat binnen ENSIA ook gemeentebreed met een zelfevaluatie getoetst wordt of de gemeente voldoet aan de normen uit de BIG.

De conclusie uit de zelfevaluatie is dat de voormalige BMWE - gemeenten eind 2018 niet voldeden aan haar eigen informatiebeveiligingsbeleid, waar de BIG aan ten grondslag ligt.

De BMWE - gemeenten scoorde goed op het gebied van betrokkenheid van haar medewerkers ten aanzien van informatiebeveiliging. Op de volgende gebieden zijn wel maatregelen getroffen, maar is een hoger volwassenheidsniveau nodig om te komen tot een basisniveau van informatieveiligheid voor gemeente Het Hogeland:

- Governance, rollen en verantwoordelijkheden ten aanzien van informatieveiligheid
- Borging van beveiliging door middel van Plan-Do-Check-Act-cyclus
- Kennis, houding en gedrag ten aanzien van informatiebeveiliging
- Autorisatiemanagement
- Wijzigingsbeheer op IT-gebied
- Incidentenbeheer
- Fysieke beveiliging
- Bedrijfscontinuïteitsmanagement
- Systeem- en netwerkbeveiliging

2019

4.7 Digitale persoonsidentificatie (DigiD)

DigiD staat voor Digitale identiteit waarmee de burger kan inloggen op de websites van de overheid en in de zorg. De focus ligt hier op de beveiliging van het DigiD-systeem waarmee vertrouwelijkheid gewaarborgd wordt. Gemeente Het Hogeland heeft per januari 2019 een DigiD-aansluiting voor iBurgerzaken. Deze aansluiting dient jaarlijks te worden getoetst of wordt voldaan aan de beveiligingseisen. In februari jl. heeft de auditor geconstateerd dat gemeente Het Hogeland voldoet aan de gestelde normen, echter heeft de auditor wel aanbevelingen beschreven in de Assurance-rapportage. Deze aanbevelingen zijn door de gemeente geëvalueerd en in een verbeterplan opgenomen.

4.8 Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. De focus ligt hier op de vertrouwelijkheid van persoonsgegevens. Ook Suwinet dient jaarlijks te worden getoetst aan de norm, opgesteld door Bureau keteninformatiesering Werk en Inkomen. Omdat gemeente Het Hogeland vorig jaar geen entiteit was en dus geen Suwinet aansluiting had, hoeft de gemeente zich niet te verantwoorden over 2018.

5. Informatiebeveiligingsincidenten en calamiteiten 2018

5.1 Incidenten

Een incident, in het kader van incidentmanagement, is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Het doel van het incidentenproces is het inzicht krijgen in incidenten en daarvan te leren voor de toekomst. De BMWE - gemeenten hebben in 2018, met het oog op Het Hogeland gezamenlijk een begin gemaakt met het opzetten van incidentenmanagement. Dit wordt in 2019 geoptimaliseerd.

In de onderstaande tabel staan de statistieken weergegeven van de informatiebeveiligingsincidenten, die zijn geregistreerd in het jaar 2018. Naar aanleiding van de incidenten hebben de BMWE - gemeenten gezamenlijk passende organisatorische, fysieke en of technische maatregelen genomen.

Informatiebeveiligingsincidenten BMWE - gemeenten 2018	
Datalekken totaal	17
Datalekken gemeld aan AP	13
Datalekken gemeld aan betrokkenen	10
Overige informatiebeveiligingsincidenten	31

5.1.1. Datalekken

Er is sprake van een datalek wanneer onbevoegden kennis kunnen nemen van persoonsgegevens waar zij niet toe zijn geautoriseerd. In 2018 zijn er 17 datalekken geconstateerd. Deze datalekken zijn conform de geldende procedure meldplicht datalekken gemeld bij de Functionaris Gegevensbescherming en vervolgens afgehandeld en geregistreerd op het interne datalekregister.

Als zich een datalek voordoet dient er conform de procedure een afweging gemaakt te worden of het nodig is het datalek te melden aan de Autoriteit Persoonsgegevens. In sommige gevallen kan het namelijk zo zijn dat dit niet nodig is. Dit is bijvoorbeeld het geval wanneer er voor de betrokkenen geen aanmerkelijke kans is dat zich schade zal voordoen. Vervolgens dient de afweging gemaakt te worden is of ook de betrokkenen geïnformeerd dienen te worden, hiervoor geldt ook dat dit niet altijd noodzakelijk is wanneer het probleem al is opgelost of wanneer dit een onredelijke inspanning vergt van de organisatie. Deze afweging is aan de Functionaris Gegevensbescherming.

Nagenoeg alle datalekken hebben als oorzaak dat er fouten worden gemaakt in de verzending. Zo vindt er regelmatig, door verscheidene teams, een verwisseling plaats. Er wordt bijvoorbeeld een verkeerde bijlage bij een brief gedaan of een brief/e-mail wordt verkeerd geadresseerd. Enerzijds heeft dit als oorzaak dat er onzorgvuldig gewerkt wordt en anderzijds is soms de werkdruk te hoog waardoor er te spoedig gewerkt moet worden. Daarnaast worden waar mensen werken fouten gemaakt en het feit dat deze datalekken gemeld worden is in het kader van de verplichte transparantie uit de AVG een positieve ontwikkeling.

In het oog springende datalekken uit 2018 waren:

1. In de voormalige gemeente Winsum werden 136 personen aangeschreven vanwege het verlopen van hun reisproduct (paspoort, rijbewijs, e.d.). Deze brieven zijn per abuis dubbelzijdig geprint waardoor de helft van de personen geen brief ontving en de andere helft een brief met een brief aan een ander gericht op de achterkant. Qua gevoeligheid van de gegevens viel het uiteindelijk mee omdat er slechts Naam, adres, woonplaats gegevens en een documentnummer van het reisproduct op de brief vermeld waren. De procedure is destijds keurig verlopen en zowel de Autoriteit Persoonsgegevens als de betrokken zijn spoedig geïnformeerd over het incident.

2. Bij het team jeugd vroeg een ouder een inschrijfformulier voor jeugdzorg op en per ongeluk kreeg zij i.p.v. een blanco formulier een ingevuld formulier. Hierop stonden behoorlijk gevoelige gegevens als BSN en gegevens over de gezondheid van een minderjarige. Ook hier is de procedure correct nagelopen en zijn zowel Autoriteit Persoonsgegevens als betrokkenen spoedig geïnformeerd.

3. Tijdens de verhuizing in het najaar is per ongeluk een dossierkast weggegooid waar hoogstwaarschijnlijk nog allerlei gevoelige documenten in lagen. Na contact met de organisatie die de kast heeft opgehaald kon worden vastgesteld dat de kast is vernietigd, daarmee lijkt het ook waarschijnlijk dat de inhoudt daarmee ook is vernietigd. Ook hiervan is melding gemaakt bij de Autoriteit Persoonsgegevens. In dit geval is geen melding gemaakt bij de betrokkenen, simpelweg omdat niet te achterhalen viel van welke personen er persoonsgegevens achter waren gebleven in de kast.

5.1.2 Overige beveiligingsincidenten

De overige beveiligingsincidenten waren gebeurtenissen die door controle of bewust handelen geen gevolgen hebben gehad voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie of informatiesystemen. Hier kun je o.a. denken aan:

- Ontvangen phishingmails
- Foutmelding in de database van een applicatie.
- Onderbreking in het alarmsysteem met alarmcentrale.
- Valse inbraakmeldingen.
- Het niet optimaal functioneren van een noodstroom aggregaat.

5.2 Calamiteiten

Een calamiteit is een voorval dat langdurige uitval van resources en voorzieningen veroorzaakt, en daardoor tot gevolg heeft dat kritische bedrijfsprocessen van de organisatie worden verstoord en de dienstverlening aan de inwoners van Het Hogeland stagneert. Het bedrijfscontinuïteitsplan is gericht op het voorkomen van de gevolgschade. In 2019 is de gemeente van start gegaan met het inrichten van een bedrijfscontinuïteitsplan.

In 2018 hebben er 3 calamiteiten plaatsgevonden. Naar aanleiding van de calamiteiten hebben de BMWE - gemeenten passende organisatorische, fysieke en of technische maatregelen genomen. Dit om herhaling te voorkomen en om calamiteiten in de toekomst te stabiliseren, om de continuïteit van de dienstverlening te garanderen. Hieronder staan de calamiteiten kort weergegeven.

1. 07-04-2018: Ten gevolge van een defecte ventilator van de airco is de overdruk ventiel ingeschakeld van de airco. Als gevolge hiervan heeft de airco in de serverruimte niet gefunctioneerd, waardoor de tempratuur hoog op liep in de serverruimte. Een veiligheidsinstrument heeft ervoor gezorgd dat de server zichzelf heeft uitgeschakeld. De ICT-systemen hebben vervolgens een melding gegenereerd

wat is opgemerkt door team automatisering. Op 07-04-2018 is na reparatie van de airco het serverpark opnieuw opgestart. Rond het middaguur kon de dienstverlening weer worden voorgezet.

2. 07-06-2018: Tijdens het Hogeland dag waren de gemeentehuizen gesloten. Voor team automatisering was dit een gelegenheid om voorbereidende werkzaamheden te verrichten op het computernetwerk, om zowel de burgers als ook de eigen organisatie niet te hinderen. Tijdens de werkzaamheden kreeg het team rond 10:00 meerdere meldingen dat er delen van het systeem uit waren gegaan. Bij nader onderzoek op locatie bleek er een voeding van onze server defect geraakt, die vervolgens diverse aardlekschakelaren had geactiveerd waardoor er geen stroomtoevoer meer was. Gezien de gemeente deze voedingen op voorraad hebben liggen is na vervanging de stroom opnieuw ingeschakeld en het systeem weer opgestart. Na 3 uur was het systeem weer beschikbaar.

3. 29-10-2018: Rond 14:00 is ten gevolge van bouwwerkzaamheden van de nieuwe school naast het gemeentehuis in Leens een stroomkabel geraakt door een kraan. Hierdoor was er geen levering van stroom vanuit het nutsbedrijf als van de noodstroom voorzienig mogelijk. Na 8 minuten was de UPS (batterij voorziening) in de server ruimte leeg. Na de melding is er snel gereageerd om schade van de servers te beperken. Nadat de kabel was gerepareerd is er begonnen met het opnieuw opstarten van alle servers en was het netwerk rond 17:00 weer beschikbaar.

6. Meerjarenperspectief

In 2020 wordt de normenkader Baseline Informatiebeveiliging Gemeenten vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De BIO is een doorontwikkeling, ofwel een ‘update’, van de nu bestaande BIG. De werkzaamheden die voor de BIG zijn verricht zijn grotendeels in lijn met de BIO. Waar de BIG zich specifiek richt op de gemeenten, is de BIO voor toepassing op de rijksdienst, provincies, gemeenten en waterschappen.

De gemeente Het Hogeland richt zich de komende jaren op het verbeteren en borgen van de informatieveiligheid door BIO-normen en de informatiebeveiligingsaspecten van de audits en zelfevaluaties (waaronder ENSIA) in te richten, te ondersteunen en te bewaken. Op basis van risico, (lopende) projecten en beschikbare tijd en middelen wordt jaarlijks maatregelen uitgewerkt in een jaarplan. De maatregelen in het jaarplan worden aan het einde van het jaar 1x getoetst is aan opzet, bestaan en werking. Hierna wordt in het kader van de PDCA-cyclus jaarlijks de opzet, bestaan en werking getoetst.

7. Tot slot

Bij informatie is het van belang dat deze op een passende wijze wordt beveiligd. Zoals in de inleiding gesteld: hoe waardevoller en gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. 100% beveiliging bestaat echter niet en dient ook niet nagestreefd te worden. De kosten van beveiliging moeten in verhouding zijn tot de risico’s. Bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico’s, maatregelen, kosten en werkbaarheid. Hierbij kan het voorkomen dat een risico zich manifesteert, ondanks de getroffen maatregelen. Het is wel van belang dat de risico’s bekend zijn en dat een bewuste afweging is gemaakt over de te nemen risico’s.