Raadsvoorstel

Gemeente De Marne

Raadsvergadering d.d. : 28 maart 2017

Agendapunt : 8

Portefeuillehouder : dhr. F.H. Wiersma

Onderwerp : Informatiebeveiliging in BMWE

B&W besluit d.d. : 14 maart 2017

Leens, 14 maart 2017

Aan de raad.

Inleiding

Dit advies gaat over de opgave voor de naleving, toetsing en uitvoering van het informatiebeveiligingsbeleid voor de komende jaren. De aanstelling van een gezamenlijke informatiebeveiligingsfunctionaris (IBF)[1] voor de BMWE gemeenten staat centraal. Het college stelde in januari 2016 reeds de adviesnota 'Informatiebeveiliging BMW gemeenten' vast, en wenst hier nader gevolg aan te geven met onderhavig raadsvoorstel.

De BMWE-colleges hechten, in navolging van de Resolutie Informatieveiligheid[2] die eind 2013 unaniem door de ledenraad van de VNG is omarmd, belang aan een zorgvuldige en veilige uitwisseling van (persoons)gegevens die goed aansluit bij de praktijk. Hier is en wordt in geïnvesteerd door de Baseline Informatiebeveiliging Gemeenten (BIG) te implementeren. Op dit moment gebeurt dit in Eemsmond onder leiding van de informatiebeveiligingsfunctionaris en in de BMW gemeenten onder leiding van een tijdelijk ingehuurde informatiebeveiligingsfunctionaris.

Met het oog op de herindeling van de BMWE gemeenten tot één gemeente, wat de vier raden onlangs bekrachtigden, bestaat de wens onder de directies van de gemeenten het thema informatiebeveiliging onder te brengen bij één gezamenlijke informatiebeveiligingsfunctionaris. In deze adviesnota wordt die wens verder uitgewerkt.

Voorstel

- Ter dekking van de incidentele kosten € 52.218,- beschikbaar stellen voor de uitvoering van informatiebeveiliging BMWE (2017: € 26.109,- en 2018: € 26.109,-);
- Ter dekking van de structurele kosten € 14.753,30 beschikbaar stellen voor het aanstellen van de informatiebeveiligingsfunctionaris vanaf 2017 e.v.;
- De hierop betrekking hebbende begrotingswijziging vast te stellen;
- Dit besluit ter beoordeling voor te leggen aan de colleges van burgemeester en wethouders van de partnergemeenten in de herindeling;
- Dit besluit op basis van artikel 21 van de Wet ARHI voor te leggen aan Gedeputeerde Staten van de provincie Groningen ter goedkeuring.

[1] Voor dezelfde functie wordt ook veelal de Engelse term CISO gebruikt; Chief Information Security Officer

[2] https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente

Beoogd effect

Alleen met het aanstellen van één informatiebeveiligingsfunctionaris voor de BMWE gemeenten kan, in de aanloop naar de herindeling, het volgende beoogde resultaat worden behaald:

- Een veilige gegevensverwerking en –uitwisseling binnen de BMWE gemeenten door een succesvolle implementatie van de Baseline Informatiebeveiliging Gemeenten.
- Blijvende monitoring en controle op het stelsel van maatregelen met behulp van het Information Security Management System (ISMS).
- Structureel en blijvend aandacht en bewustzijn voor informatiebeveiliging (en privacy) op alle levels binnen de gemeenten.
- Integrale en professionele verantwoording conform de planning & control cyclus.

Argumenten

Beleid

De opgave op het gebied van informatiebeveiliging is binnen de BMWE-colleges al in een eerder stadium onder de aandacht geweest. Het college van Eemsmond stelde de beleidsuitgangspunten vast in april 2015 en het informatiebeveiligingsbeleid, naar verwachting, in januari 2017. Het management van Eemsmond stelde het informatiebeveiligingsbeleid reeds vast in augustus 2016.

De colleges van Bedum, De Marne en Winsum hebben het informatiebeveiligingsbeleid vastgesteld in januari/februari 2017. De beleidskaders zijn alle vier een afgeleide van het informatiebeveiligingsbeleid zoals dat is opgesteld door de Informatiebeveiligingsdienst (IBD)[3]. Dat maakt het in gezamenlijkheid uitvoeren van dit beleidsveld praktisch goed haalbaar.

In het informatiebeveiligingsplan staat nader uitgewerkt welke maatregelen er nog geïmplementeerd dienen te worden, volgens welke planning en volgordelijkheid dit geschiedt, alsmede de verantwoordelijke voor de uitvoering. De BMWE gemeenten maken bij de uitvoering reeds gebruik van hetzelfde Information Security Management System (ISMS[4]) om zodoende de maatregelen ook organisatorisch te borgen tijdens én na de implementatie.

Informatiebeveiliging en privacy zijn twee kanten van dezelfde medaille. De privacy-opgave voor de BMWE gemeenten overlapt ten dele met de opgave op het gebied van informatiebeveiliging. In december 2016 is reeds besloten door de colleges van de BMWE gemeenten tot de aanstelling van een gezamenlijke privacyfunctionaris. In dat licht bezien is het wenselijk dat de informatiebeveiligingsfunctionaris ook de ‘scope’ BMWE krijgt in plaats van een deel daarvan. Op deze manier wordt de samenwerking ten volle benut, zowel tussen de gemeenten als tussen beide functionarissen.

Tot slot is het hier van belang te benadrukken dat een informatiebeveiligingsfunctionaris zijn/haar werk doet vanuit een onafhankelijke positie (buiten de lijn c.q. het primaire proces). De persoon moet in staat zijn onafhankelijk te rapporteren en te adviseren over informatiebeveiliging aan het management en het bestuur.

Uitvoering

De coördinatie van de uitvoering van het informatiebeveiligingsbeleid ligt in handen van de informatiebeveiligingsfunctionaris. Alhoewel de verantwoordelijkheid voor de uitvoering van de maatregelen belegd is bij het lijnmanagement, vervult de informatiebeveiligingsfunctionaris een belangrijke rol in de implementatie en het beheer van de BIG maatregelen. Het is de persoon die de BIG implementatie gemeentebreed coördineert en hierover rapporteert aan het management en het bestuur.

[3] De IBD is een initiatief van KING en de VNG

[4] Een ISMS is een management proces voor de besturing van, en verantwoording over informatiebeveiliging

Formatie implementatie
Bij het bepalen van de benodigde formatie voor de implementatie onder leiding van de informatiebeveiligingsfunctionaris en ondersteuner wordt uitgegaan van de vuistregel zoals die wordt aangereikt door de Informatiebeveiligingsdienst: het implementeren van BIG maatregelen kost gemiddeld 8u per maatregel voor de informatiebeveiligingsfunctionaris(sen). De uren van de vakafdelingen zijn niet meegenomen in deze berekening (zie daarvoor 'Adviesnota BMW - uitvoering informatiebeveiliging'). Grofweg hebben de BMWE gemeenten ieder 200 BIG maatregelen te implementeren over een periode van 2 jaar. Vier gemeenten maal 100 maatregelen per jaar vertaalt zich naar 400x8u=3200u per jaar. Afgerond komt dit neer op 2 FTE. Na de implementatiefase zal dit geleidelijk afnemen naar 1 FTE. In bijlage 1 ziet u op welke taken de ondersteuner ondersteuning biedt aan de informatiebeveiligingsfunctionaris.

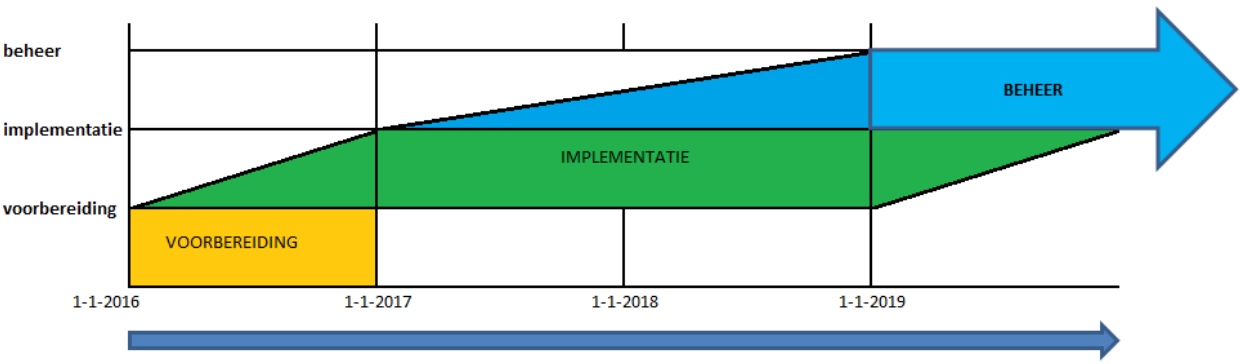
De winsten van het gezamenlijk implementeren van de BIG vertalen zich op korte termijn (tot aan de herindeling) nog niet terug om de volgende drie redenen:

1) De herindeling zal op z'n vroegst per 1 januari 2019 geeffectueerd zijn wat betekent dat de informatiebeveiligingsfunctionaris tot aan dat moment werkt voor vier afzonderlijke gemeenten met een zekere mate van inefficiëntie.
2) De implementatie van de BIG brengt veel uitvoerend werk met zich mee dat ook ten dele door de informatiebeveiligingsfunctionaris wordt uitgevoerd. Daarnaast coördineert hij/zij de implementatie van de maatregelen waarvan de uitvoering bij een vakafdeling belegd is. Daarbij is de uitgangssituatie per gemeente verschillend.
3) Binnen de BMW gemeenten is het ISMS pas recent geïmplementeerd waardoor de werkwijze in de komende periode moet worden uitgelijnd met de procedures uit dit ISMS. Daartoe zijn de eerste stappen gezet, maar deze nieuwe werkwijze zorgt echter wel voor een extra urenbelasting in de eerste jaren.

Het is daarom raadzaam de informatiebeveiligingsfunctionaris voor BMWE in ieder geval in de implementatiefase van de BIG te laten ondersteunen door een andere functionaris. De kosten voor de informatiebeveiligingsfunctionaris zijn daarom structureel terwijl de kosten voor de ondersteuner incidenteel zijn (voor een periode van tenminste twee jaar).

BMW
Om het verloop van de BIG implementatie als project overzichtelijk te houden treft u hieronder een grafische weergave aan. Begin 2016 hebben de colleges van de BMW gemeenten ingestemd met de adviesnota 'Informatiebeveiliging BMW-gemeenten'. De vier aldaar benoemde fasen komen als volgt overeen met onderstaande figuur.

Voorbereiding	fase 1 (inventariseren en analyseren) en fase 2 (afwegen en vaststellen)
Implementatie	fase 3 (implementeren)
Beheer	fase 4 (monitoren en controleren)



Eemsmond
Het verloop van de BIG implementatie bij de gemeente Eemsmond is anders van bij de BMW gemeenten. Als één van de eerste stappen van de BIG implementatie is in Eemsmond de functie van informatiebeveiligingsfunctionaris beschreven met als belangrijkste bevoegdheid om op elke plek binnen de organisatie gevraagd en ongevraagd
onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. De Medewerkers gegevensbeheer 1 zijn in die functie benoemd.
Uit een onlangs uitgevoerde formatieberekening van het team gegevensbeheer is duidelijk geworden dat het aantal taken van dit team vier formatieplaatsen vereist, terwijl de formatie uit twee fte's bestaat. Een uitbreiding van formatie is daarom zeer gewenst.
De beleidsuitgangspunten zijn door het bestuur vastgesteld, de GAP-analyse is uitgevoerd en de Verklaring van Toepasselijkheid (VVT) is voorlopig vastgesteld. Het Informatiebeveiligingsbeleid is door het MT akkoord bevonden om ter vaststelling aan burgemeester en wethouders te worden voorgelegd. Verder zijn er reeds diverse procedures vastgesteld die een hoger niveau van informatiebeveiliging garanderen.
De ingestelde beveiligingscommissie werkt thans aan de voorbereiding van meerdere maatregelen in het kader van de BIG. Eén van de maatregelen die in Eemsmond hoog op de agenda staat is de uitvoering van het iBewustzijnsprogramma dat in oktober van dit jaar is gestart en in januari een vervolg krijgt in de vorm van een eLearningstraject.

Herindeling
Het aanstellen van één gezamenlijke informatiebeveiligingsfunctionaris voor de BMWE gemeenten sorteert uitstekend voor op de herindeling. Immers, de vier gemeenten dienen aan exact dezelfde eisen te voldoen en door in de aanloop naar de herindeling al één informatiebeveiligingsfunctionaris te hebben worden beleid, processen en, waar mogelijk, applicaties al zoveel mogelijk uitgelijnd zodat er één werkwijze gaat ontstaan. Kortom, een gezamenlijke informatiebeveiligingsfunctionaris versterkt, en geeft (alvast) concreet invulling aan de steeds nauwere samenwerking met als stip aan de horizon de herindeling.

Uitvoering

Financiën
In de begrotingen 2017 van de BMWE gemeenten is vooralsnog geen post opgenomen voor de invulling van de informatiebeveiligingsfunctionaris. Binnen Eemsmond wordt op dit moment de functie informatiebeveiligingsfunctionaris ingevuld door twee medewerkers van de afdeling gegevensbeheer. Om die reden is er in de begroting van Eemsmond eveneens geen post opgenomen voor de informatiebeveiligingsfunctionaris.

Binnen BMWE wordt gebruik gemaakt van het functiewaarderingssysteem HR21[5] van de VNG. P&O van BMW heeft de functiebeschrijving van de informatiebeveiligingsfunctionaris voor inpassing in het HR21 model voorgelegd aan het bureau BuitenhekPlus/Leeuwendaal. Op basis van hun advies en verdere inpassing in het HR21 model bedragen de formatiekosten maximaal € 73.000 voor de informatiebeveiligingsfunctionaris en maximaal € 60.000 voor de ondersteuner. Beide bedragen zijn inclusief werkgeverslasten en voor de BMWE gemeenten samen. In de gemeentelijke begrotingen 2017 is geen dekking opgenomen voor deze beide functies.
Hieronder volgt een overzicht van de te ramen bedragen voor de formatie van beide functionarissen. De verdeelsleutel is gebaseerd op het aantal inwoners per 1-1-2016 (Bedum 20,87%, De Marne 20,21%, Winsum 27,28%, Eemsmond 31,64%).

Omdat de ondersteuner tijdens de implementatiefase de informatiebeveiligingsfunctionaris bijstaat, voor een periode van tenminste twee jaar, zijn de kosten respectievelijk incidenteel en structureel.

[5] http://www.hr21.nl/

Gemeente	Geraamde kosten	
	Incidenteel (cumulatief voor 2 jaar)	*Structureel (jaarlijks)*
Bedum	€ 25.044,-	€ 15.235,10
De Marne	€ 24.252,-	€ 14.753,30
Winsum	€ 32.736,-	€ 19.914,40
Eemsmond	€ 37.968,-	€ 23.097,20
Totale kosten:	**€ 120.000,-**	**€ 73.000,-**

Daarnaast heeft de informatiebeveiligingsfunctionaris een eigen budget nodig om goed invulling te geven aan zijn/haar verantwoordelijkheden. Uit dit budget worden zaken als bewustwording, penetratietesten, audits en tooling bekostigd. Dit bedrag zal na 1-1-2019 aanzienlijk lager zijn omdat de verantwoordingslast op dat moment van vier naar één gemeente teruggaat. Na afronding van de implementatie wordt heroverwogen of de informatiebeveiligingsfunctionaris een eigen budget dient te behouden, of dat ook dit budget wordt ondergebracht bij de diverse vakafdelingen. Tot slot zijn aan het eerder genoemde ISMS van Segment ook jaarlijkse kosten verbonden.

De kosten voor het ISMS en het budget informatiebeveiliging worden, net als de formatiekosten voor de ondersteuner, gezien als incidentele kosten. Na de herindeling moet opnieuw worden vastgesteld of er een contractuele verplichting moet worden aangegaan met Segment en wie de budgethouder wordt van het budget informatiebeveiliging alsmede de hoogte van het budget zelf. Er is gekozen om voor nu dekking te vragen tot aan de herindeling.

De dekking voor de informatiebeveiligingsfunctionaris is structureel omdat deze (nieuwe) functionaris vanzelfsprekend ook na de herindeling zal blijven bestaan.

Kosten informatiebeveiliging	BMWE	Bedum	De Marne	Winsum	Eemsmond
- ISMS Segment	€ 39.600,-	€ 9.900,-	€ 9.900,-	€ 9.900,-	€ 9.900,-
- Budget informatiebeveiliging	€ 120.000,-	€ 30.000,-	€ 30.000,-	€ 30.000,-	€ 30.000,-
- Formatiekosten ondersteuner	€ 120.000,-	€ 25.044,-	€ 24.252,-	€ 32.736,-	€ 37.968,-
Totale incidentele kosten in 2017 en 2018 (cumulatief)	**€ 279.600,-**	**€ 64.944,-**	**€ 64.152,-**	**€ 72.636,-**	**€ 77.868,-**
Aanwezig dekking*	€ 45.702,-	€ 11.934,-	€ 11.934,-	€ 11.934,-	€ 9.900,-
Nog te ramen incidentele kosten	**€ 233.898,-**	**€ 53.010,-**	**€ 52.218,-**	**€ 60.702,-**	**€ 67.968,-**
- Formatiekosten informatiebeveiligingsfunctionaris	€ 73.000,-	€ 15.235,10	€ 14.753,30	€ 19.914,40	€ 23.097,20
Totale structurele kosten 2017 e.v.	**€ 73.000,-**	**€ 15.235,10**	**€ 14.753,30**	**€ 19.914,40**	**€ 23.097,20**
Aanwezige dekking	€ 0,-	€ 0,-	€ 0,-	€ 0,-	€ 0,-
Nog te ramen structurele kosten	**€ 73.000,-**	**€ 15.235,10**	**€ 14.753,30**	**€ 19.914,40**	**€ 23.097,20**

* Deze post is reeds opgenomen in de begroting 2017, ter dekking van de contractuele verplichting met Segment, voor levering van het ISMS. Deze verplichting loopt af in 2018.

Het college van Burgemeester en Wethouders van de gemeente De Marne,

de gemeentesecretaris, **de burgemeester,**

mevr. drs. J.C.H.G.M. Bottema **dhr. F.H. Wiersma**