Vergadering:	23 februari 2016
Agendanummer:	7
Status:	Opiniërend
Portefeuillehouder:	M.A.P. Michels
Behandelend ambtenaar	A. Pettinga (I&A-BMW), 0595-447723/421167
E-mail:	gemeente@winsum.nl (t.a.v. André Pettinga)

Aan de gemeenteraad,

Onderwerp:
Uitvoering Informatiebeveiliging

Voorgestelde besluit:
- Een incidenteel bedrag van €22.633,- beschikbaar te stellen voor de uitvoering de informatiebeveiliging in 2016;
- Deze kosten in 2016 te dekken door een onttrekking aan de post onvoorzien tot ditzelfde bedrag;
- Een voorstel voor de structurele kosten en dekking voor de jaren 2017 en volgende mee te nemen in de Kadernota 2016.

Samenvatting:
De gemeente Winsum hecht belang aan een betrouwbare en veilige informatievoorziening. De behoefte aan verbetering komt niet alleen van de gemeente zelf, maar is ook ingegeven door actuele ontwikkelingen:

- Het ministerie Sociale Zaken en Werk (SZW) doet onderzoek naar het gebruik van Suwinet (de keten van werk en inkomen). Dit onderzoek raakt het toezicht op de informatiebeveiliging in een groot deel van de organisatie;
- De accountant heeft opmerkingen gemaakt over de "Betrouwbaarheid en continuïteit van de automatiseringsomgeving". Er moet een plan van aanpak komen;
- De decentralisaties van het Sociale Domein resulteren in de nodige opslag en uitwisseling van persoonsgegevens bij en door gemeenten. Een belangrijk aspect daarvan is de borging van de privacy. Bij de privacy gaat het er enerzijds om welke gegevens uitgewisseld/gekoppeld mogen worden, anderzijds dient de verwerking van deze gegevens ook veilig te gebeuren. Door middel van goede informatiebeveiliging wordt de privacy van burgers beter geborgd.

- De Europese Unie is komt met een nieuwe Algemene Verordening Gegevensbescherming (AVG). Vooruitlopend op de AVG wordt de Meldplicht Datalekken vanaf 1 januari 2016 ingevoerd.

Om de informatiebeveiliging te verbeteren heeft het college de adviesnota "Informatiebeveiliging BMW-gemeenten" vastgesteld. Dit in navolging van de colleges van De Marne en Bedum. Om de adviesnota uit voeren is budget nodig. Incidenteel voor 2016 wordt de raad middels dit voorstel gevraagd een bedrag van €22.633,- beschikbaar te stellen. Onderzoek moet uitwijzen wat de structurele kosten na 2016 zullen zijn. De dekking voor deze kosten worden meegenomen in de begroting 2017.

Probleem:
Om de gemeentelijke taken uit te voeren is het nodig dat de informatiebeveiliging op orde is. Aan de ene kant mogen burgers er op vertrouwen dat de gemeenten adequate maatregelen neemt om de veiligheid van gegevens te waarborgen. Aan de andere kant krijgt de gemeente te maken met verdergaande digitalisering van voorzieningen en een toenemende ketensamenwerking. De gemeente moet meer dan voorheen laten zien dat de informatiebeveiliging gemeentebreed op orde is. Wanneer de gemeente de informatiebeveiliging niet op orde heeft, of onvoldoende kan aantonen dat de informatiebeveiliging op orde is, loopt de gemeente onder meer de volgende risico's;

- De gemeente kan worden afgesloten van landelijke voorzieningen zoals bijv. Basis Registratie Personen (BRP), DigiD, Suwinet. Met als gevolg dat de gemeente taken niet meer kan uitvoeren;
- Boetes als gevolg van de Meldplicht Datalekken per 1 januari 2016;
- Negatief accountants rapport;
- Imagoschade.

Wat willen we bereiken
Informatiebeveiliging is per eind 2018:

- een logisch onderdeel van de werkprocessen, diensten en producten;
- bestuur, management en medewerkers zijn zich voldoende bewust van de nut en noodzaak van informatieveiligheid;
- als standaard onderdeel opgenomen in de Planning & Control cyclus;
- de basis informatiebeveiliging van de gemeenten is op orde.

Hoe gaan we dat doen

- Het informatiebeveiligingsbeleid vaststellen op basis van de Baseline Informatiebeveiliging Nederlandse gemeenten (BIG);
- Invoeren Information Security Management Systeem (ISMS);
- Het aanstellen van één informatiebeveiligingsfunctionaris voor de gemeente Bedum, de Marne & Winsum;
- Budget beschikbaar stellen voor informatiebeveiliging (incidenteel en structureel).

Inleiding:

Informatieveiligheid gaat over de kwaliteit van de informatievoorziening en wordt voornamelijk gedefinieerd in termen van **beschikbaarheid, integriteit** en **vertrouwelijkheid.** Om de gegevens en informatiesystemen waarover de gemeente beschikt is het noodzakelijk een informatiebeveiligingsbeleid te hebben. We beschouwen informatieveiligheid als het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de organisatie.

Dit informatiebeveiligingsbeleid richt zich niet alleen op de geautomatiseerde gegevensverwerking door middel van ICT-voorzieningen, maar uitdrukkelijk ook op de bescherming van niet geautomatiseerde gegevens (zoals fysieke documenten) en bedrijfseigendommen.

Informatieveiligheid is een onderwerp waarbij techniek en mentaliteit de twee pijlers zijn. Met name, het voelen van eigen verantwoordelijkheid vanuit de gemeentelijke organisatie, vormt hierbij de sleutel tot succes. Het is een fragiel evenwicht tussen ‘willen’ (eigen verantwoordelijkheid, zelfregulering en bewustwording) en ‘moeten’ (wet- en regelgeving).

Vanuit de VNG worden gemeenten voortdurend gewezen op hun verantwoordelijkheid ten aanzien van informatieveiligheid. Om gemeenten te ondersteunen is op initiatief van de VNG de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) ontwikkeld.
Het doel van de invoering van de BIG is informatieveiligheid te bevorderen en een professionelere bedrijfsvoering te realiseren.

Wat is de BIG?
De BIG is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD), in samenwerking met de Vereniging Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). Hierbij is de Baseline Informatiebeveiliging Rijksdienst (BIR), eveneens een variant van de ISO 27001-norm, als basis genomen en is een vertaalslag gemaakt naar een richtlijn voor de gemeentelijke markt. De BIG is een zelfreguleringsinstrument en bestaat uit een set van beveiligingsmaatregelen, inclusief fysieke beveiliging, waarmee gemeenten op een vrij eenvoudige manier een basis beveiligingsniveau kunnen halen.

Wanneer iedere gemeente deze BIG implementeert en naleeft, is een basisbeveiligingsniveau gerealiseerd. De hoofddoelen van de BIG zijn:
- Een goed basisbeveiligingsniveau voor gemeenten neer leggen;
- Gemeenten op een vergelijkbare manier efficiënt laten werken met informatiebeveiliging;
- Gemeenten een hulpmiddel bieden om aan alle eisen op het gebied van informatiebeveiliging te kunnen voldoen;
- Informatiebeveiliging een integraal onderdeel te laten zijn van de bedrijfsvoering en van de keuzes die het management maakt.

BMW-Gemeenten en De BIG
De BMW-gemeenten zijn drie kleine organisaties die slechts beperkte mogelijkheden hebben om informatieveiligheid afdoende te regelen. Enerzijds is dat bijvoorbeeld zichtbaar bij de vormgeving van noodzakelijke functiescheiding; anderzijds is daarvoor niet voldoende tijd beschikbaar gegeven de andere taken.

In de huidige situatie is het zo dat de functionele afdelingen de verplichte audits/zelfevaluaties uitvoeren. Dat is niet optimaal omdat informatieveiligheid zich niet beperkt tot de eigen afdeling. Voor een bredere toepassing conform de BIG zijn de betreffende afdelingen onvoldoende toegerust op hun taak (hetzij in beschikbare tijd, hetzij in aanwezige kennis).

Het is de insteek van de BIG dat informatieveiligheid vanuit een centraalpunt voor de hele organisatie wordt gecoördineerd. Bundeling van de krachten bevordert het beter en sneller doorlopen van de audits en zelfevaluaties door de afzonderlijke organisatieonderdelen en doet de informatieveiligheid toenemen.

Wettelijk- of beleidskader:
De relevante wettelijke beleidskaders voor het informatiebeveiligingsbeleid en –plan zijn:

- Baseline Informatiebeveiliging Gemeenten
- Wet Basisregistratie Personen (BPR)
- Wet Basisregistratie Adressen & Gebouwen (BAG)
- Wet Structuur Uitvoeringsorganisatie Werk & Inkomen (Suwi)
- Participatiewet
- Wet Maatschappelijke Ondersteuning (WMO) 2015
- Jeugdwet
- Archiefwet
- Wet algemene bepalingen Burgerservicenummer
- Wet Bescherming Persoonsgegevens (WBP)
- Wet Computercriminaliteit
- Privacywetgeving

Advies / Voorstel:

- Een bedrag van € 22.633,- beschikbaar te stellen voor de uitvoering de informatiebeveiliging in 2016. Waarbij, samen met de gemeenten De Marne en Bedum (BMW) gefaseerd wordt toegewerkt naar een structurele en organisatie brede inbedding van informatiebeveiliging in 2018. De BIG wordt hierbij als
  richtlijn gebruikt. De hogere kosten in 2016 kunnen worden gedekt door een
  onttrekking aan de post onvoorzien.
- De dekking voor structurele lasten mee te nemen in de Kadernota 2016.

Financiën

1. voor 2016 is €22.633,- nodig om te kunnen starten met de uitvoering. Het betreft hier om de kosten voor aanschaf en beheer ISMS en inhuur/tijdelijke aanstelling Informatiebeveiligingsfunctionaris/ projectleider Informatiebeveiliging voor de BMW-gemeenten;
2. vanaf 2017 bedragen de structurele kosten voor het onderhoud van het ISMS €5.967;
3. Het streven is om één Informatiebeveiligingsfunctionaris voor de BMW-gemeenten aan te stellen. Kosten voor de gemeente Winsum bedragen circa € 11.666,- E.a. is afhankelijk van de benodigde betrekkingsomvang, functie-inhoud en zwaarte. Een definitieve krediet aanvraag volgt na vaststelling van het informatiebeveiligingsbeleid 2e helft 2016.

Voorgesteld wordt om de lasten voor 2016 te dekken door middel van een onttrekking aan de post onvoorzien. De dekking van structurele lasten mee te nemen in de Kadernota 2016.

Uitvoering:
Uitvoering vindt volgens onderstaande fasering plaats;

Fase 1 Inventariseren/Analyseren (december 2015 – 3e kwartaal 2016)
Onder verantwoordelijkheid van de afdeling I&A-BMW voert de projectleider samen met de vertegenwoordigers, van de drie gemeenten, een risicoanalyse uit. Uit deze analyse blijkt welke risico's de gemeente loopt en welke maatregelen er nodig zijn.

Fase 2 Afwegen/Vaststellen (3e kwartaal 2016 – 4e kwartaal 2016)
Nadat de risico's zijn afgewogen en de te nemen maatregelen zijn benoemd, wordt e.a. vastgelegd in een informatiebeveiligingsplan. In een advies worden de risico's en de te nemen maatregelen voorgelegd aan het bestuur. Tevens wordt op basis van een verklaring van toepasselijkheid bepaald welke maatregelen wel en welke niet (en waarom niet) uit de BIG worden overgenomen. Hierdoor zal het bestuur zijn verantwoordelijkheid kunnen nemen.

Fase 3 Implementeren (Vanaf eind 4e kwartaal 2016)
Als alle te nemen maatregelen in beeld zijn, wordt gestart met de implementatie. De Informatiebeveiligingsfunctionaris gaat aan de slag met de implementatie van de maatregelen.

Fase 4 Monitoren en controleren (Loopt vanaf 2017 parallel met P&C-cyclus)
Jaarlijks controleert de Informatiebeveiligingsfunctionaris of de informatiebeveiliging van de gemeente nog voldoet aan de BIG en of de maatregelen nog actueel zijn.

Evaluatie:
Na uitvoering van fase 1 en 2 vindt de eerste evaluatie plaats. Vanuit deze evaluatie volgt een voorstel die er voor moet zorgen dat de benodigde maatregelen vanuit het informatiebeveiligingsbeleid worden uitgevoerd. Vervolgens vindt er rapportage plaats volgens de P&C-cyclus en zal worden ondergebracht bij het hoofdstuk "bedrijfsvoering".

Relatie met:
Het onderdeel privacy wordt momenteel opgepakt vanuit het sociaal domein. Hierbij is aandacht voor beleid, werkprocessen, trainingen en een organisatie brede borging. Door de nieuwe taken in het sociaal domein en nieuwe wetgeving (Meldplicht datalekken, Europese privacy verordening), is structurele aandacht voor privacy nodig.

Informatiebeveiliging en privacy hebben veel raakvlakken, maar zijn inhoudelijk toch anders. Informatiebeveiliging is met name gericht op de harde kant, de (technische) beveiliging. Privacy legt de nadruk op de zachte kant, het gedrag van medewerkers. Deze twee kunnen niet zonder elkaar en zijn als het ware twee kanten van dezelfde medaille.

Het is van belang om een goede verbinding te hebben tussen privacy- en informatiebeveiligingsbeleid. Daar waar mogelijk wordt al gezamenlijk gewerkt aan beleid, bewustwording en borging. Met name de rol die de informatiebeveiligingsfunctionaris kan gaan spelen op het gebied van privacy beleid is daarbij nog onderwerp van gesprek. Uitgewerkte voorstellen hieromtrent volgen in de loop van 2016.

Achterliggende documenten:
Ter inzage de adviesnota “Informatiebeveiliging BMW-gemeenten”

Burgemeester en wethouders van Winsum,

M.A.P. Michels, burgemeester

drs. R.J. Bolt, secretaris

Agendanummer:
Vergadering:

De raad van de gemeente Winsum;

gezien het voorstel van burgemeester en wethouders;

gelet op het bepaalde in:
de relevante wet- en regelgeving

b e s l u i t :

- Een bedrag van € 22.633,- beschikbaar te stellen voor de uitvoering de informatiebeveiliging in 2016;
- Dit bedrag te dekken door een onttrekking aan de post onvoorzien tot ditzelfde bedrag;
- De dekking voor de structurele lasten mee te nemen in de Kadernota 2016.

Aldus vastgesteld door de raad van de gemeente Winsum in zijn openbare vergadering van

De raad voornoemd,

voorzitter,

griffier,