gemeente Gemert-Bakel

Adviesnota aan de raad

Raadsvergadering:
22 mei 2019
Agendanummer:
Afdeling/werkterrein: griffie
Zaaknr: -2019

Onderwerp: Aanbevelingen Rekenkamercommissie Informatieveiligheid

---

Aan de raad

Samenvatting

In deze adviesnota worden de aanbevelingen uit het Rekenkamercommissieonderzoek gerapporteerd inzake informatieveiligheid. Het onderzoek is uitgevoerd door bureau Secura in opdracht van de gezamenlijke Rekenkamercommissie Gemert-Bakel/Laarbeek.
De taken, bevoegdheden en verantwoordelijkheden van met name colleges van B&W op het gebied van informatiebeheer en informatiebeveiliging, nemen sterk toe. In de praktijk blijkt dat, voor het kunnen realiseren en waarborgen van informatieveiligheid, deskundigheid nodig is en vanuit het college van B&W specifiek aandacht vraagt. En daarbij komt dan ook nog het effectief worden van de geactualiseerde Europese privacyregelgeving per 25 mei 2018, de AVG. Dit is complexe materie met voor burgers en gemeenten belangrijke regels en handvatten over hoe om te gaan met het verwerken van persoonsgegevens en voorzien van stevige boetebepalingen. Een forse uitdaging. Hoe nu bevestigd te krijgen dat de gemeente voldoende is voorbereid op deze bedreigingen, relevante aandachtspunten helder zijn en het college van B&W voldoende handvat heeft voor het aangaan van deze uitdagingen? Daarom heeft de Rekenkamercommissie het initiatief genomen een onderzoek te laten uitvoeren naar de wijze waarop de betreffende colleges grip hebben op informatieveiligheid en het voldoen aan de actuele privacy regelgeving.

Dit onderwerp komt aan de orde in:

Raadsvergadering d.d. 22 mei 2019

Dit onderwerp is aan de orde geweest in:

De Commissie Financiën en Bestuur op 7 mei jl.

Inleiding

De dienstverlening van gemeenten aan burgers en bedrijven is in hoge mate afhankelijk van geautomatiseerde informatiesystemen. Gemeenten krijgen steeds meer taken toebedeeld waar in de uitvoering intensief gebruik wordt gemaakt van informatiesystemen en daarin opgeslagen gegevens. Hierbij vervult de gemeente ook vaak taken als onderdeel van een keten van organisaties en is daarmee afhankelijk van andere organisaties en externe databases en vormt zelf ook een cruciale schakel in het realiseren van een voldoende beveiligingsniveau over de keten heen. Dat de bedreigingen toenemen, en de kans dat deze plaatsvinden stijgt, blijkt uit recente incidenten en onderzoeken zoals die van de IBD (Informatiebeveiligingsdienst als onderdeel van de VNG) in 2018.
De taken, bevoegdheden en verantwoordelijkheden van met name de colleges van B&W op het gebied van informatiebeheer en informatiebeveiliging, nemen sterk toe. In de praktijk blijkt dat, voor het kunnen realiseren en waarborgen van informatieveiligheid, deskundigheid nodig is en vanuit het college van B&W specifiek aandacht vraagt. En daarbij komt dan ook nog het effectief worden van de geactualiseerde Europese privacyregelgeving per 25 mei 2018, de AVG. Dit is complexe materie met voor burgers en gemeenten belangrijke regels en handvatten over hoe om te gaan met het verwerken van persoonsgegevens en voorzien van stevige boetebepalingen. Een

forse uitdaging. Hoe nu bevestigd te krijgen dat de gemeente voldoende is voorbereid op deze bedreigingen, relevante aandachtspunten helder zijn en het college van B&W voldoende handvat heeft voor het aangaan van deze uitdagingen?

Onderwerp van onderzoek
De Rekenkamercommissie heeft daarom het initiatief genomen een onderzoek te laten uitvoeren naar de wijze waarop de betreffende colleges grip hebben op informatieveiligheid en het voldoen aan de actuele privacy regelgeving. Zij heeft daarvoor twee centrale onderzoeksvragen geformuleerd:
1. In hoeverre is de (digitale) informatiebeveiliging van de gemeenten Gemert-Bakel en Laarbeek in de praktijk op orde?
2. Zijn beide gemeenten alert en actief genoeg om de informatiebeveiliging oplossingsgericht te verbeteren en kan de raad ervan op aan dat het goed gaat?

In overleg met de gemeenten is het onderzoek opgedeeld in een aantal fasen waarbij de uitkomsten van een eerdere fase bepalen wat de inhoud en aanpak van het opvolgende onderzoek zal zijn voor zover dat nog relevant is. Secura B.V. is de opdracht gegeven dit onderzoek uit te voeren. De eerste fase betreft een vooronderzoek. Dit vooronderzoek is niet gericht op het (met zekerheid) afgeven van een oordeel over de kwaliteit van de informatiebeveiliging maar heeft als doelstelling inzicht te krijgen in de wijze waarop het college van B&W een organisatie heeft ingericht, medewerkers heeft betrokken en technische en/of procedurele maatregelen heeft getroffen reeds, als onderdeel van de planning & control cyclus, ingerichte verantwoordingen en uitgevoerde audits. Oftewel de mate waarin de gemeenten nu al beschikken over een ingerichte organisatie voor het realiseren van informatieveiligheid en het kunnen voldoen aan de AVG.

Deze rapportage geeft de uitkomsten van het vooronderzoek verricht door Secura in de periode van 24 september tot en met 2 november 2018.

Opzet van het onderzoek
Voor dit vooronderzoek zijn de volgende onderzoeksvragen uitgewerkt op basis van de centrale (overkoepelende) vragen. De geformuleerde subvragen zijn:
1. Voldoet de gemeente Gemert-Bakel aan de ‘normen’?
2. Hoe is de organisatorische inrichting van de informatiebeveiliging?
3. Welke beveiligingschecks worden zoal uitgevoerd?
4. Welke maatregelen zijn getroffen rond back-ups?
5. Hoe vindt de opvolging plaats bij gesignaleerde tekortkomingen?
6. Hoe is de monitoring ingericht door de raad?

Hierbij is nadrukkelijk bepaald dat er binnen het onderzoek geen technische testen plaatsvinden maar de onderzoeker enkel inventariseert welke maatregelen de gemeenten zelf hebben genomen en welk informatie over de kwaliteit van de inrichting daarvan al voorhanden is.

Na het opleveren van de rapportages door het onderzoeksbureau is ambtelijk wederhoor gevolgd om feitelijke onjuistheden en onvolledigheden te voorkomen. Daarna zijn conclusies geformuleerd en beide colleges van burgemeester en wethouders om een bestuurlijke reactie gevraagd. De bestuurlijke reactie van Gemert-Bakel is in het rapport opgenomen.

Procedure
De gezamenlijke Rekenkamercommissie heeft het rapport voor inhoudelijke behandeling aangeboden, waarna het rapport is geagendeerd in de vergadering van de gemeenteraad d.d. 22 mei 2019 en voorbereidend in de vergadering van de raadscommissie Financiën en Bestuur d.d. 7 mei 2019. De voorzitter van de Rekenkamercommissie zal, ondersteund door één van de onderzoekers, bij de raadscommissievergadering aanwezig zijn om eventuele vragen te beantwoorden en de aanbevelingen toe te lichten.

Aanbevelingen
Uw raad wordt voorgesteld de aanbevelingen tegen de achtergrond van het onderzoeksrapport over te nemen.

1. Het nadrukkelijk advies is een afhankelijkheden- en kwetsbaarheden analyse uit te laten voeren om vast te stellen welke systemen kritiek zijn en specifieke beveiligingsmaatregelen vergen om de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid te kunnen garanderen. Dit is tevens noodzakelijk voor het kunnen formuleren van adequaat (actueel) informatiebeveiligingsbeleid. Met de uitkomsten van de analyse, en het geformuleerde beleid in de hand, kan de gemeente ook haar huidige continuïteitsmaatregelen evalueren in relatie tot de beschikbaarheidseisen.
2. Richt een risicomanagementproces in voor het identificeren, analyseren en evalueren van risico's en voor het bepalen van de risicohouding: accepteren of maatregelen treffen. Dit dient een continu proces te zijn. Maak hierbij o.a. gebruik van de best practices van de IBD en andere gemeenten, betrek hierin ook de eisen uit de BIO (Baseline informatiebeveiliging overheid) die als opvolger van de BIG de minimumnorm voor de komende jaren zal zijn.
3. Leg op zeer korte termijn het informatiebeveiligingsbeleid vast dat is geactualiseerd op het nieuwe informatiebeleid en met de uitkomsten van de nog uit te voeren risicoanalyse. Neem daarin de aandachtspunten uit dit vooronderzoek mee.
4. Laat een nieuwe nulmeting informatiebeveiliging uitvoeren aan de hand van het nieuwe beleid om vast te stellen welke risico's en aandachtspunten aanwezig zijn. Stel daaropvolgend een goed implementatieplan op en leg de overwegingen rond de selectie van te nemen maatregelen vast.
5. Leg procedures rond kritieke beheertaken als wijzigingenbeheer, toegangsbeheer en incidentenbeheer vast. Overweeg de uitvoering van periodieke audits op de werking van deze beheersmaatregelen. Deels kan hier gebruik worden gemaakt van de uitkomsten van de audit voor de jaarrekeningcontrole en de DigiD assessment.
6. Completeer de bewerkersovereenkomsten met leveranciers en besteed daarbij aandacht aan de mogelijkheid onderzoeken te doen bij de leveranciers, of beter nog: het ontvangen van (onafhankelijke) Assurance rapporten over de kwaliteit van beveiligingsmaatregelen bij die leveranciers (opzet, bestaan en werking).
7. Vorm inhoudelijk een beeld van de huidige status van de implementatie van de AVG maatregelen. Mogelijk dat een nulmeting AVG hierbij een goede eerste aanzet kan zijn.

Planning/uitvoering
Voor implementatie van aanbevelingen is een vervolg nodig. De raad kan het college uitnodigen om een voorstel tot nadere aanpak voor te leggen.

Ter inzage gelegde stukken
Rapport van de Rekenkamercommissie en aanbiedingsbrief.

Ontwerpbesluit gemeenteraad
De raad wordt voorgesteld:

1. de aanbevelingen over te nemen;
2. het college op te dragen dat een voorstel tot nadere aanpak wordt voorgelegd in het vierde kwartaal van 2019, met de uitzondering dat aan aanbeveling 3 uiterlijk 1 oktober 2019 is voldaan.

Gemert, 22 mei 2019

de griffier,

P.G.J.M. van Boxtel