Rekenkamer Den Haag

Retouradres: Postbus 19157, 2500 CD Den Haag

Commissie Bestuur

Uw kenmerk

Ons kenmerk
RK/2015.02
RIS 280510

Doorkiesnummer
070-3532048

E-mailadres
rekenkamer@denhaag.nl

Aantal bijlagen

Datum
2 februari 2015

Onderwerp: Beleidskader informatieveiligheid 2015-2018

Geachte voorzitter,

De rekenkamer heeft het voornemen in het kader van de nazorg bij uitgevoerde onderzoeken de raad te ondersteunen bij het vaststellen in hoeverre en op welke wijze het college invulling geeft aan raadsbesluiten naar aanleiding van rekenkamerrapporten. In deze brief gaan wij in op het aan u toegezonden beleidskader informatieveiligheid 2015-2018.

Op 20 januari 2015 verzond het college van burgemeester en wethouders aan de commissie bestuur het beleidskader informatieveiligheid 2015-2018 (RIS 280309). In de begeleidende brief geeft het college aan dat met het beleidskader invulling wordt gegeven aan het onderdeel van het raadsbesluit van 16 oktober 2014 naar aanleiding van het rekenkameronderzoek Digitale Veiligheid (RIS 273602), waarin het college wordt opgedragen om in 2014 een kader voor informatieveiligheid op te stellen.

Naar ons oordeel komt het college slechts ten dele tegemoet aan het betreffende onderdeel van het raadsbesluit. Onder punt II besluit de raad ten eerste (dictum II.1) het college op te dragen ‘een conceptkader voor informatieveiligheid op te stellen en ter besluitvorming voor te leggen aan de raad’.

De status van het aan u toegezonden beleidskader komt niet tegemoet aan de opdracht in het raadsbesluit. In plaats van een conceptkader ter besluitvorming, krijgt u een vastgesteld kader ter informatie voorgelegd. Het college heeft met zijn instemming met toezending van het beleidskader aan de voorzitter van de raadscommissie tevens het beleid vastgesteld.

De overige sub-punten van punt II van het dictum zijn inhoudelijker van aard, afgezien van de opdracht de raad binnen een half jaar te informeren over de aanpak van de punten uit het raadsbesluit. Wij lopen de punten van het dictum II hieronder in volgorde na.[1]

[1] Punt I van het dictum is het besluit van de raad in te stemmen met aanbevelingen en conclusies van de rekenkamer.

Dictum II gelet op het rapport van de rekenkamer 'Digitale Veiligheid' in navolging van de aanbevelingen van de rekenkamer het college op te dragen:

1. Nog in 2014 een conceptkader voor informatiebeveiliging op te stellen en voor te leggen aan de raad ter besluitvorming.

Ad 1. Naast de opmerking ten aanzien van de status van het beleidskader informatiebeveiliging (zie hierboven) het volgende. In de aanbevelingen bij haar rapport geeft de rekenkamer aan dat in een kader voor informatiebeveiliging een afweging gemaakt moet worden tussen veiligheidsrisico's, te nemen maatregelen en de werkbaarheid van ICT voorzieningen, in relatie tot de beschikbare middelen (rekenkamerrapport p. 19). Het college neemt in het beleidskader een risicoclassificatie van verschillende categorieën informatie op (beleidskader p. 10). Er wordt hierbij echter niet een afweging gemaakt tussen deze risico's en de te nemen maatregelen in relatie tot de beschikbare middelen. Het beleidskader geeft onder paragraaf 7.0 (p. 17) wel aan dat invulling van het beleidskader uitbreiding van capaciteit en een investering in hulpmiddelen betekent. Dit wordt echter niet concreet gemaakt.

2. Tenminste één maal per jaar de gemeentelijke informatiebeveiliging door een externe partij te laten testen op kwetsbaarheden en dit in de planning en controlcyclus op te nemen.

Ad 2. Het college geeft in het beleidskader aan elk jaar een test uit te gaan voeren (beleidskader p. 7). Niet aangegeven wordt of dit opgenomen wordt in de planning & controlcyclus. Het is daardoor niet duidelijk of de gemeenteraad (in de planning & controlcyclus) geïnformeerd gaat worden over de uitkomsten van deze tests.

3. Het gemeentelijk netwerk te gaan monitoren op verdachte activiteiten en een calamiteitenplan op te stellen voor ingrijpen bij aanvallen op de informatiebeveiliging.

Ad 3. Het college geeft in het beleidskader aan gestart te zijn met continue monitoring en een 'draaiboek' op te gaan stellen voor het reageren op aanvallen op de informatiebeveiliging (beleidskader p. 20). Daarmee wordt volgens de rekenkamer deels invulling gegeven aan dit punt van het besluit. In de aanbevelingen geven wij aan dat het calamiteitenplan onderdeel zou moeten zijn van het beleidskader informatieveiligheid. Door de nu gekozen uitwerking is het calamiteitenplan geen onderwerp van besluitvorming door de raad.

4. De benodigde bestuurlijke inbedding van informatiebeveiliging tot stand te brengen door de verantwoordelijkheid hiervoor expliciet en als apart onderwerp bij een portefeuillehouder te beleggen.

Ad 4. In het beleidskader is de bestuurlijke inbedding niet opgenomen. Daarmee lijkt de situatie te blijven bestaan dat informatieveiligheid bestuurlijk een deelonderwerp is van het ICT beleid en onder de verantwoordelijkheid van één en dezelfde wethouder blijft vallen. Wij zijn van oordeel dat informatieveiligheid verder strekt dan ICT en daaraan dus niet ondergeschikt kan zijn en dat dit tot uiting moet komen door het onderwerp apart en expliciet te beleggen bij een portefeuillehouder.

5. In te zetten op een proces van bewustwording, cultuurverandering en bekwaamheid ten aanzien van informatiebeveiliging dat verder gaat dan vrijblijvend informeren.

Ad 5. Het beleidskader gaat in op de verantwoordelijkheid van medewerkers bij informatieveiligheid en gaat concreet in op te nemen maatregelen om kennis, bewustzijn en naleving van regels hierover te verbeteren (bijvoorbeeld door het verplicht maken van cursussen en opnemen van het onderwerp in de gesprekscyclus, p. 14 van het beleidskader).

6. Het onderwerp informatiebeveiliging als afzonderlijk onderwerp op te nemen in de planning en controlcyclus (begroting en programmarekening) en daarbij de raad minimaal jaarlijks te informeren over resultaten en stand van zaken.

Ad 6. In het beleidskader is sprake van een planning & controlcyclus waarover de wethouder periodiek wordt geïnformeerd (beleidskader p. 7). In het beleidskader is opgenomen dat aan de gemeenteraad in het jaarverslag verantwoording wordt afgelegd over de informatieveiligheid (beleidskader p. 7). Niet aangegeven wordt of informatieveiligheid ook als afzonderlijk onderwerp wordt opgenomen in de begroting en op welke manier de raad wordt geïnformeerd.

Wij hopen met deze brief een bijdrage te leveren aan de behandeling van het beleidskader informatieveiligheid.

Met vriendelijke groet,

Watze de Boer
voorzitter