

Onderwerp Raadsstuk bij RKC Rapport Verantwoordelijkheid voor Veiligheid - Onderzoek naar Informatiebeveiliging	
Nummer	2019/143523
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	Rekenkamercommissie
Auteur	Mulders, I.
Telefoonnummer	023-5114885
Email	imulders@haarlem.nl
Kernboodschap	De rekenkamercommissie (RKC) heeft onderzoek gedaan naar de informatiebeveiliging van de gemeente Haarlem. Onvoldoende beveiliging kan grote gevolgen hebben voor de werkprocessen van de gemeente en de gegevens van inwoners die de gemeente beheert. Uit het rapport blijkt dat de informatiebeveiliging niet op orde is. Een groot deel van het onderzoek is in opdracht van de RKC uitgevoerd door Hoffmann Cybersecurity. Zij hebben het informatiebeveiligingsbeleid en een deel van de informatiesystemen van de gemeente onderzocht. Het rapport bevat de bevindingen van dit onderzoek, conclusies en aanbevelingen om de informatiebeveiliging van de gemeente Haarlem te verbeteren.
Behandelveorstel voor commissie	De commissie Bestuur wordt verzocht advies te geven aan de raad over het voorstel van de rekenkamercommissie in paragraaf 2 en over de wijze van agendering van het raadsstuk in de raadsvergadering. De rekenkamercommissie heeft besloten tot het opleggen van geheimhouding aan de raad op grond art. 25, tweede lid van Gemeentewet <u>op de bijlage</u> van het Rapport Verantwoordelijkheid voor Veiligheid vanwege de bescherming van de economische en financiële belangen van de gemeente en het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden als bedoeld in artikel 10, tweede lid aanhef en onder b en g van de Wet openbaarheid van bestuur.
Besluit RKC d.d. 14 februari	1. Tot het opleggen van geheimhouding aan de raad op grond artikel 25, tweede lid van Gemeentewet op de bijlage van het Rapport Verantwoordelijkheid voor Veiligheid vanwege de bescherming van de economische en financiële belangen van de gemeente en het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden als bedoeld in artikel 10, tweede lid aanhef en onder b en g van de Wet openbaarheid van bestuur, welke geheimhouding vanwege de aard van dit document voor onbepaalde duur wordt opgelegd.

	2. De raad voor te stellen de opgelegde geheimhouding in de eerstvolgende raadsvergadering te bekrachtigen.
Besluit Raad d.d. (wordt ingevuld door de griffie)	De raad der gemeente Haarlem, Gelezen het voorstel van de rekenkamercommissie, Besluit: 1. De aanbevelingen van de rekenkamercommissie zoals geformuleerd in paragraaf 2 van dit raadsstuk over te nemen en als opdracht neer te leggen bij het college. 2. De geheimhouding door de rekenkamercommissie aan de raad opgelegd op grond art. 25, tweede lid van Gemeentewet op de bijlage van het Rapport Verantwoordelijkheid voor Veiligheid te bekrachtigen. De geheimhouding wordt vanwege de aard van dit document voor onbepaalde duur opgelegd. de griffier, de voorzitter,

1. Inleiding

Vanwege de inherent vertrouwelijke aard van het onderwerp informatiebeveiliging is de voor de gemeenteraad beschikbare informatie hierover beperkt. En door het technische karakter zijn bovendien kennis over en inzicht in deze materie gering. Desondanks moet de gemeenteraad voor de uitoefening van zijn drie rollen goed geïnformeerd zijn over de stand van zaken en de risico's. De rekenkamercommissie wil de raad dit inzicht verschaffen.

Een tweede aanleiding voor het onderzoek is de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018.

Hoffmann Cybersecurity heeft in opdracht van de rekenkamercommissie onderzoek gedaan.

naar de veiligheid van persoonsgegevens en andere informatie bij de gemeente Haarlem.

Daarbij luidde de centrale vraag: *Is de informatiebeveiliging van de gemeente Haarlem op orde?*

Op basis van de bevindingen uit het onderzoek komt de RKC tot 3 conclusies en aanbevelingen.

De reactie van het college op het onderzoek en de aanbevelingen is in het rapport opgenomen.

2. Voorstel aan de raad

De rekenkamercommissie stelt de raad voor de volgende aanbevelingen over te nemen en als opdracht bij het college neer te leggen:



1. Vóór eind 2019 daadkrachtige en volledige implementatie van het eigen informatiebeveiligingsbeleid te realiseren door onder meer:
 - a. Een nieuwe gap-analyse uit te voeren om in beeld te krijgen welke, volgens relevante wet- en regelgeving en het eigen beleid voorgeschreven, maatregelen nog niet zijn geïmplementeerd. Hieruit wordt ook zichtbaar wat er sinds 2014 al is gerealiseerd.
 - b. Het informatiebeveiligingsbeleid zo spoedig mogelijk, doch uiterlijk in het eerste kwartaal van 2019 opnieuw te laten vaststellen door het college.
 - c. Naar aanleiding van bovenstaande punten op korte termijn het budget, de capaciteit en de benodigde competenties die beschikbaar zijn voor informatiebeveiliging te heroverwegen.
 - d. Hiervoor een plan van aanpak met tijdpad en verantwoordelijken op te stellen en de voortgang van de implementatie te laten bewaken door de IT-auditor.
 - e. Over de implementatie en uitvoering van het beleid dient structureel verantwoordingsinformatie te worden opgesteld en ook de aansturing van het beleid door directie en bestuur moet traceerbaar zijn.
2. De informatiesystemen weerbaarder te maken tegen cybercrime door:
 - a. De resterende kwetsbaarheden uit de penetratietesten overeenkomstig de aanbevelingen van Hoffmann te verhelpen.
 - b. Vóór de zomer van 2019 een hertest te laten uitvoeren op de gevonden kwetsbaarheden en de gemeenteraad hierover te informeren en deze periodiek en met verschillende invalshoeken te herhalen.
3. De raadsinformatie over informatiebeveiliging te verbeteren door naast de verplichte paragraaf en de ENSIA verklaring:
 - a. De gemeenteraad middels een (zo nodig geheime) nota inhoudelijk te informeren over de mate van compliancy aan wet en regelgeving en het eigen beleid aan de hand van een jaarlijkse samenvatting met duiding van de scores op de ENSIA-zelfevaluatievragenlijst.
 - b. Aan de hand van een objectieve maatstaf (bijvoorbeeld het volwassenheidsniveau) te rapporteren over de ontwikkeling van de verschillende onderdelen van de informatievoorziening, waaronder informatiebeveiliging.

3. Beoogd resultaat

Een verbetering van de informatieveiligheid bij de gemeente Haarlem en een over dit onderwerp beter geïnformeerde gemeenteraad.

4. Argumenten

1. Informatiebeveiliging is essentieel om de continuïteit van de werkprocessen van de gemeente te kunnen borgen.

In de primaire processen en de bedrijfsvoering van gemeenten wordt steeds intensiever gebruik gemaakt van ICT. Het gebruik van ICT en het beheer van gegevens (in databanken) in combinatie met de decentralisering van overheidstaken van het rijk naar gemeenten en het werken in regie

betekenen dat er steeds meer gegevens tussen verschillende organisaties en systemen worden uitgewisseld.

2 Informatiebeveiliging is van groot belang voor de bescherming van de grote hoeveelheid (persoons-)gegevens van inwoners die de gemeente Haarlem beheert.

De waarborg van de veiligheid van persoonsgegevens van burgers is van groot publiek belang. Als persoonsgegevens in verkeerde handen komen, kunnen bijvoorbeeld vertrouwelijke gegevens openbaar worden of kan identiteitsfraude worden gepleegd. Dit heeft potentieel grote gevolgen voor de privacy van burgers en voor het imago van de overheid.

3 Uit het onderzoek blijkt dat het informatiebeveiligingsbeleid onvoldoende is geïmplementeerd en dat er bij de informatiesystemen sprake is van (ernstige) kwetsbaarheden. De gemeente is niet 'in control'.

Het informatiebeveiligingsbeleid van de gemeente is op zich van goede kwaliteit maar is onvoldoende geïmplementeerd. Bij het testen van de informatiesystemen zijn verschillende (ernstige) kwetsbaarheden aan het licht gekomen.

4 Uit het onderzoek blijkt ook dat de raad slechts summier over de stand van de informatiebeveiliging is geïnformeerd.

Hoewel informatiebeveiliging tot de bedrijfsvoering wordt gerekend en daarmee een college-bevoegdheid is, vormt het grote maatschappelijke belang voldoende aanleiding voor de raad om de vinger goed aan de pols te houden. Het college is verplicht de raad hierover te informeren.

5 Het college herkent het beeld en heeft op onderdelen direct actie ondernomen.

Uit opvolging van de eerste aanbeveling moet blijken of er aanvullend budget nodig is.

Het college geeft niet aan alle aanbevelingen te zullen opvolgen.

5. Risico's en kanttekeningen

1 Uit de bestuurlijke reactie op het rapport maakt de RKC op dat het urgentiebesef is toegenomen. Of met de aangekondigde maatregelen de capaciteit en het budget voldoende zijn moet blijken uit de aanbevolen GAP-analyse.

2. Door de snelle ontwikkelingen op het terrein van de cybercrime en de grote risico's van onvoldoende beveiliging is hoge prioriteit en flexibiliteit in de inzet gewenst. Niet de reeds aanwezige, maar de benodigde capaciteit zou richtinggevend moeten zijn.

3. Het niet of vertraagd opvolgen van de aanbevelingen vergroot de risico's. Het is voor de raad van belang hierover goed geïnformeerd te blijven.

6. Uitvoering

- Het college zal uitvoering moeten geven aan de aanbevelingen.



- *De overgenomen aanbevelingen worden geregistreerd en de opvolging zal door de rekenkamercommissie worden gemonitord. De raad zal hierover worden geïnformeerd.*

7. Bijlagen

- Bijlage 1 RKC Rapport Verantwoordelijkheid voor Veiligheid – Onderzoek naar Informatiebeveiliging 2019/144202
- Bijlage 2 **GEHEIM** Bijlage van het RKC Rapport - Rapportage onderzoek informatiebeveiliging gemeente Haarlem, Hoffmann Cybersecurity 2019/135999
- Bijlage 3 RKC Besluit tot opleggen geheimhouding op de bijlage van het RKC rapport Verantwoordelijkheid voor Veiligheid, Onderzoek naar Informatiebeveiliging 2019/130460