Gemeente Roosendaal

Toelichting raadsvoorstel aan de raad van de gemeente Roosendaal

Samenvatting
De Rekenkamer West-Brabant (hierna: rekenkamer) is door de gemeente Roosendaal ingesteld om onderzoek te doen naar doelmatigheid, doeltreffendheid en rechtmatigheid van het door het gemeentebestuur gevoerde bestuur.

In 2018 heeft de rekenkamer een onderzoek uitgevoerd naar de informatieveiligheid en privacy binnen de gemeente Roosendaal. Middels dit raadsvoorstel wordt het onderzoeksrapport aan u als gemeenteraad van Roosendaal aangeboden en wordt u het volgende voorgesteld:

1. Het onderzoeksrapport van de Rekenkamer West-Brabant getiteld 'Onderzoek informatieveiligheid en privacy' te onderschrijven en in te stemmen met de in het rapport opgenomen conclusies en aanbevelingen;
2. Het college op te dragen de aanbevelingen nader op te pakken en de raad hierover periodiek te informeren.

Aanleiding
Gemeenten investeren steeds meer in digitale dienstverlening om diensten te verlenen en met hun doelgroepen in contact te komen. Gemeenten worden daardoor steeds afhankelijker van een ongestoorde werking van hun ICT-voorzieningen om klanten goed en tijdig van dienst te kunnen zijn. Wanneer deze voorzieningen uitvallen en/of data (onbedoeld) in verkeerde handen komen, leidt dit mogelijk tot financiële - en imagoschade en mogelijk tot een boete van de toezichthouder.

De onderwerpen informatieveiligheid en privacy hebben in toenemende mate aandacht van de gemeente Roosendaal. In 2018 heeft de gemeenteraad van Roosendaal de onderwerpen informatieveiligheid en privacy als onderzoeksthema aangemerkt en de rekenkamer gevraagd hierna onderzoek te laten uitvoeren. In het onderzoeksrapport staat een beschrijving van de onderzoeksvragen en -aanpak en worden de bevindingen, conclusies en aanbevelingen gerapporteerd.

Aanpak
Het onderzoek is uitgevoerd langs een tweetal sporen:

<u>SPOOR 1 De ambtelijke organisatie en wettelijke kaders</u>
Dit spoor bestond uit drie delen, namelijk het bewustzijn van informatieveiligheid op de werkvloer, de kaders en wettelijke verplichtingen en de risico's op dit vlak. Hiervoor is de zogenaamde QuickScan BIG ingezet. De BIG - Baseline Informatieveiligheid Gemeenten - is het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van gemeentelijke informatie(systemen) bevordert. De BIG is daarmee een richtlijn die een totaalpakket aan informatie, beveiligingscontroles en -maatregelen omvat, die voor iedere gemeente noodzakelijk is om te implementeren. Middels de QuickScan is onderzocht of en hoe gemeente Roosendaal zich aan deze richtlijn houdt.

<u>SPOOR 2 De bestuurlijke context en wisselwerking daarbinnen</u>
In dit spoor is de bestuurlijke context en de wisselwerking tussen raad en college nader onderzocht. Er is aandacht besteed aan kaderstelling, communicatie, afstemming en sturing met betrekking tot het informatieveiligheidsbeleid.

Aanbevelingen
In het rapport is per spoor duidelijk gemaakt welke stappen er zijn ondernomen in het onderzoek en welke bevindingen en conclusies dit heeft opgeleverd. De bevindingen en de conclusies leiden vervolgens tot meerdere aanbevelingen en deze zijn als volgt geformuleerd in het rapport:

SPOOR 1

- We stellen voor dat de gemeente zich conformeert aan de BIG-norm door wel per systeem of proces een expliciete risicoanalyse uit te voeren. Hierdoor ontstaat een completer beeld van de risico's.
- Stel een procedure vast voor het rapporteren van beveiligingsgebeurtenissen en borg deze in de organisatie. Hierin wordt rekening gehouden met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident. Daarnaast is het wenselijk dat er een stuurgroep ingericht wordt die rapportages over informatiebeveiligingsincidenten beoordeelt.
- Maak met de Gemeenschappelijke Regeling-ICT West-Brabant West specifieke afspraken over informatiebeveiliging (aanvullend op het gezamenlijke informatiebeveiligingsbeleid) en leg deze vast in de dienstverleningsovereenkomst. Zorg dat hier ook afspraken over periodieke rapportages in opgenomen zijn.
- Verbeter de registratie van bedrijfsmiddelen door ook de registratie van desktops te actualiseren.
- Het is belangrijk om te borgen dat tijdelijke medewerkers, die via externe partijen zoals uitzendbureaus worden ingezet bij de gemeente Roosendaal ook bekend gemaakt worden met de huisregels (specifiek rondom informatieveiligheid) bij de gemeente. Dit kan door bijvoorbeeld met enige regelmaat een steekproef te houden.
- Tot op heden is niet planmatig aandacht besteed aan het actueel houden van de kennis van medewerkers op het gebied van informatiebeveiliging. Dit staat op de planning van de gemeente voor najaar 2018. Het planmatig bewust maken van medewerkers en actueel houden van hun kennis is niet een eenmalige activiteit en dient regelmatig aandacht te krijgen.
- Maak een overzicht van kwetsbare functies binnen de gemeente zodat de gemeente in staat is daarop gericht maatregelen te nemen om de risico's voor deze functies te beperken.
- Maak aanvullende afspraken rondom reparaties van laptops en telefoons, zodat informatiebeveiligingsrisico's geborgd zijn.
- Zorg dat de informatiebeveiligingseisen voor systemen en de daarbij behorende acceptatiecriteria goed gedefinieerd en gedocumenteerd zijn, zodat bij de acceptatie van nieuwe versies van systemen hier rekening mee gehouden wordt.
- Zorg dat er periodiek gerapporteerd wordt aan het management over de status van informatiebeveiliging binnen de gemeente.
- Zorg dat er voor de cruciale processen Data Privacy Impact Analyses worden uitgevoerd.

SPOOR 2

- De gemeenteraad wordt te weinig frequent en inhoudelijk te summier ingelicht door de ambtelijke organisatie. Het is belangrijk om afspraken (tussen college en raad) te maken over de manier waarop en de frequentie waarmee het college en de ambtelijke organisatie de gemeenteraad kan informeren, zodat zowel de informatiebehoefte van de gemeenteraad vervuld wordt, als dat er voldoende rekening gehouden wordt met de bezwaren (zoals vertrouwelijkheid) van de ambtelijke organisatie.

- De beantwoording van schriftelijke vragen wordt als summier ervaren. Omdat het onderwerp inhoudelijk soms ingewikkeld is, zou het college er goed aan doen om extra uitleg te geven bij de beantwoording van vragen.
- Het organiseren van een informerende themabijeenkomst kan helpen om de kennis van de raad met betrekking tot informatieveiligheid en privacy te verbreden. De bijeenkomst zou specifiek over de gemeente Roosendaal moeten gaan ('waarom doen we bepaalde dingen, welke afwegingen zijn gemaakt, hoe verloopt de samenwerking met ICT West-Brabant, waar zijn zij voor verantwoordelijk en zijn wij dan wel in control, etc.), met een laag instapniveau (bijvoorbeeld in de vorm van een kort inleidend college over het normenkader BIG) en daarna een verdieping op de specifieke situatie van de gemeente. Daarin zouden volgens de deelnemers maatregelen van de gemeente en de wisselwerking tussen raad en college aan bod moeten komen, met een toelichting op hoe bepaalde keuzes gemaakt worden door het college. Bijvoorbeeld het wel of niet delen van rapportages met de raad en de openbaarheid daarvan.

Overall: met het gebruik van een ISMS is de gemeente op weg om informatieveiligheid goed te borgen. ISMS staat voor Information Security Management System en is een managementsysteem voor informatiebeveiliging. Het is niet een tool, maar een manier van werken om (vertrouwelijke) informatie beter te beveiligen en dit dient geïntegreerd te worden in de werkprocessen.
De uitdaging zit in het goed bijhouden hiervan zodat men grip heeft op alle risico's en maatregelen. Daarnaast is informatieveiligheid een kwestie van volharding. Het is meer dan naar aanleiding van een rapport actie ondernemen, want het vraagt om constante aandacht en hier zo transparant mogelijk over te communiceren richting de gemeenteraad.

Financiën
Er zijn aan het voorliggende rapport geen directe financiële risico's of consequenties verbonden.

Communicatie
De rekenkamer heeft het college uitgenodigd een reactie te geven op het rapport en de daarin opgenomen conclusies en aanbevelingen. De reactie van het college is integraal opgenomen in het rapport.

Op woensdag 13 maart jl. heeft de rekenkamer aan raadsleden een toelichting gegeven op het onderzoeksrapport en aansluitend was er een themabijeenkomst over informatieveiligheid en privacy. Beide presentaties zijn te raadplegen in de vergaderapp GO (zie themabijeenkomst 13 maart 2019).