gemeente
Zoetermeer

> Retouradres Postbus 15, 2700 AA Zoetermeer

Rekenkamercommissie Zoetermeer
t.a.v. mevrouw E.J. Wallet-Boers
Afdeling Griffie
Postbus 15
2700 AA ZOETERMEER

Bezoekadres
Markt 10
2711 CZ Zoetermeer

Postadres
Postbus 15
2700 AA Zoetermeer

Telefoon 14 079
www.zoetermeer.nl

Datum
31 januari 2018

Uw kenmerk

Ons kenmerk
06 37204764

Bijlagen
1

Onderwerp: Reactie van het college op de conclusies en aanbevelingen van het rekenkameronderzoek Informatiebeveiliging

Geachte mevrouw Wallet-Boers,

Hierbij ontvangt u de bestuurlijk reactie op het rekenkameronderzoek Informatiebeveiliging.

Burgemeester en wethouders van Zoetermeer,
de secretaris, de burgemeester,

drs. H.M.M. Koek Ch.B. Aptroot

Bijlage: Bestuurlijke reactie onderzoek rekenkamercommissie Zoetermeer Informatiebeveiliging

Bestuurlijke reactie

Conclusies

Conclusie 1
Het huidige informatiebeveiligingsbeleid is opgezet volgens de normen van de Baseline Informatiebeveiliging Gemeenten (BIG). Het integrale beleid is door het college van B&W vastgesteld en publiek gemaakt. Het beleid is risico-gebaseerd. De governance is in termen van draagvlak bij de top van de organisatie goed geregeld; dat wordt door een visitatiecommissie van de VNG bevestigd. De chief information officer (CIO) maakt deel uit van de directie. Opmerkelijk is dat de CIO tevens chief information security officer (CISO) is, een functie die het directielid deelt met de coördinator informatiebeveiliging.

Reactie college:
De rol van CIO is bij het Informatie Management Overleg (IMO) belegd. De CISO-rol is belegd bij één van de directeuren. Deze directeur is tevens voorzitter van het IMO. De CISO deelt de functie niet met de coördinator informatiebeveiliging, maar de coördinator vervult wel een aantal taken in opdracht van de CISO, hierbij legt de coördinator verantwoording af aan de CISO. Er is geen sprake van delen van de functie, de coördinator legt altijd verantwoording af aan de CISO.

De overige onderdelen van deze conclusie deelt het College volledig.

Conclusie 2
Het informatiebeveiligingsbeleid van Zoetermeer is conform de BIG voor drie jaar vastgelegd; de huidige periode loopt eind 2017 af. Er is nog geen nieuw beleid geformuleerd. De verwachting is dat het huidige beleid, met een check op aanpassingen, nog met een jaar zal worden verlengd.

Reactie college:
Het college deelt deze conclusie. Het beleid zit dan ook momenteel in het besluitvormingsproces om voor 2 jaar verlengd te worden. Dit zal worden afgerond in het eerste kwartaal van 2018.

Conclusie 3
In afwijking van de BIG is er tot nu toe geen continuïteitsplan opgesteld. Wel zijn er diverse maatregelen genomen om de continuïteit te borgen, waaronder het compartimenteren van het interne netwerk en het inrichten van twee interne datacenters. Back-ups worden dagelijks gemaakt en ondergebracht bij een externe partij.

Reactie college:
Het college deelt de mening, in lijn met de conclusie uit het onderzoek, dat er nog geen integraal continuïteitsplan is opgesteld. Wel bestaan er continuïteitsplannen voor delen van de informatiehuishouding. In 2018 zal een gemeente breed continuïteitsplan worden opgeteld.

Conclusie 4
De gemeente voert periodiek beveiligingsaudits en zelfevaluaties uit. Eventuele verbeteracties die daaruit voortkomen, worden door de vakafdelingen opgepakt. De gemeenteraad krijgt niet gerapporteerd over de controles op informatiebeveiliging, behalve de ICT audit van de accountant die in het accountantsverslag is opgenomen.

Reactie college:
Het college deelt deze conclusie deels. De gemeenteraad wordt ook geïnformeerd wanneer het gaat om de jaarlijkse zelfevaluaties zoals bijvoorbeeld Basisregistratie Personen (BRP). Met ingang van 2018 wordt via ENSIA jaarlijks verantwoording afgelegd over informatieveiligheid gebaseerd op de BIG. Het gaat hier dan om de informatieveiligheid van Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

Aan de raad

Aanbeveling 1

Geef het college opdracht om op korte termijn – nog in de eerste helft van 2018 – een geactualiseerd informatiebeveiligingsbeleid voor de periode 2018-2020 op te stellen en vast te stellen. De wereld van ICT en cybercrime ontwikkelt zich zo dynamisch dat het verstandig is om het informatiebeveiligingsbeleid ten minste eenmaal in de drie jaar goed tegen het licht te houden, zoals ook in de BIG is vastgelegd. De BIG zal over enige jaren met de Baseline Informatiebeveiliging Rijksoverheid (BIR) opgaan in de Baseline Informatiebeveiliging Overheid (BIO). Dit is geen reden om in Zoetermeer te wachten met het herijken van het informatiebeveiligingsbeleid.

Reactie College:

Op basis van Informatie vanuit de Informatie Beveiligingsdienst (IBD) is aangegeven dat de planning vooralsnog is dat dat de werkgroep die werkt aan een combinatie van alle overheidsbaselines er met alle overheidslagen begin 2018 uit zal zijn en dat de BIO aan de BALV (ledenvergadering VNG) wordt aangeboden in het najaar van 2018 waarbij hij zal ingaan per 1 januari 2019. Op basis van deze informatie is dan ook het besluitvormingsproces in gang gezet om het beleid met twee jaar te verlengen. Dit al naar verwachting worden afgerond in het eerste kwartaal van 2018.

Aanbeveling 2

Spreek met het college van B&W af op welke wijze en met welke regelmaat de raad in het vervolg over informatiebeveiliging geïnformeerd wil worden.
Informatiebeveiliging vormt een cruciale succesfactor in de dienstverlening van de gemeente. Informatiebeveiliging roept ook dilemma's op die een inhoudelijke bespreking in en met de raad verdienen. Het zijn nu vooral incidenten die vragen bij de raad oproepen; meer structurele aandacht voor het onderwerp is gepast gelet op de controlerende taak van de raad.

Reactie College:

Het college deelt deze aanbeveling. Het college zal hiertoe aan de Raad een voorstel doen inzake op welke wijze en met welke regelmaat de raad geïnformeerd kan worden. Dit voorstel zal in het eerste kwartaal van 2018 worden opgeleverd.

Aanbeveling 3

Positioneer de CISO zelfstandig en onafhankelijk van de lijn, met een directe verbinding met de gemeentesecretaris. De CISO heeft een van de lijn onafhankelijke taak met betrekking tot informatiebeveiliging. De CISO-functie is nu belegd bij twee personen, een directielid (tevens CIO) en de coördinator informatiebeveiliging. Beide betrokkenen zijn ervan overtuigd dat deze constructie goed werkt. Desondanks moet gerekend worden met het risico dat, bij conflicterende belangen tussen de lijn en informatiebeveiliging, benodigde maatregelen om informatiebeveiliging te borgen niet, onvoldoende of te laat genomen worden. Met het oog daarop vindt de rekenkamercommissie het beter om de functie van CISO zelfstandig te positioneren.

Reactie College:

De CISO deelt de functie niet met de coördinator informatiebeveiliging, de coördinator vervult wel in opdracht van de CISO een aantal taken, hierbij legt de coördinator verantwoording af aan de CISO. Er is geen sprake van delen van de functie, de coördinator legt altijd verantwoording af aan de CISO.

De rol van de CISO ligt nu inderdaad in de lijn. Het College meent dat dit voor meerdere soortgelijke rollen nu ook het geval is en dat er daar het risico op conflicterende belangen tussen lijn en de rol ook mogelijk is maar dat de kans hierop zo klein is dat er vooralsnog geen reden is om de positionering te heroverwegen. Wel meent het College dat elk risico op belangenverstrengeling moet worden vermeden en zal zich daarom hier nader op beraden. Het College zal daarom een nieuwe afweging maken en die delen met de Raad in het eerste kwartaal van 2018.

Aanbeveling 4

Blijf investeren in het bewustzijn van digitale bedreigingen en het veilig omgaan met ICT onder middenmanagement en medewerkers en scherp de (handhaving van de) regels voor inschakeling van derden aan. De gemeente onderneemt sinds 2016 diverse activiteiten om medewerkers individueel en in teamverband te wijzen op digitale risico's. De menselijke factor vraagt voortdurende aandacht, ook door gerichte trainingen in veilig omgaan met ICT. Daarnaast is het nodig om de naleving van contracten met derden op het punt van informatiebeveiliging scherper te monitoren.