Rekenkamercommissie
ZOETERMEER

Bestuurlijke nota

Informatiebeveiliging

December 2017

Quick scan Informatiebeveiliging gemeente Zoetermeer

Conclusies en aanbevelingen

Gemeenten beheren veel persoonlijke en gevoelige data van burgers. En de dienstverlening verloopt steeds meer digitaal. Tegelijkertijd neemt de dreiging van cybercrime toe. Dit onderstreept het belang van een goede informatiebeveiliging.

Als standaard voor de informatiebeveiliging is in VNG-verband de Baseline Informatiebeveiliging Gemeenten (BIG) afgesproken. De BIG schrijft voor dat het integrale beleid op het gebied van informatiebeveiliging door het college van B&W wordt vastgesteld en wordt gepubliceerd voor werknemers en relevante externe partijen.

Het college van B&W heeft in december 2014 het informatiebeveiligingsbeleid van de gemeente Zoetermeer voor de periode 2015-2017 vastgesteld.

Conclusies

De algemene indruk is dat de informatiebeveiliging technisch goed op orde is en voldoende aandacht van de top van de organisatie krijgt. Tegelijkertijd is de organisatiecultuur vooral gericht op 'doen' en minder op het schriftelijk vastleggen. De menselijke factor wordt – terecht – als zwakke schakel gezien.

De raad toont geen structurele aandacht voor informatiebeveiliging. Het college vindt het ook niet nodig om deze aandacht te voeden of te vragen.

Conclusie 1

Het huidige informatiebeveiligingsbeleid is opgezet volgens de normen van de 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.

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.

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.

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.

Conclusie 5

Technisch zijn de ICT en de informatiebeveiliging op orde. De organisatie weet vrij goed te reageren op incidenten en noodsituaties. In 2016 is besloten om met het oog daarop een Computer Emergency Response Team (CERT) op te zetten. Het crisisbeheersingsbeleid is nog in ontwikkeling.

Conclusie 6

De kwetsbare schakels in de informatiebeveiliging zijn de menselijke factor en de inschakeling van externe partijen, bijvoorbeeld op het sociaal domein. Het is cruciaal dat door de hele organisatie heen het belang van informatieveiligheid wordt onderkend en dat middenmanagement en medewerkers daarnaar handelen, ook als het gaat om het uitbesteden van werkzaamheden aan derde partijen. Het toekennen van toegangsrechten tot applicaties kan nog worden aangescherpt – bijvoorbeeld met het oog op aanpassingen van autorisaties bij functiewijzigingen; een overall autorisatiebeleid op gemeentelijk niveau ontbreekt nog.

Conclusie 7

De gemeente Zoetermeer is aangesloten bij de informatiebeveiligingsdienst voor gemeenten (IBD) tot en met stap 3, het doorgeven aan de IBD van de bij de gemeente in gebruik zijnde IP-adressen en URL's. Stap 4, het aanleveren van de foto van de software en de hardware, is nog niet gezet. Dit betekent dat Zoetermeer – anders dan tweederde van de gemeenten – geen kwetsbaarheidsmeldingen van de IBD krijgt die specifiek zijn toegesneden op de eigen situatie.

Conclusie 8

De gemeente moet per 25 mei 2018 voldoen aan de Algemene Verordening Gegevensbescherming (AVG) van de EU. Daartoe heeft de gemeente vanaf oktober 2017 een privacyfunctionaris aangesteld. Boven deze functionaris komt de (verplichte) functionaris gegevensbescherming. Deze functionaris moet aansluiten bij het Informatie Management Overleg – dat dan het besluitvormende orgaan voor privacy- en informatiebeveiligingsaangelegenheden wordt.

Aanbevelingen

Bij het formuleren van de aanbevelingen is de rekenkamercommissie ervan uitgegaan dat de gemeente de resterende periode tot mei 2018 benut om de governance en de gegevenshuishouding in alle opzichten aan te passen aan de vereisten van de AVG. Daarnaast veronderstelt de rekenkamercommissie dat de gemeente conform de plannen in 2018 een integraal management informatiesysteem (IMIS) op informatiebeveiliging gaat invoeren. Door koppeling aan de P&C- en leercyclus kan de structurering van beleid en controle dan goed vorm krijgen. Verder wil de rekenkamercommissie de gemeente aansporen onderzoek te doen naar de (veiligheid van) volledige aansluiting bij de IBD.

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.

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.

Aan het college

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.

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.

Bijlage: Overzicht met afkortingen Bestuurlijke Nota Informatiebeveiliging

Afkorting	Volledige term
AVG	Algemene Verordening Gegevensbescherming
BIG	Baseline Informatiebeveiliging Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BIR	Baseline Informatiebeveiliging Rijksoverheid
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
IBD	Informatiebeveiligingsdienst voor Gemeenten
ICT	Informatie-en Communicatietechnologie
IMIS	Integraal Management Informatiesysteem
IP-adres	Internetprotocol adres, bestaande uit vier setjes van drie cijfers. Met behulp van deze set cijfers is elke computer en apparaat dat op internet is aangesloten te traceren.
P&C-cyclus	Planning & Control cyclus
URL	Uniform Resource Locator. Verwijst naar een uniek adres waarmee de locatie van een webpagina op internet wordt aangegeven of een e-mailadres
VNG	Vereniging Nederlandse Gemeenten