Jaarstukken 2017

gemeente
gouda

4.5.4 Informatieveiligheid

Beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en privacy zijn thema's die doorlopend aandacht nodig hebben.

Voor de gemeente is het uitgangspunt informatiebeveiligingsbeleid conform de Baseline Informatiebeveiliging Gemeenten (BIG). Dit kader bevat 303 beveiligingsmaatregelen onderverdeeld in technische, bouwkundige, organisatorische maatregelen om de gemeentelijke informatie te beschermen. De gemeente volgt de BIG om te voldoen aan wet- en regelgeving, voor een betrouwbare en continue dienstverlening, voor het zorgvuldig omgaan met informatie en het beheersen van risico's.

De gemeente streeft naar een optimale informatieveiligheid, maar 100% veiligheid is helaas een illusie.

Uit het onlangs verschenen Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten blijkt dat de vijf belangrijkste gesignaleerde bedreigingen voor de lokale informatievoorziening zijn:

- mensen maken fouten;
- gemeenten zijn net als alle organisaties kwetsbaar;
- dreigingen liggen ook (vlak) buiten de eigen organisatie;
- de waan van de dag bepaalt de agenda;
- we weten niet wat we niet weten.

Resultaten afgelopen periode
In de afgelopen jaren zijn de maatregelen uit de BIG opgepakt. In 2017 heeft de gemeente ongeveer 90% (5% meer dan in 2016) van de maatregelen geheel of deels gerealiseerd. Ongeveer 2% van de maatregelen vormen een geaccepteerd risico. De resterende 8% van de maatregelen zijn minder urgent en staan op de planning ter realisatie.

Beheersmaatregelen
Om nog meer in control te komen met betrekking tot informatiebeveiliging is de organisatie van de informatiebeveiliging herzien en is een Chief Information Security Officer (CISO) functionaris toegevoegd.

Om de informatiebeveiliging te monitoren wordt gebruik gemaakt van een Information Security Management Systeem dat uitgaat van de planning en control-cyclus.

Een aantal procedures is succesvol getest, waaronder de uitwijktest voor de BRP en de BAG. Ook is het afgelopen jaar met een penetratietest het Goudse netwerk getest op kwetsbaarheden van buitenaf.

Realisatie doelstelling IB-beleid (effectiviteit beheersmaatregelen en risico's)
In 2017 is voor het eerst de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek gehanteerd waarmee getoetst is in hoeverre de beheersmaatregelen getroffen zijn in het kader van het IB-Beleid.

Hiermee sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de gemeente.

Uit de zelfevaluatie blijkt dat Gouda de goede dingen doet maar dat er enkele punten ter verbetering blijven. Zo kan informatieveiligheid als onderwerp beter geborgd worden door dit explicieter terug te laten komen in de wijze waarop stuur- en verantwoordingsinformatie plaatsvindt, zowel intern onze organisatie als extern met leveranciers en samenwerkingsverbanden.

Andere aandachtspunten zijn onder meer:

- het actualiseren van het informatiebeveiligingsbeleid;
- meer investeren in het bevorderen van kennis en bewustwording van medewerkers ten aanzien van informatieveiligheid;
- herzien procedure wijziging of beëindiging dienstverband;
- opstellen beleid voor werken met informatiesystemen buiten de reguliere kantooromgeving en
- het doorvertalen van leverancierseisen naar onderaannemers.

Naast de horizontale verantwoording is het doel van ENSIA ook om de verticale verantwoording richting de rijksoverheid, over de 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) te structureren.

Voor de BRP en PNIK zijn twee zelfevaluaties ingevuld, de kwaliteitsmonitor en ENSIA. De kwaliteitsmonitor bevatte de vragen over de processen en in ENSIA waren de vragen over informatieveiligheid opgenomen. Het resultaat voor de zelfevaluatie Paspoorten en Nederlandse Identiteitskaarten (PNIK) is goed met een totaalscore van 98,7%. Het resultaat

voor de zelfevaluatie BRP is voldoende met een totaalscore van 90,6%. De gestelde normen voor de bestandscontroles BRP zijn behaald.

Voor de BAG is in 2017 voor het eerst de nieuwe zelfevaluatie uitgevoerd. Daaruit kwam dat tijdigheid een aandachtspunt blijft maar in het algemeen Gouda boven gemiddeld scoort.

Voor de BGT gemeenten bronhouders voor het gemeentelijk grondgebied dat niet wordt beheerd door provincie, waterschap, Rijkswaterstaat of ministerie van economische zaken.In 2017 is de opbouw van de BGT afgerond. De zelfevaluatie via ENSIA was nog niet verplicht, maar mocht als proef worden ingevuld. Daaruit kwam dat extra tijd besteed moet worden aan het uitwerken en kenbaar maken van de procesafspraken en het vastleggen van de kwaliteitsborging.

Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet
De stuurgroep ENSIA heeft besloten dat in het eerste jaar van ENSIA het college middels een verklaring verantwoording aflegt over de opzet en het bestaan van beheersmaatregelen en nog niet over de werking daarvan. Het verantwoordingsjaar 2017 richt zich op de DigiD-normen en een selectie van Suwinet normen. Een onafhankelijke ITauditor controleert de collegeverklaring en stelt een assurancerapport op waarmee verklaard wordt dat de collegeverklaring een getrouw beeld geeft.

Bovengenoemd proces is medio 2018 afgerond. Daarna wordt de collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet inclusief bijlage 1 DigiD en bijlage 2 Suwinet gezamenlijk met het assurancerapport separaat van het jaarverslag aan de gemeenteraad aangeboden.

Bescherming persoonsgegevens, datalekken en incidenten
Informatiebeveiliging en privacy overlappen elkaar en worden in de praktijk vaak als één gezien en dit zorgt nog wel eens voor verwarring. Het zijn twee verschillende aandachtsgebieden waarbij informatiebeveiliging wel zonder privacy kan, maar privacy niet zonder informatiebeveiliging. Met het invoeren van de BIG is wel de informatiebeveiliging op orde en daarmee de randvoorwaarde ingevuld om privacy mogelijk te maken. Voor privacy geldt ook wetgeving. Op 25 mei 2018 treedt de Europese Algemene Verordening Gegevensbescherming (AVG) in werking. De Wet bescherming persoonsgegevens komt daarmee te vervallen. Om tijdig te kunnen voldoen aan de AVG is in 2017 het project Gouda Privacyproof opgestart. Het project bestaat uit drie fases. Fase 1 is afgerond met het uitvoeren van een organisatie brede inventarisatie en analyse privacy plus het vaststelling van het privacy beleid. Fase 2 (betreft het invoeren van het privacybeleid op operationeel niveau) wordt momenteel uitgevoerd en met fase 3 (beheerfase) is ook een start gemaakt.

In 2017 zijn 10 datalekken geregistreerd in het daarvoor bestemde register. Daarvan zijn er 7 gemeld bij de Autoriteit Persoonsgegevens, omdat er (mogelijk) schade is en of gevolgen zijn voor de betrokkene(n). In 2017 hebben 230 medewerkers 1 of 2 dagen training gevolgd over privacy.

Meerjaren perspectief
De komst van de AVG en het dreigingsbeeld informatiebeveiliging Nederlandse Gemeenten vragen om herijking van de uitgangspunten informatieveiligheid en actualisatie van het informatiebeveiligingsbeleid en de daarbij horende maatregelen.

Deze maatregelen en de verbeterpunten uit ENSIA zijn ingrediënten voor het verbeterplan Informatieveiligheid 2018-2019.

4.5.5 Informatievoorziening en automatisering

Geheugen van Gouda
Het doel van het programma “Geheugen van Gouda” is de (digitale) dienstverlening te verbeteren door informatie op een betere manier te verwerken en op te slaan. Helaas heeft de gemeente de keuze moeten maken om de samenwerking met de softwareleverancier van het zaaksysteem te beëindigen. Dit heeft geleid tot vertraging in de uitvoering van het programma. In 2018 wordt dit opnieuw aanbesteed. Wel is het onderdeel vernieuwing van het Intranet gerealiseerd. Hiermee is de communicatie tussen medewerkers ondersteund.

Standaardisatie ICT
De organisatie heeft zich ten doel gesteld door standaardisatie het aantal applicaties waar mogelijk terug te dringen. In 2017 zijn de mogelijkheden geïnventariseerd. In het nieuwe informatieplan wordt aangegeven hoe de sturing op het aantal applicaties wordt ingericht en welke maatregelen daartoe worden genomen.
Met Waddinxveen en Zuidplas is een samenwerking op ICT-beheer. Daarbinnen wordt ook de mogelijkheid tot het gemeenschappelijk gebruiken van applicaties onderzocht. Twee applicaties worden al gemeenschappelijk gebruikt.