Rekenkamer Heemstede

Datum augustus 2022
Onderwerp Rekenkameronderzoek Informatiebeveiliging

Geachte leden van de gemeenteraad,

De Rekenkamer van de gemeente Heemstede heeft zichzelf voorgenomen om jaarlijks, naast een groot onderzoek dat veelal door derden in opdracht van de Rekenkamer wordt uitgevoerd, zelf een kleiner onderzoek uit te voeren. De bevindingen van een dergelijk onderzoek kunnen aanleiding geven tot een vervolgonderzoek, maar dat is uiteraard mede afhankelijk van de bevindingen almede van andere omstandigheden en/of mogelijke prioriteringen.

In 2021 heeft de Rekenkamer besloten om een kleiner onderzoek te doen naar het thema Informatiebeveiliging. Informatieveiligheid is een onderwerp dat met de toenemende digitalisering en het thuiswerken steeds belangrijker wordt.

Gemeenten verwerken grote hoeveelheden persoonsgegevens en andere belangrijke gegevens die goed beschermd moeten zijn. Zonder goede informatiebeveiliging liggen cybercriminaliteit, fraude en ondermijning van de interne gemeentelijke processen op de loer.

De centrale onderzoeksvraag van het rekenkameronderzoek was:

Is de informatieveiligheid bij de gemeente Heemstede voldoende gewaarborgd?

De centrale vraag is door de Rekenkamer uitgesplitst naar de volgende onderzoeksvragen:

- Beschikt de gemeente Heemstede over een beleid op het gebied van informatiebeveiliging?
- Heeft de gemeente Heemstede een centraal programma voor informatiebewustzijn?
- Hoe is de informatie die de gemeente Heemstede tot zijn beschikking heeft beveiligd tegen cyberaanvallen?
- Hoe heeft de gemeente Heemstede de fysieke beveiliging van informatie ingericht?
- Zijn de aanwezige risico’s ten opzichte van informatiebeveiliging bekend en hoe worden deze beheerst?
- Hoe houdt de gemeente Heemstede grip op (informatie)veilig thuiswerken?
- Voldoet de gemeente Heemstede aan het normenkader voor informatiebeveiliging, de Baseline Informatiebeveiliging Overheid (BIO)?

Het onderzoek is uitgevoerd op basis van een documentenanalyse en een interview met de heer Bryson en mevrouw De Porto.

Bevindingen

- De gemeente beschikt over een stevig beleid met betrekking tot informatiebeveiliging dat vrijwel alle aspecten van informatiebeveiliging afdekt.
- De raad ontvangt jaarlijks een voortgangsrapport in samengevatte vorm. Uit de rapportage het volgende:
    - De gemeente moet de informatiebeveiliging inrichten conform de Baseline Informatiebeveiliging Overheid (BIO). De BIO is verplicht sinds 1-1-2020 voor alle overheidslagen. Dit is een normenkader gebaseerd op de internationele ISO 270001/270002 normen.
    - Jaarlijks wordt een zelf audit uitgevoerd volgens de Eenduidige Normatiek Singel Information Audit (ENSIA). Met de uitkomsten van deze zelfaudit legt het college verantwoording af aan de gemeenteraad en aan diverse ministeries.
    - Naast het voldoen aan de BIO worden er ook informatiebeveiligingseisen gesteld aan de Basisregistratie Personen, de verwerking van Reisdocumenten, het gebruik van Suwinet, het gebruik van DigiD inlog voor burgers, de basisregistraties Adressen en Gebouwen (BAG), Grootschalige Topografie (BGT), Registratie Ondergrond (BRO) en Waardering Onroerende Zaken (WOZ).
- De gemeente voldoet voor ongeveer 60/70% aan de eisen van BIO (Baseline Informatiebeveiliging Overheid). Volgens de geïnterviewden is dit percentage niet veelzeggend, gegeven het grote aantal maatregelen en de beperkte relevante van een groot aantal daarvan. Zij zijn van mening dat de gemeente ‘in control’ is op het gebied van informatiebeveiliging.
- In de voortgangsrapportage zijn de volgende gebieden onvoldoende:
    - Continuïteit en incidenten: Zorgen voor de continuïteit van onze dienstverlening en het opvolgen van incidenten.
    - Informatiesystemen: Veilige omgang met informatiesystemen en afspraken hierover maken met onze leveranciers.
- Er wordt een zogenaamde GAP analyse gemaakt met openstaande issues. De onderkende risico’s zijn talrijk, maar kennen een beperkte importantie. De veelheid aan openstaande issues komt ook als gevolg van grote drukte. De drukte wordt mede veroorzaakt door het regelen van de Administratieve Organisatie (toegangsbeheersprocedures en controles) en de rol van de proceseigenaar binnen de ambtelijke organisatie. Deze verantwoordelijkheid voor een proces verdient aandacht.
- In 2021 is er een bewustwordingsplan geïmplementeerd. Zo ontvangen nieuwe medewerkers na drie maanden een online opleiding over informatiebeveiliging en alle medewerkers ontvangen regelmatig trainingen op dit gebied. Hierbij wordt nauw samengewerkt met de privacy officer. Het bewustzijn ten aanzien van informatiebeveiliging neemt toe, volgens de geïnterviewden ook bij het Bestuur.

- Thuiswerken wordt goed en veilig ondersteund met Citrix en de beveiligde mail oplossing Zivver. Ook hier geldt dat de aandacht ligt op bewustwording.
- Er zijn op jaarbasis ongeveer 15 veiligheidsincidenten die worden opgenomen in een meldingensysteem (zoals de AVG verplicht). De incidenten zijn veelal te wijten aan menselijk handelen. In een beperkt aantal gevallen is ook een melding gedaan aan de Autoriteit Persoonsgegevens. De incidenten hebben niet geleid tot een maatregel richting een medewerker (waarschuwing, ontslag, o.i.d.).
- Er is geen crisisplan beschikbaar, de ambitie is dat er snel een dergelijk plan moet zijn.
- De fysieke beveiliging verdient aandacht, de leden van de Rekenkamer kunnen met hun 2 jaar oude pas ongestoord door het gemeentehuis wandelen.

Daarnaast hebben we gesproken over ICT en 'outourcing', iets buiten de probleemstelling, maar wel relevant voor het onderwerp.

In 2020 is de 'technische portefeuille' aanbesteed en de gemeente doet nu zaken met OGD op basis van een Service Level Agreement. OGD levert nog niet naar behoren, moet worden scherp gehouden en er zijn zelfs al waarschuwende signalen aan OGD afgegeven. Harde maatregelen zijn nog niet getroffen.

Het contract met OGD loopt t/m medio 2024 en het contract voorziet in een mogelijke verlenging tot medio 2026. Of tegen die tijd opnieuw voor zo een groot contract gekozen zal worden, is nu nog niet te voorzien en uiteraard mede afhankelijk van diverse ook automatisering technische ontwikkelingen, met name beschikbaarheid en wenselijkheid SAAS oplossingen (Service as a Service).

Conclusies
De gemeente beschikt over helder en stevig beleid en heeft goed zicht op de mogelijke risico's. Hierover wordt ook regelmatig gerapporteerd, ook aan de raad. De uitdagingen liggen op het vlak van bewustwording en het nakomen van afspraken ten aanzien van de openstaande issues. Hiervoor is de medewerking van het ambtelijk apparaat noodzakelijk.

Daarnaast is het zo dat de fysieke toegangsbeveiliging aandacht verdient en dat het goed is als er snel een crisisplan beschikbaar komt.

Aanbevelingen
- Los de openstaande issues volgens BIO op of leg uit waarom de issues niet relevant zijn ('comply or explain'), kortom maak de omgang met de openstaande issues transparant, ook voor de raad.
- Blijf aandacht geven aan bewustwording bij medewerkers en denk na over eventuele maatregelen voor medewerkers die lichtvaardig/slordig omgaan met (privacy gevoelige) informatie.
- Zorg dat informatiebeveiliging onderdeel is van ieder proces en dat de proceseigenaar op de hoogte is van zijn/haar verantwoordelijkheden in deze.
- Stel een crisisplan op.
- Zorg dat fysieke toegangsbeveiliging beter wordt geborgd, bijvoorbeeld door beperkte toegang en jaarlijkse actualisatie van rechten.

Tenslotte wil de Rekenkamer haar waardering uitspreken voor de medewerking van de ambtelijke staf, in het bijzonder Dydier Bryson en Wineke de Porto

Met vriendelijke groet,
Namens de Rekenkamer Heemstede,

Coos Appelman
Voorzitter Rekenkamer