GEMEENTE HEERENVEEN
REKENKAMERCOMMISSIE

Aan de gemeenteraad van de gemeente Heerenveen

Onderwerp: resultaat monitoringsonderzoek Informatiebeveiliging

Heerenveen, 8 april 2021

Geachte raad,

Met deze brief informeert de Rekenkamercommissie Heerenveen (hierna: RKc) u over de uitkomsten van een monitoringsonderzoek naar de stand van zaken met betrekking tot de informatiebeveiliging van de gemeente Heerenveen.

Aanleiding monitoringsonderzoek informatiebeveiliging

Datasecurity c.q. informatiebeveiliging is een hot item de laatste jaren. Zie onder andere de voorbeelden bij gemeenten Bergen op Zoom, Lochem en Hof van Twente waar gemeentelijke systemen zijn gehackt. Het niet zorgvuldig omgaan met persoonsgegevens van de burgers betekent naast het risico op reputatieschade ook een risico op een officiële waarschuwing of een forse boete van de Autoriteit Persoonsgegevens. Ernstige consequenties maar waarvan de kans wel verminderd kan worden met het treffen van passende maatregelen. Door proactief de juiste maatregelen te treffen, wordt de kans op schade voor de gemeente Heerenveen aanzienlijk kleiner.

Dit was voor de RKc aanleiding om onderzoek te doen naar dit onderwerp. Op 11 september 2017 had de RKc dan ook besloten een verkenning te doen naar de informatiebeveiliging van de gemeente Heerenveen. De doelstelling was een nulmeting informatiebeveiliging uit te voeren om zo het niveau van de informatiebeveiliging binnen de gemeente Heerenveen inzichtelijk te maken, de belangrijkste risico's te benoemen en een advies te geven over welke beveiligingsmaatregelen mogelijk kunnen worden getroffen of geoptimaliseerd.

Voor deze RKc verkenning was een raadsbrief opgesteld. Voor de publicatie van de raadsbrief kwam de ambtelijke reactie dat er een interne audit liep naar de informatiebeveiliging. Uit de perspectiefnota 2017 van Heerenveen bleek dat het door de raad ondersteunde collegevoornemen bedoeld was om de gemeente tegen datalekken te beschermen. Hierdoor bestond op dat moment geen toegevoegde waarde meer om vanuit de RKc een verkenning te doen naar de informatiebeveiliging. Dit leidde ertoe dat het onderzoek achterwege is gebleven.

Monitoringsonderzoek 2021:

In een recent verkennend onderzoek[1] concluderen de onderzoekers dat de gemeenten beperkt voorbereid zijn op cybercrises. De grote uitdagingen zijn een gebrek aan samenwerking en daardoor onbenutte kennis over crisismanagement en cybersecurity. Ook blijkt uit dit onderzoek dat de gemeenten nu druk bezet zijn met Covid-19. Het is een enorme prestatie dat alle dienstverlening en thuiswerkfaciliteiten vanwege de Covid-19 crisis in no-time zijn uitgerold, maar het is een enorme vergroting van het aanvalsoppervlak voor hackers en een toename van de digitale kwetsbaarheid van de gemeenten.
Des te meer reden voor de RKc om dit monitoringsonderzoek in deze periode uit te voeren. Met dit monitoringsonderzoek wil de RKc nagaan hoe de gemeente na 2017 invulling heeft gegeven aan informatiebeveiliging.

De centrale vraag van de RKc in dit monitoringsonderzoek is:

Wat is de stand van zaken met betrekking tot de informatiebeveiliging na september 2017?

Enkele deelvragen hierbij zijn:

Wat is de uitkomst van de interne audit uit 2017 en is hiervan een rapport beschikbaar? Zijn er nog andere onderzoeken geweest naar de informatiebeveiliging na 2017 anders dan de interne audit in 2017?

De RKc heeft deze vragen in oktober 2020 gesteld aan de ambtelijke organisatie. Deze vragen zijn vervolgens beantwoord door het afdelingshoofd Informatiemanagement en ICT (I&I).

Bevindingen monitoringsonderzoek:

Het afdelingshoofd I&I heeft aangegeven dat bij hem niets bekend is van een interne audit noch dat hier documenten van gevonden kunnen worden. Wel is een managementletter 2019 van Deloitte aangeleverd evenals wat de afdeling I&I doet ten behoeve van informatie veilig werken.

Werkzaamheden van de afdeling I&I t.b.v. informatie veilig weken:

· *"We laten ons ethisch hacken. Dat is voor de eerste keer gedaan eind 2018. De rapportage daarover is uitgebracht begin 2019. Die rapportage kan niet verstrekt worden aan de rekenkamercommissie omdat de rapportage aantoonbaar maakt waar de*

[1] 'Cybercrisis bij gemeenten' – Haagse Hogeschool en NHL Stenden Hogeschool, 1-2-2021

kwetsbaarheden zitten in de informatiebeveiliging. Wanneer dat in verkeerde handen komt, heeft gemeente Heerenveen echt een enorm probleem.

· *We phishen ethisch. Dat doen wij jaarlijks. Daarvan krijgen wij de resultaten terug in een soort digitaal portaal, niet in een rapportage.*

· *We zorgen voor een bezoek van een mystery guest in opdracht van de directie. Dat doen wij jaarlijks en daar hebben we ook rapportages van. Hier geldt eigenlijk hetzelfde voor. De rapportage maakt aantoonbaar waar de kwetsbaarheden zitten in de toegang tot en het gebruik van gemeentelijke huisvesting. Wanneer dat in verkeerde handen komt, kan dat een behoorlijk probleem veroorzaken."*

Naar aanleiding van deze rapportages is de commissie AZ in 2019 in een besloten vergadering geïnformeerd over de stand van zaken m.b.t. informatiebeveiliging. De bijbehorende rapportage *"Rapportage stand van zaken 2018-begin 2019"* is aan de RKc vertrouwelijk verstrekt en zal na dit monitoringsonderzoek vernietigd worden. Door de vertrouwelijke status van dit document kunnen de volgende bevindingen alleen in hoofdlijnen worden benoemd door de RKc:

Er is sprake van een ICT visie, informatiebeveiligingsbeleid, risicoanalyse en genomen maatregelen. De door de afdeling I&I hiervoor genoemde tests en rapportages worden onderbouwd middels dit document. De risico's worden concreet gemeten en gemonitord evenals de effecten van de ingezette maatregelen o.b.v. Security assessment. Bij de maatregelen is o.a. aandacht voor de communicatie en trainingen in lijn met de Security assessment. Er vindt toezicht plaats door de Security officer I&I.

Op basis van de uitkomsten van de bovenstaande rapportages en tests is verdere uitvoering gegeven aan de vermindering van onacceptabele kwetsbaarheden in de ICT van gemeente Heerenveen. De afdeling I&I geeft aan dat hier stappen in zijn gezet. Het voornemen is om gemeente Heerenveen in 2021 opnieuw ethisch te laten hacken om te zien of er uitsluitend sprake is van acceptabele kwetsbaarheden. Wat de toegang tot de gemeentelijke huisvesting en het gebruik daarvan betreft, is bij herhaling het management door de afdeling I&I gewezen op de onacceptabele kwetsbaarheden. Er wordt aangegeven dat de afdeling DIm (Dienstverlening & Informatiemanagement) aan de slag is gegaan om met voorstellen te komen die kwetsbaarheden verminderen.

Verwacht wordt verder dat begin 2021 de commissie AZ in een besloten vergadering weer geïnformeerd zal worden door de Security Officer over de stand van zaken met betrekking tot informatiebeveiliging.

De volgende bevindingen zijn gedaan door de accountant Deloitte in de managementletter bij de interimcontrole 2019 t.a.v. informatie veilig werken:

Geconstateerd is dat de gemeente actief in alle lagen van de organisatie het bewustzijn vergroot op het gebied van informatieveilig werken. Het vergroten van het bewustzijn en het nemen van de nodige maatregelen wordt onder andere op de volgende wijze gerealiseerd:

- De Security officer is twee keer per jaar aanwezig bij de werkoverleggen om vragen op het gebied van informatieveilig werken van medewerkers te beantwoorden dan wel toelichting te geven op de laatste ontwikkelingen.

- Periodiek (minimaal 2 keer per jaar) wordt een nep-phishingmail verstuurd binnen de organisatie. Resultaten en tips worden vervolgens gedeeld binnen de gemeente.

- Een mystery guest[2] wordt door de gemeente ingezet om kwetsbaarheden aan het licht te brengen en hiervoor maatregelen te nemen.

- Door een ethische hacker is een security assessment uitgevoerd om mogelijke zwakheden zichtbaar te maken.

- Nieuwe medewerkers krijgen een informatievideo te zien op gebied van informatieveilig werken binnen de gemeente.

Daarnaast heeft de gemeente haar belangrijkste data, de informatierisico's die samenhangen met deze data en ingevoerde beheersmaatregelen in kaart gebracht. De gemeente heeft haar visie, kaders, verwachtingen en monitoring op het gebied van informatieveilig werken verwerkt in een door de directie vastgesteld beleidsplan. Het beleidsplan is ter kennisgeving aangeboden aan het college. Ontwikkelingen en resultaten worden tweemaal per jaar door het afdelingshoofd I&I gerapporteerd aan het management, de directie, het college en de gemeenteraad.

Conclusies

Er is geen expliciete uitvoering gegeven aan het in september 2017 aan de RKc aangegeven voornemen tot het uitvoeren van een interne audit naar de informatiebeveiliging.

In de ambtelijke toelichting op dit monitoringsonderzoek wordt aangegeven en middels documenten onderbouwd dat indirect hieraan opvolging is gegeven in het proces. Hierbij

[2] Een mystery guest kan o.a. een check doen op de 'clean deskpolicy' of op het toegangsbeleid fysieke ruimtes.

wordt door de gemeente Heerenveen zowel op strategisch, tactisch en operationeel niveau visie, beleid en uitvoering gegeven met betrekking tot informatiebeveiliging.

Er is sprake van een ICT visie, informatiebeveiligingsbeleid, risicoanalyse en genomen maatregelen. Er worden periodiek tests gedaan en hierover gerapporteerd, risico's worden concreet gemeten en gemonitord evenals de effecten van de ingezette maatregelen o.b.v. Security assessment. Ook wordt de gemeenteraad (commissie AZ) evenals het college periodiek hierover geïnformeerd. Deze stand van zaken wordt ook door de controlerende accountant van de gemeente Heerenveen onderschreven. Ten aanzien van de toegang tot de gemeentelijke huisvesting en het gebruik daarvan lijkt sprake te zijn van onacceptabele kwetsbaarheden.

Dit monitoringsonderzoek is op basis van een beperkt aantal documenten uitgevoerd omdat de specifieke en gedetailleerde documentatie zoals testresultaten als vertrouwelijk wordt beschouwd in het organisatiebelang van de gemeente Heereveen. Hier dient rekening mee gehouden te worden bij het lezen van deze raadsbrief.

Aanbevelingen

Indien de gemeenteraad hier aanleiding toe ziet, kan een vervolgonderzoek worden gedaan in de vorm van een evaluatief onderzoek. Hierin kan verdieping worden gezocht op de eerste bevindingen van dit monitoringsonderzoek.

Er zou hier ingezoomd kunnen worden op de vier aspecten op het gebied van informatiebeveiliging:

- **Juridisch:** aan de juridische kant is het verstandig (en verplicht) om bewerkersovereenkomsten af te sluiten met partijen die persoonsgegevens opslaan.
- **Mens:** het mensgerichte deel betreft kennis, houding en gedrag van de medewerkers op het gemeentehuis m.b.t. de informatiebeveiliging.
- **Organisatorisch:** databeveiliging is een ingebed onderdeel van de bedrijfsprocessen. Bijv. het invoeren van een registratiesysteem waarin verschillende soorten data in de organisatie geclassificeerd worden naar gevoeligheid en waarin eisen worden gesteld aan de omgang met de verschillende soorten data.
- **Technisch:** beveiligingstechnieken, het up-to-date houden van besturingssystemen, regelmatige en versleutelde back-ups maken etc.

Ook zou dan de vraag kunnen worden beantwoord in welke mate het gemeentelijk informatiebeveiligingsbeleid efficiënt, effectief en conform de procedures wordt uitgevoerd.

Er zouden daarbij ook penetratietests uitgevoerd kunnen worden en een beoordeling gedaan kunnen worden op de beveiliging van de belangrijkste applicaties.

Voor de uitvoerbaarheid van dit brede onderzoek is specifieke expertise en ervaring vereist. Daarom zou het vervolgonderzoek onder begeleiding van de rekenkamercommissie door een externe partij c.q. onderzoeksbureau worden uitgevoerd.

Deze raadsbrief is op 22 februari 2021 voor om wederhoor voorgelegd aan het college. De reactie van het college d.d. 3-3-2021 is bijgesloten in de bijlage bij deze raadsbrief.

Het bevreemdt ons als rekenkamercommissie dat in de bestuurlijke reactie een nieuwe ambtelijke feitencheck gedaan is terwijl wij twee keer eerder feitencheck hebben uitgevraagd aan de ambtelijke organisatie en gelegenheid hebben gegeven de bevindingen van dit onderzoek te checken.

Met vriendelijke groet,

Rekenkamercommissie Heerenveen

Emina Lukovac, extern lid RKc