Rekenkamercommissie
Meneer S. Dijk

verzenddatum:	27 oktober 2022	onderwerp:	Rekenkameronderzoek informatieveiligheid Bestuurlijke reactie
ons kenmerk:	1579873 / 1722093	uw kenmerk:	1569929 / 1647332
inlichtingen bij:	de heer R. Gerritsen	uw brief van:	23 september 2022
telefoonnummer:	(0314)	bijlage:	--

Beste meneer Dijk,

U heeft ons 23 september de nota van bevindingen informatiebeveiliging en privacy toegestuurd. Deze rapportage gaat over de manier waarop wij invulling geven aan de voorgenoemde onderwerpen. U vraagt ons een bestuurlijke reactie te geven op de rapportage en de daarin opgenomen aanbevelingen.

Dank voor het onderzoek en de conclusies en aanbevelingen. Informatiebeveiliging en privacy zijn onderwerpen die ons zeer aan het hart gaan. We beseffen dat we op dit terrein nog veel te ontwikkelen en te verbeteren hebben. Wij bezien daarom uw conclusies en aanbevelingen in het licht van continu verbeteren van onze kennis en kunde, juist op een terrein dat zich razendsnel ontwikkelt. En een bevestiging van diverse genomen stappen de afgelopen periode. Landelijke incidenten zoals de hack bij de gemeente Hof van Twente en het incident Log4J zorgen dat we bij moeten blijven. Uw onderzoek stimuleert ons verdere stappen te zetten.

De resultaten van het onderzoek naar informatiebeveiliging en privacy binnen de gemeente Doetinchem zijn voor ons voor een deel te herkennen en nemen we over. Voor een deel zijn deze volgens ons niet compleet en/of vragen nuancering. Graag lichten we dit hieronder toe.

Als algemene opmerking vooraf willen we aangeven dat voor ons enkele conclusies en aanbevelingen deels niet goed herleidbaar waren op uw waarnemingen en daarmee waar het oordeel van uw rekenkamer op is gebaseerd. Dit oordeel kan bijvoorbeeld gebaseerd zijn op gehouden interviews, de bestudeerde literatuur of wellicht een eigen oordeel in vergelijking met andere gemeenten. Dit gegeven hebben we waar relevant benoemd en onderstaand meegenomen in onze reacties. Wij nodigen u graag uit – alvorens u uw rapport afrondt – uw bevindingen toe te lichten.

Reactie op hoofdconclusie
- Hoofdconclusie: *De gemeente Doetinchem heeft nog een ontwikkeling door te maken om 'in control' te komen op informatieveiligheid.*

Reactie: Deze hoofdconclusie is naar onze mening erg algemeen gesteld. Enerzijds onderschrijven wij dat we in ontwikkeling zijn vanuit de wetenschap dat op een groeiend

en complex terrein van informatiebeveiliging en privacy het wellicht pretentieus zou zijn om te kunnen stellen dat we volledig "in control" zijn. Anders doet uw hoofdconclusie niet volledig recht aan veel inspanningen die gedaan zijn en worden aan het beschermen, beheren en beheersen van alle informatie van de gemeente Doetinchem. Bijvoorbeeld, op gebied van bewustzijn van informatieveiligheid bij alle medewerkers dienen nog stappen te worden gezet. Dit onder meer gebaseerd op de uitkomsten van de uitgevoerde testen in vergelijking met andere gemeenten. Een eerder opgesteld verbeterplan daartoe wordt inmiddels uitgevoerd voor het jaar 2022/2023.

Als het gaat over de meer wettelijke, organisatorische en technisch infrastructurele informatieveiligheidsmaatregelen zijn wij van mening dat we in vergelijking met andere gemeenten relatief gezien 'goed in control' zijn. We monitoren steeds op basis van IBD-meldingen (op basis van 'best-effort') meldingen van eigen medewerkers, ICT-partners en onze specifiek hiervoor ingekochte systemen. Op basis hiervan zijn we van mening dat we dit deel van informatieveiligheid goed en actief volgen en daarmee 'goed' in control zijn. Dit geldt zowel als gemeente Doetinchem, maar ook gezamenlijk binnen de ICT-samenwerking.

Reactie op aanbevelingen
- Aanbeveling I: *Versterk de positie van de strategische functionarissen op informatiebeveiliging en privacy en plaats deze in een staffunctie.*

• *Positioneer de CISO1 en Functionaris Gegevensbescherming (FG) in een van de lijn onafhankelijk staffunctie.*
• *Verstevig wat betreft omvang de formatie van deze strategische functies op informatieveiligheid.*

Reactie:
De gemeente kent momenteel geen staffuncties die los staan van teams: alle medewerkers maken onderdeel uit van een team. In dat licht zijn de FG en de CISO ook lid van een team. Zij hebben echter hun eigen onafhankelijke taken, verantwoordelijkheden en escalatiemogelijkheden naar de gemeentesecretaris en de bestuursorganen. Wat betreft de positionering zijn wij van mening dat deze onafhankelijkheid en escalatielijn belangrijke pijlers zijn.

Programmabegroting 2023
Nadat u uw onderzoek heeft afgerond, hebben wij de programmabegroting 2023 aan de raad aangeboden. Wat betreft de omvang van strategische functies kiest het college nadrukkelijk voor een intensivering van budgetten voor versterking van onze ICT-organisatie tegen specifieke ICT-dreigingen. Dit is inmiddels van een belangrijk deel gerealiseerd, dan wel opgenomen in de inmiddels vastgestelde begroting van de ICT-samenwerking al voor het jaar 2023. Om dit op het benodigde professionaliteitsniveau naar de laatste standaarden op peil te kunnen houden is het vanaf het jaar 2023 structureel nodig een uitgebreidere vorm ICT-beveiligingsservice te gaan contracteren.

Daarnaast hebben wij de raad in de programmabegroting 2023 voorgesteld € 100.000 extra in te zetten voor de taken die voortvloeien uit de Wet Politiegegevens (Wpg). Naast deze nieuwe wet zien we meer werk door:
• Toename van de complexiteit van de privacyvraagstukken door meer en verschillende samenwerkingsverbanden en de regionale taak die wij vanuit onze Centrumfunctie uitvoeren;
• Toename van het aantal verplichte Data Protection Impact Assessments (DPIA);

• Toename van algemene vragen omdat Privacy nu ook onderdeel is geworden van onze interne controles.

Bovenstaande is reden voor het college opnieuw naar de bezetting van onze vakgroep privacy te kijken. De uitbreidingen in taken en rollen zorgen ervoor dat de huidige uren van onze Functionaris Gegevensbescherming en Privacy Coördinator niet toereikend zijn. Met deze extra middelen willen we de formatie en de werkprocessen passend maken. Tevens zetten we in op meer bewustwording en kennis bij alle collega's in onze organisatie.

- Aanbeveling II: *Formuleer de ambitie om het gemiddelde niveau van de medewerkers van de gemeente te verhogen.*

Reactie:
Wij onderschrijven het belang van deze aanbevelingen en gaan een ambitie op dit vlak formuleren die zal worden opgenomen in het informatieveiligheidsbeleid.

- Aanbeveling III: *Betrek de raad meer bij het formuleren van ambities op informatieveiligheid en informeer de raad meer op de voortgang op deze ambities.*

Reactie:
Recent is het nieuwe college geïnstalleerd, waarbij informatieveiligheid expliciet is benoemd als portefeuille. Het betrekken van de raad bij informatieveiligheid wordt door de FG en CISO besproken met de portefeuillehouder, waarbij ambities en wensen wederzijds zijn uitgesproken.

- Aanbeveling IV: *Inventariseer de risico's in de samenwerking op ICT, bespreek deze met de partners en richt daarop de vernieuwde samenwerking in.*

Reactie:
De aanbeveling op zich is juist en wordt in deze vorm feitelijk uitgevoerd. De aanbeveling geeft de huidige situatie weer en zien we als aansporing om dit voort te zetten. Ter informatie dient dat dit ingevuld wordt in de vorm van bespreking en agendering in de drie belangrijkste overleggen in de ICT-samenwerking. De ICT-samenwerkingsorganisatie wordt hierin steeds gevoed met signalen vanuit de IBD, onze ICT-partners en eigen medewerkers. Na afstemming worden in overleg steeds passende maatregelen doorgevoerd. Ter illustratie twee recente voorbeelden. Naar aanleiding van de hack bij de gemeente Hof van Twente zijn de IBD-aanbevelingen geagendeerd en besproken in het reguliere ICT-A en deelnemersoverleg van de ICT-samenwerking. Dit heeft tot nadere afstemming van verantwoordelijkheden en aanpak geleid. Rond het incident Log4J is er vanuit de richtlijnen en waarschuwingen van de IBD proactief actie ondernomen. Hier zijn ICTA-leden, deelnemers en het gemeentesecretarissenoverleg apart geïnformeerd en heeft daarop waar nodig besluitvorming plaatsgevonden. Ter afsluiting merken we op dat bespreking van risico's in relatie tot continuïteit, technische kwetsbaarheid en organisatorisch onderwerpen zijn die regelmatig vanuit de ICT-samenwerking en deelnemers afgestemd worden.

- Aanbeveling V: *Stel een beleidskader op basis van de Digitale Agenda Gemeenten 2024 van de VNG.*

Reactie:
Deze aanbeveling zullen wij in het informatieveiligheidsbeleid meenemen. Hoewel de gemeente Doetinchem in 2021 nagenoeg volledig voldeed aan de ENSIA eisen, hebben wij de ambitie om aanvullende maatregelen te treffen vanuit de ENSIA voor 2022 en verder.

Reactie op deelconclusie
- Deelconclusie: *De ICT samenwerking waarvan Doetinchem gastheer is kent risico's die niet afdoende zijn afgedekt in de dienstverleningsovereenkomst.*

Wij werken met vier andere gemeenten en een aantal andere overheden goed samen binnen de ICT samenwerking. Daarbij worden afspraken omtrent de omvang en de kwaliteit van de dienstverlening regelmatig herijkt. Op het vlak van informatiebeveiliging voeren we juist de afgelopen tijd intensieve gesprekken. Wij hebben, zoals u beschrijft, binnen de gemeente Doetinchem de crisisbeheersingsstructuur specifiek voor ICT-vraagstukken ingericht en voeren we met onze partners gesprekken hoe zij tegen de beheersing op lokaal en lokaal overstijgend niveau van acute vraagstukken aankijken. Voor ons is de dienstverleningsovereenkomst voortdurend voorwerp van verbetering. Uw aanbeveling zien wij als een aanmoediging deze dienstverleningsovereenkomst actueel te blijven houden.

Reactie op inhoudelijke teksten

- Opmerking: *Een ander punt van aandacht is het beheer van wachtwoorden. De accountant heeft daar in het verleden ook op gewezen en de rekenkamer constateert dat daar nog steeds het een en ander aan schort.* (Pagina 1)

Wij herkennen ons niet volledig in deze constatering. De accountant heeft in de management letter 2021 onder hoofdstuk 3.2 de toegangsbeveiliging beschreven. De accountant stelt hierin dat de ingestelde wachtwoordeisen van het netwerk van voldoende niveau zijn. De accountant stelt ook dat de ingestelde wachtwoordeisen van de applicatie van voldoende niveau zijn. Wij nodigen de rekenkamer daarom uit nader te concretiseren waar het nog steeds zou schorten aan wachtwoordbeheer.

- Opmerking: *Het data gedreven werken staat nog in de kinderschoenen. Hiervoor is nog geen beleidskader ontwikkeld. Hierdoor is er nog geen zicht op het waarborgen van de privacy van burgers.* (Pagina 1)

Het data gedreven werken wordt langs twee lijnen in de organisatie verder gebracht. Enerzijds via de intergemeentelijke samenwerking binnen DatalabGO. Hiervoor geldt een aparte governancestructuur met inbreng vanuit iedere deelnemende gemeente. Onderdeel van de werkwijze is een toets op privacy van burgers bij uitwerking van onderzoeksvragen. Tweede lijn binnen Doetinchem vormt het leren wat data gedreven werken is en wat dit vraagt in termen van goede onderzoeksvragen. Nu wordt per geval op basis van de vraagstelling bezien of overleg met de privacyfunctionaris is aangewezen, gelet op de onderzoeksvraag. In het opstellen van een beleidskader ter toetsing en beoordeling vooraf zien wij de toegevoegde waarde.

Wij gaan er vanuit u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,
burgemeester en wethouders van Doetinchem,

secretaris burgemeester