Bestuurlijke nota

Rekenkamerrapport

Informatiebeveiliging en privacy

Gepubliceerd op:

7 februari 2023

Rekenkamer
gemeente Doetinchem

Informatiebeveiliging en privacy gemeente Doetinchem

Inleiding

De rekenkamercommissie Doetinchem (hierna 'de rekenkamer') heeft een onderzoek laten uitvoeren naar het informatiebeveiligings- en privacybeleid van de gemeente. Dit onderzoek is uitgevoerd door bureau 'PRAE - advies en onderzoek' te Utrecht. Gekeken is naar het gevoerde beleid, de organisatie, de techniek en het menselijk handelen. In deze inleiding gaat de rekenkamer kort in op de belangrijkste conclusies.

Uit het onderzoek blijkt dat het over het algemeen op orde is, maar dat betekent niet dat de gemeente tevreden achterover kan leunen; er is werk aan de winkel.

De volwassenheid van de organisatie wordt door de gesprekspartners bij de gemeente Doetinchem wisselend ingeschat. Op sommige gebieden, zoals bij DigiD, is die op een hoog niveau aanwezig en op andere applicaties is dat minder het geval. De cultuur is erop gericht om zaken te doen, dingen te regelen zonder alles op papier op orde te hebben.

Een ander punt van aandacht is de bewustwording van de medewerkers. Door ethische hackers is er in het rekenkameronderzoek getest hoe medewerkers reageren op phishing en smishing mails (bij phishing proberen criminelen mensen door e-mails naar een valse website te lokken. Smishing of SMS-phishing is elke vorm van oplichting via sms. Oplichters versturen sms'en met valse links).

Een volgend punt waar de rekenkamer aandacht voor vraagt in deze inleiding is de positie van Doetinchem als gastheer van de omliggende gemeenten op het gebied van ICT en het steeds voldoende afgedekt zijn van actuele risico's daarbinnen.

Het datagedreven 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.

Ten slotte wil de rekenkamer hier wijzen op het feit dat de raad te weinig betrokken wordt bij en te summier geïnformeerd wordt over informatieveiligheid. De rekenkamer benadrukt dat deze conclusie twee kanten heeft. Het college kan meer informatie verschaffen en de raad kan meer vragen stellen.

Het onderzoek

De centrale onderzoeksvraag luidt: "Welke kwetsbaarheden kent de beveiliging van de vertrouwelijkheid van de informatie van de gemeente en op welke wijze gaat de gemeente om met de privacygevoelige gegevens en informatie waarover zij beschikt?"

Dit onderzoek heeft geleid tot een Nota van bevindingen. Deze nota is als bijlage bijgevoegd. Hier volgen de conclusies en de aanbevelingen.

Conclusies

De gemeente Doetinchem onderneemt de stappen om te voldoen aan het beleid op informatiebeveiliging en privacy, samen het informatieveiligheidsbeleid.

Hoofdconclusie

De gemeente Doetinchem heeft nog een ontwikkeling door te maken om 'in control' te komen op informatieveiligheid.

Deelconclusies

Deze hoofdconclusie leidt tot de volgende deelconclusies:

1. Het informatiebeveiligings- en privacybeleid, samen in het informatie-veiligheidsbeleid, is actueel.
2. Bewustwording van medewerkers krijgt aandacht en blijft continu punt van aandacht.
3. De strategische formatie op informatieveiligheid moet versterkt worden en los van de lijn in de staf geplaatst worden.
4. Er moet een doelstelling geformuleerd worden om het gemiddelde volwassenheidsniveau op informatieveiligheid te verhogen.
5. De technische kant van informatieveiligheid is conform de normen, maar moet nog beter gemonitord worden.
6. De ICTsamenwerking waarvan Doetinchem gastheer is, kent risico's die niet afdoende zijn afgedekt in de dienstverleningsovereenkomst.
7. De raad wordt te weinig betrokken bij en te summier geïnformeerd over informatieveiligheid.

8. Er ontbreekt een beleidskader voor de uitdagingen die de transformatie van de digitale dienstverlening van de gemeente biedt.

Aanbevelingen

De conclusies leiden tot de volgende aanbevelingen:

1. Versterk de positie van de strategische functionarissen op informatiebeveiliging en privacy en plaats deze in een staffunctie.

Aan college

- Positioneer de CISO (Chief Information Security Officer) en Functionaris Gegevensbescherming (FG) in een van de lijn onafhankelijk staffunctie.
- Verstevig wat betreft omvang de formatie van deze strategische functies op informatieveiligheid.

1. Formuleer de ambitie om het gemiddelde niveau van de medewerkers van de gemeente te verhogen.
2. Betrek de raad meer bij het formuleren van ambities op informatieveiligheid en informeer de raad meer op de voortgang op deze ambities.
3. Inventariseer de risico's in de samenwerking op ICT, bespreek deze met de partners en richt daarop de vernieuwde samenwerking in.
4. Stel een beleidskader op basis van de Digitale Agenda Gemeenten 2024 van de VNG.

Aan college en raad

Ga samen het gesprek aan om de vrije ruimte in het kader van ENSIA in te vullen, zodat de raad voor zijn controlerende rol zicht krijgt op opzet, bestaan en werking van de maatregelen op informatiebeveiliging en privacy. ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit. Het project ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid.

Over het onderzoek

Aanpak

Voor het onderzoek zijn beleidsdocumenten en rapportages op informatiebeveiliging en privacy bestudeerd. Daarnaast zijn in opdracht van de rekenkamercommissie enkele testen uitgevoerd op de systemen en is een phishing/smishing campagne uitgezet onder de medewerkers van de gemeente.

Interviews zijn gehouden met een aantal sleutelpersonen. Ook zijn casestudies naar de praktijk van gegevensverwerking uitgevoerd in de teams Sociaal Domein en Toezicht en Handhaving. Hieronder volgt de beantwoording van de onderzoeksvragen, gevolgd door conclusies en aanbevelingen.

Beantwoording onderzoeksvragen

1. Beschikt de gemeente over een adequaat informatiebeveiligingsbeleid?
2. Beschikt de gemeente over een beleid voor het gebruik van belangrijke en gevoelige (privacy)informatie?
3. Hoe wordt dat beleid uitgevoerd en wordt het gemonitord?
4. Hoe is de informatievoorziening aan de gemeenteraad?
5. Wat zijn de toekomstige opgaven?

Onderzoeksvraag 1: Beschikt de gemeente over een adequaat informatiebeveiligingsbeleid?

Informatiebeveiligingsbeleid

De gemeente Doetinchem heeft een actueel informatiebeveiligings- en privacybeleid dat in april 2020 door het college van burgemeester en wethouders is vastgesteld. Doel is te voldoen aan de BIO- en AVG-richtlijnen (BIO is Baseline Informatiebeveiliging Overheid en AVG is Algemene Verordening Gegevens-bescherming). Het informatieveiligheidsbeleid maakt onderdeel uit van de Informatievisie 2020-2022, samen met de dienstverlenings- en communicatievisie. In het strategisch beleid zijn de verantwoordelijkheden, functies en rollen belegd op basis van het RASCI-model (R(esponsible), A(ccountable), C(onsulted), S(upportive), I(nformed)). Jaarlijks wordt het informatieveiligheidsplan opgesteld door de CISO (Chief Information Security Officer), met activiteiten voor dat jaar en waarin ook wordt teruggeblikt. Het jaarplan wordt geaccordeerd door het MT.

Protocollen en richtlijnen

De meeste protocollen en richtlijnen zoals voorgeschreven door de BIO, het basisnormenkader, zijn aanwezig bij de gemeente. Een aantal wordt nog gemist, zoals protocollen op mobiele datadragers, cryptografie, leveranciersmanagement en op onderdelen logging/monitoring. Een compleet en integraal bedrijfscontinuïteitsplan staat voor 2022 op de rol. Onderdelen daarvan, zoals het opschalingsmodel cybercrisis, zijn recent gereed gekomen.

Functies

De teamleiders zijn integraal verantwoordelijk voor informatieveiligheid.
De informatieveiligheidsbeheerders en de informatieveiligheidscoördinator zijn respectievelijk op operationeel en tactisch niveau op informatiebeveiliging actief. Op strategisch niveau opereert de CISO op informatiebeveiliging. Deze is sinds eind 2021 'dedicated' voor 16 uur bij het team Informatiemanagement gepositioneerd. Idealiter moet deze functie apart van de lijnorganisatie gepositioneerd zijn.

Daarnaast kent het team ter ondersteuning op operationeel niveau drie informatieadviseurs. Vanwege de gemeentegrootte zijn veel functies duo-functies, ook op informatieveiligheid, en is het lastig capaciteit uit de markt te halen.

Overleggen

In Doetinchem is intern een vierwekelijks overleg tussen de portefeuillehouder, teamleider ICTsamenwerking en manager bedrijfsvoering, onder andere over informatieveiligheid. De CISO kan zelfstandig naar de gemeentesecretaris, portefeuillehouder of burgemeester schakelen. De gemeentelijke partners in de samenwerking participeren in de werkgroep informatiebeveiliging, met een adviesrol. De informatieveiligheidscoördinator van Doetinchem neemt daaraan deel. Daarnaast is er alleen een ambtelijk overleg tussen de gemeentesecretarissen van de deelnemende gemeenten.

Rapportages

Het jaarlijkse informatieveiligheidsplan gaat vanaf 2022 naast het MT ook naar de teamleiders. Elk kwartaal worden de incidenten, datalekken en de verbeterpunten aan het MT gerapporteerd. De informatieveiligheidscoördinator verzorgt ook de ENSIA-rapportage voor de verticale verantwoording richting landelijke toezichthouders en de horizontale verantwoording richting de gemeenteraad. Daarvoor gebruikt de gemeente geen informatiemanagementsysteem, wat een van de voorwaarden in de BIO is.
Tot slot gaat de accountant ook nog in op informatiebeveiliging in de jaarlijkse managementletters.

Onderzoeksvraag 2: Beschikt de gemeente over een beleid voor het gebruik van belangrijke en gevoelige (privacy)informatie?

Privacybeleid

Vanaf 2020 heeft de gemeente in informatieveiligheid het privacybeleid gekoppeld aan informatiebeveiligingsbeleid. De verantwoordelijkheden met betrekking tot privacybeleid zijn belegd. Net zoals bij informatiebeveiliging is de uitvoering van het privacybeleid belegd bij de teamleiders.

Elementen

De voor de AVG verplichte elementen en instrumenten zijn aanwezig, zoals het verwerkingsregister, privacystatement, verwerkersovereenkomsten, een procedure voor datalekken en risicobeoordeling met behulp van dataprotection impact assessments (dpia's).

Functies

De Functionaris Gegevensbescherming (FG) is voor 36 uur bij de gemeente Doetinchem aangesteld en vult deze functie in voor meerdere gemeenten en instellingen. In totaal is de FG voor 170 uur per jaar beschikbaar op strategisch niveau voor Doetinchem. Op tactisch niveau is een privacycoördinator aanwezig en op operationeel gebeid zijn privacybeheerders in de teams aangewezen.

Overleggen

De FG is betrokken bij de werkgroep informatiebeveiliging in het ICT samenwerkingsverband. De FG en CISO hebben maandelijks een overleg over informatieveiligheid. De privacy- en informatiebeveiligingscoördinator hebben wekelijks onderling overleg. Daarnaast heeft de FG een regionaal overleg met de privacycoördinatoren van de gemeenten en instellingen waar deze de FG-functie vervult. Aanvullend is er een overleg met FG'en uit de Achterhoek.

Rapportages

De FG stelt jaarlijks een rapportage op met een toetsing aan de AVG, met aandacht voor de wisselende focusgebieden van de Autoriteit Persoonsgegevens (AP). Net als voor informatiebeveiliging wordt geen gebruikgemaakt van een informatiemanagementsysteem om de rapportages op te stellen.

Onderzoeksvraag 3: Hoe wordt dat beleid uitgevoerd en wordt het gemonitord?

Hieronder gaan we in op vijf punten: bewustwording, uitvoering van de AVG, ICTsamenwerking, autorisatieproces, monitoring en pentesten.

Bewustwording

Bewustwording van medewerkers op de risico's met betrekking tot informatiebeveiliging en privacy is groeiende, zoals het melden van incidenten en datalekken. Maar bewustwording blijft continu inspanningen vragen. Daarop stelt de gemeente jaarlijks een apart bewustwordingsplan op met verschillende activiteiten. Daarbij wordt bewustwording organisatiebreed onder de aandacht gebracht en onderdeel van functioneringsgesprekken. Het proces van bewustwording verloopt traag en niet alle geledingen worden even doeltreffend met activiteiten en verbeterplannen bereikt.

De bewustwordingsactiviteiten worden ook gericht op MT en college. Het draagvlak bij management en bestuur voor informatiebeveiliging en privacy is groeiende. In het MT worden de rapportages en verbeterplannen op beide onderwerpen doorgesproken en vastgesteld. De rekenkamer heeft de indruk dat onderwerpen als investeringen op informatiebeveiliging en privacy in het college niet de hoogste prioriteit hebben.

Het kennisniveau in de organisatie bij de proceseigenaren blijft op het gebied van informatiebeveiliging achter op privacy en is met name aanwezig bij de medewerkers die met cruciale applicaties werken, zoals financiën, DigiD en Suwinet. Informatiebeveiliging is dan ook meer technisch van aard. Het gemiddelde volwassenheidsniveau conform de NOREA-index, is weliswaar niet gemeten, maar wordt niet heel hoog ingeschat (NOREA is de beroepsorganisatie van IT-auditors, die in de NOREA-index normen heeft vastgelegd. Dat heeft onder andere te maken met de cultuur om zaken te regelen zonder alles op papier te documenteren. Het beeld is dan ook dat de gemeente niet volledig in control is op gebied van informatiebeveiliging en privacy.

AVG (Algemene verordening gegevensbescherming)

Vanaf 2017 is de gemeente met medewerkers aan de slag gegaan op het gebied van privacy. De verplichte elementen en instrumenten op gegevensbescherming zijn aanwezig. De (pre)dataprotection impact assessments ([pre-]dpia's) worden door de proceseigenaren gehouden, maar vergen nog veel ondersteuning door de privacycoördinator. Ook hierbij wordt geconstateerd dat het

volwassenheidsniveau op naleving van de processen en vastlegging van activiteiten omhoog kan.

De FG rapporteert jaarlijks aan MT en college over de voortgang op de AVG-maatregelen. En monitort daarbij de activiteiten op onder andere beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking beveiliging en verantwoording. De positie van de FG mist een zekere strategische inbedding, daar MT en bestuur met name contact heeft met de privacycoördinator. In de bestuurlijke processen wordt het privacy aspect vaak te laat betrokken.

ICTsamenwerking

De gemeente Doetinchem is sinds 2015 gastheer van het samenwerkingsverband op ICT met omliggende gemeenten en regionale instellingen. In 2018 is het samenwerkingsverband herbevestigd. Het is een verband met een lichte structuur, zonder uitgebreide dienstverleningsovereenkomsten. Er is geen bestuurlijk overleg binnen de samenwerking, wel hebben de gemeentesecretarissen een overleg.

Inhoudelijk is er op informatiebeveiliging een werkgroep die adviezen geeft. Vanwege de vele verschillende functieniveaus van de participanten is het nog een zoektocht waarover op informatiebeveiliging en privacy overlegd kan worden. De werkgroep kan bij crisissituaties optreden, zoals bij de Log4J-dreiging in december 2021 (Log4J-dreiging wordt uitgebreid beschreven op pagina 23 van het rapport in de bijlage). Een interdisciplinair actieteam is in Doetinchem opgezet, waarbij in samenspraak met de deelnemende partners naar tevredenheid is gecommuniceerd en geacteerd.

Doetinchem is als gastheer verantwoordelijk voor de continue en veilige werking van de ICT. Technische maatregelen zijn en worden daartoe genomen. En de gemeente voert periodiek technische testen uit op de beveiliging van de systemen, zoals uitwijk- en pentesten (zie over pentesten ook hierna).

Betwijfeld kan worden of de governance op het samenwerkingsverband toekomstbestendig is ingeregeld.

Autorisaties

Met het autorisatieproces wordt geregeld dat medewerkers toegang krijgen tot de applicaties en gegevens die ze nodig hebben voor de uitoefening van hun functie. Het autorisatiebeleid ziet er dan ook op toe dat medewerkers niet bij

gegevens kunnen die zij niet nodig hebben. Bij door- of uitstroom van de medewerker moeten de autorisaties worden aangepast. Dat is afhankelijk van de melding door de leidinggevende en de tijdigheid daarvan blijkt niet altijd gegarandeerd. Het autorisatieproces verdient nog meer aandacht en controle. Ook de accountant adviseerde het college begin 2022 om onder andere hieraan aandacht te besteden.

Casestudies

Uit de casestudies bij het Sociaal Domein en Toezicht en Handhaving werd duidelijk dat beide teams al langere tijd ervaring hebben met de verwerking van persoonsgegevens. Dat is met de Algemene Verordening Gegevensbescherming (AVG) sinds 2018 en recenter de Wet politiegegevens (Wpg) sinds 2020 nog strikter geworden. De teams gaan consciëntieus met de richtlijnen hierin om. Op de meeste gegevensverwerkingsprocessen in het sociaal domein zijn (pre)dpia's gehouden, bij toezicht en handhaving nog geen.

In het sociaal domein wordt enige hinder ervaren in de preventiesfeer doordat de AVG drempels opwerpt bij het onderling delen van gegevens met andere instanties. En uit de casus bij toezicht en handhaving kwam naar voren dat het beveiligd mailverkeer met behulp van de applicatie Zivver nog niet voor alle medewerkers is geïmplementeerd.

Monitoring

Monitoring van de uitvoering van het beleid op informatiebeveiliging en privacy geschiedt op verschillende manieren. De implementatie van de BIO-maatregelen gebeurt via op basis van een GAP- en risicoanalyse, die input voor de activiteiten voor de jaarplannen opleveren. Zoals aangegeven is, door het vastleggen van de controleactiviteiten en de checks een aandachtspunt. Daardoor is in de organisatie zicht in bestaan en opzet van beleid en maatregelen, maar ontbreekt een volledig zicht op de werking ervan in de praktijk. Dat is niet het geval bij de applicaties DigiD en Suwinet, daar hierbij de vastlegging van activiteiten, logging en monitoring in het kader van ENSIA landelijk wordt afgedwongen.

Pentesten

De gemeente Doetinchem laat door externen pentesten uitvoeren op de systemen die de gemeente voor de ICTsamenwerking als gastheer beheert. Daar komen verbeterpunten uit die door de ICTsamenwerking worden opgepakt. In het kader van het rekenkameronderzoek zijn ook pentesten uitgevoerd. Om de scope van de testen te bepalen, zijn de recentste externe en interne

netwerkpentesten van de gemeente door de ethische hackers die de rekenkamer heeft ingehuurd bekeken. Op basis van die analyse is door de rekenkamer besloten de wifi-netwerk pentest, AD audit (AD staat voor Active Directory en geeft beheerders de mogelijkheid om de rechten van medewerkers te beheren) en een phishing/smishing test uit te voeren, en niet een externe en interne netwerk pentest over te doen. Ook is afgezien van een in eerste instantie voorgenomen mystery guest bezoek. Omdat veel medewerkers thuis werkten gedurende de coronamaatregelen had zo'n test weinig zin.

De testen leverden laag tot gemiddelde risico's op, geen hoog kritieke risico's. De resultaten van deze testen zijn vertrouwelijk gedeeld met de gemeentesecretaris, zodat de gemeente aan de slag kan met de verbeter- en aandachtspunten uit de testen. Deze verbeterpunten hadden onder andere te maken met bewustzijn van de medewerkers, wat een continu aandachtspunt is.

Onderzoeksvraag 4: Hoe is de informatievoorziening aan de gemeenteraad?

Summier geïnformeerd

De raad heeft volgens het informatieveiligheidsbeleid geen kaderstellende maar alleen een controlerende rol. Het college en management vat het beleid als onderdeel van bedrijfsvoering op. De onderwerpen worden incidenteel geadresseerd in de raad. De gemeenteraad wordt in het kader van de P&C-cyclus over informatiebeveiliging en privacy summier geïnformeerd. In de jaarstukken van de gemeente wordt over het informatiebeveiligingsbeleid gerapporteerd en worden de resultaten van de ENSIA-rapportage behandeld. Kort worden activiteiten op informatiebeveiliging en privacy belicht.

Op privacy krijgt de raad een infographic en samenvatting van de jaarrapportage van de FG. De raad krijgt apart in het kader van de horizontale verantwoording, waarvoor ENSIA is bedoeld, de college- en assuranceverklaring over de audits op DigiD en Suwinet. Het college heeft de ENSIA-stukken geheim verklaard en deze ter inzage gelegd voor raadsleden.

De informatievoorziening op informatieveiligheid aan de raad voldoet in principe aan de gestelde eisen, maar is als summier te beoordelen. Ook al is het voor veel raadsleden een technisch onderwerp, gelet op de risico's die de gemeente hierop loopt, kan de raad hierin meegenomen worden. Naast de rapportages die via het college komen, geeft de accountant in de controles ook op onderdelen van informatiebeveiligingsbeleid oordelen over de werking ervan.

Onderzoeksvraag 5: Wat zijn de toekomstige opgaven?

Risico's en kansen

De verwachting is dat door verdergaande digitalisering de risico's op en de investeringen in informatieveiligheid alleen maar zullen toenemen. Daarentegen gebeurt digitalisering niet zomaar, het biedt ook kansen en de mogelijkheid tot verbetering van de efficiëntie en effectiviteit van het door de gemeente gevoerde beleid. Digitalisering is niet alleen meer van de afdeling ICT, maar doordesemt alle takken van de gemeentelijke werkzaamheden. De Digitale Agenda Gemeenten 2024 van de VNG heeft drie doelstellingen geformuleerd voor de transitie van de digitale gemeentelijke dienstverlening: mogelijk maken – kansen benutten – duiden en reflecteren.

Datagedreven werken

In Doetinchem staat datagedreven werken en koppelen van gegevens nog in de kinderschoenen. De gemeente participeert sinds 2020 in Datalab GO, een project van gemeenten in Oost Gelderland waarvan Bronckhorst de penvoerder is. Vooralsnog gaat het daarbij om koppeling van gegevens in het fysieke domein. Maar het wordt niet uitgesloten dat ook andere gegevens gebruikt gaan worden. In het sociaal domein experimenteert de gemeente met koppeling van gegevens, en dat gebeurt geanonimiseerd en niet tot personen herleidbaar.

Algemene landelijke kaders zijn er slechts ten dele of in ontwikkeling. De gemeente heeft geen eigen visie of beleid geformuleerd om de kansen te benutten die de nieuwe technologieën bieden, of om de risico's met betrekking tot gegevensverwerking te duiden. Daardoor ontbreekt het kader om de transformatie van de digitale dienstverlening van de gemeente optimaal vorm te geven.