Startnotitie onderzoek informatiebeveiliging en privacy

1. Inleiding

Het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de door de gemeente beheerde informatie en data is een basistaak geworden. Als gevolg van de decentralisaties binnen het sociaal domein (Wmo, jeugdzorg en participatie) is het aantal door de gemeente beheerde bijzondere persoonsgegevens daarnaast sterk gegroeid. Samen met gegevens die de gemeente daarvoor al tot haar beschikking had, is het beveiligen van de toegang tot, het gebruik en het verstrekken van deze data essentieel geworden.

Door keten- en netwerksamenwerking ontvangt en deelt de gemeente veel van deze data en informatie. Door de digitalisering van de maatschappij en de gangbare norm van tijd- en plaatsonafhankelijke toegang tot data, zijn privacybescherming en beveiliging van deze data en informatie een 24/7 verantwoordelijkheid.

De kans op ongeautoriseerde toegang tot en misbruik van deze data en informatie is de afgelopen jaren groter geworden. Bijna dagelijks zijn er bij gemeenten (pogingen tot) cyberaanvallen, verstoringen van de informatiebeveiliging of andere (bijna) incidenten. Het gaat hierbij om aanvallen van buitenaf via internet of e-mail (bv. via phishing mails of gijzelingsvirussen), onveilige verbindingen en links, virussen via besmette bestanden/computers e.d. waardoor computers, systemen en bestanden overgenomen, afgeluisterd, geblokkeerd, versleuteld of beschadigd kunnen worden. Ook gaat het om eventuele informatielekken van binnenuit (al dan niet moedwillig) en onveilig omgaan met gegevens(dragers) c.q. oneigenlijk gebruik van bestanden en (vertrouwelijke) gemeentelijke gegevens.

De impact van een beveiligingsincident kan zeer groot zijn. De afgelopen jaren zijn in de directe omgeving van de gemeente Oude IJsselstreek nieuwswaardige incidenten geweest. Denk hierbij aan de datadiefstallen bij de GGD in januari 2021 tijdens de coronapandemie, de hacks of pogingen daartoe bij de gemeenten Lochem en Hof van Twente in 2019 en 2020 en van de Veiligheidsregio Noord en Oost-Gelderland in september 2020.

De verantwoordelijkheid die de overheid draagt voor de fysieke veiligheid zou in gelijke mate moeten gelden voor de digitale veiligheid. Burgers, bedrijven en organisaties moeten erop kunnen vertrouwen, dat hun gegevens in goede handen zijn bij de overheid. Dat is de essentie van het vertrouwen dat men in de overheid moet kunnen stellen.

Het beveiligen van (digitale) informatie en het bewaken van de privacy is van een ICT-vraagstuk veranderd in een bestuurlijk relevant onderwerp. Daarmee is het ook een verantwoordelijkheid van de gemeenteraad geworden, die kaders zou moeten stellen en het college moet controleren op het uitvoeren van zijn taken op dit gebied. Het is belangrijk om ook als gemeenteraad goed bij dergelijke belangrijke strategische kwesties betrokken te zijn.

2. Doelstelling en vraagstelling

De rekenkamer beoogt met een onderzoek naar informatiebeveiliging en privacy de gemeenteraad inzicht te geven in:

1. De doeltreffendheid van het actuele informatiebeveiligings- en privacybeleid en de bijbehorende beheersmaatregelen.
2. De eventuele risico's die de gemeente loopt op het gebied van informatiebeveiliging en privacy intern en in samenwerkingsverbanden (gedeelde ICT-voorzieningen).
3. De impact van toekomstige opgaven (zoals Artificial Intelligence (AI), datagedreven werken en Europese eisen) op het gebied van informatiebeveiliging en privacy.

Om tot deze inzichten te komen geldt de volgende centrale onderzoeksvraag:

Is de informatiebeveiliging en privacybescherming van de gemeente Oude IJsselstreek – mede in relatie tot samenwerkingsverbanden – doeltreffend en doelmatig ingericht?

In de kern is het de zoektocht naar de vraag of de gemeente Oude IJsselstreek een goed beeld heeft van de belangrijkste risico's op het gebied van informatiebeveiliging en specifiek de privacybescherming van gevoelige informatie zoals (bijzondere) persoonsgegevens.

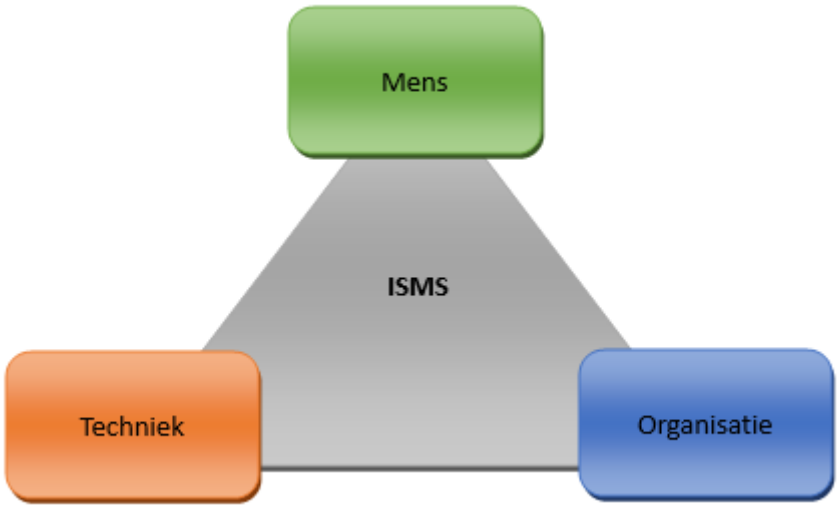
Om deze centrale vraag te kunnen beantwoorden, hanteert de rekenkamer de volgende deelvragen:

1. Heeft de gemeente op een adequate manier invulling gegeven aan haar informatiebeveiligings- en privacybeleid?
2. In hoeverre is de sturing van de gemeente binnen samenwerkingsverbanden toereikend op het gebied van informatiebeveiliging- en privacy?
3. In hoeverre zijn risico's en beheersmaatregelen (intern en binnen samenwerkingsverbanden) in kaart gebracht en op welke wijze worden deze consequent opgevolgd?
4. Op welke wijze anticipeert de gemeente op toekomstige ontwikkelingen (die invloed hebben) op het gebied van informatiebeveiliging en privacy?
5. Hoe wordt de gemeenteraad betrokken bij de thema's informatiebeveiliging en privacy?

We onderzoeken daartoe enerzijds de mate waarin het systeem voor onbevoegden toegankelijk is en anderzijds de mate waarin de medewerkers informatieveilig en privacybeschermend handelen. Daarnaast beschrijven we het beleid en de organisatie van de informatiebeveiliging en privacy en deze wijze waarop de gemeenteraad over dit onderwerp wordt geïnformeerd.

3. Onderzoeksopzet

Informatiebeveiliging en privacy zijn via drie 'velden' met elkaar verbonden en vormen gezamenlijk het zogeheten Informatie Beveiligings Management Systeem (in het Engels: ISMS). Visueel weergegeven ziet dat er als volgt uit:



Om tot een goed antwoord op de centrale onderzoeksvraag te komen worden alle drie de velden onderzocht.

3a. De mens

De mens is doorgaans de zwakste schakel van elk beveiligingssysteem. Er zijn verschillende manieren om te testen hoe sterk het veiligheidsbewustzijn van de gemeentemedewerkers is en in welke mate er in dit opzicht juist wordt gehandeld:

- ***Phishing***. Dit is een manier om, meestal via e-mail, in één keer bij een grote groep mensen te proberen om ze naar een site te lokken en te verleiden om daar persoonlijke gegevens in te voeren. Herkennen medewerkers deze mails en gaan ze er goed mee om?
- ***Inlooptest.*** Gemeentehuizen zijn openbare gebouwen waar iedereen naar binnen moet kunnen, maar niet overal bij moet kunnen. In een inlooptest wordt gekeken in hoeverre onbevoegden zich fysieke toegang kunnen verschaffen tot de medewerkerszones van het gemeentehuis en welke informatie ze daarbij kunnen vinden.
- ***Vishing.*** Hierbij kan een representatieve afvaardiging van de medewerkers gebeld worden om te testen of ze gevoelige (persoons)gegevens delen van zichzelf en/of van burgers.
- ***Zelfevaluatie***. Vanuit het gemeentelijk informatiebeveiligingsbeleid zijn normaalgesproken gedragsregels bekend gemaakt aan medewerkers. Middels een korte vragenlijst kan getoetst worden in hoeverre medewerkers deze gedragsregels kennen en zich hieraan houden.

3b. De techniek

Naast de mens is er de 'harde' kant van informatiebeveiliging en privacy: het geheel van technische maatregelen dat getroffen is om 1) ongeautoriseerde toegang tot de digitale omgeving van de gemeente te voorkomen, en 2) te voorkomen dat data en informatie ongewenst van binnen naar buiten gaat.

Om dit te onderzoeken worden er twee verschillende testen uitgevoerd:

1. ***Externe toegankelijkheid.*** Kunnen kwaadwillenden op afstand via bijvoorbeeld (web)applicaties in de informatiesystemen van de gemeente komen? (***blackbox test***).
2. ***Interne kwetsbaarheden.*** Wat zijn de gevolgen van een aanval op het systeem vanaf het eigen netwerk van de gemeente, bijvoorbeeld door medewerkers met slechte bedoelingen of hackers die zich toegang hebben verschaft tot het interne netwerk? Welke interne barrières zijn er ter bescherming van de vertrouwelijkheid van de gegevens? (***greybox test***).

3c. De organisatie

Bij het onderdeel organisatie wordt in kaart gebracht welk beleid de gemeente heeft vastgesteld op de thema's informatiebeveiliging en privacy, welke beheersmaatregelen geëffectueerd zijn en hoe bevoegdheden en verantwoordelijkheden voor deze gebieden zijn geborgd. Tevens onderzoeken we of en op welke wijze de gemeente deze thema's structureel heeft geborgd. Ook kijken we op welke wijze de gemeenteraad wordt geïnformeerd over informatieveiligheid.

4. Planning

Gelet op de gevoeligheid van het onderwerp en het behoud van het "verrassingseffect" zal de opzet en de planning van dit onderzoek niet in grote kring verspreid worden.

Voor de start informeren we in ieder geval de burgemeester (als voorzitter van de raad én tevens portefeuillehouder), de gemeentesecretaris, de voorzitter van de Auditcommissie van de gemeenteraad en de CISO en FG. Na afronding van de deelonderzoeken met het 'verrassingseffect' (beschreven onder 3a. en 3b.) kunnen en zullen relevante anderen worden geïnformeerd over dit rekenkameronderzoek.

Het doel van de rekenkamer is het opleveren van een onderzoeksrapport met conclusies en aanbevelingen dat goed leesbaar is voor haar doelgroep: de gemeenteraad. Nadrukkelijk dient het geen technisch rapport met veel vaktermen te zijn, die alleen begrijpelijk is voor ICT-deskundigen. Het feitelijke onderzoek zal naar verwachting 9-10 maanden in beslagnemen. Uitgaande van een start in mei 2024 zal het onderzoek in januari 2025 zijn afgerond en het eindrapport aan de gemeenteraad worden gepresenteerd en aangeboden.

Het onderzoek zal grotendeels in eigen beheer worden uitgevoerd. Voor de deelonderzoeken op 3a (De mens, uitgezonderd de zelfevaluatie) en 3b (De techniek) wordt externe deskundigheid ingehuurd.