ONDERZOEKSPLAN INFORMATIEVEILIGHEID

Datum: 11 september 2020

1. INLEIDING

Informatieveiligheid is een onderwerp dat met de toenemende digitalisering steeds belangrijker wordt. Gemeenten verwerken grote hoeveelheden gegevens in een veelvoud aan systemen en programma's. Veel van deze gegevens betreffen (bijzondere) persoonsgegevens of andere belangrijke gegevens die goed beschermd moeten zijn. Denk bijvoorbeeld aan:

- Persoonsgegevens van inwoners in de Basisregistratie Personen (BRP);
- Persoonsgegevens in het sociaal domein (Wmo, jeugd, participatie) waarbij ook bijzondere persoonsgegevens worden geadministreerd, bijvoorbeeld welke ondersteuning iemand ontvangt;
- Informatie over grote ruimtelijke projecten;
- Informatie over de veiligheid in de stad.

Zonder goede informatiebeveiliging liggen cybercriminaliteit, fraude, oplichting en ondermijning op de loer.

De gemeenteraad heeft het onderwerp informatieveiligheid verschillende keren als onderzoeksthema aangedragen bij de Rekenkamer Utrecht. In de bijeenkomst van de rekenkamer met de gemeenteraad in november 2019 bleek dat er bij de raadsleden vragen leven rondom informatieveiligheid, maar ook over de visie en aanpak van de gemeente Utrecht en de bewustwording binnen het gemeentelijk apparaat van de risico's. Daarbij was het de vraag wat de gemeente Utrecht doet ten opzichte van de Rijksoverheid en andere grote steden.

In dit onderzoeksplan werken we deze vragen rondom informatieveiligheid verder uit in een opzet voor een rekenkameronderzoek.

2. ACHTERGROND

Definitie informatieveiligheid

De begrippen informatieveiligheid en informatiebeveiliging worden vaak door elkaar gebruikt, afhankelijk van de context. Informatieveiligheid verwijst veelal naar het doel en informatiebeveiliging naar de instrumenten en maatregelen om dat doel te bereiken. De definitie van informatieveiligheid/informatiebeveiliging is: alles wat je doet om ervoor te zorgen dat informatie steeds toegankelijk is, dat de informatie klopt en dat de informatie niet bij anderen terecht komt. Het gaat daarbij vaak om een computersysteem, maar dat hoeft niet. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen. Informatiebeveiliging zorgt ervoor dat de gevolgen van problemen met informatie zoveel mogelijk beperkt worden.[1]

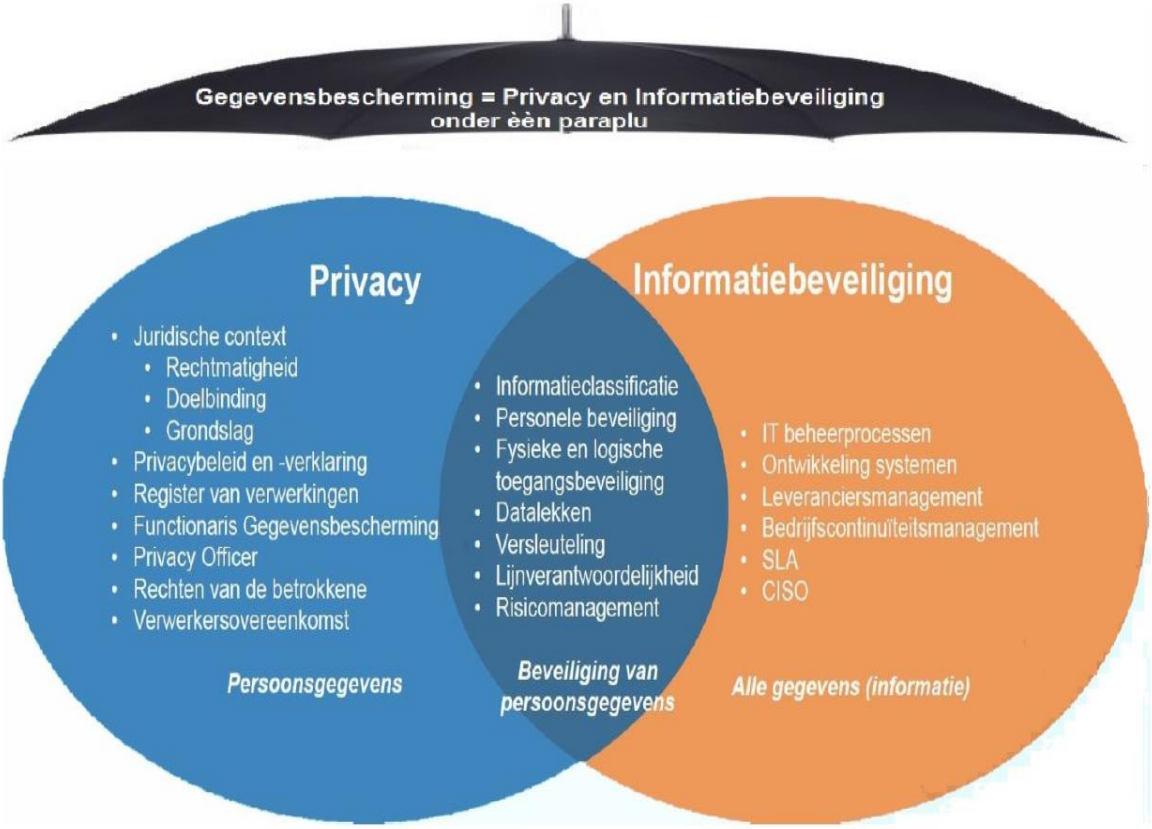
1 Cybersecurity Woordenboek van Cyberveilig Nederland (2019).

Binnen de gemeente Utrecht hoort informatiebeveiliging samen met het onderwerp privacy onder de paraplu gegevensbescherming[2], zie figuur 1. Deze indeling is gemaakt in het laatste beleidsplan, het 'Beleid voor gegevensbescherming 2019-2022'.

Informatiebeveiliging gaat over alle gegevens van de gemeente. Onderdelen van de informatiebeveiliging zijn bijvoorbeeld IT-beheerprocessen en de ontwikkeling van systemen. Privacy gaat over persoonsgegevens. Hieronder valt bijvoorbeeld het privacybeleid.

Waar privacy en informatiebeveiliging elkaar raken, gaat het over de beveiliging van persoonsgegevens. De beveiliging van de toegang tot de gegevens, versleuteling, risicomanagement en datalekken vallen onder dit onderwerp.

Figuur 1 Privacy en informatiebeveiliging beide onder gegevensbescherming



Bron: Gemeente Utrecht (2019). *Beleid voor gegevensbescherming 2019-2022*

[2] Gemeente Utrecht (2019). *'Gegevensbescherming in Utrecht'*. Jaarverslag van de Functionaris Gegevensbescherming, 2018

Stand van zaken
In het Jaarverslag van de Functionaris Gegevensbescherming (FG) over het jaar 2018 en de bijbehorende raadsbrief staat de stand van zaken rondom gegevensbescherming, en daarmee ook over informatieveiligheid, beschreven.

Een aantal highlights uit dit verslag en de raadsbrief:

- In 2018 is het beleidsplan geschreven, is de privacyverordening aangepast aan de AVG en is de FG bij de Autoriteit Persoonsgegevens (AP) aangemeld. Er is een Stuurgroep Gegevensbescherming gestart.
- De Stuurgroep Gegevensbescherming heeft een prioriteitenlijst met risico's voor de organisatie waar zij op sturen en een roadmap voor de uitvoering. Het risico rondom de uitwisseling van informatie met ketenpartners en andere externe partijen en het risico op ongeautoriseerde toegang tot gevoelige informatie staan bovenaan de prioriteitenlijst.
- In 2019 waren interne audits voorzien, die zijn echter door capaciteitsgebrek niet uitgevoerd. Ze staan voor 2020 en 2021 op de agenda. Wel heeft Interne Audit een toets uitgevoerd op de beveiliging van het SAP-systeem waarmee de gemeente haar financiële huishouding beheerst.
- In 2019 is er een plan gemaakt om met beperkte middelen een minimale bewustwordingscampagne voor medewerkers uit te voeren.

De FG doet in het verslag drie aanbevelingen:

- Neem interne audits m.b.t. gegevensbescherming als een vast onderdeel op in de jaarplanning.
- Onderschrijf het belang van het op een hoger niveau brengen van het bewustwordingsprogramma en van een intensievere inzet om datalekken te voorkomen.
- Stuur via de Stuurgroep Gegevensbescherming strak op de te behalen resultaten om de doelstellingen van de roadmap tijdig te halen.

Landelijke normen
Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO)[3] van kracht. De BIO vervangt de baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies (BIG). Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. De VNG heeft de BIO als standaard verklaard voor alle gemeenten en Utrecht heeft zich via een convenant hieraan verbonden. In het Jaarverslag 2019[4] staat dat Utrecht voorbereidingen heeft getroffen om in 2020 te voldoen aan de BIO.

In de BIO staat onder meer beschreven waar het informatiebeveiligingsbeleid aan moet voldoen, wat er georganiseerd moet zijn in de interne organisatie, welke eisen er zijn aan het werken met mobiele apparatuur, eisen aan (fysieke) toegangsbeveiliging en eisen rondom cryptografie.

3 Baseline Informatiebeveiliging Overheid: https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/
4 Jaarverslag 2019, paragraaf Bedrijfsvoering: https://utrecht.jaarverslag-2019.nl/p28556/bedrijfsvoering

De BIO is ook bedoeld als verantwoordingsmiddel voor informatiebeveiliging aan de gemeenteraad en toezichthouders binnen het Rijk. Vanaf 2020 wordt de BIO geïncorporeerd in de landelijke ENSIA verantwoordingsmethodiek. Het college legt jaarlijks via de verplichte ENSIA-zelfevaluatie verantwoording af over de stand van zaken van informatiebeveiliging ten opzichte van de BIG (tot en met 2019) of de BIO (vanaf 2020). Er is in Utrecht in april een raadsbrief verschenen over de ENSIA verantwoording 2019. Daarin staan per onderdeel tabellen opgenomen die laten zien aan hoeveel van de normen de gemeente voldoet, volgens de auditor of naar aanleiding van een zelfevaluatie. De gemeente voldoet aan het grootste deel van de normen. Voor alles wat niet aan de normen voldoet, geldt dat er komend jaar verbetermaatregelen worden doorgevoerd.

3. DOEL EN ONDERZOEKSVRAGEN

Het doel van de rekenkamer is om de gemeenteraad inzicht te geven in de manier waarop de gemeente Utrecht invulling geeft aan de informatieveiligheid. We kijken daarbij naar drie aspecten; organisatie/proces, mens en techniek.

De centrale vraag van het onderzoek is:
Is de informatieveiligheid bij de gemeente Utrecht voldoende gewaarborgd?

Deze centrale vraag is uitgewerkt in de volgende onderzoeksvragen:

1. (Organisatie/proces:) Wat doet de gemeente Utrecht op het gebied van informatieveiligheid?
    a. Welk beleid voert de gemeente op informatieveiligheid?
    b. Welke risico's en maatregelen heeft de gemeente benoemd?
    c. In hoeverre zijn de maatregelen geïmplementeerd?
2. (Mens:) Op welke manier zet de gemeente in op het bewust omgaan met informatie? Hoe gaan de medewerkers van de gemeente in de praktijk om met informatieveiligheid?
3. (Techniek:) Zijn gegevens bij de gemeente voldoende beschermd tegen de toegang door onbevoegden? Zo niet, wat zijn daarvan de gevolgen voor burgers en ondernemers? Wat zijn de risico's en kwetsbaarheden?
4. Welke (verdere) maatregelen zijn mogelijk om de informatieveiligheid te optimaliseren?

Analyse- en normenkader
Vertrekpunt is de indeling organisatie-mens-techniek. Daarnaast kijken we naar de bepalingen in de wet- en regelgeving (BIO) en de gemeentelijke beleidsdocumenten zoals beleidsnota's, raads- en commissiebrieven. Ook zal gebruik gemaakt worden van ander rekenkameronderzoek en vakliteratuur op het terrein van informatieveiligheid, bijvoorbeeld van de Informatiebeveiligingsdienst (IBD).

Onderdeel	Vraag	Norm	Aspecten / criteria
Organisatie/ proces 	1	De gemeente werkt risicogestuurd.	De gemeente heeft de risico's in beeld.
			De gemeente neemt maatregelen om de risico's te laten afnemen.
Mens 	2	De gemeente zorgt voor het informatiebewustzijn van medewerkers.	Er is een plan/programma voor medewerkers over informatiebewustzijn, dat medewerkers in staat stelt om op een bewuste manier om te gaan met informatie.
		Medewerkers gaan in de praktijk bewust met informatie/gegevens om.	Medewerkers weten wat ze wel en niet mogen/moeten doen met informatie/gegevens en herkennen incidenten, dit is te relateren aan de leerdoelen van de instructies/opleiding.
Techniek 	3	Informatie/gegevens zijn goed beschermd tegen inbraak van buitenaf.	Systemen/applicaties doorstaan pentesten.
			Medewerkers hebben een thuiswerkplek met adequate beveiliging.

Dit is een eerste aanzet tot het normenkader. De beoordelingscriteria die wij gebruiken bij het beantwoorden van de onderzoeksvragen zullen tijdens het onderzoek nader worden uitgewerkt.

4. PLAN VAN AANPAK

Hieronder schetsen we de globale aanpak van het onderzoek per onderzoeksvraag.

Vraag 1. Organisatie/proces

Om het beleid en de organisatie rondom informatieveiligheid in de gemeente Utrecht in kaart te brengen voeren wij een **documentenstudie** uit. We bestuderen in ieder geval het beleid dat door de gemeente is vastgesteld. De risico's die geïdentificeerd zijn, worden door de rekenkamer ingezien aan de hand van de risicorapportages die door de gemeente zijn opgesteld. Wij betrekken daarbij ook de uitkomsten van door de gemeente uitgevoerde beveiligingstesten, zelfassessments en audits. Hierbij bekijken we specifiek de systemen die de pentesten zullen ondergaan (zie vraag 3). Daarnaast analyseren wij de beheersmaatregelen die de gemeente Utrecht heeft genomen of voornemens is te nemen. We bekijken, indien aanwezig, documenten over datalekken van de afgelopen jaren. De menskracht en het geld die voor gegevensbescherming – en in het bijzonder informatieveiligheid – beschikbaar zijn, zullen wij globaal met de hulp van **interviews** inzichtelijk maken. Wij voeren in ieder geval gesprekken met de medewerkers van de gemeente die deel uitmaken van de stuurgroep gegevensbescherming. We gaan hierbij ook na waar en op welke manier rollen, taken en bevoegdheden zijn vastgelegd en toegekend.

Vraag 2. Mens

Door middel van **documentenstudie** en **interviews** gaan we na hoe bewustwording onder medewerkers onderdeel uitmaakt van het beleid en de uitvoering. Wij gaan hierover in gesprek met medewerkers die verantwoordelijk zijn voor informatieveiligheid bij de gemeente of taken uitvoeren die op dit gebied. Vervolgens gaan we in een (digitale) **enquête** onder medewerkers na hoe dit in de praktijk wordt ingevuld en ervaren. Daarbij besteden we ook aandacht aan de nieuwe werkwijze bij de gemeente Utrecht waar thuis werken een wezenlijk onderdeel van is.

Vraag 3. Techniek

Voor het uitvoeren van **testen** op het oneigenlijk toegang verkrijgen tot gegevens wordt een externe partij ingezet. Wij hebben hen gevraagd om de volgende testen uit te voeren:

- Social engineering test: dit onderdeel kan bestaan uit een voice phishing test (telefonisch) of een spear phishing test (per e-mail) waarmee verzocht wordt om vertrouwelijke gegevens te delen, het verspreiden van usb-sticks die bij gebruik malware installeren en/of een inlooptest waarbij onbekende gasten ongeautoriseerd toegang proberen te verkrijgen tot een kantoorruimte.
- Penetratietesten (pen-testen): intern en extern. Bij de interne penetratietest wordt vanaf een gemeentelijke locatie (een werkruimte) gepoogd oneigenlijke toegang tot informatie te krijgen. Bij de externe test wordt vanaf een niet-gemeentelijke locatie via internet geprobeerd om oneigenlijk toegang te verkrijgen.

Er wordt ook specifiek aandacht besteed aan de risico's die werken vanuit huis met zich meebrengen. Waar mogelijk zullen ook daar testen uitgevoerd worden.

De uitvoering van dit onderdeel vindt pas plaats na overleg met de gemeente Utrecht en na het opstellen en tekenen van een vrijwaringsovereenkomst tussen de

gemeente, de rekenkamer en de geselecteerde externe partij. De gemeente Utrecht zal voorafgaand aan de testen op de hoogte gesteld worden van de activiteiten en er wordt gewaakt voor schade of verstoring van de bedrijfsprocessen. Daarnaast dient de externe partij vertrouwelijk met de eventueel verkregen informatie om te gaan. Medewerkers die oneigenlijk toegang verschaffen of vertrouwelijke informatie delen zullen niet met naam worden genoemd. Als uit de testen grote beveiligingsrisico's naar voren komen, melden wij deze direct aan de verantwoordelijken bij de gemeente Utrecht.

Analyse en rapportage

We leggen de uitkomsten van de analyses vast in een nota van bevindingen. Deze leggen wij voor ambtelijk wederhoor voor aan de gemeente. Aansluitend stelt de rekenkamer een bestuurlijke nota op met conclusies en aanbevelingen. Daarbij besteden wij ook aandacht aan de maatregelen die mogelijk zijn om de informatieveiligheid te optimaliseren. Samen met de definitieve nota van bevindingen – na verwerking van de ambtelijke reactie – leggen wij het geheel voor aan het college van burgemeester en wethouders (B&W) voor een bestuurlijke reactie. Met de bestuurlijke reactie maakt de rekenkamer het definitieve rapport op – inclusief nawoord – en biedt dit aan de gemeenteraad en het college van B&W aan en zorgt voor verdere openbaarmaking.

5. AFBAKENING

Het onderzoek richt zich op informatieveiligheid. We hebben gekozen voor de focus op de onderdelen organisatie/proces, mens en techniek, waarbij de nadruk zal liggen op mens en techniek. We willen met name weten hoe het er nu voor staat. Wat de gemeente doet als het toch onverhoopt misgaat, bijvoorbeeld bij een datalek, hackaanval of storing, nemen we niet in dit onderzoek mee.

Bij het onderdeel organisatie/proces kijken we met name naar wat er wordt gedaan op het gebied van informatieveiligheid. Het gaat erom een beeld te geven op hoofdlijnen. We gaan geen risicoanalyses en audits overdoen, maar bekijken wat er ligt en welke maatregelen de gemeente neemt. Hierbij nemen we ook de activiteiten die de gemeente onderneemt rondom de BIO en ISO in de analyse mee.

Bij het onderdeel mens bekijken we de inzet van de gemeente om de medewerkers bewust te laten omgaan met informatie. We bezien hier per organisatieonderdeel op welke manier zij bijdragen. We denken bijvoorbeeld aan welke campagnes er zijn geweest en wanneer, hoe medewerkers worden gescreend en opgeleid om op een goede manier met informatie om te gaan, en hoe gezorgd wordt voor een veilige werkomgeving. We bekijken op hoofdlijnen de inhoud van de activiteiten, maar beoordelen deze niet op detailniveau en ook niet onderwijskundig.

Voor het onderdeel techniek geldt dat we social engineering testen en pentesten (laten) uitvoeren. Bij dit soort testen wordt veelal gewerkt met een tijdslimiet; lukt het om binnen X uur/dagen aan informatie te komen? De afbakening van dit onderdeel zit dan ook voor een deel in tijd. Daarnaast houden we rekening met de activiteiten die de gemeente Utrecht zelf uitvoert in de onderzoeksperiode.

Onderdeel van de vraag vanuit de gemeenteraad is een vergelijking met andere gemeenten. We geven in de rapportage beknopt aan in hoeverre de bevindingen in Utrecht overeenkomen of verschillen met die in andere gemeenten die een rekenkameronderzoek over informatieveiligheid hebben uitgevoerd, zoals Rotterdam en Den Haag. Hiervoor bekijken we de rapportages van die rekenkamers. We houden de vergelijking beknopt, omdat de vergelijking naar verwachting niet één-op-één te maken valt doordat de organisatie en het IT-landschap in ieder gemeente anders zijn en doordat de rekenkameronderzoeken uit de genoemde gemeenten al van een aantal jaren geleden zijn.

6. ORGANISATIE EN PLANNING

De volgende personen van de rekenkamer voeren het onderzoek uit:

- Naomi Meys, onderzoeker en projectleider
- Johan Snoei, senior onderzoeker
- Pauline de Jong, onderzoeker

Voor een deel van het onderzoek is expertise nodig op informatieveiligheid. Hiervoor zullen de werkzaamheden bij een extern bureau worden belegd.

Planning

Publicatie van het eindrapport is voorzien in het eerste kwartaal 2021. De (indicatieve) planning van het onderzoek is als volgt:

Stap in onderzoeksproces	Periode
Documentstudie	Q3&4 2020
Digitale enquête onder medewerkers	Q4 2020
Interviews	Q4 2020
Pentesten door extern bureau	Q4 2020
Analyse en rapportage	Q4 2020
Ambtelijk wederhoor	Q4 2020 / Q1 2021
Bestuurlijk wederhoor	Q1 2021
Beoogde publicatie	Q1 2021

Contactpersonen

Voor meer informatie kunt u contact opnemen met:

- Naomi Meys, onderzoeker en projectleider, naomi.meys@utrecht.nl, 06 – 55 55 84 22
- Gerth Molenaar, secretaris rekenkamer, g.molenaar@utrecht.nl, 030-286 1391