ONDERZOEKSPLAN OPVOLGINGSONDERZOEK INFORMATIEVEILIGHEID

REKEN KAMER UTRECHT

ONDERZOEKSPLAN OPVOLGINGSONDERZOEK INFORMATIEVEILIGHEID

20 februari 2024

1 INLEIDING

Gemeenten verwerken steeds grotere hoeveelheden informatie in allerlei systemen en programma's. Deze informatie bevat vaak (bijzondere) persoonsgegevens die goed beschermd moeten zijn. De informatieveiligheid moet daarom voldoende geborgd zijn. In 2021 voerde Rekenkamer Utrecht onderzoek uit naar de manier waarop de gemeente Utrecht invulling geeft aan de informatieveiligheid. De uitkomsten gaven ons aanleiding om het onderwerp te blijven volgen. Ook gaven we al in ons bestuurlijk rapport aan op een later moment de verschillende testen te gaan herhalen. In het voorliggend plan werken we de achtergrond, het doel en de onderzoeksvragen en het plan van aanpak voor dit opvolgingsonderzoek verder uit.

2 ACHTERGROND

Verschillende momenten maken opvolging aanbevelingen zichtbaar
Op 7 april 2021 publiceerde de rekenkamer de uitkomsten van het onderzoek naar de informatieveiligheid bij de gemeente Utrecht. Het rapport is tijdens een technische bijeenkomst op 13 april 2021 aan de Utrechtse gemeenteraad gepresenteerd. Vervolgens werd het op 29 april 2021 behandeld in de commissie Mens & Samenleving en op 3 juni 2021 in de gemeenteraad. De raad heeft het raadsvoorstel unaniem aangenomen.

Op 9 juli 2021 ontving de raad de raadsbrief 'Plan van aanpak bij het rekenkameronderzoek'. Het college informeerde de raad daarmee over de wijze waarop zij het raadsbesluit over de aanbevelingen van de rekenkamer wilde uitvoeren. Gelijktijdig heeft het college de raad het jaarverslag gegevensbescherming 2021 aangeboden. Op 2 september 2021 verscheen in reactie op deze beide documenten een rekenkamerbrief. In januari 2022 heeft het college enkele actiepunten uit de rekenkamerbrief nader toegelicht in een raadsbrief.

Op 14 april 2022 heeft de fractie van de VVD schriftelijke vragen gesteld over de stand van zaken. Deze zijn op 18 mei 2022 beantwoord. Meest recent is op 10 oktober 2023 een raadsbrief toegestuurd waarin door het college een update wordt gegeven over de stand van zaken in de opvolging van het raadsbesluit.

Naast deze schriftelijke doorwerking zijn ook in de praktijk en fysieke omgeving verschillende maatregelen genomen die zichtbaar opvolging geven aan de aanbevelingen van het rekenkameronderzoek. Enkele belangrijke voorbeelden zijn de vervanging van de werkstations (*thin clients*) van de medewerkers, het toepassen van multifactor-authenticatie bij het inloggen en de aanpassingen aan de fysieke toegang op het Stadhuis.

Informatieveiligheid raakt aan organisatie en processen, mens en techniek
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 die wij hanteren 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]

In ons onderzoek van 2021 hebben we onze focus gelegd op drie onderdelen: 1) organisatie en proces, 2) mens en 3) techniek. Met de nadruk op mens en techniek. Ook in het opvolgingsonderzoek zullen we deze onderdelen als uitgangspunt nemen. Daarnaast zijn er vanuit de raadsbehandeling van het rapport een aantal onderwerpen naar voren gekomen die we in dit opvolgingsonderzoek een plaats willen geven. Het gaat dan om:

- De afhandeling van incidenten en meldingen.
- De governance en managementinformatie.
- Het gebruik en de veiligheid van telefoons.

Samenvattend
Gegeven het groeiende belang van informatieveiligheid en de eerdere uitkomsten van het rekenkameronderzoek heeft de rekenkamer in het nawoord op de bestuurlijke reactie in 2021 al aangegeven het onderwerp te blijven volgen en een opvolgingsonderzoek te zullen uitvoeren. Uit verschillende raadsbrieven en de verkennende gesprekken die wij hebben gevoerd is op te maken dat de gemeente stappen heeft gezet, maar het is de vraag hoe deze in de praktijk zijn uitwerking hebben. En of het gewenste effect ook bereikt wordt. Daarom zullen wij dit in de eerste helft van 2024 nader (laten) onderzoeken.

3 DOEL EN ONDERZOEKSVRAGEN

Het doel van dit onderzoek is om de Utrechtse gemeenteraad inzicht te geven in de mate waarin de besluiten naar aanleiding van het rekenkamerrapport “Zo sterk als de zwakste schakel” zijn opgevolgd. Daarnaast besteden we aandacht aan enkele aanvullende onderwerpen die in het onderzoek uit 2021 onderbelicht waren gebleven.

De centrale vraag van het onderzoek luidt:

> In hoeverre heeft de gemeente Utrecht uitvoering gegeven aan de aanbevelingen van het rekenkameronderzoek uit 2021 en is de informatieveiligheid nu voldoende gewaarborgd?

[1] Cybersecurity Woordenboek van Cyberveilig Nederland (2021)

Deze centrale vraag werken we uit aan de hand van vier onderzoeksvragen:

1) Organisatie/proces:
    a. In hoeverre zijn de aanbevelingen/beslispunten over het onderdeel organisatie en proces door de gemeente Utrecht opgevolgd?
    b. Aanvullend: In hoeverre zijn de afhandeling van incidenten en meldingen, de managementinformatie en het incidentenmanagementproces adequaat?
2) Mens:
    a. In hoeverre zijn de aanbevelingen over het onderdeel mens door de gemeente Utrecht opgevolgd?
3) Techniek:
    a. In hoeverre zijn de aanbevelingen over het onderdeel techniek door de gemeente Utrecht opgevolgd?
    b. Aanvullend: in hoeverre is bij het gebruik van gemeentelijke telefoons en bij het thuiswerken de informatieveiligheid technisch beveiligd?
4) Welke (verdere) maatregelen zijn mogelijk om de informatieveiligheid te optimaliseren?

Normenkader

Bij de beantwoording van deze onderzoeksvragen – in termen van bevindingen – hanteren wij een normenkader. In tabel 1 is een eerste concept uitgewerkt. In de eerste fase van het onderzoek bespreken we dit in een startgesprek met de gemeentelijke contactpersonen en maken het normenkader vervolgens definitief. Deze normen nemen we mee in het onderzoek. In de nota van bevindingen zetten wij de uitvoering af tegen deze normen, wat leidt tot bevindingen en een beoordeling.

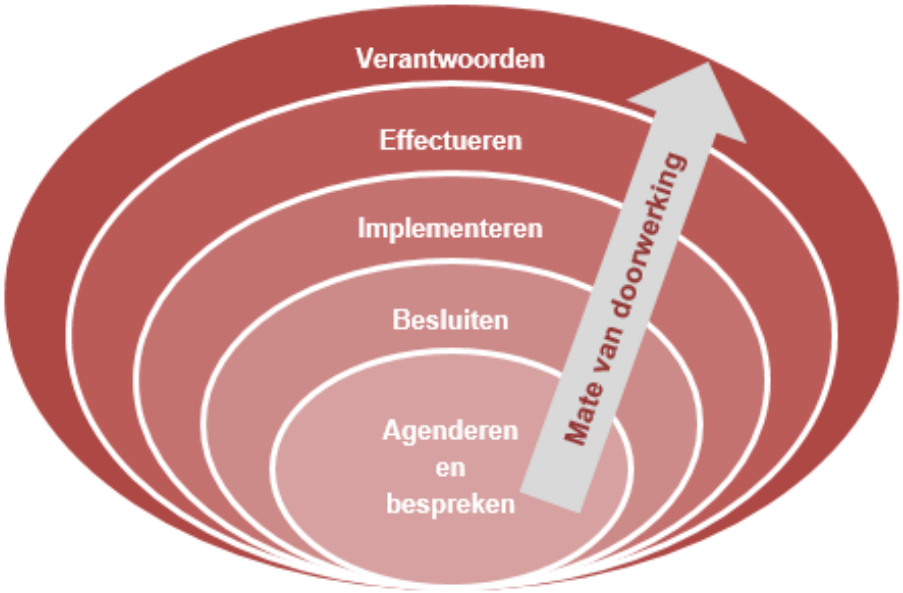
Tabel 1 *Conceptnormenkader opvolgingsonderzoek informatieveiligheid*

Vraag	Norm	Uitwerking
1. Organisatie en proces	De gemeente Utrecht werkt risicogestuurd.	De gemeente heeft de risico's in beeld.
		De gemeente neemt maatregelen om de risico's te laten afnemen.
		Er wordt over het functioneren van de informatiebeveiliging gerapporteerd aan het management, bij voorkeur op basis van een ISMS (Information Security Management System).
		De gemeente gebruikt incidentmeldingen om te leren en de informatieveiligheid te verbeteren.
2. Mens	De gemeente zorgt voor het informatiebewustzijn van medewerkers	Het plan over informatiebewustzijn is concreet en stelt medewerkers in staat om op een bewuste manier om te gaan met informatie.
		Medewerkers nemen deel aan de E-learning en andere trainingen rondom informatieveiligheid.

	De medewerkers gaan in de praktijk bewust en veilig om met informatie	Medewerkers weten wat ze wel en niet mogen doen met informatie.
		Medewerkers gaan niet in op verzoeken van externen om informatie te delen of gegevens af te staan.
		Medewerkers weten wat ze moeten doen bij incidenten en melden deze ook.
3. Techniek	Informatie is goed beschermd tegen inbraak	Systemen en applicaties doorstaan externe penetratietesten
		Systemen en applicaties doorstaan interne penetratietesten
		De fysieke beveiliging van het Stadhuis en Stadskantoor voorkomen dat *mystery quests* toegang kunnen krijgen tot (geheime of vertrouwelijke) informatie.
		De thuiswerkplekken van medewerkers zijn op adequate manier beveiligd.
4. Beoordeling opvolging aanbeveling	De gemeente heeft opvolging gegeven aan de aanbevelingen van het rekenkameronderzoek uit 2021.	De beslispunten zijn door het college uitgevoerd in de organisatie, beleid en uitvoering.
		Het rapport heeft effecten op het beleid en draagt bij aan de gewenste maatschappelijke effecten.
		Het college heeft verantwoording afgelegd aan de gemeenteraad over de opvolging van het raadsbesluit.
		De gemeenteraad heeft toegezien of het besluit de gewenste navolging heeft gekregen en of de besluiten de gewenste resultaten heeft opgeleverd.

Bij de analyse van de doorwerking zullen wij het analyseschema hanteren zoals wij dat hebben ontworpen voor het opvolgingsonderzoek uit 2020. Dit schema is gebaseerd op het NVRR model en benoemt verschillende fasen van doorwerking die gerelateerd zijn aan het proces van onderzoek, raadsbehandeling en opvolging van het raadsbesluit. Het gaat dan om het agenderen en bespreken, besluiten, implementeren, effectueren en publiek verantwoorden.

Figuur 2 *Cirkels van doorwerking NVRR*



Wat verstaan wij onder deze begrippen?

- Agendering en bespreking: is er in de politiek-bestuurlijke context aandacht voor het onderzoek en het rapport en vindt er een goede bespreking plaats van het rapport en de conclusies en aanbevelingen van de rekenkamer? Het agenderen en bespreken heeft zowel betrekking op de voorbereiding en uitvoering van het onderzoek als op de behandeling van het rapport. De programmering van onderzoek valt hier onder, maar ook het ambtelijk en bestuurlijk wederhoor, het presenteren van uitkomsten aan de raad, het agenderen door middel van een raadsvoorstel en de behandeling door de raad in een commissie- en raadsvergadering.
- Besluitvorming: is er besluitvorming door de gemeenteraad over het rekenkamerrapport en het raadsvoorstel met aanbevelingen en zijn hierbij moties of amendementen aangenomen?
- Implementeren: zijn de aanbevelingen/beslispunten van het raadsbesluit door het college van B&W en de ambtelijke organisatie doorgevoerd in de organisatie, beleid en/of uitvoering? Hieronder valt ook of het college een plan van aanpak opstelt, hoe de opvolging intern is georganiseerd, of de rekenkamer acties onderneemt om de opvolging te bevorderen, en of de opvolging van het raadsbesluit geleid heeft tot aanpassing van beleid of werkwijzen.
- Effectueren: wat is het effect van het opvolgen van de raadsbesluiten over rekenkameronderzoek op de resultaten van het beleid en op het realiseren van beoogde maatschappelijke effecten van het beleid?
- Publiek verantwoorden: dit heeft op diverse partijen betrekking. De rekenkamer informeert het publiek over de uitvoering en uitkomsten van het onderzoek. Het college moet verantwoording aan de raad afleggen over de opvolging van het raadsbesluit. De raad heeft een controlerende en kaderstellende rol en ziet er op toe of haar besluiten de beoogde navolging krijgen binnen de door de raad gestelde kaders en of deze besluiten het gewenste resultaat opleveren.

4 PLAN VAN AANPAK EN AFBAKENING

Wij voeren het onderzoek uit aan de hand van vier onderzoekstappen (zie figuur 4). Deze stappen worden hieronder kort toegelicht.

Figuur 4 *Aanpak van het onderzoek in vier stappen.*

1. *Documentstudie*
   Wij richten ons bij de documentstudie op het beleid voor gegevensbescherming van de gemeente Utrecht en de verdere uitwerking daarvan in bijvoorbeeld programma's, richtlijnen en protocollen. We bestuderen daarnaast ook de beschikbare managementinformatie om een beeld te krijgen van de interne informatievoorziening.

2. *Interviews professionals bij de gemeente*
   Wij gaan binnen de gemeentelijke organisatie in gesprek met de medewerkers die verantwoordelijk zijn voor de informatieveiligheid. We denken daarbij op voorhand aan de leden van de stuurgroep, de regiegroep, maar ook integraal resultaatverantwoordelijk managers (IRM-ers) en medewerkers van DomstadIT. We gaan met hen in gesprek over de drie onderdelen van informatieveiligheid en hun ervaringen daarbij. Daarnaast gaan we waar mogelijk in op de manier waarop het rekenkameronderzoek van 2021 heeft doorgewerkt op hun werkzaamheden en welke verbetermogelijkheden zij nog zien voor de toekomst.

3. *Testen*
   We zetten een externe partij in voor het uitvoeren van testen op het oneigenlijk toegang verkrijgen tot gegevens. Wij vragen hen om dezelfde testen uit te voeren als in het onderzoek van 2021. Het gaat om de volgende testen:

- 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.

- 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.

Er zal ook specifiek aandacht besteed aan de risico's die werken vanuit huis met zich meebrengen. De daarvoor benodigde apparatuur – laptops, telefoons – zullen daarom ook onderdeel uitmaken van de testen.

De uitvoering van dit onderdeel vindt evenals in 2021 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. In tegenstelling tot destijds zal de gemeente Utrecht zal bij dit opvolgingsonderzoek niet voorafgaand aan de testen op de hoogte gesteld worden dat de testen zullen plaatsvinden. Wel delen we voorafgaand aan de periode waarin de testen zullen plaatsvinden de activiteiten die bij dit onderdeel zullen worden uitgevoerd 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. De resultaten van de testen en daaruit voortkomende beveiligingsrisico's, melden wij direct aan de verantwoordelijken bij de gemeente Utrecht.

4. *Overkoepelende analyse en rapportage*
   Wij analyseren de verzamelde informatie en brengen die in verband met de vooraf vastgestelde normen. De normenbeoordelingen leggen wij vervolgens vast in een conceptnota van bevindingen en leggen die voor aan de ambtelijke organisatie voor feitelijk wederhoor. Na verwerking van de ambtelijke reactie stelt de rekenkamer een bestuurlijk rapport op met conclusies en aanbevelingen. Het geheel wordt vervolgens voorgelegd aan het college van burgemeester en wethouders voor bestuurlijk wederhoor. De rekenkamer maakt daarna het definitieve rapport op met een nawoord, biedt het geheel aan de gemeenteraad aan en zorgt voor verdere openbaarmaking.

Afbakening

Wij houden in de afbakening in ieder geval met de volgende zaken rekening:

- Met dit onderzoek kijken we naar drie eerdergenoemde onderdelen: organisatie/proces, mens en techniek. Daarbij gaan wij per onderdeel specifiek aandacht besteden aan aanvullende onderwerpen die onder andere bij de behandeling in 2021 zijn benoemd.

- De focus van ons onderzoek richt zich op de periode vanaf de uitvoering van het eerdere onderzoek (najaar 2020) tot op heden.
- We voeren geen aanvullende risicoanalyses en audits uit, maar maken gebruik van de informatie die er op dit onderdeel al ligt en welke maatregelen de gemeente naar aanleiding van de analyses heeft genomen.
- Er zal geen vergelijking plaatsvinden met andere gemeenten. Het terrein is continue in beweging en ook de inrichting van de organisatie en systemen verschillen sterk. Bij het eerdere onderzoek bleek al dat de situatie bij andere gemeente te afwijkend was om een goede inhoudelijke benchmark te kunnen maken.
- De beoordeling van de doorwerking richten we op de onderdelen implementeren, effectueren en (publiek) verantwoorden.

5 ORGANISATIE EN PLANNING

De volgende personen van de rekenkamer voeren het onderzoek uit:
- Johan Snoei, projectleider / onderzoeker
- Vince van Houten, onderzoeker

Planning
Ons doel is om de nota van bevindingen in het derde kwartaal 2024 af te hebben en het onderzoek vervolgens in zijn geheel af te ronden en te publiceren. De uitkomsten komen daarmee halverwege de huidige raadsperiode zodat waar nodig nog kan worden bijgestuurd.

Stappen	**Periode**
Documentenstudie	1e en 2e kwartaal 2024
Interviews professionals	1e en 2e kwartaal 2024
Pentesten	2e kwartaal 2024
Opstellen nota van bevindingen	2e kwartaal 2024
Feitelijk wederhoor	2e kwartaal 2024
Verwerking wederhoor en opstellen bestuurlijk rapport	3e kwartaal 2024
Bestuurlijk wederhoor	3e kwartaal 2024
Beoogde publicatie	3e kwartaal 2024

Contactpersonen
Voor meer informatie kunt u contact opnemen met:
- Johan Snoei, onderzoeker en projectleider, j.snoei@utrecht.nl , 06 – 34 61 22 80
- Gerth Molenaar, secretaris rekenkamer, g.molenaar@utrecht.nl , 06 – 49 75 43 00