

Voorstel aan de gemeenteraad

Rekenkamerrapport: *De mens als zwakste schakel*

Beleidsvelden	Personeel en Organisatie
Organisatieonderdeel	Informatie en procesmanagement (IPM) en Mens en Organisatie
Opsteller	Johan Snoei
Kenmerk	30032582
Vergaderdatum Raad	Volgt
Geheim	Nee

De rekenkamer stelt de raad voor te besluiten om het college van burgemeester en wethouders het volgende te verzoeken:

1. De resterende technische risico's en kwetsbaarheden zo spoedig mogelijk te beheersen.
2. Verdere maatregelen uit te voeren om de fysieke beveiliging van gebouwen en het informatiebewustzijn van medewerkers te vergroten.
3. Binnen de hele organisatie op de lange termijn in te zetten op een cultuurverandering.
4. Te zorgen voor meer centrale aansturing van het informatieveiligheidsbeleid.
5. De raad binnen zes weken door middel van een plan van aanpak te informeren over de wijze waarop deze aanbevelingen worden uitgevoerd.

De rekenkamer,

de secretaris,

dr. G. Molenaar

de voorzitter,

drs. P.W.D. Venhoeven

Samenvatting

De Rekenkamer Utrecht heeft een opvolgingsonderzoek gedaan naar de informatieveiligheid van de gemeente Utrecht. De resultaten hiervan zijn vastgelegd in het rapport *De mens als zwakste schakel*.

Context

Aanleiding

Gemeenten verwerken steeds grotere hoeveelheden informatie. De laatste decennia gebeurt dat in allerlei gedigitaliseerde en geautomatiseerde systemen en programma's. De verwerkte informatie bevat vaak (bijzondere) persoonsgegevens die goed beschermd moeten zijn. De informatieveiligheid moet daarom op alle aspecten – in organisatie en proces, bij de medewerkers en in de techniek – voldoende geborgd zijn. In 2021 voerde Rekenkamer Utrecht onderzoek uit naar de manier waarop de gemeente Utrecht invulling gaf aan de drie aspecten van informatieveiligheid. De uitkomsten gaven ons aanleiding om het onderwerp te blijven volgen. We gaven in ons bestuurlijk rapport daarom aan op een later moment (na ongeveer een jaar) een opvolgingsonderzoek uit te gaan voeren. In september 2022 heeft concernaudit een follow-up audit uitgevoerd naar de stand van zaken van de uitvoering van het raadsbesluit. Mede op basis daarvan besloot de rekenkamer om het aangekondigde opvolgingsonderzoek uit te stellen. Uiteindelijk heeft de rekenkamer in de periode februari tot en met juli 2024 onderzoek gedaan naar de opvolging van aanbevelingen uit 2021 en de actuele stand van zaken van de informatieveiligheid.

Juridische context

De Rekenkamer Utrecht is een onafhankelijk bestuursorgaan van de gemeente Utrecht, met een grondslag in de gemeentewet (artikel 81 en 182-185). De rekenkamer heeft taken en bevoegdheden op een bij wet duidelijk afgebakend terrein. De rekenkamer onderzoekt de doelmatigheid, doeltreffendheid en rechtmatigheid van het door het gemeentebestuur gevoerde bestuur (gemeentewet, artikel 182). Een door de rekenkamer ingesteld onderzoek naar de rechtmatigheid van het door het gemeentebestuur gevoerde bestuur bevat daarbij geen controle van de jaarrekening aangezien dat het werkterrein is van de accountant. De gemeenteraad heeft binnen de kaders van de wet voor Rekenkamer Utrecht het juridisch kader nader vastgelegd in de Verordening Rekenkamer Utrecht (Gemeentebblad nr. 473707, 7 november 2023).

Beoogd effect

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 aanvullende onderwerpen die in het onderzoek uit 2021 onderbelicht waren gebleven. Het gaat onder meer om de managementinformatie, de afhandeling van incidenten, het gebruik van de gemeentelijke telefoons en de maatregelen om het thuiswerken te beveiligen.

De centrale vraag van het onderzoek was:

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

Eerdere besluitvorming en informatievoorziening aan de raad

Op 3 juni 2021 heeft de gemeenteraad ingestemd met het [raadsbesluit](#) bij het rekenkameronderzoek *Zo sterk als de zwakste schakel*. Tijdens de behandeling van het rekenkamerrapport deed de wethouder een aantal toezeggingen aan de gemeenteraad. Twee van die toezeggingen kwamen niet in het gemeentelijke [plan van aanpak](#) van 9 juli 2021 terug. In de [rekenkamerbrief](#) van september 2021 waarin wij onze visie op het plan van aanpak gaven wezen wij daarop. Het college heeft daarop in januari 2022 in een [raadsbrief](#) aangegeven in welke mate zij aan de gedane toezeggingen invulling zou gaan geven.

Vervolgens heeft het college in juni 2022 in de Jaarstukken 2021 de gemeenteraad per aanbeveling beknopt geïnformeerd over de planning en stand van zaken van de uitvoering. Daarna is in oktober 2022 het [Jaarverslag Gegevensbescherming 2021](#) gepubliceerd, waarin de gemeentelijke organisatie verantwoording aflegde aan de gemeenteraad over de ontwikkelingen in 2021 op het gebied van

gegevensbescherming. Meest recent is de [raadsbrief](#) van oktober 2023 waarin het college een update heeft gegeven van de opvolging van het raadsbesluit.

Sinds de raadsbehandeling van het rekenkamerrapport is door de gemeenteraad niet meer over het onderwerp gedebatteerd. In april 2022 heeft de VVD-fractie nog wel schriftelijke vragen aan het college gesteld over het gebruik van ethische hackers. Daarin wordt het college onder andere gevraagd naar de voortgang op de acties die zijn en worden ondernomen naar aanleiding van het rekenkamerrapport. Deze vragen zijn in mei 2022 door het college [beantwoord](#).

Beslispunten, Argumenten en Kanttekeningen/Risico's

Beslispunt	
1	De resterende technische risico's en kwetsbaarheden zo spoedig mogelijk te beheersen.
Argumenten	
1.1	Vrijwel alle technische risico's die in 2021 nog openstonden zijn opgelost. Er zijn daarmee geen kritieke risico's meer aanwezig.
1.2	Uit de nieuwe penetratietesten van dit onderzoek bleek wel dat er nog altijd verouderde software aanwezig is. Dit krijgt te weinig aandacht.
1.3	De verouderde software die aanwezig is, wordt niet langer onderhouden, wordt daardoor kwetsbaar en kan door hackers worden uitgebuit.
1.4	De laptops en telefoons die door de gemeente worden beheerd en uitgegeven blijken technisch goed beveiligd.
1.5	Door de invoering van multi-factor authenticatie is de informatieveiligheid bij het thuis- en op afstand werken van medewerkers sterk verbeterd.
Beslispunt	
2	Verdere maatregelen uit te voeren om de fysieke beveiliging van gebouwen en het informatiebewustzijn van medewerkers te vergroten.
Argumenten	
2.1	Er is geïnvesteerd in de fysieke beveiliging van de gemeentelijke gebouwen.
2.2	Het lukte de insluipers van het door de rekenkamer ingehuurde bureau bij de inlooptesten vrijwel altijd om het Stadskantoor binnen te komen.
2.3	De fysieke beveiliging van het Stadhuis is door de grote inspanningen sinds 2021 sterk verbeterd. Indringen was daardoor lastig, maar niet onmogelijk doordat medewerkers nog altijd onoplettend waren.

2.4	Er zijn veel maatregelen genomen om het informatiebewustzijn van medewerkers te vergroten, maar dit levert nog te weinig resultaten op omdat de uitvoering vrijblijvend is.
2.5	Deelname aan de e-learning is te laag en er zijn aanzienlijke verschillen tussen de organisatieonderdelen.
2.6	Raads-, commissie- en fractieleden worden zelfs helemaal niet uitgenodigd voor de e-learning. Dit geldt ook voor de leden van de rekenkamer.
2.7	De e-learning biedt inhoudelijk te weinig maatwerk waardoor de aanpak niet altijd aansluit op de behoefte van de verschillende organisatieonderdelen.
2.8	Medewerkers trappen nog steeds in USB-dropping en staan hun gegevens af tijdens de <i>voice phishing</i> test.
Beslispunt	
3	Binnen de hele organisatie op de lange termijn in te zetten op een cultuurverandering.
Argumenten	
3.1	De organisatiecultuur binnen de gemeente Utrecht is de afgelopen jaren onveranderd.
3.2	Medewerkers spreken elkaar nog altijd onvoldoende aan op ongewenst gedrag.
3.3	Ook onbekenden – <i>mystery quests</i> – worden niet op hun aanwezigheid aangesproken en kunnen daardoor voor langere tijd in de gemeentelijke gebouwen verblijven.
Beslispunt	
4	Te zorgen voor meer centrale aansturing van het informatieveiligheidsbeleid.
Argumenten	
4.1	Organisatieonderdelen zijn zelf verantwoordelijk voor het identificeren en beheersen van de verschillende risico's rond informatieveiligheid.
4.2	Op strategisch niveau ontbreekt het op sleutelposities aan overzicht, slagkracht en mandaat om met informatieveiligheid aan de slag te gaan.
4.3	Vanuit de directie is de afgelopen jaren te weinig toegezien en gehandhaafd.
4.4	De voortgang van maatregelen duurt daardoor lang en hangt te veel af van de bereidwilligheid van leidinggevenden en individuele medewerkers.

4.5	Op tactisch niveau – bij de verschillende organisatieonderdelen – zijn achterstanden ontstaan in het identificeren en beheersen van de risico's, waardoor deze langer blijven bestaan.
4.6	Het wordt onvoldoende duidelijk of er een risicogebaseerde afweging ten grondslag ligt aan de tactische risico's die wél worden beheerst.
4.7	De ondersteuning van de organisatieonderdelen door gemeentelijke medewerkers van informatie- en procesmanagement wordt niet risicogebaseerd verdeeld.
4.8	We kunnen door een gebrek aan informatie niet vaststellen hoe het er met het beheersen van de geïdentificeerde operationele risico's voor staat.
Beslispunt	
5	De raad binnen zes weken door middel van een plan van aanpak te informeren over de wijze waarop deze aanbevelingen worden uitgevoerd.
Argumenten	
5.1	Bij de formulering van de aanbevelingen heeft de rekenkamer ruimte gelaten aan het college om de aanbevelingen nader in te vullen.
5.2	In artikel 12 (lid 9) van de Verordening rekenkamer gemeente Utrecht 2023 is opgenomen dat het college binnen zes weken na besluitvorming over de aanbevelingen van de rekenkamer een plan van aanpak opstelt over de implementatie van de raadsbesluiten.
Kanttekeningen	
5.1	Indien nuttig kan via een expliciet besluit van de gemeenteraad van de standaardtermijn van zes weken worden afgeweken.
5.2	In artikel 12 (lid 10) is opgenomen dat het college jaarlijks (bij de Jaarstukken) aan de raad rapporteert over de stand van zaken van de uitvoering van de raadsbesluiten die genomen zijn naar aanleiding van rekenkamerrapporten.

Financiën

De financiële consequenties van dit voorstel zijn op dit moment onbekend. Deze zijn afhankelijk van de besluitvorming en de precieze opvolging van de beslispunten daarna.

Vervolg

Met het voorliggend besluit wordt het college verzocht om de raad binnen zes weken door middel van een plan van aanpak te informeren over de wijze waarop de aanbevelingen worden uitgevoerd.

Participatie

Binnen de gemeentelijke organisatie sprak de rekenkamer met medewerkers die binnen de verschillende organisatieonderdelen verantwoordelijk zijn voor en uitvoering geven aan de opgaven rond de informatieveiligheid. Dit betrof niet alleen de organisatieonderdelen Informatie en procesmanagement (IPM en Mens en Organisatie, maar ook leidinggevend en deskundigen van andere onderdelen. Daarnaast zijn door een extern bureau – naast de digitale penetratietesten – *social engineering testen* uitgevoerd waarbij medewerkers van de gemeente zijn benaderd om te proberen gegevens buit te maken.

Communicatie

Rekenkamer Utrecht stuurt het rapport en de bijbehorende documenten in eerste instantie toe aan de gemeenteraad en het college van B&W. Vervolgens worden deze ook openbaar gemaakt op de website van de rekenkamer. Daarbij worden ook de respondenten, perscontacten en andere geïnteresseerden op de hoogte gesteld. In een technische bijeenkomst licht de rekenkamer de onderzoeksresultaten nader toe.

Bijlagen

Bijlagen besluitvorming:

- Rekenkamerrapport *De mens als zwakste schakel. Een opvolgingsonderzoek naar de informatieveiligheid van de gemeente Utrecht.*

Bijlagen informatief:

- Persbericht.
- Publiekssamenvatting.
- Infographic.