Afzender: Raadsgriffie **dd** 27 januari 2023
Datum bespreking: 15 februari 2023
Portefeuillehouder gewenst: ja
Naam steller initiatiefvoorstel: Michiel van Hoof (vanuit de hoedanigheid voorzitter auditcommissie)
E-mail steller reactie op voorstel: m.van.hoof@d66.nijmegen.nl

Voorblad met toelichting over

Initiatiefvoorstel Rekenkameronderzoek Informatiebeveiliging en privacybescherming

Fasering

- Informeren
- Opinievorming
- **Advies besluitvorming**
- Besluit

In het kort

Wie: De bewoners van Nijmegen

Wat: Een raadsbesluit over hoe de gemeente de aanbevelingen van de Rekenkamer uitvoert

Waar: Nijmegen en Rijk van Nijmegen

Waarom: Om ervoor te zorgen dat de gemeente zorgvuldig met gegevens omgaat en goed opgewassen is tegen cybercriminaliteit

Hoe: Met het nemen van dit besluit

Over het onderwerp

Doel van de bespreking

De vier Rekenkamers van de gemeenten Berg en Dal, Beuningen, Nijmegen en Wijchen hebben onderzoek gedaan naar de informatiebeveiliging en privacybescherming door deze gemeenten en door het regionaal ondersteuningsbedrijf voor ICT (IRvN). De Rekenkamers sluiten hun onderzoek af met een aantal regionale en lokale aanbevelingen. In dit raadsvoorstel is opgenomen hoe de gemeenteraad van Nijmegen de conclusies en aanbevelingen wil verwerken in gemeentelijk beleid.

Zoals het onderzoek ook constateert, gaat het om ingewikkelde materie. Extra belangrijk is het daarom dat het beleid en de rapportages voor iedereen goed inzicht bieden (informatie in plaats van gegevens) en duidelijk wordt opgeschreven met zo min mogelijk jargon. Verder is ook de regionale component hierin van belang. Nijmegen participeert immers samen met de regiogemeenten in het IRvN. Regionale afstemming van beleidsvoornemens is essentieel om te voorkomen dat IRvN teveel verschillende opdrachten krijgt. De gemeenteraden hebben daarom in september 2022 een gezamenlijke bijeenkomst gehad, waarin een toelichting over het onderzoek is gegeven en afstemming is geweest over het vervolg. De gemeenteraden van Beuningen, Wijchen en Berg en Dal hebben inmiddels vergelijkbare raadsvoorstellen vastgesteld met dat van Nijmegen. Hiermee is een eenduidige sturing vanuit de raden geborgd.

De afspraak is dat een rekenkameronderzoek wordt vergezeld door een raadsvoorstel vanuit een klankbordgroep van raadsleden. Gezien het onderwerp heeft de auditcommissie dit voorstel verzorgd.

Over de procedure

Verloop gespreksronde

1. Er is ruimte voor het delen van standpunten en het stellen van vragen aan elkaar, de steller van het stuk en aan de portefeuillehouder.
2. Er is ruimte om met elkaar in gesprek te gaan over de ingenomen standpunten
3. Afronding: samenvatting van afspraken en conclusies door voorzitter over vervolg

Vervolgproces

1. Na het advies van de gespreksronde neemt de raad naar verwachting een besluit op 8 maart 2023.

Bijlagen

1. Rekenkameronderzoek Informatiebeveiliging en privacybescherming ‘Weten wat je moet weten’
2. Initiatiefraadsvoorstel van de auditcommissie
3. ---NAZENDING --- Schriftelijke reactie van het college op het initiatiefvoorstel d.d. 31 januari jl
4. --- NAZENDING --- voorbeeld format ENSIA rapportage Amersfoort.

De toelichting van de Rekenkamer over het onderzoek is terug te kijken in de agenda in iBabs onder 13 september 2022.

Zie verder het vervolgblad.

Moties, amendementen en toezeggingen

Moties

Er zijn eerder geen moties ingediend of vastgesteld.

Amendementen

Er zijn eerder geen amendementen ingediend of vastgesteld.

Toezeggingen

Er zijn geen openstaande toezeggingen op dit onderwerp.

Vervolg – achtergrondinformatie

De links naar de besluitvorming over 'Weten wat je moet weten' aan de hand van vergelijkbare raadsvoorstellen in de buurgemeenten:

- Beuningen: 11 oktober 2022, zie: https://beuningen.bestuurlijkeinformatie.nl/Reports/Item/5789cbbc-c5b5-4da0-8958-7e557022e04e
- Wijchen: 20 oktober 2022, zie: https://wijchen.bestuurlijkeinformatie.nl/Agenda/Index/67d2f060-5be9-4823-84b7-3a5e53fcd37a#87ced86f-9e90-4be2-9445-c1835b049e99 (agendapunt 9.b)
- Berg en Dal: 15 december 2022, zie: https://raad.bergendal.nl/Agenda/Index/75556929-7734-4af9-801f-e3f9c6fcc597 (agendapunt 6d)

Opmerkingen Rekenkamer bij de collegereactie bij het initiatiefvoorstel bij het Rekenkamerrapport

1. **Kritische prestatie indicatoren**

Reactie college in kader van bestuurlijk wederhoor op aanbeveling 10: Ga KPI's gebruiken.
'Deze aanbeveling nemen wij ter harte. In de actualisatie van het privacy beleid zullen wij aandacht besteden aan meetbare resultaten aan de hand van het borgingsproduct van de Informatiebeveiligingsdienst (IBD). In samenwerking met iRvN zijn wij op het gebied van informatiebeveiliging begonnen met het opbouwen van KPI's.'

Reactie college op Initiatiefraadsvoorstel op beslispunt 2c over KPI's
'Uw raad vraagt ons om een voorstel te doen rond Kritische Prestatie-Indicatoren (KPI's) om voortgang te toetsen. Maar de prestaties en gerealiseerde effecten in de domeinen van informatieveiligheid en privacybescherming laten zich niet eenvoudig vastleggen in KPI's. Want hoe meten we of we voldoende informatieveilig werken en de privacybescherming op orde is? Betekent een hoger aantal datalekmeldingen dat de informatieveiligheid af neemt of dat het iBewustzijn toe neemt? Betekent meer deelnemers aan de verplichte eLearning een groter iBewustzijn? Dit neemt niet weg dat we met de iRvN op het gebied van informatiebeveiliging het gesprek voeren wat zinvolle KPI's zijn. Wellicht heeft u als raad concrete KPI's in gedachten die de prestaties en gerealiseerde effecten in de domeinen van informatieveiligheid en privacybescherming meten. Wij nodigen u van harte uit deze met ons te bespreken.'

Suggestie
De Rekenkamer verwijst in het onderzoek naar de format van de gemeente Hilversum als goed voorbeeld. Ook de gemeente Amersfoort heeft een duidelijke opzet. Nu het college vraagt aan de raad welke concrete KPI's de raad in gedachten heeft, is de suggestie om de formats uit Hilversum en Amersfoort te bekijken. De opzet van de gemeente Hilversum is bijlage 6 bij het rapport. De opzet van de gemeente Amersfoort is als aparte bijlage bij het voorblad gevoegd.

2. **Informeren over voortgang (beslispunt 2d)**

Uit de collegereactie:
'Uw raad wenst de mogelijkheid dat ons college twee keer per jaar aan de raad verslag doet over de voortgang op de doelstellingen, planning, risico's, maatregelen en middelen, zo mogelijk als vervanging van bestaande rapportages op dit

gebied (beslispunt 2d). Vanwege wettelijke bepalingen kunnen we de twee huidige rapportages (het FGjaarverslag en de ENSIA-audit) niet aanpassen naar andere vormen van rapporteren. Die blijven daarmee in stand. Aanvullend zullen wij uw raad tweemaal per jaar via een raadsinformatiebrief rapporteren over de stand van zaken.'

Een paar opmerkingen hierbij:

- De vorm waarin en de frequentie waarmee de FG (aan het college) rapporteert is vrij. Als goed voorbeeld hebben de rekenkamers het jaarverslag van de FG van Hilversum bij het rapport gevoegd. Hierin wordt gewerkt met prestatie-indicatoren. Zie ook de format uit Amersfoort, bij dit voorblad gevoegd.
- De invulling van de ENSIA-rapportage (en overige voortgangsinformatie) was tot nu toe beperkt, zie onderstaande passages uit het rapport.
- Ook nu wordt ook al op een andere manier gerapporteerd, zie onderstaande passages uit het rapport over de bruikbaarheid (kwaliteit) hiervan voor de raad.

Bestuurlijk rapport p50 /51:
'De informatievoorziening in de jaarstukken is beperkt. Het ontbreekt grotendeels aan verantwoordingsinformatie. Het gaat vooral om beschrijvingen van uitgevoerde activiteiten, meer algemene toelichtingen en op onderdelen gaat het letterlijk om dezelfde teksten als in de begroting. Dit maakt een goede controle door de gemeenteraad niet echt mogelijk.
In het kader van ENSIA informeert het college de raad door toezending van de Collegeverklaring ENSIA en een Rapportage Informatiebeveiliging en Privacy. In de Collegeverklaringen wordt ingegaan op de mate waarin de gemeente voldoet aan de normen voor Suwinet en DigiD. Met de 'Rapportages Informatiebeveiliging en Privacy' wordt de raad 'bijgepraat' over uitgevoerde activiteiten. Ook is een vooruitblik op de komende jaren opgenomen. Er wordt in die rapportages geen directe relatie gelegd met de BIO - wat juist de bedoeling is van ENSIA - en ook niet met de uitgangspunten van het gemeentelijke informatiebeveiligings- en privacybeschermingsbeleid. Er wordt ook niet gerapporteerd aan de hand van KPI's. Dat is opvallend, omdat één van de uitgangspunten van het informatiebeveiligingsbeleid (2019 én 2022) is dat "het sturen en rapporteren over de voortgang en de kwaliteit van de informatiebeveiliging gebeurt op basis van KPI's". Tot nu toe zijn die KPI's niet geformuleerd. In de boardletter 2021 vraagt de accountant aandacht voor de uitwerking hiervan. De gemeenteraad heeft de verantwoording in het kader van ENSIA, inclusief de 'Rapportages Informatiebeveiliging en Privacy' steeds voor kennisgeving aangenomen.

Al met al is de informatiewaarde van de verschillende voortgangs- en verantwoordingsrapportages voor de raad te beperkt om goed invulling te kunnen geven aan zijn controlerende rol.'

Ten aanzien van dit punt zijn aanbeveling 9 en 16 uit het rapport van belang:

Aanbeveling 9: Leg vast hoe je gaat toetsen en rapporteren
Vraag het college om in het beleid op te nemen hoe je als gemeente wilt gaan toetsen en rapporteren. Neem de PDCA-cyclus als uitgangspunt en expliciteer de momenten waarop getoetst en gerapporteerd wordt. Belangrijk bij het toetsen is dat periodiek pentesten worden uitgevoerd en periodiek extern getoetst wordt. Belangrijk bij het rapporteren is dat – na overleg met de raad (zie aanbeveling 16) - ook wordt aangegeven hoe en wanneer aan de raad gerapporteerd wordt. Maak in het college (en ook in de raad, zie paragraaf 3.9) in elk geval meer werk van de jaarlijkse verantwoordingsrapportage over informatieveiligheid en privacybescherming; leg daarbij ook een relatie met de bevindingen van de accountant. Nodig de CISO en FG uit voor een toelichting en bespreking.

Aanbeveling 16: Richt als raad je controlerende rol beter in:
Vraag de griffie om in een beknopte nota vast te leggen:

- waarover je als raad wilt worden geïnformeerd: de stand van zaken rond doelen, risico's en maatregelen, de resultaten van testen en toetsen, de toereikendheid van middelen, etc.
- op welke manier je als raad wilt worden geïnformeerd: enkel via de P&C-cyclus, of ook via periodieke informatiebrieven of voortgangsrapportages, via de auditcommissie (desnoods in beslotenheid), etc.
- dat je in ieder geval de jaarlijkse rapportages (ENSIA, privacyjaarverslag) wilt ontvangen en dat die moeten worden voorzien van een begeleidende toelichting. Voor beide rapportages geldt dat daarin inhoudelijk moet worden gerapporteerd op het voldoen aan de vereisten: voor informatiebeveiliging (ENSIA) zijn dat de BIO-normen en voor privacybescherming de AVG. Verwijs in de nota bijvoorbeeld naar het goede voorbeeld in Hilversum.
- hoe je als raad die informatie agendeert en behandelt, en hoe je de vinger aan de pols houdt. Overweeg om een externe toets of second opinion te vragen, of een adviseur in te schakelen.