Nijmegen

Postadres
Gemeente Nijmegen
Postbus 9105
6500 HG Nijmegen

Bezoekadres
Korte Nieuwstraat 6
6511 PP Nijmegen

T 14 024
nijmegen.nl

Contactpersoon
Otto Ritsema
o.ritsema@nijmegen.nl
T 024 – 329 24 65

Ons kenmerk
E23.000058

Aan de gemeenteraad van Nijmegen

Datum 31 januari 2023
Onderwerp "Weten wat je moet weten"

Geachte leden van de raad,

Naar aanleiding van het regionale rekenkameronderzoek naar informatieveiligheid en privacybescherming (“Weten wat je moet weten”) heeft uw raad een initiatiefvoorstel opgesteld. In het onderzoeksproces hebben wij al onze bestuurlijke reactie mogen geven, waar uw raad dan ook bekend mee is. Als reactie op uw initiatiefvoorstel maken we graag van de mogelijkheid gebruik enkele punten bij de uitvoering van de aanbevelingen van het rekenkameronderzoek nader onder uw aandacht te brengen.

Informatieveiligheid en privacybescherming belangrijke thema’s
Met het raadsinitiatiefvoorstel geeft u duidelijk het signaal af informatieveiligheid en privacybescherming als belangrijke thema’s te zien. Wij delen uw standpunt. Het zijn thema’s waarop we investeren in tijd, capaciteit, expertise en middelen. Door voortdurende ontwikkelingen in beide domeinen zullen we nooit klaar zijn en moeten we onszelf voortdurend scherp houden. Het (regionale) rekenkameronderzoek helpt daarbij.

Zoals u bekend nemen wij de aanbevelingen uit het rekenkameronderzoek ter harte. Het onderzoek biedt ons inzicht waar we staan. Het toont ook wat we nog kunnen of moeten ondernemen in het verbeteren van onze informatieveiligheid en privacybescherming. Wij doen dit vanuit het belang van onze inwoners en onze dienstverlening aan hen. Enkele voorbeelden uit de praktijk van alledag die exact de spanning raken waar het hier om gaat zijn:
- Een verloren USB-stick met gevoelige informatie.
- Een mail die onbedoeld naar een verkeerde ontvanger wordt geadresseerd.
- Het gijzelen van data of systemen die de dienstverlening aan inwoners belemmert.

Het is onze plicht een goede dienstverlening aan inwoners te organiseren waarbij we onze zaken rond informatieveiligheid en privacybescherming op orde houden én tegelijkertijd het werk en achterliggende processen uitvoerbaar blijven.

Vanuit onze verantwoordelijk voor een goede uitvoering, willen we uw raad een aantal aandachtspunten in uw besluitvorming meegeven. Deze aandachtspunten zullen we vervolgens toelichten. Het gaat om:

1. We kunnen niet alles in één keer en tegelijk.
2. Een passend volwassenheidsniveau behalen én behouden.
3. Sturen met de juiste informatie.

1. We kunnen niet alles in één keer en tegelijk.

De rekenkamers concluderen (2022; 14) dat *"(…) de gemeenten en iRvN hard werken aan informatiebeveiliging en privacybescherming, maar ook dat er nog veel moet gebeuren om van voldoende beheersing te kunnen spreken."* De rekenkamers tekenen ook op (2022; 1) dat *"de aanbevelingen een forse inspanning vergen van de colleges van B&W."* In uw raadsinitiatiefvoorstel geeft uw raad aan te streven naar *"samen de prioriteiten afstemmen en transparant het gesprek voeren over de planning en over de inhoud van de opgave"*. Hier werken we als college graag aan mee (zie ook aandachtspunten 2 en 3). Want we kunnen niet alles in één keer en tegelijk. Wij ervaren dit aan de hand van de volgende elementen:

1. Voortdurend toenemende complexiteit en dreiging in beide domeinen vraagt om voortdurende aanpassing met stapsgewijze aanpak.
2. Zowel techniek als gedrag moet verbeteren. Verandering in gedrag vraagt vaak meer tijd en een meer veranderkundige aanpak om het gewenste resultaat te bereiken, als ook te laten beklijven.
3. Onze uitvoeringscapaciteit is beperkt, gelet op alle andere opdrachten die we onze organisatie vragen ook te realiseren.

Maar we zitten niet stil. Ten aanzien van de uitvoering van de aanbevelingen, willen we uw raad informeren dat we:

- Eind eerste kwartaal 2023 een hernieuwd strategisch privacybeleid aan uw raad voor willen leggen (aanbeveling 3).
- Een externe organisatie een risicoanalyse laten uitvoeren. Deze komt in de tweede week van januari ambtelijk in concept gereed (aanbeveling 5).

Ondertussen werken we in dit kader ook aan:

- Het met de iRvN uitvoeren van het meerjarige investeringsplan. Dit plan omvat het uitvoeren van maatregelen gericht op preventie, monitoring/bewaking en maatregelen die ertoe leiden dat in geval van dreiging of uitval, de functionaliteit snel hersteld is (curatie). Aanleiding voor dit plan was de analyse tussen de huidige situatie en gewenste situatie rond informatieveiligheid (ook bekend als GAP-analyse). Voor deze maatregelen heeft uw raad oplopend tot 2025 extra geld in de begroting opgenomen.
- Het jaarlijks oefenen en verbeteren van ons i-crisis protocol zodat we gesignaleerde kwetsbaarheden van passende maatregelen voorzien en we daarmee alert blijven op cybercriminaliteit.
- De ontwikkeling en beheer van continuïteitsplannen die we in kunnen zetten als er onverhoopt uitval van systemen door cybercriminaliteit of andere oorzaken plaatsvindt.

- Onszelf in de praktijk van alledag uitdagen door ons te laten bezoeken door een mystery-guest.
- Onze systemen testen op kwetsbaarheden tijdens HackNijmegen.

Wat en wanneer we iets doen, hangt sterk samen met het (na te streven) volwassenheidsniveau.

2. Een passend volwassenheidsniveau behalen én behouden

De goede dingen op het juiste moment doen, hangt samen met de ambitie die we onszelf stellen. Het rekenkameronderzoek (2022: p.15) toont dat om volledig en aantoonbaar in control te zijn, organisaties over de volle breedte minimaal op volwassenheidsniveau 3 moeten zitten. Het onderzoek toont dat wij tussen 1,5 en 2 scoren wat betreft informatiebeveiliging. Voor privacybescherming scoren we tussen 2 en 3. De iRvN scoort voor informatiebeveiliging rond niveau 2. Oók stelt het onderzoek dat de meeste gemeenten in Nederland nog niet op volwassenheidsniveau 3 (of hoger) zitten.

We móeten en wíllen in control zijn wat betreft informatieveiligheid en privacybescherming. Wat ons betreft is het *behalen* van volwassenheidsniveau 3 voor onze organisatie een stevige basis én een stevige ambitie. Het is een volwassenheidsniveau dat passend is voor een goede dienstverlening aan onze inwoners en een efficiënte en effectieve uitvoering voor onze organisatie. Het is tegelijkertijd een stevige ambitie, omdat het reeds de nodige inspanning van de gehele organisatie vraagt om dit niveau te behalen én daarna vast te houden. Het raakt immers álle medewerkers en niet een beperkt aantal gespecialiseerde functionarissen. Dit naast alle andere inspanningen op de primaire processen zoals tijdige verstrekking van energiecompensatie, opvang vluchtelingen, vervanging kapitaalgoederen, woningbouw, etc. Bovendien zijn beide domeinen voortdurend in beweging richting meer dreiging en een grotere complexiteit. Dit vraagt voortdurend om aanpassingen om het gewenste volwassenheidsniveau te behalen én behouden.

Zoeken naar optimale balans

Hoewel niveau 5 het hoogste niveau is, zien wij dat niet als beste niveau om na te streven. Het model beschrijft hoe een organisatie zich gedraagt op ieder volwassenheidsniveau. Hoe hoger het niveau, hoe strakker alle werkprocessen rond informatieveiligheid en privacybescherming in opzet, bestaan en werking geregeld en bewezen moeten zijn. Het zal leiden tot een dienstverlening tegen hogere kosten, omdat we bij het nastreven van die hogere niveaus meer capaciteit kwijt zijn aan meer controles en processen vastleggen.

We zijn voortdurend op zoek naar een optimale balans tussen een efficiënte en betrouwbare dienstverlening aan onze inwoners én uitvoerbaarheid van de processen die dat moeten bewerkstelligen. Het is een afweging van publieke waarden bij inzet van digitale middelen. In dit geval tussen: betaalbaarheid, uitvoerbaarheid en veiligheid.

Daarin speelt het verbeteren van de techniek een kleinere rol dan ons gedrag. Een hoger ambitieniveau dan volwassenheidsniveau 3 willen we dan ook ontraden. Indien uw raad een hoger ambitieniveau nastreeft, dan is dit niet iets dat we in de komende drie jaar kunnen realiseren. Bovendien zal een dergelijke ambitie gepaard gaan met kosten waarvoor geen dekking in onze begroting is voorzien. Aanvullend maakt het rekenkameronderzoek duidelijk dat we nog genoeg te doen hebben om volwassenheidsniveau 3 te behalen.

3. Sturen met de juiste informatie.

Zoals de rekenkamers benoemen, heeft uw raad de juiste informatie nodig om de kaders te kunnen stellen en te controleren. Ook ons college heeft voor een juiste uitvoering zicht nodig op of we de goede dingen goed doen en om op goede wijze verantwoording af te kunnen leggen. Uw raad geeft aan hierover graag het gesprek te voeren met het college. Om te bepalen welke informatiebehoefte u precies heeft, gaan wij dat gesprek graag met u aan. Twee van de beslispunten uit uw voorstel raken namelijk de achterliggende informatiebehoefte.

Voorstel Kritische Prestatie-Indicatoren (beslispunt 2c)

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.

Informeren over voortgang (beslispunt 2d)

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 FG-jaarverslag 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.

Tot slot
Met deze brief hebben wij uw raad inzicht willen geven dat ons college met de aanbevelingen van het rekenkameronderzoek aan de slag is. Daarbij moeten we kiezen als het gaat om wat we wanneer doen. Wij gaan hierover graag met uw raad in gesprek.

Hoogachtend,

Het college van burgemeester en wethouders van Nijmegen

A.P.W. van de Klift
gemeentesecretaris

H.M.F. Bruls
burgemeester