



Rekenkamercommissie gemeente Noordenveld

Onderzoek Informatiebeveiliging

Deel 1: Conclusies en aanbevelingen

Noordenveld, november 2023

Rekenkamercommissie gemeente Noordenveld

Samenstelling:

Erik van Zuidam (externe voorzitter)

Arne Bakker (extern lid)

Christine Stille (raadslid)

Casper Colenbrander (raadslid)

2

Contact met de rekenkamercommissie:

Henriette Johannes (secretaris)

Postbus 109, 9300 AC Roden

Raadhuisstraat 1, 9301 AA Roden

050-50 27 222

h.johannes@gemeentenordenveld.nl

Inhoudsopgave

1. Inleiding	4
2. Leeswijzer	6
3. Verantwoording	7
4. Conclusies	9
5. Aanbevelingen	12
6. Slot	14

Bijlage: bestuurlijke reactie B&W op rapport

1. INLEIDING

De rekenkamercommissie van de gemeente Noordenveld heeft in 2023 onderzoek wil een bijdrage leveren aan het versterken van de digitale weerbaarheid van de gemeente Noordenveld. Vanuit dat perspectief is onderzoek gedaan naar de wijze waarop op dit moment invulling wordt gegeven door de verschillende verantwoordelijken binnen Noordenveld op het gebied van informatiebeveiliging.

Rekenkameronderzoek is bedoeld om een bijdrage te leveren aan de transparantie en de effectiviteit van het bestuur. De onderzoeken van de rekenkamercommissie kunnen een rol spelen in de verantwoording van het college aan de raad, maar ook in de publieke verantwoording.

De centrale vraag in dit onderzoek luidt:

In hoeverre is het gemeentebestuur van Noordenveld zich op dit moment bewust van de risico's op het gebied van informatieveiligheid en wordt ze in staat gesteld om actief te kunnen sturen op dit onderwerp?

Deze hoofdvraag valt uiteen in de volgende deelvragen.

Beleid

- Welk beleid heeft de gemeente Noordenveld gericht op informatiebeveiliging?
- In hoeverre voldoet het informatiebeveiligingsbeleid aan de gestelde (wettelijke) eisen en normen, waaronder de Baseline Informatiebeveiliging Overheid (BIO)?

Organisatie

- Op welke wijze is informatieveiligheid intern georganiseerd binnen het ambtelijk apparaat en wordt er op dit thema gestuurd binnen de ambtelijke organisatie?
- Hoe is de uitvoering van het informatiebeveiligingsbeleid qua taken, rollen en verantwoordelijkheden belegd binnen de gemeente?
- Hoe is de organisatie toegerust op de uitvoering van het informatiebeveiligingsbeleid (allocatie van middelen, capaciteit, kennis en vaardigheden)?

Uitvoering

- Hoe wordt in de dagelijkse uitvoeringspraktijk van de gemeente gevolg gegeven aan het informatiebeveiligingsbeleid?
- Op welke wijze is de afgelopen jaren invulling gegeven aan eerder opgestelde adviezen op dit onderwerp?

Signaleren, verantwoorden en leren

- Worden mogelijke cyberincidenten ook periodiek beproefd, bijvoorbeeld met een cyberoefening? Worden de uitkomsten hiervan geëvalueerd, gedeeld en eventuele verbeterpunten geïmplementeerd?
- In welke mate is er op bestuurlijk niveau aandacht voor en sturing op informatiebeveiliging?
- Op welke wijze en in welke mate wordt het gemeentebestuur van Noordenveld meegenomen in de aanwezige risico's op het gebied van informatieveiligheid en leidt dit tot een voldoende bewustzijn van het belang van dit onderwerp?
- Op welke wijze wordt het gemeentebestuur geïnformeerd over het onderwerp informatieveiligheid en is ze op basis hiervan voldoende in staat om te kunnen (bij)sturen op dit onderwerp?
- Wat zijn de ambities van het gemeentebestuur voor wat betreft de sturing op informatiebeveiliging?
- In hoeverre is het informatiebeveiligingsbeleid van de gemeente Noordenveld en de uitvoering daarvan toekomstbestendig? En waar liggen eventuele mogelijkheden voor verbetering?

In hoofdstuk 4 van dit deel geven wij antwoord op de deelvragen (conclusies) en in hoofdstuk 5 die wij aanbevelen.

2. LEESWIJZER

Het eindrapport bestaat uit twee delen. Het eerste deel, het deel dat u nu onder ogen heeft, de nota van conclusies en aanbevelingen, is het bestuurlijke rapport. Hierin staan de belangrijkste resultaten en conclusies van het onderzoek, evenals de aanbevelingen die de rekenkamercommissie heeft geformuleerd. In de bijlage is de bestuurlijke reactie van het college van burgemeester en wethouders opgenomen.

Het tweede deel is het rapport van bevindingen van het onderzoeksbureau. In dit rapport zijn de resultaten van het onderzoek opgenomen en toegelicht. Het opgestelde rapport is onderverdeeld in vijf inhoudelijke hoofdstukken. Naast de onderzoeksaanpak gaan de hoofdstukken over de manier waarop het beleid is vormgegeven (hoofdstuk 3), de organisatie van informatiebeveiliging (hoofdstuk 4), de wijze waarop uitvoering wordt gegeven aan het beleid (hoofdstuk 5) en als laatste signaleren, verantwoorden en leren (hoofdstuk 6). Per hoofdstuk wordt tevens een korte analyse gemaakt.

Het rapport van bevindingen vormt de basis voor de conclusies en aanbevelingen.

3. VERANTWOORDING

Opdrachtgeverschap en begeleiding van het onderzoek

Het onderzoek is uitgevoerd door twee onderzoekers van het bureau BMC. Het eindrapport is gebaseerd op deskresearch en interviews met vertegenwoordigers van de ambtelijke organisatie, en een vertegenwoordiging van de gemeenteraad. Daarnaast is in opdracht van de rekenkamercommissie door BMC een externe partij ingeschakeld om een zogenaamde aanvullende externe kwetsbaarheden test (penetratietest) uit te voeren. De uitkomsten van deze test zijn besproken en gedeeld met de ambtelijke organisatie en zijn verwerkt in dit rapport. De uitkomsten van de test zijn dusdanig technisch en vertrouwelijk van aard dat deze verder niet worden gedeeld met anderen.

Proces van totstandkoming

Bij start van het onderzoek (april 2023) was aanvankelijk het idee om geen externe kwetsbaarheden test uit te voeren omdat het ambtelijk apparaat had aangegeven deze zelf te gaan uitvoeren. Op verzoek van de ambtelijke organisatie heeft de rekenkamercommissie deze onder haar verantwoordelijkheid als onderdeel van het onderzoek naar informatiebeveiliging laten uitvoeren. Gedurende de periode juni t/m september is het onderzoek daadwerkelijk uitgevoerd en is sprake geweest van een bijzonder positieve en constructieve samenwerking van alle betrokkenen aan het onderzoek.

7

Opgeleverd rapport

Het onderzoeksbureau heeft bijgaand rapport van bevindingen (deel 2) gemaakt. Het rapport vormt een integraal onderdeel van de rapportage van de Rekenkamercommissie. Het concept rapport van bevindingen is ter verificatie (voor wederhoor) voorgelegd aan de ambtelijke organisatie en het college. Vanuit de ambtelijke organisatie is een beperkt aantal op- en aanmerkingen op het rapport gekomen. Op basis hiervan is een aantal aanpassingen doorgevoerd en is het bevindingenrapport vastgesteld. Op basis van het bevindingenrapport heeft de rekenkamercommissie conclusies getrokken en aanbevelingen opgesteld.

Integriteit

Het ministerie van BZK vraagt rekenkamer(commissies) alert te zijn bij hun onderzoeken op signalen van niet-integer gedrag en omstandigheden die integriteitsrisico's met zich mee kunnen brengen.

In dit onderzoek zijn geen feiten naar voren gekomen die duiden op belangenverstrengeling of integriteitskwesties.

4. CONCLUSIES

4.1. CONCLUSIES

Doel van het onderzoek

De centrale vraag in dit onderzoek luidt:

In hoeverre is het gemeentebestuur van Noordenveld zich op dit moment bewust van de risico's op het gebied van informatieveiligheid en wordt ze in staat gesteld om actief te kunnen sturen op dit onderwerp?

Conclusies

- 1) **De afgelopen periode is een aantal goede stappen gezet om het bewustzijn van de risico's op het gebied van informatieveiligheid te vergroten en is de basis gelegd om te gaan sturen op het onderwerp informatieveiligheid.**

8

Met de aanstelling van een CISO (overall verantwoordelijke voor informatieveiligheid), het uitvoeren van diverse bewustwordingsactiviteiten, het opstellen van beleid etc, is een aantal goede stappen gezet om een basis te leggen voor het vergroten van het bewustzijn van de risico's en de mogelijkheden om te sturen op het onderwerp informatieveiligheid. Hierbij onderkennen we dat binnen een relatief kleine gemeente continue het vraagstuk meespeelt van waar de beschikbare capaciteit het beste op kan en moet worden ingezet.

- 2) **Het gemeentebestuur is zich nog onvoldoende bewust van de risico's op het gebied van informatieveiligheid en moet nog de nodige aanvullende stappen zetten om daadwerkelijk goed te kunnen gaan sturen op het onderwerp informatieveiligheid.**

De gemeenteraad wordt onvoldoende geïnformeerd over de ontwikkeling en de stappen die gemaakt moeten worden op basis van het vastgestelde strategische informatiebeveiligingsbeleid. Daardoor is ze onvoldoende in staat om de aanwezige risico's te duiden en te sturen op de voortgang. Ook het college stuurt niet op basis van een PDCA-cyclus op dit onderwerp.

3) Op alle terreinen van informatieveiligheid moeten vervolgstappen gezet worden.

Op alle terreinen is het noodzakelijke werk te verzetten. Enerzijds om een inhaalslag te maken, anderzijds om ervoor te zorgen dat de gemeente het juiste niveau van beveiliging bereikt en behoudt. Hierbij gaat het dan om de terreinen: mens, organisatie & techniek. Dit betekent onder meer extra aandacht voor bewustwording (*mens*), het op de juiste manier beleggen van de diverse taken, bevoegdheden en verantwoordelijkheden (*organisatie*), en het periodiek laten uitvoeren van technische penetratietesten en de bevindingen oplossen (*techniek*).

4) Er zijn nu meer dan voldoende onderzoeken uitgevoerd met bijbehorende goede analyses. Daarnaast is er ook de nodige externe expertise snel toegankelijk beschikbaar.

Uit het onderzoek blijkt dat er op diverse momenten onderzoeken naar informatieveiligheid zijn uitgevoerd. Helaas heeft dit nog onvoldoende geleid tot een situatie waarin de opgeleverde adviezen toekomstbestendig zijn ingebed binnen de organisatie en een bijbehorende PDCA-cyclus is ingericht om te groeien naar de structurele inbedding van dit onderwerp. Daar moet nu de komende periode de nadruk op gaan liggen middels actieve sturing vanuit het college en de raad op de daadwerkelijke uitvoer van de diverse adviezen. Hierbij kan goed gebruik gemaakt worden van aanwezige externe expertise vanuit bijvoorbeeld de IBD (informatie beveiligingsdienst) en de veiligheidsregio waarbij dan ook de relatie gelegd kan worden naar bredere risico's (ondermijning).

5) De organisatie van informatiebeveiliging is belegd in verschillende rollen en functies binnen de gemeente Noordenveld, maar de wijze waarop hieraan invulling wordt gegeven verloopt niet zoals beoogd.

De organisatie is op dit moment onvoldoende toegerust op hetgeen er vanuit het oogpunt van informatiebeveiliging van de gemeente wordt gevraagd op strategisch, tactisch en operationeel niveau. Het gaat daarbij niet alleen om de beschikbare capaciteit, gevoel of feeling en expertise op het gebied van informatiebeveiliging, maar ook om de bewustwording en verantwoordelijkheidsgevoel bij alle leidinggevend en medewerkers.

5. AANBEVELINGEN

Aanbevelingen aan het College

Aanbeveling 1

Geef de ambtelijke organisatie opdracht om de bevindingen van de technische penetratietesten op zo'n kort mogelijke termijn op te pakken en daar waar dit niet mogelijk is mitigerende maatregelen te treffen. Geef daarnaast opdracht om als regulier proces de uitvoering van penetratietesten binnen de organisatie te beleggen. Kijk hierbij – gegeven de huidige beschikbare capaciteit – kritisch naar de wijze waarop de beschikbare capaciteit het beste kan worden ingezet en in hoeverre samenwerking met derden niet de druk op de organisatie kan verlagen.

Aanbeveling 2

Geef de CISO opdracht om te komen tot een leerlijn waarin alle medewerkers van de organisatie nadere scholing krijgen op het gebied van informatieveiligheid. Betrek bij de doelgroepen ook het college en raad hier bij.

Aanbeveling 3

Zorg dat de vastgestelde principes voor informatiebeveiliging ook daadwerkelijk gaan leven en gehanteerd worden. Stuur en rapporteer hier actief op. Beleg daarnaast een sessie met raad en college om hier gezamenlijk gevoel & urgentie bij te krijgen. Gebruik hier ook de expertise van externe partijen bij.

Aanbeveling 4

Stuur op de PDCA voor informatieveiligheid, onderken daarbinnen de nodige prioriteiten om de juiste focus aan te brengen. Besteed nadrukkelijk aandacht aan het niet alleen toewijzen van verantwoordelijkheden maar vooral ook op de wijze waarop dit dan door de verantwoordelijken wordt opgepakt & uitgevoerd. Stuur actief bij als blijkt dat dit onvoldoende wordt gedaan. Sluit hierbij zoveel mogelijk aan bij de bestaande kwaliteitscyclus. Kijk hierbij kritisch naar de huidige situatie waarbij de CISO ook de rol van privacy officer vervult. Ook privacy vraagt in toenemende mate meer energie en aandacht.

Aanbevelingen aan de raad

Aanbeveling 1

Onderken het belang van digitale weerbaarheid van de gemeente Noordenveld en de rol van de raad hierin: actief sturen op de wijze waarop de digitale weerbaarheid van de organisatie zich ontwikkelt. Onderzoek hierbij in hoeverre bijvoorbeeld de audit-commissie hier als vooruitgeschoven post kan fungeren namens de raad.

Aanbeveling 2

Participeer zelf actief in diverse beveiligingsinitiatieven (geef het goede voorbeeld) en trek ook zelf lering hier uit (phishing mails, mystery guest visits, digitale leeromgeving).

Aanbeveling 3

Geef het college opdracht om periodiek (bijvoorbeeld twee keer per jaar) te rapporteren aan de gehele raad over de ontwikkeling van digitale weerbaarheid en de wijze waarop dit verder verbeterd kan worden; neem hierbij het huidige rapport als basis, maar vraag het college ook lering te trekken uit eerder opgestelde rapporten.

Aanbeveling 4

Laat het college binnen 4 maanden terugkomen met een plan waarin de aanbevelingen aan het college nader uitgewerkt worden inclusief een concrete planning;

Aanbeveling 5

Laat het college na de zomer van 2024 met het MT terugkomen en de raad informeren over het verbetertraject en ervaringen aangaande de uitvoering en nieuwe leerlijn van het informatieveiligheidsbeleid.

De reactie van het college van B&W is als bijlage 1 opgenomen.

6. SLOT

De rekenkamercommissie wil door de uitvoering van dit onderzoek een bijdrage in stimulerende en prikkelende zin leveren aan de kwaliteit van het gemeentebestuur van Noordenveld, in het bijzonder de kaderstellende en controlerende taken van de gemeenteraad.

De rekenkamercommissie dankt de betrokkenen voor hun coöperatieve bijdrage aan het onderzoek.

Bijlage 1: reactie B&W op rapport informatiebeveiliging

