Rekenkamer Soest

Behandeld door dhr.
Y. Pieters
doorkiesnummer 035-6093121

Aan de leden van de
gemeenteraad van Soest

Soest, ?? ???? 2025 verzonden: ?? ???? 2025

afdeling : Rekenkamer
zaaknummer : 723098
onderwerp : Aanbieden rapport onderzoek Informatieveiligheid

Geachte leden van de gemeenteraad,

Graag biedt de Rekenkamer u het resultaat aan van ons onderzoek naar het informatieveiligheidsbeleid van de gemeente Soest. Het volledige resultaat van het onderzoek is weergegeven in het rapport 'Onderzoek informatieveiligheid'.

Centrale onderzoeksvragen

De hoofdvraag van dit onderzoek is:

> Is het informatieveiligheidsbeleid van de gemeente Soest doeltreffend om cyberaanvallen zo veel mogelijk tegen te gaan en is de gemeentelijke organisatie voldoende toegerust om bij een toch geheel of gedeeltelijk geslaagde cyberaanval effectief te handelen?

Om deze hoofdvraag te beantwoorden heeft de Rekenkamer een onderzoeksbureau ingehuurd dat deskundig is op dit beleidsterrein. Dit bureau heeft een documentstudie uitgevoerd en verdiepende interviews gehouden. Om te onderzoeken hoe in Soest het beleid in praktijk wordt gebracht zijn twee focusgroepen en een raadsbijeenkomst georganiseerd. Op basis van de verkregen informatie is een analyse uitgevoerd en een rapportage opgesteld.

De Rekenkamer heeft geconstateerd dat het onderzoeksbureau terughoudendheid bij de ambtelijke organisatie heeft ervaren in het aanleveren van de benodigde informatie. Ook bij het plannen van de focusgroepen met ambtenaren is niet optimaal verlopen en de opkomst was mager. De Rekenkamer constateert dat dit de uitvoering van het onderzoek heeft bemoeilijkt en de doorlooptijd heeft verlengd.

Beantwoording hoofdvraag van het onderzoek

Naar aanleiding van de opgehaalde bevindingen doet de Rekenkamer een achttal conclusies. Op basis van het onderzoek wordt gesteld dat:

1. De gemeente Soest in RID verband samenwerkt aan digitale veiligheid, maar dat de gemeente zelf verantwoordelijk blijft voor het eigen beleid en de implementatie daarvan;
2. De gemeente in 2024 een adequaat Strategisch Beleidsplan heeft vastgesteld, maar dat er thans onvoldoende conform dit plan wordt gewerkt;
3. De noodzaak wordt onderkend om te voldoen aan de wettelijke kaders die zijn aangegeven in de Europese NIS2 Richtlijn en in de loop van 2025 verplicht worden gesteld in de Cyberbeveiligngswet;
4. De gemeente hiervoor moet groeien van volwassenheidsniveau een naar volwassenheidsniveau vier;
5. Hiervoor extra inspanningen gevraagd worden van de ambtelijke organisatie en
6. De raad op dit moment onvoldoende in staat wordt gesteld om de sturende rol op dit dossier waar te maken.
7. De gemeente thans niet voldoet aan de Baseline Informatieveiligheid Overheden, de BIO norm waardoor de gemeente veiligheidsrisico's loopt.
8. Deze risico's kunnen leiden tot hacks met grote maatschappelijke en financiële gevolgen;

Aanbevelingen

Naar aanleiding van de voorgaande conclusies doet de Rekenkamer drie aanbevelingen:

1. Investeer in een robuuste digitale veiligheidsorganisatie
2. Stel op basis van het strategisch beleid een 'aanvalsplan' Digitale Veiligheid op dat erop gericht is om aan de wettelijke verplichtingen te voldoen
3. Ontwikkel in samenwerking met de raad een begrijpelijke rapportage gebaseerd op gangbare normenkaders, risico's en kosten.

De volledige conclusies en aanbevelingen zijn te vinden op de pagina's 1 – 4 van het rapport.

Bestuurlijke reactie

Het college van burgemeester en wethouders gaf een bestuurlijke reactie op het rapport dat als bijlage C in het rapport op de pagina's 28 – 30 is gevoegd.

Reactie van de Rekenkamer op bestuurlijke reactie

Gezien de bestuurlijke reactie van het college van B en W is het voor de Rekenkamer de vraag of er voldoende urgentie is om de benodigde stappen voortvarend te zetten.

De eerste aanbeveling van de Rekenkamer is om te investeren in een robuuste digitale veiligheidsorganisatie waarin duidelijkheid komt over de rol en de taken van het lijnmanagement en er meer capaciteit nodig is van de CISO, de FG en de PO. De Rekenkamer wijst ook op de noodzaak van voldoende middelen voor deze versterking. Deze zijn nodig om aan het eigen reeds vastgestelde beleid van de gemeente te voldoen. De reactie van het college is dat momenteel wordt onderzocht hoe de genoemde functies het beste kunnen worden ingevuld en dat er met betrokken partners kennis wordt uitgewisseld en instrumenten ontwikkeld. De Rekenkamer is van mening dat uit deze reactie weinig urgentie spreekt om op korte termijn daadwerkelijke veranderingen in gang te zetten.

De tweede aanbeveling van de rekenkamer is het opstellen van een aanvalsplan om te voldoen aan wettelijke verplichtingen. Uit de reactie blijkt niet dat het college een dergelijk aanvalsplan wil opstellen. De BIO is sinds 2018 van kracht en later dit jaar (naar verwachting) wordt het voldoen aan het volwassenheidsniveau 4 een wettelijke verplichting als de Cyberveiligheidswet van kracht wordt. De Rekenkamer ziet het als een goede ambitie dat de gemeente wil doorgroeien naar volwassenheidsniveau 4. Tegelijkertijd is er onvoldoende besef dat een groei van het huidige volwassenheidsniveau 1 naar het toekomstige niveau 4 een zeer grote verandering van de gehele organisatie vergt en dat het niet realistisch is om deze op korte termijn te realiseren zonder het drastisch opstarten en versnellen van de benodigde acties.

De Rekenkamer stelt ten slotte vast dat het college de aanbeveling overneemt om een begrijpelijke rapportage met de raad te ontwikkelen. De Rekenkamer ziet hierin voor de raad een mogelijkheid om het college te vragen met een concreet plan te komen waarin het college duidelijk maakt hoe zij aan de wettelijke verplichtingen op het gebied van informatieveiligheid wil gaan voldoen. Als laatste bevelen wij de raad aan om het college van B en W te vragen binnen 3 maanden aan de raad te rapporteren over de aanpak of implementatie van de overgenomen aanbevelingen.

Tot slot

Wanneer u het rapport behandelt, zijn wij graag bereid de bevindingen te presenteren en een toelichting te geven. Heeft u nadere vragen, neemt u dan gerust contact op met secretaris/onderzoeker Y. Pieters, via y.pieters@soest.nl.

Met vriendelijke groet,
Namens de Rekenkamer,

F. Muijzers
Voorzitter Rekenkamer Soest

Bijlage(n): Rapport Onderzoek informatieveiligheid

Telefoon: 035-6093411 Internet: www.soest.nl
Bezoekadres: Raadhuisplein 1, Soest Postadres: Postbus 2000, 3760 CA Soest E-mail: postbus2000@soest.nl