Beantwoording Raadsvragen

Onderwerp:	1e Berap 2025	Datum antwoord:	27 mei 2025
Type vraag:	Technische vraag t.b.v. commissie / raad		
Datum vraag:	13 mei 2025	Portefeuillehouder:	mw. A.J.M.H. van de Ven burgemeester
Gesteld door:	B. van den Bosch / D66		
Registratienr.:	25.10781 / Z24002817		

Vraag

1. Er worden maatregelen ingezet om politiek dichter bij de inwoners te brengen. Heeft dit ook het effect dat het zou moeten hebben? Komt er meer belangstelling voor politiek? Krijgen we meer aanmeldingen om allerlei functies te bekleden?
2. Wat zijn de risico's op ICT vlak? In hoeverre is de gemeente bestand tegen cyberaanvallen van buitenaf?

Antwoord

1.
Sinds 1 januari 2025 zijn er een aantal acties genomen door het presidium met als doel de zichtbaarheid van de raad te vergroten en meer inwoners te stimuleren om politiek actief te worden. Deze doelstelling is vloeit ook voort uit het coalitieakkoord. Het gaat om de volgende acties:

- In het lokale blad De Uitstraling wordt één keer per twee maanden een column geplaatst namens de gemeenteraad.
- De gemeenteraad is aanwezig geweest op de Open Bedrijvendag op 29 maart.
- De gemeenteraad heeft sinds 6 mei een Facebook- en Instagram pagina.

De volgende stap die gezet gaat worden is de introductie van het concept 'De Raad op Straat'. De bedoeling is dat de gemeenteraad (als orgaan, niet als afzonderlijke fracties) de kernen ingaat om in gesprek te gaan met inwoners. De Raad op Straat wordt op 14 en 24 juni voor het eerst georganiseerd.

Aangezien al deze maatregelen pas recent genomen zijn is het op dit moment lastig te zeggen wat het effect hiervan is. In de eerste week na oprichting van de kanalen heeft de gemeenteraad 71 volgers op Facebook en 25 volgers op Instagram. De gemeenteraad heeft in een week in totaal 2100 gebruikers bereikt, wat geresulteerd heeft in 103 interacties met de content. Na een halfjaar zal het gebruik van social media voor de gemeenteraad geëvalueerd worden.

2.
Het technische deel van de beveiliging wordt afgevangen door het SSC. Zij hebben zich aan de BIO (Baseline Informatiebeveiliging Overheid) te houden en worden daar ook op ge-audit. Zij houden cyberaanvallen zoveel mogelijk tegen. Als een aanval toch door de technische beveiliging heen komt en onze collega's weten niet hoe ze dit moeten herkennen of hoe zij hiermee om moeten gaan, dan geeft dit risico's. Om die reden trainen we doorlopende medewerkers op het gebied van informatieveiligheid. Deelname hieraan is verplicht en wordt gemonitord. Ook worden er phishingtests uitgevoerd. Een 100% cybercrime-proof organisatie is helaas niet realistisch, zeker ook omdat cybercriminelen steeds nieuwe dingen proberen. Het mitigeren van de risico's daarentegen wel.

Vanuit de Europese Unie is de NIS2-richtlijn opgesteld. Deze wordt in Nederland, samen met de BIO2 (opvolger van de eerdergenoemde BIO), geïmplementeerd middels de Cyberbeveiligingswet (Cbw). Hoewel deze nog niet van kracht is, wordt er binnen de organisatie en binnen de samenwerking met de andere kempenorganisaties al hard aan gewerkt om aan deze nieuwe wetgeving te kunnen voldoen.