GEMEENTE ZEVENAAR

Secretaris Rekenkamer Zevenaar
Mevr. E. van Welij
Postbus 10
6900 AA Zevenaar

datum
zaaknummer Z/26/521817-UIT/26/1313523
onderwerp Bestuurlijke reactie rekenkameronderzoek informatieveiligheid

Beste mevrouw Van Welij,

Op 28 mei 2026 heeft u ons het rekenkamerrapport van het onderzoek informatieveiligheid gemeente Zevenaar aangeboden en op 22 september 2026 heeft u het rekenkamerrapport aangevuld met uw conclusies en aanbevelingen toegestuurd. Wij willen de Rekenkamer danken voor uw inzet en de waardevolle aanbevelingen die volgen uit het rapport. Met belangstelling hebben wij het rapport gelezen. Dit rapport biedt waardevolle handvatten om de digitale weerbaarheid van onze organisatie verder te versterken en de raad beter in positie te brengen bij zijn kaderstellende en controlerende rol op dit belangrijke thema.

De Rekenkamer Zevenaar heeft het college gevraagd een bestuurlijke reactie te geven. Hieronder geven wij onze reactie op de bevindingen zoals geformuleerd in het onderzoeksrapport. Het college geeft omwille van de bescherming van de beveiliging van kritieke processen en de weerbaarheid van de gemeentelijke organisatie geen gedetailleerd reactie op de door u in bijlage 1 bij het onderzoeksrapport beschreven aanbevelingen.

Het college herkent zich in het beeld dat de Rekenkamer schetst dat informatiebeveiliging een continu aandachtspunt is en blijvende investeringen vraagt in mensen, processen en techniek. Ook herkennen wij de conclusie dat verdere professionalisering van de governance, bewustwording, vastlegging van processen en versterking van de technische weerbaarheid noodzakelijk zijn om de digitale weerbaarheid van de organisatie verder te vergroten.

Daarnaast concludeert de Rekenkamer dat de gemeente reeds diverse maatregelen heeft getroffen op het gebied van informatieveiligheid, maar dat de huidige inrichting nog kwetsbaarheden kent. Met name op het gebied van bestuurlijke sturing, bewustwording, fysieke beveiliging, technische weerbaarheid, monitoring en incidentrespons zijn verdere verbeteringen noodzakelijk om beter voorbereid te zijn op het toenemende cyberdreigingslandschap en de strengere wettelijke eisen die op gemeenten afkomen.

Om verbeteringen door te voeren zijn er een aantal acties nodig die volgen uit de aanbevelingen in het rekenkameronderzoek. Het college gaat hieronder in op een aantal van de door u genoemde aanbevelingen in het rekenkamerrapport en geeft hierbij kort aan welke acties het college reeds heeft opgepakt in relatie tot de benoemde aanbevelingen.

Versterken van de kennispositie van de raad
Wij onderschrijven het belang van een goed geïnformeerde raad. Informatieveiligheid en digitale weerbaarheid zijn bij uitstek onderwerpen waarbij de raad zijn kaderstellende en controlerende rol actief moet kunnen vervullen. Wij zullen bezien hoe de raad periodiek kan worden meegenomen in relevante ontwikkelingen, risico's en landelijke trends, zodat zij voldoende in positie wordt gebracht om haar rol goed uit te oefenen.

Vergroten van de bestuurlijke betrokkenheid bij informatieveiligheid
Wij kunnen ons vinden in deze aanbeveling. ENSIA biedt een belangrijk verantwoordingsinstrument, maar geeft niet het volledige beeld van de digitale weerbaarheid van de organisatie. Wij zijn bereid te onderzoeken op welke wijze en met welke frequentie de raad aanvullend kan worden geïnformeerd over de ontwikkeling van informatieveiligheid, bijvoorbeeld door middel van periodieke toelichting door de CISO.

Voldoende aandacht voor informatieveiligheid binnen de begroting
Wij herkennen dat informatieveiligheid een structurele opgave is die voortdurend investeringen vraagt. Tegen de achtergrond van een toenemend cyberdreigingslandschap en nieuwe wettelijke verplichtingen is hier zowel in het collegeprogramma als in de meerjarenbegroting 2027-2030 reeds prioriteit aangegeven. Wij zullen dan ook bij de reguliere planning- en controlcyclus expliciet aandacht blijven besteden aan de middelen die nodig zijn om de digitale weerbaarheid van de organisatie op peil te houden.

Versterken van de verantwoording richting de raad
Wij onderschrijven het belang van een structurele en transparante verantwoording richting de raad. Daarbij merken wij op dat reeds op verschillende momenten verantwoording wordt afgelegd over informatieveiligheid. Wij zullen onderzoeken hoe deze informatie kan worden gebundeld en doorontwikkeld tot een meer integrale rapportage, zodat de raad beter inzicht krijgt in de voortgang, risico's en verbetermaatregelen op het gebied van informatieveiligheid.

Aanbevelingen voor het college van B&W
Het college neemt de bevindingen en aanbevelingen over en voert deze uit via een tweejarig programma voor digitale weerbaarheid en informatievoorziening. Het doel van het programma is om ervoor te zorgen dat de onderwerpen uit de programmalijnen geïmplementeerd en geborgd worden in de organisatie.

Het programma omvat vijf samenhangende programmalijnen:

1. Bestuurlijke regie en governance: versterking van sturing, eigenaarschap en voortgangsbewaking.
2. Integraal risicomanagement en crisisbeheersing: structurele beheersing van risico's voor informatiebeveiliging, privacy en continuïteit.
3. Opdrachtgeverschap richting de RID: scherpere afspraken over prioriteiten, prestaties, verantwoordelijkheden en verantwoording.

4. Technische weerbaarheid en continuïteit: versterking van beveiliging, monitoring, herstelvermogen en continuïteit.
5. Mens en gedrag: duurzame versterking van bewustwording, eigenaarschap en handelingsbekwaamheid.

Het college stelt voor twee jaar een programmamanager aan en informeert de raad periodiek over voortgang, risico's en resultaten.

Tot slot
Samenvattend danken wij u voor het opleveren van dit rapport. Wij herkennen ons in de richting van de aanbevelingen en onderschrijven het belang daarvan. Zoals hiervoor is toegelicht, zijn verschillende aanbevelingen reeds in uitvoering of maken zij onderdeel uit van lopende verbetertrajecten binnen onze organisatie. Hierbij stelt het college bestuurlijke de prioriteit vast op basis van bijvoorbeeld risico's, wettelijke verplichting en uitvoerbaarheid. Volledigheidshalve merken wij op dat de uitvoering van aanbevelingen die betrekking hebben op de RID niet uitsluitend door de gemeente kan worden bepaald, maar mede afhankelijk is van gezamenlijke keuzes en prioritering binnen de gemeenschappelijke regeling.

Tot slot zijn wij ons ervan bewust dat informatieveiligheid geen eindpunt kent en blijvende aandacht vraagt. In dat licht waarderen wij de constatering dat gemeenten geconfronteerd worden met een steeds complexer cyberdreigingslandschap, toenemende digitale afhankelijkheden, snelle digitale ontwikkelingen en strengere wet- en regelgeving. Juist daarom zien wij dit rapport als een waardevolle ondersteuning om onze digitale weerbaarheid verder te versterken en onze organisatie ook in de toekomst weerbaar en veilig te houden.

De rekenkamer heeft in haar rapport het college verzocht om de bevindingen en aanbevelingen die betrekking hebben op het RID aan het RID voor te leggen en daar een formele reactie op verlangen zodat voor uw raad helder is wat de RID gaat doen met de bevindingen. Deze reactie is als bijlage bij deze brief gevoegd.

Met vriendelijke groet,
burgemeester en wethouders van Zevenaar,

Danielle Jansen	Lucien van Riswijk
secretaris	burgemeester

Bijlage: Reactie SDL/ RID op rekenkameronderzoek (INT/26/1315200)