REKENKAMER

Gemeente Meppel

Aan de raad van de gemeente Meppel
Postbus 501
7940 AM Meppel

- per e-mail verzonden –

Nieuwleusen, 2 juli 2026

Geachte raadsleden,

Hierbij bieden wij u, namens de rekenkamer Meppel, het onderzoeksrapport over het rekenkameronderzoek 2025 inzake de informatiebeveiliging van de gemeente Meppel aan.

Het onderzoek maakt deel uit van een gezamenlijk initiatief van de personele unie van de rekenkamers van Meppel, Staphorst, Steenwijkerland en Westerveld. Voor iedere gemeente is een afzonderlijk onderzoek uitgevoerd. Het voorliggende rapport bevat uitsluitend de bevindingen voor de gemeente Meppel.

Voordat wij ingaan op de inhoud van het onderzoek, willen wij stilstaan bij de totstandkoming van dit rapport. Het rapport bereikt u later dan wij als rekenkamer hadden gewenst. De oorzaak hiervan ligt onder meer in de wisseling van raad en college gedurende het onderzoeksproces en de zorgvuldige afstemming die heeft plaatsgevonden tussen de betrokken gemeenten, de griffiers, de onderzoekers en de rekenkamers over de omgang met gevoelige informatie. Die zorgvuldigheid vonden wij noodzakelijk, maar heeft geleid tot vertraging.

De rekenkamer realiseert zich dat dit onderzoek een relatief technisch karakter heeft. Informatiebeveiliging is een specialistisch vakgebied waarin technische, organisatorische en juridische aspecten samenkomen. Om de toegankelijkheid van het rapport te vergroten, is daarom een managementsamenvatting opgenomen waarin de belangrijkste conclusies, risico's en aanbevelingen overzichtelijk zijn weergegeven.

De centrale conclusie van het onderzoek is overwegend positief. De onderzoekers constateren dat de gemeente Meppel de afgelopen jaren belangrijke stappen heeft gezet om de informatiebeveiliging verder te versterken. Informatiebeveiliging heeft binnen de organisatie een duidelijke plaats gekregen en op

organisatorisch, technisch en fysiek vlak is een breed pakket aan beheersmaatregelen ingericht. De gemeente beschikt daarmee over een stevige basis om de digitale weerbaarheid verder te ontwikkelen, waarbij de volgende stap vooral ligt in het duurzaam borgen en aantoonbaar maken van de werking van de getroffen maatregelen.

Het onderzoek laat zien dat verdere ontwikkeling noodzakelijk blijft. De aanbevelingen richten zich onder meer op het verder professionaliseren van het managementsysteem voor informatiebeveiliging, het versterken van risicomanagement, het verder ontwikkelen van business continuity management en leveranciersmanagement en het vergroten van de aantoonbaarheid van de getroffen beheersmaatregelen. Daarnaast vragen de onderzoekers aandacht voor de voorbereiding op cyberincidenten, de monitoring van dreigingen en het verder terugdringen van de afhankelijkheid van informele werkwijzen. Daarmee kan de gemeente haar digitale weerbaarheid verder vergroten en de continuïteit van haar dienstverlening ook onder bijzondere omstandigheden beter waarborgen.

De onderzoekers constateren daarnaast dat de gemeenteraad een belangrijke rol vervult bij het versterken van de digitale weerbaarheid van de gemeente. Daarbij wijzen zij erop dat de reguliere verantwoordingsinformatie, waaronder de ENSIA-verantwoording, niet altijd een volledig beeld geeft van de feitelijke werking van de informatiebeveiliging. Om de kaderstellende en controlerende rol goed te kunnen vervullen, is het daarom van belang dat de raad het onderwerp regelmatig bespreekt en zich periodiek laat informeren over de ontwikkeling van de digitale weerbaarheid van de gemeente, bijvoorbeeld door de CISO.

De rekenkamer onderschrijft de conclusies en aanbevelingen van het rapport. Daarbij merken wij op dat het rapport een groter aantal aanbevelingen bevat dan gebruikelijk is bij rekenkameronderzoeken. Dit hangt rechtstreeks samen met het technische karakter van het onderwerp. Veel aanbevelingen hebben betrekking op operationele en specialistische onderdelen van informatiebeveiliging en zijn primair gericht aan het college van burgemeester en wethouders en de ambtelijke organisatie.

De rekenkamer adviseert uw raad daarom niet om zich op het niveau van afzonderlijke technische maatregelen uit te spreken. Veel van de aanbevelingen vragen specialistische kennis en raken de inrichting van processen, systemen en beveiligingsmaatregelen. Wij geven uw raad in overweging het college de ruimte te bieden om, binnen de bestuurlijke kaders die de raad stelt, een eigen afweging te maken over de wijze waarop en de volgorde waarin de aanbevelingen worden overgenomen en uitgevoerd.

De rol van de raad ligt daarbij primair in het beoordelen van de richting en de ambitie van de voorgestelde verbeteringen. De vraag voor de raad is niet zozeer welke technische maatregel moet worden getroffen, maar of het college voldoende doet om de digitale weerbaarheid van de gemeente duurzaam te versterken, risico's beheersbaar te houden en de continuïteit van de gemeentelijke dienstverlening te waarborgen. De verantwoordelijkheid van de raad ligt daarmee vooral in het stellen van kaders, het volgen van de voortgang en het bewaken van de resultaten.

Juist op dat punt heeft uw raad een belangrijke rol. Digitale veiligheid is niet uitsluitend een technische of ambtelijke aangelegenheid, maar nadrukkelijk ook een bestuurlijke verantwoordelijkheid. De gemeenteraad vervult hierin een belangrijke kaderstellende en controlerende rol door het onderwerp regelmatig te agenderen, prioriteiten te stellen, toe te zien op de beheersing van digitale risico's en ervoor te zorgen dat voldoende middelen beschikbaar zijn om de digitale weerbaarheid van de gemeente te versterken.

Wij bevelen uw raad daarom aan om:

- informatiebeveiliging structureel en regelmatig op de bestuurlijke agenda te plaatsen, hierover actief het gesprek te voeren met het college en bij de behandeling van de begroting blijvend aandacht te hebben voor voldoende middelen om de informatiebeveiliging en digitale weerbaarheid van de gemeente verder te versterken;
- gebruik te maken van de beschikbare handreikingen en hulpmiddelen van de VNG om invulling te geven aan de kaderstellende en controlerende rol van de raad;
- periodiek met het college en de CISO in gesprek te gaan over de ontwikkeling van de digitale weerbaarheid en de beheersing van risico's.

De rekenkamer benadrukt dat de aanbevelingen niet moeten worden gezien als een aanwijzing voor tekortschietend functioneren. Integendeel, zij zijn vooral gericht op het verder versterken en professionaliseren van een organisatie die op veel onderdelen al een stevige basis heeft gelegd.
Wij danken alle betrokken bestuurders, medewerkers en overige gesprekspartners voor hun openheid en medewerking aan dit onderzoek.

Wij hopen dat dit rapport bijdraagt aan een constructieve bespreking van de digitale weerbaarheid van onze gemeente.

Indien uw raad daaraan behoefte heeft, is de rekenkamer graag bereid het onderzoek, de conclusies en de aanbevelingen nader toe te lichten tijdens een bijeenkomst van uw raad of een commissie. Uiteraard zijn wij daarbij ook beschikbaar om vragen over het onderzoek en de bevindingen te beantwoorden.

Met vriendelijke groet,
Namens de rekenkamer Meppel,

Herman Odink,
Voorzitter

Bijlage:

- Rekenkamer onderzoek Informatiebeveiliging Gemeente Meppel
- Bestuurlijke reactie conceptrapport college Meppel d.d. 9 maart 2026