

Raadsvoorstel

Zaaknummer: 39851 / 2026

Onderwerp: Cybersecurity en de digitale weerbaarheid van de gemeente Maashorst

Auteur	: André Hengeveld
Team	: Rekenkamer Maashorst
E-mail	: Andre.Hengeveld@gemeentemaashorst.nl
Port.	: G.V.I.C. van Heeswijk

Effect op de begroting

☐ Ja ☒ Nee

Onderwerp

Rapportage Cybersecurity en de digitale weerbaarheid van de gemeente Maashorst

Voorstel

Het college van burgemeester en wethouders te verzoeken om:

1. In aansluiting op de planning- en controlcyclus de gemeenteraad periodiek te informeren over de belangrijkste cybersecurityrisico's, de voortgang van beheersmaatregelen, relevante wettelijke ontwikkelingen en de implementatie daarvan en de benodigde middelen en deskundigheid.
2. De gemeenteraad periodiek te informeren over de voortgang van de implementatie van aankomende wettelijke eisen op het gebied van cybersecurity.
3. Op korte termijn, uiterlijk in de eerstvolgende plannings- en controlcyclus, te zorgen voor een structurele inrichting van monitoring en sturing op cybersecurity, waarbij:
 - verantwoordelijkheden voor risico's en maatregelen expliciet worden belegd;
 - de voortgang van maatregelen systematisch wordt gevolgd;
 - de status van openstaande actiepunten uit audits en rapportages inzichtelijk is.
4. Te zorgen voor structurele borging van de benodigde cybersecuritydeskundigheid door intern de capaciteit te beoordelen en op niveau te houden, en de raad te informeren over de gemaakte keuzes.
5. Te zorgen voor een structurele en doorlopende aanpak van bewustwording rond cybersecurity, gericht op alle medewerkers, en de opzet en bereik hiervan periodiek inzichtelijk te maken voor de raad.
6. Te zorgen voor periodieke overlegmomenten met bestuur, management en relevante functionarissen (CISO, FG) over de stand van zaken van cybersecurity, en hierover aan de raad te rapporteren.

Inleiding

De Rekenkamer is, gelet op de actualiteit van het onderwerp, in de tweede helft van 2025 een onderzoek gestart naar de risico's en maatregelen rond cybersecurity en naar de mate waarin de gemeenteraad hierover geïnformeerd wordt.

Belangrijkste conclusie van het onderzoek is dat er een basis is gelegd voor cybersecuritybeleid maar dat de uitvoering verder operationeel belegd moet worden. Het onderwerp wordt met name door de IT-professionals gedreven en de bewustwording, inclusief de bestuurlijke aandacht, moeten nader uitgebouwd worden. Medio 2026 wordt wetgeving ingevoerd waarbij het verplicht wordt om zichtbaar te maken hoe risico's en maatregelen gemonitord worden. Hier zijn dus concrete stappen voor nodig. Datzelfde geldt voor de informatievoorziening naar de gemeenteraad, die tot nu niet actief en structureel geïnformeerd is over het proces van cybersecurity.

Beoogd effect

Het doel van de aanbevelingen van de Rekenkamer is om het proces van cybersecurity in organisatie en bestuur te versterken en om de gemeenteraad daarover structureel te laten informeren.

Argumenten

1.1 en 2.1 Periodieke informatievoorziening aan de gemeenteraad

De gemeenteraad wordt niet actief en structureel geïnformeerd over cybersecurity. De huidige ENSIA-informatie is onvoldoende om de kaderstellende en controlerende rol te kunnen vervullen. Bovendien verplicht de Cbw (verwacht medio 2026) dat bestuurlijk aantoonbaar is hoe toezicht op het cybersecurityproces plaatsvindt.

3.1 Structurele monitoring en sturing

De basis is gelegd, maar verantwoordelijkheden zijn nog niet concreet belegd en monitoring is nog niet structureel ingebed. Aankomende wetgeving vereist dat dit aantoonbaar op orde is, wat verdere uitwerking op korte termijn noodzakelijk maakt.

4.1 Borging van cybersecuritydeskundigheid

De benodigde deskundigheid staat onder druk door schaarste op de arbeidsmarkt. Zonder gerichte aanpak komt de continuïteit van het cybersecuritybeleid in gevaar. Samenwerking met collega-gemeenten en benutting van VNG-ondersteuning verdienen daarbij uitdrukkelijk aandacht.

5.1 Structurele bewustwording bij medewerkers

Cybersecurity is in de praktijk nog vooral een IT-aangelegenheid, terwijl het de hele organisatie raakt. De gestarte bewustwordingstrainingen zijn een mooi startpunt, maar een structureel programma gericht op alle medewerkers is nodig.

6.1 Periodiek overleg met bestuur, management en CISO/FG

Bestuurlijke betrokkenheid is reactief in plaats van structureel, waardoor cybersecurity te veel op uitvoerend niveau blijft. Periodiek overleg tussen bestuur, management en relevante functionarissen is nodig om het onderwerp op bestuurlijk niveau te verankeren.

Kanttekeningen

Wetgeving trad in werking tijdens het onderzoek

De Tweede Kamer nam de Cyberbeveiligingswet (Cbw) pas op 15 april 2026 aan; inwerking-treding wordt voorzien in het tweede kwartaal van 2026¹. Dit onderstreept de urgentie van de aanbevelingen: de gemeente loopt vooruit op wetgeving die op het punt staat in werking te treden.

Financiën

Dit voorstel heeft zelf geen financiële gevolgen.

Duurzame ontwikkeling

Dit voorstel draagt bij aan veilige, betrouwbare en toekomstbestendige digitale dienstverlening. Door de digitale weerbaarheid te versterken worden risico's op cyberincidenten en verstoringen beperkt en blijft de continuïteit van dienstverlening beter gewaarborgd. Dit is van belang voor nu én op de lange termijn.

SDG 16 – Vrede, justitie en sterke publieke diensten

Het voorstel draagt bij aan betrouwbare en weerbare publieke dienstverlening door systemen, gegevens en processen beter te beschermen tegen digitale dreigingen. Daarmee wordt het vertrouwen in de organisatie en digitale dienstverlening versterkt.

SDG 17 – Partnerschap om doelstellingen te bereiken

Cybersecurity vraagt om samenwerking tussen overheden, leveranciers en andere partners. Het voorstel stimuleert kennisdeling en gezamenlijke aanpak van digitale veiligheidsvraagstukken.

Het voorstel heeft geen directe negatieve effecten op de genoemde SDG's. Mogelijke extra ICT-kosten en energieverbruik blijven naar verwachting beperkt.



Participatie

Het onderzoek is verricht met betrokkenheid van de directe medewerkers. Hoer en wederhoor is ambtelijk toegepast en bestuurlijk is het rapport ook voor een reactie aangeboden.

Communicatie

De Rekenkamer biedt de onderzoeksrapportage aan bij zowel de gemeenteraad als het college. Wanneer de agendacommissie hiermee instemt, is de Rekenkamer bereid om de onderzoeksresultaten kort toe te lichten in een vergadering van de commissie Samenleving en Bestuur.

Vervolg

¹ [Tweede Kamer neemt Cyberbeveiligingswet aan](#)

Het is aan de gemeenteraad en het college om opvolging te geven aan de aandachtspunten die door de Rekenkamer zijn benoemd.

Bijlagen die onderdeel uitmaken van het besluit

Niet van toepassing.

Bijlagen ter informatie

1. Aanbiedingsbrief Rekenkamer Cybersecurity
2. Rapportage Cybersecurity en de digitale weerbaarheid van de gemeente Maashorst

Maashorst, 21 mei 2026

de voorzitter,

A. Hengeveld