

Raadsinformatiebrief

Aan: de leden van de raad
Van: het college
Datum: 8 september 2026
Onderwerp: Voortgang NIS2 & BIO2
Doel: ter kennisname/ter informatie
Aanleiding: toezegging tijdens raadsvergadering 7 juli 2026
Aard informatie: openbaar
Aantal bijlagen: 0

Aanleiding

Tijdens de behandeling van de jaarrekening op 7 juli jl. is gevraagd naar de voortgang van de Baseline Informatiebeveiliging Overheid 2 (BIO2) en de Network and Information Security Directive 2 (NIS2). Toegezegd is terug te komen op uw vragen. Naar aanleiding van deze vraag informeren wij u over de stand van zaken op het gebied van informatiebeveiliging, digitale weerbaarheid en de Cyberbeveiligingswet.

Informatie

Toezegging	Portefeuillehouder Pulles doet de toezegging om schriftelijke terug te komen op de vraag van Heusden Transparant Verbindt over hoe het staat met de voortgang van de gemeente m.b.t. BIO2 (Baseline Informatiebeveiliging Overheid 2) en NIS2 (Network and Information Security Directive 2).
Reactie	De Cyberbeveiligingswet is de Nederlandse implementatie van de Europese NIS2-richtlijn en stelt aanvullende eisen aan de digitale weerbaarheid van organisaties, waaronder gemeenten. De Cyberbeveiligingswet richt zich voor gemeenten voornamelijk op de zorgplicht, meldplicht, registratieplicht, bestuurlijke verantwoordelijkheid, risicomanagement, leveranciersmanagement en de aantoonbaarheid van getroffen maatregelen. De gemeente Heusden werkt volgens de uitgangspunten van de Baseline Informatiebeveiliging Overheid (BIO) en volgt actief de verdere ontwikkeling en toepassing van de Baseline Informatiebeveiliging Overheid 2 (BIO2) en de Cyberbeveiligingswet (Cbw). Daarbij sluiten wij aan op de landelijke kaders en adviezen van onder andere de Vereniging van Nederlandse Gemeenten (VNG), de Informatiebeveiligingsdienst (IBD) en het Nationaal Cyber Security Centrum (NCSC). De gemeente heeft zich bij het NCSC geregistreerd en geeft daarmee invulling aan de registratieplicht uit de Cyberbeveiligingswet. De invoering van de Cyberbeveiligingswet is geen nieuw startpunt voor de gemeente, maar sluit aan op de maatregelen en werkwijzen die de afgelopen jaren al zijn ingericht op basis van de BIO. Uit het onderzoek van de Rekenkamer blijkt dat de gemeente Heusden beschikt over een compleet en actueel beleidskader voor digitale veiligheid dat aansluit bij de geldende landelijke richtlijnen. Daarnaast constateert de Rekenkamer dat de gemeente actief werkt aan de verdere uitwerking van beleid naar tactische en operationele maatregelen.

	In de afgelopen jaren zijn verschillende technische, organisatorische en procesmatige maatregelen geïmplementeerd. Zo is in 2026 monitoring en response ingericht, waarmee de gemeentelijke ICT-omgeving continu wordt bewaakt op afwijkingen en mogelijke beveiligingsincidenten. Hiermee wordt verder invulling gegeven aan de zorgplicht die gemeenten hebben op het gebied van informatiebeveiliging en digitale weerbaarheid. Om de digitale weerbaarheid verder te versterken worden risicoanalyses en penetratietesten uitgevoerd en beveiligingsincidenten geëvalueerd. De uitkomsten hiervan worden gebruikt om risico's te beheersen en waar nodig aanvullende maatregelen te treffen. In 2025 is gestart met een verdere samenwerking tussen privacy, informatiebeveiliging en risicomanagement, zodat deze onderwerpen integraal worden benaderd binnen de organisatie. Daarnaast zijn afspraken gemaakt om informatiebeveiliging, privacy en digitale weerbaarheid nadrukkelijker onderdeel te maken van het integrale risicomanagement van de gemeente. Ontwikkelingen op het gebied van digitalisering, technologische innovatie en het veranderende cyberdreigingsbeeld worden daarbij structureel meegenomen in risicoanalyses en beheersmaatregelen, zodat de continuïteit van de dienstverlening en een betrouwbare informatievoorziening gewaarborgd blijven. Ook op het gebied van leveranciersmanagement worden stappen gezet. De gemeente heeft deelgenomen aan de VNG-pilot Samen Controleren, waarbij gezamenlijk wordt gewerkt aan het beoordelen van beveiligingsmaatregelen bij leveranciers. De gemeente is voornemens ook de komende jaren deel te nemen aan dergelijke initiatieven om de beheersing van leveranciersrisico's verder te versterken. Op dit moment verwachten wij dat de naleving van de Cyberbeveiligingswet voornamelijk vraagt om de doorontwikkeling van bestaande processen, beheersmaatregelen en governance. Eventuele aanvullende investeringen worden meegenomen binnen de reguliere begrotingscyclus.
--	---

Bijlage(n): ----