Hilversum
Mediastad

Raadsvoorstel

zaaknummer:

raadsvergadering:	11 november 2026
afdelingsnaam:	Rekenkamer
steller:	Eva de Spa, secretaris rekenkamer
datum:	29 september 2026
onderwerp:	Rekenkameronderzoek Informatiebeveiliging

Gevraagde beslissing

De raad besluit:

1. De aanbevelingen van de rekenkamer aan het college over te nemen en het college opdracht te geven deze uit te voeren.
2. De aanbevelingen van de rekenkamer aan de raad over te nemen en het college te verzoeken deze verder te laten uitwerken in concrete voorstellen.

Inleiding

In de afgelopen 30 jaar is de informatievoorziening van gemeenten enorm veranderd. Zo is de basisadministratie van (lokale) overheden volledig gedigitaliseerd, wordt steeds meer informatie digitaal opgeslagen en worden systemen en data steeds vaker aan elkaar gekoppeld. Gemeenten hebben als gevolg van de decentralisaties in het sociaal domein bovendien steeds meer (bijzondere) persoonsgegevens in beheer. Deze ontwikkelingen brengen veel voordelen met zich mee, maar ook risico's voor de beveiliging van deze informatie. Deze risico's worden vaak aangeduid met termen als *phishing*, *malware*, *spyware*, *ransomware*, *datalek* en *hack*.

Daarnaast hebben alle gemeenten inmiddels te maken met aangescherpte wetgeving. De Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke) zijn op 15 augustus 2026 in werking getreden. Dat betekent dat ruim 8.000 organisaties, waaronder gemeenten, in Nederland de komende jaren moeten voldoen aan strengere nieuwe regels voor digitale en fysieke weerbaarheid. De Cbw is de Nederlandse vertaling van de nieuwe Europese Network and Information Security richtlijn (NIS2). Samen met de Wwke vervangt deze wet de oude Wet beveiliging netwerk- en informatiesystemen (Wbni). Zowel de informatiebeherende als toezichthoudende instanties zullen op deze nieuwe, aangescherpte wetgeving moeten anticiperen.

Doel en vraagstelling onderzoek

Dit onderzoek heeft als doel inzicht te verkrijgen in de mate waarin de informatiebeveiliging van de gemeente Hilversum is gewaarborgd, mede in het licht van geldende en aankomende wet- en regelgeving. Daartoe is in het onderzoek gekeken naar de informatiebeveiliging vanuit drie

samenhangende onderdelen: opzet, bestaan en werking van maatregelen. Informatiebeveiliging is het proces van het nemen en beheren van passende technische en organisatorische maatregelen om informatie beschikbaar, integer en vertrouwelijk te houden. Het beleid en de organisatie van informatiebeveiliging moeten op papier in orde zijn, maar daarnaast in de praktijk ook goed worden uitgevoerd. Daarom is in dit onderzoek rekening gehouden met drie verschillende belangrijke factoren: mens, proces en techniek.

De rekenkamer vroeg zich af hoe weerbaar de gemeente is tegen actuele dreigingen als cybercriminaliteit en hoe het is gesteld met de informatieveiligheid van de gemeente Hilversum. In dit onderzoek is de rekenkamer uitgegaan van de volgende hoofdvraag: "*In hoeverre is de informatieveiligheid van de gemeente Hilversum gewaarborgd?*"

Methode

Het onderzoek heeft plaatsgevonden in de periode december 2025 tot en met juni 2026. Er zijn interviews gehouden en er is een documentanalyse uitgevoerd. De werking van maatregelen is in dit onderzoek getoetst door middel van operationele testen, waaronder een technische *pentest* (een '*hack*' op het digitale interne én externe netwerk), een *mailphishingtest* en een fysieke inlooptest. Deze testen geven inzicht in de weerbaarheid van de organisatie in de praktijk. Het onderzoek is uitgevoerd door onderzoeksbureau Hoffmann.

De bevindingen zijn vastgelegd in een Nota van Bevindingen, deze is voorgelegd voor ambtelijk wederhoor. Het eindrapport (inclusief de conclusies en aanbevelingen) is voorgelegd voor een bestuurlijke reactie. Een deel van de bevindingen is in geheime bijlagen gedeeld met de gemeentelijke organisatie, het college en de gemeenteraad. De rekenkamer wil immers geen gevoelige informatie openbaar maken die de informatiebeveiliging zou kunnen schaden.

Uitkomsten van dit onderzoek

Uit het onderzoek blijkt dat de gemeente Hilversum in de afgelopen jaren actief heeft geïnvesteerd en stappen heeft gezet om de informatiebeveiliging te verbeteren. De gemeente is zich bewust van het toenemende belang hiervan voor de continuïteit van de dienstverlening, de bescherming van persoonsgegevens en het vertrouwen van burgers. Het onderzoek laat zien dat de informatiebeveiliging een duidelijke basis kent, maar ook aandacht behoeft om nog beter te voldoen aan wetgeving. Zowel op het gebied van technische, organisatorische als menselijke factoren zijn verbeteringen mogelijk.

De gemeente Hilversum beschikt bijvoorbeeld over een vastgesteld Strategisch Gegevensbescherming en Informatiebeveiligingsbeleid (2025-2029), maar tegelijkertijd ontbreken her en der nog (uitwerkingen van) beleid en procedures en voldoet het informatiebeveiligingsbeleid nog niet aan de Baseline Informatieveiligheid Overheid (BIO en BIO2); het verplichte normenkader voor informatiebeveiliging dat zorgt voor een betrouwbaar basisniveau van informatiebeveiliging bij alle Nederlandse overheden. Ook is de impact van de wettelijk aangescherpte vereisten nog niet in beeld. Het *Information Security Management Systeem* (ISMS) is daarbij niet volledig en onvoldoende risicogestuurd ingericht. Een goed functionerend informatiemanagementsysteem kan bijdragen aan expliciete risicosturing, structurele toetsing van maatregelen en adequate informatievoorziening aan de raad.

Rollen en verantwoordelijkheden rondom informatiebeveiliging zijn op hoofdlijnen belegd, onder andere via het '*three lines of defense'*-model. De samenwerking met ICT, Facilitair en Informatiemanagement draagt bij aan de uitvoering van maatregelen. Echter, keuzes en verantwoordelijkheden zijn niet altijd eenduidig vastgelegd en het is de vraag of binnen het huidige toezichtsmodel met name de derde lijn voldoende is ingericht om tijdig en zelfstandig kwetsbaarheden in opzet, bestaan en werking van het

informatiebeveiligingsbeleid te signaleren (en de gemeenteraad hier voldoende scherp over te kunnen informeren).

Uit de in dit onderzoek uitgevoerde operationele testen is gebleken dat de organisatie in de praktijk niet altijd weerbaar is als het gaat om (digitale) techniek, menselijke factoren en fysieke beveiliging van vertrouwelijke gegevens. De externe digitale weerbaarheid van de gemeente Hilversum bleek op orde: het netwerk is van buitenaf niet toegankelijk voor onbevoegden. De interne digitale weerbaarheid daarentegen liet verbeterpunten zien. De resultaten van de *mailphishingtest* lieten zien dat het bewustzijn van digitale dreigingen bij medewerkers nog onvoldoende is. De fysieke inlooptesten toonden aan dat ook de fysieke informatiebeveiliging op onderdelen kwetsbaar is. De gevonden kwetsbaarheden zijn na uitvoering van de operationele testen direct gemeld aan de gemeente, zodat passende maatregelen konden worden getroffen.

Aanbevelingen

De rekenkamer beveelt aan:

Aanbevelingen aan het college

Aanbeveling 1: Zorg voor een volledig informatiebeveiligingsbeleid, dat aan de geldende wettelijke normen voldoet en is uitgewerkt in werkprocessen.

Uitleg: Zorg voor een volledig Informatiebeveiligingsbeleid dat in lijn is met de vereisten uit de BIO, Cbw en Wwke. Zorg dat het (strategische) informatiebeveiligingsbeleid op tactisch en operationeel niveau kan worden uitgevoerd door het te vertalen in concrete richtlijnen, procedures en werkinstructies. Evalueer welke uitwerkingen nog ontbreken en vul aan.

Aanbeveling 2: Zorg dat het informatiebeveiligingsbeleid is toegerust voor de overgang naar toekomstige wetgeving.

Uitleg: Zorg voor een Informatiebeveiligingsbeleid dat rekening houdt met nieuwe wetgeving en maak de overgang naar de BIO2 en de Cyberbeveiligingswet expliciet via een impact- en gap-analyse. Richt daarnaast een structurele werkwijze in om wijzigingen in wet- en regelgeving tijdig te signaleren, te beoordelen en door te vertalen naar beleid en maatregelen.
In deze analyses en uitwerking kan de impact van de fusie met Wijdemeren meteen worden meegenomen. Maak inzichtelijk welke stappen worden gezet en welke keuzes zijn gemaakt, zodat de voortgang en naleving aantoonbaar zijn.

Aanbeveling 3: Versterk de fundamenten van informatiebeveiliging door een volledig en risicogestuurd ISMS in te richten conform de BIO(2), in samenhang met het bredere risicomanagement binnen de organisatie.

Uitleg: Richt het ISMS zodanig in dat beleid, risico's, maatregelen, middelen en periodieke controles aantoonbaar samenhangen. Richt in samenhang met concern control structureel risicomanagement in, inclusief een centraal risicoregister als basis voor sturing, en kom tot een gedeeld beeld van de belangrijkste risico's. Gebruik risicoanalyses als basis voor prioritering, besluitvorming en de invulling van jaarplannen en inzet van middelen. Werk het principe van risicogestuurd werken concreet uit in beleid en processen, zodat duidelijk is op basis van welke risico's keuzes worden gemaakt en hoe deze worden vertaald naar maatregelen, procedures en werkinstructies.

Borg daarnaast een effectieve beleidscyclus (PDCA), waarin maatregelen en verbeterpunten structureel worden opgevolgd, geïmplementeerd en periodiek geëvalueerd en getoetst. Neem hierbij ook structureel testen van de digitale en fysieke beveiliging op, op basis van vastgesteld beleid en planning.

Aanbeveling 4: Intensiveer activiteiten om kennis van en bewustzijn over informatiebeveiliging en -risico's onder medewerkers te bevorderen.

Uitleg: Investeer structureel in informatieveiligheidsbewustzijn van medewerkers, (lijn)management, college en raad, waarbij menselijk handelen expliciet wordt meegenomen als kritieke risicofactor. Zorg dat het risicobewustzijn, de taakvolwassenheid en het eigenaarschap verder wordt versterkt om (vertrouwelijke) informatie bij de gemeente beter te beschermen. Bijvoorbeeld met een programma met bewustwordingsactiviteiten, dat kan worden geëvalueerd door de raad, met duidelijke, praktische uitleg gebaseerd op de belangrijkste risico's. Evalueer welke testen (zoals phishing-mails of incidentscenario's) kunnen bijdragen aan het verhogen van het bewustzijn van medewerkers en voer deze regelmatig uit.

Zorg dat taken, verantwoordelijkheden en bevoegdheden duidelijk belegd zijn bij alle functionarissen en dat deze nageleefd worden. Maak hierbij gebruik van de concrete verbetersuggesties in het vertrouwelijke rapport 'Bijlage 5.2 Verloop Mailphishing Gemeente Hilversum'.

Aanbeveling 5: Versterk de fysieke beveiliging van vertrouwelijke gegevens van de gemeente.

Uitleg: Maak hierbij gebruik van de concrete, technische verbetersuggesties in het vertrouwelijke rapport 'Bijlage 5.3 Verloop Fysieke Inlooptest Gemeente Hilversum'. Deze verbetersuggesties zijn, met het oog op de veiligheid, vooralsnog enkel gedeeld met de organisatie.

Aanbeveling 6: Vergroot de interne digitale weerbaarheid van de gemeente.

Uitleg: Maak hierbij gebruik van de concrete, technische verbetersuggesties in het vertrouwelijke rapport 'Bijlage 5.4 Verloop Digitale Pentest Gemeente Hilversum'. Deze verbetersuggesties zijn, met het oog op de veiligheid, vooralsnog enkel gedeeld met de organisatie.

Aanbeveling 7: Toets periodiek of het toezicht van de derde lijn voldoende aansluit bij de gewenste diepgang en effectiviteit, en voer waar nodig gerichte verbeteringen door.

Uitleg: Breng in kaart in hoeverre de taken, verantwoordelijkheden en bevoegdheden binnen het 'three lines of defense'-model helder zijn belegd en in de praktijk ook daadwerkelijk worden uitgevoerd. Dit draagt bij aan een meer realistisch en integraal beeld van de informatiebeveiliging en maakt het mogelijk om risico's en verbeterpunten eerder te signaleren.

Voer waar nodig aanpassingen door, bijvoorbeeld door rollen te verduidelijken, taken scherper af te bakenen of de samenwerking tussen de drie lijnen te versterken. Zo kan vanuit gedeelde verantwoordelijkheden en voldoende taakvolwassenheid effectiever worden gestuurd op informatiebeveiliging. Borg daarbij dat de onafhankelijkheid van de CISO, FG en interne auditfunctie behouden blijft, en dat deze rollen hun toezichthoudende taken onafhankelijk kunnen blijven uitvoeren.

Aanbeveling 8: Verbeter de periodieke informatievoorziening.

Uitleg: Zorg voor een informatievoorziening (bijvoorbeeld via een vast bestuurlijk dashboard, kwartaalrapportage of jaarlijkse themasessie) waarin raadsleden, B&W en ambtenaren actief en consistent worden geïnformeerd over actuele risico's, relevante regels, incidenten en ontwikkelingen op het gebied van informatieveiligheid. Dit voert verder dan de huidige ENSIA-rapportages. Zorg dat college en raad op basis van deze informatievoorziening structureel en consistent kunnen sturen en controleren op risico's, voortgang en naleving van de wettelijke zorgplicht op het gebied van informatiebeveiliging.

Zorg dat structureel en consistent een eenduidig, begrijpelijk risico- en dreigingsbeeld voor de gemeente wordt gedeeld. Zorg daarnaast dat raadsleden, B&W en ambtenaren gewezen worden op hun specifieke rollen, rechten en plichten rondom deze risico's in informatieveiligheid.

Aanbevelingen aan de raad

Aanbeveling 9: Maak afspraken over hoe en wanneer de raad geïnformeerd wordt over informatieveiligheid.

Uitleg: Bespreek in commissieverband op welke wijze de raad geïnformeerd wordt over informatieveiligheid en met welke frequentie. Leg deze afspraken vast.

Organiseer bijvoorbeeld halfjaarlijks een extra verdiepend (commissie)overleg naar aanleiding van de ENSIA-rapportages en de rapportages van de FG. En maak bijvoorbeeld afspraken over een structurele informatievoorziening aan de raad, opgesteld vanuit risicomanagementperspectief (m.b.v. een dashboard of rapportage). Door de focus te leggen op kritieke processen, en door te rapporteren op strategisch niveau, kan deze informatiestroom overzichtelijk worden gehouden voor de raad.

Aanbeveling 10: Intensiveer activiteiten voor de raad om kennis van en bewustzijn over informatiebeveiliging(srisico's) onder raads- en commissieleden te bevorderen.

Uitleg: Bevorder het kennisniveau en bewustzijn van veiligheidsrisico's onder raads- en commissieleden, bijvoorbeeld door periodiek een awareness-sessie te organiseren. Organiseer bewustwordingsactiviteiten met duidelijke, praktische uitleg, gebaseerd op de belangrijkste risico's specifiek voor raads- en commissieleden. Sluit hierbij waar mogelijk aan bij de activiteiten en trainingen die door de griffie en/of de organisatie worden georganiseerd. Vraag het college om de raad structureel mee te nemen in testen die bijdragen aan het verhogen van het bewustzijn.

Vervolg

In zijn *Bestuurlijke reactie rapport rekenkameronderzoek Informatieveiligheid 2026*, geeft het college onder andere een reflectie op de aanbevelingen aan de raad. De rekenkamer adviseert de raad om het college te verzoeken de aanbevelingen van de rekenkamer aan de raad verder te laten uitwerken in concrete voorstellen.

De Rekenkamer

De rekenkamer onderzoekt de doeltreffendheid, doelmatigheid en rechtmatigheid van het door de gemeente gevoerde beleid. De uitkomsten van de onderzoeken ondersteunen de raad bij het uitvoeren van de controlerende en kaderstellende taak, waarbij het accent ligt op het mogelijk lerend effect dat van de uitgebrachte onderzoeken kan uitgaan. De rekenkamer trekt op grond van het verrichte onderzoek conclusies en verstrekt vervolgens aanbevelingen aan de raad voor de toekomst. De griffier biedt vanuit zijn rol de raad een raadsvoorstel aan, waarin de conclusies en aanbevelingen van de rekenkamer zijn opgenomen. Op grond van dit raadsvoorstel besluit de raad over de afdoening van het rapport van de rekenkamer. De aanbevelingen van de rekenkameronderzoeken vanaf 1 januari 2023 worden jaarlijks gemonitord met het zogenoemde aanbevelingenregister. Daarmee is het instrument van kracht geworden voor college en raad, dat ervoor zorgt dat aanbevelingen van de rekenkamer in beeld blijven tot deze zijn uitgevoerd of in proces gebracht.

Hilversum, 29 september 2026,
De griffier,

dr. M. Pen

Bijlagen:

1. Eindrapport Rekenkameronderzoek Informatiebeveiliging
2. Collegebrief Bestuurlijke reactie rapport rekenkameronderzoek Informatieveiligheid 2026
3. Nawoord Rekenkamer Hilversum onderzoek Informatiebeveiliging
4. Persbericht afronding rekenkameronderzoek Informatiebeveiliging

Via het geheime kastje:

5. Bijlage 5.2 Verloop Mailphishing Gemeente Hilversum (geheim)
6. Bijlage 5.3 Verloop Fysieke Inlooptest Gemeente Hilversum (geheim)
7. Bijlage 5.4 Verloop Digitale Pentest Gemeente Hilversum (geheim)
8. Bijlage 5.9 Overzicht bestudeerde documenten (geheim)