Rapportage Cybersecurity en de digitale weerbaarheid van de gemeente Maashorst

Rekenkamer Maashorst

Hengeveld, A.
Rokers, P.

Uden
April 2026

maashorst

Voorwoord

De Rekenkamer, die in 2023 door de gemeenteraad van Maashorst is ingesteld, presenteert met dit document haar vierde rapport.

In deze onderzoeksrapportage lichten wij de resultaten en bevindingen van ons onderzoek naar cybersecurity en de digitale weerbaarheid van de gemeente Maashorst toe.

Gelet op het toenemende belang van cybersecurity is de huidige stand van zaken in kaart gebracht. Voorliggend rapport geeft weer op welke wijze aan dit onderwerp invulling gegeven wordt en beoogt tevens de gemeenteraad zich over haar kaderstellende en controlerende rol uit te laten spreken.

Wij spreken onze waardering uit voor de inzet van alle betrokken medewerkers van de gemeente en de andere geïnterviewden die aan dit onderzoek hebben meegewerkt.

Met vriendelijke groet,

De Leden van de Rekenkamer Maashorst

Inhoudsopgave

Voorwoord 2
Inleiding 4
Doel- en vraagstelling 5
Onderzoeksvragen 5
Methode en Planning 6
Resultaten 7
Subvraag 1. Wat is de huidige situatie rond cybersecurity? 7
Subvraag 2. Wat is de rol van de VNG? 8
Subvraag 3. Welke digitale risico's worden onderkend? 9
Subvraag 4. Welke maatregelen zijn/worden getroffen? 10
Subvraag 5. Welke rol voor de medewerkers? 11
Subvraag 6. Hoe vindt monitoring en evaluatie plaats? 12
Subvraag 7. Welke informatie gaat naar de gemeenteraad? 13
Conclusies 14
Aanbevelingen 16
Aan de gemeenteraad 16
Aan het college 16
Bijlagen 18
Bijlage 1: Teamplan ICT voortgang 18

Inleiding

De digitale dreiging voor publieke organisaties neemt toe. Voor gemeenten betekent dit dat vitale processen in toenemende mate afhankelijk zijn van goed beveiligde digitale systemen. Om deze reden hebben gemeenten en andere overheidsorganisaties te maken met regelgeving voor informatieveiligheid en privacy.

De Baseline Informatiebeveiliging Overheid (BIO) geeft al enkele jaren standaarden voor overheidsorganisaties die inmiddels door Europese regelgeving wordt aangevuld. Van deze Europese regels worden de Network and Information Security Directive (NIS2) en de Critical Entities Resilliance Directive (CERD) door vertaald in wetgeving voor ons land, de Cyberbeveiligingswet (CBW) en de Wet Weerbaarheid Kritieke Entiteiten (Wwke).

De VNG helpt gemeenten in het proces van cybersecurity en heeft daarvoor in juni 2025 de Agenda Digitale Veiligheid gepresenteerd (zie hierna).

Doel- en vraagstelling

De Rekenkamer wil met dit onderzoek naar cybersecurity inzicht krijgen in:

- De mate waarin de gemeente zicht heeft op digitale risico's;
- Hoe deze risico's worden beheerst;
- Welke informatie hierover beschikbaar is voor de leden van de gemeenteraad.

Door deze doelen na te streven kunnen wij het proces in kaart brengen en deze bondig rapporteren aan de gemeenteraad.

Onderzoeksvragen

De doelen van dit onderzoek worden gerealiseerd door het beantwoorden van een aantal onderzoeksvragen. De centrale onderzoeksvraag is:

- Hoe beheerst de gemeente de risico's op het gebied van cybersecurity, en hoe worden deze risico's inzichtelijk gemaakt voor de gemeenteraad?

De volgende subvragen worden hierbij gehanteerd:

1. Wat is de huidige situatie rond cybersecurity in de gemeente?
2. Welke rol speelt de Vereniging van Nederlandse Gemeenten (VNG)?
3. Welke digitale risico's worden onderkend?
4. Welke maatregelen zijn/worden getroffen?
5. Wat is de rol van medewerkers?
6. Hoe vindt monitoring en evaluatie plaats?
7. Welke informatie gaat naar de gemeenteraad?

Methode en Planning

Om tot antwoorden op de deelvragen te komen zijn externe en interne documenten bekeken en interviews gehouden met medewerkers. De medewerkers waren in eerste instantie voor de beeldvorming vooral ICT-gerelateerde medewerkers, in een later stadium zijn ook andere medewerkers betrokken in het onderzoek.

Vervolgens is in de laatste fase met de Chief Information Security Officer (CISO), ICT-management en -medewerkers een bijeenkomst georganiseerd, waarbij de laatste vragen, verzoeken en stand van zaken ter sprake zijn gekomen.

Resultaten

In deze sectie zijn de resultaten per subvraag beschreven. De resultaten zijn verkregen door medewerkers te interviewen en documenten te bestuderen.

Subvraag 1. Wat is de huidige situatie rond cybersecurity?

In deze paragraaf wordt de huidige situatie met betrekking tot de organisatie, beleid en beheer rondom cybersecurity beschreven.

Binnen de organisatie is een CISO werkzaam met cybersecurity als verantwoordelijkheid, samen met de Functionaris Gegevensbescherming (FG) als secondant voor privacy en Algemene Verordening Gegevensbescherming (AVG).

Vanwege de vereiste onafhankelijkheid is de CISO onlangs, lopende het onderzoek, bij Concern control geplaatst. De CISO moet vanuit zijn functie zicht hebben en houden om van daaruit vrij te kunnen rapporteren en daar is onafhankelijkheid bij gewenst. De capaciteit van de CISO is recent, met een doorlooptijd tot het eerste kwartaal 2026, uitgebreid met een externe functionaris. De CISO en FG werken nauw samen met de ICT-afdeling/-medewerkers.

De huidige CISO-functionaris is ruim 1,5 jaar in dienst. De FG is begin september 2025 met pensioen gegaan en momenteel wordt deze functie extern ingehuurd.

Cybersecurity wordt aangepakt met vier aandachtsgebieden:

- Mensen (organisatie): Beleid/Gedrag en bewustwording
- Mensen (IT): Digitale Awareness en beveiligingstrainingen/Toezicht en compliance/Toezicht en externe samenwerking
- Processen/Sturing: Controles en audits/Toezicht en risicomanagement/Incident- en changemanagement/Strategische en operationele sturing/Ontwikkelprogramma's
- Techniek: Technische maatregelen/Toegangsbeheer/Continuïteit en herstel/ Applicatiebeheer/Beleid

Voor de afdeling ICT is een Teamplan 2025 opgesteld met de doelstellingen voor 2025. De doelstellingen zijn in drie invalshoeken benoemd, te weten:

- Strategie en beleid;
- Veilige en betrouwbare (digitale) werkomgeving;
- Organisatiewensen.

In Bijlage 1 worden deze doelstellingen weergegeven. Ook voor 2026 is een teamplan opgesteld.

In 2024 is een Eenduidige Normatiek Single Information Audit (ENSIA) uitgebracht, het jaarlijks BIO-verantwoordingsdocument voor gemeenten en andere overheidsorganisaties om informatieveiligheid en datakwaliteit te toetsen en aan te tonen. De rapportage heeft een aantal aandachtspunten opgeleverd die zijn opgepakt. Verdeeld over de onderwerpen Beleid en organisatie, Personeel en toegang, Continuïteit en incidenten, Informatiesystemen en Databescherming zijn er totaal 180 maatregelen getroffen die overall een “groen” beeld opleverden.

Ook is een BIO-zelfevaluatie Verbeterlijst opgesteld en is er een assurance-rapport met collegeverklaring beschikbaar gekomen. De BIO-zelfevaluatie-rapportage heeft eveneens aandachtspunten opgeleverd die onder de aandacht van de organisatie zijn gebracht en waarvan een aantal nog onderhanden is.

De accountant besteedt jaarlijks in zijn managementletter aandacht aan informatieveiligheid. Daarbij ligt de focus op de betrouwbaarheid van de financiële verantwoording en niet specifiek op cybersecurity. In de managementletter 2024 stelt de accountant dat er een solide basis is gelegd voor cybersecurity door een uitgebreide risicoanalyse uit te voeren en diverse maatregelen te implementeren. Wel wordt opgemerkt dat het jaarlijks oefenen op het reageren op een gesimuleerd cyberincident continue aandacht behoeft, hetgeen inmiddels door scenariotrainingen wordt ingevuld.

Binnen de organisatie is de betrokkenheid van de directie belegd bij een van de directieleden. En ook met het College is de formele betrokkenheid ingevuld.

Belangrijke bevinding: De organisatie heeft de afgelopen 1,5 jaar stappen gezet in het verkrijgen van zicht op het cybersecurity-proces en hetgeen voor de weerbaarheid noodzaak is aan te nemen maatregelen. Een basis is gelegd maar deze moet verder uitgebouwd worden.

Subvraag 2. Wat is de rol van de VNG?

De VNG heeft middels de InformatieBeveiligingsDienst (IBD) voor alle gemeenten een ondersteuningsfunctie beschikbaar, die voor de gevolgen van de cyberbeveiligingswet beschikbaar is. Van belang hierbij zijn de cyberbeveiligingswet en de Wwke. De CBW is nog niet van kracht Dit houdt in dat de zorgplicht, meldplicht en toezicht op informatiebeveiliging gaan veranderen.

Qua zorgplicht moet een analyse van cyberrisico’s net als financiële en andere risico’s deel uitmaken van regulier risicobeheer. Het college van B&W is verplicht om informatiebeveiligingsmaatregelen goed te keuren en training te volgen om risico’s en bijbehorende maatregelen te kunnen beoordelen. In 2026 zal een duidelijke bestuurlijke aansprakelijkheid gelden voor invulling en beheersing van cybersecuritymaatregelen.

Voor digitale incidenten geldt een meldplicht.

Binnen de gemeente is het van belang dat de gemeenteraad toezicht houdt op de naleving van de wet. Kaderstelling en controleren alsmede het borgen van voldoende budget spelen hierbij een rol. Het is dus zaak dat de gemeenteraad zorgt dat ze de daartoe benodigde informatie tijdig ontvangt.

De Rijksinspectie Digitale Infrastructuur (RDI) houdt toezicht op de naleving en kan ook sancties opleggen voor gemeenten, maar ook voor bestuurders die in gebreke blijven.

Belangrijke bevinding: De VNG is beschikbaar als partner in het vergroten van de weerbaarheid en zal ook moeten worden ingezet waar mogelijk.

Subvraag 3. Welke digitale risico's worden onderkend?

Om te kunnen bepalen welke maatregelen noodzakelijk zijn om een veilige en betrouwbare digitale informatievoorziening te waarborgen, zullen allereerst de risico's die kunnen ontstaan, in beeld moeten zijn. In hoofdlijnen zal het hierbij gaan om risico's als gevolg van:

- Toegang van personen, fysiek dan wel functioneel, tot gebouwen, systemen en gegevens
- Uitval van processen en dienstverlening
- Ontbreken van juiste/voldoende capaciteit
- Onvoldoende awareness bij bestuur, management en medewerkers
- Datalek
- Het niet melden/registreren van incidenten
- Het niet maken en bewaken van de juiste afspraken met leveranciers van soft- en hardware

Volledigheidshalve wordt opgemerkt dat de IT-strategie/-architectuur en de inrichting van de technische systemen buiten de scope van het onderzoek zijn gelaten.

Een regelmatige risicoanalyse zal moeten worden uitgevoerd. Hierbij worden IT-specialisten, het management en medewerkers betrokken, zodat een juiste en breed gedragen uitkomst wordt bereikt. Op basis hiervan ontstaat vervolgens het inzicht dat nodig is om de juiste maatregelen te bespreken en weloverwogen keuzes te maken voor de invulling daarvan.

Door de gemeente Maashorst is eind 2025/begin 2026 een uitgebreide analyse uitgevoerd conform BIO2. Het door de IBD van de VNG beschikbaar gestelde normenkader met impact- en kanstabellen voor het bepalen van kritieke processen en risicoanalyses is hiervoor de basis geweest. Aan de hand van impact-, kans- en risicotabel kan een risicoregister voor de organisatie worden opgebouwd, waarmee gemeenten een

gemeenschappelijk kader gebruiken voor het bepalen van impact en kans van incidenten die kunnen optreden en tot een risico kunnen leiden.

Aan de hand van deze tabellen is door de CISO eind 2025/begin 2026 een uitgebreide analyse uitgevoerd waarbij risico's, kansen en maatregelen voor verschillende invalshoeken zijn vastgelegd. Per invalshoek (mens/apparatuur/programmatuur/gegevens/organisatie/omgeving/diensten) zijn risico's, kans op schade, impact etc. in kaart gebracht en vastgelegd met een aanzet naar de verantwoordelijke functionarissen in de organisatie. Deze verantwoordelijkheidstoewijzing moet nog verder worden gecompleteerd, zodat voor alle geconstateerde risico's het strategische en operationeel eigenaarschap is ondergebracht en kan worden opgevolgd.

Beheer en monitoring van het risicoregister zijn van belang en zullen nader moeten worden bepaald.

Voor de gemeenteraad is het gewenst inzicht te hebben in het proces van risicoanalyse en in de hoofdlijnen van de gekozen maatregelen/oplossingen. Op grond hiervan kan de gemeenteraad zich uitspreken over de keuzes die voorliggen, waar nodig bijsturen en vervolgens de budgettaire voorstellen beoordelen en goedkeuren.

Belangrijke bevinding: De risico's voor de gemeente zijn recentelijk geanalyseerd en geregistreerd. De verantwoordelijkheden die daarbij horen, zijn nog niet gedefinieerd en toegewezen. Dit zal de komende maanden worden vastgelegd opdat opvolging kan plaatsvinden.

Subvraag 4. Welke maatregelen zijn/worden getroffen?

Aan de hand van de uitgevoerde risicoanalyse, zoals hiervoor geduid, worden per invalshoek (mens, apparatuur, programmatuur, gegevens, organisatie, omgeving, diensten) maatregelen genoemd die ingevoerd kunnen worden.

Mede door veranderende wet- en regelgeving worden gemeenten en andere overheidsorganisaties geacht over te gaan tot het inschakelen van specifieke dienstverlening, Security Information and Event Management/Security Operations Center (SIEM-SOC). Hier zijn inmiddels voorstellen voor gedaan. Het SIEM-systeem verzamelt en analyseert logbestanden van IT-systemen en vangt realtime signalen op, wat de signaleringstijd heel kort maakt. SOC bestaat uit een ondersteuningsteam dat continue meldingen van SIEM beoordeelt en actie neemt. Inmiddels zijn er middelen in de begroting van 2026 beschikbaar gesteld, is een opdracht geformuleerd en wordt een projectleider geworven.

Maatregelen zijn sterk afhankelijk van de risico's die gelopen worden. De recent uitgevoerde risicoanalyse is de basis en aan de hand van de vastgelegde risico's zal het risicomanagement moeten worden geconcretiseerd.

In de teamplannen voor 2025 en 2026 zijn er acties opgenomen die deels al zijn gerealiseerd en deels voor de toekomst gepland zijn. Belangrijke zaken om de risico's die volgen uit de BIO2 die is uitgevoerd door de CISO te beheersen zijn:

- Toewijzen van verantwoordelijkheden in de organisatie;
- Inrichten van monitoring en beheersing van het risicoregister.

Belangrijke bevinding: De onlangs uitgevoerde en vastgelegde risicoanalyse geeft ook de te nemen maatregelen weer. Deze zullen in het monitoringsproces van de drie geschetste niveaus zichtbaar moeten worden.

Subvraag 5. Welke rol voor de medewerkers?

Zoals bij subvraag 1 beschreven, is er aandacht in het teamplan voor de digitale awareness van de medewerkers. Trainingen in de vorm van e-learning zijn in ontwikkeling op het gebied van informatie- en dataveiligheid en AVG. Het huidige e-learningsysteem wordt vervangen en het platform hiervoor wordt vernieuwd. Vanuit ENSIA is het een verplichting om dit aan te bieden.

De huidige stand van zaken is dat het nieuwe systeem is aanbesteed en wordt geïmplementeerd. Nadat dit is afgerond kunnen de leermodules worden toegevoegd en beschikbaar worden gesteld. De inhoud van de modules is in de basis bekend en bestaat hoofdzakelijk uit de onderwerpen die al voorhanden waren. Nieuw is de training met betrekking tot AI-geletterdheid, voor deze toevoeging zijn middelen ter beschikking gesteld door de directie. Volledigheidshalve wordt vermeld dat de externe accountant in zijn laatste managementletter duidelijk aangeeft dat regelmatige oefening bewaakt moet worden.

In de organisatie worden er diverse systemen in de buitendienst gehanteerd die worden geleverd en vaak worden beheerd door de leveranciers of andere externe partijen. Dat betekent dat deze partijen toegang hebben tot de data waarvan de gemeente eigenaar is. Uit interviews blijkt dat er vanuit deze systemen gecommuniceerd wordt met de buitendienstmedewerkers. De externe partijen die het hier betreft, voeren het beheer van de systemen en dienen te voldoen aan eisen die zijn opgesteld. Daarnaast wordt niet toegestaan dat externen toegang krijgen, hiervoor is geen protocol. De verantwoordelijkheid hiervoor is neergelegd bij de functioneel beheerders. Voor het onderzoek is er gesproken met de functioneel beheerders voor riolering, verkeersinstallaties en gladheidsbestrijding.

Het feit dat de organisatie voorstander is van "mandateren zo laag mogelijk in de organisatie" levert voor cybersecurity een aandachtspunt op, want niet alleen medewerkers moeten verantwoordelijkheid voelen, maar ook de leidinggevenden hebben een duidelijke verantwoordelijkheid bij cybersecurity.

Belangrijke bevinding: Er ligt een basis voor het betrekken en informeren van de medewerkers. Structurele inbedding in de organisatie vraagt aandacht.

Subvraag 6. Hoe vindt monitoring en evaluatie plaats?

Niveaus van monitoring

Monitoring en evaluatie van het cybersecurityproces moet in drie niveaus worden onderscheiden.

- Allereerst is monitoring en evaluatie van belang voor het interne cybersecurityproces. CISO, FG en hoofd ICT zijn hierbij de functies in wiens takenpakket dit primair thuis hoort. In de reguliere activiteiten dienen zij de gang van zaken te volgen en te reageren waar zaken anders verlopen dan afgesproken of bedoeld.
- Daarnaast zal binnen de organisatie de gang van zaken moeten worden gevolgd en moet duidelijk gemaakt worden of en zo ja welke afwijkingen van het beoogde proces zijn vastgesteld en wat daarna gedaan is. Lijnmanagement, directie en college zullen elk op het eigen niveau moeten kunnen vaststellen of het cyberproces voor hen regulier verloopt of dat er afwijkingen en verstoringen zijn.
- Een derde niveau ligt op het niveau van de gemeenteraad. Cybersecurity is dermate van belang voor het functioneren van de organisatie dat de gemeenteraad in hoofdlijnen moet sturen en controleren dat binnen de gemeente al het mogelijke gedaan wordt/is om de weerbaarheid op cybersecurity te borgen.

Instrumenten voor monitoring

Er worden verschillende rapportages en onderzoeken opgesteld die voor de monitoring en evaluatie gebruikt kunnen worden.

De jaarlijkse ENSIA-rapportage is binnen de regelgeving een autonoom instrument dat van belang is om aan te tonen dat men “in control” is. Via de Planning & Controlcyclus is hier in 2025 over gerapporteerd.

Andere documenten die van belang zijn, zijn onder andere de rapportages van uitgevoerde penetratietesten en uitgevoerde zelfevaluaties. Maar ook de managementletter van de extern accountant is een te hanteren document hierbij.

In de loop van 2026 zal wetgeving van de organisatie bestuurlijke verplichtingen vragen die erop neerkomen dat bestuurlijke verantwoordelijke functionarissen zichtbaar moeten kunnen maken dat “actief toezicht heeft plaatsgevonden”, met andere woorden dat kan worden aangetoond hoe met de uitkomsten en bevindingen van die rapportages is omgegaan. Blijft men in gebreke, dan kunnen boetes opgelegd worden.

Het is van belang dat vooraf bepaald wordt hoe de niveaus van monitoring zich met elkaar verhouden en op elkaar aansluiten. En hoe welke instrumenten daarbij een rol spelen.

Belangrijke bevinding: Monitoring en evaluatie van het cybersecurityproces vinden plaats, maar zijn nog niet structureel en samenhangend organisatorisch ingebed.

Subvraag 7. Welke informatie gaat naar de gemeenteraad?

De informatieverschaffing aan de gemeenteraad over cybersecurity bestaat uit generieke informatie over ENSIA-verantwoording in Planning & Control documenten. Dit betreft wettelijk verplichte informatie (op hoofdlijnen). In welke mate andere wenselijke informatie voor de gemeenteraad gewenst is, zal moeten worden nagegaan. Zeker onder nieuwe wetgeving zal de gemeenteraad blijk moeten geven van betrokken willen zijn bij sturing en controle van het cybersecurityproces. De informatie die daarbij nodig is, moet nog worden bepaald.

Belangrijke bevinding: De gemeenteraad ontvangt momenteel generieke, wettelijk verplichte informatie over de ENSIA-verantwoording van het cybersecurityproces. Welke aanvullende informatie nodig is om goed te kunnen sturen en controleren, is nog niet bepaald.

Conclusies

Dit hoofdstuk geeft de conclusies die op basis van de bevindingen van de onderzoeksvragen getrokken kunnen worden. De relatie met de onderzoeksvragen wordt per conclusie aangegeven.

1. Basis voor cybersecuritybeleid aanwezig, maar uitvoering nog niet operationeel belegd binnen de organisatie (deelvraag 1, 3, 4)

De gemeente heeft de afgelopen anderhalf jaar stappen gezet om de situatie met betrekking tot cybersecurity in beeld te krijgen en op grond daarvan het beheersingsproces in te richten (deelvraag 1). Er is inmiddels een uitgebreide, op de voorgeschreven regelgeving gebaseerde, risicoanalyse (deelvraag 3) beschikbaar met daarin de maatregelen (deelvraag 4) die nodig kunnen zijn indien bepaalde risico's daarom vragen. Het toewijzen van de verantwoordelijkheden voor deze risico's (en maatregelen) aan de betrokken organisatieonderdelen is echter nog niet uitgevoerd.

2. Cybersecurity primair IT-gedreven, proactieve bestuurlijke sturing nog in ontwikkeling (deelvraag 2, 6)

Cybersecurity is op dit moment vooral nog een issue voor de IT-professionals. Als er bestuurlijke aandacht nodig is, is die bereikbaar en beschikbaar. Maar andersom kan de bestuurlijke aandacht voor het proces meer proactief gestructureerd worden, wat de inbedding van het onderwerp in de organisatie zal versterken (deelvraag 6). Juiste positionering van de VNG-ondersteuningsmogelijkheden moet hierbij worden meegenomen (deelvraag 2). Het onderwerp is immers niet alleen voor de IT-professionals van belang.

3. Capaciteit van deskundigheid staat onder druk, bewustwording binnen de organisatie staat nog aan het begin (deelvraag 5)

De huidige stand van cybersecurity is in belangrijke mate gerealiseerd dankzij beschikbare deskundigheid. De capaciteit staat onder druk, waardoor de continuïteit en verdere ontwikkeling van het cybersecuritybeleid onder druk kunnen komen te staan (deelvraag 5).

Aandacht voor en bewustwording bij de medewerkers voor cybersecurity wordt door middel van e-learning en andere trainingen ingevuld, maar is nog maar kort gestart. Een benadering met een continue aandacht naar de organisatie is gewenst.

4. Monitoring en sturing zijn in ontwikkeling (deelvraag 6)

Op basis van wettelijke regelgeving die in de loop van 2026 ingevoerd gaat worden, moet er bestuurlijk zichtbaar worden gemaakt of en hoe men actief toezicht op het cybersecurityproces houdt. Monitoring en evaluatie zijn dus van belang om goed in te regelen. Beiden vinden momenteel wel plaats, maar zijn nog niet structureel en samenhangend organisatorisch ingebed. Dit moet de organisatie op korte termijn gaan invullen.

5. Informatievoorziening aan de gemeenteraad is ontoereikend (deelvraag 7)

De gemeenteraad is de afgelopen periode niet actief en structureel geïnformeerd over de

stand van zaken rondom cybersecurity, anders dan generieke, wettelijk verplichte ENSIA-informatie over de hoofdlijnen van het cybersecurityproces in P&C-documenten. ENSIA-informatie op hoofdlijnen is nodig, maar niet voldoende. Zonder aanvullende, risicogerichte en bestuurlijk relevante informatie kan de raad zijn kaderstellende en controlerende rol op dit onderwerp nog onvoldoende uitoefenen. Gevolg is dat de gemeenteraad moeilijk kan beoordelen over benodigde middelen en of wordt voldaan aan beleid en wet- en regelgeving.

Overkoepelend beeld

De gemeente heeft de basis voor cybersecuritybeleid gelegd, maar de bestuurlijke inbedding, verantwoordelijkheidsverdeling en structurele monitoring dienen nog te worden uitgewerkt. Wil er sprake zijn van een aantoonbaar en integraal beheerst cybersecurityproces, dan is die verdere uitwerking noodzaak.

Aanbevelingen

Aan de gemeenteraad

1. Versterk de informatiepositie van de gemeenteraad.

Draag het college op om, in aanvulling op de generieke ENSIA-informatie, een structurele rapportagesystematiek in te richten, waarbij de gemeenteraad in aansluiting op de planning- en controlcyclus (en zo nodig tussentijds) wordt geïnformeerd over:

- de belangrijkste cybersecurityrisico's;
- de voortgang van beheersmaatregelen;
- benodigde middelen en deskundigheid.

Informatievoorziening aan de raad kan bestaan uit het rapporteren over het volwassenheidsniveau t.a.v. cybersecurity. Hiervoor zijn gedefinieerde niveaus die dan ook direct kunnen worden gebruikt om de ambitie te verwoorden. Aan het college dan de taak om dit assessment uit te voeren en het niveau te verantwoorden.

Het rapport van Berenschot (2025)[1] dat in opdracht van de VNG is uitgevoerd, geeft richting aan de in te zetten middelen, rekening houdend met het volwassenheidsniveau en de omvang van de gemeente.

2. Zorg dat de raad zicht heeft op voorbereiding op wetgeving.

Laat het college de raad periodiek informeren over de voortgang van de implementatie van aankomende wettelijke eisen op het gebied van cybersecurity. De raad gebruikt deze informatie om te beoordelen of het college tijdig en effectief maatregelen neemt en kan op basis daarvan inzet van middelen toekennen.

Aan het college

3. Richt monitoring en sturing structureel in.

Zorg 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.

Realiseer dit op korte termijn en uiterlijk in de eerstvolgende planning- en controlcyclus.

[1] https://vng.nl/artikelen/rapport-inzicht-in-gemeentelijke-kosten-en-aanpak-van-informatiebeveiliging

4. Borg de beschikbaarheid van deskundigheid.

Zorg voor structurele borging van de benodigde cybersecuritydeskundigheid door intern de capaciteit te beoordelen en op niveau te houden. Onderzoek daarbij onder meer de mogelijkheden voor samenwerking met andere gemeenten of gezamenlijke inkoop van expertise, en informeer de raad over de gemaakte keuzes.

5. Versterk structureel de bewustwording binnen de organisatie

Zorg voor een structurele en doorlopende aanpak van bewustwording rond cybersecurity, gericht op alle medewerkers, en maak de opzet en het bereik hiervan periodiek inzichtelijk voor de raad.

6. Organiseer structurele bestuurlijke en ambtelijke afstemming

Zorg voor periodieke overlegmomenten met bestuur, management en relevante functionarissen (CISO, FG) over de stand van zaken van cybersecurity. Leg de resultaten vast en rapporteer deze aan de raad ter ondersteuning van toezicht en evaluatie.

Bijlagen

Bijlage 1: Teamplan ICT voortgang

De afdeling ICT werkt met een teamplan waarin jaarlijks de te behalen doelen worden weergegeven. Dit teamplan kent drie onderdelen, te weten:

- Strategie en beleid
- Veilige en betrouwbare (digitale) werkomgeving
- Organisatiewensen.

Bijlage 1 geeft een beeld van de doelstellingen per onderdeel van het teamplan.

Het deel Strategie en beleid kent twee doelstellingen met directe betekenis voor informatiebeveiliging. Per 31-12-25 moet het ICT-beveiligingsbeleid zijn vastgesteld en het calamiteitenbeleid en -proces moet per 1-3-25 beschikbaar zijn.

Van het deel Veilige en betrouwbare (digitale) werkomgeving zijn alle doelstellingen direct van belang voor informatieveiligheid. In 2025 zijn afgerond:

- Uitgebreide uitwijktest per 1-6-2025
- Bedrijfssportal en IT-compliance ingericht en uitgerold voor 1-2-2025
- Cybersecuritysimulatie afgerond voor 1-6-2025
- Managed Data-omgeving (MDO) voor externe laptops voor 1-9-2025

Van o.a. onderstaande doelstellingen moet de definitieve afronding in 2026 plaatsvinden:

- Onderzoek en managen van alle beveiligingsrisico's (1-9-2026)
- Hogere norm vaststellen voor autorisaties (1-9-2026)
- Siem/SOC beveiligingsoplossing in werking (31-12-2026)

Om ook in 2026 de na te streven doelen te kunnen realiseren is aandacht voor de capaciteit van de afdeling een attentiepunt.