Resultaten vervolgonderzoek
Informatiebeveiliging
Rekenkamercommissie Haarlemmermeer
Juli 2020

1. Inleiding

De Rekenkamercommissie (RKC) gaat enige jaren na publicatie van een onderzoek na wat er met de door de raad overgenomen aanbevelingen van de RKC is gebeurd. Dit doen we in een 'vervolgonderzoek'. We hebben een vervolgonderzoek gedaan naar het onderzoek *Bewustwording als sleutel, de staat van de informatiebeveiliging in Haarlemmermeer* uit 2016. De resultaten hiervan staan in deze notitie.

1.1. Wat verstaan we onder informatiebeveiliging?

Informatiebeveiliging gaat over het treffen en onderhouden van maatregelen om de beschikbaarheid, vertrouwelijkheid en betrouwbaarheid van de informatievoorziening en informatiesystemen te garanderen.

1.2. Wat onderzochten we in 2016 en wat besloot de raad?

Het onderzoek *Bewustwording als sleutel, de staat van de informatiebeveiliging in Haarlemmermeer* uit 2016 richt zich alleen op maatregelen om de *vertrouwelijkheid* van informatie te garanderen. Vertrouwelijkheid wil zeggen dat informatie alleen te benaderen is door mensen die hiertoe gemachtigd zijn.

De centrale onderzoeksvraag in het onderzoek luidt:

> *In hoeverre heeft de gemeente Haarlemmermeer de informatiebeveiliging van de informatiesystemen in de organisatie doeltreffend ingericht, waarmee risico's worden afgedicht, waardoor geen oneigenlijke toegang tot de gevoelige informatie (zoals persoonsgegevens) kan worden verkregen en/of informatie in verkeerde handen kan vallen?*

In het onderzoek hebben we ons op drie aspecten van informatiebeveiliging gericht, te weten de organisatie, de techniek en de mens.

Het rapport bevat vijf aanbevelingen. In de raadsvergadering van 31 maart 2016 besloot de raad deze aanbevelingen unaniem over te nemen (zie ook hoofdstuk 2).

Voor een uitgebreide beschrijving van de vraagstelling, resultaten, conclusies, aanbevelingen en bestuurlijke toezeggingen van het oorspronkelijke onderzoek uit 2016 verwijzen we naar de website van de RKC[1].

1 https://haarlemmermeergemeente.nl/rekenkamer/onderzoeken-2016

1.3. Wat is de reikwijdte van dit vervolgonderzoek?

In dit vervolgonderzoek toetsen we in hoeverre het college het besluit van de raad heeft uitgevoerd. Het vervolgonderzoek beperkt zich hiertoe. We hebben geen nieuw onderzoek gedaan naar de stand van de informatiebeveiliging bij de gemeente.

1.4. Hoe hebben we dit vervolgonderzoek uitgevoerd?

We hebben informatie vergaard door documenten te analyseren en interviews te houden. Op basis hiervan hebben we onze bevindingen vastgelegd in deze notitie. Deze bevindingen zijn voor wederhoor op de feiten aan de ambtelijke organisatie voorgelegd. De conclusies en aanbevelingen komen voor rekening van de RKC.

1.5. Hoe is deze notitie opgebouwd?

Hoofdstuk 2 gaat in op de bevindingen van dit vervolgonderzoek. Hoofdstuk 3 geeft onze conclusies weer en hoofdstuk 4 bevat twee nieuwe aanbevelingen en een korte slotbeschouwing.

2. Bevindingen

Dit hoofdstuk beschrijft achtereenvolgens:

- wat de raad in maart 2016 heeft besloten (§ 2.1.);
- hoe het college dit besluit tussen maart 2016 en maart 2020 heeft opgevolgd (§ 2.2.) en
- wat samengevat de belangrijkste bevindingen zijn (§ 2.3.).

2.1. Wat heeft de raad besloten in 2016?

Tabel 1 geeft een overzicht van de aanbevelingen in het RKC-onderzoek uit 2016 en het besluit dat de raad op 31 maart 2016 nam over dit onderzoek.

Tabel 1 – Aanbevelingen en beslispunt naar aanleiding van RKC-onderzoek Informatiebeveiliging

	Oorspronkelijke formulering	**Gewijzigde formulering**
Aanbeveling 1	Vraag het College om het ambitieniveau voor informatiebeveiliging duidelijker uit te werken, en dit op te nemen in de planning en control cyclus.	*Ongewijzigd overgenomen*
Aanbeveling 2	De gemeente moet meer inzetten op het verhogen van bewustwording ten aanzien van informatiebeveiliging.	*Ongewijzigd overgenomen*
Aanbeveling 3	Investeer in de organisatie van informatiebeveiliging en zorg dat informatiebeveiliging een taak van de hele gemeentelijke organisatie wordt.	*Ongewijzigd overgenomen*
Aanbeveling 4	Voer regelmatig een integrale audit of pentesten uit op kwetsbaarheden.	*Ongewijzigd overgenomen*
Aanbeveling 5	Investeer in de ontwikkeling van monitoring en signalering, zodat je kunt ingrijpen bij aanvallen op de informatiebeveiliging.	*Ongewijzigd overgenomen*
Geamendeerd beslispunt	Het college van B&W opdracht te geven aan de aanbevelingen van de RKC invulling te geven en de raad hierover binnen een jaar te informeren.	*Gewijzigd in:* Het college van B&W opdracht te geven de aanbevelingen van de RKC te verwerken in een plan van aanpak met daarbij een gespecificeerde begroting, en deze ter besluitvorming aan de raad voor te leggen bij de behandeling van de Voorjaarsrapportage.

Uit de tabel blijkt dat de raad de vijf aanbevelingen ongewijzigd overnam en instemde met een gewijzigd beslispunt.

2.2. Hoe heeft het college het besluit en de aanbevelingen opgevolgd?

Hieronder geven we aan wat het college in de periode tussen maart 2016 en maart 2020 heeft gedaan met het (gewijzigde) beslispunt en de vijf aanbevelingen.

Dit doen via de volgende structuur:

- Formulering: Hoe luidt het besluit of de aanbeveling?
- Beoordeling: Vindt de RKC dat het college heeft voldaan aan het besluit of de aanbeveling?
- Toelichting: Waarop baseert de RKC deze beoordeling?

2.2.1. Opvolging geamendeerd beslispunt

Formulering

Het college van B&W opdracht te geven de aanbevelingen van de RKC te verwerken in een plan van aanpak met daarbij een gespecificeerde begroting, en deze ter besluitvorming aan de raad voor te leggen bij de behandeling van de Voorjaarsrapportage.

Beoordeling

Het college heeft voldaan aan deze opdracht.

Toelichting

Op 16 juni 2016 heeft het college een Nota van B&W *Informatiebeveiliging op orde*[2] met een bijbehorend Plan van Aanpak ter informatie aan de raad aangeboden. De nota gaat uitgebreid in op het rekenkameronderzoek *Bewustwording als sleutel*. Bijlage 1 van deze nota geeft in een schema weer hoe de aanbevelingen van de RKC zijn verwerkt in het Plan van Aanpak.

In het Plan van Aanpak is een begroting opgenomen voor de te nemen structurele maatregelen. Deze begroting is op twee manieren gespecificeerd:

- onderscheid in kostensoorten: structurele en incidentele kosten;
- onderscheid in maatregelen: technisch, personeel en organisatorisch.

Deze financiële gevolgen zijn bij de Voorjaarsrapportage 2016 verwerkt in de gemeentebegroting die de raad op 30 juni 2016 heeft vastgesteld.

2.2.2. Opvolging aanbeveling 1

Formulering

Werk het ambitieniveau voor informatiebeveiliging duidelijker uit, en neem dit op in de planning en control cyclus.

Beoordeling

Het college heeft deze aanbeveling deels opgevolgd.

Toelichting

In het Plan van Aanpak bij de nota *Informatiebeveiliging op orde* uit mei 2016 geeft het college aan nog dat jaar de internationale standaard *COBIT/CMMI maturity level 2* te willen halen om een minimale basis te hebben. Het is niet vast te stellen of dit niveau destijds is gerealiseerd omdat de gemeente dit niet expliciet heeft gemeten.

In het Plan van Aanpak stelt het college ook later in 2016 het ambitieniveau voor de jaren erna te bepalen. Dit is niet gebeurd.

Op 27 november 2018 heeft het college nieuw beleid voor informatiebeveiliging vastgesteld. In dit beleid wordt de Baseline Informatiebeveiliging Gemeenten (BIG) als meetlat genoemd, een

[2] 2016.0022206

landelijke (niet volledig verplichte) norm voor gemeenten op het gebied van informatie-beveiliging. De gemeente wil aan de hand van deze meetlat de lat van informatiebeveiliging in stappen hoger leggen.

Per 1 januari 2020 is de BIG vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De BIO bouwt voort op de BIG en vormt één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normen[3]. De BIO legt meer nadruk op risicomanagement dan de BIG, die meer gaat over specifieke maatregelen. Een ander belangrijk verschil is dat maatregelen in de BIO wettelijk verplicht zijn.

Uit de *Nota privacy, informatiebeveiliging en informatiebeheer* en het *Informatiebeveiligings-beleid gemeente Haarlemmermeer 2018* van 27 november 2018 en de interviews voor dit vervolgonderzoek komt naar voren dat de gemeente tussen 2016 en 2019 nooit volledig heeft voldaan aan de normen van de BIG. Dit was ook niet verplicht. De gemeente voldoet in maart 2020 niet aan alle normen uit de BIO, die wél verplicht is. Enkele voorbeelden van normen waaraan in maart 2020 nog *niet* is voldaan, zijn:

- "Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel."
- "De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is."
- "Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis."

De gemeente kiest voor een 'risicogestuurde' werkwijze bij het verbeteren van de informatiebeveiliging. Risicosturing richt zich op het effectief en efficiënt beheersen van de risico's die het behalen van gestelde doelen bedreigen. Het volledig voldoen aan de landelijke norm (BIO) is hieraan ondergeschikt voor de gemeente. De RKC ziet het nut van een risicogestuurde werkwijze in. Dit laat onverlet dat de gemeente ook aan de landelijk verplichte normen moet gaan voldoen. Hoe en wanneer de gemeente dit gaat doen is nu niet nader gespecificeerd en/of meetbaar gemaakt.

Het college rapporteert op structurele basis in de P&C cyclus over het informatiebeveiligings-beleid zonder expliciet te zijn over (de ontwikkeling van) het ambitieniveau en hoe dit te meten.

2.2.3. Opvolging aanbeveling 2

Formulering
Zet meer in op het verhogen van bewustwording ten aanzien van informatiebeveiliging.

Beoordeling
Het college heeft deze aanbeveling deels opgevolgd.

Toelichting
De gemeente heeft in het Plan van Aanpak uit 2016 een bewustwordingsprogramma aangekondigd dat later dat jaar van start zou gaan. Concrete maatregelen zijn geformuleerd om medewerkers bewuster te maken van risico's op het gebied van informatiebeveiliging, zoals:

- Lesmodules van VNG als onderdeel van de uitrol van De Nieuwe Werkplek. Medewerkers moesten in 2017 certificaten behalen voor deze modules voordat ze hun nieuwe laptop kregen.

[3] Zie https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/ voor meer informatie.

- Het voeren van campagnes met vloer- en wandstickers, whiteboardstickers en posters, gericht op bijvoorbeeld het zichtbaar dragen van toegangspassen en het bevorderen van ‘schone bureaus’ (clean desk policy).

De RKC constateert dat deze maatregelen in 2016 zijn uitgevoerd.

Ook in de Nota privacy, informatiebeveiliging en informatiebeheer van november 2018 is in algemene termen aandacht voor bewustwording. Dit geldt ook voor de programmabegroting 2020. Dit is verder (nog) niet uitgewerkt in een concreet plan of communicatiecampagne.

Uit de interviews met de gemeente komt naar voren dat het bewustwordingsniveau in de organisatie nog laag lijkt. Vanaf eind 2019 is een aantal nieuwe acties ondernomen. Zo heeft de directie in maart 2020 een mail gestuurd naar alle interne medewerkers over de start van een nieuwe campagne voor het verhogen van het 'iBewustzijn’ via elektronische opleidingsmodules. Ook deze keer is het behalen van certificaten verplicht voor alle medewerkers. Ook zijn in het voorjaar van 2020 voorlichtingsbijeenkomsten gehouden om teams voor te lichten en bewuster te maken van informatieveiligheid. Verder heeft de gemeente een inloopspreekuur ingesteld waar medewerkers vragen kunnen stellen aan specialisten op het gebied van informatiebeveiliging. Tenslotte heeft de gemeente een interne website gemaakt met specifieke informatie over informatieveiligheid en privacy.

De RKC concludeert dat in 2016 voortvarend is begonnen en dat er eind 2019 opnieuw sprake is van een voortvarende aanpak om medewerkers bewuster te maken van risico’s op het gebied van informatiebeveiliging. In de tussenliggende periode kende de gemeente geen structurele aanpak om de bewustwording op een hoger niveau te krijgen.

2.2.4. Opvolging aanbeveling 3

Formulering
Investeer in de organisatie van informatiebeveiliging en zorg dat informatiebeveiliging een taak van de hele gemeentelijke organisatie wordt.

Beoordeling
Het college heeft deze aanbeveling deels opgevolgd.

Toelichting
De gemeente heeft in het Plan van Aanpak uit 2016 concrete maatregelen geformuleerd voor 2016 en 2017 om de organisatie van informatiebeveiliging te versterken, zoals:

- het inrichten van een stuurgroep informatiebeveiliging;
- het uitvoeren van risicoanalyses en
- het inrichten van een risicoregister.

Ook in de Nota privacy, informatiebeveiliging en informatiebeheer van november 2018 is aandacht voor het versterken van de organisatie, vooral om de aandacht en verantwoordelijkheid voor informatiebeveiliging breder te beleggen met een sleutelrol voor het lijnmanagement. Dit sluit aan bij onze aanbeveling uit 2016. De RKC ziet ook dat concrete punten uit de toelichting bij de aanbeveling uit 2016 nog niet zijn uitgevoerd. Er is geen formatieruimte voor de Chief Information Security Officer (CISO) functie in Haarlemmermeer. De gemeente is hier wel mee bezig. De functie wordt sinds februari 2019 door een interim-manager vervuld die de gemeente extern inhuurt en is nog ondergebracht bij het cluster INFO+. Het advies van de RKC was en is om deze rol als een strategische staffunctie te positioneren. Hierdoor krijgt de Security Officer een organisatiebreed mandaat. Informatiebeveiliging vraagt namelijk meer dan alleen een ICT-aanpak.

In juni 2019 zijn ambtelijk voorstellen aan de directie gedaan om de CISO als staffunctie te positioneren onder de gemeentesecretaris. Dit is tot op heden niet geëffectueerd.

De RKC constateert dat de maatregelen om de organisatie te versterken de afgelopen vier jaar deels zijn uitgevoerd. Zo is de gemeente in 2016 een stuurgroep gestart die de status en voortgang van de kwaliteit van de informatiebeveiliging met de afdelingen en het management van de organisatie bespreekt. Ook voert de gemeente van tijd tot tijd risicoanalyses uit en evalueert de gemeente zichzelf jaarlijks via de in VNG-verband afgesproken ENSIA-methodiek[4]. Binnen de gemeente is de (interim-)CISO het aanspreekpunt voor informatiebeveiliging. Hij heeft een deel van de verantwoordelijkheden belegd bij de afdelingshoofden zodat informatiebeveiliging integraal onderdeel uitmaakt van de verantwoordelijkheden van de lijnorganisatie.

Verder constateert de RKC dat het onderwerp informatiebeveiliging soms[5] op de agenda's staat van het college en de raad, vooral na concrete informatiebeveiligingsincidenten. Het college heeft aandacht en belangstelling voor informatieveiligheid, vooral voor het vergroten van de bewustwording onder medewerkers en het bestuur. De verantwoordelijk wethouder geeft aan dat raad en college zich bewuster zijn van het belang van een informatieveilige omgeving dan een aantal jaren geleden. Dit komt deels door het aantreden van de (interim-)CISO die zich intensief en persoonlijk inspant om het belang van informatieveiligheid op verschillende plekken in de organisatie onder de aandacht te brengen. Het college handelt vooral reactief.

De RKC beoordeelt de huidige bestuurlijke en ambtelijke organisatie nog als kwetsbaar, vooral door het ontbreken van heldere doelen, het ontbreken van een positie van CISO in de organisatiestructuur én het feit dat deze cruciale rol op interimbasis wordt vervuld.

2.2.5. Opvolging aanbeveling 4

Formulering
Voor regelmatig een integrale audit of pentesten uit op kwetsbaarheden.

Beoordeling
Het college heeft deze aanbeveling deels opgevolgd.

Toelichting
Op grond van de BIO zijn gemeenten verplicht hun verschillende informatiesystemen jaarlijks te controleren op de technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten[6].

---

[4] ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Zie https://www.ensia.nl/ voor meer informatie.

[5] Op de agenda van het college van B&W stonden in de periode 2016-2019: één plan van aanpak, één beleidsnota, drie ENSIA-besluiten en één nota naar aanleiding van het beveiligingsincident.

[6] Pentest is een afkorting van 'penetration testing'. Bij een pentest kruipen testers in de huid van een hacker. Ze proberen op allerlei manieren en met alle mogelijke middelen toegang te krijgen tot de geteste IT-omgeving. Op die manier leggen ze de zwakke plekken van een website, applicatie of zelfs gehele IT-infrastructuur bloot. Na afloop van een pentest kan een organisatie met gerichte maatregelen deze kwetsbaarheden zo goed mogelijk verhelpen.

De gemeente heeft in de periode tussen maart 2016 en maart 2020 twee keer een aanvullende pentest (beide in 2019) laten uitvoeren en geen integrale audits. Aanvullend wil zeggen: bovenop verplichte audits uit de BIO en testen in het kader van de jaarrekening (jaarlijks), DigiD (jaarlijks) en Suwinet (tweejaarlijks).

De gemeente implementeert ten tijde van dit onderzoek (april 2020) een systeem dat automatisch kwetsbaarheden monitort en detecteert. De gemeente kan op basis van deze risicoanalyses gericht pentesten gaan uitvoeren.

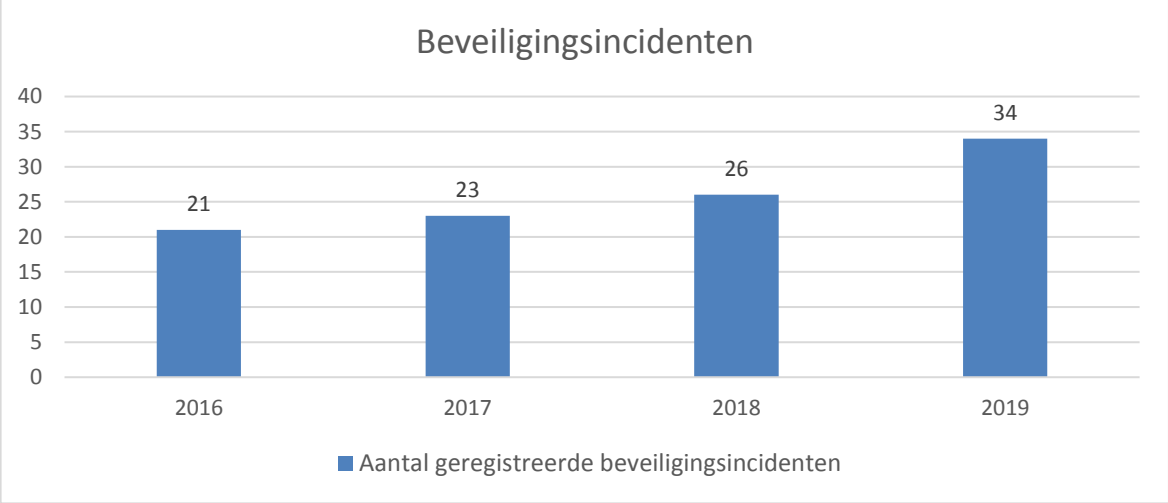
De RKC constateert op basis hiervan dat de gemeente de afgelopen vier jaar hoofdzakelijk op ad hoc basis een bescheiden aantal niet-integrale audits en pentesten heeft uitgevoerd in aanvulling op wat de gemeente verplicht is. Hiermee heeft de gemeente deels voldaan aan de aanbeveling. We adviseren om dit vaker te doen en meer integraal. Hierdoor komen mogelijke kwetsbaarheden *tussen* applicaties ook eerder aan het licht.

2.2.6. Opvolging aanbeveling 5

Formulering
Investeer in de ontwikkeling van monitoring en signalering, zodat ingegrepen kan worden bij aanvallen op de informatiebeveiliging.

Beoordeling
Het college heeft deze aanbeveling grotendeels opgevolgd.

Toelichting
In onderstaande grafiek staan de aantallen geregistreerde beveiligingsincidenten in de afgelopen jaren.



Grafiek 1 – Aantal geregistreerde beveiligingsincidenten in de periode 2016-2019

Bij 22 van de 70 geregistreerde incidenten in de periode 2016-2018 ging het om datalekken. Vanaf medio 2019 is er een specifiekere registratie van incidenten. Bij de incidenten in 2019 gaat het bijvoorbeeld om verlies of diefstal van apparatuur, incidenten met mailadressen, datalekken en een gemeentelijke hack.

De RKC constateert dat de gemeente de afgelopen vier jaar vooral reactief heeft geopereerd. Zodra de gemeente aanvallen constateert, probeert ze kwetsbaarheden zo snel en zo goed mogelijk te dichten. De praktijk in de afgelopen jaren was nog beperkt gericht op het signaleren en dichten van interne kwetsbaarheden *voordat* hackers toeslaan.

In een vertrouwelijke nota d.d. 29 oktober 2019 heeft het college de raad geïnformeerd over een aantal technische maatregelen die het college neemt om de continuïteit en veiligheid van de informatiebeveiliging voor de korte en langere termijn te borgen. Deze zouden bij het publiceren van dit vervolgonderzoek geïmplementeerd moeten zijn.

Eind 2019 heeft de gemeente besloten om het monitoren en signaleren van aanvallen op informatiesystemen uit te besteden aan KPN mede omdat de benodigde kennis hiervoor niet goed intern te organiseren is. Hierdoor zou de gemeente beter in staat moeten zijn om adequaat te reageren op aangetoonde kwetsbaarheden in de beveiliging. De implementatie hiervan is bijna afgerond, waarmee de aanbeveling grotendeels is opgevolgd.

2.3. Samenvatting van de bevindingen

Tabel 2 vat de uitkomsten van paragraaf 2 samen.

Tabel 2 – Opvolging aanbevelingen en beslispunt

	(Gewijzigde) formulering	Beoordeling RKC
Geamendeerd beslispunt	Het college van B&W opdracht te geven de aanbevelingen van de RKC te verwerken in een plan van aanpak met daarbij een gespecificeerde begroting, en deze ter besluitvorming aan de raad voor te leggen bij de behandeling van de Voorjaarsrapportage.	*Voldaan*
Aanbeveling 1	Vraag het College om het ambitieniveau voor informatiebeveiliging duidelijker uit te werken, en dit op te nemen in de planning en control cyclus.	*Deels voldaan*
Aanbeveling 2	De gemeente moet meer inzetten op het verhogen van bewustwording ten aanzien van informatiebeveiliging.	*Deels Voldaan*
Aanbeveling 3	Investeer in de organisatie van informatiebeveiliging en zorg dat informatiebeveiliging een taak van de hele gemeentelijke organisatie wordt.	*Deels voldaan*
Aanbeveling 4	Voer regelmatig een integrale audit of pentesten uit op kwetsbaarheden.	*Deels voldaan*
Aanbeveling 5	Investeer in de ontwikkeling van monitoring en signalering, zodat je kunt ingrijpen bij aanvallen van de informatiebeveiliging.	*Grotendeels voldaan*

3. Conclusies

Op basis van de bevindingen in dit vervolgonderzoek trekt de RKC de volgende conclusies.

Algemene conclusies

1. De gemeente heeft de aanbevelingen van de RKC uit 2016 deels, grotendeels of geheel opgevolgd.
2. De gemeente voldoet nog niet aan de basisverplichtingen die gelden voor gemeenten zoals nu verwoord in de Baseline Informatiebeveiliging Overheid (BIO). De gemeente geeft prioriteit aan risicosturing boven het nakomen van normen.
3. De gemeente heeft geen heldere bestuurlijke doelen voor het verbeteren van de informatiebeveiliging van de gemeente.

Conclusie over het aspect 'mens'

4. De gemeente zet instrumenten in om medewerkers bewuster te maken van het belang van informatiebeveiliging.
5. Het bewustzijn van beveiligingsrisico's lijkt laag onder medewerkers van de gemeente[7].

Conclusies over het aspect 'organisatie'

6. Informatiebeveiliging is in 2020 meer dan in 2016 een taak van de gehele gemeentelijke organisatie, maar deze gedeelde verantwoordelijkheid is (nog) niet voldoende verankerd.
7. De functie van Chief Information Security Officier (CISO) is nog niet formeel opgenomen in de organisatie van de gemeente en wordt sinds februari 2019 door een interim-manager vervuld.

Conclusies over het aspect 'techniek'

8. De gemeente investeert in monitoring en signalering om adequater te kunnen reageren op aangetoonde kwetsbaarheden in de informatiebeveiliging. Over het effect van deze maatregelen is nog niets bekend.

[7] We spreken over 'lijkt' omdat de RKC dit alleen baseert op de uitspraken in een interview en dit verder niet heeft onderzocht.

4. Aanbevelingen

Dit hoofdstuk bevat twee nieuwe aanbevelingen van de RKC voor de gemeenteraad (§ 4.1.), een slotbeschouwing (§ 4.2.) en enkele stellingen om een debat over dit vervolgonderzoek te voeden (§ 4.3.).

De gemeente heeft het merendeel van de aanbevelingen uit 2016 deels opgevolgd. We constateren dat de conclusies en aanbevelingen die de RKC toen deed nog steeds actueel zijn ondanks de inzet van de gemeente.

4.1. Aanbevelingen voor de Raad

De RKC doet op basis van de conclusies twee aanbevelingen aan de raad:

1. **Geef het college opdracht om te gaan voldoen aan alle verplichtingen van de Baseline Informatiebeveiliging Overheid (BIO), hiervoor een aanpak te maken met heldere streefdata en via de reguliere P&C-producten te rapporteren over de voortgang.**

   Los van het ambitieniveau (zie aanbeveling 2) is het noodzakelijk dat de gemeente snel gaat voldoen aan de verplichtingen op grond van de BIO. De gemeente kan dit combineren met een risicogestuurde werkwijze voor het beveiligen van informatie.

2. **Vraag het college om het ambitieniveau voor informatiebeveiliging voor de periode 2020-2023 concreet uit te werken via meetbare doelen en dit op te nemen in de planning- en controlcyclus.**

   Welke doelen stelt het college voor op het gebied van informatiebeveiliging? Welke subdoelen stelt het college voor de organisatie, de techniek en de mens? Is het voldoende te voldoen aan de wettelijke verplichtingen? Moet Haarlemmermeer de meest informatieveilige gemeente van Nederland worden? Of iets hier tussenin? En wat dan precies? En hoeveel mag dit kosten?

   Helderheid over de ambities geeft duidelijkheid aan de raad én de ambtelijke organisatie. Door deze doelen concreet en meetbaar te maken kan de gemeente ook meten of Haarlemmermeer op de goede weg is en zo nodig tussentijds bijsturen.

4.2. Slotbeschouwing

In dit vervolgonderzoek heeft de RKC onderzocht in hoeverre het college uitvoering heeft gegeven aan de opdracht van de raad en de aanbevelingen van de RKC. Hierop hebben de documentstudie en interviews zich gericht.

Tijdens dit onderzoek bekroop de RKC de vraag of de gemeente geheel zelfstandig de informatiebeveiliging op orde kan krijgen. We hebben dit in dit vervolgonderzoek niet expliciet onderzocht. Wel constateren we dat Haarlemmermeer sinds 2019 door VNG aanbestede diensten voor het monitoren en signaleren van aanvallen op informatiesystemen afneemt. We zien een aantal argumenten waarom het zelfstandig op orde krijgen van informatiebeveiliging voor Haarlemmermeer moeilijk kan zijn, zoals:

- De uitgangspositie van Haarlemmermeer (zoals beschreven in dit vervolgonderzoek).
- De schaarste aan beveiligingsexperts op de arbeidsmarkt: het is lastig om goede mensen aan te trekken en te behouden.
- De toenemende afhankelijkheid van informatie en informatiesystemen voor de kerntaken van de gemeente: de relatieve lat komt steeds hoger te liggen.
- De toename van de kwantiteit en kwaliteit van *hacks*: de 'tegenstanders' worden sterker.

De RKC vermoedt dat ook andere (grote) gemeenten voor vergelijkbare opgaven staan. Een belangrijke strategische keuze voor de gemeente Haarlemmermeer kan zijn of en zo ja in welke mate de gemeente in de toekomst wil samenwerken met andere gemeenten om de informatiebeveiliging (en wellicht de gehele informatievoorziening van de gemeente) op orde te krijgen.

4.3. Stellingen voor een debat

Hieronder staan stellingen die de raadsleden kunnen gebruiken om een politiek debat over deze notitie te voeden. Deze stellingen geven nadrukkelijk niet de mening weer van de RKC.

1. De gemeente Haarlemmermeer moet informatiebeveiliging zoveel mogelijk uitbesteden aan private partijen.
2. Informatiebeveiliging is geen thema voor de gemeenteraad van Haarlemmermeer.
3. De gemeente Haarlemmermeer moet de meest informatieveilige gemeente van Nederland worden.
4. De gemeente Haarlemmermeer moet meer samenwerken met andere gemeenten voor betere informatiebeveiliging.
5. De gemeenteraad heeft een voorbeeldfunctie op het gebied van informatiebeveiliging.

Bijlage 1: Documentatie over informatiebeveiliging sinds het verschijnen van het RKC-rapport in februari 2016

Mei 2016	Voorjaarsrapportage 2016	Is ter kennisname naar de raad gegaan
Juni 2016	B&W Nota Plan van aanpak Basis informatiebeveiliging op orde	Is ter informatie naar de raad gegaan
Dec 2018	B&W Nota privacy, informatiebeveiliging en informatiebeheer	Is ter informatie naar de raad gegaan
Juni 2019	Memo positionering CISO	Intern document van clustermanager aan directie
Okt 2019	GEHEIM B&W Nota Extra impuls voor informatiebeveiliging	Is ter informatie naar de raad gegaan
Dec 2019	Voorstel positionering Privacy en Security functies (CISO/ISO FG/PO)	Intern document van HRM voor directie