Gemeente Haarlem

Verantwoordelijkheid voor Veiligheid

Onderzoek naar Informatiebeveiliging

5 februari 2019

Rekenkamercommissie

Inhoudsopgave

Samenvatting & Aanbevelingen

De rekenkamercommissie (RKC) heeft onderzoek gedaan naar de informatiebeveiliging van de gemeente Haarlem. Een onderwerp dat steeds vaker in het nieuws is en ook bij de overheid steeds meer prioriteit krijgt. Onvoldoende beveiliging kan grote gevolgen hebben voor de werkprocessen van de gemeente en de gegevens van inwoners die de gemeente beheert.
Een groot deel van het onderzoek is in opdracht van de RKC uitgevoerd door Hoffmann Cybersecurity. Zij hebben het informatiebeveiligingsbeleid en een deel van de informatiesystemen van de gemeente onderzocht. Bij het informatiebeveiligingsbeleid is bekeken in hoeverre dit beleid goed is opgezet, of het is geïmplementeerd en of het wordt uitgevoerd. De conclusie ten aanzien van het beleid is, dat het onvoldoende is geïmplementeerd en dat de gemeente daardoor niet *'in control'* is. De informatiesystemen zijn getest met een aantal *penetratietesten*. Hieruit bleek dat er sprake was van meerdere (ernstige) kwetsbaarheden in de systemen. Deze informatie is direct met de gemeente gedeeld en de kwetsbaarheden zijn voor een deel al verholpen. Ten slotte is ook gekeken hoe de raad over de informatiebeveiliging is geïnformeerd. De RKC concludeert dat dit onvoldoende is.
In de bestuurlijke reactie op het onderzoek, de conclusies en de aanbevelingen geeft het college aan het geschetste beeld te onderkennen en uit inmiddels genomen acties maakt de RKC op dat het urgentiebesef is toegenomen. Ondanks de inmiddels getroffen maatregelen handhaaft de RKC haar aanbevelingen.

De aanbevelingen luiden als volgt:

1. Vóór eind 2019 daadkrachtige en volledige implementatie van het eigen informatiebeveiligingsbeleid te realiseren door onder meer:
   a. Een nieuwe gap-analyse uit te voeren om in beeld te krijgen welke, volgens relevante wet- en regelgeving en het eigen beleid voorgeschreven, maatregelen nog niet zijn geïmplementeerd. Hieruit wordt ook zichtbaar wat er sinds 2014 al is gerealiseerd.
   b. Het informatiebeveiligingsbeleid zo spoedig mogelijk, doch uiterlijk in het eerste kwartaal van 2019 opnieuw te laten vaststellen door het college.
   c. Naar aanleiding van bovenstaande punten op korte termijn het budget, de capaciteit en de benodigde competenties die beschikbaar zijn voor informatiebeveiliging te heroverwegen.
   d. Hiervoor een plan van aanpak met tijdpad en verantwoordelijken op te stellen en de voortgang van de implementatie te laten bewaken door de IT-auditor.
   e. Over de implementatie en uitvoering van het beleid dient structureel verantwoordingsinformatie te worden opgesteld en ook de aansturing van het beleid door directie en bestuur moet traceerbaar zijn.
2. De informatiesystemen weerbaarder te maken tegen cybercrime door:
   a. De resterende kwetsbaarheden uit de penetratietesten overeenkomstig de aanbevelingen van Hoffmann te verhelpen.
   b. Vóór de zomer van 2019 een hertest te laten uitvoeren op de gevonden kwetsbaarheden en de gemeenteraad hierover te informeren en deze periodiek en met verschillende invalshoeken te herhalen.
3. De raadsinformatie over informatiebeveiliging te verbeteren door naast de verplichte paragraaf en de ENSIA verklaring:
   a. De gemeenteraad middels een (zo nodig geheime) nota inhoudelijk te informeren over de mate van compliancy aan wet en regelgeving en het eigen beleid aan de hand van een jaarlijkse samenvatting met duiding van de scores op de ENSIA-zelfevaluatievragenlijst.
   b. Aan de hand van een objectieve maatstaf (bijvoorbeeld het volwassenheidsniveau) te rapporteren over de ontwikkeling van de verschillende onderdelen van de informatievoorziening , waaronder informatiebeveiliging.

1. Inleiding

Informatiebeveiliging is een actueel thema, dat steeds meer aandacht en investeringen van overheden vraagt. Tegenwoordig is het onderwerp vrijwel wekelijks in het nieuws.
Dat gaat ook de gemeente Haarlem aan. In de primaire processen en de bedrijfsvoering van gemeenten wordt namelijk steeds intensiever gebruik gemaakt van ICT en ook beheren gemeenten steeds meer gegevens van burgers. Het gebruik van ICT en het beheer van gegevens (in databanken) in combinatie met de decentralisering van overheidstaken van het rijk naar gemeenten en het werken in regie betekenen bovendien dat er steeds meer gegevens tussen verschillende organisaties en systemen worden uitgewisseld. Het beheer, gebruik en uitwisseling van gegevens gaat gepaard met risico's ten aanzien van de veiligheid van de informatie.
De waarborg van de veiligheid van persoonsgegevens van burgers is van groot publiek belang. Als persoonsgegevens in verkeerde handen komen, kunnen bijvoorbeeld vertrouwelijke gegevens openbaar worden of kan identiteitsfraude worden gepleegd. Dit heeft potentieel grote gevolgen voor de privacy van burgers en voor het imago van de overheid. Het kan ook leiden tot maatschappelijke onrust en het kan zelfs de fysieke veiligheid in gevaar brengen.

Informatiebeveiliging heeft tot doel te borgen dat de informatiehuishouding van de gemeente:
- betrouwbaar (de gegevens kloppen en zijn actueel);
- beschikbaar (op moment dat het nodig is);
- veilig (alleen toegankelijk voor geautoriseerden) is.

Vanwege de inherent vertrouwelijke aard van het onderwerp beveiliging is de voor de gemeenteraad beschikbare informatie hierover beperkt. En door het technische karakter zijn bovendien kennis over en inzicht in deze materie gering. Desondanks moet de gemeenteraad voor de uitoefening van zijn drie rollen goed geïnformeerd zijn over de stand van zaken en de risico's. De rekenkamercommissie wil de raad dit inzicht verschaffen.
Een tweede aanleiding voor het onderzoek is de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018.

Hoffmann Cybersecurity heeft in opdracht van de rekenkamercommissie onderzoek gedaan.
naar de veiligheid van persoonsgegevens en andere informatie bij de gemeente Haarlem.
Daarbij luidde de centrale vraag: *Is de informatiebeveiliging van de gemeente Haarlem op orde?*

Leeswijzer
In deze rapportage wordt allereerst de onderzoeksopzet (H2) gepresenteerd, vervolgens de hoofdlijnen van het beleid in Europa, Nederland en in Haarlem (H3). In de hoofdstukken daarna de bevindingen van het bureau (H4) en de conclusies (H5) en aanbevelingen (H6) van de rekenkamercommissie. Over de bevindingen van het bureau wordt uitsluitend op hoofdlijnen gerapporteerd. Het onderliggende rapport wordt niet openbaar gemaakt, omdat het delen van de specifieke kwetsbaarheden van de systemen de veiligheidsrisico's zou vergroten.

Het onderzoek is uitgevoerd in het voorjaar van 2018 en de resultaten zijn direct met de gemeente Haarlem gedeeld. Dit betekent dat bij publicatie van dit rapport de gemeente gelegenheid heeft gehad de meest dringende kwetsbaarheden te verhelpen. De rekenkamercommissie is de gemeente Haarlem zeer erkentelijk voor de medewerking aan het onderzoek.

2. Onderzoeksopzet

De rekenkamercommissie heeft het onderzoek laten uitvoeren door Hoffmann Cybersecurity met specialistische kennis. Hierbij zijn zowel het informatiebeveiligingsbeleid als de informatiesystemen onderzocht. Het is belangrijk te benadrukken dat de rekenkamercommissie geen integraal onderzoek heeft laten uitvoeren op alle systemen van de gemeente. Er is een keuze gemaakt om binnen het beschikbare budget een zo relevant mogelijk deel van de informatiebeveiliging te kunnen onderzoeken. De onderzoeksmethoden die hierbij zijn toegepast zijn documentenanalyse, gesprekken en penetratietesten.

In het onderzoek naar het informatiebeveiligingsbeleid is naar drie aspecten gekeken:
- ***Opzet***: zijn beleid, processen en procedures van informatiebeveiliging beschreven?
- B***estaan***: worden processen in de praktijk doorlopen?
- ***Werking***: werken de processen zoals bedoeld is?

Hiervoor zijn vele documenten (zie bronnenlijst) bestudeerd en naar aanleiding daarvan zijn vragen gesteld aan de gemeentelijke organisatie. In de opzet was ook een nader onderzoek van de zogenoemde kroonjuwelen opgenomen. Tijdens het onderzoek bleek dat de gemeente deze meest kritische applicaties niet had geïdentificeerd. Dat zijn de belangrijkste applicaties van de gemeente. Meestal zijn het applicaties gerelateerd aan de Basisregistratie Personen of aan het sociaal domein. Ook is nagegaan of de ENSIA (zie § 3.1.4) richtlijnen zijn toegepast.

In het onderzoek naar de informatiesystemen zijn penetratietesten uitgevoerd.

Box: penetratietesten

Een penetratietest is een toets van computersystemen op kwetsbaarheden in de beveiliging, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Het penetreren of *hacken* van systemen zonder toestemming van de eigenaar is niet rechtmatig. Om die reden is met de gemeentelijke organisatie een zogenoemde vrijwaringsovereenkomst getekend. Hierin is onder andere vastgelegd dat de gemeente Haarlem toestemming geeft voor de test, dat de uitvoerder van het onderzoek zorgvuldig met de persoonsgegevens omgaat, dat de resultaten van de *hack* worden gedeeld en dat beveiligingsincidenten direct zullen worden gemeld met een voorstel voor een oplossing. De gemeente was dus vooraf in kleine kring op de hoogte van de *hack*. Dit wordt ook wel een *ethical hack* genoemd.

Er wordt bij penetratietesten of pentesten onderscheid gemaakt tussen:
- Black box - d.w.z. zonder enige voorkennis over de informatiesystemen.
- Grey box - d.w.z. met beperkte voorkennis en toegang
- White box - d.w.z. met volledige voorkennis en toegang.

De penetratietest op de systemen wordt vaak uitgevoerd in combinatie met een fysieke penetratietest. Daaronder wordt verstaan het zonder toestemming binnendringen in de gebouwen van de gemeente. Ook hiervoor heeft de gemeente een vrijwaringsverklaring gegeven. In de combinatie wordt vervolgens getracht in het gebouw toegang tot het netwerk te krijgen.

Penetratietest Haarlem
De penetratietest is uitgevoerd in april en mei 2018 en bestond uit drie verschillende onderdelen:

1) Externe penetratietests vanaf een locatie buiten de gemeente
Een black box test vanaf het internet. Hierbij is bij alle vanaf het internet benaderbare systemen

getoetst of het mogelijk was binnen te dringen. De gemeente heeft hiervoor de IP-adressen verstrekt.

2) Interne penetratietests vanaf locaties binnen de gemeentegebouwen:
a) Blackbox – Met een meegebrachte laptop via een van de vele vrij toegankelijk netwerk-aansluitingen in de muur proberen toegang te krijgen tot het netwerk.
b) Greybox - 1) Vanaf een werkstation van de gemeente
2) Vanaf een werklocatie van de gemeente buiten de kantoren van de gemeente.
c) Het wifi-netwerk in de gemeentegebouwen

3) Fysieke penetratietests bij de drie grote kantoorgebouwen van de gemeente.

Bij onderdeel 1 en 2 is gebruik gemaakt verschillende soorten aanvalstechnieken en tools, die grotendeels standaard zijn en vrij beschikbaar op het internet. Voor onderdeel drie is een *mystery guest i*ngezet. Bij de externe penetratietest is vanwege de organisatorische impact niet de vaak succesvolle techniek van social engineering of spear phishing toegepast: de methodiek waarbij bijvoorbeeld door een mail met een geprepareerde bijlage of een usb-stick via medewerkers wordt getracht toegang te krijgen tot de systemen.

3. Informatiebeveiligingsbeleid

De kaders voor het informatiebeveiligingsbeleid bij gemeenten zijn vastgesteld op Europees, nationaal en gemeentelijk niveau. Daarnaast bestaan er niet verplichtende *good practices*, richtlijnen of convenanten. In dit hoofdstuk worden de hoofdlijnen kort weergegeven.

3.1 Informatiebeveiligingsbeleid in Nederland

3.1.1 Algemene Verordening Gegevensbescherming (AVG)

Sinds mei 2018 is de AVG volledig van kracht[1] en leidend voor het beheer en gebruik van persoonsgegevens. De AVG is een Europese verordening (dus met rechtstreekse werking in Nederland) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert. Volgens de Europese Commissie zijn persoonsgegevens “alle gegevens die betrekking hebben op een individu, ongeacht of het gaat om zijn privé-, beroeps- of openbare leven". Het kan gaan om een naam, een huisadres, een foto, een e-mailadres, bankgegevens, berichten op sociale netwerksites, medische informatie of het IP-adres van een computer. Voor dit onderzoek is in het bijzonder het principe van integriteit en vertrouwelijkheid van belang: de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
De AVG vervangt Wet bescherming persoonsgegeven (Wbp).
Ook de Meldplicht Datalekken is sinds 25 mei 2018 geregeld door de AVG. Organisaties moeten alle datalekken documenteren. In bepaalde situaties (met name bij het lekken van persoonsgegevens) moeten datalekken worden gemeld bij het Meldpunt Datalekken van de Autoriteit Persoonsgegevens en als er waarschijnlijk ongunstige gevolgen voor de betrokkene(n) zijn moeten ook zij worden geïnformeerd. Voorbeelden van datalekken zijn: persoonsgegevens bij het oud-papier of op afgedankte of verloren apparatuur, ongeautoriseerde toegang tot persoonsgegevens of een datalek bij een verwerker van door de organisatie verstrekte persoonsgegevens.

3.1.2 Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

De BIG is ontwikkeld in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Het is de opvolger van de Baseline Informatiehuishouding Gemeenten (2011), destijds ‘het normenkader voor informatiebeheer’. Dat was een product dat voortvloeide uit het Kennisprogramma Informatiehuishouding van de Rijksoverheid. Belangrijke pijlers van de BIG zijn risicomanagement, de Deming-circle (Plan-Do-Check-Act) en NEN-ISO-normen.

De BIG is bedoeld om:
- Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.
- Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van informatiebeveiliging te kunnen voldoen.
- De auditlast bij gemeenten te verminderen.
- Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

De integrale Baseline Informatiebeveiliging Nederlandse Gemeenten bestaat uit twee delen:
4. BIG – Strategische Baseline, die kan gezien worden als de ’kapstok’ waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente.
5. BIG – Tactische Baseline, die de normen en maatregelen ten behoeve van controle en risicomanagement beschrijft.

[1] De AVG is al sinds mei 2016 van kracht, met een transitieperiode tot 25 mei 2018.

Diverse incidenten[2] droegen bij aan het urgentiebesef over informatieveiligheid bij gemeenten. In 2013 werd de Informatiebeveiligingsdienst (IBD) opgericht en werd door een buitengewone Algemene Leden Vergadering van de VNG de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Met de resolutie werd de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) tot basisnorm bepaald.
Verder is in de resolutie opgenomen, dat informatieveiligheid in de collegeambities wordt opgenomen, onderdeel wordt van de portefeuille van een van de leden van het college, dat er een aparte paragraaf informatieveiligheid in het jaarverslag wordt gewijd en de lokale invulling transparant wordt gemaakt door gebruik te maken van waarstaatjegemeente.nl.

3.1.3 Informatiebeveiligingsdienst (IBD)

De informatiebeveiligingsdienst is een zogenoemd CERT/CSIRT, Computer Emergency Response Team of Cyber Security and Incident Response Team voor gemeenten. Een CERT/CSIRT is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te beperken en snel herstel van de dienstverlening te bevorderen. Naast reageren op incidenten richt een CERT zich ook op preventie en preparatie. Een andere belangrijke taak van de IBD is het beheren van de BIG. Voorts is de IBD voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).
De VNG is de opdrachtgever van de IBD, maar de IBD opereert onafhankelijk.

3.1.4 Eenduidige Normatiek Single Information Audit (ENSIA)

De Eenduidige Normatiek Single Information Audit (ENSIA) is een gezamenlijk initiatief van het Rijk en de VNG. ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG. De ENSIA volgt uit de al eerder genoemde resolutie uit 2013. Met een uniforme online vragenlijst en een verbinding tussen horizontale en verticale verantwoording moet ENSIA een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel creëren voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
In ENSIA is de verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) samengevoegd en gestroomlijnd.
Uitgangspunt is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan nationale partijen die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe van single information single audit toegepast; alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces.
Het is de bedoeling dat ENSIA aansluit aan op de gemeentelijke planning en control-cyclus. Zo krijgt het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan hier beter op sturen.

Hoe werkt ENSIA?
Gemeenten vullen de zelfevaluatievragenlijsten (circa 250 vragen) in op de zelfevaluatietool op ENSIA.nl. Iedere gemeente heeft een coördinator implementatie ENSIA om ENSIA goed te implementeren. Het college legt o.b.v. de zelfevaluatie een verklaring af die bestemd is voor de gemeenteraad over opzet en bestaan van. Op de collegeverklaring moet een *IT-audit* worden uitgevoerd waaruit een *assurance-rapport* volgt. De voorgeschreven specifieke aandachtsgebieden voor de IT-audit in 2017 zijn Digid en Suwinet.
Afgelopen jaar was het eerste jaar waarin deze werkwijze werd toegepast. Daardoor zijn processen in veel gemeenten waarschijnlijk nog niet helemaal gestroomlijnd.

[2] *DigiNotar-crisis en Lektober in 2011 Dorifel virus*

De collegeverklaring gaat uitdrukkelijk uitsluitend over *opzet* en *bestaan* en niet over de *werking* van de beheersmaatregelen.

3.1.5 Digitale Agenda 2020

De Digitale Agenda 2020 van de VNG ondersteunt gemeenten bij de steeds verdere digitalisering van de informatievoorziening. DA2020 is gericht op de uitvoering van beleid. Ondersteuning wordt geleverd in de vorm van verkenningen (bijv. kennissessies of factsheets), instrumenten (bijv. uniforme ICT-inkoopvoorwaarden en handreikingen) en producten (applicaties zoals Digitale overlijdensaangifte).
De Digitale Agenda 2020 wordt hier voor de volledigheid vermeld om dat het in P&C-documenten vaak in dezelfde paragraaf staat als informatiebeveiliging, maar het heeft hier geen betrekking op.

3.2 Informatiebeveiligingsbeleid in Haarlem

Deze paragraaf beschrijft de voor informatieveiligheid belangrijkste bestuurlijke documenten en mijlpalen van de gemeente Haarlem.

3.2.1 Informatiebeveiligingsbeleid 2014-2018

De kaderstellende nota Informatiebeveiligingsbeleid 2014-2018 is gebaseerd op BIG. Dat is overigens geen wettelijke verplichting. Wel heeft de algemene ledenvergadering van de VNG zich aan invoering van de BIG gecommitteerd.

De belangrijkste uitgangspunten bij het informatiebeveiligingsbeleid zijn:

- Het college van B&W is eindverantwoordelijk voor de informatiebeveiliging en stelt het informatiebeveiligingsbeleid vast.
- De directie stelt jaarlijks het informatiebeveiligingsplan vast op basis van een risicoanalyse.
- De Chief Information Security Officer (CISO) heeft een onafhankelijke rol en rapporteert rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken. De onderwerpen, die als risicovol worden gezien, moeten worden opgenomen in de auditplannen.
- De Information Security Officer (ISO) is geplaatst binnen de afdeling Informatievoorziening en is verantwoordelijk voor de tactische en operationele aspecten van de informatiebeveiliging. De positie van de CISO en de ISO binnen de organisatie zal de komende periode nader worden bepaald.
- Het lijnmanagement is verantwoordelijk voor de uitvoering van de informatiebeveiliging.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement.

De belangrijkste randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld, gebaseerd op een risicoanalyse.

De organisatie van het beleid

Er wordt in lijn met de BIG in het beleid onderscheid gemaakt tussen het strategisch niveau waarop de CISO opereert en het informatiebeveiligingsbeleid opstelt en het tactisch niveau waarop de ISO opereert en het informatiebeveiligingsplan opstelt. Namens de directie wordt de informatiebeveiliging aangestuurd door de Chief Information Officer (CIO).
Het beleid wordt elke vier jaar geactualiseerd en vastgesteld door het college.

3.2.2 Relevante nota's

Nota Informatievoorziening in samenhang (2014)
Om te komen tot kaderstelling en strategievorming wordt voorgesteld om, naast de in het IB 2014-2018 al benoemde functies van CIO, CISO en ISO, een Information Architect (IA) en een Chief Data Officer (CDO), een Coördinator Privacy Informatievoorziening en een Programmamanager Informatiehuis te benoemen en zonodig hiervoor extern te werven. Deze medewerkers vormen samen Team CIO die de CIO moeten ondersteunen. De CIO is de directeur die bedrijfsvoering in portefeuille heeft.
Team CIO bestaat sinds 2014 en vergadert maandelijks. Aan dit overleg nemen naast de CIO, CISO ook de CDO, de afdelingsmanager Informatievoorziening en de managers van afdelingen die veel met gegevens werken deel. Dit maandelijks overleg heeft een veel bredere insteek dan alleen informatiebeveiliging. Informatiebeveiliging is wel een vast agendapunt, maar uit de verslagen van het overleg is niet altijd op te maken of bespreking heeft plaatsgevonden.

Nota transparant en veilig (2015)
De nota beschrijft verdere stappen gericht op transparante en veilige informatievoorziening. Ten aanzien van informatieveiligheid wordt gesteld dat uitvoering van het eigen beleid en opvolging van de richtlijnen van de IBD flinke inspanningen vragen.
Tevens wordt geconstateerd dat Haarlem gemiddeld scoort vergeleken met andere gemeenten, maar dat het gehele speelveld onvoldoende presteert.
Voor het handhaven en verbeteren van de informatieveiligheid wordt structureel € 150.000,- gevraagd.

Nota privacy beleid (2016)
Ter voorbereiding op de inwerkingtreding van de AVG is het Privacybeleid geformuleerd en wordt € 85.000,- extra budget gevraagd voor het aanstellen van een privacyadviseur voor de voorbereiding op de AVG.

Nota Gegevensmanagement (2017)
Deze nota beschrijft het beleid om van gefragmenteerd gegevensmanagement tot een data-governance-structuur met centrale regie te komen die moet bijdragen aan een kwalitatief, transparant en toegankelijk gegevenslandschap. Gegevens worden als bedrijfsmiddel benoemd en in die zin gelijk gesteld aan personeel, organisatie en financiën. Mede om die reden is informatiebeveiliging van groot belang.

Informatienota Informatievoorziening en -veiligheid in de P&C-cyclus (2017)
Deze is opgesteld naar aanleiding van vragen van de Auditcommissie over de inbedding van informatiebeheer en - beveiliging in de P&C-cyclus. Deze werden gesteld mede naar aanleiding van bevindingen van de accountant. Het college geeft aan dat dit een ontwikkel- en leerproces is en dat het door de reorganisatie beperkte adaptatievermogen van de organisatie meerdere jaren in beslag zal nemen (t/m 2020). Ook heeft de verplichte invoering van ENSIA er volgens de gemeente voor gezorgd dat de capaciteit om aan de inbedding in de P&C-cyclus te werken beperkt was. De nota bevat nog geen concrete inzichten over wat de raad kan verwachten na inbedding in de P&C-cyclus.

3.2.3 ENSIA Haarlem

Over 2017 geeft het college van Haarlem met de ENSIA-verklaring aan dat opzet en bestaan van de beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet. Er zijn ook enkele belangrijke uitzonderingen, waarover de verklaring geen nadere informatie bevat. Deze verklaring is door de IT-auditor van de gemeente beoordeeld.
ENSIA was in 2017 in Haarlem nog niet ingebed in de P&C-cyclus. Voor 2018 is dit wel de bedoeling.

3.2.4 Overige aspecten

Ook uit andere beleidsdocumenten blijkt dat de eisen aan de gemeenten op het gebied van IT steeds hoger worden en meer aandacht van de gemeente vragen.

IT-auditor

Begin 2017 wordt extra formatie toegekend voor een IT-auditor, dit is een vereiste vanuit de BIG. De IT-auditor moet gaan bijdragen aan het professionaliseren van het verantwoordingsproces, het verbeteren van de risicobeheersing en zal de organisatie gaan toewerken naar het voldoen aan de BIG normen. De IT-auditor is in september 2017 aangesteld.
De IT-auditor is voorzitter van het Compliancy Overleg, dat er op is gericht te voldoen aan wet- en regelgeving en eigen beleid op het gebied van informatiebeveiliging van privacy. Aan dit overleg nemen naast de CIO, de CISO en de ISO ook de CDO, de FG, de privacy adviseur en diverse andere adviseurs op het gebied van gegevens en informatievoorziening deel. Door tweewekelijks overleg wordt door afstemming van activiteiten en het oppakken van dringende zaken getracht compliancy te bereiken. Er wordt geen verslag gemaakt.

Functionaris Gegevensbescherming (FG)

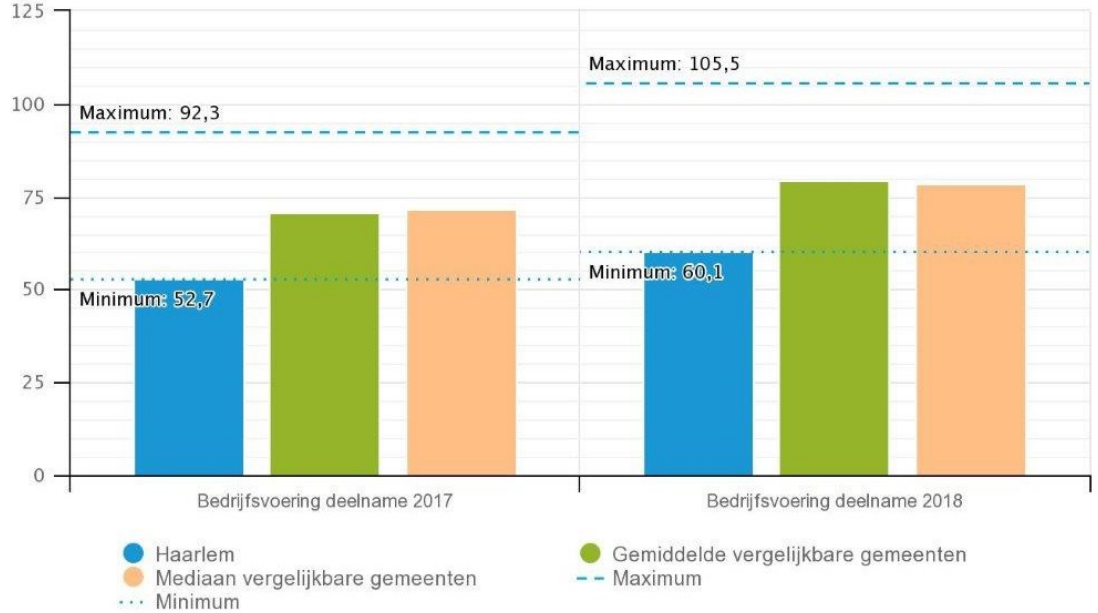
In maart 2018 is een FG aangesteld en is besloten voor 2018 aanvullend budget van € 150.000,- aan te vragen om te kunnen voldoen aan de AVG. Al eerder (maart 2017) was er door de raad € 85.000,- budget beschikbaar gesteld voor een privacyadviseur.

Financiën

Zoals hierboven geschetst, werd met diverse college- en raadsbesluiten de afgelopen jaren extra budget toegekend voor verschillende aspecten van IT. Na een inhaalslag op dit gebied vanaf 2010, was het beschikbare budget weer gedaald. Uit de nota Informatievoorziening transparant en veilig (2015) blijkt, dat het ICT-budget sinds 2012 lager is dan in andere 100.000+ gemeenten.

Uit de benchmark Vensters voor Bedrijfsvoering 2017 en 2018 blijkt dat Haarlem het laagste ICT-budget per inwoner heeft van de deelnemende 100.000+ gemeenten. Het bedrag van € 52,70 (in 2017) en € 60,10 (in 2018) per inwoner is aanzienlijk lager dan het gemiddelde van € 70,2 (in 2017) en €79,20 per inwoner (in 2018).

Grafiek ICT budget gemeente per inwoner



Bron: Vensters voor Bedrijfsvoering 2017 en 2018

3.2.5 Raadsinformatie over de status van informatiebeveiliging

Uit de P&C-cyclus

Het jaar 2014 is het eerste jaar dat het informatiebeveiligingbeleid van kracht is. In het jaarverslag staat daarover dat er belangrijke beleidsstappen zijn gezet voor de periode 2014-2018 en dat de organisatie is ingericht om dit beleid tot volwassenheid te brengen (o.a. Team CIO). Er zijn twee datalekken gemeld bij het College Bescherming Persoonsgegevens[3], er zijn beveiligingstests uitgevoerd en er was sprake van enkele beveiligingskwesties.

Het jaarverslag 2015 stelt dat de omslag is gemaakt van reactief naar proactief handelen en dat daardoor het aantal incidenten en de doorlooptijd van het uitvoeren van software updates sterk is afgenomen.

Het jaarverslag 2016 stelt dat op basis van een gap-analyse kan worden vastgesteld dat de informatiebeveiliging ten opzichte van 2014 sterk is verbeterd. Ook is er veel aandacht voor bewustwording bij medewerkers en is een securitypartner in gehuurd die gevraagd en ongevraagd advies geeft. Volgens het jaarverslag wordt Haarlem door VNG/KING als voorbeeld gemeente genoemd voor de ontwikkeling van de informatiebeveiliging.

Het jaarverslag 2017 stelt, dat er versneld is gewerkt aan het verbeteren van informatiebeveiliging zodat deze op het niveau van de BIG komt en blijft. Ook wordt gesteld dat bij alle wijzigingen het Informatiebeveiligingbeleid 2014-2018 van kracht is en dat dit tenminste elke vier jaar wordt vastgesteld door het college.

In de kadernota 2018 worden al nieuwe en extra inspanningen voor de digitale transformatie, waarvan cybersecurity een aspect is, aangekondigd. Er worden nog geen middelen aangevraagd.

Overig

De collegeverklaring is ter kennisname geagendeerd voor de commissie Bestuur van 31 mei 2018 en is verder niet besproken met of door de raad.

[3] *Tegenwoordig Autoriteit Persoonsgegevens*

4. Bevindingen onderzoek

Hoffmann Cybersecurity heeft het onderzoek conform de onderzoeksopzet uitgevoerd en heeft vele kwetsbaarheden geconstateerd. De rapportage daarover wordt niet openbaar gemaakt, omdat daarmee de specifieke kwetsbaarheden van de informatiebeveiliging van de gemeente Haarlem openbaar zouden worden.

Het bureau doet ook aanbevelingen om de kwetsbaarheden weg te nemen. Volgens de afspraken met de organisatie vooraf is het rapport wel met de gemeentelijke organisatie gedeeld. Inmiddels is een aantal aanbevelingen uit dat rapport al door de gemeente opgevolgd.
Tijdens het onderzoek is ook twee keer direct een aanbeveling aan de organisatie doorgegeven naar aanleiding van een bevinding met een kritiek hoog risico.

4.1 Bevindingen informatiebeveiligingsbeleid

Hoffmann is kritisch over de wijze waarop het Informatiebeveiligingsbeleid 2014-2018 wordt uitgevoerd. Het beleid van de gemeente is op zich van goede kwaliteit, maar wordt niet aantoonbaar uitgevoerd. De eigen uitgangspunten (zie § 3.2.1) worden niet nageleefd. Hieronder volgen de belangrijkste bevindingen:

- Risicoanalyses worden niet periodiek uitgevoerd en er wordt ook niet op basis van die analyse jaarlijks een informatiebeveiligingsplan door de directie vastgesteld. De wijze waarop de risicoanalyses zouden moeten worden uitgevoerd is ook van belang volgens het bureau.
- De werking van het uitgangspunt, dat het lijnmanagement verantwoordelijk is voor de informatiebeveiliging, is in de praktijk niet waar te nemen.
- Over de maatregelen die in het beleid worden genoemd is geen verantwoordingsinformatie beschikbaar.

In hoeverre vanuit de directie wordt gestuurd op resultaat is onduidelijk. Er vindt wel regelmatig overleg plaats, maar hierover wordt geen verslag gemaakt wegens capaciteitstekort. Deze punten tezamen betekenen dat de gemeente geen zicht heeft op de status van de uitvoering of de effectiviteit van het beleid.

Het bureau constateert tegelijkertijd dat er wel degelijk veel effectieve maatregelen zijn getroffen en dat er veel initiatieven worden genomen door medewerkers. Door het ontbreken van risicoanalyses is echter niet duidelijk of de juiste en voldoende maatregelen zijn getroffen. Het volwassenheidsniveau van de informatiebeveiliging van de gemeente Haarlem komt volgens de externe onderzoeker ruwweg uit op een niveau tussen 1 en 2 op de schaal van volwassenheid van 1 tot 5 (zie tabel op blz. 15)[4]. Op niveau 1 zijn beheersmaatregelen niet of gedeeltelijk gedefinieerd en/of worden op een inconsistente wijze uitgevoerd. Er is grote afhankelijkheid van individuen. Op niveau 2 worden de beheersmaatregelen consistent, gestructureerd, maar op informele wijze uitgevoerd. De BIG verlangt (impliciet) een niveau van 4 (meer dan gemiddeld). Op niveau 4 worden de beheersmaatregelen periodiek geëvalueerd en kwalitatief gecontroleerd.

[4] O.b.v. Volwassenheidsmodel Informatiebeveiliging Koninklijk Nederlandse Beroepsorganisatie Accountants (NBA), 2016. Dit model is op gericht organisaties te ondersteunen het verschil tussen het actuele en het gewenste volwassenheidsniveau te overbruggen.

Tabel indeling volwassenheidsniveaus

Score	Niveau	Omschrijving
1	Laag	Initieel
2	Beperkt	Herhaalbaar
3	Gemiddeld	Gedefinieerd
4	Meer dan gemiddeld	Beheerst en meetbaar
5	Hoog	Continu verbeteren

Bron: Handreiking Volwassenheidsmodel NBA

Ook ten aanzien van landelijke kaders zijn er tekortkomingen:

- Het beleid van de gemeente Haarlem is gebaseerd op de BIG. Door het niet uitvoeren van het eigen beleid, wordt ook de BIG niet nageleefd. De gemeente voldoet daardoor nog niet aan het merendeel van de normen uit de BIG. Zo is er bijvoorbeeld geen classificatie van zogenaamde kroonjuweel-applicaties gemaakt en bestaat daarover geen managementinformatie, waarmee de inzet gericht kan worden gestuurd. De uitzonderingen op de ENSIA-verklaring van het college ten aanzien van Digid en Suwinet hebben een (aanzienlijke) impact op de beveiligingsrisico's. De uitzonderingen betekenen, dat de gemeente Haarlem ook op dat vlak niet voldoet aan een aantal belangrijk normen.
- De AVG wordt op onderdelen overtreden. Zo wordt er bijvoorbeeld getest met niet-geanonimiseerde gegevens en zijn er geen (verifieerbare) afspraken met externe samenwerkingspartners over informatiebeveiliging.

4.2 Bevindingen beveiliging informatiesystemen

Zoals in de inleiding is aangekondigd, kunnen de specifieke bevindingen van dit onderzoek niet in een openbaar rapport worden gepubliceerd. In de onderstaande tabel daarom alleen de hoofdlijnen van de bevindingen van het bureau naar aanleiding van de penetratietests.

Tabel bevindingen

Bevindingen	Gevolgen
Bevindingen t.a.v. externe beveiliging: • Vanaf het internet is de gemeente goed beschermd • Niet alle websites zijn optimaal beschermd	• De gemeente loopt onnodig risico in geval van hacking of cyber attacks.
Bevindingen t.a.v. Interne beveiliging[5]: De beveiliging is niet op orde m.b.t.: • Netwerkauthenticatie en segmentatie • Wachtwoordbeleid en beheer • Beveiliging van werkstations • Beveiligingsupdates	• Ongeautoriseerden kunnen toegang krijgen tot persoonsgegevens en andere informatie van de gemeente. • De privacy van inwoners is niet goed gewaarborgd.
Bevindingen t.a.v. fysieke beveiliging: • Via de personeelsingangen is het eenvoudig ongeautoriseerd toegang te krijgen tot de gebouwen.	• Het netwerk is kwetsbaar voor ‘indringers’. • Diefstal van o.a. hardware is mogelijk.

[5] *Bij de te onderzoeken werklocatie buiten de hoofdgebouwen van de gemeente bleek al in een vroeg stadium dat er geen segmentering/filtering bestond tussen het netwerk en de locatie en dit dus benaderbaar was. De locatie is vervolgens verder niet onderzocht.*

4.3 Risicoclassificaties

In totaal formuleert Hoffmann 16 bevindingen. Bij elke bevinding wordt een inschatting van het risico gegeven (laag, gemiddeld, hoog) en de potentiele impact (wat zouden de gevolgen kunnen zijn als kwaadwillenden misbruik maken van de gevonden kwetsbaarheid). Het bureau constateert, dat met name de risico's van de kwetsbaarheden ten aanzien van de interne en fysieke beveiliging hoog zijn. Voor de externe informatieveiligheid zijn de risico's laag tot gemiddeld. Bij elke bevinding wordt ook een aanbeveling geformuleerd om de kwetsbaarheid te verhelpen.

4.4 Raadsinformatie

De gemeenteraad is zeer beperkt geïnformeerd over de status van de informatiebeveiliging van de gemeente Haarlem. De door de BIG voorgeschreven paragraaf in het jaarverslag over informatiebeveiliging is beknopt. Dat heeft vanzelfsprekend ook te maken met de zeer vertrouwelijke aard van het onderwerp, maar over de zorgen over bijvoorbeeld vertraging in de uitvoering en het capaciteitsgebrek die uit interne verslagen en de interviews wel naar voren komen, wordt niets gedeeld met de raad. De informatie die wel wordt gedeeld met de raad is overwegend geruststellend en betreft mededelingen over 'proactief handelen', 'voorbeeldgemeente' en 'het beleid blijft op niveau van de BIG'.

5. Conclusies & Aanbevelingen

5.1 Conclusies

Op basis van de bevindingen van Hoffmann en eigen onderzoek komt de rekenkamercommissie tot de volgende drie conclusies:

1. Het informatiebeveiligingbeleid is onvoldoende geïmplementeerd waardoor de gemeente niet *in control* is.

In ***opzet*** heeft de gemeente Haarlem sinds 2014 een volwaardig informatiebeveiligingsbeleid dat voldoet aan de BIG. Het is echter vooral een papieren beleid. Van het ***bestaan*** van het beleid in de praktijk is weinig sprake. Kernelementen van beleid als risicoanalyses, jaarplannen, verantwoordelijkheid bij lijnmanagement worden onvoldoende toegepast ondanks de jaren die al zijn verstreken sinds het vaststellen van het beleid. Een zelfde conclusie geldt voor de verantwoordingsstructuur van het beleid. Het management en bestuur (college en gemeenteraad) zijn er weinig inhoudelijk op aangehaakt. Voortgangsrapportages worden niet opgesteld en dus ook niet besproken.

Enige voorbeelden van de gevolgen:
- Zonder jaarlijkse risicoanalyse is het onduidelijk waar de belangrijkste risico's liggen en weet de organisatie niet of de capaciteit op de prioriteiten is ingezet.
- Zonder actueel jaarplan en voortgangsmonitoring door het management komen achterstanden niet aan het licht, kan niet geïnformeerd worden bijgestuurd en kunnen de eindverantwoordelijken niet goed worden geïnformeerd. Ook kan er geen verantwoording worden afgelegd.
- Zonder verslaglegging is het onduidelijk wie welke besluiten heeft genomen en welke werkafspraken zijn gemaakt
- Het werk is niet goed overdraagbaar bij uitval van sleutelfiguren.

Het ICT-budget per inwoner is het laagst van gemeenten met een vergelijkbare omvang, terwijl het actuele volwassenheidsniveau van de informatiebeveiliging lager is dan het gewenste niveau. Er lijkt onvoldoende urgentiebesef aanwezig te zijn. Volledige compliancy aan het eigen beleid en de BIG is niet een administratieve verplichting, maar een vereiste.
De toenemende urgentie blijkt ook uit de Kamerbrief 'Verhogen informatieveiligheid bij de overheid' van 16 oktober 2018 waarin de Baseline Informatiebeveiliging Overheid (BIO) wordt aangekondigd. Deze zal de BIG gaan vervangen en meer uniformiteit voor alle overheden moeten bewerkstelligen. Het kabinet overweegt de BIO-systematiek voor te schrijven door middel van een algemene maatregel van bestuur. Dat is minder vrijblijvend dan de VNG-resolutie waarop de BIG is gebaseerd.

2. De informatiesystemen kennen meerdere (ernstige) kwetsbaarheden

Uit de penetratietesten die Hoffmann Cybersecurity binnen de beperkte scope van het onderzoek heeft uitgevoerd, kwamen verschillende zwakke plekken in de informatiesystemen naar voren, waarvan enkele ernstig en tevens onbekend bij de organisatie waren. Deze onvoldoende ***werking*** van het beleid is (mede) het gevolg van het onvoldoende ***bestaan*** van het beleid. Met andere woorden: door het niet uitvoeren van het eigen beleid was er sprake van onbekende en grote risico's.
Uit met name de interne penetratietest bleken grote kwetsbaarheden. Dit is uiteraard ongewenst. De resultaten zijn direct met de organisatie gedeeld en een aantal kwetsbaarheden is inmiddels verholpen en verschillende andere worden binnenkort verholpen. Het is van groot belang op de

hoogte te zijn van de actuele kwetsbaarheden en dus de risico's van de informatiesystemen en deze middels risicomanagement te beheren.

3. De raad is onvoldoende geïnformeerd

De paragrafen in de jaarverslagen zijn heel algemeen en vereisen een goede lezer om alert te raken over de stand van zaken met betrekking tot de informatiebeveiliging. Zo moet proactief handelen vanzelfsprekend zijn. Ook lijkt het jaarverslag tegenstrijdigheden te bevatten over de mate van compliancy als er staat dat de beveiliging op het BIG-niveau is, maar tegelijkertijd ook nog op dat niveau moet komen. Gap-analyses zijn in 2014 en 2016 uitgevoerd, maar daarna niet meer. Verder moet het informatiebeveiligingsbeleid uit 2014 tenminste eens in de vier jaar worden vastgesteld, maar dit is in 2018 nog niet gebeurd.
De ter kennisname geagendeerde ENSIA-verklaring bevat geen informatie die de raad inhoudelijk op de hoogte brengt over de stand van zaken.

5.2 Aanbevelingen

Naar aanleiding van de conclusies formuleert de rekenkamercommissie de volgende drie aanbevelingen:

1. Vóór eind 2019 daadkrachtige en volledige implementatie van het eigen informatiebeveiligingsbeleid te realiseren door onder meer:
   a. Een nieuwe gap-analyse uit te voeren om in beeld te krijgen welke, volgens relevante wet- en regelgeving en het eigen beleid voorgeschreven, maatregelen nog niet zijn geïmplementeerd. Hieruit wordt ook zichtbaar wat er sinds 2014 al is gerealiseerd.
   b. Het informatiebeveiligingsbeleid zo spoedig mogelijk, doch uiterlijk in het eerste kwartaal van 2019 opnieuw te laten vaststellen door het college.
   c. Naar aanleiding van bovenstaande punten op korte termijn het budget, de capaciteit en de benodigde competenties die beschikbaar zijn voor informatiebeveiliging te heroverwegen.
   d. Hiervoor een plan van aanpak met tijdpad en verantwoordelijken op te stellen en de voortgang van de implementatie te laten bewaken door de IT-auditor.
   e. Over de implementatie en uitvoering van het beleid dient structureel verantwoordingsinformatie te worden opgesteld en ook de aansturing van het beleid door directie en bestuur moet traceerbaar zijn.

2. De informatiesystemen weerbaarder te maken tegen cybercrime door:
   a. De resterende kwetsbaarheden uit de penetratietesten overeenkomstig de aanbevelingen van Hoffmann te verhelpen.
   b. Vóór de zomer van 2019 een hertest te laten uitvoeren op de gevonden kwetsbaarheden en de gemeenteraad hierover te informeren en deze periodiek en met verschillende invalshoeken te herhalen.

3. De raadsinformatie over informatiebeveiliging te verbeteren door naast de verplichte paragraaf en de ENSIA verklaring:
   a. De gemeenteraad middels een (zo nodig geheime) nota inhoudelijk te informeren over de mate van compliancy aan wet en regelgeving en het eigen beleid aan de hand van een jaarlijkse samenvatting met duiding van de scores op de ENSIA-zelfevaluatievragenlijst.
   b. Aan de hand van een objectieve maatstaf (bijvoorbeeld het volwassenheidsniveau) te rapporteren over de ontwikkeling van de verschillende onderdelen van de informatievoorziening , waaronder informatiebeveiliging.

6. Bestuurlijke reactie

Gemeente Haarlem

Rekenkamercommissie
t.a.v. I. Mulders

Ons kenmerk CC/2019/13268
Datum 15 januari 2019
Afdeling Concerncontrol
Contact E. Hotting en M. van Geffen
Telefoon 023-5114312
E-mail mvangeffen@haarlem.nl

Onderwerp: Collegereactie rekenkamerrapport Informatiebeveiliging

Geachte Rekenkamercommissie,

Het college van Burgemeester en Wethouders heeft met belangstelling kennisgenomen van uw conceptrapport informatiebeveiliging en van het rapport dat Hoffmann Cybersecurity in opdracht van de rekenkamercommissie heeft opgesteld.

De Rekenkamer concludeert op basis van haar onderzoek dat gemeente Haarlem wat betreft informatiebeveiliging (nog) onvoldoende 'in-control' is. Dit beeld is herkenbaar voor het college en ook vergelijkbaar met andere gemeenten (recente Rekenkamer onderzoeken in Rotterdam, Dordrecht en Amersfoort). Informatiebeveiliging is met verdergaande digitalisering een beleidsveld dat de laatste jaren sterk in ontwikkeling en beweging is. Het belang van het onderwerp neemt toe en onze inwoners moeten erop kunnen blijven vertrouwen dat zijn of haar gegevens bij de gemeente Haarlem in veilige handen is. Deze snelle ontwikkelingen en groei van taken is gepaard gegaan met groeistuipen, waarbij er géén prioriteit is gegeven aan rapportage en verantwoording over informatiebeveiliging.

Het college vindt het een positieve ontwikkeling dat er door dit onderzoek aandacht op het onderwerp wordt gevestigd en wil naar de toekomst toe de informatievoorziening richting de Raad op een hoger niveau brengen. Intussen heeft de organisatie proactief een aantal verbeteringen al doorgevoerd. Zo is er o.a. vooruitlopend op het rekenkameronderzoek besloten om het huidige Informatiebeveiligingsbeleid te vervangen door een beleid gebaseerd op de nieuwe Baseline Informatiebeveiliging Overheid (BIO). Hiermee is de 'compliance based' aanpak gewijzigd in de door u geadviseerde 'risk-based' aanpak. De nadruk verschuift weer naar het proces van eigen risicoafwegingen in plaats van puur op basis van normen maatregelen treffen en zorgt er bovendien voor dat het bestuur goed 'in control' blijft.

Daarnaast hebben de pen-testen[1] (uitgevoerd door Hoffman Cybersecurity in opdracht van de Rekenkamer) de organisatie gewezen op een aantal bruikbare en waardevolle technische inzichten die het college meeneemt bij de verdere ontwikkeling van de informatiebeveiliging. De meest acute veiligheidsrisico's zijn reeds verholpen.

Het rapport van de rekenkamer zien wij als belangrijke input voor de jaarlijkse herijking van de prioriteiten. Op basis van de bevindingen en aanbevelingen van de rekenkamer gaan we de komende jaren een aantal maatregelen anders en sneller treffen.

Gelet op het voorgaande zijn wij erkentelijk voor uw werk. Uw opmerkingen, conclusies en aanbevelingen zullen (waar van toepassing) worden ingezet om te komen tot een verdere verbetering van de informatiebeveiliging van de gemeente. Op basis van de conclusies van beide rapporten trekt u drie hoofdconclusies en doet u drie aanbevelingen. Alvorens per aanbeveling in te gaan op hoe we hier mee omgaan wordt de historie en context toegelicht. Tenslotte wordt ingegaan op een aantal specifieke bevindingen.

Context

Informatiebeveiliging in de vorm zoals we het nu kennen heeft bij gemeenten een relatief korte historie. In minder dan vijf jaar is het uitgegroeid van een interne zorg die vooral binnen de afdeling ICT werd afgehandeld naar een onderwerp dat veel onderdelen van de organisatie raakt en waar veel energie in gestoken wordt. Deze snelle groei van taken zonder dat hier een wetswijziging aan ten grondslag ligt is ongewoon en gaat gepaard met groeistuipen. Niet alleen in Haarlem, dit geldt voor vrijwel alle gemeenten. Voor een goed begrip van de reactie van het college is het relevant om op een rij te zetten hoe deze korte historie van de informatiebeveiliging er uit ziet bij de gemeente Haarlem.

Medio 2014 is een begin gemaakt met de invoering van de Baseline Informatieveiligheid Gemeenten (BIG). In het collegebesluit van december 2014 waarmee het "Informatiebeveiligingsbeleid 2014 – 2018" (BBV 2014/467799) wordt vastgesteld staat o.a. "Volledige realisatie van het beoogd resultaat zal meerdere jaren in beslag nemen en ook daarna zal het op peil houden van de informatieveiligheid een doorlopende activiteit blijven." Voornemen was om de BIG in vijf jaar tijd in te voeren, dat is de periode van 2015 – 2019. Vijf jaar waarin de middelen van de P&C-cyclus worden ingezet om de vrijblijvendheid af te laten nemen in een tempo wat de organisatie aankan.

In jaren 2015 en 2016 is gestart met de implementatie. Er zijn teams gevormd en procedures opgesteld voor het omgaan met incidenten. Er is gewerkt aan het creëren van bewustzijn, eerst bij

[1] Bij een pentest kruipen pentesters in de huid van een hacker. Ze proberen op allerlei manieren en met alle mogelijke middelen toegang te krijgen tot de geteste IT-omgeving om zo kwetsbaarheden te ontdekken.

de afdeling ICT, daarna bij de rest van de organisatie met een groot aantal verplichte bewustzijnstrainingen en campagnes. Met de Informatiebeveiligingsdienst is een werkrelatie opgebouwd en volgens een drietal "speerpunten" zijn de grootste technische risico's aangepakt. Ook is een vaste adviespartner voor informatiebeveiliging gevonden en is informatiebeveiliging een vast onderdeel geworden in alle technische projecten.

De invoering van de Eenduidige Normatiek Single Information Audit (ENSIA) heeft in 2017 en 2018 echter de aandacht verlegd van de ingeslagen weg naar het uitvoeren van zaken die met de ENSIA gemoeid zijn, om daarmee o.a. te voorkomen dat de gemeente zou worden afgesloten van DigiD en / of Suwinet. ENSIA introduceerde ook een tweede, parallelle rapportagecyclus. De nadruk is komen te liggen op compliance in plaats van doelgerichte ingrepen op basis van risico-afwegingen. Naast ENSIA zijn er meer ontwikkelingen en externe factoren die maken dat het takenpakket rond informatiebeveiliging in hoog tempo in omvang toeneemt. Volgens de Informatiebeveiligingsdienst is de huidige groei uit te drukken als een verdubbeling per drie jaar.

Het onderzoek van de rekenkamercommissie komt op een moment dat de organisatie zelf ook concludeerde dat het beleid niet langer kan worden uitgevoerd zoals in 2014 was vastgesteld. Met bovenstaande context in het achterhoofd heeft het college uw aanbevelingen gelezen.

Reactie op de aanbevelingen

Op basis van de conclusies van beide rapporten doet u drie aanbevelingen. Graag geven wij hieronder per aanbeveling aan hoe we hier mee omgaan.

Aanbeveling 1 is om vóór eind 2019 daadkrachtige en volledige implementatie van het eigen informatiebeveiligingsbeleid te realiseren, uitgewerkt in sub-punten.

Het college is van mening dat het uitvoeren van het beleid zoals in 2014 vastgesteld niet langer mogelijk is gelet op de veranderde omstandigheden. In plaats daarvan kiest het college voor het vaststellen van een geheel vernieuwd beleid, waarbij de huidige Baseline Informatiebeveiliging Gemeenten (BIG) wordt vervangen door de geheel nieuwe Baseline Informatiebeveiliging Overheid (BIO). Deze nieuwe Baseline is onlangs beschikbaar gekomen en per 2020 verplicht voor alle overheidsorganisaties. Het nieuwe beleid met de nieuwe baseline verschuift de nadruk weer naar het proces van eigen risicoafwegingen en zorgt er bovendien voor dat het bestuur goed 'in control' blijft. Dit wordt o.a. gerealiseerd door de rapportagecyclus in te richten volgens ENSIA. Het beleid wordt daarmee weer uitvoerbaar voor de organisatie en stelt de organisatie in staat om te werken zoals gewenst, namelijk op basis van risicoanalyses.

Dit nieuwe beleid is inmiddels op 18 december 2018 vastgesteld, zie collegebesluit "Strategisch Informatiebeleid 2019-2023" (BBV nr. 2018/812821). Ook wordt de rol van CISO een volledige functie (van 0,2 fte naar 1,0 fte). De werving heeft inmiddels plaatsgevonden. Per 1 april 2019 start een fulltime functionaris als CISO met coördinatie op de uitvoering van het nieuwe beleid. De eerste taken zullen zijn gericht op het verbeteren van de aansluiting op de P&C cyclus en de aanhaking van het bestuur. Volgens het beleid zal ieder jaar een Informatiebeveiligingsplan worden opgesteld waarmee de uitvoering planbaar en volgbaar wordt. Eind 2017 is een functionaris aangesteld als IT auditor, deze ziet objectief toe op de uitvoering, voert audits uit en rapporteert (vanuit de ENSIA methodiek) zelfstandig aan het college. Met de vaststelling van de BIO zal bovendien de ENSIA grondig moeten wijzigen, dit is een taak voor VNG Realisatie, waarbij gemeente Haarlem een rol zal spelen als pilot-gemeente.

Aanbeveling 2 behelst het weerbaarder maken van de informatiesystemen tegen cybercrime door de bevindingen van Hoffmann te verhelpen, hierover een hertest te doen en (cyclisch) te rapporteren.

De meest urgente kwetsbaarheden uit de penetratietesten zijn gedurende het onderzoek van Hoffmann direct verholpen. De overige kwetsbaarheden, welke door de organisatie zijn vertaald in 28 problemen, zijn deels wel en deels nog niet verholpen. Het college maakt een risicoafweging t.a.v. het geheel aan gemeentelijke activiteiten en t.a.v. de te maken extra kosten/investeringen om, en op welke termijn, deze maatregelen te treffen. De stand van zaken is op moment van schrijven als volgt:

1) In totaal zijn inmiddels 12 van de 28 problemen geheel verholpen.
2) De implementatie van zeven problemen heeft een langere doorlooptijd, deze zijn gepland afgerond te zijn in het eerste kwartaal van 2019.
3) Vier van de aanbevelingen worden meegenomen in de momenteel onderhanden vervanging van de infrastructuur, waaronder de implementatie van het nieuwe rekencentrum (project ANY). De afronding hiervan is gefaseerd gepland in de tweede helft van 2019 en de eerste helft van 2020.
4) Voor vijf problemen vindt momenteel de analyse nog plaats, of wordt nog nagedacht over de oplossing. Hiervan is de oplossing nog niet gepland, dit wordt in de komende weken verwacht.

In kader van de vervanging van de gehele infrastructuur was reeds voorgenomen een test naar kwetsbaarheden te laten uitvoeren door onze vaste adviespartner op het gebied van Informatieveiligheid. Dit gebeurt voorafgaand aan de implementatie van het nieuwe rekencentrum nog op de huidige infrastructuur, om zoveel mogelijk problemen te kennen die in de nieuwe situatie moeten zijn opgelost. Om een betrouwbaar beeld te kunnen schetsen in voorbereiding op de implementatie, zal deze test een bredere scope en langere doorlooptijd hebben dan de onderzoeksopzet van Hoffman Security. Na de implementatie van de nieuwe infrastructuur in 2020 zal vervolgens nogmaals een vergelijkbare test worden uitgevoerd, maar dan op de nieuwe infrastructuur. Hiermee geven wij invulling aan de aanbevolen hertest.

Aanbeveling 3 betreft het verbeteren van de raadsinformatie over informatiebeveiliging en de volwassenheid van de informatievoorziening als geheel.

Het college herkent de noodzaak om de bestuurlijke informatie over informatiebeveiliging te verbeteren. Door beperkte capaciteit is er weinig aandacht uitgegaan richting rapportage en verantwoording. Het college kan zich vinden in de aanbeveling en zegt toe om de ENSIA-verklaring en inhoudelijk meer uitgebreide paragraaf conform het nieuwe Strategisch Informatiebeleid 2019-2023 op te nemen in de jaarstukken van Gemeente Haarlem. Daarnaast heeft de - in april 2019 startende - CISO als aandachtspunt meegekregen om de managementinformatievoorziening op een hoger niveau te brengen. Om objectief te meten hoe wij er voorstaan wat betreft de volwassenheid van de informatievoorziening zal de gemeente onder andere opnieuw mee gaan doen aan een jaarlijkse benchmark voor gemeenten (van M&I partners). Dit zodat we onze voortgang kunnen relateren aan die van andere 100.000+ gemeenten.

Specifieke bevindingen

Het college onderschrijft op hoofdlijnen de hoofdconclusies van de rekenkamer. Wel plaatst het college kanttekeningen bij een aantal bevindingen:

Kroonjuweel applicaties (paragraaf 4.1):
In de huidige situatie bestaat een gedeeltelijke uitwijkmogelijkheid voor het uitvoeren van processen. Daarbij is een afweging gemaakt op basis van de waarde van processen en applicaties versus de kosten voor het realiseren van uitwijkmogelijkheid. Dit betreft de belangrijkste applicaties en processen, onze kroonjuwelen. Deze zijn echter niet als zodanig benoemd.
De nieuwe situatie wordt momenteel voorbereid, daarbij gaan we uit van (vrijwel) volledige uitwijkmogelijkheid van alle applicaties en processen. Dit betreft het project waarin de gehele infrastructuur wordt vervangen. Dit is in lijn met de BIO, waarbij wordt gesteld dat alle processen belangrijk zijn. In de praktijk is het vaak ook meer efficiënt om zoveel mogelijk uniformiteit aan te brengen, en zo min mogelijk verschillende niveaus van veiligheid. Verscheidenheid in toe te passen maatregelen brengt hogere beheerslasten en kosten met zich mee. Alle veiligheid gaat dus naar een gemiddeld hoger standaardniveau, waarnaast nog een specifiek hoger beveiligingsniveau wordt onderkend voor een klein aantal zeer specifieke processen.

Informatiebeheer plannen (paragraaf 4.1)
In de jaren 2014, 2017 en 2018 zijn wel Informatiebeveiligingsplannen opgesteld op basis van de grootste risico's, welke alle jaren (ook in 2015 en 2016) hebben gediend als leidraad voor het operationeel uit te voeren werk. Terechte bevinding is dat deze niet, zoals het beleid voorschrijft, zijn vastgesteld door de directie. Op de integratie in de P&C cyclus valt ook het e.e.a. aan te merken, waardoor kan worden gesteld dat de gemeente op dit punt niet "in control" was. De plannen zijn echter wel opgesteld en gebruikt in de organisatie, wat ook merkbaar is in de tevens genoemde "vele effectieve maatregelen".

De AVG (paragraaf 4.1)
Het rekenkamerrapport stelt dat 'de AVG op onderdelen [wordt] overtreden. Zo wordt er bijvoorbeeld getest met niet-geanonimiseerde gegevens en zijn er geen (verifieerbare) afspraken met externe samenwerkingspartners over informatiebeveiliging'. Deze conclusie wordt gestaafd op basis van twee bevindingen van tekortkomingen: 1) Het ontbreken van aantoonbare afspraken over informatiebeveiliging met externe leveranciers, 2) het verstrekken van productiegegevens (niet alle testen vinden plaats met geanonimiseerde gegevens) ten behoeve van het testen van applicaties.

Met samenwerkingspartners (verbonden partijen) die persoonsgegevens ten behoeve van gemeente Haarlem (als verwerkingsverantwoordelijke) verwerken zijn - in overeenstemming met de AVG - verwerkingsovereenkomsten gesloten. Deze bevinding heeft enkel betrekking op aantoonbare afspraken met leveranciers. Op 3 april 2018 zijn de nieuwe algemene (en algemene IT) inkoopvoorwaarden door het college van B&W vastgesteld (BBV nr. 2018/141865), waar uitdrukkelijk aandacht uitgaat naar informatiebeveiliging. Deze inkoopvoorwaarden zijn op alle te sluiten overeenkomsten expliciet van toepassing met ingang van 5 april 2018. Daarnaast is de inkooporganisatie van de gemeente sterk in ontwikkeling. Er is een traject gaande om het contractbeheer beter op orde te brengen.

Voor wat betreft het werken met productiegegevens geeft het college opdracht te onderzoeken wat de mogelijkheden zijn om geautomatiseerd geanonimiseerde gegevens te gaan gebruiken in alle testomgevingen.

Bevindingen informatiesystemen (4.2)
In het overzicht wordt een bevinding t.a.v. externe beveiliging opgetekend: "Vanaf het internet is de gemeente goed beschermd". Dit was een speerpunt in de eerste jaren, in lijn met de dreigingsbeelden zoals verstrekt door het Nationaal Cyber Security Centrum (NCSC). Toch wordt als gevolg genoemd: "De gemeente loopt onnodig risico bij hacking of cyber attacks", op basis van de andere bevinding: "Niet alle websites zijn optimaal beveiligd". Wat het college betreft rechtvaardigt de bevinding het genoemde gevolg niet. Achterliggend gaat het hier om het niet op alle websites in gebruik zijn van de techniek HSTS. Het ontbreken daarvan levert geen noemenswaardig extra risico op. Zonder te willen beweren dat 100% veiligheid wordt gegarandeerd stelt het college zich op het standpunt dat het onderzoek geen aanleiding geeft om aan de externe veiligheid te twijfelen op basis van het ontbreken van HSTS.

Tot slot

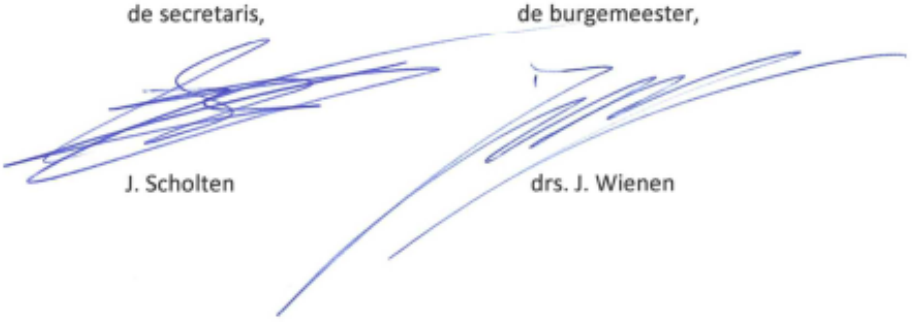
Het agenderen van dit onderwerp door de rekenkamercommissie heeft het college aanleiding gegeven om versneld een aantal ingrepen te doen, zoals het vaststellen van het nieuwe beleid op basis van de BIO. Haarlem is de eerste gemeente die deze stap zet. Het voor Haarlem opgestelde beleid wordt door de VNG als basis gebruikt voor een modelbeleid wat alle gemeenten kunnen gebruiken. Daarmee is uit het onderzoek van de rekenkamercommissie een verbetering

voortgekomen waar ook andere gemeenten mee vooruit kunnen. Alle overheden leren momenteel met vallen en opstaan veel over hoe correct met de vraagstukken van informatieveiligheid moet worden omgegaan. Samenwerking en voortdurende aandacht vanuit het bestuur zijn daarbij van groot belang. Het college dankt de rekenkamercommissie voor de bijdrage hieraan.

Hoogachtend,

Het college van burgemeester en wethouders,

de secretaris, de burgemeester,



J. Scholten drs. J. Wienen

7. Nawoord

De RKC is verheugd na ontvangst van de bestuurlijke reactie het onderzoek naar de informatiebeveiliging van de gemeente Haarlem te kunnen afronden en de resultaten aan de raad te kunnen presenteren[6]. De RKC maakt uit de bestuurlijke reactie op dat het urgentiebesef ten aanzien van goede informatiebeveiliging flink is toegenomen. Het college herkent het beeld dat de RKC over de informatiebeveiliging schetst en gaat in zijn reactie in op de context, de aanbevelingen en een aantal specifieke bevindingen.
In afwijking van de Werkwijze RKC werd door het college dit keer in de bestuurlijke reactie op verschillende onderdelen aanvullende nieuwe inhoudelijke informatie gepresenteerd, waarvan het onderzoeksteam niet eerder op de hoogte was gesteld. De aanvullende informatie is bezien en vormt voor het bureau Hoffmann Cybersecurity en in navolging daarvan de RKC geen aanleiding om de bevindingen, conclusies en de aanbevelingen te wijzigen.

De bestuurlijke reactie en de nieuwe informatie zetten de RKC wél aan tot het benadrukken van het beoogd resultaat van de drie aanbevelingen.

1. Het beoogde doel van de eerste aanbeveling , opvolging te geven aan het eigen beleid door het planmatig daadwerkelijk volledig te implementeren, blijft even urgent. Het beleid dat in december 2018 door het college is vastgesteld (de facto opvolging van aanbeveling 1b) betekent niet dat de overige onderdelen van aanbeveling 1 vervallen. Of met het nieuwe beleid en de uitbreiding van de formatie voor de CISO de capaciteit en het budget voldoende zijn om actuele en toekomstige uitdagingen het hoofd te bieden, moet blijken uit de gapanalyse. Informatiebeveiliging vraagt vanwege de snelle ontwikkelingen en de grote risico's om flexibiliteit in de inzet. Niet de reeds aanwezige, maar de benodigde capaciteit zou richtinggevend moeten zijn.
2. Ook de tweede aanbeveling, om de aangetroffen kwetsbaarheden te verhelpen en dit aan te tonen door middel van een penetratietest, blijft van kracht. Om de implementatie van de nieuwe infrastructuur niet onnodig te belasten, zouden alleen de kwetsbaarheden die niet zijn gerelateerd aan de vervanging van de infrastructuur voor de zomer van 2019 moeten worden onderworpen aan een hertest. Het college kan hiermee aan de raad laten zien dat de getroffen kwetsbaarheden voldoende aandacht hebben gekregen en dat de door de gemeente beheerde gegevens geen onnodig risico meer lopen.
3. De derde aanbeveling is gericht op verbeterde raadsinformatie en de RKC is blij met de toezegging van het college om die te verbeteren. De toezegging gaat echter voorbij aan het aspect van de nadere duiding van de ENSIA-scores. Ook dat onderdeel van de aanbeveling, gericht op meer transparantie naar en inzicht voor de raad, vraagt om opvolging. De M&I-benchmark van gemeentelijke ICT-gegevens waaraan de gemeente Haarlem weer gaat deelnemen betreft een zelfevaluatie. Deze benchmark kwalificeert daardoor niet als de aanbevolen objectieve maatstaf voor de volwassenheid van de informatiebeveiliging.

Hoewel informatiebeveiliging tot de bedrijfsvoering van de gemeente wordt gerekend en daarmee een collegebevoegdheid is, wil de RKC tot slot opmerken dat het grote publieke belang ervan voor de raad voldoende aanleiding is om de vinger hierbij stevig aan de pols te houden.

[6] In dit onderzoek zijn zowel de termijn voor ambtelijke wederhoor als de termijn voor de bestuurlijke wederhoor op verzoek van de gemeente verlengd en als gevolg daarvan wordt dit urgente rapport veel later dan gepland gepubliceerd. Het onderzoek zelf is uitgevoerd in de periode april en mei 2018.

Bronnenlijst

Haarlem
Afwijkingen ENSIA 2017 mbt Suwinet (2018)
Assurance rapport 2017 Collegeverklaring ENSIA 2017 (2018)
Bijlage B Informatievoorziening binnen de P&C-cyclus (IT-auditor) (Positioneringsdocument B) (2017)
Collegebesluit aanstellen IT-auditor (2017)
Collegebesluit aanstellen functionaris gegevensbescherming en voorbereiding op de Algemene Verordening Gegevensbescherming (2018)
Collegeverklaring ENSIA 2017 (2018)
ENSIA 2017 rapportage Digid (2018)
Informatiebeveiligingsbeleid 2014-2018 (2014)
Informatienota Informatievoorziening en - veiligheid in de P&C-cyclus (2017)
Kadernota 2018
Nota gegevensmanagement (2017)
Nota Informatievoorziening Transparant en Veilig (2015)
Nota Informatievoorziening in samenhang (2014)
Nota Privacybeleid Haarlem (2017)
Notitie aanstelling FG (2018)
Positioneringsdocument A (2017)
Programmabegroting gemeente Haarlem 2018-20122
Raadsbesluit Nota Privacybeleid Haarlem (2017)
Raadsinformatieformulier over aanstellen IT-auditor (2017)
Raadsstuk Nota Informatievoorziening Transparant en Veilig (2015)
Verslagen Team CIO

Overig
Cybersecuritybeeld Nederland, NCSC (2015)
Handleiding AVG, Autoriteit Persoonsgegevens (2018)
Handreiking bij Volwassenheidsmodel Informatiebeveiliging, NBA, 2016
ICT Benchmark Gemeenten 2016, Haarlem, M&I Partners, 2016
Informatievoorziening Nederlandse Gemeenten (2015)
In onveilige handen, Rekenkamer Rotterdam (2017)
Kamerbrief Verhogen informatieveiligheid bij de overheid, 16 oktober 2018
Nederlandse Cyber Security Agenda
Nederlandse digitaliseringsstrategie, Ministerie BKZ
Resolutie Informatieveiligheid (2013)
Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten (2016)
Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (2016)
VNG Ledenbrief informatieveiligheid en privacy (2017)
VNG Ledenbrief nieuw verantwoordingsproces en informatieveiligheid (2017)
VNG Stand van zaken Informatieveiligheid gemeenten (2017)

Websites
Autoriteitpersoonsgegevens.nl
Ensia.nl
Digitaleoverheid.nl
Informatiebeveiligingsdienst.nl
Venstersvoorbedrijfsvoering.nl
Vngrealisatie.nl
Waarstaatjegemeente.nl

Dit is een uitgave van de Rekenkamercommissie,
5 februari 2019

Postbus 511
2003 PB Haarlem
Tel. 14 023

haarlem.nl