Gemeente Haarlem

# Raadsinformatiebrief

| | | | |
|---|---|---|---|
| **Onderwerp** | Informatiebeveiliging en Gegevensbescherming – aanvullende informatie | | |
| Nummer | 2019/241916 | Datum college | 26 maart 2019 |
| Portefeuillehouder | Botter, J. | | |
| Programma/beleidsveld | Bestuur | | |
| Afdeling | Concerncontrol | | |
| Auteur | E. Hotting | | |
| Telefoon | 023 – 511 5061 | | |
| E-mail | ehotting@haarlem.nl | | |
| Actueel behandelvoorstel | Behoort bij onderwerp RKC Rapport Verantwoordelijkheid voor Veiligheid - Onderzoek naar Informatiebeveiliging in de raadsvergadering dd 28 maart 2019 | | |
| Bijlagen | Overzicht ontplooide activiteiten 2014 - 2018 | | |

In deze brief informeert het college u nader over een aantal onderwerpen die in de commissie Bestuur op 14 maart ter sprake zijn gekomen tijdens de behandeling van het rapport "Verantwoordelijkheid voor Veiligheid" van de Rekenkamercommissie en het nieuwe Informatiebeveiligingsbeleid. Ook wordt ingegaan op een aantal vragen die naar aanleiding van deze behandeling zijn gesteld.

Achtereenvolgens komen aan de orde:

A. Stand van zaken aanbevelingen RKC
B. Testen met niet-geanonimiseerde persoonsgegevens
C. Capaciteitsplanning en drie lijnen van defensie
D. Veiligheid van het systeem waarmee de vergaderingen worden geregistreerd
E. Overzicht van activiteiten vanaf 2014 tot nu
F. Aankondiging nog te behandelen onderwerpen

## A. Stand van zaken aanbevelingen RKC

In het rapport van de Rekenkamercommissie worden aanbevelingen gedaan. Hieronder wordt uiteengezet hoe deze aanbevelingen worden uitgevoerd en wat de stand van zaken is.

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.*

      Dit zal voor eind 2019 worden uitgevoerd. Meer concrete informatie volgt in het toegezegde Plan van Aanpak (zie punt 1 d).

   b) *Het informatiebeveiligingsbeleid zo spoedig mogelijk, doch uiterlijk in het eerste kwartaal van 2019 opnieuw te laten vaststellen door het college.*

      Het nieuwe Informatiebeveiligingsbeleid 2019 – 2023 is vastgesteld door het college op 18 december 2018. Daarmee is uitvoering gegeven aan deze aanbeveling.

   c) *Naar aanleiding van bovenstaande punten op korte termijn het budget, de capaciteit en de benodigde competenties die beschikbaar zijn voor informatiebeveiliging te heroverwegen.*

      Toegezegd is om dit nog voor de Kadernota zo goed als mogelijk in beeld te brengen. Hier wordt momenteel aan gewerkt. Dit punt wordt hieronder verder uitgewerkt bij de toelichting op het model met drie lijnen van defensie.

   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.*

      Dit Plan van Aanpak zal worden opgesteld in de komende maanden. Hierin wordt vastgelegd hoe en wanneer de nog niet uitgevoerde aanbevelingen van de RKC worden opgevolgd; op welke wijze halfjaarlijks (de implementatie van) het informatiebeveiligingsbeleid wordt geëvalueerd, hoe de raad hierover wordt geïnformeerd en op welke wijze vorm en inhoud wordt gegeven aan een risicoregister.

   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.*

Het nieuwe Informatiebeveiligingsbeleid (punt 1 b) bevat op dit punt belangrijke verbeteringen waardoor de organisatie ervan overtuigd is dit ook te kunnen uitvoeren. Om deze reden is de functie van CISO uitgebreid van 0,2 fte naar 1,0 fte. Deze nieuwe functionaris begint per 1 april 2019. De taken en het mandaat worden hieronder beschreven bij de toelichting over het 3LoD model.

2) De informatiesystemen weerbaarder te maken tegen cybercrime door:

   a) *De resterende kwetsbaarheden uit de penetratietesten overeenkomstig de aanbevelingen van Hoffmann te verhelpen.*

      Op het moment van schrijven zijn 21 van de 28 geïdentificeerde problemen opgelost. Van de resterende problemen worden drie punten opgelost met de oplevering van project Any, een grote vervanging van de infrastructuur. Dit versnellen zou onevenredig hoge kosten met zich meebrengen. De overige punten worden in de komende weken (dus nog voor de zomer) opgelost, waarna een hertest plaatsvindt (zie hieronder 2b). Voor één punt is vooralsnog geen goede oplossing gevonden die op korte termijn kan worden doorgevoerd. Dit wordt hieronder bij B toegelicht wanneer het gaat over het gebruik van persoonsgegevens in de testomgeving.

   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.*

      De eerste hertest door een externe partij start op 9 april. Daarin wordt achtereenvolgens onderzocht of de organisatie alle aanbevelingen van Hoffmann correct heeft geïnterpreteerd, of de juiste oplossing is gevonden en of deze correct is uitgevoerd. Wanneer na deze hertest nog punten open blijken te staan zal een nieuwe hertest worden uitgevoerd net zolang tot alle punten zijn verholpen. Naar verwachting slaagt dit voor de zomer, met uitzondering van de punten die worden verholpen in het grote traject voor vervanging van de infrastructuur en het testen met echte persoonsgegevens.

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.*

      Dit kan met ingang van de rapportage over het jaar 2019 worden uitgevoerd. Over het jaar 2019 zal de organisatie de ENSIA-rapportage dubbel uitvoeren, met een rapportage ten

opzichte van de BIG en een rapportage ten opzichte van de BIO. Dit is vooralsnog de wens vanuit de toezichthouders als gevolg van het overgangsjaar – mogelijk verandert dit nog.

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.*

Dit wordt meegenomen in het bij punt 1 d genoemde Plan van Aanpak.

**B. Testen met niet-geanonimiseerde persoonsgegevens**

In het rapport van de Rekenkamercommissie wordt opgemerkt dat de Algemene Verordening Gegevensbescherming (AVG) wordt overtreden omdat wordt getest met niet-geanonimiseerde persoonsgegevens. Het blijkt dat we niet anders kunnen dan testen met werkelijke persoonsgegevens. Dat is in een brief lastig uiteen te zetten en te visualiseren. Wel kan dit goed toegelicht worden met een korte presentatie over hoe het gegevensmanagement van de overheid in elkaar steekt en hoe dit doorwerkt naar het testen van ketens. Kort samengevat komt het erop neer dat methoden die worden aanbevolen om correct te testen niet kunnen worden toegepast op oude systemen doordat cruciale keten- en regressietesten dan niet langer werken, en dat vervanging van deze software financieel niet kan worden gedragen door een enkele gemeente.

Uit navraag bij een aantal andere gemeenten blijkt dat dit probleem bij iedereen speelt; niemand heeft op dit moment al een adequate oplossing gevonden voor dit knelpunt.

Naar onze opvatting is de enige reële mogelijkheid tot oplossen van dit probleem om samen met alle gemeenten en andere overheden een alternatieve manier van omgaan met gegevens te ontwikkelen. Hieraan wordt gewerkt vanuit het programma Samen Organiseren van de VNG. Ook dit kan worden toegelicht in een presentatie.

Een presentatie waarbij de aard van het probleem en de oplossingsrichting wordt toegelicht kan worden georganiseerd in de commissie Bestuur. Het college hoort graag van u of u hier behoefte aan heeft.

Het radicaal stoppen met het testen van wijzigingen in de software is geen reële optie. Iedere wijziging moet worden getest, door dit te doen worden regelmatig fouten in de uitvoering van processen voorkomen. Bij elke wijziging van een proces, groot (bijv. een nieuwe wet) of klein (bijv. het wijzigen van een rekenregel) moet het gehele proces grondig worden getest om fouten met vervelende gevolgen voor inwoners te voorkomen. Ook dit is overigens deel van de eisen die volgen uit het Informatiebeveiligingsbeleid.

Wat ons dus rest is het mitigeren van het risico bij het testen met persoonsgegevens. In de testomgeving staan dezelfde persoonsgegevens als in de productieomgeving, wellicht minder actueel en minder in aantal. Het aantal mensen dat toegang heeft tot een testomgeving is over het algemeen

kleiner, namelijk de functioneel beheerders en een paar medewerkers die testen. Dit zijn altijd mensen die ook al geautoriseerd zijn voor de productieomgeving en die dus feitelijk precies diezelfde gegevens al kunnen zien. Het levert per saldo geen grote vergroting van risico's op. Ook komt de informatie hiermee niet onder ogen van medewerkers die deze niet mogen inzien.

### C. Capaciteitsplanning en drie lijnen van defensie

Bij het onderwerp informatieveiligheid worden verantwoordelijkheden bekeken door de bril van de drie lijnen van defensie (3LoD).

Het model is als volgt:

- De 1e lijn bestaat uit de lijnmanagers in het primaire proces. Deze lijn is primair verantwoordelijk voor een goede interne beheersing. Daarbij wordt gebruikgemaakt van adviezen en methoden welke ontwikkeld worden in de tweede lijn.
- De 2e lijn bestaat uit specialisten die methoden ontwikkelen en de 1e lijn adviseren en ondersteunen.
- De 3e lijn voorziet de bestuurders van de organisatie over aanvullende zekerheid en objectieve informatie over het functioneren van de 1e en 2e lijn.

Er is inmiddels enige bekendheid in Haarlem met het van het 3LoD -model bij het beoordelen van de processen die van invloed zijn op het financiële beeld van getrouwheid en rechtmatigheid. Dit model geeft handvatten om te beoordelen waar in de interne beheersing risico's met een financieel effect worden ondervangen.

Op dezelfde wijze kan bij het toepassen van de drie lijnen van defensie bij informatieveiligheid handvatten aangereikt worden waar in de interne beheersing risico's met een informatieveiligheid effect ondervangen worden.

Ook is het de bedoeling dat de bevindingen die uit interen en externe audits m.b.t. informatieveiligheid in de leercyclus wordt opgenomen. Een proces van continu verbeteren aan de hand van bevindingen.

Er is in Haarlem al langere tijd ervaring opgedaan bij het inrichten van deze leercyclus voor financiële processen. Het inrichten van de 3 lijnen van defensie voor informatieveiligheid en het inrichten van de daarop betrokken leercyclus is van recente datum en daar is tijd van inregelen voor noodzakelijk. Ervaring op doen en weer bijstellen op een technisch georiënteerd vakgebied, vraagt aanpassingstijd van de organisatie, in cadans met de landelijke ontwikkelingen op dit terrein.

Zolang 1e lijn niet optimaal functioneert is zal 2e lijn (in dit deel van de bedrijfsvoering met name Security Officers en Privacy Officers) overvraagd worden. Zolang 1e en 2e lijn het werk niet in voldoende mate aankunnen heeft 3e lijn het relatief druk en zal deze omissies rapporteren.

In dit geheel zijn de volgende rollen en mandaten van specifiek belang:

- De IT-auditor vormt de 3e lijn voor de Informatiebeveiliging. Dit bestaat uit het objectief rapporteren over de stand van zaken en het doen van aanbevelingen voor verbetering. Voor elk onderzoek is een opdracht nodig. Tot nu toe behelst dit opdrachten welke verplicht zijn in het kader van ENSIA. Daarnaast adviseert de IT-auditor de organisatie over het correct uitvoeren van de aanbevelingen.
- De Functionaris Gegevensbescherming (FG) is een wettelijk verplichte functie vanuit de Algemene Verordening Gegevensbescherming (AVG). Deze functionaris houdt toezicht op het naleven van wet- en regelgeving rondom de bescherming van persoonsgegevens en heeft daarnaast een adviserende rol. In Haarlem voert de FG taken uit binnen de 3e lijn (toezichthoudend) en 2e lijn (adviserend). Wanneer een hogere volwassenheid wordt bereikt kan de FG zich beperken tot activiteiten in de 3e lijn. De FG rapporteert onafhankelijk.
- De Chief Information Security Officer (CISO) regelt op strategisch niveau dat de organisatie bezig is met continue verbeteren op het gebied van Informatiebeveiliging. Dit behelst het rapporteren en het prioriteren van activiteiten in de 1e en 2e lijn. Daarnaast coördineert de CISO in geval van incidenten. De CISO heeft een aantal specifieke mandaten, namelijk het uitvoeren van onderzoeken naar alles wat nodig is in het kader van de informatiebeveiliging, en het actief en acuut ingrijpen in systemen wanneer dit nodig is om gevolgen van incidenten te beperken.
- Privacy- en Security Officers zijn specialisten die adviseren, begeleiden en middelen ontwikkelen vanuit de 2e lijn. Momenteel zijn dit in totaal drie functionarissen.
- Bij de afdeling ICT is een Security Specialist fulltime specifiek belast met het operationaliseren van maatregelen op het gebied van ICT.
- Het team datalekken bestaat uit drie privacy- en securityadviseurs en de FG. Als een datalek wordt gemeld, melden zij dit aan de Autoriteit Persoonsgegevens en begeleiden ze de betrokken vakafdeling in de te nemen maatregelen.

De IT-auditor is in functie sinds september 2017 en heeft als taak om vast te stellen in hoeverre de organisatie zich houdt aan de normen op het gebied van IT. Daaronder vallen ook privacy normen. Daarnaast is in maart 2018 de Functionaris Gegevensbescherming benoemd. De FG heeft een toezichthoudende en adviserende rol op het gebied van privacy. Toezicht en advisering strekken zich uit over alle privacy aangelegenheden, dus ook daar waar het gaat om koppelen van gegevensbestanden. Een voornemen om veel persoonsgegevens te koppelen (waarover de motie ‘Big data en privacy: een ongelukkig huwelijk’ gaat) zal altijd tevoren moeten worden beoordeeld door een risicoanalyse te doen. De uitkomst daarvan wordt beoordeeld door de FG. Daarnaast kunnen zowel de IT-auditor als de FG op eigen initiatief een audit doen of op andere manieren onderzoeken of privacy goed wordt beschermd. Zij zullen waar enigszins mogelijk daarin samen optrekken.

In welke mate de huidige capaciteit voldoende is (uitgaande van een systeem van continue verbeteren) of dat een uitbreiding nodig is zal worden behandeld in samenhang met de capaciteitsplanning voor de Kadernota. In voorbereiding hierop is onder andere aan een extern bureau gevraagd om inzicht te geven in de benodigde ontwikkeling inclusief mogelijke scenario’s en

een advisering rond het meten van de volwassenheid. Daarbij wordt de Haarlemse situatie vergeleken met die van andere gemeenten op basis van informatie uit benchmarks.

### D. Veiligheid van het systeem waarmee de vergaderingen worden geregistreerd

Het audiosysteem van Haarlem is door middel van een encoder verbonden met de leverancier van het systeem. Deze verbinding is beveiligd, o.a. op basis van IP-filtering aan onze kant en aan de kant van de leverancier. Deze verbinding wordt pas opgebouwd als er een uitzending is. Voor deze verbinding zijn Haarlem en de leverancier gezamenlijk nodig, Haarlem om de uitzending te starten en leverancier om de ontvangst te accepteren. Als er een besloten vergadering is dan is er geen uitzending. Als tijdens een openbare vergadering een vertrouwelijk agendapunt aan de orde komt dan wordt op dat moment de uitzending gestopt. Dit kan op twee plaatsen gebeuren, zowel op de bedieningspost in de raadszaal als bij de leverancier. Via de bedieningspost wordt de uitzending gestopt en weer aangezet als het vertrouwelijke deel voorbij is.

De leverancier kan hier op ingrijpen op verzoek van de Griffie.

Iemand die in staat zou zijn in te breken op de beveiligde verbinding zou niets horen en zien wanneer de vergadering een vertrouwelijk punt behandelt, omdat op dat moment geen gegevens worden uitgewisseld.

De Griffie controleert voor de vergadering het audiosysteem. Deel van dat proces is het correct omgaan en instellen van vertrouwelijke behandeling van agendapunten.

### E. Overzicht van activiteiten vanaf 2014 tot nu

In de bijlage is een overzicht opgenomen van activiteiten op hoofdlijnen zoals in de afgelopen jaren ontplooid door de organisatie. Dit om een indruk te geven van de omvang van de inspanningen. Wanneer hier behoefte aan is kan dit in de hierboven aangeboden presentatie nader worden toegelicht, zodat een beeld ontstaat van de omvang en complexiteit van deze activiteiten.

### F. Aankondiging nog te behandelen onderwerpen

Omdat momenteel uitgebreid wordt gesproken over Informatiebeveiliging en Gegevensbescherming (privacy) is het goed om aan te kondigen wat er op dit gebied nog volgt in de komende maanden, zodat u niet wordt verrast wanneer dit wordt geagendeerd.

De rapportages over ENSIA worden dit jaar behandeld in de cyclus met de jaarstukken. Hierin wordt horizontaal verantwoording afgelegd naar de gemeenteraad over o.a. SUWInet en DigiD. ENSIA zelf is breder, een groot verantwoordingsstelsel waarbij voornamelijk wordt gerapporteerd naar meerdere toezichthouders.

Wanneer de capaciteitsplanning van de organisatie wordt behandeld zal in samenhang ook de capaciteit rond Informatiebeheer en Gegevensbescherming worden behandeld, zoals hierboven beschreven.

De CISO rapporteert nog over de stand van zaken van de Informatiebeveiliging.

De Functionaris Gegevensbescherming zal nog rapporteren over de stand van zaken van de bescherming van persoonsgegevens. Dit behelst ook rapportage over eventuele datalekken.

Mogelijk worden de rapporten over Informatiebeveiliging en Gegevensbescherming gecombineerd tot één rapportage, omdat de raad het onderwerp graag meer in samenhang beschouwt.

Het college van burgemeester en wethouders,

de secretaris de burgemeester

# Overzicht ontplooide activiteiten 2014 – 2018

## Informatiebeveiliging en Gegevensbescherming

**2014**

- werken met 3 speerpunten informatiebeveiliging (werken aan onderdelen BIG)
- netwerk bouwen met hoofdafdelingen en teams
- opzetten en verzorgen van bewustwordingsbijeenkomsten
- aanbevelingen naar organisatie (incidenten en onderzoeken)
- opzetten en initiëren van CSIRT team (interventieteam voor incidenten)
- aansluitproces bij IBD Informatiebeveiligingsdienst van VNG (stap 1 en 2)
- Opzetten rol en aanstellen CISO, ISO en CIO team

**2015**

- verzorgen van 40 tal bewustwordingsbijeenkomsten
- coördinatie CSIRT (interventieteam)
- vervangen en verbeteren van antivirus pakket op vaste werkplekken
- aanbevelingen naar organisatie (incidenten en onderzoeken)
- Inventariseren en wegen van BIG taken
- aansluitproces bij IBD (stap 3 en 4)
- Security Patchmanagement - proces IBD meldingen en mitigeren van kwetsbaarheden
- toegang tot Document managementsysteem via single logon vanuit Active Directory
- aanschaf en aanbesteding van Intrusion Prevention System
- verzoek tot aanpassing van inkoopvoorwaarden
- introduceren extra pro-actieve endpoint beveiliging tegen ransomware

**2016**

- verzorgen van 30-tal bewustwordingsbijeenkomsten
- Inventarisatie domeinnamen geregistreerd op naam van gemeente Haarlem
- coördinatie CSIRT (interventieteam)
- blokkeren van Internet Explorer extenties (met gecontroleerde uitzonderingen)
- implementeren van extra pro-actieve endpoint beveiliging op alle vaste werkplekken
- Cloud Risk Assessment Netskope
- Maken afspraken Pleio over het delen van gevoelige informatie op Insite
- risico inventarisatie en onderzoek RIEC-NH
- aanbevelingen naar organisatie (incidenten en onderzoeken)
- realiseren van raamcontract Security met adviespartij ITSec (meer kennis in huis)
- Application Risk Assessment Publieksbalie
- selectie van tool voor ISMS voor BIG (governance & compliancy)
- Insite pagina met goede informatie over Informatiebeveiliging
- vaak aandacht voor phishing e-mails, inclusief houden van een phishing test
- media onderzoek ‘Digitale Veiligheid gemeenten’
- opstarten proces datalekken
- aandacht gevraagd voor persoonsgegevens in de email
- werkgroep BIG

- input voor digitaliseringsprojecten
- advies en uitwisseling van kennis met Cocensus
- start aanpassen van inkoopvoorwaarden overeenkomstig GIBIT
- implementatie van veilige mail standaarden

**2017 t/m begin 2018**

- Adblock en traceerbeveiliging laten activeren in Internet Explorer
- Advies voor de geheime raadsstukken – in overleg met griffie
- Input op project motie25 – deelname aan PIA
- Onderhouden en bijwerken ICT foto IBD
- Productverkenning en advisering diverse applicaties
- Veilige bestandsdeling voor interne medewerkers (met adoptie van OneDrive in Office365)
- Functionele protectie test en oplossen enkele risico's
- Bewustwording:
    - Sessies 'Heb je wat te verbergen?' op de Winterschool 2017
    - Spreker Maria Genova 2 sessies
    - Diverse waarschuwingen op Insite+
    - Hacking workshops voor ICT 2 sessies
    - 6 Bewustwordingssessies in Haarlem en 4 in Zandvoort
- Inrichting governance en compliance tool voor de BIG gereed, functioneel getest, diverse maatregelen benoemd, het beleggen ervan bij juiste actoren volgt in 2018
- Aandacht voor Learning Management Systeem bij HRM, TOM leiderschapstraject
- Betrokken bij ontwikkeling van de dienstverlening bij de bezoekersbalie: nieuwe apps, host PC, tablets, nieuwe betaalmogelijkheden
- Betrokken bij ontwikkeling bezoekersparkeren
- Betrokken bij aanbestedingen eHRM, Sociale wijkteams
- Activiteiten team Datalekken
- Meer grip op webdomeinen van Haarlem in samenwerking met webbureau (Webvisie en beleid)
- Regelen mandatering CISO in organisatiestatuut
- Pro-actief security en privacy inbrengen in digitaliseringsprojecten
- CSIRT, diverse activiteiten ter voorkoming van incidenten
- Begeleiding voor pentesten en om toegang goed te houden DigiD
- DigiD audit april 2017
- Maandmonitor ICT Patchmanagement
- Volgen van diverse kennissessies DA2020, InfoSecurity, Cloud Identity 2017, NCSC One
- ENSIA rapportage opleveren
- Installeren Functionaris gegevensbescherming
- uitvoeren van privacy assessments
- ontwikkelen plan van aanpak voor implementatie van AVG.
- vaststellen nota Privacybeleid
- vaststellen privacyreglement en privacyverklaring

Bovenstaande lijst is in 2018 opgesteld en is niet uitputtend. De lijst met activiteiten dekt de tijd tot het RKC onderzoek: Q2 van 2018.