Gemeente Haarlem

Informatienota

Onderwerp Opvolging RKC aanbevelingen Informatiebeveiliging	
Nummer	2019/465158
Portefeuillehouder	Botter, J.
Programma/beleidsveld	6.2 Gemeentelijk Bestuur
Afdeling	CC
Auteur	Hut, F.J.
Telefoonnummer	023-5114955
Email	fhut@haarlem.nl
Kernboodschap	De aanbevelingen van het RKC rapport over informatiebeveiliging worden serieus opgepakt. Deze notitie beschrijft hoe de gemeenteraad regelmatig over Informatiebeveiliging zal worden geïnformeerd en wat de status is van de afhandeling van de bevindingen van de RKC.
Behandelvoorstel voor commissie	Het college stuurt de informatienota ter kennisname naar de commissie Bestuur. Met deze nota worden de volgende toezeggingen afgedaan - 2019/221188 over inzicht in benodigde formatie en middelen voor informatiebeveiliging - 2019/221144 plan van aanpak informatiebeveiliging
Relevante eerdere besluiten	- Raadstuk RKC rapport Verantwoordelijkheid voor Veiligheid, onderzoek naar Informatiebeveiliging (2019/143523) in de raadsvergadering van 28 maart 2019 - Raadsinformatiebrief Informatiebeveiliging en gegevensbescherming, aanvullende informatie (2019/241916) in de raadsvergadering van 28 maart 2019 - Informatienota Motie 14.2 Testen doen we met geanonimiseerde gegevens (2019/443656) in de collegevergadering van 11 juni 2019
Besluit College d.d. 18 juni 2019	Het college besluit om: 1. de informatienota aan de commissie vast te stellen; 2. op de bij dit besluit behorende **bijlage 1** geheimhouding op te leggen aan de commissie Bestuur op grond van artikel 86 van de Gemeentewet, vanwege de bescherming van de economische of financiële belangen van de gemeente, als bedoeld in artikel 10, tweede lid, aanhef en onder van de Wet openbaarheid van bestuur. de secretaris, de burgemeester,

Inleiding
Conform het Strategisch Gemeentelijk Informatiebeveiligingsbeleid wordt toegewerkt naar een beveiliging die – gebaseerd op risico's – continu verbetert. Hierbij is de nieuwe Baseline Informatiebeveiliging Overheid (BIO) een belangrijk instrument. De RKC heeft door haar onderzoek onderwerpen aangewezen die met voorrang moeten worden aangepakt.

Deze notitie beschrijft hoe de gemeenteraad regelmatig over Informatiebeveiliging zal worden geïnformeerd en wat de status is van de afhandeling van de bevindingen van de RKC.

2. Kernboodschap
Implementeren van het beleid
Haarlem neemt deel aan de pilot met de BIO onder regie van VNG Realisatie. De planning van Haarlem is binnen de planning van VNG Realisatie gepast. Benodigde middelen en capaciteit zullen worden beoordeeld als het totaalbeeld duidelijk is.

Voor het daadwerkelijk realiseren van verbeteringen is het nodig dat iedere afdeling structureel tijd en aandacht aan risico's en beveiliging besteedt. Ook speelt de pilot met de nieuwe Baseline Informatiebeveiliging Overheid (BIO) die in het vierde kwartaal van dit jaar nog kan leiden tot bevindingen waarin moet worden geïnvesteerd. Het college beoordeelt de benodigde middelen en capaciteit als er concrete inrichtingsvoorstellen zijn uitgewerkt en er ook zicht is op de uitkomsten van de zelfevaluatie volgens de BIO.

De belangrijkste focus voor de rest van 2019 is gericht op drie onderwerpen:

- Compliance volgens het ENSIA stramien. Dit is noodzakelijk om DigiD, Suwinet en basisregistraties te mogen blijven gebruiken.
- De pilot met de BIO. Eén van de resultaten hiervan is dat een Self Assessment wordt uitgevoerd waardoor zichtbaar wordt welke zaken nog ontbreken.
- Uitwerken van inrichtingsvoorstellen, die rekening zullen houden met de eerste ervaringen met de BIO.

De planning

Het BIO pilotprogramma door VNG Realisatie hanteert de volgende planning:

- Op 1 juli worden de vragenlijsten opgeleverd.
- Tussen 1 juli en 1 november vinden de zelfevaluaties van deelnemende gemeenten plaats.
- Tussen 1 oktober en 1 november wordt proefgedraaid met de eerste verantwoording
- Tussen 1 november en 1 januari wordt geëvalueerd

De planning van Haarlem sluit hierop aan:

- Tot 1 juli – participeren in BIO werkgroepen ter voorbereiding van de BIO pilot
- 1 juli – 1 november – BIO zelfevaluatie
- 1 oktober – 1 november – eerste BIO verantwoording
- 1 oktober – Uitgewerkte inrichtingsvoorstellen en prioriteiten ten behoeve van de capaciteitstoewijzing 2020

<u>Weerbaarheid tegen Cybercrime</u>
De technische bevindingen van Bureau Hoffmann zijn en worden opgepakt. Een eerste hertest is uitgevoerd in april, een tweede hertest wordt uitgevoerd na 15 juli.
Er is goede voortgang. Hierop wordt op toegezien door de Chief Information Security Officer (CISO) die erover rapporteert aan de CIO.

Het project Any vernieuwt de verouderde ICT infrastrucuur. Dit project zal een aantal structurele punten verhelpen. Een onafhankelijke partij krijgt de opdracht om te beoordelen of de voorgestelde implementatie inderdaad het gewenste effect gaat hebben.

De technische bevindingen uit het rapport van Bureau Hoffmann zijn en worden opgepakt. De eerste verificatie door een externe partij heeft in april plaatsgevonden. Hieruit zijn restpunten naar voren gekomen die weer worden opgepakt. De tweede externe verificatie zal gepland worden na 15 juli als weer een aantal openstaande punten zal zijn afgerond.

Een aantal belangrijke punten zal worden opgelost door het project Any. Een derde partij zal gevraagd worden om te verifiëren dat de beoogde resultaten van dit project inderdaad de bevindingen van Hoffmann zullen verhelpen. Dit is tevens de uitwerking van de gevraagde second opinion uit de motie van OPH cs.

Met een externe partij is een contract afgesloten waaronder het komende jaar pentests kunnen worden uitgevoerd. Bij een pentest zoekt een Ethisch Hacker naar zwakke plekken zodat deze kunnen worden hersteld.

De CISO houdt toezicht op de voortgang en rapporteert hierover aan de CIO.

In de werkwijze van ICT worden taken gesplitst en onderverdeeld over afdelingen en mensen. Oorspronkelijk waren de 17 bevindingen van Bureau Hoffman uitgesplitst in 28 taken.

Resultaten van een hertest en gedeeltelijke afhandeling met vervolgwerkzaamheden leiden in de administratie van ICT tot nieuwe taken waardoor de totaalaantallen veranderen. Een getalsmatige rapportage op basis hiervan wordt hiermee een bewegend doel waarmee voortgang niet goed is te volgen.

Deze rapportage gaat daarom terug naar de 17 bevindingen van Bureau Hoffmann en rapporteert over de status daarvan. In de bijlage zijn deze bevindingen opgenomen.

De huidige (20 juni 2019) stand van zaken voor wat betreft de technische onderwerpen is:

- Beleid en Privacy (1)
    - Met betrekking tot het testen met geanonimiseerde gegevens is de commissie geïnformeerd via een separate informatienota (2019/443656)

- Bevindingen vanuit de externe pentest (7)
    - 5 (van 7) bevindingen zijn verholpen.
    - 1 (van 7) is gedeeltelijk verholpen. Een leverancier moet nog een update uitvoeren waarvoor geen planning is afgegeven. Toegang tot de desbetreffende applicatie vanaf internet is geblokkeerd om daarmee het risico te verminderen.
    - 1 (van 7) Two-factor authenticatie zal opgeleverd worden door project Any

- Bevindingen vanuit de interne pentest (8)
    - 3 (van 8) bevindingen zijn verholpen.
    - 2 (van 8) zijn gepland gereed in juni en juli.
    - 1 (van 8) ontbrekende updates zijn gedeeltelijk verholpen. Het resterende gedeelte betreft het uitfaseren van een oude Oracle omgeving die gepland voor 1 oktober zal zijn afgerond.
    - 1 (van 8) versleutelen van schijven zal worden opgeleverd door project Any. Om het risico in de tussentijd te mitigeren wordt op dit moment getest met maatregelen om het opslaan van gegevens op vaste PC's grotendeels te voorkomen waardoor het beschreven risico's op een andere wijze grotendeels wordt ondervangen.
    - 1 (van 8) voor netwerkauthenticatie zijn de eisen uitgewerkt. Haarlem doet mee aan de aanbesteding GGI-veilig door VNG. De gunning van deze aanbesteding wordt verwacht omstreeks juli 2019**.** De vraag naar een geïmplementeerd product wordt zo snel mogelijk na de gunning in de markt gezet.

- Bevindingen vanuit het fysiek binnendringen (1)
    - Gepland op 15 juli zullen vrije aansluitingen standaard inactief zijn gemaakt, en zal het niet meer zomaar mogelijk zijn om de kabel uit een ander apparaat te gebruiken. Netwerkauthenticatie en versleutelen van schijven spelen bij het beperken van risico's ook een rol. Deze onderwerpen staan al beschreven bij de vorige paragraaf over de interne pentest.

Raadinformatie
De raad wordt tweemaal per jaar via een informatienota geïnformeerd over de ontwikkeling van de Informatiebeveiliging. Bij het opstellen van deze informatienota worden externe deskundigen betrokken.

Opzetten van een risicoregister
Van belang is dat Haarlem risico's kent en serieus neemt. In juli zal een eerste risico-inschatting bekend zijn op basis waarvan prioriteiten gesteld kunnen worden. Deze informatie zal na de zomer met de raadscommissie worden gedeeld.

De theorie verwacht dat een methode wordt gekozen (dit maakt het proces herhaalbaar), dat risico's worden geïnventariseerd en geanalyseerd en een Kans en Impact krijgen, dat ieder risico een eigenaar krijgt die besluit hoe ermee om te gaan, en dat iedere hieruit voortkomende actie een eigenaar krijgt. Over de voortgang van de acties wordt gerapporteerd, en de risicoanalyse wordt periodiek herhaald om de ontwikkelingen te kunnen volgen. Centraal in dit proces staat het risicoregister.

Het opzetten, vullen en beheren van een risicoregister is een grote hoeveelheid werk waarvoor op dit moment de capaciteit niet beschikbaar is. Vanuit de optiek van IV speelt mee dat IV-risico's niet in isolement bestaan maar ook relaties hebben met andere domeinen. Bv een applicatie wordt niet op tijd opgeleverd, hierdoor wordt een ingeboekte besparing bij afdeling X niet gerealiseerd. Risico's kunnen daarom het best integraal worden gemanaged.

Er kan een verstandige stap worden gezet door grootste risico's te benoemen zonder in veel detail te gaan, en tegen deze grootste risico's beheersmaatregelen te treffen. De op 1 april gestarte CISO zal in juli in concept zijn eerste analyse en voorgestelde aanpak opleveren.

Hierbij wordt helemaal in lijn met de opmerkingen in de raadsvergadering breder gekeken dan alleen de kwetsbaarheid voor hackers. Onderdeel van de aanpak zal zijn om externe deskundigen in te zetten om een oordeel te geven over gebieden waar specialistische kennis ontbreekt en risico's hoog kunnen zijn.

De analyse en voorgestelde aanpak zal na de zomer met de raadscommissie worden gedeeld.

3. Consequenties
Met deze aanpak komt de Gemeente Haarlem voor informatiebeveiliging In Control.

De gemeenteraad krijgt na de zomer beter zicht op risico's en wordt via de toegezegde informatienota's actief geïnformeerd.

4. Vervolg
Na de zomer wordt de eerste analyse van de CISO en de voorgestelde aanpak met de raadscommissie gedeeld.

Halfjaarlijks wordt de raadscommissie door middel van een informatienota geïnformeerd.

5. Bijlagen
De samengevatte bevindingen uit het rapport van Bureau Hoffmann zijn als bijlage 1 toegevoegd.

Het wordt kwaadwillenden makkelijker gemaakt als de tekst van de bevindingen openbaar wordt gemaakt. Daarom is gevraagd om deze bijlage geheim te verklaren.