Gemeente Haarlem

Informatienota

Onderwerp Informatienota Informatiebeveiliging voorjaar 2021	
Nummer	2021/217257
Portefeuillehouder	Botter, J.
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	CC
Auteur	Hut, F.J.
Telefoonnummer	023-5114955
Email	fhut@haarlem.nl
Kernboodschap	Volgens afspraak wordt tweemaal per jaar gerapporteerd over informatiebeveiliging. In deze nota wordt ingegaan op de afgesproken onderwerpen van de juni-rapportage: • Status van openstaande punten gerelateerd aan het RKC onderzoek • Voortgang van de beveiligingsprioriteiten • Voortgang van verbeterplannen DigiD en Suwinet • Analyse van Security incidenten • ENSIA verantwoording over het vorige jaar met duiding van de resultaten en de relatie tot de benoemde beveiligingsprioriteiten.
Behandelvoorstel voor commissie	Het college stuurt de informatienota ter kennisname naar de commissie Bestuur. In juni 2020 is met informatienota 2020/465284 (bijlage A) afgesproken dat over deze onderwerpen jaarlijks in juni wordt gerapporteerd.
Relevante eerdere besluiten	2019/311846 RKC Onderzoek / Raadsinformatie 2019/311830 RKC Onderzoek / Implementatie beleid 2019/311840 RKC Onderzoek / Kwetsbaarheden 2020/465284 Stand van zaken informatiebeveiliging 2020/948418 Rapportage informatiebeveiliging najaar 2020 2021/90637 ENSIA verantwoording 2020 Haarlem 2021/55774 Rapportage volwassenheid Informatiebeveiliging januari 2021
Besluit College d.d. 25 mei 2021	1. Het college stelt de informatienota aan de commissie vast. 2. Op de bij deze nota behorende bijlagen 2, 3, 4 en 5 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
In juni 2020 is met informatienota 2020/465284 (bijlage A) afgesproken dat over de volgende onderwerpen ieder jaar in juni wordt gerapporteerd:

- Status van openstaande punten gerelateerd aan het RKC onderzoek
- Voortgang van de beveiligingsprioriteiten
- Voortgang van verbeterplannen DigiD en Suwinet
- Analyse van Security incidenten
- ENSIA verantwoording over het vorige jaar met duiding van de resultaten en de relatie tot de benoemde beveiligingsprioriteiten.

Hieronder wordt op ieder van deze punten ingegaan.

2. Kernboodschap
Rapportages worden vanuit verschillende perspectieven en voor verschillende doelen gemaakt. Om ze goed te kunnen duiden is in bijlage 1 inzichtelijk gemaakt hoe de onderlinge samenhang is.

De Baseline Informatiebeveiliging Overheid (BIO) wordt risico-gebaseerd geïmplementeerd. Hierbij wordt het mechanisme van ISO27001 gebruikt om jaarlijks prioriteiten te stellen.

De onafhankelijke volwassenheidsrapportage ten opzichte van de ISO27001 geeft het beste beeld om de ontwikkeling van de beveiliging te volgen. Het omvat de BIO, omvat de domeinen die het RKC-onderzoek heeft geraakt, en het is het oordeel van een onafhankelijke derde. Voorstel is om in de jaarcyclus aan het ISO27001-rapport het meeste gewicht te geven.

Als verplichte overheidsnorm wordt de BIO geïmplementeerd. De ISO27001 benadering met een risicoanalyse wordt gebruikt om ieder jaar prioriteiten te stellen. Dit betekent dat verminderen van risico's de primaire drijfveer is, met uiteindelijk een hogere score op de BIO-Zelfevaluatie als gevolg.

<u>BIO-Zelfevaluatie</u>
De BIO-Zelfevaluatie is consistent met de ISO27001 volwassenheidsrapportage (2021/55774) en met de risicoanalyse bij de informatienota (2020/948418) die in december in de Commissie Bestuur is behandeld.

In bijlage 2 (Geheim) staat de beantwoording van de zelfevaluatie voorafgegaan door een korte toelichting over de opzet van de vragenlijst.

In bijlage 3 (Geheim) wordt duiding gegeven, en wordt de relatie gelegd met prioriteiten en verbeteracties.

<u>Status van openstaande punten gerelateerd aan het RKC onderzoek</u>

2019/311846 RKC Onderzoek / Raadsinformatie – Aan de RKC is onderbouwd aangegeven dat dit wordt beschouwd als afgehandeld. Hierop is positief gereageerd. Het proces zal worden gestart om dit punt formeel af te doen.

2019/311830 RKC Onderzoek / Implementatie beleid – De stappen hiervoor zijn allemaal genomen, dit zal aan de RKC worden voorgelegd.

2019/311840 RKC Onderzoek / Kwetsbaarheden – Van 15 bevindingen uit de interne- en de externe pentest zijn 12 verholpen, 2 gedeeltelijk verholpen en staat 1 nog open. In bijlage 4 (Geheim) staat dit nader toegelicht.

Voortgang van de beveiligingsprioriteiten
Binnen de afdeling IV is een programmamanager gestart om de veelheid van onderwerpen in samenhang aan te sturen. Manager IV en de CISO zijn beide lid van de stuurgroep.

In bijlage 5 (Geheim) wordt de status beschreven van de onderwerpen die in december 2020 zijn geprioriteerd.

Voortgang van verbeterplannen DigiD en Suwinet
Voor DigiD wordt aan één standaard niet voldaan. Hiervoor is het nodig dat een externe leverancier zijn software aanpast. Volgens planning levert deze leverancier de aangepaste software in de maand mei op. Daarna wordt door ons getest en maken we het plan voor de implementatie.

Voor Suwinet hebben we het controleprogramma met externe ondersteuning duidelijker gestructureerd. Er wordt nu volgens dit programma gewerkt. De bedoeling is om medio dit jaar een tussentijds extern review uit te laten voeren om zeker te weten dat aan alle normen wordt voldaan.

Analyse van Security incidenten
Er zijn vooral kleinere incidenten zoals verkeerd verstuurde berichten, SPAM-infecties in Apple-agenda's en het klikken op linkjes.

Wat toeneemt is dat relaties worden gehackt, en dat van daaruit de gemeente wordt aangevallen. Dit leidt dan bijvoorbeeld tot een valse factuur of een vals linkje dat – vanwege de vertrouwde herkomst – eerder wordt vertrouwd. In één geval heeft een medewerker gegevens ingevoerd – dit direct gemeld – en door direct actie te nemen is dit zonder nadelige gevolgen gebleven.

Bij urgente meldingen vanuit de Informatiebeveiliginsdienst (IBD, onderdeel van VNG) zijn we steeds in staat om snel te handelen, ook zonder dat hiervoor formele 24/7 afspraken zijn gemaakt.

3. Consequenties
Er zijn geen bijzondere consequenties te melden. Geplande activiteiten worden gedekt vanuit beschikbare budgetten.

4. Vervolg
Er wordt continu gewerkt aan verbetering. In het najaar is de volgende rapportage.

5. Bijlagen
Bijlage 1 – Onderlinge verhouding van perspectieven en rapportages
Bijlage 2 – GEHEIM – BIO-Zelfevaluatie Haarlem 2020
Bijlage 3 – GEHEIM – Duiding van BIO-Zelfevaluatie en relatie met prioriteiten en verbeteracties
Bijlage 4 – GEHEIM – Openstaande kwetsbaarheden uit het RKC onderzoek
Bijlage 5 – GEHEIM – Voortgang van beveiligingsprioriteiten