Gemeente Haarlem

# Informatienota

| | |
|---|---|
| **Onderwerp**<br>Informatienota informatiebeveiliging voorjaar 2022 | |
| Nummer | 2022/645996 |
| Portefeuillehouder | Botter, J. |
| Programma/beleidsveld | 7.2 Algemene dekkingsmiddelen |
| 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:<br>• Status van openstaande punten gerelateerd aan het RKC onderzoek<br>• Voortgang van de beveiligingsprioriteiten<br>• Voortgang van verbeterplannen DigiD en Suwinet<br>• Analyse van Security incidenten<br>• 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<br>2019/311830 RKC Onderzoek / Implementatie beleid<br>2019/311840 RKC Onderzoek / Kwetsbaarheden<br>2020/465284 Stand van zaken informatiebeveiliging<br>2021/217257 Informatienota Informatiebeveiliging voorjaar 2021<br>2021/517885 Informatienota Informatiebeveiliging najaar 2021<br>2022/380516 ENSIA verantwoording Haarlem 2021 |
| Besluit College<br>d.d. 24 mei 2022 | 1. Het college stelt de informatienota aan de commissie vast.<br>2. Op de bij deze nota behorende bijlagen 1, 2, 3 en 4 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 onder artikel 5.1, tweede lid, onder b, Wet open overheid.<br><br>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 gaan regelmatig over dezelfde onderwerpen, maar worden vanuit verschillende perspectieven en voor verschillende doelen gemaakt. Vorig jaar is de onderlinge samenhang van de verschillende rapportages uitgewerkt (zie bijlage 1 van 2021/217257 *Informatienota Informatiebeveiliging voorjaar 2021)*.

*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, de domeinen die het RKC-onderzoek heeft geraakt, en het is het oordeel van een onafhankelijke derde.

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 en met de risicoanalyse bij de informatienota (2021/517885) die op 20 januari 2022 in de Commissie Bestuur is behandeld.

In bijlage 1 (Geheim) staat de beantwoording van de BIO-zelfevaluatie voorafgegaan door een korte toelichting over de opzet van de vragenlijst.

In bijlage 2 (Geheim) wordt duiding gegeven, en wordt de relatie gelegd met prioriteiten en verbeteracties.

Status van openstaande punten gerelateerd aan het RKC onderzoek
2019/311846 RKC Onderzoek / Raadsinformatie: is afgehandeld.

2019/311830 RKC Onderzoek / Implementatie beleid: is afgehandeld.

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 3 (Geheim) staat dit nader toegelicht.

Voortgang van de beveiligingsprioriteiten
In bijlage 4 (Geheim) wordt de status beschreven van de onderwerpen die in informatienota 2021/517885 zijn geprioriteerd.

Voortgang van verbeterplannen DigiD en Suwinet
Voor DigiD werd voor één aansluiting niet aan alle normen voldaan. De verantwoordelijke beheerders hebben gemeld dat alle issues zijn verholpen. De herbeoordeling door de externe auditor zal dit middels een Assurance Verklaring bevestigen, waarna wij deze verklaring aan toezichthouder Logius zullen sturen.

Voor Suwinet werd aan alle normen voldaan. Hier is geen verbeterplan nodig.

Analyse van Security incidenten
Er is een aantal langdurige verstoringen geweest na onderhoud van de Any-omgeving. Hieruit zijn lessen geleerd: zulk werk wordt nu formeler voorbereid om verstoringen te voorkomen, en specialistische externe ondersteuning wordt vooraf georganiseerd om verstoringen sneller op te kunnen lossen.

Er is een Wifi-verstoring geweest doordat een kabel van Vodafone is beschadigd.

Daarnaast zijn er altijd ook kleinere incidenten. Hierin vallen geen bijzondere patronen op.

Bij urgente meldingen vanuit de Informatiebeveiligingsdienst (IBD, onderdeel van VNG) zijn we steeds in staat geweest om snel te handelen, ook zonder dat hiervoor formele 24/7 afspraken zijn gemaakt. Ook is het voorgekomen dat wij al actie hadden ondernomen voordat de IBD de melding had gedaan.

**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 – GEHEIM – BIO-Zelfevaluatie Haarlem 2021
Bijlage 2 – GEHEIM – Duiding van BIO-Zelfevaluatie en relatie met prioriteiten en verbeteracties
Bijlage 3 – GEHEIM – Openstaande kwetsbaarheden uit het RKC onderzoek
Bijlage 4 – GEHEIM – Voortgang van beveiligingsprioriteiten