Gemeente Haarlem

Informatienota

Onderwerp Informatienota Informatiebeveiliging najaar 2022	
Nummer	2022/1508877
Portefeuillehouder	Raadt, E. de
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	CC
Auteur	Hut, F.J.
Telefoonnummer	023-5114955
Email	fhut@haarlem.nl
Kernboodschap	Het college informeert de commissie Bestuur over de afgesproken onderwerpen op het gebied van Informatiebeveiliging: • Status van openstaande punten gerelateerd aan het RKC onderzoek • Voortgang van de beveiligingsprioriteiten • Voortgang van verbeterplannen DigiD en Suwinet • Analyse van Security incidenten • Risico analyse • Voorgestelde beveiligingsprioriteiten voor het volgende jaar • Beoordeling van de informatiebeveiliging, waaronder de volwassenheid
Behandelvoorstel voor commissie	Het college stuurt de informatienota ter kennisname naar de commissie Bestuur. Hiermee wordt invulling gegeven aan de afspraak om tweemaal per jaar over de stand van informatiebeveiliging te rapporteren.
Relevante eerdere besluiten	2019/311846 RKC Onderzoek / Raadsinformatie 2019/311830 RKC Onderzoek / Implementatie beleid 2019/311840 RKC Onderzoek / Kwetsbaarheden 2019/355441 Motie 14.1 Integraal Risicomanagement 2019/940161 Afstemmen structuur van voortgangsrapportage 2020/854267 Referentiekader voor volwassenheid van Informatiebeveiliging
Besluit College d.d. 29 november 2022	Het college besluit: 1. De informatienota aan de commissie Bestuur vast te stellen; 2. Geheimhouding op te leggen aan de commissie Bestuur ten aanzien van de bij deze informatienota behorende bijlagen A, B, C en D, 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, aanhef en onder b, van de Wet open overheid. De geheimhouding op bijlagen A, B, C en D geldt voor een periode van 3 jaar, en vervalt op 1 december 2025.

	de secretaris,	de burgemeester,

Inleiding
Deze notitie met bijlagen is de afgesproken halfjaarlijkse rapportage over Informatiebeveiliging.

In notitie *2019/940161 Afstemmen structuur van voortgangsrapportage* zijn de onderwerpen beschreven waarover 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
- Risico analyse
- Voorgestelde beveiligingsprioriteiten voor het volgende jaar
- Beoordeling van de informatiebeveiliging, waaronder de volwassenheid.

2. Kernboodschap
Het lezen van de bijlagen is nodig om een goed beeld van de situatie te krijgen. Vanwege het soort informatie daarin zijn deze bijlagen geheim gemaakt, en is de strekking ervan niet in de kernboodschap samengevat.

<u>Status van openstaande punten gerelateerd aan het RKC onderzoek</u>
Bij de bespreking van het RKC onderzoek zijn de acties ondergebracht in drie verschillende categorieën die ieder apart in de administratie zijn opgenomen:

- Raadsinformatie
- Implementatie van beleid
- Kwetsbaarheden.

2019/311846 RKC Onderzoek / Raadsinformatie:
Dit onderdeel is afgesloten.

2019/311830 RKC Onderzoek / Implementatie beleid:
Dit onderdeel is afgesloten.

2019/311840 RKC Onderzoek / Kwetsbaarheden.
In het rapport zijn 15 technische kwetsbaarheden genoemd. Hiervan zijn 13 geheel verholpen, 1 is gevorderd maar nog niet afgerond, 1 moet nog worden gestart.

Uitgebreidere informatie is te vinden in Bijlage A (Geheim).

Voortgang van beveiligingsprioriteiten
Er is voortgang, waarbij beschikbare capaciteit een belemmering is. Uitgebreidere informatie is te vinden in Bijlage B (Geheim).

Voortgang van verbeterplannen DigiD en Suwinet
Suwinet voldeed bij de audit aan alle normen, hier was geen verbeterplan nodig.

Eén DigiD-aansluiting voldeed niet aan alle normen. Binnen de door Logius aangegeven hersteltermijn is een heraudit gedaan met positief resultaat. De assurance verklaring is ingeleverd, waarna dit onderwerp is afgesloten.

Analyse van Security incidenten
De geregistreerde incidenten gaan vooral over standaard onderwerpen als:

- Een verloren of gestolen mobiel apparaat.
- Het klikken op een onbetrouwbaar linkje, mogelijk gevolgd door het invoeren van gebruikersnaam en wachtwoord.

De volgende onderwerpen zijn hier het vermelden waard:

- Een aantal keren is de Any-omgeving niet beschikbaar geweest als gevolg van onderhoud, of als gevolg van herstelacties na onderhoud. Hierbij is spanning tussen snel doorvoeren van wijzigingen enerzijds (dit is onze keus, want criminelen kunnen gebruik maken van bekend geworden kwetsbaarheden), en even rustig afwachten anderzijds (zodat anderen tegen problemen aanlopen, en daarvoor oplossingen zijn als je zelf de wijziging doorvoert). Hierin is een modus gevonden door grondig voor te bereiden en tijdens en na de wijziging extern specialisme paraat te hebben waarop direct kan worden teruggevallen.
- In mei is een hacker erin geslaagd om een bestand naar één van onze webservers te gaan uploaden. Dit is door de beveiligingssoftware direct gestopt. Voor nadere analyse is de website een weekend offline geweest.
  De conclusie van de analyse was:
  - We begrijpen wat de toedracht is geweest.
  - Als de beveiligingssoftware niet zou hebben ingegrepen, dan was de aanval door een volgende beheersmaatregel gestopt.
  - Er is geen toegang geweest tot gegevens, er zijn geen wijzigingen op de server aangebracht.
  - Samenvattend heeft de bescherming goed gewerkt.

Er zijn geen aanwijzingen voor andere, ernstige incidenten.

Risico analyse en voorgestelde beveiligingsprioriteiten voor het volgende jaar
Er is conform het beleid een Informatiebeveiliging Risico Analyse uitgevoerd waarop de prioriteiten van het beveiligingsplan worden gebaseerd.

In bijlage C is het gevolgde proces stap voor stap te volgen.

Beoordeling van de informatiebeveiliging, waaronder de volwassenheid
In collegebesluit 2020/854267 is gekozen voor het gebruik van ISO 27001 als referentiekader.

Eind augustus en begin september is de audit van 2022 uitgevoerd. Fysieke beveiliging met waarnemingen ter plaatse zijn nu voor het eerst meegenomen, omdat de Covid-beperkingen voorbij zijn. De aanbevelingen uit de audit zijn meegewogen bij de beveiligingsprioriteiten van 2023.

Het rapport van de audit is opgenomen als bijlage D (Geheim).

De norm ISO 27001 en daaraan gekoppeld ISO 27002 zijn recent aangepast om beter te passen bij de manier waarop informatieveiligheid zich ontwikkelt. Volgend jaar zal beoordeeld worden tegen de nieuwe versie van deze normen.

Op 1 september 2021 is een Business Continuïteitsmanager gestart. Continuïteit is een onderdeel informatiebeveiliging dat heel breed is. Hiervoor is een specifieke ISO-norm, de ISO 22301. Het is de intentie om bij de audit van volgend jaar de opstart van Business Continuïteit tegen dit kader te beoordelen.

Geheimhouding
Ten aanzien van de bij deze nota behorende bijlagen A, B, C en D wordt geheimhouding opgelegd aan de commissie Bestuur.

In de bijlagen is informatie opgenomen over de informatiebeveiligingsmaatregelen die de gemeente treft om haar gegevens en de systemen te beveiligen. Deze informatie kan kwaadwillenden helpen bij het doorbreken van de beveiliging, wat kan leiden tot grote schade voor de gemeente.

De geheimhouding op bijlage A, B, C en D geldt voor een periode van 3 jaar, en komt te vervallen op 1 december 2025. Tegen die tijd zullen de belangrijkste kwetsbaarheden verholpen zijn, en daarmee zal de reden vervallen zijn waarom geheimhouding nu wordt opgelegd.

Indien de commissie Bestuur zich met betrekking tot dit collegebesluit richt tot de raad en de vertrouwelijke aard van de in de bijlagen opgenomen informatie geldt op dat moment onverminderd, zal alsnog bekrachtiging van de opgelegde geheimhouding dienen te plaats te vinden, als bedoeld in artikel 25, derde lid van de Gemeentewet. In dat geval is ook alleen de raad bevoegd de opgelegde geheimhouding op te heffen.

3. Consequenties
--

4. Vervolg
Het beveiligingsplan voor 2023 zal nu worden uitgewerkt. De commissie Bestuur zal geïnformeerd blijven via de afgesproken halfjaarlijkse rapportages.

5. Bijlagen

Bijlage A GEHEIM - Status van openstaande punten gerelateerd aan het RKC onderzoek
Bijlage B GEHEIM - Status van beveiligingsprioriteiten
Bijlage C GEHEIM - Informatiebeveiliging Risico Analyse najaar 2022 en prioriteiten 2023
Bijlage D GEHEIM - Volwassenheidsbepaling ISO 27001 Gemeente Haarlem