Gemeente Haarlem

Informatienota

Onderwerp Informatienota Informatiebeveiliging najaar 2021	
Nummer	2021/517885
Portefeuillehouder	Botter, J.
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. 2 november 2021	1. Het college stelt de informatienota aan de commissie vast. 2. Op de bij deze nota behorende bijlagen A, B, C en D 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 alsmede het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden, als bedoeld in artikel 10, tweede lid, aanhef en onder b en g van de Wet Openbaarheid van Bestuur. De geheimhouding op bijlage A, C en D geldt voor onbepaalde tijd. De geheimhouding op bijlage B geldt voor een periode van een jaar en komt te vervallen op 1 december 2022.

	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

Met deze nota wordt toezegging 2019/940161 afgesloten. Het is nu een regulier proces geworden. Er zijn vijf halfjaarlijkse rapportages geweest en de rapportages van volgend jaar juni en december zijn al weer ingepland.

Met deze nota wordt motie 2019/355441 afgesloten. Het is nu een regulier proces geworden. Er is nu drie keer een jaarlijkse risicoanalyse uitgevoerd op basis waarvan prioriteiten voor het komend jaar worden bepaald. De risicoanalyse van volgend jaar staat in december al weer geagendeerd.

2. Kernboodschap

<u>Status van openstaaande 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

Ieder van deze categorieën wordt met een eigen planning opgepakt, en van ieder wordt separaat de status beschreven. Het geheel aan acties van het RKC onderzoek zal zijn afgerond als ieder van deze drie categorieën is afgerond.

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

2019/311830 RKC Onderzoek / Implementatie beleid:
Het beleid is eind 2018 opnieuw vastgesteld. De benodigde capaciteit is inzichtelijk gemaakt, en een groei daarvan is in de begroting opgenomen. De gap-analyse is uitgevoerd, verbeteringen zijn gestart. Per half jaar wordt er uitgebreid gerapporteerd, en een onafhankelijke auditor geeft zijn kritische mening. Aan de RKC is voorgesteld om dit punt te sluiten. In afwachting van administratieve afhandeling staat dit punt nog open.

2019/311840 RKC Onderzoek / Kwetsbaarheden.
In het rapport zijn 15 technische kwetsbaarheden genoemd. Hiervan zijn 12 geheel verholpen, 3 zijn gevorderd maar nog niet helemaal afgerond.
Hackers worden structureel ingezet om de beveiliging te testen. Er is een applicatie aangeschaft waarmee iedere maand op kwetsbaarheden wordt gecontroleerd.

Eén onderwerp is doorgeschoven naar 2022 omdat een vervangingstraject van apparatuur randvoorwaardelijk is. Het hiermee verbonden risico is op andere manieren al verminderd. Het vervangen van de apparatuur staat in het eerste kwartaal van 2022 gepland.

Uitgebreidere informatie is te vinden in Bijlage A.

Voortgang van beveiligingsprioriteiten
Er is gestage voortgang. Uitgebreidere informatie is te vinden in Bijlage B (Geheim).

Voortgang van verbeterplannen DigiD en Suwinet
Bij een heraudit op 17 juni 2021 is door de externe auditor vastgesteld dat aan alle Suwinet normen wordt voldaan. Hiervoor is een assurance verklaring opgesteld die aan toezichthouder BKWI is verstrekt.

Voor DigiD werd aan één norm niet voldaan, waarvoor toezichthouder Logius tot 1 november respijt heeft gegeven. Bij de heraudit door de externe auditor is op 15 oktober vastgesteld dat *mijn.haarlem.nl* aan de norm voldoet, en dat *haarlem.nl* nog niet geheel aan de norm voldoet. Voor *haarlem.nl* is vastgesteld dat het risico op een andere manier wordt gemitigeerd, waardoor verlengd uitstel kan worden verleend. De assurance verklaringen zijn aan toezichthouder Logius verstrekt.

Er is gepland dat *haarlem.nl* in december 2021 aan de norm zal voldoen. Dit zal tijdens de geplande externe DigiD-audit van 2021 worden vastgesteld.

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

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

Het begint een “normaal” patroon te worden dat valse berichten worden ontvangen na een digitale inbraak bij een leverancier of partner. Ook via Zorgmail – een meer vertrouwd kanaal – zijn zulke berichten ontvangen. Voordien werden berichten via Zorgmail minder streng gecontroleerd, dat is nu gelijk getrokken met de controle van de mail via Internet.

Om weerbaarheid tegen linkjes / phishing te verhogen worden regelmatig phishingtests gedaan, vaak via E-mail en soms via SMS. Bij het nabespreken in werkoverleggen vertellen medewerkers hun verhaal. Wie erin trapt klikt meestal zonder er met de gedachten bij te zijn. Heel vaak weet de persoon direct bij de klik al dat hij of zij iets doms aan het doen is en kan dat dan op de automatisch getoonde instructiepagina direct nalezen.

Er is “Click Protection” geactiveerd waardoor een medewerker na de eerste keer klikken een tweede scherm krijgt waarin wordt gevraagd de link te controleren om daarna nogmaals te klikken. De gedachteloze klikker heeft dan de kans om er in tweede instantie alsnog niet in te trappen.

Er zijn geen aanwijzingen voor 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.

In september is de audit van 2021 uitgevoerd. Vergeleken met de audit van december 2020 is op 13 van de 20 beoordeelde gebieden de score verbeterd, op 7 gebieden is de score gelijk gebleven. Het volwassenheidsniveau is gestegen naar een ruime 2. Extra middelen en hard werken hebben resultaat gehad.

Voor de ISO 27001 ligt de lat hoog: ieder onderdeel moet niveau 3 zijn: herhaalbaar en van goede kwaliteit. De beschikbare mensen en middelen maken de ruime 2 mogelijk, maar de 3 zal niet structureel gehaald worden.

Over het ambitieniveau voor beveiliging wordt een passage opgenomen in de Factsheets die voor de verkiezingen worden voorbereid.

De aanbevelingen uit de audit zijn meegewogen bij de beveiligingsprioriteiten van 2022.

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

Geheimhouding
Op de bij deze nota behorende bijlagen A, B, C en D dient geheimhouding opgelegd te worden aan de commissie Bestuur op grond van artikel 86 van de Gemeentewet vanwege de bescherming van de

economische of financiële belangen van de gemeente alsmede het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden, als bedoeld in artikel 10, tweede lid, aanhef en onder b en g van de Wet Openbaarheid van Bestuur. De geheimhouding op bijlage A, C en D geldt voor onbepaalde tijd. De geheimhouding op bijlage B geldt voor een periode van een jaar en komt te vervallen op 1 december 2022.

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. Dit leidt tot onevenredige benadeling van de gemeente (artikel 10, tweede lid, onder g van de Wob en kan de financiële belangen van de gemeente (artikel 10, tweede lid, onder b van de Wob) schaden.

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 2022 zal nu worden uitgewerkt. De Commissie 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 2021 en prioriteiten 2022
Bijlage D GEHEIM - Volwassenheidsbepaling ISO 27001 Gemeente Haarlem