Gemeente Haarlem

# Informatienota

| | |
|---|---|
| **Onderwerp**<br>Stand van zaken informatiebeveiliging | |
| Nummer | 2020/465284 |
| Portefeuillehouder | Botter, J. |
| Programma/beleidsveld | 6.2 Gemeentelijk bestuur |
| Afdeling | CC |
| Auteur | Hut, F.J. |
| Telefoonnummer | 023-5114955 |
| Email | fhut@haarlem.nl |
| Kernboodschap | Er wordt gerapporteerd over de stand van zaken op het gebied van informatiebeveiliging:<br>• De status van openstaande punten gerelateerd aan het RKC onderzoek<br>• De voortgang van beveiligingsprioriteiten<br>• Voortgang van verbeterplannen DigiD en Suwinet<br>• Een analyse van Security incidenten<br><br>Aanpak en accenten zijn beïnvloed door de Corona-situatie. |
| Behandelvoorstel voor commissie | Het college stuurt de informatienota ter kennisname naar de commissie Bestuur.<br><br>Deze rapportage is toegezegd bij behandeling van de informatienota van november 2019 (2019/8557650) |
| Relevante eerdere besluiten | 2019/311846 RKC Onderzoek / Raadsinformatie<br>2019/311830 RKC Onderzoek / Implementatie beleid<br>2019/311840 RKC Onderzoek / Kwetsbaarheden<br>2019/355441 Motie 14.1 Integraal Risicomanagement<br>2019/940161 Afstemmen structuur van voortgangsrapportage<br>2019/970446 ENSIA beantwoording |
| Besluit College<br>d.d. 19 mei 2020 | 1. De informatienota vast te stellen.<br>2. Op de bij deze nota behorende bijlage B 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 en ter voorkoming van onevenredig benadeling van de gemeente, als bedoeld in artikel 10, tweede lid, aanhef en onder b en g van de Wet Openbaarheid van Bestuur. De geheimhouding wordt opgelegd voor onbepaalde duur.<br><br>de secretaris, de burgemeester, |

**1. Inleiding**

Volgens afspraak wordt hierbij gerapporteerd over de stand van zaken op het gebied van informatiebeveiliging.

Achtereenvolgens wordt ingegaan op:
- De status van openstaande punten;
- De voortgang van beveiligingsprioriteiten;
- Voortgang van verbeterplannen DigiD en Suwinet;
- Een analyse van Security incidenten.

**2. Kernboodschap**

<u>Status van openstaande punten gerelateerd aan het RKC onderzoek</u>
*Afhandeling van RKC aanbevelingen verloopt volgens planning*

De aanbevelingen van het RKC Onderzoek informatiebeveiliging bestaan uit de volgende onderdelen:
2019/311846 RKC Onderzoek / Raadsinformatie
2019/311830 RKC Onderzoek / Implementatie beleid
2019/311840 RKC Onderzoek / Kwetsbaarheden

In de commissie van 12 maart 2020 is voor de afdoening onderstaande planning gegeven die nog steeds geldt. Hier zal te zijner tijd het formele proces via de RKC worden gevolgd.

| Nr | Gepland gereed | Opmerkingen met updates |
|---|---|---|
| **2019/311846** | November 2020 | |
| Sub a | Mei 2020 | Update 8 mei 2020: Duiding en samenvatting is op 12 juni 2020 geagendeerd |
| Sub b | November 2020 | Volwassenheid komt als onderwerp in de rapportage. |
| **2019/311840** | September 2020 | |
| Sub a | September 2020 | Any lost nog aantal punten op. Nazorg van project Any is afgerond. |
| Sub b | September 2020 | Structureel meten van kwetsbaarheden kan worden aangetoond. |
| **2019/311830** | | |
| Sub a | Mei 2020 | Update 8 mei 2020: De detailantwoorden van de BIG zelfevaluatie zijn op 12 juni 2020 geagendeerd. |
| Sub b | December 2018 | Beleid is vastgesteld. |
| Sub c | | Update 8 mei 2020: Scenariokeuze is ingebracht in proces van kadernota. |
| Sub d | | Plan is afhankelijk van scenariokeuze uit c. |
| Sub e | November 2020 | Update 8 mei 2020: Een voorstel voor de rapportages is onderdeel van deze nota. Na de tweede halfjaar rapportage moet dit punt in november 2020 kunnen worden afgedaan. |

*Motie 14.1 Integraal Risicomanagement is ingevuld*
Bij de bespreking van het rapport is de volgende motie ingediend:
2019/355441 Motie 14.1 Integraal Risicomanagement

In de informatienota van november 2019 (2019/8557650) zijn de informatiebeveiligingsrisico's benoemd. Bij de begroting van 2020 zijn deze risico's in het register opgenomen en zijn kans en impact ook in het berekende weerstandsvermogen verwerkt. Hiermee is aan de strekking van deze motie voldaan.

*Voor de inhoud van de halfjaarlijkse rapportage wordt een voorstel gedaan*
Bij de bespreking van de informatienota in november 2019 is de volgende toezegging gedaan:
2019/940161 Afstemmen structuur van voortgangsrapportage

In bijlage A is het voorstel uitgewerkt voor de inhoud van halfjaarlijkse rapportages in juni en november.

<u>Voortgang van de beveiligingsprioriteiten</u>
*Er zijn veel voorbereidingen getroffen waarvan de resultaten de komende periode kunnen worden geïncasseerd. De Corona-situatie heeft impact op het proces.*

Het afgelopen half jaar is ook vanuit het perspectief van informatiebeveiliging hectisch geweest. De Citrix escalatie heeft in januari alle aandacht opgeëist, en vanaf maart bepaalt het Corona virus een belangrijk deel van de agenda. In maart zijn Security Awareness bijeenkomsten gecanceld.

Er is een verschuiving geweest naar massaal thuiswerken (ook) vanaf privé apparaten. Digitaal vergaderen is de norm geworden. Migratie naar de Any werkplek en invoering van Microsoft Teams zijn onder hoge druk in heel korte tijd gedaan.

Haarlem heeft primair gekozen voor Teams als samenwerkingsplatform, maar iedere organisatie buiten Haarlem maakt eigen keuzes. Het effect is dat veel medewerkers naast Teams ook samenwerken via applicaties als Whatsapp, Skype, Zoom, Facetime, Google, Jitsi en waarschijnlijk nog veel anderen.

Deze andere en meer digitale manieren van werken kent nieuwe risico's en afwegingen waar informatiebeveiliging direct bij is betrokken. Hiervoor is niet-urgent werk zoals het schrijven van nota's opgeschoven.

Onderdeel van goede beveiliging – dit zit ook in de beveiligingsprioriteiten – is dat mensen alleen goed gecontroleerd worden toegelaten en dat ze bij afwijkingen vlot worden geblokkeerd. Hierbij is onvermijdelijk dat gemak verandert en een gedeelte van de mensen soms ten onrechte niet wordt toegelaten of ten onrechte wordt geblokkeerd. Zo iemand gaat normaal gesproken naar kantoor om daar te werken en/of meldt zich bij de Servicedesk en wordt daar verder geholpen.

De Corona situatie maakt het aanscherpen van beveiliging lastiger, waardoor bij implementatie een voorzichtiger aanpak moet worden gevolgd:

- Het is voor veel mensen geen optie om naar kantoor te komen. Als iemand via Internet niet binnenkomt, dan kan hij of zij niet werken.
- De stress hiervan wordt toegevoegd aan alle spanning die Corona reeds geeft op de privé situatie en op het werk.
- Terwijl beheerders en Servicedesk te weinig gelegenheid hebben om dan direct te ondersteunen omdat zij al maximaal zijn belast.

In de informatienota van november 2019 (2019/8557650) bijlage I (2019/870069) zijn prioriteiten benoemd. In geheime bijlage B staat per onderdeel de status.

In bijlage B staat informatie die voor criminelen direct bruikbaar is. Ter bescherming van de economische en financiële belangen van de gemeente alsmede om een onevenredige benadeling van de gemeente te voorkomen wordt op deze bijlage geheim opgelegd. Vanwege de aard van de informatie wordt geheimhouding opgelegd voor onbepaalde duur.

Voortgang van verbeterplannen DigiD en Suwinet
*Alle punten zijn gereed gemeld. Een hertest door de externe auditor wordt gepland.*

Analyse van Security incidenten
*Het moet makkelijker gemaakt worden om Security incidenten te melden. Uit incidenten die zijn onderzocht is niet gebleken dat Haarlem slachtoffer is geweest van computer criminaliteit. Kwetsbaarheden bij anderen kunnen invloed hebben op Haarlem.*

Er komen weinig meldingen van de eindgebruikers. Hierop worden twee acties genomen:

- Duidelijker maken van het proces om te melden, dit is onderhanden.
- Vervolgens hieraan aandacht besteden in communicatie.

De volgende incidenten hebben specifieke aandacht gekregen:

- In december / januari speelde de Citrix kwetsbaarheid waardoor verbindingen via Citrix ook door Haarlem uitgeschakeld zijn geweest. Er is adequaat gehandeld, de systemen van Haarlem zijn een aantal keren door externe specialisten beoordeeld, er is geen aanwijzing dat onbevoegden toegang hebben gehad. De beperkte omvang van de beheerorganisatie is bij zo'n escalatie een risico, omdat niet 100% gegarandeerd kan worden dat ieder specialisme altijd aanwezig is. Mede naar aanleiding hiervan is een contacten netwerk opgezet waarin vrijwel alle gemeentelijke CISO's van Noord Holland elkaar makkelijk vinden.
- Regelmatig blijven berichten binnenkomen die medewerkers verleiden om hun gegevens op te geven of om op linkjes te klikken. Als een medewerker zijn of haar gegevens heeft ingevoerd dan worden wachtwoorden veranderd. In één geval zijn werkplekken afgekoppeld en heeft een extern deskundige deze onderzocht. Hierbij zijn geen sporen van computercriminaliteit aangetroffen.
  Met Multi-Factor authenticatie wordt de impact van uitgelekte wachtwoorden veel kleiner. Het klikken op ongevraagde berichten en linkjes zal altijd een risico blijven, zeker in processen waar

ongevraagde berichten veel voorkomen (bv aanvraag vergunning, sollicitatie, bezwaar, klacht, factuur). Security Awareness gaat hieraan aandacht besteden.

- Er is een valse factuur gestuurd nadat hackers toegang hadden tot de systemen van een leverancier van de gemeente. De rekening is niet betaald. Procedures voor het wijzigen van rekeningnummers zijn aangescherpt. Informatie is gedeeld met de politie.
  Het gebeurt vaker dat hackers in systemen van een relatie binnendringen en dan in staat zijn om berichten te sturen. Zulke berichten zijn voor Haarlem op geen enkele manier van echt te onderscheiden. Oplettendheid is dan geboden en intuïtie (“dit is vreemd”) is vaak een goede raadgever.

**3. Consequenties**
Voor het verbeteren van de beveiliging komt na voorbereidingen de fase waarin wordt gerealiseerd. Daarmee worden risico’s dan ook daadwerkelijk gemitigeerd.

Alle geagendeerde onderwerpen krijgen en houden aandacht.

**4. Vervolg**
In november 2020 wordt opnieuw over de voortgang gerapporteerd. Geïdentificeerde risico’s zullen worden meegenomen in het begrotingsproces. Prioriteiten voor 2021 zullen worden voorgesteld.

Bij de behandeling van de begroting zal ook informatiebeveiliging aan de orde komen. De beschikbare menskracht en middelen hebben een direct verband met de realisatiekracht en daarmee met de haalbare ambitie.

**5. Bijlagen**
Bijlage A - Voorgestelde inhoud van halfjaarlijkse rapportages
Bijlage B GEHEIM - Status van prioriteiten