Gemeente Haarlem

Informatienota

Onderwerp Rapportage informatiebeveiliging najaar 2020	
Nummer	2020/948418
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. 17 november 2020	1. Het college stelt de informatienota aan de commissie vast. 2. Op de bij deze nota behorende bijlagen A, B en C 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

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

Op ieder van deze onderwerpen wordt hieronder ingegaan, nadat eerst kort is aangegeven welke impact Corona op dit onderwerp heeft gehad.

2. Kernboodschap

<u>Corona – impact</u>
Met Corona wordt op grote schaal vanaf thuis gewerkt. Hierbij wordt gebruik gemaakt van een Virtuele Desktop die door project Any is opgeleverd. Hierbij gebeurt het feitelijke werk op systemen in een datacenter, waarbij de thuiscomputer zorgt voor beeldscherm, toetsenbord en muis op afstand. Hierdoor worden de systemen van de gemeente geïsoleerd van veel risico's van de thuiscomputers.

Het thuiswerken gebeurt op een schaal die vooraf niet was bedacht, waardoor op verschillende gebieden problemen moesten worden opgelost. De afdeling IV heeft aan het thuiswerken prioriteit gegeven, waardoor ander werk – waaronder ook Security – in de tijd is opgeschoven.

Met het aanscherpen van Security maatregelen kan en zal het effect zijn dat sommige mensen niet meer kunnen werken op de manier die ze gewend zijn. Vanaf thuis is het minder makkelijk om dan ondersteund te worden door de combinatie van grote drukte bij de IV Servicedesk en het feit dat je voor sommige zaken fysiek langs zou moeten komen. Er is daarom gekozen voor een rustige aanpak om zulke problemen hanteerbaar te houden.

<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 in een eigen ritme 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:
Met de afgesproken rapportagecyclus (waarvan ook deze informatienota onderdeel is) wordt aan de opdracht voldaan. Na het delen van de conclusies van de ISO 27001 audit van december 2020 is een hele cyclus afgerond en zal worden voorgesteld om dit punt te sluiten.

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.

2019/311840 RKC Onderzoek / Kwetsbaarheden
In het rapport zijn 15 technische kwetsbaarheden genoemd. Hiervan zijn 11 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 bewust doorgeschoven naar 2021 in verband met de volgende risico inschatting:

- Een crimineel moet eerst contact met systemen kunnen maken
- Om daarna een kwetsbaarheid in die systemen te vinden waarvan gebruik gemaakt kan worden.

Eerste prioriteit is gegeven aan (1) het beveiligen van contact vanaf internet en (2) het verhelpen van kwetsbaarheden in systemen. Het doorgeschoven punt heeft betrekking op het netwerk binnen de gebouwen. Dit is een veel kleiner risico dan toegang vanaf internet, en ook de aanvaller vanuit een kantoor maakt minder kans omdat kwetsbaarheden in systemen worden verholpen.

Uitgebreidere informatie is te vinden in Bijlage A.

<u>Voortgang van beveiligingsprioriteiten</u>
Het massaal thuiswerken door Corona en Project Any hebben de gang van zaken sterk beïnvloed, zoals eerder al is beschreven. Binnen deze beperkingen is op een aantal onderwerpen goede voortgang gerealiseerd, en gaat het tempo omhoog nu de medewerkers van project Any weer beschikbaar zijn.

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

Voortgang van verbeterplannen DigiD en Suwinet
In de Commissievergadering van 11 juni 2020 is reeds gemeld dat de externe auditor heeft vastgesteld dat aan alle Suwinet normen wordt voldaan. De verklaring van de auditor is opgestuurd naar toezichthouder BKWI.

Op 30 juli 2020 heeft de externe auditor vastgesteld dat aan alle DigiD normen wordt voldaan. De verklaring van de auditor is opgestuurd naar toezichthouder Logius.

Analyse van Security incidenten
Het aantal geregistreerde incidenten is laag. De meldprocedure moet bekender en laagdrempeliger worden, en mensen moeten worden aangespoord om een melding te doen. Dit is een aandachtspunt voor 2021.

De geregistreerde incidenten gaan vooral over onderwerpen als:

- Een verloren of gestolen mobiel apparaat.
- Het uitlekken van een wachtwoord waarna een onbekende de E-mail gebruikt.
- Het klikken op een onbetrouwbaar linkje.

Bij de risico analyse zijn ook deze scenario's meegenomen.

Er zijn geen aanwijzingen voor ernstiger 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 juli 2020 is een pre-audit uitgevoerd, in de eerste week van december 2020 zal de audit worden gedaan. Als resultaten hiervan beschikbaar zijn dan zullen deze met de commissie worden gedeeld.

3. Consequenties
--

4. Vervolg
Het beveiligingsplan voor 2021 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 2020