Gemeente Haarlem

Informatienota

Onderwerp Stand van zaken Informatiebeveiliging	
Nummer	2019/855753
Portefeuillehouder	Botter, J.
Programma/beleidsveld	6.2 Gemeentelijk Bestuur
Afdeling	CC
Auteur	Hut, F.J.
Telefoonnummer	023-5114955
Email	fhut@haarlem.nl
Kernboodschap	Begin 2019 heeft de Rekenkamer Commissie een rapport uitgebracht over Informatiebeveiliging. Op 1 april 2019 is er een Chief Information Security Officer (CISO) gestart bij de gemeente. In een vorige informatienota is toegezegd om de analyse van CISO over het niveau van informatiebeveiliging van de gemeente Haarlem te delen met de commissie. De nota beschrijft de stappen die worden gezet om informatiebeveiliging op een goed niveau te krijgen.
Behandelvoorstel voor commissie	Het college stuurt de informatienota ter bespreking naar de commissie Bestuur In de eerdere informatienota “Opvolging RKC aanbevelingen Informatiebeveiliging (kenmerk 2019/465158) is toegezegd om een analyse van de informatiebeveiliging met de raadscommissie te delen. Met deze Informatienota geeft het college uitvoering aan motie 14.1 “ICT behoeft integraal risicomanagement” (kenmerk 2019/355441)
Relevante eerdere besluiten	Informatienota “Opvolging RKC aanbevelingen Informatiebeveiliging” (2019/465158)
Besluit College d.d. 29 oktober 2019	Het college besluit: 1. De informatienota aan de commissie vast te stellen 2. Op de bij deze nota behorende bijlagen D, G, H en I 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 informatienota kent verschillende aanleidingen. Begin 2019 heeft de Rekenkamer Commissie een rapport uitgebracht over informatiebeveiliging (“Verantwoordelijkheid voor Veiligheid” met kenmerk 2019/143523) Dit rapport heeft het onderwerp hoog op de agenda gezet en adviseert om de processen zoals genoemd in het informatiebeveiligingsbeleid uit te gaan voeren. Met de reactie op het rekenkamerrapport en een informatienota over dit onderwerp heeft het college de commissie geïnformeerd over de voortgang. Deze nota behandelt daarmee onderdelen van aanbevelingen van de RKC, maar is nog niet bedoeld als formele afhandeling daarvan. Hiervoor wordt een separate nota opgesteld waarover de RKC via het afgesproken proces vooraf adviseert.

Daarnaast is op 1 april 2019 de Chief Information Security Officer (CISO) gestart. De CISO is direct aan de slag gegaan met de aanbevelingen uit het RKC-rapport. In de informatienota (kenmerk 2019/465158) waarin het college de commissie heeft geïnformeerd over de stand van zaken van de opvolging van de aanbevelingen is toegezegd om de analyse van de CISO met de raadscommissie te delen.

Bij behandeling van het RKC-rapport is specifiek ingegaan op risicomanagement en over dit onderwerp is een motie aangenomen (motie 14.1 omtrent risicomanagement voor ICT met kenmerk 2019/355441)

Deze nota en de bijlagen geeft inzicht in de huidige situatie, de risico’s, het plan, de aansturing en de rapportage over de voortgang. De nota laat zien dat er een managementsysteem wordt ingericht waardoor het onderwerp van informatiebeveiliging continu op de agenda blijft staan en in control wordt gebracht.

De informatienota is zelfstandig leesbaar, voor wie dieper inzicht wil is een groot aantal vrij technische bijlagen toegevoegd. De bijlagen **D, G, H** en **I** geven inzicht in bestaande kwetsbaarheden. Openbaarmaking daarvan kan Haarlem direct schade berokkenen. Daarom zijn deze 4 bijlagen door het college geheim verklaard op grond van art. 86, tweede lid Gemeentewet juncto art. 10, tweede lid, sub b, Wob.

2. Kernboodschap
Bij de behandeling van het RKC rapport is aanvankelijk door het college gereageerd vanuit de perceptie dat alleen een aantal punten moest worden opgelost. Dit was dan ook de kern van de reactie van het college op het RKC rapport. De nieuwe CISO is vlak na publicatie en behandeling van het RKC rapport gestart. De CISO heeft de stand van zaken grondig beoordeeld en is tot de conclusie gekomen dat er veel meer moet gebeuren. Toen dit duidelijk werd is dit op 5 september bij de mededelingen gemeld aan de commissie Bestuur en is naar deze toegezegde informatienota verwezen.

Haarlem loopt op dit moment een flink risico. Het meest sombere scenario is een ransomware aanval die alle ICT uitschakelt waarna het geruime tijd duurt voordat weer gewerkt kan worden. De kans op zoiets is groter dan werd gedacht, hiervoor zijn voldoende voorbeelden in de wereld te vinden (zie bijlage C voor voorbeelden).

Op basis van de uitgevoerde risico analyse is bepaald wat nodig is om risico's te verminderen en om structureel "in control" te komen. Duidelijk is dat er gedurende meerdere jaren werk zal zijn om een professioneel niveau van informatiebeveiliging te bereiken. Technische maatregelen zijn nog vrij makkelijk te implementeren, de kunst is om de aandacht continu vast te blijven houden en om alle mensen in de organisatie risicobewust te maken.

In het plan voor 2020 krijgen de grote risico's prioriteit. Speerpunten zijn gericht op alle relevante perspectieven: Organisatie, Mensen en Techniek.

De volgende bedragen zijn op dit moment toegekend (2019) en opgenomen in de begroting (2020)

	2019	2020	
Kadernota 2019	200.000	200.000	
Begroting 2020		230.000	Voor specifiek benoemde Privacy onderwerpen
Capaciteit toekenning		160.000	

In de kadernota 2020 zullen extra middelen worden gevraagd als de situatie daartoe aanleiding geeft.

De algemeen gebruikte ISO 27001 norm voor Informatiebeveiliging is als referentiekader gebruikt. Van deze ISO norm zijn ook de Baseline Informatiebeveiliging Gemeenten (BIG) en Baseline Informatiebeveiliging Overheid (BIO) afgeleid.

3. Consequenties

In de analyse is eerst stilgestaan bij de zogenaamde kroonjuwelen. Wat beschermen we, waarom, en hoeveel bescherming is nodig? Duidelijk is dat informatie van de gemeente groot belang heeft voor burgers, en dat goede bescherming verwacht mag worden. Betrouwbaarheid van informatie is eigenlijk altijd belangrijk. Vertrouwelijkheid van informatie heeft vaak te maken met persoonsgegevens. Beschikbaarheid van informatie is nodig om de maatschappelijke rol van de gemeente in te kunnen vullen.

Je beschermt tegen bedreigingen. Gebaseerd op dreigingsbeelden, nieuwsberichten en actuele incidenten is bepaald wat de meest relevante bedreigingen zijn waartegen Haarlem zich moet beschermen. In hoofdlijnen komt dit neer op malware, menselijke vergissingen en menselijk gedrag, gerichte acties van onbekenden en onvoldoende beveiliging van leveranciers.

De huidige bescherming is beoordeeld vanuit twee perspectieven:

- Hoe wordt beveiliging gemanaged?

- Welke maatregelen zijn er getroffen?

Het managen van beveiliging kan nog flink verbeteren. De bijlagen bij deze nota laten zien dat hiermee al een flinke start wordt gemaakt. Er was al beleid, hieraan is toegevoegd dat we weten wat we beveiligen en waarom, er is een risico analyse uitgevoerd, vanuit de risico analyse zijn prioriteiten gesteld voor het komende jaar, de sturing en rapportage zijn vastgesteld en er is menskracht en geld beschikbaar gesteld.

Getroffen maatregelen zijn er op dit moment vooral op gericht om te voorkomen dat een aanvaller via Internet van buiten naar binnen kan komen. Tot nu toe is dat behoorlijk effectief, de harde schil aan de buitenkant houdt veel tegen alleen moet je er altijd rekening mee houden dat een aanvaller toch binnen komt. Maar voor dit scenario zijn niet of nauwelijks maatregelen getroffen. Er moeten daarom maatregelen getroffen worden om de “binnenkant” te versterken. Het is noodzakelijk om te kunnen Detecteren (als het toch iemand binnen is gekomen), om te Reageren (op de detectie) en daarna te Herstellen (van de veilige situatie).

De grootste risico’s van dit moment liggen bij scenario’s die te maken hebben met:
- Malware – en dan speciaal de gerichte aanval met ransomware.
- Het overnemen van accounts.
- Insluipers met kennis van zaken.

Wat opvalt in de risicoanalyse is dat veel risico’s hun belangrijkste impact hebben in de dimensie van Imago en Reputatie (bijlage E), terwijl het Risico Management van de gemeente vooral gericht is op de Financiële dimensie. De onderlinge weging van zulke heel verschillende risico’s (een kort artikel in het Haarlems Dagblad heeft impact 3, een stuk op nu.nl heeft impact 4 of 5, een verlies van € 150.000 heeft impact 2) wordt als onderwerp op een ander niveau geagendeerd.

Mogelijke beheersmaatregelen tegen de risico’s zijn benoemd in bijlage H (geheime bijlage). Op basis van de risico’s zijn prioriteiten benoemd voor het eerste jaar, die worden opgepakt zoals onder kopje vervolg staat beschreven.

Een incident bij Gemeente Haarlemmermeer is recent in het nieuws geweest en ook door de gemeente op haar eigen website gepubliceerd. Na phishing is een E-mail account door een onbekende overgenomen waarna data is gelekt. Met de CISO van Haarlemmermeer is informatie uitgewisseld. Iets van dezelfde orde had ook in Haarlem kunnen gebeuren, vastgesteld is dat alle relevante elementen om dit te voorkomen staan in de prioriteiten van het beveiligingsplan. Ook met de IBD (Informatiebeveiligingsdienst van VNG) is contact en worden geleerde lessen vanuit andere gemeenten gedeeld. Onze prioriteiten zijn ook vanuit die optiek verstandig.

4. Vervolg

Op basis van deze uitgevoerde analyse wordt gestart met de uitvoering van het beveiligingsplan. Hiermee worden de risico’s gereduceerd.

De prioriteiten voor het eerste jaar zijn als volgt
- De organisatie op drie manieren:

- Door eigenaarschap concreet te maken worden verantwoordelijkheden duidelijk.
- Door rapportages kan er beter worden gestuurd.
- Door aanvullend beleid en handhaving daarvan krijgt risicobewustzijn een prominentere plek in de organisatie. Het beleid zal o.a. grenzen stellen aan gebruiksgemak als leidend principe.

- De mens. Er wordt aan Security Awareness gewerkt.
- De techniek. In het eigen beheer worden puntjes op de i gezet, en er worden aanvullende beveiligingsdiensten ingekocht.

Over de voortgang van de uitvoering van het beveiligingsplan wordt tweemaal per jaar aan de gemeenteraad gerapporteerd.

5. Bijlagen

Bij de behandeling van het RKC-rapport zijn veel inhoudelijke suggesties gedaan, en er is een motie over risicomanagement ingediend en aangenomen. Als achtergrondinformatie wordt in de bijlagen in meer detail ingegaan op de tussenresultaten van het analyseproces, zodat kan worden vastgesteld dat de gevraagde punten zijn opgepakt.

Bijlage A – Wat beschermen we, waarom, hoeveel bescherming is nodig
Bijlage B – Eerdere inventarisatie door de Informatiebeveiligingsdienst van VNG
Bijlage C – Relevante bedreigingen die in de analyse zijn betrokken
Bijlage D – Beoordeling van de huidige beveiliging **Geheim**
Bijlage E – Risicoscenario's met kans en impact
Bijlage F – Gehanteerde structuur voor kans en impact
Bijlage G – Uitgebreide uitwerking van risicoscenario's **Geheim**
Bijlage H – Mogelijke beheersmaatregelen tegen gesignaleerde risico's **Geheim**
Bijlage I – Prioriteiten voor het Beveiligingsplan **Geheim**
Bijlage J – Aanpak en aansturing van de uitvoering van het Beveiligingsplan