

Informatienota raad

Zaaknummer: Z-22-422517
Nummer: DOC-22-579908
Datum: 25-8-2022
Steller: College
Onderwerp: Borgen Informatieveiligheid

Ter informatie

Kennis nemen van:

Borgen Informatieveiligheid en Rapport Rekenkamercommissie.

Aanleiding

In opdracht van de rekenkamercommissie van Medemblik en Opmeer (hierna RKC) is in het eerste kwartaal van 2022 door een extern bureau onderzoek gedaan naar de informatiebeveiliging van beide gemeenten. Het college heeft het conceptonderzoeksrapport van de RKC en de daarbij behorende Nota van Bevindingen op 19 mei jl. ontvangen. Uit het conceptrapport bleek dat de informatieveiligheid op verschillende punten zorgelijk te noemen was. Hoewel het slechts een conceptrapport betrof en het definitieve rapport nog in een later stadium aan het college en de raad zou worden voorgelegd, achtte het college de genoemde punten van dien aard dat zij bij collegebesluit van 7 juni jl. hebben besloten om, vooruitlopend op het definitieve rapport, alvast diverse maatregelen te treffen.

Omdat het conceptrapport en de Nota van bevindingen door de RKC geheim waren verklaard, kon het college die informatie en het daaropvolgende collegebesluit over de genomen maatregelen niet met de raad delen. De geheimhouding was noodzakelijk, we wilden immers kwaadwillenden niet in de gelegenheid stellen misbruik te maken van de situatie. Wel heeft de burgemeester de fractievoorzitters vertrouwelijk geïnformeerd.

De RKC heeft met een persbericht de bevindingen uit hun rapport openbaar gemaakt. Om die reden kan (en moet in het kader van de wet open overheid) de geheimhouding op het collegebesluit en het daarbij behorende collegeadvies ook worden opgeheven. Het college in dat kader op 30 augustus 2022 besloten om de geheimhouding op een collegeadvies en -besluit van 7 juni en 5 juli 2022 op te heffen direct na de publicatie door de RKC. Die openbaarmaking heeft inmiddels plaatsgevonden. Hierdoor kan het college nu ook de raad informeren over de reeds getroffen en de nog te treffen maatregelen.

Met deze raadsinformatiebrief informeert het college de raad over de maatregelen die zijn getroffen naar aanleiding van het rapport van de RKC over Informatieveiligheid.

Kernboodschap

In opdracht van de RKC van Medemblik is een onderzoek inclusief pen-test (een test om te kijken hoever men de organisatie kan binnendringen) gedaan. Uit dit conceptrapport dat we op 19 mei ontvingen blijkt dat de informatieveiligheid op verschillende punten zorgelijk te noemen is.

Collegebesluit 7 juni 2022

Het college heeft het rapport op 7 juni besproken. Het onderzoek naar de organisatie van de informatiebeveiliging had tot doel om na te gaan of gemeente Medemblik de belangrijkste risico's in beeld heeft, hoe het beleid is opgesteld en of dit in de praktijk wordt toegepast. Het college is blij met dit uitgebreide en zorgvuldig opgestelde rapport. Het biedt goede inzichten en legt de vinger op een zere plek. Hierdoor biedt het ons de kans om deze zorgelijk gebleken punten op te lossen voordat er problemen ontstaan. Het college heeft besloten om de gemeentesecretaris opdracht te geven om direct alle noodzakelijke maatregelen te treffen waarbij ook middelen zijn toegekend. Waarbij het beoogd resultaat is om de informatievoorziening en de informatieveiligheid op een robuust niveau te brengen zodat de gemeente Medemblik in staat is de continuïteit van haar dienstverlening te borgen, alsook de integriteit en vertrouwelijkheid van gegevens van burgers, bedrijven en het gemeentelijk apparaat.

In de bestuurlijke reactie aan de RKC meldt het college dit ook. In die brief staat onder meer:

'De aanbevelingen van de Rekenkamercommissie zijn duidelijk, concreet en uitvoerbaar. Ze bieden ons duidelijke handvatten om de geschetste problematiek daadkrachtig aan te pakken. Het college omarmt het advies en heeft inmiddels maatregelen ingang gezet om de informatieveiligheid te verbeteren inclusief beschikbaar stellen van middelen die hiervoor nodig zijn.'

Het rapport

De weerbaarheid van de overheid is afgelopen jaren een groeiend thema geworden bij alle overheidsorganisaties. Dat geldt ook voor Medemblik. Het college acht het daarom noodzakelijk om ook in onze gemeente de benodigde stappen te zetten tegen cybercriminaliteit en ander misbruik van gevoelige gegevens.

Uit de pen-test en het daaruit volgende rapport is naar voren gekomen dat zowel in de uitvoering, de toegekende budgetten als in de formatieve omvang de gemeente tekortschiet. Het verdient naar mening van het college aanbeveling om alle geadviseerde maatregelen over te nemen.

Om de genoemde problemen en risico's gelijk zoveel mogelijk te mitigeren zijn er al verschillende maatregelen ondernomen en is in kaart gebracht welke verdere acties we zullen moeten nemen. Hieronder worden enkele al ondernomen acties en maatregelen beschreven. Daarmee zetten we de eerste stappen in de goede richting maar we beseffen dat we er nog niet zijn. Conform het advies van de RKC zullen we dit structureel evalueren en monitoren.

Reeds genomen maatregelen

Samen met SSC DeSom

Zoals uit het onderzoek blijkt, ligt een deel van de verantwoordelijkheid bij DeSom en een deel bij de eigen organisatie. Voor een spoedige en goede oplossing van de geconstateerde problemen zal een goede samenwerking met DeSom noodzakelijk zijn. Partijen zijn zich hier goed van bewust. In samenspraak met de andere gemeenten en DeSom is om die reden gelijk een bureau ingeschakeld dat een nadere analyse van het RKC-rapport heeft gemaakt en dat een concreet Plan van aanpak voor een Parapluplan heeft opgesteld om de gezamenlijke problemen te adresseren.

Interne maatregelen

1. Werven Ciso en Iso

Voor een structurele oplossing moeten we een Chief Information Security Officer en Information Security Officer aantrekken. Op dit moment heeft Medemblik formatief 0,44 fte Iso. Dit zou minimaal 1 fte Iso en 1

fte Ciso moeten zijn. Bovendien is de medewerker die deze functie vervulde recent van werkgever gewisseld. Het college op 7 juni jl. besloten om vooruitlopend op de begroting, opdracht te geven voor onmiddellijke werving van 1 fte Ciso en 1 fte Iso.

2. *Externe inhuur Ciso en Iso*

Gezien de krappe arbeidsmarkt en de specialistische taak, verwachten we deze vacatures niet gelijk ingevuld te krijgen. Om die reden is de benodigde kennis en capaciteit extern ingehuurd. Aan het ingehuurd bureau is, naast het uitvoeren van diverse andere taken zoals Ensia en actualisering beleid, onder meer de opdracht gegeven om volop in te zetten op structurele verbeteringen, zoals de inrichting van het controleproces gericht op de naleving van het nog te actualiseren beleid.

3. *Herpositionering I-taken*

Naast de werving voor een Ciso en Iso, is ook gestart met de herpositionering van de I-taken. Door een wijziging in de organisatiestructuur verwachten we een verbetering in de samenwerking en in de integraliteit van de aanpak. Een voorstel hiertoe, onderdeel van een organisatiebrede wijziging, ligt op dit moment bij de OR.

4. *Fysieke toegang*

Ten aanzien van de gemelde issues met betrekking tot de fysieke toegang van het gebouw, volgt op korte termijn voorstel om de toegangsbeveiliging van het gebouw op korte termijn aan te passen. Verder wordt dit meegenomen in het Plan van aanpak voor de toekomstbestendige huisvesting dat momenteel in ontwikkeling is.

5. *Bewustwording*

Wellicht wel een van de belangrijkste punten maar ook misschien wel de meest complexe, is de menselijke factor. We zetten veel actie in op bewustwording, bij de medewerkers, maar ook bij het bestuur. Dit varieert van de inrichting en controle op de naleving op het beleid tot E-learnings en meer bewustwordingsacties.

Financiën

Met de werving van een Ciso en Iso, en de inhuur van externe deskundigheid nemen we een eerste stap richting relevante maatregelen. Het huidige team Informatie Management is door het collegebesluit van 7 juni jl. uitgebreid met 1,55 fte. Hiervoor is nu geen dekking maar de huidige situatie vraagt wel om directe invulling.

In de huidige arbeidsmarkt zal directe invulling niet mogelijk zijn en daarom is inhuur noodzakelijk. De kosten daarvoor worden in de herfstnota 2022 meegenomen worden. Het college zal in de begroting 2023 voorstellen om deze kosten structureel mee te nemen.

Kosten nog niet in conceptbegroting

De verwachting is dat er naast de structurele (formatieve) kosten voor de Ciso en Iso, nog aanvullende kosten gemaakt moeten worden om geheel aan de aanbevelingen van de RKC te voldoen. Deels zullen die kosten in de begroting 2023 worden voorgesteld, zoals bijvoorbeeld de uitbreiding van de capaciteit voor privacy taken en de benodigde middelen voor de door het onderzoeksbureau aangetroffen verouderde applicaties. Maar we verwachten dat er nog meer kosten zullen zijn. Kosten waar we pas goed zicht op krijgen als ingehuurd externen hun Plan van aanpak gereed hebben (medio Q4 22). Ditzelfde geldt voor de punten die DeSom zelfstandig of in samenspraak met Medemblik moet oppakken en oplossen (Parapluplan). In hoeverre dat

kosten met zich meebrengt is vooralsnog onduidelijk, dit zal in de risicoparagraaf van de conceptbegroting worden opgenomen.

Consequenties

Kort en goed, het college herkent en erkent de in het rapport geschetste zorgpunten. Veel van de geconstateerde problemen zijn te herleiden naar een gebrek aan awareness. Dit is niet met louter geld op te lossen. Awareness begint met het (h)erkennen van de urgentie en het onderkennen van de eigen tekortkomingen. Hierop maar ook op de andere geconstateerde gebreken, zal geïnvesteerd moeten worden. In dat kader zijn de eerste en belangrijkste maatregelen getroffen maar we zijn er nog niet. Tegelijkertijd zal naar de aard van de informatie en systemen, een 100% garantie op veiligheid helaas nooit te geven zijn.

Communicatie

De RKC heeft op 7 september jl de raad geïnformeerd en op 8 september een persbericht verstuurd. Op 15 september as wordt het rapport door de RKC aan de raad gepresenteerd.

Vervolg

De raad krijgt op 15 september het rapport door de RKC gepresenteerd. Vervolgens kan de raad besluiten het rapport te laten agenderen.

Bijlagen