RAADSVERGADERING d.d. 29 september 2022

Zaaknummer	Z-22-419249
Voorstelnummer	DOC-22-568593
Onderwerp	Rapport Rekenkamercommissie Informatieveiligheid
Agendapunt	
Portefeuillehouder(s)	G. Gringhuis
Afdelingshoofd(en)	

Besluit

De raad van de gemeente Medemblik,

gelezen het bijbehorend voorstel ‘Rapportage Informatieveiligheid’ van de Rekenkamercommissie Medemblik-Opmeer d.d. 30 augustus 2022;

gelet op artikel 185 van de Gemeentewet;

overwegende dat de rekenkamercommissie aan de raad rapporteert;

b e s l u i t

1. Kennis te nemen van het rekenkamerrapport informatieveiligheid, de conclusies ervan over te nemen en de aanbevelingen vast te stellen;
2. Het college op te dragen
   a. nog in 2022 een beleidskader voor informatiebeveiliging op te stellen dat voldoet aan de BIO en ter besluitvorming voor te leggen aan de gemeenteraad;
   b. tenminste een keer per jaar de gemeentelijke informatiebeveiliging door een externe partij te laten testen op kwetsbaarheden en dit in de P&C cyclus op te nemen;
   c. de verantwoordelijkheid voor informatiebeveiliging expliciet en als apart onderwerp bij een portefeuillehouder te beleggen;
   d. een plan van aanpak voor bewustwording, cultuurverandering en bekwaamheid van de medewerkers op te stellen en de gemeenteraad hierover te informeren;
   e. in overleg te treden met DeSom met het doel alle relevante certificaten, normeringen en Service Level Agreement te verkrijgen.

Aldus vastgesteld in de openbare vergadering van de raad van de gemeente Medemblik, gehouden op 29 september 2022.

De griffier, De voorzitter,

Ter besluitvorming

Onderwerp

Rapportage informatieveiligheid van de Rekenkamercommissie Medemblik-Opmeer

Aanleiding

De rekenkamercommissie doet onderzoek naar de doeltreffendheid, doelmatigheid en rechtmatigheid van het door het college uitgevoerde beleid. Op 30 augustus 2022 heeft de rekenkamercommissie het rapport informatieveiligheid gepubliceerd.
Op basis van onderzoek door Hoffmann Bedrijfsrecherche B.V. trekt de rekenkamercommissie de volgende conclusies:

1. Het informatieveiligheidsbeleid in de gemeente Medemblik is niet op orde. Het beleid is op een te hoog abstractieniveau geschreven en daardoor moeilijk te operationaliseren en net zo moeilijk te monitoren.
2. Het bewustzijn van medewerkers – ambtelijk en bestuurlijk – is onder de maat. Zowel bij het mysterie guest bezoek als bij de penetratietest gaven medewerkers toegang tot fysieke ruimtes respectievelijk ICT-systemen.
3. Met het vertrek van de CISO in Medemblik is een extra risico ontstaan in de zin dat zijn vertrek het schrijven van een nieuw beleidsplan verder bemoeilijkt. Adequaat beleid en uitvoering daarvan laten daarmee te lang op zich wachten.
4. Het onderzoeksbureau heeft voor DeSom geen afschrift van ISO-certificering in de gemeente Medemblik aangetroffen, veiligheidssystemen zijn niet op orde en Hoffmann heeft kunnen inbreken in de systemen. Waar Shared Service Center DeSom zorgen uit handen zou moeten nemen, noemen meerdere medewerkers DeSom juist als een risico.
5. De samenwerking met andere gemeenten binnen DeSom - met verschillende prioritering tussen verschillende gemeenten - leidt tot trage besluitvorming, gebrek aan regie en kan daardoor leiden tot extra risico's.
6. In de uitvoering zijn op alle drie de onderzochte onderdelen mens, organisatie en techniek onvolkomenheden gevonden. Dit levert risico's op alle drie onderdelen.

De rekenkamercommissie doet op basis van bovenstaande conclusies de volgende aanbevelingen:

Aanbevelingen aan de gemeenteraad

1. Verzoek het college het informatieveiligheidsbeleid te herijken en daarbij te voldoen aan de verplichte BIO en stel dit beleid op basis daarvan als raad vast. Herhaal dit elke raadsperiode en heb in dit beleid oog voor mens, organisatie en techniek.
2. Verzoek het college het risicobewustzijn bij de medewerkers te verbeteren. Denk daarbij bijvoorbeeld aan thuiswerken, koop niet in zonder de CISO of de functionaris gegevensverwerking te raadplegen en verbeter de uitvoering van het toegangsbeleid voor het gemeentehuis.
3. Verzoek het college jaarlijks een risicoanalyse op het onderwerp informatieveiligheid te maken en de raad over de risico's en de acties die het college daarop onderneemt te informeren.

Aanbevelingen aan gemeenteraad en college

4. Neem de geldelijke waardering van het risico op informatieveiligheid realistisch op in de risicoparagraaf van de gemeentelijke begroting en in de jaarrekening. Denk bij het inschatten van dit risico bijvoorbeeld aan de kosten van
    a. forensisch onderzoek
    b. onderzoek welke data is nu precies gestolen is
    c. vervanging van alle buitgemaakte gegevens van documenten (bijvoorbeeld paspoorten of rijbewijzen van burgers)
    d. het inrichten van een call center
    e. het opnieuw opstarten of zelfs opnieuw inrichten van systemen

5. Eis van DeSom dat zij alle relevante certificaten, normeringen en Service Level Agreement heeft en houdt. Neem hierin de bestuurlijke en financiële verantwoordelijkheid die de eigen gemeente ook heeft. Overweeg, als DeSom niet aan deze eis kan of wil voldoen, een andere partner te zoeken voor de taken die bij DeSom zijn belegd.

Voorstel

1. Kennis te nemen van het rekenkamerrapport informatieveiligheid, de conclusies ervan over te nemen en de aanbevelingen vast te stellen;
2. Het college op te dragen
    a. nog in 2022 een beleidskader voor informatiebeveiliging op te stellen dat voldoet aan de BIO en ter besluitvorming voor te leggen aan de gemeenteraad;
    b. tenminste een keer per jaar de gemeentelijke informatiebeveiliging door een externe partij te laten testen op kwetsbaarheden en dit in de P&C cyclus op te nemen;
    c. de verantwoordelijkheid voor informatiebeveiliging expliciet en als apart onderwerp bij een portefeuillehouder te beleggen;
    d. een plan van aanpak voor bewustwording, cultuurverandering en bekwaamheid van de medewerkers op te stellen en de gemeenteraad hierover te informeren;
    e. in overleg te treden met DeSom met het doel alle relevante certificaten, normeringen en Service Level Agreement te verkrijgen.

Beoogd resultaat

Door bovenstaande aanbevelingen over te nemen versterkt u de informatieveiligheid. Door steeds opnieuw te laten toetsen blijft u geïnformeerd over de informatieveiligheidstoestand, zodat u kunt controleren of het informatieveiligheidsbeleid op orde is en dat beleid op een juiste wijze wordt uitgevoerd.

Argumenten

De conclusies van de rekenkamercommissie – die het college onderschrijft – zijn de argumenten om de aanbevelingen over te nemen.

Kanttekeningen

n.v.t.

Financiën

Bovenstaande aanbevelingen leiden tot het vormen en vervolgens uitvoeren van nieuw beleid. Pas als dat beleid door het college is opgesteld kan het een inschatting in kosten en opbrengsten geven.

Uitvoering/evaluatie

Dit voorstel is een uitvloeisel van een evaluatie door de rekenkamercommissie. Op zijn beurt voorziet het voorstel in jaarlijkse evaluatie.

Communicatie

n.v.t.

Bijlagen

Rekenkamerrapportage Informatieveiligheid

Raadscommissie d.d. 15 september 2022