Vragen vergaderstukken gemeenteraad of raadscommissie Ridderkerk

Algemene informatie

- Onderwerp: Rapport rekenkamercommissie Informatie in goede handen?
- Vergaderdatum: 2 september, 2020
- Steller en fractie: Peter Kranendonk, SGP
- Portefeuillehouder:
- Datum indiening vraag bij griffie: 1 september 2020
- Datum ontvangst beantwoording college: 2 september 2020

Vragen en antwoorden

Vraag 1

De BIO is pas vanaf 1 januari 2020 van kracht geworden. Het grootste deel van het onderzoek vond plaats eind 2019. Nog niet formeel vastgesteld wil nog niet zeggen dat de CISO wellicht al bezig was met het 'omzetten' van het beleid naar de nieuwe BIO. Was de organisatie ten tijde van het rekenkameronderzoek al bezig met de omzetting naar de BIO?

Antwoord 1

In q3 van 2019 zijn we gestart met de voorbereiding en in q4 met het uitvoeren van de omzetting naar de BIO. Binnen de BAR-organisatie werd per domein in beeld gebracht (gap-analyse) waar elk domein staat ten aanzien van de implementatie van de verplichte overheidsmaatregelen uit de BIO.

Vraag 2

De informatiebeveiligingsorganisatie zou moeten bestaan uit zowel een technisch als organisatorisch CISO. Formeel kan er één CISO zijn! Wel kan er een CISO organisatie zijn met verschillende medewerkers. Deelt het college dit?

Antwoord 2

Binnen de BAR-organisatie is er gekozen voor één concern CISO voor zowel de BAR-organisatie en de gemeenten Barendrecht, Albrandswaard en Ridderkerk. De concern CISO zorgt voor de samenhang tussen de technische en organisatorische informatiebeveiligingsmaatregelen. De

concern CISO maakt voor de uitvoering van de technische beveiligingsmaatregelen gebruik van de expertise binnen het cluster Informatie en Automatisering.

Vraag 3:

Veel overheden 'huren' een externe FG in omdat dit meestal geen fulltime job is. Een gekwalificeerd FG medewerker die meerdere organisaties bediend kan dan juist een voordeel zijn. Bij een medewerker de FG rol 'erbij' zou moeten doen is de conclusie vaak dat dit niet ten goede komt van een goede FG rol. Deelt het college de opvatting van de Rekenkamer dat een FG medewerker in dienst genomen moet worden?

Antwoord 3:

Het college leest in de rapportage van de Rekenkamer niet dat die de opvatting heeft dat er een FG medewerker in dienst moet komen. Voor het overige verwijzen wij voor dit antwoord naar de reactie van het college op aanbeveling 1.

Vraag 4:

Vinden er ook externe 'audits' plaats en/of zijn er afspraken gemaakt met de 50 externe partijen over de verwerktingsovereenkomsten?

Antwoord 4:

De Ensia audit is weliswaar intern maar wordt als geheel door een externe auditor beoordeeld. Voor het overige worden er met externe partijen verwerkingsovereenkomsten afgesloten.

Vraag 5:

Op pagina 17 staat: *Hoewel er een procedure voor change management is vastgelegd, blijkt dat wijzigingen in de praktijk ook ad hoc worden doorgevoerd.*

Zijn deze adhoc wijzigingen wel vastgelegd? Zo ja dan kan dit mogelijk een bewust risico zijn en daarmee, mits goed gerapporteerd, is het geen groot risico.

Antwoord 5:

De zgn. ad-hoc wijzigingen waaraan wordt gerefereerd vinden helaas weleens plaats bij calamiteiten en beperken we tot het absolute minimum.

Tevens wordt dit vervolgens wel vastgelegd in of een “problem” of als spoed “change”. Zodoende zien wij dit als bewust/beperkt risico.

Vraag 6:

Eveneens op pagina 17 staat: *Applicatiebeheerders hebben, in ieder geval bij de onderzochte applicatie, volledige toegang tot de gehele applicatie en hebben de mogelijkheid om alle data in te zien, te wijzigen en accounts aan te maken. Dat is niet nodig voor het uitvoeren van hun taken.*

Was deze onderzochte applicatie dan ook al zo ingericht dat de toegang per rol gedefinieerd kon worden?

Antwoord 6:

Niet alle applicaties bieden de mogelijkheid om een rolspecifieke inrichting op te zetten. Wanneer het in de software mogelijk is wordt hier wel gebruik van gemaakt.

Daarbij breiden wij op dit moment ons “Identity and Access Management” uit om zaken als accounts, toegang en dergelijke automatisch en (proces) geautoriseerd te laten verlopen.

Vraag 7:

Op pagina 17 staat: *Op basis van de conclusies doet de rekenkamer een aantal aanbevelingen. Informatiebeveiliging en privacy zijn thema’s die grotendeels over uitvoering gaan. Daarom zijn de aanbevelingen voornamelijk gericht op het college: aanbeveling 4 is specifiek aan de raad gericht.*

Aanbeveling 5 is toch specifiek gericht aan de raad?

Antwoord 7:

Wij hebben dit inderdaad opgevat als een typ fout, er wordt aanbeveling 5 bedoeld in plaats van 4.

Vraag 8:

Op pagina 22 staat: *De controles die op dit moment zijn ingericht op de informatiebeveiliging, zijn zelfaudits. We raden aan om periodiek ook een externe partij mee te laten kijken naar de wijze waarop de informatiebeveiliging geregeld is in Ridderkerk.*

Waarom is er niet gekozen voor jaarlijks externe audits? De Algemene Rekenkamer voert ook jaarlijkse controles uit bij de Rijksoverheid en Hoog Colleges van Staat. Juist om de bewustzijn te vergroten en de to-do lijst met verbeterpunten beheersbaar te houden.

Antwoord 8:

Hier is niet voor gekozen, omdat via de ENSIA (Eenduidige Normatiek Single Information Audit) jaarlijks verantwoording wordt afgelegd aan de interne (gemeenteraad) en externe toezichthouders (departementen) over de informatieveiligheid van de gemeente Ridderkerk.

Bovendien is dit een kostenafweging, het naast de ENSIA verantwoording jaarlijks uitvoeren van externe audits kost extra geld en extra formatie.

Vraag 9 (aan Rekenkamer):

Op pagina 22 staat eveneens: *Vergroot de betrokkenheid van de raadsleden op de thema's privacy en informatieveiligheid.*

Is de Rekenkamer met de SGP fractie van mening dat de Raad met deze aanbeveling een andere rol krijgt dan bij andere soortgelijke thema's? Als Raad bespreken we toch ook niet jaarlijks het gebouw beveiligingsplan o.i.d. ? Is de Rekenkamer het met de SGP eens dat de Raad beter een afschrift van een jaarlijks uitgevoerde audit kan ontvangen en zo nodig, aan de hand van de aanbevelingen, vragen stelt aan het college. Daarnaast kan niet verwacht worden van een raadslid alle details van deze thematiek te beheersen. Dit is een nog redelijk nieuwe en specialistische 'tak van sport'

Antwoord 9:

Griffier: volgt schriftelijk of mondeling vanavond

Vraag 10:

Op pagina 24 staat bij 'veel bereikt' een aantal voorbeelden om het bewustzijn te verhogen over de medewerkers. Is ook overwogen om bijvoorbeeld met 2 wekelijkse e-learnings te werken. Hiermee kun je het bewustzijn op een toegankelijke manier vergroten en krijg als CISO organisatie ook inzicht hoeveel mensen deelnemen en dus ook 'bijblijven'?

Antwoord 10:

Er is overwogen om met e-learnings te werken. Hier is niet voor gekozen, omdat de belasting op de medewerkers al groot is, er voor de uitrol en het onderhouden hiervan extra formatie nodig is die binnen de huidige formatie niet aanwezig is. Daarnaast vraagt dit om maatwerk, niet iedere medewerker heeft hetzelfde kennisniveau nodig. Dit is afhankelijk van de taak die men uitvoert.

Vraag 11:

Op pagina 21 staat: *In het informatiebeveiligingsbeleid staat opgetekend dat het college van B&W van de gemeente Ridderkerk een cruciale rol speelt bij de uitvoering van dit informatiebeveiligingsbeleid. Het college stelt immers het informatiebeveiligingsbeleid op, bepaalt welke informatiebeveiligingsrisico's acceptabel zijn en welke informatiebeveiligingsrisico's het wil afdekken. Daarnaast legt het college verantwoording af aan de gemeenteraad.*

Is er in het informatiebeveiligingsbeleid ook specifiek beleid en daarbij behorende maatregelen opgenomen voor raadsleden? Zo ja is dit beschikbaar gesteld? Zo nee waarom niet?

Antwoord 11

Nee er is geen specifiek beleid met bijbehorende maatregelen voor raadsleden, omdat de beleidsuitgangspunten en de te implementeren maatregelen in het gemeentelijke informatiebeveiligingsbeleid voor iedereen van toepassing zijn.