Waterschap Brabantse Delta
Algemeen Bestuur
Postbus 5520
4801 DZ BREDA

Uw schrijven van :
Uw kenmerk :
Zaaknummer : 18.ZK01432
Ons kenmerk : 18AOUT0159
Barcode :
Behandeld door : mevrouw mr. P.W van der Welle
Doorkiesnummer : 076 564 10 18
Datum : 16 november 2018
Verzenddatum :

Onderwerp: rekenkameronderzoek ICT en Veiligheid

Geachte leden van het algemeen bestuur,

De rekenkamercommissie heeft in het jaarplan 2018 aangegeven een onderzoek uit te voeren naar ICT en Veiligheid bij het waterschap. Gaandeweg het proces om dit onderzoek uit te besteden, heeft de rekenkamercommissie geconcludeerd mede aan de hand van de contacten met de inmiddels voormalig secretaris-directeur, de heer Van Stokkom, dat het niet opportuun was dit onderzoek in dit stadium uit te besteden. De rekenkamercommissie heeft daarom de secretaris-directeur verzocht de vragen uit de offerte aanvraag te beantwoorden. Wij verwijzen u voor deze vragen naar de bijlage.

De centrale onderzoeksvraag in dit onderzoek is: *In hoeverre heeft het waterschap Brabantse Delta de informatiebeveiliging van de informatiesystemen in de organisatie doeltreffend ingericht, waarmee risico's worden afgedicht, waardoor geen oneigenlijke toegang tot de gevoelige informatie (zoals persoonsgegevens) kan worden verkregen, informatie in verkeerde handen kan vallen en/of vitale systemen in werking of uit kunnen worden gezet?*

De secretaris-directeur heeft aan de rekenkamercommissie een memo verstuurd waarin de vragen die in de offerte zijn gesteld, worden beantwoord. Bij de memo zijn zes bijlagen opgenomen. Aangeven is dat alle stukken vertrouwelijk zijn. De rekenkamercommissie heeft de memo en de bijlagen gelezen en aangenomen dat de memo juist is. De rekenkamercommissie constateert dat er blijkbaar geen overkoepelend plan is, omdat de memo nog moest worden geschreven. De rekenkamercommissie constateert ook dat er nog veel kan worden gedaan om de samenhang tussen de diverse onderzoeken aan te brengen. Concluderend mist de rekenkamercommissie een overkoepelend plan, waarin onder andere is aangegeven welke onderwerpen er zijn, wie daar in de organisatie verantwoordelijk voor is, welke aanbevelingen komen er uit de verschillende rapporten, wat is er mee gedaan, wat dient er nog gerealiseerd te worden. Onderdeel van de offerteaanvraag van de rekenkamercommissie was het testen van de ICT-infrastructuur (onderdeel techniek).
Doordat ambtelijk is aangegeven dat er al verschillende testen waren uitgevoerd, heeft de rekenkamercommissie geen opdracht meer gegeven aan een externe partij om die testen uit te voeren.

De rekenkamercommissie heeft naar aanleiding van de memo met bijlagen, de volgende aanbevelingen geformuleerd:
1. Breng samenhang aan in de verschillende onderwerpen door het schrijven van een overkoepelend plan, dat gaat over het geheel;
2. Informeer het algemeen bestuur over de voortgang van het realiseren van doelstellingen als uit (extern) onderzoek blijkt dat niet of deels is voldaan aan bepaalde doelstellingen;
3. Richt de voorlichtingscampagnes over ICT en Veiligheid niet alleen op de medewerkers van de organisatie, maar ook op het algemeen bestuur.

De rekenkamercommissie heeft het dagelijks bestuur gevraagd te reageren op de aanbevelingen in de bestuurlijke reactie. Ook heeft de rekenkamercommissie het dagelijks bestuur gevraagd in de bestuurlijke reactie in te gaan op de vertrouwelijkheid die de secretaris-directeur op de stukken heeft gelegd.
De rekenkamercommissie beseft dat het aanbieden van stukken aan het algemeen bestuur wettelijk verloopt via het dagelijks bestuur. De vertrouwelijkheid, zoals aangegeven door de secretaris-directeur, zal daarbij een beslissing vragen van het dagelijks bestuur over het opleggen of in stand houden van de vertrouwelijkheid bij de aanbieding aan het algemeen bestuur.

In de bestuurlijke reactie geeft het dagelijks bestuur aan dat de eerste twee aanbevelingen op dit moment al (deels) vorm krijgen bij het waterschap. Ten aanzien van de eerste aanbeveling wijst het dagelijks bestuur erop dat zij op 16 februari 2016 heeft ingestemd met het Informatieveiligheidsbeleid.
Dit informatieveiligheidsbeleid geeft de samenhang tussen de verschillende onderwerpen, de verdeling van verantwoordelijkheden en doelstellingen van het waterschap op het gebied van ICT en Veiligheid weer. Hiermee is het Informatieveiligheidsbeleid volgens het dagelijks bestuur het overkoepelend plan.
Dit informatieveiligheidsbeleid is niet bij de opstelde memo ter beschikking gesteld aan de rekenkamercommissie. De rekenkamercommissie heeft daarom hierover geen oordeel kunnen vormen.
In de bestuurlijke reactie is aangeven dat het Informatieveiligheidsbeleid, minimaal eens per drie jaar, of zodra zich belangrijke wijzigingen voordoen, wordt beoordeeld en zo nodig bijgesteld.
De rekenkamercommissie adviseert u om het dagelijks bestuur opdracht te geven het vastgestelde informatieveiligheidsbeleid van 2016 te evalueren en het algemeen bestuur over de uitkomsten hiervan te informeren.

Het dagelijks bestuur merkt hierbij op dat in navolging van onze tweede aanbeveling, het algemeen bestuur op het onderdeel ICT en Veiligheid uitgebreider zal worden geïnformeerd omtrent de voortgang van de realisatie van doelstellingen.

De derde aanbeveling neemt het dagelijks bestuur over en zal worden meegenomen in de planning van de voorlichtingscampagnes.

Het dagelijks bestuur geeft in de bestuurlijke reactie aan dat de door de organisatie opgestelde memo met bijlagen (evenals de bespreking daarvan) vertrouwelijk blijven.
De secretaris-directeur heeft destijds aangegeven dat de memo en bijlagen wel ter inzage kunnen worden gelegd bij de afdeling Bestuur & Communicatie. Wij adviseren u met het dagelijks bestuur in overleg te treden op welke wijze de opgestelde stukken besproken kunnen worden.

De bestuurlijke reactie is als bijlage bij deze brief opgenomen.

Gelet op het voorgaande, stellen wij u voor een besluit te nemen over de volgende beslispunten:
1. Het dagelijks bestuur opdracht te geven om het algemeen bestuur inzicht te geven in de samenhang van de verschillende onderwerpen binnen ICT en Veiligheid, waarbij aandacht is voor o.a. welke deelonderwerpen er zijn binnen ICT en Veiligheid, wie daar in de organisatie voor verantwoordelijk is, welke aanbevelingen komen er uit de verschillende rapporten, wat is er mee gedaan en wat dient nog gerealiseerd te worden;
2. Het dagelijks bestuur opdracht te geven het algemeen bestuur te informeren over de voortgang van het realiseren van doelstellingen als uit (extern) onderzoek blijkt dat niet of deels is voldaan aan bepaalde doelstellingen;
3. Het dagelijks bestuur opdracht te geven de voorlichtingscampagnes over ICT en Veiligheid niet alleen op de medewerkers van de organisatie te richten, maar ook op het algemeen bestuur;
4. In overleg met het dagelijks bestuur te treden over de wijze waarop het algemeen bestuur kennis kan nemen van de memo ICT en Veiligheid met de bijbehorende zes bijlagen.
5. Het dagelijks bestuur opdracht te geven tot evaluatie van het Informatieveiligheidsbeleid van 16 februari 2016 en het algemeen bestuur over de uitkomsten hiervan informeren.

Heeft u nog vragen of opmerkingen? Ik ben namens de rekenkamercommissie aanwezig in uw vergadering van januari 2019 om dit onderwerp nader toe te lichten en op vragen en opmerkingen van u in te gaan.

Hoogachtend,
Voorzitter
Rekenkamercommissie

mr. C. M. de Graaf

Bijlage(n):
* Centrale onderzoeksvraag met deelaspecten uit offerte aanvraag
* Bestuurlijke reactie

Bijlage: Centrale onderzoeksvraag en te onderzoeken deelaspecten uit offerteaanvraag

Centrale onderzoeksvraag
In hoeverre heeft het waterschap Brabantse Delta de informatiebeveiliging van de informatiesystemen in de organisatie doeltreffend ingericht, waarmee risico's worden afgedicht, waardoor geen oneigenlijke toegang tot de gevoelige informatie (zoals persoonsgegevens) kan worden verkregen, informatie in verkeerde handen kan vallen en/of vitale systemen in werking of uit kunnen worden gezet?

Deelaspecten
De centrale onderzoeksvraag is onder te verdelen in de volgende drie aspecten:

<u>De organisatie</u>
Dit aspect betreft het toetsen van de opzet, het bestaan en de werking van de governance van het waterschap Brabantse Delta omtrent informatiebeveiliging. Deze toetsing moet plaats vinden op basis van informatiebeveiligingen voortkomend uit wettelijke bepalingen en/of gemaakte afspraken, bijvoorbeeld in Unieverband.
De organisatieaspecten dienen met behulp van documentenanalyse en interviews te worden getoetst.

<u>De techniek</u>
Dit aspect betreft het testen van de ICT-infrastructuur van het waterschap Brabantse Delta. Deze dient te worden getest op kwetsbaarheden waarmee kwaadwillenden onrechtmatig over bedrijfsgevoelige gegevens, gegevens van burgers zouden kunnen beschikken en/of infrastructuur in werking kunnen stellen of afzetten waardoor maatschappelijke schade kan ontstaan. Hierbij dient te worden gedacht aan:
- Een black box test: hierbij wordt zonder kennis vooraf geprobeerd toegang te verkrijgen tot systemen. Tijdens de black box test dienen de aan internet gekoppelde systemen waaronder de website van het waterschap Brabantse Delta en het WIFI netwerk in het kantoor en op overige werkplekken te worden onderzocht. Daarnaast moet worden onderzocht of het mogelijk is zonder autorisatie (gebruikersaccount en wachtwoord) toegang te krijgen tot het interne netwerk.
- Een grey box test: bij deze test dient gebruik te worden gemaakt van een door het waterschap beschikbaar gesteld gebruikersaccount met wachtwoord. Daarmee wordt het interne netwerk van het waterschap Brabantse Delta onderzocht, vanaf een werkplek.
- Monitoring en signaleren: hierbij dient te worden gekeken of het voor het waterschap Brabantse Delta mogelijk is om aanvallen te detecteren en actie te ondernemen.
- Forensic readiness: hiermee wordt nagegaan of het waterschap Brabantse Delta logsystemen heeft waarin de acties van kwaadwillenden terug te vinden zijn. Deze dragen bij aan mogelijkheden tot efficiënt onderzoek na incidenten.

<u>De mens</u>
Bewustwording is het belangrijkste onderdeel bij informatiebeveiliging. In dit onderzoek dient te worden onderzocht in hoeverre medewerkers zich bewust zijn van informatiebeveiliging bij het waterschap Brabantse Delta.

Het waterschap heeft in 2016/2017 tests laten uitvoeren om medewerkers bewust te maken van informatiebeveiliging, onderdeel hiervan waren het versturen van phising e-mail, inlooptest en het achterlaten van USB sticks.
Dit aspect dient met behulp van documentenanalyse en interviews te worden getoetst.

<u>Optioneel aanvullende opdracht</u>
Als uit de documentenanalyse en interviews betreffende het aspect 'De mens', blijkt dat er binnen het waterschap onvoldoende praktijktest zijn uitgevoerd om het bewustzijn van de medewerkers te testen of de rekenkamercommissie is van oordeel dat aanvullende test nodig zijn, zal de rekenkamercommissie beslissen of er een aanvullende opdracht aan u wordt gegund. Dit betreft het testen van het bewustzijn van medewerkers ten aanzien van informatiebeveiliging bij het waterschap.
Te denken valt hierbij aan het uitvoeren van verschillende tests, zoals:
- Phishing e-mail: het versturen van een phishing e-mail naar een deel van de medewerkers van het waterschap Brabantse Delta. De e-mailadressen worden verstrekt door het waterschap Brabantse Delta.
- Inlooptests: het doen van inlooptest bij verschillende locaties van het waterschap Brabantse Delta.
- USB sticks achterlaten: het achterlaten van USB sticks op locaties van het waterschap Brabantse Delta.