Gemeente Delft

Raadsvoorstel
Aan de gemeenteraad

Van : Voorzitter commissie EFB
Datum : 4 oktober 2018
Pfh. : n.v.t.
Steller : P. Bosch
tel.nr. : 015 – 260 2639
e-mail : griffie@delft.nl
Doelstelling : n.v.t.
Griffienr. : 1840278

Onderwerp: Rapport Delftse Rekenkamer onderzoek "Informatiebeveiliging binnen de gemeente Delft"

Gevraagde beslissing:
1. Aanbeveling 1 over te nemen.
2. Aanbeveling 2 over te nemen.
3. Aanbeveling 3 over te nemen.
4. Aanbeveling 4 over te nemen.
5. Aanbeveling 5 over te nemen.
6. Aanbeveling 6 over te nemen.
7. Aanbeveling 7 over te nemen.
8. Aanbeveling 8 over te nemen.
9. Aanbeveling 9 over te nemen.
10. Aanbeveling 10 over te nemen.
11. Aanbeveling 11 over te nemen.
12. Aanbeveling 12 over te nemen.
13. Aanbeveling 13 over te nemen.
14. Aanbeveling 14 over te nemen.
15. Aanbeveling 15 over te nemen.
16. Aanbeveling 16 over te nemen.
17. Het college te verzoeken om vóór 1 februari 2019 te rapporteren over de uitvoering van de aan haar gerichte, door de raad overgenomen, aanbevelingen.

Samenvatting
Van de Delftse Rekenkamer (DRK) is het rapport "Informatiebeveiliging binnen de gemeente Delft". De raad ontvangt daarbij, zoals te doen gebruikelijk, een raadsvoorstel voor de vaststelling van de aanbevelingen. In het rapport is een bestuurlijke reactie van het college opgenomen welke is te betrekken bij de bespreking.

1. Aanleiding
De DRK licht in paragraaf 1.1 (op pagina's 15 tot en met 17) van het rapport de aanleiding voor het onderzoek toe.

2. Wat willen we bereiken?
De DRK geeft in paragraaf 1.2 (op pagina 17) de doelstelling van het onderzoek aan.

3. Wat gaan we daarvoor doen?
Op pagina's 5 tot en met 7 van het rapport zijn de conclusies te lezen. Naar aanleiding van deze conclusies komt de Delftse Rekenkamer tot de volgende aanbevelingen:

Aan de raad:

1. Zie erop toe dat het college conform de wettelijke voorschriften en toepasselijke normen invulling geeft aan het IB-beleid.
2. Spreek met het college af dat zij de raad actief informeert als zich bestuurlijk risico-volle gebeurtenissen of calamiteiten op IB-gebied voordoen.
3. Laat u gericht voorlichten inzake de risico's van phishing activiteiten. Zorg dat u deze activiteiten herkent en weet wat u moet doen.

Als procedureel voorstel voor aanbevelingen 1 tot en met 3 aan de raad geeft de commissievoorzitter EFB het volgende mee:
Conform bestaande afspraken wordt politiekinhoudelijk (nieuw) informatiebeveiligingsbeleid in de commissie EFB behandeld en vindt monitoring van het informatiebeveiligingsbeleid halfjaarlijks plaats via de commissie R&A, alwaar extra aandacht kan worden geschonken aan uitvoeringsaspecten.
Voorgesteld wordt om, bij aanname van deze aanbevelingen door de raad, in de commissievergadering R&A van 28 november a.s. nader stil te staan bij aanbevelingen 1 t/m 3. Voor aanbeveling 2 geldt overigens dat voor een college o.g.v. art. 169 van de Gemeentewet reeds de zgn. "actieve informatieplicht" bestaat. Tijdens de R&A-commissie van 28 november a.s. kan aandacht worden geschonken aan een nadere definitie van hetgeen precies door de wethouder en de commissie wordt verstaan onder "*risicovolle gebeurtenissen of calamiteiten op IB-gebied*".

Aan het college:
Informatiebeveiligingsbeleid

4. Draag duidelijk uit dat informatiebeveiliging een gezamenlijke verantwoordelijkheid is, van de gehele organisatie. Draag duidelijk uit dat informatiebeveiliging tevens een individuele verantwoordelijkheid van elke leidinggevende en medewerker is in de uitoefening van zijn of haar functie.
5. Scherp het IB-beleid en eventuele uitvoeringsrichtlijnen aan om ongewenste interpretatie van het IB-beleid te voorkomen en om ongewenste handelingen met gevoelige (persoons)gegevens tegen te gaan, bijvoorbeeld voor de volgende onderwerpen: het vanuit huis of elders extern werken in de basisregistratie; het "open, tenzij"-principe voor de toegang tot de directory-structuur; het vrijelijk kunnen gebruiken van Universal Serial Bus (USB) poorten; het oneigenlijke gebruik van het Burger Service Nummer (BSN); het meesturen van gevoelige informatie in bijlagen bij e-mail; de fysieke toegang tot ruimtes met vertrouwelijke informatie; het samenwerken aan (beleids)documenten buiten de gemeentelijke IT-infrastructuur om.
6. Formuleer richtsnoeren voor de medewerkers inzake de omgang met en het aanspreken van onbekenden op de werkvloer.
7. Zorg voor voldoende middelen en capaciteit om IB ook in de toekomst te kunnen blijven realiseren.

Beveiligingsrisico's

8. Plan het regelmatig plaatsvinden van externe en interne pentesten .
9. Zorg dat leidinggevenden medewerkers consequent en consistent begeleiden bij en bewustmaken op het gebied van informatiebeveiliging.

Bewustzijn

10. Zorg dat er zo min mogelijk interpretatieverschil is tussen het, door het college vastgestelde, IB-beleid en de uitvoering daarvan. Als interpretatie van het IB-beleid toch

keuzevrijheid laat ten aanzien van de uitvoering van het IB-beleid, evalueer en zo nodig corrigeer keuzes als deze het IB-beleid niet blijken te ondersteunen.

Oneigenlijke toegang

11. Train medewerkers in het herkennen van phishing e-mails en andere pogingen tot het verkrijgen van oneigenlijke toegang tot de werkvloer en de systemen van de gemeente. Onderzoek regelmatig de uitvoering van IB in de praktijk, bijvoorbeeld door phishing mails acties en door mystery guests in te zetten.
12. Creëer een eenduidig Identity and Access Managementsysteem.
13. Maak een eenduidig en herkenbaar toegangssysteem voor gasten op de werkvloer.
14. Formuleer richtsnoeren met betrekking tot de beveiliging van gevoelige (persoons)gegevens die opgevraagd, verwerkt (en in sommige gevallen gedeeld) worden door de 100%-deelnemingen. Formuleer hierin hoe toezicht en controle worden uitgeoefend.

Voldoet de gemeente aan de AVG?

15. Beleg zo spoedig als mogelijk de functies FG en CISO bij verschillende personen.
16. Formuleer richtsnoeren hoe de FG moet handelen in geval van een belangenconflict gedurende de periode dat de FG ook de functie van CISO vervult.

4. Wat mag het kosten? (Financiële paragraaf)

In de bestuurlijke reactie van het college wordt op enkele plaatsen aandacht geschonken aan benodigde aanvullende middelen die overname van aanbevelingen met zich mee zouden brengen. Het college schrijft daarover:

"Naar de wenselijkheid en haalbaarheid van een overkoepelend Identity en Acces Management systeem (aanbeveling 12) laten we eerst onderzoek doen, omdat dit een veelomvattend onderwerp is, waaraan hoge kosten verbonden kunnen zijn."

En verderop:

"Capaciteit

Aanbeveling 7: Zorg voor voldoende middelen en capaciteit om IB ook in de toekomst te kunnen blijven realiseren, zullen wij ons zeker ter harte nemen.

Op diverse plaatsen in het rapport vestigt de DRK de aandacht op de krappe capaciteit voor het uitvoeren van informatiebeveiliging en privacybescherming, alleen al op het huidige niveau van uitvoering. Dat is inclusief de extra capaciteit die in 2018 bij de Kadernota beschikbaar is gesteld. Als het niveau van uitvoering van informatiebeveiliging en privacybescherming nu verhoogd gaat worden, bijvoorbeeld door het overnemen van aanbevelingen uit dit rapport, heeft dat ook budgettaire gevolgen. Er is dan meer budget nodig bovenop de middelen die reeds beschikbaar zijn gesteld. Deze budgettaire gevolgen nemen we mee in onze afwegingen in het kader van het Bestuursprogramma.

Conclusie

De aanbevelingen in het rapport zijn grotendeels in lijn met het beleid dat wij voorstaan, zoals wij hiervoor hebben toegelicht. Op enkele in het rapport genoemde punten zullen wij opnieuw kijken naar het evenwicht tussen flexibel en open werken en de bescherming van vertrouwelijke gegevens. De mate waarin wij kunnen voldoen aan de opvolging van deze aanbevelingen, is afhankelijk van de beschikbare middelen. Wij komen daarop terug in ons voorstel voor het Bestuursprogramma."

5. Uitkomsten commissie Economie, Financiën en Bestuur 4 oktober 2018:

Wethouder Huijsmans zegt toe met een uitwerking te komen op het gebied van *responsible disclosure*.

Bijlage:
Rapport Delftse Rekenkamer onderzoek *"Informatiebeveiliging binnen de gemeente Delft"*.

Hoogachtend,
de commissie Economie, Financiën en Bestuur,

W.M. van Geenen , voorzitter.

P.G.E. Bosch , commissiegriffier.

Raadsbesluit

Datum : 8 november 2018
Griffienr. : 1840278

Onderwerp : Rapport Delftse Rekenkamer onderzoek "Informatiebeveiliging binnen de gemeente Delft"

De raad van de gemeente Delft;
gelezen het voorstel van de commissievoorzitter Economie, Financiën en Bestuur;
gelet op het advies van de commissie Economie, Financiën & Bestuur van 4 oktober 2018;

BESLUIT:

1. Aanbeveling 1 over te nemen.
2. Aanbeveling 2 over te nemen.
3. Aanbeveling 3 over te nemen.
4. Aanbeveling 4 over te nemen.
5. Aanbeveling 5 over te nemen.
6. Aanbeveling 6 over te nemen.
7. Aanbeveling 7 over te nemen.
8. Aanbeveling 8 over te nemen.
9. Aanbeveling 9 over te nemen.
10. Aanbeveling 10 over te nemen.
11. Aanbeveling 11 over te nemen.
12. Aanbeveling 12 over te nemen.
13. Aanbeveling 13 over te nemen.
14. Aanbeveling 14 over te nemen.
15. Aanbeveling 15 over te nemen.
16. Aanbeveling 16 over te nemen.
17. Het college te verzoeken om vóór 1 februari 2019 te rapporteren over de uitvoering van de aan haar gerichte, door de raad overgenomen, aanbevelingen.

Aldus vastgesteld in de openbare raadsvergadering van 8 november 2018.

J.M. van Bijsterveldt-Vliegenthart , burgemeester

Drs. R.G.R. Jeene CMC , griffier