VOORDRACHT

Provinciale Staten van Noord-Holland

Haarlem, 12 september 2016

Onderwerp: Eindrapport Randstedelijke Rekenkamer Informatieveiligheid provincie Noord-Holland

Kenmerk: 838526

Bijlagen:
- Eindrapport
- 5-minuten versie
- Provincievergelijking informatieveiligheid

1. Inleiding

De Randstedelijke Rekenkamer onderzoekt de doelmatigheid, de doeltreffendheid en de rechtmatigheid van het door het provinciebestuur gevoerde bestuur (artikel 183 van de Provinciewet). In dit kader brengt de Randstedelijke Rekenkamer het voorliggende rapport 'Informatieveiligheid provincie Noord-Holland' aan Provinciale Staten uit.
Provinciale Staten behandelt Rekenkamerrapporten standaard in de betreffende vakcommissie en rondt deze af met een Statenbesluit.
Het doel en de centrale onderzoeksvraag van het uitgevoerde onderzoek is om inzichtelijk te maken óf de informatieveiligheid van de provincie voldoende is geborgd?

2. Conclusies en aanbevelingen

Conclusies

De conclusies voor de provincie Noord-Holland en de toelichting daarop zijn verwoord vanaf pagina 6 van het rapport.

Op de centrale onderzoeksvraag concludeert de Rekenkamer het volgende: *"De provincie besteedt voldoende aandacht aan de bewustwording van het belang van informatieveiligheid binnen de organisatie. Ook heeft de provincie het toezicht op en de verantwoording over informatieveiligheid goed geregeld. Er is een aantal beslissingen genomen, waarmee invulling wordt gegeven aan de verantwoordelijkheid voor informatieveiligheid. Er is wel verbetering mogelijk in de sturing op het tempo van de implementatie van de rollen en verantwoordelijkheden ten aanzien van informatieveiligheid. Hoewel de provincie veel zaken heeft opgepakt, behoeft de organisatorische verankering en de planmatige aanpak van informatieveiligheid verbetering. Sinds 2016 zet de provincie hiertoe wel stappen. Een ander verbeterpunt is de uitvoering van maatregelen om de informatieveiligheid te bevorderen. Het is bijvoorbeeld niet voor alle bedrijfsprocessen duidelijk welke informatieveiligheidsmaatregelen nodig zijn en de provincie heeft geen zicht of de maatregelen daadwerkelijk zijn uitgevoerd."*

Op basis van de deelvragen van het onderzoek komt de Rekenkamer met de volgende deelconclusies:

1. Er is een aantal beslissingen genomen, waarmee invulling wordt gegeven aan de verantwoordelijkheid voor informatieveiligheid. Zo zijn rollen en verantwoordelijkheden in 2012 vastgesteld. De sturing op het tempo van de besluitvorming en uitvoering ten aanzien van informatieveiligheid kan wel beter. De implementatie van de rollen en verantwoordelijkheden is vertraagd. Hoewel de provincie desondanks veel zaken heeft opgepakt, behoeft de organisatorische verankering en planmatige aanpak van informatieveiligheid verbetering. Sinds begin 2016 zet de provincie stappen met het beleggen van rollen en de invulling van verantwoordelijkheden op het gebied van informatieveiligheid.

2. Het informatieveiligheidsbeleid van de provincie voldoet in opzet aan de eisen. In 2016 dient een geactualiseerde versie van het informatieveiligheidsbeleid te worden vastgesteld. Het is niet goed te beoordelen of de provincie de benodigde informatieveiligheidsmaatregelen uitvoert, omdat de provincie de uitvoering van de informatieveiligheidsmaatregelen niet coördineert of registreert en niet voor alle bedrijfsprocessen heeft bepaald of een risicoanalyse nodig is. In deze provincie is geen test uitgevoerd of de informatie in de praktijk voldoende beschermd is.

3. De provincie heeft voldoende aandacht voor bewustwording van het belang van informatieveiligheid. De provincie heeft onafhankelijke onderzoeken laten verrichten die inzicht geven in de mate van bewustzijn van medewerkers van het belang van informatieveiligheid. De bevindingen van deze onderzoeken zijn gebruikt om het bewustzijn van medewerkers op het gebied van informatieveiligheid te vergroten. In 2015 was het bewustzijn van medewerkers verbeterd ten opzichte van 2013.

4. De provincie heeft het houden van toezicht op informatieveiligheid goed geregeld. Er zijn diverse onafhankelijke onderzoeken uitgevoerd naar de stand van zaken van informatieveiligheid. De bevindingen zijn onder de aandacht gebracht van de directie en hebben tot vervolgacties geleid.
   Ook heeft de provincie het afleggen van verantwoording over informatieveiligheid goed geregeld. Informatieveiligheid maakt onderdeel uit van de ambtelijke P&C-cyclus en sinds 2016 ook van de bestuurlijke P&C-cyclus. De provincie heeft tevens de zelfevaluatie over informatieveiligheid uitgevoerd.

<u>Aanbevelingen</u>
De Rekenkamer heeft voor de provincie Noord-Holland op basis van de deelconclusies drie aanbevelingen gedaan (zie pagina's 7 en 8 voor de aanbevelingen en onderbouwing):

1. Vraag GS om ervoor te zorgen dat er zo spoedig mogelijk volgens de rollen en verantwoordelijkheden op het gebied van informatieveiligheid die in februari 2016 zijn vastgesteld wordt gewerkt.
2. Vraag GS om ervoor te zorgen dat een geactualiseerde versie van het informatieveiligheidsbeleid in 2016 wordt vastgesteld.

3. Vraag GS te bewaken dat voor alle bedrijfsprocessen wordt bepaald of een risicoanalyse nodig is en dat deze risicoanalyses worden uitgevoerd, evenals de aanvullende maatregelen die daaruit voortkomen.

3. Reactie Gedeputeerde Staten

Voor de volledige reactie van GS zie pagina 11 t/m 13 van het rapport.

GS geeft aan tevreden te zijn met de conclusie van de Rekenkamer dat toezicht op en verantwoording over informatieveiligheid op orde is. Over de constatering dat het tempo van de implementatie van rollen en verantwoordelijkheden verbeterd kan worden, meldt GS dat zij een afweging gemaakt hebben tussen snelheid en zorgvuldigheid als het gaat om de inspanningen om informatieveiligheid organisatorisch te verankeren. Die inspanningen hangen nauw samen met de ontwikkelingen die GS in gang hebben gezet op het gebied van informatiebeleid in brede zin. Met de recente aanstelling van een Chief Information Officer (CIO) en het vaststellen van het concernbrede informatiebeleid zijn volgens GS de juiste voorwaarden gecreëerd om de rollen en verantwoordelijkheden op het gebied van informatieveiligheid stevig en duurzaam te verankeren.

<u>Reactie Gedeputeerde Staten per aanbeveling</u>

Aanbeveling 1

Vraag GS om ervoor te zorgen dat er zo spoedig mogelijk volgens de rollen en verantwoordelijkheden op het gebied van informatieveiligheid die in februari 2016 zijn vastgesteld wordt gewerkt.

Reactie:

Deze aanbeveling nemen GS over. GS achten een duidelijke rolverdeling en heldere bevoegdheden een noodzakelijke voorwaarde voor een efficiënte en effectieve organisatie, ook op het gebied van informatieveiligheid. Het besluit waarin de rollen en verantwoordelijkheden zijn gedefinieerd is het resultaat van een zorgvuldige afweging van belangen en ontwikkelingen. Momenteel wordt dit voorstel geïmplementeerd. Evaluatie van het gekozen model staat gepland voor begin 2018.

Aanbeveling 2

Vraag GS om ervoor te zorgen dat een geactualiseerde versie van het informatieveiligheidsbeleid in 2016 wordt vastgesteld.

Reactie:

Deze aanbeveling nemen GS over. Het huidige informatiebeveiligingsbeleid stamt uit 2012 en zal dit jaar geactualiseerd worden. GS hechten belang aan heldere en werkbare kaders. Informatieveiligheid is als fundament onder het Concerninformatieplan (CIP) dit jaar opnieuw stevig verankerd in een strategisch bedrijfsvoeringkader. Op ambtelijk niveau zal dit uitgewerkt worden in tactisch en operationeel informatieveiligheidsbeleid.

Aanbeveling 3
Vraag GS te bewaken dat voor alle bedrijfsprocessen wordt bepaald of een risicoanalyse nodig is en dat deze risicoanalyses worden uitgevoerd, evenals de aanvullende maatregelen die daaruit voortkomen.

Reactie:
Deze aanbeveling nemen GS over. GS achten het van belang dat voor alle processen een adequaat beveiligingsniveau is vastgesteld, en dat de benodigde aanvullende beheersmaatregelen uitgevoerd worden. Momenteel geven GS invulling aan uw aanbeveling door via de Verbijzonderde Interne Controle (VIC) de processen die door de ambtelijke organisatie als risicovol worden beschouwd aan bovengenoemde eisen te toetsen. Inspanningen om ook de overige bedrijfsprocessen aan deze werkwijze te onderwerpen worden meegenomen in nieuwe beleidsplan.

De aanbevelingen van de Rekenkamer zijn, geherformuleerd als besluiten, opgenomen in het ontwerpbesluit.

4. Voorstel

Wij stellen u voor te besluiten overeenkomstig het bijgaande ontwerpbesluit.

H. Struben, voorzitter Statencommissie Mobiliteit en Financiën

M. Spoor, griffier Statencommissie Mobiliteit en Financiën

Ontwerpbesluit

Nr. 56

Provinciale Staten van Noord-Holland;

gelezen de voordracht van de Statencommissie Mobiliteit en Financiën van 12 september 2016;

gelezen het rapport van de Randstedelijke Rekenkamer, getiteld 'Informatieveiligheid provincie Noord-Holland',

besluiten:

1. GS te verzoeken ervoor te zorgen dat er zo spoedig mogelijk volgens de rollen en verantwoordelijkheden op het gebied van informatieveiligheid die in februari 2016 zijn vastgesteld wordt gewerkt;

2. GS te verzoeken ervoor te zorgen dat een geactualiseerde versie van het informatieveiligheidsbeleid in 2016 wordt vastgesteld;

3. GS te verzoeken te bewaken dat voor alle bedrijfsprocessen wordt bepaald of een risicoanalyse nodig is en dat deze risicoanalyses worden uitgevoerd, evenals de aanvullende maatregelen die daaruit voortkomen.

Haarlem, 3 oktober 2016

Provinciale Staten voornoemd,

, voorzitter

, statengriffier