Statenvoorstel

Onderwerp
Statenvoorstel - Onderzoeksrapport RRK - Informatieveiligheid

Gedeputeerde Staten stellen voor

1. Beslispunten
   1. Kennis te nemen van het eindrapport Informatieveiligheid Flevoland;
   2. Kennis te nemen van de bestuurlijke reactie van Gedeputeerde Staten;
   3. In te stemmen met de volgende aanbevelingen:
      1a.
      Vraag GS om ervoor te zorgen dat rollen en verantwoordelijkheden bij informatieveiligheid door de gehele organisatie goed worden ingevuld.
      1b.
      Vraag GS om u te informeren over de invulling van rollen en verantwoordelijkheden en de scheiding van functies bij informatieveiligheid.
      2a.
      Vraag GS om te bewaken dat alle generieke maatregelen voor informatieveiligheid zo snel mogelijk worden uitgevoerd.
      2b.
      Vraag GS om te bewaken dat voor alle processen en systemen wordt bepaald of een risicoanalyse nodig is, dat deze risicoanalyses worden uitgevoerd en dat aan vullende maatregelen die daaruit voortkomen, worden uitgevoerd.

2. Verdere behandeling PS
   PS bespreken de aan haar gerichte aanbevelingen uit het eindrapport en de bestuurlijke reactie van GS daarop.

3. Korte toelichting op voorstel
   Centrale onderzoeksvraag
   Heeft de provincie Flevoland de informatieveiligheid voldoende geborgd?

   De centrale onderzoeksvraag is beantwoord aan de hand van vier deelvragen:
   1. Heeft de provincie de sturing op en de verantwoordelijkheid voor informatieveiligheid goed verankerd?
   2. Is het informatieveiligheidsbeleid in opzet, uitvoering én in resultaat adequaat?
      a. Heeft de provincie een informatieveiligheidsbeleid opgesteld dat voldoet aan de daaraan te stellen eisen?
      b. Voert de provincie de benodigde informatieveiligheidsmaatregelen uit?
      c. Is informatie in de praktijk voldoende beschermd tegen toegang door onbevoegden?
   3. Heeft de provincie voldoende aandacht voor bewustwording op het gebied van informatieveiligheid?
   4. Heeft de provincie het afleggen van verantwoording over en het houden van toezicht op informatieveiligheid goed geregeld?

   Conclusie:
   De provincie stuurt voldoende op informatieveiligheid. Er zijn goede aanzetten voor de verdeling van verantwoordelijkheden en er is voldoende aandacht voor toezicht op en verantwoording over informatieveiligheid.
   Ook worden sinds eind 2015 acties ondernomen om het bewustzijn voor informatieveiligheid te vergroten. De invulling van verantwoordelijkheden in de praktijk behoeft nog wel verbetering. Een ander verbeterpunt is de uitvoering van maatregelen om de informatieveiligheid te verbeteren. Generieke maatregelen zijn nog niet volledig geïmplementeerd. Ook zijn risicoanalyses om te bepalen of aanvullende maatregelen nodig zijn, slechts beperkt uitgevoerd.

   Deelconclusie 1

Provinciale Staten
26 oktober 2016

Agendapunt

Lelystad

Registratienummer
1957806

Inlichtingen
M. Hinzen

Afdeling/Bureau
SGR

Portefeuillehouder
Rijsberman, M.A.

Routing

Commissie Bestuur:
7 september 2016

Statenvoorstel

Verantwoordelijkheden zijn over het geheel genomen goed verdeeld, met een duidelijke rol voor de directie. Verder is een opzet gemaakt voor de toedeling van het eigenaarschap van informatiesystemen. De invulling van verantwoordelijkheden voor informatieveiligheid in de managementlaag onder de directie behoeft nog wel verbetering. Verder is de controlerende rol bij informatieveiligheid niet goed gescheiden van de beleidsrol en de uitvoerende rol.

Deelconclusie 2
Het informatieveiligheidsbeleid van de provincie voldoet in opzet aan de eisen. De provincie heeft de benodigde informatieveiligheidsmaatregelen nog niet allemaal uitgevoerd. Er moeten nog generieke informatieveiligheidsmaatregelen worden uitgevoerd, ook bij kritieke systemen. Risicoanalyses om te bepalen voor welke systemen en processen aanvullende maatregelen nodig zijn, zijn slechts in beperkte mate gedaan. Om te beoordelen of de informatie van de provincie in de praktijk voldoende beschermd is, is een test uitgevoerd. Daarbij is een aantal kwetsbaarheden met een hoog risico ontdekt. Voor zover deze kwetsbaarheden technisch van aard zijn, zijn deze grotendeels verholpen. Op basis van de test kan overigens geen algemene uitspraak worden gedaan over de bescherming van de informatie van de provincie.

Deelconclusie 3
Binnen de provincie bestaat sinds eind 2015 voldoende aandacht voor bewustwording van het belang van informatieveiligheid. Het voornemen om meer aandacht te geven aan bewustwording bestaat sinds eind 2012, maar het duurde tot eind 2015 voordat dit voornemen in actie is omgezet.

Deelconclusie 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 hebben geleid tot vervolgacties ter verbetering van de informatieveiligheid.
Het afleggen van verantwoording over informatieveiligheid in de provincie is eveneens goed geregeld. Informatieveiligheid maakt deel uit van zowel de bestuurlijke als de ambtelijk P&C cyclus. Verder gebruikt de provincie de interprovinciale monitor zelfevaluatie om de voortgang bij informatieveiligheid te volgen.

4. Wijze van opstellen Statenvoorstel

Dit statenvoorstel is opgesteld conform de afspraken in het seniorenconvent (25-11-2015) over het opstellen en agenderen van statenvoorstellen voor rekenkameronderzoeken. Deze afspraken luiden:

- Alle rekenkameronderzoeken worden vastgesteld in PS;
- de reactie van het college op aanbevelingen worden opgenomen in het statenvoorstel onder het kopje ‘kanttekeningen’;
- het statenvoorstel omvat standaard alle aanbevelingen van de rekenkamer;
- de aanbevelingen worden letterlijk opgenomen in het statenvoorstel;
- het statenvoorstel wordt oordeelsvormend geagendeerd in de relevante commissie, voor advies;
- hierop volgt agendering in PS met een weergave van het commissieadvies, indien relevant ook in de beslispunten;
- het oorspronkelijke statenvoorstel wordt bijgevoegd.

5. Kanttekeningen: bestuurlijke reactie College van GS op aanbevelingen

U heeft ons op 17 juni jongstleden de bestuurlijke nota Informatieveiligheid in concept toegezonden.
Graag maken we van de gelegenheid gebruik om daarop in het kader van het bestuurlijk wederhoor te reageren.

Algemeen
Eind augustus 2015 is de opzet voor dit onderzoek gepubliceerd. In de maanden die daarop volgden is intensief met de ambtelijke organisatie gesproken, merendeels met de medewerker belast met informatieveiligheid. Het onderzoeksproces hebben wij als zorgvuldig ervaren en dat geldt ook voor de test van de mobile devices. In de uitvoering van uw onderzoek herkennen wij de aanpak uit uw onderzoeksopzet. Uw aanbevelingen zijn via Provinciale Staten (PS) aan ons gericht en wij gaan daarom hieronder daar op in.

Het onderzoek is gelijktijdig uitgevoerd in de vier provincies waar de Randstedelijke Rekenkamer werkzaam is. Wij hadden op basis van de laatste zin van hoofdstuk 6 Werkwijze van uw onderzoeksopzet verwacht dat het eindrapport op een aantal onderdelen een provincievergelijking zou bevatten. Deze interprovinciale vergelijking zouden we gebruiken bij onze doorontwikkeling.

Ontwikkeling
De.rekenkamer constateert dat de provincie veel aandacht besteed aan informatieveiligheid. Wij vinden het prettig dat de onderzoekers dit hebben geconcludeerd. De laatste jaren zijn we er in geslaagd om informatieveiligheid op een hoger plan te brengen. Onze risico-georiënteerde aanpak heeft aantoonbaar geleid tot een structurele verbetering van de Informatieveiligheid. Inmiddels hebben andere provincies onze aanpak overgenomen. Onze directie bepaalt en monitort de activiteiten die daarvoor worden uitgevoerd.

Conclusies en aanbevelingen
De hoofdvraag die u heeft gesteld is in hoeverre de provincie Flevoland de informatieveiligheid voldoende heeft geborgd. In onze directie is recent over het rapport gesproken.

	Conclusies en aanbevelingen	**Bestuurlijke reactie**
Conclusie	De provincie Flevoland stuurt voldoende op informatieveiligheid. Er zijn goede aanzetten voor de verdeling van verantwoordelijkheden en er is voldoende aandacht voor toezicht op en verantwoording over informatieveiligheid. Ook worden sinds eind 2015 acties ondernomen om het bewustzijn voor informatieveiligheid te vergroten. De invulling van verantwoordelijkheden in de praktijk behoeft nog wel verbetering. Een ander verbeterpunt is de uitvoering van maatregelen om de informatieveiligheid te verbeteren. Generieke maatregelen zijn nog niet volledig geïmplementeerd. Ook zijn risicoanalyses om te bepalen of aanvullende maatregelen nodig zijn, slechts beperkt uitgevoerd.	Wij stemmen met grote tevredenheid met deze conclusie in. Onze inspanningen van vooral de laatste jaren hebben goede resultaten opgeleverd. Onze insteek daarbij is met name een risicogeoriënteerde aanpak geweest. Sinds de twaalf provincies gezamenlijk een ambitie hebben geformuleerd en onderschreven, hebben wij daaraan in onze organisatie structureel aandacht gegeven. En ook in de recent vastgestelde Meerjarenaanpak Bedrijfsvoering is informatieveiligheid een cruciaal element.
Deelconclusie 1	Verantwoordelijkheden zijn over het geheel genomen goed verdeeld, met een duidelijke rol voor de directie. Verder is een opzet gemaakt voor de toedeling van het eigenaarschap van informatiesystemen. De invulling van verantwoordelijkheden voor informatieveiligheid in de managementlaag onder de directie behoeft nog wel verbetering. Verder is de controlerende rol bij informatieveiligheid niet goed gescheiden van de beleidsrol en de uitvoerende rol.	Deze conclusie onderschrijven wij. deels, aangezien deze verdeling in het informatieveiligheidsbeleid is vastgelegd
Aanbeveling 1a	Vraag GS om ervoor te zorgen dat rollen en verantwoordelijkheden bij informatieveiligheid door de gehele organisatie goed worden ingevuld.	De aanbeveling pakken wij risicogeoriënteerd op, waarbij we de tien meest kritische systemen eerst ter hand nemen. Het eigenaarschap van de systemen met bijbehorende rollen en verantwoordelijkheden wordt aan de hand van een PDCA-aanpak op voldoende niveau gebracht.
Aanbeveling 1b	Vraag GS om de controlerende rol op informatieveiligheid gescheiden van de beleidsrol en de uitvoerende rol te positioneren.	Deze aanbeveling kunnen wij niet onderschrijven. Bij het vaststellen van het informatiebeveiligingsbeleid in mei 2015 is bepaald dat de directie verantwoordelijk is voor het vaststellen van het beleid. Het voorbereiden en toetsen van het beleid zijn belegd bij de adviseur informatievei-

		ligheid. Het uitvoeren en verbeteren ligt bij de afdelingshoofden / systeemeigenaren. in het kader van de ontwikkeling van informatievoorziening is besloten om de controlerende rol – met name de twee-jaarlijkse onafhankelijke toetsen –onder de verantwoordelijkheid van de concerncon-troller te brengen. Wij vinden dat hiermee een juiste invulling was gegeven aan functiescheiding en dat het nu nog verder verbeterd is.
Deelconclusie 2	Het informatieveiligheidsbeleid van de provincie voldoet in opzet aan de eisen. De provincie heeft de benodigde informatieveiligheidsmaatregelen nog niet allemaal uitgevoerd. Er moeten nog generieke informatieveiligheidsmaatregelen worden uitgevoerd, ook bij kritieke systemen. Risicoanalyses om te bepalen voor welke sys-temen en processen aanvullende maatregelen nodig zijn, zijn slechts in beperkte mate gedaan. Om te beoordelen of de informatie van de provin-cie in de praktijk voldoende beschermd is, is een test uitgevoerd. Daarbij is een aantal kwetsbaar-heden met een hoog risico ontdekt. Voor zover deze kwetsbaarheden technisch van aard zijn, zijn deze grotendeels verholpen. Op basis van de test kan overigens geen algemene uitspraak worden gedaan over de bescherming van de informatie van de provincie.	Deze conclusie onderschrijven wij
Aanbeveling 2a	Vraag GS om te bewaken dat alle generieke maatregelen voor informatieveiligheid zo snel mogelijk worden uitgevoerd.	Wij hebben alle geïdentificeerde maatre-gelen geïnventariseerd en geprioriteerd voor de komende vier jaar. De maatrege-len met een hoog risico worden in 2016 gemitigeerd. Alle maatregelen met een midden risico zijn eind 2017 in uitvoering. Vervolgens kan een onafhankelijke toets bepalen of de directie een zogenaamde “in control”-verklaring kan afgeven. De uitvoering van de door de directie vastge-stelde verbeteracties wordt maandelijks gemonitord en gerapporteerd aan de IT-Raad.
Aanbeveling 2b	Vraag GS om te bewaken dat voor alle processen en systemen wordt bepaald of een risicoanalyse nodig is, dat deze risicoanalyses worden uitge-voerd en dat aanvullende maatregelen die daaruit voortkomen, worden uitgevoerd.	De inventarisatie van de systemen wordt in juli 2016 afgerond. Elke systeemeigenaar gaat vervolgens indien relevant een Afhankelijkheids- en Kwetsbaarheidsanalyse uitvoeren. Alle

		uitkomsten worden door de adviseur Informatieveiligheid gebundeld en ter goedkeuring voorgelegd aan de directie. Dit besluit bevat ook de keuze voor de tien meest kritische systemen van de provincie. Het uitvoeren van risicoanalyses op processen is inmiddels interprovinciaal ingebracht bij het Strategische Overleg, maar is daar vooralsnog niet opgepakt. We hebben hierbij voorgesteld om de tien meest kritische processen van de provincies vast te stellen.
Deelconclusie 3	Binnen de provincie bestaat sinds eind 2015 voldoende aandacht voor bewustwording van het belang van informatieveiligheid. Het voornemen om meer aandacht te geven aan bewustwording bestaat sinds eind 2012, maar het duurde tot eind 2015 voordat dit voornemen in actie is omgezet.	Wij stemmen met deze conclusie in en zijn ons ervan bewust dat in de organisatie structureel aandacht nodig is voor informatieveiligheid.
Deelconclusie 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 hebben geleid tot vervolgacties ter verbetering van de informatieveiligheid. Het afleggen van verantwoording over informatieveiligheid in de provincie is eveneens goed geregeld. Informatieveiligheid maakt deel uit van zowel de bestuurlijke als de ambtelijk P&C cyclus. Verder gebruikt de provincie de interprovinciale monitor zelfevaluatie om de voortgang bij informatieveiligheid te volgen.	Deze conclusie onderschrijven wij.

Het onderwerp gaat over de kwaliteit van de informatieveiligheid in de organisatie. Onze organisatie is daar intensief mee bezig. Ook in het kader van de Meerjarenaanpak bedrijfsvoering komt het aan de orde. We zijn dan ook geïnteresseerd in de behandeling van dit onderzoek in de staten en zien wij deze met vertrouwen tegemoet.

6. Advies commissie bestuur

7. Bijlagen

Naam stuk:	eDocs nummer:	Bijgevoegd of periode ter inzage
Eindrapport Informatieveiligheid Flevoland	1944763	Bijgevoegd
5 minuten versie Informatieveiligheid Flevoland	1944757	Bijgevoegd
Provincievergelijking Informatieveiligheid	1944761	Bijgevoegd