College van Gedeputeerde Staten
statenbrief

Aan Provinciale Staten
Statencommissie Bestuur, Europa en Middelen

DATUM	31 januari 2017	REFERENTIE	Visbeen
ONS NUMMER	81A4C214	DOORKIESNUMMER	2150
NUMMER PS	2017BEM22	E-MAILADRES	john.visbeen@provincie-utrecht.nl
BIJLAGE	1	PORTEFEUILLEHOUDER	Verbeek-Nijhof

Onderwerp Statenbrief: eerste voortgangsrapportage informatieveiligheid

Voorgestelde behandeling: ter informatie

Geachte dames en heren,

Inleiding

Bijgaand treft u de eerste voortgangsrapportage informatieveiligheid. In uw vergadering van september 2016 is afgesproken om deze voortgangsrapportage twee keer per jaar aan u aan te bieden.

Aanleiding
De beschikbaarheid, integriteit en vertrouwelijkheid in informatie betreffen de kwaliteit van informatievoorziening. Het is belangrijk dat informatie niet in verkeerde handen valt door bijvoorbeeld externe dreigingen, zoals hacking, ddos aanvallen, of door interne menselijke fouten. Verder is van belang dat de gegevens juist, accuraat en beschikbaar zijn op het moment dat dit nodig is. Daarom hebben de provincies gezamenlijk afspraken gemaakt over informatieveiligheid en dit is vastgelegd in het “Convenant interprovinciale regulering informatieveiligheid” uit 2014 (hierna: convenant).

Voorgeschiedenis
Op 9 december 2014 hebben Gedeputeerde Staten van de provincie Utrecht ingestemd met dit convenant en is gestart met het project Informatieveiligheid. Op basis van het convenant heeft herijking van het beleid op informatieveiligheid plaatsgevonden. In 2015 en 2016 is eigen onderzoek gedaan en heeft een onderzoek van de Randstedelijke Rekenkamer plaatsgevonden. Als rode draad door de bevindingen en aanbevelingen door beide onderzoeken loopt dat:
- Het besef van urgentie op het gebied informatieveiligheid verbeterd moet worden in de organisatie;
- Door middel van rapportages meer inzicht moet worden geboden in de status van de informatieveiligheid maatregelen en borging in P&C cyclus.

Als uitwerking van het beleidsplan en om de aanbevelingen uit eigen onderzoek en het onderzoek van de Rekenkamer op te volgen, is het Plan van Aanpak Informatieveiligheid 2016-2017 opgesteld. Hierin worden de belangrijkste activiteiten benoemd die noodzakelijk zijn om informatieveiligheid meer planmatig in te richten, het besef van urgentie voor informatieveiligheid te verhogen en om aan het basisniveau van informatieveiligheid te voldoen.

Essentie / samenvatting:
Met het vaststellen van het Convenant Informatieveiligheid, het oppakken van bevindingen van eigen onderzoek en het onderzoek van de Rekenkamer is door bestuur en management en is opdracht gegeven tot het herijken van informatieveiligheidsbeleid en het opstellen van een Plan van Aanpak. Daarmee is het belang van het treffen van maatregelen om de beschikbaarheid en integriteit van informatie te borgen onderkend. De activiteiten in het plan van aanpak zijn er op gericht om doelstellingen uit het Convenant te realiseren, waaronder het implementeren van maatregelen uit de Interprovinciale Baseline voor informatieveiligheid (IBI).

Ten opzichte van juni 2016 is op de vier kernthema's uit het convenant (sturing & verantwoordelijkheid, beleid & normenkader, verantwoording & toezicht en bewustwording) vooruitgang geboekt. Het portefeuillehouderschap is stevig verankerd, de IBI is uitgangspunt voor ons beleidskader, het awareness programma voor medewerkers is nagenoeg gereed en de periodieke en onafhankelijke toets (audit) staat gepland voor 2017. Uit het activiteiten overzicht blijkt dat alle activiteiten gestart zijn volgens planning. De GAP analyse om te onderzoeken in welke mate de maatregelen uit de IBI al zijn doorgevoerd kan daarbij worden gezien als een vorm van tussentijdse interne audit naast de onafhankelijke audit.

Vervolgprocedure/voortgang
Het is noodzakelijk informatieveiligheid nog steviger te verankeren binnen de provincie om te voorkomen dat de verantwoordelijkheid gedragen blijft door enkelingen. In 2015 heeft een onafhankelijke audit van AuditConnect plaatsgevonden en is gewerkt met niveau's van volwassenheid op het gebied van informatieveiligheid. Om toe te groeien van de "ad-hoc-fase" naar "de fase 2/3 (herhaalbaar/gedefinieerd) uit het procesvolwassenheidsmodel is het noodzakelijk dat de proceseigenaren nog beter toegerust worden om hun verantwoordelijkheid te kunnen nemen.

Er hebben zich een aantal beveiligingsincidenten voorgedaan waarop actie is genomen. De maatregelen moeten nog beter verankerd worden om verder toe te groeien naar een volgende fase in het procesvolwassenheids-model. Denk hierbij aan het opstellen, aanpassen en uitvoeren van procedures en instructies. Een deel van de activiteiten in deze rapportageperiode heeft zich gericht op het treffen van voorbereidingen voor nadere bewustwording en instructie voor CMT, directie en teamleiders. Omdat risk-based werken een belangrijk uitgangspunt is bij het nemen van besluiten, zal aan de implementatie van dit proces en de rol van de proceseigenaar/teamleider hierin ruim aandacht worden besteed.

Om proceseigenaren/teamleiders goed te kunnen faciliteren en om de rapportagelasten te vereenvoudigen is het belangrijk om de toolbox informatieveiligheid goed te gebruiken. Om te bepalen wat het juiste (detail)niveau is van het gebruik van dit instrument en daarmee draagvlak voor het gebruik te creëren, wordt nader overleg en besluitvorming met de proceseigenaren/teamleiders georganiseerd. De provincie Utrecht anticipeert hiermee op de Baseline Informatieveiligheid Overheden die momenteel wordt ontwikkeld en waarvan de verwachting is dat zij grote delen van de IBI en toolbox systematiek zullen overnemen.

Innovaties met betrekking tot technische maatregelen worden betrokken in het project Verbetering Infrastructuur Provincie Utrecht. Dit betreft onder meer de kavels netwerk/ICT infra, printers, connectiviteit en laptops. Diverse activiteiten die zijn genoemd in het Plan van Aanpak worden onder dit project gebracht (bv. Mobile Device Management, anti ramsomware-protection). Daarbij wordt de afweging gemaakt over deze technische investeringen en het beschermingsniveau dat hiermee gerealiseerd kan worden. Samen met bewustwording van medewerkers blijft het doel van de technische maatregelen om informatieveilig tijd en plaats onafhankelijk te kunnen werken.

In september 2017 volgt de tweede voortgangsrapportage informatieveiligheid.

Concreet voorliggende vraag aan statencommissie / Provinciale Staten
Kennis te nemen van deze brief en de voortgangsrapportage.

Gedeputeerde Staten van Utrecht,

De voorzitter,

De secretaris,