College van Gedeputeerde Staten
statenbrief

Aan Provinciale Staten
Statencommissie Bestuur, Economie en Middelen

DATUM	27-5-2020	REFERENTIE	Saskia Rolsma
ONS NUMMER	820E0D82	DOORKIESNUMMER	06 2112 4624
NUMMER PS	2020BEM71	E-MAILADRES	saskia.rolsma@provincie-utrecht.nl
BIJLAGE	-	PORTEFEUILLEHOUDER	Strijk

Onderwerp Statenbrief:
Interventie binnen concernopgave 'Digitale Overheid'

Voorgestelde behandeling:
Ter informatie

Geachte dames en heren,

Inleiding
U heeft op 21 april jl. de statenbrief *Resultaten Assessment informatiebeveiliging 2019* (briefnr. 820568B0) van ons ontvangen. In die brief hebben wij voorliggende reactie aangekondigd.

Voorgeschiedenis
De provincies hebben sinds 2013 met ondersteuning van het IPO en de Taskforce Bestuur & Informatieveiligheid de dienstverlening en de provinciale informatiebeveiliging een impuls gegeven. Dit heeft geleid tot de ondertekening van het convenant interprovinciale regulering informatieveiligheid op 16 december 2014, waarin de provincies zich committeren aan afspraken voor zelfregulering van informatiebeveiliging. Eén van de afspraken van dit convenant betreft verantwoording over dit onderwerp: 1 keer per 2 jaar een assessment naar het beveiligingsniveau.
In 2015 werd dit voor het eerst uitgevoerd (0-meting); in 2017 voor de tweede maal (1-meting). Bij de provincie Utrecht zijn vanaf 2015 activiteiten ontplooid voor het bereiken van een adequaat beveiligingsniveau en het verhogen van veilig gedrag van medewerkers. Met ingang van 1 januari 2019 is het programma Informatieveiligheid & Privacy (IV&P) onderdeel van de concernopgave Digitale Overheid.

Essentie/samenvatting:
De 'Notitie van bevindingen Assessment informatiebeveiliging 2019' concludeert dat de verbetering van privacy en informatiebeveiliging stagneert. Het rapport schrijft de stagnatie toe aan een combinatie van twee factoren: de zwakke verbinding tussen lijn, opgave, programma en ICT-beheer enerzijds en het gebrek aan top-down sturing anderzijds. Deze bevindingen gelden voor de informatievoorziening binnen de hele organisatie.

De zwakke verbinding tussen de opgave 'Digitale Overheid' en de lijnorganisatie, leidt tot groeiende onduidelijkheid in verantwoordelijkheden over rapportage en verantwoordelijkheden over aansturing. Deze onduidelijkheid is zichtbaar in de (voortdurende) discussies over de inrichting van de governance (van de informatievoorziening), in de positionering van de Business informatiemanagement (BIM-functies), in het op orde hebben van het informatiebeheer en bij het voldoen aan de Archiefwet.

Naast bovenstaande analyse en conclusies, geeft het rapport tevens richting aan interventies, die aansluiten bij de zwakte van de verbinding en het gebrek aan sturing. Het rapport stelt dan ook twee interventies voor:

- Versterk de governance waarbij de focus komt te liggen op eigenaarschap en verantwoording over beheersing van risico's in privacy- en informatiebescherming.
- Versterk de verbinding tussen lijn, ter zake doende professionals en ICT-beheer, zodat een krachtige samenwerking ontstaat.

De effectiviteit van de maatregelen hangt ons inziens af van de wijze waarop deze worden geïmplementeerd, uitgevoerd en geborgd. Door de veranderingen vanuit het domein Bedrijfsvoering door te voeren (en dus niet meer via de huidige concernopgave 'Digitale Overheid') wordt het beveiligingsniveau van de gehele organisatie, op alle domeinen, opgaven en projecten alsook voor het kabinet van de commissaris en Provinciale- en Gedeputeerde Staten op noodzakelijk niveau gebracht. In deze brief richten wij ons dan ook op het programma IV&P dat per 4 maart jl. door domein Bedrijfsvoering wordt opgepakt.

Governance
Per 4 maart jl. is een van de domeinmanagers Bedrijfsvoering verantwoordelijk gemaakt voor de dagelijkse aansturing van het programma IV&P. Hiermee is het hele programma, dus ook het hele team, onder lijnverantwoordelijkheid geplaatst. Met de keuze om het programma IV&P onder te brengen bij het domein Bedrijfsvoering in plaats van onderdeel te laten blijven van de concernopgave Digitale Overheid is een belangrijke stap genomen om de verandering van binnen de ambtelijke organisatie uit te laten plaatsvinden. Vanuit het domein Bedrijfsvoering wordt gewerkt met een programmateam, die onder aansturing van een stuurgroep (brede delegatie) de maatregelen in verbinding met de rest van de organisatie treft opdat het beveiligingsniveau wordt verhoogd.

Om de dagelijkse aansturing goed uit te voeren heeft de domeinmanager een tijdelijk kernteam geformeerd met daarin: opgavemanager Digitale Overheid, programmamanager IV&P, de CISO (*Corporate information security officer*), teamleider Informatievoorziening & Automatisering (I&A), programmamanager samenwerken & dossiers en een adviseur. Deze aansturing is tijdelijk. Er wordt zo snel mogelijk een aanjager gezocht die de dagelijkse aansturing gaat doen. In de zomer zal het programma IV&P volledig in de lijnorganisatie ingebed zijn.

Sinds afgelopen najaar hebben wij de meeste functies in huis die nodig zijn om aan de wettelijke eisen voor IV&P te kunnen gaan voldoen, te weten: een CISO, een Functionaris gegevensbescherming (FG), *Privacy officers* (PO'S), *Security officers* (SO's). Per 1 april jl. is de laatst benodigde functie *Technical Information security officer* (TISO) ingevuld. Dit team zal samen met de Business Informatiemanagers (BIM) middels de wasstraat, zie hieronder, domeinen helpen de IV&P-aangelegenheden op orde te brengen en te houden.

Het team is echter nog niet op orde, omdat nog niet het gewenste aantal medewerkers die functies bekleedt. De BIM-functie moet in elk domein aanwezig zijn, dat is nog niet overal gerealiseerd. Op dit moment staat een vacature staat uit en in de andere domeinen is men bezig met het formuleren van een profiel.

Wasstraat
In aanvulling op de reeds bestaande maatregelen heeft het CMT besloten om de interne processen door een 'wasstraat' te halen. Dit wordt door een domeinmanager van Bedrijfsvoering en een domeinmanager van het primaire proces getrokken. Na een *pilot* met teams die zich vrijwillig hebben aangemeld, wordt het verplicht op basis van dataclassificatie (beschikbaarheid, integriteit en vertrouwelijkheid van data) de wasstraat toe te passen. Daarmee worden de processen met (potentieel) de grootste kwetsbaarheden en risico's als eerste beet gepakt.

Per team worden de werk- en informatieprocessen, waar de teamleider eigenaar van is, doorgelicht. Een groep experts ondersteunt de teams bij het doorlichten en verbeteren van hun werkprocessen op de volgende aspecten: optimalisatie van de uitvoering, digitalisering, het voldoen aan wet- en regelgeving, archivering en of er genoeg benodigde kennis en vaardigheden binnen het team zijn. Daar waar nodig worden verbeteringen doorgevoerd. IV&P is hier een verplicht en prominent onderdeel van. Hiermee worden alle processen van de organisatie in samenhang en systematisch doorgelicht. In het verlengde daarvan worden preventieve technische maatregelen hierbij gestructureerd uitgevoerd. De toets of de Algemene verordening gegevensbescherming (AVG) binnen deze processen is toegepast, is een vast onderdeel.

Wij gebruiken de wasstraat voor IV&P, omdat wij hiermee een instrument in handen hebben, waarbij de informatieveiligheid op de acties die nodig zijn op een structurele wijze in de eigen werkzaamheden van een team geïntegreerd wordt. Hiermee komen wij tegemoet aan wijdverbreide notie dat de noodzaak wel gevoeld wordt, maar de toepassingen in de werkprocessen nog niet helder zijn. De lijnorganisatie nam hierdoor een afwachtende houding aan omdat men ervan uitging dat het programma wel alles inregelde en organiseerde. Met dit instrument gaan wij op een nieuwe wijze, van binnenuit, het eigenaarschap van de lijnorganisatie aanjagen.

Afgesproken is om twee keer per jaar aan u te rapporteren over de voortgang. Om de rapportage overzichtelijker te maken, gaan wij er vanaf de volgende voortgangsrapportage een splitsing in aanbrengen: wij gaan het *Wat* en

Hoe scheiden. Over het *Wat gaan wij doen/wat moet er gebeuren* gaan wij u rapporteren. Over het *Hoe gaan wij dat doen* gaan wij u summier rapporteren, dit nemen wij mee in het *Wat*. Hierdoor worden de rapportages korter en compacter.

Meetbaar/beoogd beleidseffect
Het waarborgen van de integriteit, beschikbaarheid en vertrouwelijkheid van informatie en het versterken van de weerbaarheid voor beveiligingsincidenten van buitenaf en binnenuit.

Financiële consequenties
n.v.t.

Vervolgprocedure/voortgang
Naast berichtgeving over de voortgang bij de reguliere P&C-momenten, is afgesproken dat er per halfjaar een voortgangsrapportage IV&P wordt toegestuurd. Graag sluiten wij aan bij deze momenten om u blijvend te informeren over de voortgang.

Concreet voorliggende vraag aan Statencommissie/Provinciale Staten
Kennis te nemen van deze statenbrief.

Gedeputeerde Staten van Utrecht,

De voorzitter,

De secretaris,