College van Gedeputeerde Staten
statenbrief

Aan Provinciale Staten
Statencommissie Bestuur, Europa en Middelen

DATUM	12-6-2018	REFERENTIE	Victor Roos / Paul Frencken
ONS NUMMER	81D1BB02	DOORKIESNUMMER	3761 / 2501
NUMMER PS	2018BEM56-01	E-MAILADRES	victor.roos@provincie-utrecht.nl paul.frencken@provincie-utrecht.nl
BIJLAGE	1	PORTEFEUILLEHOUDER	Straat

Onderwerp Statenbrief: assessment informatieveiligheid 2017 en rapportage opzet en uitvoering programma informatieveiligheid en privacy

Voorgestelde behandeling: ter informatie

Geachte dames en heren,

Inleiding

Bijgaand treft u aan de rapportage opzet en uitvoering programma informatieveiligheid en privacy (bijlage 1). De directe aanleiding voor het met voorrang starten van dit programma vormde de resultaten van het assessment informatieveiligheid 2017. Middels deze brief wordt u ook over die resultaten geïnformeerd.

Aanleiding/voorgeschiedenis
De provincies hebben sinds 2013 met ondersteuning van het IPO en de Taskforce de provinciale informatie-veiligheid 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 (het zelf borgen van een adequaat niveau) van informatieveiligheid. In het afsprakenkader wordt verwezen naar de Interprovinciale Baseline Informatieveiligheid. Dit betreft een nadere uitwerking van de norm ISO27001 voor provincies. Eén van de afspraken van het convenant betreft verantwoording over dit onderwerp: 1x per 2 jaar een assessment naar het beveiligingsniveau. In 2015 werd dit voor het eerst uitgevoerd (0-meting). Bij de provincie Utrecht zijn sindsdien activiteiten ontplooid, gericht op het bereiken van een adequaat beveiligingsniveau en het verhogen van veilig gedrag van medewerkers. Daarover bent u met voortgangsrapportages geïnformeerd op 31 januari (eerste voortgangsrapportage) en 26 september 2017 (tweede voortgangsrapportage).

Essentie / samenvatting:

<u>Assessment informatieveiligheid 2017</u>
In de sterk digitaliserende maatschappij neemt het belang van informatieveiligheid steeds meer toe door groeiende afhankelijkheid van mobiele apparatuur, netwerken, IT-systemen en clouddiensten die blootstaan aan risico's van uitval, diefstal en cyberaanvallen met soms ontwrichtende impact, als gevolg van de almaar toenemende dreiging van cybercrime. Dit dwingt bedrijven, overheden en burgers blijvend te investeren in digitale weerbaarheid. De afgelopen jaren hebben grote hacks geleid tot het openbaar worden of het verhandelen van enorme hoeveelheden persoonlijke gegevens door criminelen. Daarnaast wordt door grote internetbedrijven op

grote schaal persoonsgegevens verzameld, waardoor de privacy[1] van burgers onder druk staat. De nieuwe EU-verordening AVG[2] moet deze trend keren door hoge eisen te stellen aan de bescherming van persoonsgegevens door organisaties.

In lijn met de afspraak in het convenant interprovinciale regulering informatieveiligheid over verantwoording heeft Concerncontrol het assessment informatieveiligheid gedurende augustus – november 2017 voor de tweede keer uitgevoerd, bijgestaan door externe specialisten. Het assessment geeft inzicht in het informatiebeveiligingsniveau en de implementatiestatus van het beleid informatieveiligheid bij de provincie Utrecht. De bevindingen en de aanbevelingen zijn hieronder samengevat, waarbij onderscheid gemaakt wordt tussen het dashboard informatieveiligheid met procesvolwassenheid en de bevindingen over het organisatiebrede beveiligingsniveau.

Uit de meting van de procesvolwassenheid en de bevindingen van het assessment komt naar voren dat het bewustzijn en veilig gedrag weliswaar zijn toegenomen, maar dat de provincie Utrecht haar informatieveiligheid nog niet kan reguleren zoals bedoeld in het convenant van 2014.

Voor bestuur en management is het dashboard informatieveiligheid 2017 opgeleverd waarin is opgenomen welk niveau van procesvolwassenheid bij informatieveiligheid is bereikt (schaal 0 tot 5). De organisatie heeft in het plan informatieveiligheid van 2016 en de eerste voortgangsrapportage naar GS/PS aangegeven te willen groeien naar niveau 2-3. De huidige status is:
De procesvolwassenheid van informatieveiligheid bij de PU beweegt zich overwegend op niveau 1–Initieel (ook wel ad-hoc genoemd). Niveau 2-Herhaalbaar is inmiddels voor de onderdelen Leerstrategie en Aansluiten bereikt.

De belangrijkste bevindingen over het organisatiebrede beveiligingsniveau zijn:

a. De governance (sturing, beheersing, verantwoording) op het gebied van informatieveiligheid staat nog niet stevig.
b. Een gebrek aan verantwoordelijkheid voor informatieveiligheid, het benoemen en uitdragen van eigenaarschap.
c. Een gebrek aan urgentie voor informatieveiligheid, in relatie tot de ontwikkeling van dreigingen en nieuwe wetgeving (nakomen afspraken convenant, voorbereiding op AVG).
d. Toenemende aandacht voor veilig gedrag. Denken en handelen vanuit de afdeling of team in plaats van op concernniveau of ketenniveau.
e. In de keten (partners, dienstverleners) wordt informatieveiligheid gekenmerkt door vertrouwen, ontbrekende afspraken en een gebrek aan regie.
f. De samenhang tussen beleid, architectuur en inrichtingseisen voor beveiligingsmaatregelen is niet duidelijk.

De aanbevelingen voor het verbeteren van het organisatiebrede beveiligingsniveau zijn:

a. Versterk en formaliseer de governance van informatieveiligheid met aandacht voor sturing, beheersing en verantwoording.
b. Zorg voor een eenduidige methodiek voor beheersing van informatieveiligheidsrisico's en neem managers hierin mee zodat zij hun verantwoordelijkheid kunnen nemen en daarover rapporteren.
c. Maak een inhaalslag om alsnog aan de afspraken uit het convenant te gaan voldoen. Reguleer informatieveiligheid door processen naar een hoger volwassenheidsniveau te brengen en te sturen op risicobeheersing en tijdige compliance met nieuwe wet- en regelgeving, in het bijzonder de AVG.
d. Maak na bewustwording de volgende stap naar het versterken van de bekwaamheid en reguleer dit door op concernniveau hieraan sturing te geven.
e. Versterk bewustwording van informatieveiligheidsrisico's in de keten en de mogelijkheden om deze te beheersen. Breng en houd centraal in beeld welke provinciale gegevens buiten worden verwerkt en hoe deze worden beschermd.
f. Breng samenhang aan in beleid, architectuur en inrichting van beveiligingsmaatregelen en valideer dat de beveiligingsmaatregelen adequaat functioneren.

<u>Programma informatieveiligheid en privacy</u>
De bevindingen uit het assessment zijn zorgwekkend en reden tot urgentie. Naar aanleiding van het assessment heeft de algemeen directeur opdracht gekregen om prioritair een programma informatieveiligheid en privacy uit te voeren. De stuurgroep dient als taskforce. Onder leiding van de algemeen directeur heeft deze taskforce de opdracht om met voorrang de AVG te implementeren, zo spoedig mogelijk de informatieveiligheid te verbeteren, de doelstellingen van de provincie Utrecht te realiseren en te kunnen voldoen aan de wettelijke verplichtingen. Daarbij worden de aanbevelingen uit het assessment expliciet meegenomen.

---

[1] Voor het borgen van de privacy (grondwettelijk recht) moeten persoonsgegevens goed worden beschermd en dat maakt onderdeel uit van informatieveiligheid.
[2] Algemene verordening gegevensbescherming: nieuwe wetgeving m.b.t. de bescherming van persoonsgegevens, per 25 mei 2018 van toepassing.

Het programma is er op gericht om voor 25 mei 2018 belangrijke stappen, zoals genoemd door de Autoriteit Persoonsgegevens, te hebben gezet. Dit is inmiddels gebeurd. In de maanden na 25 mei wordt de inbedding in de organisatie verder voltooid. De provincie Utrecht is op die wijze in staat om structureel te voldoen aan de AVG.
Het programma levert ook een voorstel over een governance op het gebied van informatieveiligheid en privacy, waarmee de staande organisatie in control kan zijn en blijven op informatieveiligheid en privacy en op basis van pdca-cycli en risicomanagement kan door ontwikkelen.
Het programma draagt ook zorg voor een masterplan met een aanpak om informatieveiligheid (MIBP) structureel te verbeteren en stapsgewijs toe te werken naar ISO27001 certificering. Daarbij worden ook aanbevelingen en verbeterpunten uit eerdere (externe) onderzoeken en audits meegenomen.
Ook richt het programmateam zich op het verbeteren van informatiebeveiliging en privacy op korte termijn, door te adviseren over het treffen van (aanvullende) maatregelen of door actuele zaken aanvullend op te nemen in het MIBP. Daartoe wordt op korte termijn ook een healthcheck uitgevoerd op de systemen.
Het programma Informatieveiligheid en Privacy omvat aldus vier programmalijnen:

I. De implementatie AVG;
II. Het inrichten van de governance voor informatieveiligheid en privacy binnen de provincie Utrecht;
III. Het opstellen Masterplan InformatieBeveiliging en Privacy (MIBP);
IV. Het gestructureerd in control komen op het gebied van informatieveiligheid en het snel en adequaat oppakken en afhandelen van datalekken en/of security-incidenten indien deze zich voordoen.

De uitvoering van het programma verloopt volgens schema.

Meetbaar / beoogd beleidseffect
Met het assessment wordt verantwoording afgelegd over het informatiebeveiligingsniveau van de provincie Utrecht en de implementatiestatus van het beleid voor informatieveiligheid. De resultaten worden gebruikt om de ontwikkeling op het vlak van informatieveiligheid te volgen en bij te sturen, gericht op het in standhouden van een adequaat informatiebeveiligingsniveau.

Het thans gestarte programma informatieveiligheid en privacy beoogt een versnelde implementatie van de doelstellingen van de provincie Utrecht en wettelijke verplichtingen op het gebied van informatieveiligheid en privacy. De rapportage in bijlage 1 geeft de opzet en uitvoering tot dusver van het programma informatieveiligheid en privacy weer.

Wettelijke grondslag
- artikel 158, eerste lid, onder a, van de Provinciewet
- Algemene Verordening Gegevensbescherming (AVG)
- Uitvoeringswet Algemene Verordening Gegevensbescherming

Financiële consequenties
In de concept kadernota zijn middelen opgenomen noodzakelijk voor uitvoering van het programma informatieveiligheid en privacy.

Vervolgprocedure/voortgang
In december volgt de volgende rapportage over de uitvoering van het programma informatieveiligheid en privacy.
Het volgende assessment informatieveiligheid staat gepland voor 2019.

Concreet voorliggende vraag aan statencommissie / Provinciale Staten
Kennis nemen van deze brief en rapportage opzet en uitvoering programma informatieveiligheid en privacy.

Gedeputeerde Staten van Utrecht,

De voorzitter,
De secretaris,