26-5-2016 3320

gemeente Brunssum

Oplegnotitie Quick Scan "Brunssum op weg naar BIG, digitale veiligheid Brunssum" van de rekenkamercommissie Brunssum
Registratiekenmerk 651978
Gemeenteblad nr. 2016/13

Rol van de raad
De raad krijgt dit raadsvoorstel voorgelegd naar aanleiding van de behandeling van de Quick Scan in de auditcommissie op 23 februari 2016 en de commissie Middelen van 12 april 2016, om in het kader van haar controlerende taak waar nodig bij te sturen en nieuwe kaders te stellen.

Context van het raadsvoorstel
In deze Quick Scan heeft de Rekenkamercommissie Brunssum een onderzoek uitgevoerd naar digitale veiligheid. Onder andere vanwege het sociale domein gaan gemeenten, en hun partners, steeds meer met digitale (vertrouwelijke) gegevens om. Veel bedrijfsvoeringsprocessen verlopen digitaal. Daardoor worden bedrijfsvoeringsprocessen en het beheren en verwerken van gegevens kwetsbaar, zoals blijkt uit recente incidenten.
De gemeente Brunssum heeft al veel gedaan op het gebied van informatieveiligheid en er is aandacht voor dit onderwerp. Het onderzoek door de rekenkamercommissie moet vooral gezien worden als 'wake-up call' en/of bewustwording, mede vanwege de verscherpte wetgeving op het gebied van de privacywetgeving en het melden van datalekken

Opties van het raadsvoorstel op hoofdlijnen
De rekenkamercommissie heeft op basis van de Quick Scan naar de digitale veiligheid in Brunssum een tweetal aanbevelingen geformuleerd:
1. Bespreek als gemeenteraad het integraal implementatieplan en voorzie de implementatie van voldoende middelen en formatie.
2. Benoem als gemeenteraad informatieveiligheid tot een kritieke succesfactor en geef opdracht aan het college informatieveiligheid vanaf 2016 op te nemen in de informatie die vanuit de P&C-cyclus periodiek naar de raad wordt gestuurd.

De rekenkamercommissie heeft tevens een viertal aansporingen geformuleerd, mede omdat het ambtelijk apparaat heeft aangegeven met deze aandachtspunten aan de slag te zijn of in 2016 aan de slag te gaan.
1. Stel uiterlijk eind 1e kwartaal 2016 op basis van de actualisatie en risicoanalyse een integraal implementatieplan informatiebeveiliging op;
2. Stel uiterlijk eind 1e kwartaal 2016 een uitwijktestplan op;
3. Maak in 2016 afspraken met externe partijen die voor de gemeente informatie beheren en/of bewerken, op basis van de bewerkersovereenkomst van IBD;
4. Draag er zorg voor dat de vierde fase aansluiting op de Informatiebeveiligingsdienst voor gemeenten (IBD) wordt gerealiseerd in 2016, door middel van het doorgeven van de in gebruik zijnde hard- en software.

Financiële/personele/juridische gevolgen? Ja, indien de aanbevelingen worden overgenomen.

Is achteraf meetbaar of de doelstellingen gehaald zijn? Ja, indien aanbevelingen worden overgenomen middels het integraal implementatieplan informatieveiligheid, de P&C cyclus en raadsinformatiebrieven.

Is er een tijdpad bijgevoegd? Ja, de geformuleerde aansporingen en aanbevelingen worden gerealiseerd in 2016.

Zijn er bijlagen bijgevoegd of ter inzage? Quick Scan Brunssum op weg naar BIG; Digitale veiligheid Brunssum (627609)

26-5-2016 3320

Raadsvoorstel

Collegeverg. d.d.	:	
Registratiekenmerk		651978
Gemeenteblad nr.	:	2016/13
Dienst/Afdeling	:	Griffie
Behandelvoorstelnr.	:	651978
Portefeuillehouder	:	C.J.C.P. de Rijck
Onderwerp	:	Quick Scan "Brunssum op weg naar BIG, digitale veiligheid Brunssum" van de rekenkamercommissie Brunssum
Raadsverg. d.d.	:	26-4-2016
Uiterlijke beslisdatum	:	(Motivering, wettelijke verplichting c.q. toezegging)

Aan de raad.

Voorstel/ambtelijk advies

1. De aanbevelingen van de Quick Scan " Brunssum op weg naar BIG, digitale veiligheid Brunssum " van de Rekenkamerscommissie over te nemen;
2. Het college de opdracht te geven het integraal implementatieplan informatieveiligheid in 2016 aan de raad voor te leggen;
3. Het college de opdracht te geven informatieveiligheid vanaf 2016 op te nemen in de informatie die vanuit de P&C-cyclus periodiek naar de raad wordt gestuurd.

Inleiding

In 2013 hebben gemeenten zich verplicht te werken aan verbetering van de digitale veiligheid bij gemeenten. Ondersteund door VNG en het Rijk, hebben gemeenten daartoe de Baseline Informatiebeveiliging Gemeenten (BIG) opgesteld. Deze formuleert op strategisch en tactisch niveau eisen waaraan informatiebeveiliging bij gemeenten moet voldoen.
Vanaf 2014 heeft de Auditcommissie meerdere malen aandacht gevraagd voor de digitale veiligheid bij de gemeente Brunssum. In het jaarplan 2015 heeft de Rekenkamercommissie Brunssum een Quick Scan opgenomen met 'Digitale Veiligheid' als onderwerp. De Rekenkamercommissie Brunssum heeft, op basis van een vragenlijst van de Rekenkamer van de gemeente Den Haag en de Taskforce Bestuur & Informatieveiligheid Dienstverlening (Taskforce BID), tien vragen voorgelegd aan de ambtelijke organisatie. De vragen gaan in op belangrijke aspecten van de BIG, teneinde een beeld te krijgen van de implementatie van beleid rond digitale veiligheid in het gemeentelijk apparaat van Brunssum.
Met de voorliggende Quick Scan rapporteert de rekenkamercommissies Brunssum naar de raad.

Probleemstelling/Doelstelling

Informatieveiligheid is binnen gemeenten verscherpt op het netvlies gekomen na crises zoals die in het nieuws kwamen bij DigiNotar en Lektober. Deze hebben aangetoond dat gemeenten digitaal kwetsbaar zijn. Wat gebeurt er bijvoorbeeld als gevoelige informatie op straat komt te liggen? Of als de dienstverlening aan burgers niet meer mogelijk is? Naast financiële, juridische en technische gevolgen kunnen deze crises het imago van de gemeente en de privacy van de burgers aantasten.
Het beeld dat uit de Quick Scan naar voren komt is dat Brunssum stuurt op digitale veiligheid en dat belangrijke stappen op weg naar een digitaal veiligheidsbeleid op basis van BIG gezet zijn. Echter, de stap om het beleid risico-gebaseerd en integraal op te zetten, zoals de BIG dat vereist, moet nog gezet worden.

Kaderstelling

De auditcommissie heeft op 23 februari 2016 de Quick Scan besproken en besloten de aanbevelingen als besluit aan de raad voor te leggen. Het is geen traditioneel oordeelvormend onderzoek van de Rekenkamercommissie. De Quick Scan is erop gericht in beperkte mate een inzicht te geven in de stand van zaken rond de implementatie van de BIG. De Rekenkamercommissie hanteert wel een referentiekader om de antwoorden te plaatsen. Deze zijn gegeven in de Strategische en Tactische variant van de BIG.

De Rekenkamercommissie heeft de volgende 10 vragen uitgezet bij de ambtelijke organisatie:

1. Stuurt de gemeente op de afspraken die benoemd zijn in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de BIG en zo ja hoe?
2. Heeft de gemeente de risico's op informatieveiligheidsvlak in een Informatiebeveiligingsplan benoemd, is helder in hoeverre risico's beheerst dan wel geaccepteerd worden, inclusief de bijbehorende maatregelen uit de BIG, en op

26-5-2016 3320

welk niveau is dit plan vastgesteld (ambtelijke organisatie, college, raad)?

3. Rapporteert en bespreekt de organisatie het functioneren van de cyclus van informatieveiligheid op management- en bestuursniveau (college en raad)? Is zij daarover transparant richting haar ketenpartners door via waarstaatjegemeente.nl te rapporteren over informatieveiligheid? Zijn er nog andere wijzen van rapporteren?
4. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?
5. Kent de gemeente de leveranciers en partners waarmee ze samenwerkt en toetst zij die ook op informatieveiligheidsaspecten en zo ja hoe?
6. Is de gemeente 'officieel' aangesloten bij de Informatiebeveiligingsdienst voor gemeenten (IBD) en wat is de exacte status van deze aansluiting?
7. Weet de organisatie hoe te handelen bij een (ernstig) informatieveiligheidsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet dit eruit?
8. Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatieveiligheid via peer reviews, audits of zelfassessments? En wordt over het functioneren van de cyclus van informatieveiligheid gerapporteerd aan de raad? Hoe ziet deze toets eruit?
9. Zijn de beleidsuitgangspunten nog valide of zijn er interne of externe ontwikkelingen die leiden tot heroverwegingen van de gemeentelijke risico-inschattingen? Indien dit laatste het geval is, wat zijn dan deze ontwikkelingen?
10. Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houdt de gemeente kennis vast en bouwt zij hierop door?

De bevindingen uit het onderzoek afgezet tegen het normenkader resulteerden in de volgende conclusies. De cursief gedrukte tekst geeft het kader van de betreffende conclusie aan.

1. *Stuurt de gemeente op de afspraken die benoemd zijn in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de BIG en zo ja hoe?*

De Rekenkamercommissie constateert dat er wordt gewerkt aan een actualisering door het lijnmanagement, maar dat er nog geen integraal implementatieplan informatieveiligheid ter vaststelling bij het college voorligt. De verwachting is dat het implementatieplan eind eerste kwartaal 2016 gereed zal zijn. Wanneer deze gereed is loopt de organisatie in de pas met de afspraken die opgenomen zijn in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'.
Informatieveiligheid is niet alleen maar een bedrijfsvoeringskwestie. Informatieveiligheid is aan te merken als kritieke succesfactor voor de gemeentelijke dienstverlening en daar zullen strategische en kaderstellende keuzen op gemaakt moeten worden. De gemeenteraad zal dan ook in zijn kaderstellende rol aangeschakeld moeten zijn bij de voortgang op de implementatie van de maatregelen die in het kader van de BIG zijn afgesproken. Bij een integraal implementatieplan op informatiebeveiliging behoren voldoende formatie en middelen gereserveerd te worden voor de uitvoering van het beleid.

Aanbeveling 1 Bespreek als gemeenteraad het integraal implementatieplan dat eind eerste kwartaal 2016 gereed komt en voorzie de implementatie van voldoende middelen en formatie.

2. *Heeft de gemeente de risico's op informatieveiligheidsvlak in een Informatiebeveiligingsplan benoemd, is helder in hoeverre risico's beheerst dan wel geaccepteerd worden, inclusief de bijbehorende maatregelen uit de BIG, en op welk niveau is dit plan vastgesteld (ambtelijke organisatie, college, raad)?*

De organisatie geeft aan dat er een informatiebeveiligingsplan is dat door het college is vastgesteld. Daarin zijn risico's benoemd. De beheersingsmaatregelen worden besproken in het Beveiligingsforum. Het forum controleert de voortgang op informatiebeveiliging en monitort de audits, zelftests en assessments en de opvolging daarvan. De Rekenkamercommissie heeft gevraagd inzage te krijgen in het informatiebeveiligingsplan, maar deze is niet ontvangen. De Rekenkamercommissie kan zich daar dan ook geen oordeel over vormen.

3. *Rapporteert en bespreekt de organisatie het functioneren van de cyclus van informatieveiligheid op management- en bestuursniveau (college en raad)? Is zij daarover transparant richting haar ketenpartners door via waarstaatjegemeente.nl te rapporteren over informatieveiligheid? Zijn er nog andere wijzen van rapporteren?*

Volgens de verstrekte informatie is rapportage via waarstaatjegemeente.nl in het verleden wel gebeurd. Na de actualisatie van het informatieveiligheidsbeleid wordt overlegd of rapportage op die site weer mogelijk is, zodat ketenpartners en burgers de voortgang op informatieveiligheid kunnen nagaan.
In de actualisering van het beleid op informatieveiligheid wil de organisatie de betrokkenheid van het gemeentebestuur

26-5-2016 3320

meenemen. Het Beveiligingsforum komt periodiek bijeen en bespreekt de voortgang van de implementatie van de maatregelen op informatieveiligheid. Het ligt in de bedoeling het college te informeren op basis van de verslagen van het Beveiligingsforum. Het jaarlijkse DigID assessment wordt aan Logius toegezonden en teruggekoppeld aan het Beveiligingsforum. De zelfevaluaties op deelgebieden worden besproken en vastgesteld in het college. Deze beperken zich vooralsnog tot informeren van het college op de resultaten van onderzoeken en audits. Daaronder vallen de SUWINET-steekproef, de zelfevaluaties van de Basisregistratie Adressen en Gebouwen (BAG) en Paspoorten en Nederlandse Identiteitskaarten (PNIK).
De gemeenteraad is nog niet structureel aangesloten op het informatiebeveiligingsbeleid. Het ligt volgens de ambtenaren in de bedoeling de raad over de beleidsaanpassingen via een raadsinformatiebrief te informeren en de resultaten op de audits, zelfevaluaties en assessments mee te delen. Op dit moment wordt in de P&C-cyclus op onderdelen over informatieveiligheid aan de raad gerapporteerd bij het onderdeel ICT. In het vervolg wordt het onderwerp als item opgenomen in de bedrijfsvoeringsparagraaf binnen de P&C-cyclus. De rekenkamercommissie vraagt zich af of deze informatie voldoende tegemoet komt aan de informatiebehoefte van de raad. Informatieveiligheid is een kritieke succesfactor voor de gemeentelijke dienstverlening, en het is de taak en rol van de gemeenteraad de voortgang op de implementatie van maatregelen hierop te controleren.

Aanbeveling 2. Benoem als gemeenteraad informatieveiligheid tot een kritieke succesfactor voor de gemeentelijke dienstverlening en geef opdracht aan het college vanaf 2016 informatieveiligheid op te nemen in de informatie die vanuit de P&C-cyclus periodiek naar de raad wordt gestuurd.

4. *Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?*

Met betrekking tot borging van de continuïteit van de (digitale) dienstverlening, neemt de gemeente Brunssum deel aan de gemeenschappelijke regeling Parkstad-IT (PIT).
PIT beschikt over volledig gespiegeld datacenter waarbij een volledige uitwijk van alle systemen mogelijk is. Er zijn geen decentrale systemen die niet onder PIT vallen.
De uitwijkmogelijkheid is medio 2014 op beperkte schaal getest. De Rekenkamercommissie constateert dat daarmee burgers, instellingen en bedrijven wat betreft dienstverlening waarschijnlijk weinig tot niets hoeven te merken van een uitval of storing van de ICT.

Desondanks spoort de Rekenkamercommissie aan om de uitwijkmogelijkheden uitgebreider en grondiger dan tot nu toe te testen, teneinde risico's op de continuïteit zoveel mogelijk te voorkomen. Voor 2016 staat in de planning een uitwijktestplan op te stellen en deze bij Parkstad-IT onder te brengen.
De gemeenteraad kan de voortgang hierop monitoren als aanbeveling 2 wordt opgevolgd.

5. *Kent de gemeente de leveranciers en partners waarmee ze samenwerkt en toetst zij die ook op informatieveiligheidsaspecten en zo ja hoe?*

PIT is een belangrijke partner van de gemeente op het gebied van digitale informatieveiligheid. Deze wordt zelf geaudit en de resultaten van de audits worden aan de deelnemende gemeenten beschikbaar gesteld. Bij andere partners op terrein van ICT, zoals leveranciers van informatiesystemen, kan een accountantsverklaring gevraagd worden. Onduidelijk is of het opvragen van accountantsverklaringen standaard gebeurt en of het nakomen van afspraken over informatieveiligheid regelmatig getoetst wordt. Dit nalaten kan een risico op informatieveiligheid inhouden. Voor 2016 staat in de planning dat ketenpartners, die met de gemeente Brunssum op het gebied van informatieveiligheid te maken hebben, contact wordt opgenomen en afspraken worden gepland.

De Rekenkamercommissie spoort deze actie aan en geeft daarbij in overweging om met externe partijen afspraken te maken die gebaseerd zijn op de bewerkersovereenkomst die IBD als model aanbiedt.

6. *Is de gemeente 'officieel' aangesloten bij de Informatiebeveiligingsdienst voor gemeenten (IBD) en wat is de exacte status van deze aansluiting?*

Vanaf 11 februari 2014 is de gemeente Brunssum voor de eerste twee fasen aangesloten op de IBD.
De aansluiting op IBD fase 3 is op 24 november 2014 gerealiseerd.
De laatste fase, aanleveren van de zogenoemde ICT-foto, met de in gebruik zijnde hard- en software is nog niet gerealiseerd. Door volledige aansluiting kan de IBD de gemeente voorzien van op maat van meldingen en adviezen die toegesneden zijn op de aanwezige hard- en software.

26-5-2016 3320

De Rekenkamercommissie acht volledige aansluiting op IBD nastrevenswaardig en spoort de gemeente aan om ook de vierde fase van aansluiting in 2016 te realiseren.

7. *Weet de organisatie hoe te handelen bij een (ernstig) informatieveiligheidsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet dit eruit?*

De BOL-gemeenten, en daarmee ook de gemeente Brunssum, beschikken over een procedure voor het melden van incidenten op informatieveiligheid. Deze procedure is aan college, managementteam en medewerkers tijdens een zogenoemde bewustwordingsfase geïntroduceerd, via bijeenkomsten, mail en artikelen op intranet.
De procedure bestaat in eerste instantie uit de registratie van het incident door de beveiligingsfunctionaris. Daardoor weet de functionaris of bepaalde voorvallen incidenteel of structureel voorkomen. Als er aanleiding toe bestaat beziet de functionaris of een andere partij een rol moet spelen bij de afhandeling van het incident, zoals de privacyfunctionaris.
De incidenten worden geëvalueerd, met het doel ervan te leren.
Het registratiesysteem kent de volgende punten:

- het maken van een BOL-brede rapportage informatiebeveiligingsincidenten;
- het instellen van een meldplicht voor dergelijke incidenten. Niet uit repressief ('Wie is de schuldige?'), maar uit preventief oogpunt ('Wat kunnen we ervan leren?');
- het informeren van alle medewerkers over deze meldplicht;
- het maken van één BOL-brede procedure voor het afhandelen van meldingen over incidenten, met daaraan gekoppeld een evaluatie.

De Rekenkamercommissie spoort aan om deze procedure op korte termijn op te zetten, mede met het oog op de meldplicht datalekken die vanaf 1-1-2016 in werking is getreden. De procedure daarop is met Parkstad-IT opgepakt

8. *Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatieveiligheid via peer reviews, audits of zelfassessments? En wordt over het functioneren van de cyclus van informatieveiligheid gerapporteerd aan de raad? Hoe ziet deze toets eruit?*

De afgelopen twee jaar hebben accountants bij de jaarlijkse controle een ICT-survey uitgevoerd. Deze beperkt zich evenwel grotendeels tot het financiële informatiesysteem. Daarbij komen volgens de ambtelijke organisatie generieke processen rond toegangscontrole, autorisatie, beveiliging, beleid enz. aan bod. Daarnaast staat voor 2016 een PEN-test bij Parkstad-IT in de planning, ter ondersteuning van de accountantsverklaring.

Tevens worden jaarlijks twee zelfevaluaties gedaan, op de Basisregistratie Personen (BRP) en Paspoorten en Nederlandse Identiteitskaarten (PNIK). En audits op de Basisregistratie Adressen en Gebouwen (BAG) en de steekproef SUWINET. Deze audits richten zich op één specifieke gemeentelijke taak, maar hebben volgens de gemeentelijke organisatie generieke elementen die het volledige informatiebeveiligingsbeleid betreffen. Tot slot zijn er de jaarlijkse assessments van de DigID-loketten, waarover aan Logius wordt gerapporteerd. Als Logius geen assessmentrapportage van de gemeente ontvangt wordt het DigID-loket afgesloten.

Het Beveiligingsforum, waarin het lijnmanagement vertegenwoordigd is, wordt gerapporteerd over het functioneren en de voortgang van de informatiebeveiliging. De gemeenteraad wordt daarover via een raadsinformatiebrief geïnformeerd, maar niet regulier inde P&C-cyclus.

9. *Zijn de beleidsuitgangspunten nog valide of zijn er interne of externe ontwikkelingen die leiden tot heroverwegingen van de gemeentelijke risico-inschattingen? Indien dit laatste het geval is, wat zijn dan deze ontwikkelingen?*

In de planning voor 2016 staat het in kaart brengen van de Europese privacyregelgeving en beschrijving van de impact daarvan op het gemeentelijk informatieveiligheidsbeleid.

De bijstelling van het beleid zal in het eerste kwartaal van 2016 geschieden in het kader van de actualisatieslag, risicogebaseerd en door de lijn opgesteld. Indien dat is afgerond is te verwachten dat de beleidsuitgangspunten up to date zijn en conform de BIG opgesteld.

10. *Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houdt de gemeente kennis vast en bouwt zij hierop door?*

In het informatiebeveiligingsbeleid uit 2012 is in een aparte paragraaf aandacht besteed aan het leren, met als doel de beheersmaatregelen te verbeteren. Door middel van een bewustwordingsfase is getracht medewerkers, managementteam en college te doordringen van het belang van het onderwerp informatieveiligheid. Door ontbrekende middelen is er

26-5-2016 3320

volgens de antwoorden van de ambtenaren te weinig aandacht gegenereerd om het gewenste leereffect op te bouwen en te borgen.
De urgentie voor het onderwerp is hernieuwd onder de aandacht gebracht van het managementteam en het college, waarbij het verzoek is gedaan voldoende middelen beschikbaar te stellen. Zie aanbeveling 1.
Volgens de antwoorden van de ambtenaren zal het nieuwe beveiligingsbeleid een nieuw startpunt opleveren om informatieveiligheid onder de aandacht te brengen van alle geledingen.
In de fase van de ambtelijke hoor en wederhoor is aangegeven dat Brunssum sinds 2008 beschikt over een vergaand integriteitsbeleid. Dat is in 2012 geactualiseerd is, onder andere met aspecten op informatiebeveiliging. Voor 2016 staat op de rol dat in samenwerking met het Beveiligingsforum een integriteitsplan op te stellen. Iedere medewerker moet bij in dienst treden een VOG overleggen, waarbij informatieveiligheid wordt meegenomen. Dat geldt ook voor de tijdelijke medewerkers. In 2013 is een bewustwordingscampagne gevoerd. Via het Intranet worden medewerkers bewust gemaakt van afspraken op informatiebeveiliging, meestal naar aanleiding van incidenten.

Op grond van bovenstaande heeft de rekenkamercommissie een tweetal aanbevelingen en een viertal aansporingen geformuleerd, mede omdat het ambtelijk apparaat heeft aangegeven met deze aandachtspunten aan de slag te zijn of in 2016 aan de slag te gaan.

De raad beslist per aanbeveling om de betreffende aanbeveling wel of niet over te nemen. De aanbevelingen zijn de volgende:

1. Bespreek als gemeenteraad het integraal implementatieplan en voorzie de implementatie van voldoende middelen en formatie.
2. Benoem als gemeenteraad informatieveiligheid tot een kritieke succesfactor en geef opdracht aan het college informatieveiligheid vanaf 2016 op te nemen in de informatie die vanuit de P&C-cyclus periodiek naar de raad wordt gestuurd.

De aansporingen zijn de volgende:

1. Stel uiterlijk eind 1e kwartaal 2016 op basis van de actualisatie en risicoanalyse een integraal implementatieplan informatiebeveiliging op;
2. Stel uiterlijk eind 1e kwartaal 2016 een uitwijktestplan op;
3. Maak in 2016 afspraken met externe partijen die voor de gemeente informatie beheren en/of bewerken, op basis van de bewerkersovereenkomst van IBD;
4. Draag er zorg voor dat de vierde fase aansluiting op de Informatiebeveiligingsdienst voor gemeenten (IBD) wordt

Uitvoering
Na besluitvorming door de raad op 26 april 2016, zal de raad in 2016 het implementatieplan informatieveiligheid bespreken. Het is aan het college om naar de raad terug te koppelen hoe zij deze aanbevelingen uitvoert.

Raming van de gevolgen in geld en menskracht
Of er gevolgen in geld of menskracht zijn, hangt af van welke aanbevelingen worden overgenomen. Het overnemen van aanbevelingen houdt in dat het college bepaalde stukken opstelt en dat hiervoor ambtelijke capaciteit wordt ingezet.

Verdere procedure en momenten van verantwoording
Het college zal tussentijds via de auditcommissie de stand van zaken van de uitvoering van de aanbevelingen en aandachtspunten terugkoppelen.

Namens de Auditcommissie,

Voorzitter H.J.S.M. Broers

Bijlage:
Quick Scan "Brunssum op weg naar BIG; Digitale veiligheid Brunssum"

26-5-2016 3320

Raadsbesluit

Gemeenteblad nr. : 2016/13
Dienst/Afdeling : Griffie
Registratiekenmerk : 651978

De Raad der Gemeente Brunssum;

gelet op het bepaalde in de Gemeentewet, artikel 81 oa
gelet op het bepaalde in de verordening Rekenkamercommissie Brunssum 2013, artikel 9, lid 1 en artikel 10, lid 3;
gelezen het voorstel van de rekenkamercommissie Brunssum;
gehoord de Auditcommissie van 23 februari 2016;
gehoord de commissie Middelen van 12 april 2016.

Besluit:

1. De aanbevelingen van de Quick Scan " Brunssum op weg naar BIG, digitale veiligheid Brunssum " van de Rekenkamercommissie over te nemen;
2. Het college de opdracht te geven het integraal implementatieplan informatieveiligheid in 2016 aan de raad voor te leggen;
3. Het college de opdracht te geven informatieveiligheid vanaf 2016 op te nemen in de informatie die vanuit de P&C-cyclus periodiek naar de raad wordt gestuurd.

Aldus vastgesteld in de openbare vergadering van 26 APR. 2016

De Raad voornoemd,

voorzitter.

griffier.