Brunssum op weg naar BIG

Digitale veiligheid Brunssum

CONCEPT

Rekenkamercommissie Brunssum

Quick Scan, januari 2016

Drs. E.J.M. Lemmens, voorzitter Rekenkamercommissie Brunssum

Inhoud

Samenvatting 3
1 Inleiding 5
2 Aanpak 5
3 Vraag en antwoord 7

Samenvatting

In deze Quick Scan heeft de Rekenkamercommissie Brunssum een onderzoek uitgevoerd naar digitale veiligheid. Gemeenten, en hun partners, gaan met digitale (vertrouwelijke) gegevens om en veel bedrijfsvoeringsprocessen verlopen digitaal. Dat is kwetsbaar.

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. 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. De aanpak voor het korte onderzoek voor deze Quick Scan is in hoofdstuk 2 geschetst. In dat hoofdstuk zijn de tien onderzoeksvragen opgenomen. In hoofdstuk 3 worden de onderzoeksvragen beantwoord.

Dit onderzoek is een Quick Scan en geen diepgravend onderzoek. De Rekenkamercommissie beoordeelt het beleid op informatieveiligheid door de gemeente globaal en voornamelijk op papier. Dat leidt tot een aantal aandachtspunten of aansporingen, en twee aanbevelingen die erop gericht zijn de gemeenteraad op het beleid inzake informatieveiligheid aan te schakelen.

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. De Rekenkamercommissie formuleert de volgende aansporingen, daar het ambtelijk apparaat aan heeft gegeven op deze aandachtspunten aan de slag te zijn of van plan is in 2016 aan de slag te gaan:

- Stel uiterlijk eind 1e kwartaal 2016 op basis van de actualisatie en risicoanalyse een integraal implementatieplan informatiebeveiliging op;
- Stel uiterlijk eind 1e kwartaal 2016 een uitwijktestplan op;
- Maak in 2016 afspraken met externe partijen die voor de gemeente informatie beheren en/of bewerken, op basis van de bewerkersovereenkomst van IBD;
- 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.

Informatieveiligheid wordt opgevat als een hoog risico. De kans op incidenten is, bij naleving van de procedures en implementatie van de BIG laag, maar als incidenten zich voordoen is de impact zeer hoog. En deze impact doet zich voor op terrein van financiën, privacy en reputatie. Daarmee is informatieveiligheid niet alleen een uitvoeringsaangelegenheid en een thema op het gebied van uitsluitend bedrijfsvoering, maar van strategisch belang en een beleidskwestie. De Rekenkamer-commissie beveelt aan om de gemeenteraad aangeschakeld te laten zijn op de voortgang van de maatregelen op informatieveiligheid.

Daartoe heeft de Rekenkamercommissie de volgende twee aanbevelingen geformuleerd:

Aanbeveling 1. Bespreek als gemeenteraad het integraal implementatieplan en voorzie de implementatie van voldoende middelen en formatie.

Aanbeveling 2. Benoem als gemeenteraad informatieveiligheid tot een kritieke succesfactor[1] 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.

Toelichting op de aanbevelingen: Sturing op en borging van informatieveiligheid kan beschouwd worden als een essentieel element voor de continuïteit, kwaliteit en betrouwbaarheid van de gemeentelijke dienstverlening. De rekenkamer beveelt de raad aan dit gegeven te erkennen en informatieveiligheid als kritieke succesfactor aan te laten merken. De informatie die de raad nu eenmaal per jaar krijgt is te summier bevonden om de raad op dit belangrijke thema aangeschakeld te laten zijn. Te denken is aan opname van een aantal kengegevens in de raadsrapportages in de reguliere P&C-cyclus. Zoals het aantal ernstige en minder ernstige incidenten op informatiebeveiliging, of opvolging is gegeven aan de ernstige incidenten, of de audits en zelftesten afgehandeld zijn, geïmplementeerde maatregelen van de BIG, enz.

Indien de 2 aanbevelingen worden opgevolgd, kan de raad de verdere stappen in de implementatie van de BIG volgen, inclusief de opvolging van de aansporingen.

[1] Een kritieke succesfactor is een kenmerk van de organisatie of van de omgeving, dat essentieel is voor de levensvatbaarheid en het succes van die organisatie. Dat kan zowel positief als negatief zijn. In hoofdzaak gaat het erom dat iets zo belangrijk is dat de organisatie er extra aandacht aan moet besteden. Lees: het moeten besturen op strategisch niveau.

1 Inleiding

Informatieveiligheid is binnen gemeenten verscherpt op het netvlies gekomen na crises zoals die in het nieuws kwamen bij DigiNotar en Lektober.[2] 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.

Op de Buitengewone Algemene Ledenvergadering van de VNG op 29 november 2013 hebben de leden besloten in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' de BIG als basisnorm te nemen voor hun beleid op informatieveiligheid. Gemeenten hebben zich met deze resolutie een 'verplichte zelfregulering' opgelegd om de informatieveiligheid bij de gemeenten te verbeteren. Gemeenten zijn dus zelf aan zet. Daartoe is de Baseline Informatiebeveiliging Gemeenten (BIG) opgesteld, door Rijk en gemeenten.

In het Jaarplan heeft de Rekenkamercommissie Brunssum een Quick Scan opgenomen met 'Digitale Veiligheid' als onderwerp. De Rekenkamercommissie heeft daartoe een vragenlijst uitgezet.

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 heeft zich voor de vragenlijst gebaseerd op een notitie van de Rekenkamer van de gemeente Den Haag en de Taskforce Bestuur & Informatieveiligheid Dienstverlening (Taskforce BID).[3] De vragen gaan op een aantal belangrijke aspecten van de BIG in.

Dit is geen traditioneel oordeelvormend onderzoek van een Rekenkamercommissie, omdat het beleid en uitvoering in de meeste gemeenten nog in de kinderschoenen staan. De Rekenkamercommissie hanteert wel een referentiekader om de antwoorden te plaatsen. Deze zijn gegeven in de Strategische en Tactische variant van de BIG.[4]

2 Aanpak

In een gesprek op 25 juni 2015 met de directeur Beleid & Strategie, is de startnotitie overhandigd. In de startnotitie zijn 10 vragen over informatieveiligheid en de implementatie van de BIG opgenomen.

---

[2] DigiNotar verzorgde elektronische handtekeningen en certificaten voor een groot deel van de overheid, zoals die van DigID. In juli 2011 ontdekte DigiNotar dat deze een maand eerder gehackt was en kwam daarmee pas eind augustus mee naar buiten. Uit onderzoek bleek dat DigiNotar fouten in de procedures en systemen had gemaakt. Dit leidde ertoe dat alle overheidscertificaten onveilig waren.

In oktober 2011 bleek dat de websites van vijftig gemeenten en gemeentelijke diensten open stonden vanwege een verouderde Windows-versie. Daardoor konden kwaadwillenden informatie ophalen en bestanden aanpassen of wissen. Ook kon men door het lek DigID's misbruiken en namens een inwoner handelingen uitvoeren bij een van de vijftig 'lekke' gemeenten. Oktober 2011 werd daardoor Lektober genoemd.

[3] Zie Notitie Opties rekenkameronderzoek Informatieveiligheid, Rekenkamer Den Haag & Taskforce Bestuur & Informatieveiligheid Dienstverlening, 2014. (http://www.rekenkamerdenhaag.nl/rekenkamer/to/Workshop-digitale-veiligheid.htm)

[4] Zie: Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten vs 1.0, KING; Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten vs 1.0, KING.

Deze 10 vragen zijn:

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 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 Rekenkamercommissie heeft op 8 september antwoorden op de bovenstaande vragen ontvangen. Naar aanleiding daarvan heeft de Rekenkamercommissie aanvullende vragen gesteld. Daarop is op 16 september een kort begeleidend gesprek gevoerd met twee ambtenaren, een van de afdeling Controlling en een verantwoordelijk voor de uitvoering van digitale veiligheid. De antwoorden op de aanvullende vragen zijn op 24 september ontvangen. De conceptversie van de Quick Scan is op 28 oktober voor ambtelijke hoor & wederhoor aangeboden. De ambtelijke reactie is op 8 december door de rekenkamercommissie ontvangen.

3 Vraag en antwoord

Hieronder wordt ingegaan op de gestelde vragen en antwoorden en worden waar nodig aanbevelingen gedaan.

3.1 Vraag: 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?

Antwoord: In de BIG is afgesproken dat het integrale beleid op het terrein van informatiebeveiliging door de colleges van B&W moet worden vastgesteld en gepubliceerd. Het beleid is risico gebaseerd en een verantwoordelijkheid van het lijnmanagement. Deze stelt op basis van een analyse en assessments de risico's vast.[5]

Reeds vanaf 2012, voor de introductie van BIG in 2014, voerden Brunssum, Onderbanken en Landgraaf (BOL-gemeenten) een gezamenlijk informatiebeveiligingsbeleid en –plan uit. Dit beleid was, evenals BIG, gebaseerd op de Code voor Informatiebeveiliging (ISO 27002). De organisatie geeft aan dat het de bedoeling was om in 2015 het informatiebeveiligingsbeleid te updaten, op basis van risico gebaseerde actualisatieslag. Daarmee verwacht de organisatie te voldoen aan de beleidsmatige uitgangspunten van BIG. 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'.

In BIG is met name aandacht voor betrokkenheid van management en college, en helaas slechts indirect de gemeenteraad. Informatieveiligheid is een kwetsbare en kritieke factor in de gemeentelijke dienstverlening. De risico's op continuïteit van de dienstverlening aan burgers, juridisch gebied, reputatieschade en inbreuk op privacy van burgers worden over het algemeen hoog ingeschat. De impact van incidenten op informatieveiligheid is zeer groot. Daarmee is informatie-veiligheid 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 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.

[5] Zie Tactische BIG, items 5 en 6, resp. Informatiebeveiligingsbeleid en Interne organisatie.

3.2 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)?

Zie voor wat in de BIG is afgesproken § 3.1.

De organisatie geeft aan dat er een informatiebeveiligingsplan is dat door het college is vastgesteld. Daarin zijn risico's benoemd en zoals in § 3.1 is aangegeven, is het lijnmanagement bezig met aan actualisatieslag. De beheersingsmaatregelen worden besproken in het Beveiligingsforum. Het forum controleert de voortgang op informatiebeveiliging en monitort de audits, zelf tests en assessments en de opvolging daarvan. In het Beveiligingsforum zijn de volgende functies vanuit het ambtelijke werkveld aangesloten hoofd Burgerzaken, hoofd Facilitaire Zaken, hoofd Informatiebeheer, directeur Gemeentewinkel, consulent P&O en de beveiligingsfunctionaris.

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.

Deze vraag kan bijgevolg deels bevestigend beantwoord worden.

3.3 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?

In de BIG hebben gemeenten afgesproken dat over het functioneren van de informatiebeveiliging aan het management en bestuur wordt gerapporteerd, in het kader van de P&C-cyclus. [6] *In de BIG staat niets over rapporteren aan waarstaatjegemeente.nl over het thema digitale veiligheid. In de Resolutie van de VNG staat dat gestreefd wordt naar transparantie en dat deze onder meer bereikt wordt door gebruik te maken van waarstaatjegemeente.nl.*

Volgens de door de ambtenaren 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 informatie-veiligheid kunnen nagaan.

In de actualisering van het beleid op informatieveiligheid wil de organisatie de betrokkenheid van het gemeentebestuur 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 (zie § 3.2) 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 (zie § 3.1). Het ligt volgens de ambtenaren in de bedoeling de raad over de beleidsaanpassingen via een

---

[6] Zie Tactische BIG, item 6.1.8, Beoordeling van het informatiebeveiligingsbeleid.

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. Zoals in § 3.1 is gesteld is informatieveiligheid een kritieke succesfactor voor de gemeentelijke dienstverlening, en is het 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.

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

In de BIG is afgesproken dat op basis van een risicobeoordeling een continuïteitsplan met betrekking tot informatiebeveiliging wordt opgesteld. Daarmee worden essentiële procedures voor continuïteit geïdentificeerd, zoals het veilig stellen, herstel en reconstructie van informatie enz.[7]

Met betrekking tot borging van de continuïteit van de (digitale) dienstverlening, neemt de gemeente Brunssum deel aan de gemeenschappelijke regeling Parkstad-IT (PIT). Het centrale ICT-beheer is bij deze GR ondergebracht. De afspraken daarover zijn in een dienstverleningsovereenkomst vastgelegd. Deze samenwerking is volgens de gemeentelijke organisatie ingegeven als gevolg van de toegenomen eisen rond informatiebeveiliging, en de complexiteit inzake techniek en continuïteit. 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.

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

In de BIG hebben gemeenten afgesproken dat risico's op informatieveiligheid die betrekking hebben op externe partijen, die bijvoorbeeld persoonsgegevens verwerken, expliciet worden meegenomen. Daarover moet jaarlijks worden gerapporteerd. Het aspect informatiebeveiliging moet behandeld worden in overeenkomsten met derde partijen.[8]

---

7 Zie Tactische BIG, item 14, Bedrijfscontinuïteitsbeheer.

8 Zie Tactische BIG, item 6.2, Externe Partijen.

De ambtelijke organisatie geeft aan dat tijdens aanbestedingstrajecten privacygevoelige informatie uitgewisseld kan worden. Maar dat stukken tijdens deze procedures niet openbaar zijn, zoals CV's van medewerkers van derden. Voor statutaire bestuurders en de rechtspersonen gelden andere regels. De rechtspersoon zelf heeft geen persoonlijke gegevens en de bestuurders staan ingeschreven als statutaire vertegenwoordigers in het openbare handelsregister.

In de aanbestedingsstukken van de gemeente staat aangegeven dat de opdrachtnemer zich dient te houden aan de vigerende wet- en regelgeving. In het inkoopbeleid wordt verwezen naar de gedragscodes (voor bestuurders en ambtenaren) waarin staat dat met privacygevoelige gegevens van burgers vertrouwelijk dient te worden omgegaan. Bij verwerking van persoonsgegevens van Brunssumse burgers door derden, bijv. cliëntbestanden, geldt de Wet bescherming persoons-gegevens (Wbp). In de standaardovereenkomsten is een bepaling opgenomen omtrent de omgang met persoonsgegevens. Tevens gelden de Algemene Inkoopvoorwaarden van de gemeente Brunssum, met artikel 31 over geheimhouding met betrekking tot (persoons)gegevens die over en weer gedeeld worden.

Met betrekking tot gegevens van Brunssumse burgers die bij derden worden opgeslagen, zoals in het sociale domein, geeft de organisatie aan dat dat alleen de zorgverleners zijn. Zij gebruiken hun eigen systemen en informatie, en wisselen geen persoonsgegevens uit. De gemeente Maastricht voert in opdracht van 18 gemeenten in Zuid-Limburg de administratie rond declaraties en betaling van de jeugdhulp uit. Volgens de gemeentelijke organisatie registreert de gemeente Maastricht geen (persoonlijke) gegevens van burgers. In de ambtelijke hoor & wederhoor is aangegeven dat met name de autorisaties van de jeugdzorg in 2016 in kaart worden gebracht. Daarbij wordt het werkproces herijkt en in samenspraak met de zorgverleners bijgesteld.

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.[9]

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

Dit aspect is niet geregeld in de BIG. De contactpersonen, Algemene Contactpersoon Informatiebeveiliging (ACIB) en Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) , kunnen aangesloten zijn bij IBD. IBD stroomlijnt de meldingen van beveiligingsincidenten en waarschuwt voor bedreigingen, zoals lekken in software. Voor aansluiting moeten 4 stappen gerealiseerd zijn en wel: benoeming van twee functionarissen (ACIB en VCIB); doorgeven van

[9] Zie: Bewerkersovereenkomst, versie 1.0, februari 2014, IBD, KING. (https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0218-bewerkersovereenkomst-v1.0.pdf)

IP-adressen en URL's en doorgeven van de in gebruik zijnde hard- en software (de zogenoemde ICT-foto).

Vanaf 11 februari 2014 beschikt de gemeente Brunssum over een Algemene en Vertrouwde Contactpersoon Informatiebeveiliging (resp. ACIB en VCIB) en zijn vervangers voor deze functionarissen aangewezen. De VCIB behandelt incidentmeldingen met een vertrouwelijk karakter, de ACIB behandelt de andere meer algemene incidentmeldingen. De registratie van meldingen en verantwoordingsverdeling worden in 2016 gemaakt. De vertrouwelijk contactpersoon (VCIB) voert de verantwoording mondeling uit en legt de registratie anoniem vast. Daarmee is de gemeente Brunssum vanaf die datum voor de eerste twee fasen aangesloten op de IBD. Vanaf dat moment kan de IBD meldingen van incidenten met betrekking tot gebruik van hard- en software naar de gemeente sturen. De ACIB en VCIB, en hun vervangers, hebben volgens de organisatie voldoende kennis om de meldingen van de IBD te beoordelen.

Een melding kan betekenen dat de eigen organisatie zaken kan of moet oplossen, of dat de specialisten van PIT ingeschakeld moeten worden, of dat er niets hoeft te gebeuren omdat de incidentmelding geen risico voor de eigen organisatie in zich bergt. Vaak gaan de specialisten van PIT zelf al proactief aan de slag met de meldingen.

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

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

In de BIG is opgenomen dat er een procedure wordt vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd. Ook geeft de BIG aan dat er geleerd moet worden van de incidenten.[10]

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.

Deze 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?');

[10] Zie Tactische BIG, item 13, Beheer van informatiebeveiligingsincidenten.

- 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.[11] De procedure daarop is met Parkstad-IT opgepakt, zie ook § 3.9.

3.8 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?

Ten aanzien van de beoordeling van het beveiligingsbeleid is in de BIG geregeld dat er periodieke beveiligingsaudits worden uitgevoerd. Over het functioneren van informatiebeveiliging wordt conform de P&C-cyclus gerapporteerd aan het lijnmanagement. [12] *Voor rapportage aan gemeenteraden geeft de BIG geen richtlijnen.*

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[13] 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. Voor een aanbeveling dienaangaande zie aanbeveling 3.

---

[11] Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

[12] Zie Tactische BIG, item 6.1.8, Beoordeling van informatiebeveiligingsbeleid; 15.2, Naleving van beveiligingsbeleid en –normen en technische naleving.

[13] Een PEN-test is een test op de sterkten en zwaktes van de IT-beveiliging van de organisatie.

3.9 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 BIG hebben gemeenten afgesproken dat het informatiebeveiligingsbeleid eens in de drie jaar, of zodra zich belangrijke wijzigingen voordoen, wordt geëvalueerd.[14]

Het informatiebeveiligingsbeleid is in 2012 geformuleerd, waardoor volgens de organisatie de uitgangspunten deels niet langer valide zijn. Dat heeft te maken met interne en externe ontwikkelingen zoals in het sociale domein, vergaande integratie van informatiesystemen, digitalisering van documenten en de reeds vermelde toename van internetfraude en –criminaliteit. Dat vergt volgens de ambtenaren specialistische kennis, waardoor samenwerking op bovenlokaal niveau steeds vaker gezocht moet worden. Deze samenwerking is mede ingegeven door overwegingen op gebied van kwaliteit, continuïteit van de dienstverlening en kosten die ermee gemoeid zijn.

Specifiek als nieuwe ontwikkeling op wetgeving is de Wet meldplicht datalekken te noemen, die per 1 januari 2016 ingaat. Deze meldplicht houdt in dat bedrijven en overheden direct een melding moeten doen bij het Meldloket Autoriteit Persoonsgegevens zodra zij een ernstig datalek constateren. [15] Met Parkstad-IT en Heerlen is de inrichting van het proces hierop opgepakt, zowel intern als bij de ketenpartners van de gemeente.

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.

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

In de BIG is afgesproken om te leren van beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren.[16] *Als randvoorwaarde is in de BIG onder andere geformuleerd dat informatieveiligheid een verantwoordelijkheid is van het lijnmanagement en dat kennis en expertise essentieel zijn.*[17]

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 (zie ook §4.7). Door ontbrekende middelen is er 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 management-team en het college. Waarbij het verzoek is gedaan voldoende middelen beschikbaar te stellen. Zie voor een aanbeveling hierop aanbeveling 1. Volgens de antwoorden van de ambtenaren zal het

---

14 Zie Tactische BIG, item 5.1.2, Beoordeling van het informatiebeveiligingsbeleid.
15 Zie noot 10.
16 Zie Tactische BIG, item 13.2.2, Leren van informatiebeveiligingsincidenten.
17 Zie Tactische BIG, 1.3, Randvoorwaarden.

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. Ook wordt in de ambtelijke hoor en wederhoor aangegeven dat in 2013 een bewustwordingscampagne is gevoerd. Via het Intranet worden medewerkers bewust gemaakt van afspraken op informatiebeveiliging, meestal naar aanleiding van incidenten.