Rekenkamercommissies BEL

BEL op weg naar BIG

Digitale veiligheid BEL-gemeenten

Quick Scan
augustus 2015

Samenvatting

In deze Quick Scan hebben de Rekenkamercommissies van de BEL-gemeenten een onderzoek uitgevoerd naar digitale veiligheid. Gemeenten, en hun partners, gaan met digitale (vertrouwelijke) gegevens om en veel bedrijfsvoerings-processen 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 Rekenkamercommissies van de BEL-gemeenten hebben, 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 BEL-organisatie. De vragen gaan in op belangrijke aspecten van de BIG, teneinde een beeld te krijgen van de implementatie van beleid rond digitale veiligheid bij de BEL-gemeenten. In hoofdstuk 2 zijn de tien onderzoeksvragen weergegeven.

In hoofdstuk 3 worden de onderzoeksvragen beantwoord. Het beeld dat hieruit naar voren komt is dat de BEL-Combinatie en de colleges sturen op digitale veiligheid en dat de eerste belangrijke stappen op weg naar digitale veiligheid gezet zijn. Echter, belangrijke stappen om het beleid risico-gebaseerd te maken moeten nog gezet worden. Ook moeten stappen gezet worden om de organisatie en bestuur bewust te laten zijn van de risico's op digitale veiligheid. En 'in control' te laten zijn op deze risico's en de voortgang op de bestrijding ervan. Daartoe heeft de Rekenkamercommissie de volgende aanbevelingen geformuleerd:

Aanbeveling 1. Aan de colleges: Breng het Handboek Informatieveiligheid van de BEL-combinatie op gelijk niveau en nummering als de BIG (tactische variant).

Aanbeveling 2. Aan de raden: Laat u informeren ten aanzien van het integraal implementatieplan dat volgens de huidige planning van de organisatie in het najaar wordt opgesteld, op basis van de GAP- en risicoanalyse, en voorzie de implementatie van voldoende middelen en formatie.

Aanbeveling 3. Aan de raden: Benoem informatieveiligheid tot een kritische succesfactor en geef opdracht aan het college informatieveiligheid op te nemen in de informatie die vanuit de P&C-cyclus periodiek naar de raad wordt gestuurd.

Aanbeveling 4. Aan de raden: Geef de colleges de opdracht informatieveiligheid tot expliciet aandachtspunt bij personeelsbeleid en verbetercycli (PDCA) te maken.

1 Inleiding

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.

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 hebben de Rekenkamercommissies BEL een Quick Scan opgenomen met 'Digitale Veiligheid' als onderwerp, mede op verzoek van een aantal raadsfracties in de gemeenten. De Rekenkamercommissies hebben daartoe een vragenlijst uitgezet en besproken met de verantwoordelijk ambtenaar.

De Quick Scan is er op gericht een inzicht te geven in de stand van zaken rond de implementatie van de BIG. De Rekenkamercommissies hebben zich voor de vragenlijst gebaseerd op een notitie van de Rekenkamer van de gemeente Den Haag en de Taskforce Bestuur & Informatieveiligheid Dienstverlening (Taskforce BID).[1] 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 Rekenkamercommissies hanteren wel een referentiekader om de antwoorden te plaatsen. Deze zijn gegeven in de Strategische en Tactische variant van de BIG.[2]

2 Aanpak

In een gesprek op 15 april 2015 met de directeur van de BEL-Combinatie en de directiesecretaris/adviseur Beleid, Bestuur en Kwaliteit, in de hoedanigheid van chief information security officer (CISO), is de startnotitie voor de Quick Scan overhandigd. In de startnotitie zijn 10 vragen over informatieveiligheid en de implementatie van de BIG opgenomen.

---

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

2 Zie: Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten vs 1.0, KING; Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten vs 1.0, KING.

Deze 10 vragen zijn:

1. Sturen de gemeenten 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. Hebben de gemeenten 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 (BEL-organisatie, colleges, raden)?
3. Rapporteert en bespreekt de organisatie het functioneren van de cyclus van informatieveiligheid op management- en bestuursniveau (BEL-organisatie, 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. Kennen de gemeenten de leveranciers en partners waarmee ze samenwerken en toetsen zij die ook op informatieveiligheidsaspecten en zo ja hoe?
6. Zijn de gemeenten '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 self-assessments? En wordt over het functioneren van de cyclus van informatieveiligheid gerapporteerd aan de raden? 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?

Bijlage 1 bevat de antwoorden op de vragen, die de Rekenkamercommissies op 27 mei 2015 hebben ontvangen, na verlening van één week uitstel in verband met onder andere vakanties.

Naar aanleiding van de antwoorden hebben de leden van de Rekenkamercommissies op 11 juni 2015 op het BEL-kantoor het handboek Informatieveiligheid ingezien en een gesprek gehad met de CISO.

3 Vraag en antwoord

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

3.1 Sturen de gemeenten 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?

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 risicogebaseerd en een verantwoordelijkheid van het lijnmanagement. Deze stelt op basis van een analyse en assessments de risico's vast.[3]

De colleges van de BEL-gemeenten hebben in juni/juli 2014 de beleidskaders voor informatiebeveiliging vastgesteld. Deze beleidskaders zijn vertrouwelijk en zijn opgenomen in het handboek Informatiebeveiliging. De Rekenkamer-commissies constateren dat niet alle items uit de (Tactische) BIG in het handboek Informatieveiligheid zijn opgenomen. Tevens komt de nummering van items niet overeen met de (Tactische) BIG. De verklaring die in het gesprek met de CISO werd gegeven is dat het handboek Informatiebeveiliging medio 2014 is samengesteld uit een aantal reeds bestaande handboeken op deelonderwerpen, zoals de BasisRegistratiePersonen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK) en Basisregistratie Adressen & Gebouwen (BAG). Op dat moment was de (Tactische) BIG nog niet geheel gereed, waardoor de nummering niet overgenomen kon worden. Ook na de afronding van de BIG is de nummering in het handboek niet aangepast. Dat maakt het lastig om direct zicht te krijgen op wat wel en niet vanuit de BIG is overgenomen. Bovendien is het lastig om direct zicht te krijgen op welke items de beleidskaders nog lacunes vertonen.

De Rekenkamercommissies constateren dat er daarmee nog geen integraal implementatieplan is. Voor het najaar 2015 staat een GAP-analyse in de planning. Daarmee wordt de 'gap' (kloof) in kaart gebracht tussen wat er aan beleidskaders is en wat er volgens de BIG zou moeten zijn. Daartoe behoort ook een risico-inventarisatie. Op basis van deze analyses zou in het najaar een implementatieplan worden opgesteld, met bijbehorend tijdpad en kostenoverzicht.

De gemeenten sturen daarmee op de afspraken uit de Resolutie 'Informatieveiligheid' die door de VNG is aangenomen.

In de BIG wordt een aantal functionarissen genoemd waarvan de benoeming noodzakelijk is. Deze benoemingen, zoals die van de CISO, zijn gerealiseerd. Wat de CISO naar eigen zeggen mist is voldoende tijd, bestuurlijke aandacht en middelen om slagen te maken met volledige implementatie van de BIG. Informatieveiligheid is bestuurlijk geen 'sexy' onderwerp. Er zijn wellicht 'bijna'-

---

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

incidenten met betrekking tot informatieveiligheid of er kunnen incidenten zijn die niet opgemerkt worden. Aandacht voor het onderwerp is daardoor lastig te genereren.

Aanbeveling 1. Aan de colleges: Breng het Handboek Informatieveiligheid van de BEL-Combinatie op gelijk niveau en nummering als de BIG (tactische variant).

Aanbeveling 2. Aan de raden: Laat u informeren ten aanzien van het integraal implementatieplan dat volgens de huidige planning van de organisatie in het najaar wordt opgesteld, op basis van de GAP- en risicoanalyse, en voorzie de implementatie van voldoende middelen en formatie.

3.2 Hebben de gemeenten 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 (BEL-organisatie, colleges, raden)?

Zie voor wat in de BIG is afgesproken paragraaf 3.1.

Deze vraag kan deels bevestigend beantwoord worden. Op deelgebieden worden externe audits en/of jaarlijkse zelfevaluaties gehouden, zoals de externe DigID-audits en de jaarlijkse zelfevaluaties met betrekking tot BRP, PNIK en BAG.

De resultaten van de GAP-analyse en risico-inventarisatie worden in het najaar van 2015 verwacht. Op basis daarvan wordt een integraal implementatieplan, met verbetermaatregelen, effect op de beheersing van risico's en noodzakelijke middelen in uren en kosten aan de gemeentebesturen voorgelegd.

3.3 Rapporteert en bespreekt de organisatie het functioneren van de cyclus van informatieveiligheid op management- en bestuursniveau (BEL-organisatie, college en raad)? [4] Is zij daarover transparant richting haar ketenpartners door via waarstaatjegemeente.nl te rapporteren over informatieveiligheid? Zijn er nog andere wijzen van rapporteren? [5]

De audits en zelfevaluaties op deelgebieden (zie 3.2) worden besproken en vastgesteld in de colleges. In het gesprek van de Rekenkamercommissies met de CISO is aan de orde gekomen dat het bestuur van de BEL-Combinatie in de kwartaalrapportages van de reguliere P&C-cyclus geïnformeerd wordt over functioneren van procedures en plan van aanpak, en risico's ten aanzien van informatieveiligheid op de deelterreinen. De integrale rapportage hierover wordt, ook weer volgens de CISO, meegenomen in de GAP-analyse van het najaar 2015.

---

[4] In de BIG hebben gemeenten afgesproken dat over het functioneren van de informatie-beveiliging aan het management en bestuur wordt gerapporteerd, in het kader van de P&C-cyclus. Zie Tactische BIG, item 6.1.8, Beoordeling van het informatiebeveiligingsbeleid.

[5] 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.

De BEL-gemeenten hebben volgens de CISO in november 2014 een per mail ontvangen en online beantwoorde vragenlijst van waarstaatjegemeente.nl met betrekking tot informatieveiligheid beantwoord. De Rekenkamercommissies constateren dat de BEL-gemeenten hierop transparant rapporteren.

De raden worden over informatiebeveiliging gerapporteerd in de paragraaf Bedrijfsvoering in de Jaarrekeningen van de gemeente. De raden krijgen per kwartaal een scorecard op een aantal bedrijfsvoeringsprocessen. De eerste drie kwartalen wordt daarover apart gerapporteerd, over het vierde kwartaal via de jaarrekening. Daarin wordt nog niet over de voortgang en risico's op informatieveiligheid gerapporteerd, omdat dit aspect van de bedrijfsvoering nog niet als kritische succesfactor is aangemerkt

Aanbeveling 3. Aan de raden: Benoem informatieveiligheid tot een kritische succesfactor en geef opdracht aan het college 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.[6]

De vraag moet met 'deels' beantwoord worden. Voor medio 2015 moeten alle softwaresystemen buiten de BEL geplaatst zijn. Dan moet een continu werkend parallel uitwijksysteem op een backup-locatie actief zijn, zodat calamiteiten die de (digitale) dienstverlening verstoren, opgevangen kunnen worden. Daarvoor zijn, volgens de CISO, snelle en dubbele lijnen aangelegd vanuit de BEL naar twee servers elders in het land. Deze uitwijkmogelijkheid wordt in de zomer van 2015 gerealiseerd en zal uiterlijk in de herfst van 2015 getest moeten worden. Het is de bedoeling uiterlijk eind oktober een continuïteitsplan gereed te hebben.

Doel van het continuïteitsplan en de uitwijkmogelijkheid is dat burgers, instellingen en bedrijven niets hoeven te merken van een calamiteit met betrekking tot digitale dienstverlening. Dat is op moment van schrijven van de conceptversie van deze Quick Scan nog niet geheel geïmplementeerd en getest.

3.5 Kennen de gemeenten de leveranciers en partners waarmee ze samenwerken en toetsen 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

---

[6] Zie Tactische BIG, item 14, Bedrijfscontinuïteitsbeheer.

gerapporteerd. Het aspect informatiebeveiliging moet behandeld worden in overeenkomsten met derde partijen.[7]

In het inkoop- en aanbestedingsbeleid zijn garanties opgenomen met betrekking tot aspecten als kwaliteit, milieu, gezondheid en veiligheid. Informatieveiligheid is daarin, volgens de CISO, nog onvoldoende geborgd, met name de toetsing op dat aspect.

Op deelterreinen, zoals de Jeugdhulp waarin met veel gevoelige persoonsgegevens wordt gewerkt, is het aspect informatieveiligheid wel meegenomen. Bij SoZa HBEL is de informatieveiligheid met een derde partij georganiseerd, volgens de ambtenaar. Voor deze Quick Scan hebben de Rekenkamercommissies dat niet gecheckt. Op andere terreinen zijn de regels te algemeen om goed toetsbaar te zijn.

Op digitale loketten van de gemeente en leveranciers, waar burgers met hun DigID kunnen inloggen, vinden verplichte assessments plaats door Logius. Daarover worden de gemeente en de rijksoverheid gerapporteerd. De BEL-Combinatie is voornemens de eisen met betrekking tot zogenoemd ketengericht informatieveilig werken aan te scherpen op basis van het self-assessment (GAP-analyse), in het najaar van 2015.

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

De ACIB en VCIB zijn september 2014 benoemd. Weliswaar in dezelfde persoon, maar dat is toegestaan in de BIG. Bij voorkeur is er een functiescheiding, maar dit werkt volgens de CISO binnen organisatie als de BEL Combinatie niet praktisch. Wel is een vervanger bij vakantie/ziekte benoemd. Beiden zijn meer beleidsmatig geschoolde medewerkers. Overwogen wordt een derde ACIB/VCIB te benoemen, met een meer technische achtergrond, omdat veel van de IBD-meldingen ICT-technisch van aard zijn.

De CISO vermeldt wel dat aan deze benoeming op dit moment geen extra uren/formatie zijn gekoppeld, terwijl er uiteraard wel extra (structurele) werkzaamheden uit voortvloeien. Hij is van plan dit formatieve aspect mee te nemen als onderdeel van de GAP-rapportage richting het bestuur.

Het doorgeven van IP-adressen en URL's (stap 3) is eind 2014 gerealiseerd. De ICT-foto van de hard- en software die in gebruik is, is in mei 2015 aangeleverd.

---

[7] Zie Tactische BIG, item 6.2, Externe Partijen.

Volledige aansluiting van de BEL-Combinatie en de BEL-gemeenten op IBD is gerealiseerd en er komen reeds kwetsbaarheidsmeldingen binnen.

Naar aanleiding van het door de ambtenaar gesignaleerde formatietekort verwijzen we naar aanbeveling 2.

3.7 Weet de organisatie hoe te handelen bij een (ernstig) informatieveiligheids-incident 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.[8]

Het Informatiebeveiligingshandboek bevat procedures voor het beheer van incidenten op informatieveiligheid. Vier van de vijf procedures die zijn beschreven zijn ingevuld, zoals

- Melden van incidenten
- Onrechtmatige kennisneming
- Inbraakdetectie en alarmopvolging
- Identiteit vaststellen en machtigen

De vijfde procedure is het inschakelen van de politie. Daarover moet nog overleg plaatsvinden met de politie. Dat komt op de agenda van het Dagelijks Bestuur van de BEL-Combinatie op 8 oktober 2015.

De in de BIG vereiste procedure rond melding van (ernstige) incidenten op het gebied van informatieveiligheid is grotendeels, maar nog niet geheel, ingevuld. Voor een aanbeveling dienaangaande verwijzen we naar aanbeveling 2.

Voor leren van incidenten en verbetering van procedures, zie paragraaf 3.10.

3.8 Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatieveiligheid via peer reviews, audits of self-assessments? En wordt over het functioneren van de cyclus van informatieveiligheid gerapporteerd aan de raden? 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. [9] *Voor rapportage aan gemeenteraden geeft de BIG geen richtlijnen.*

Regelmatige audits zijn verplicht vanwege het toezicht door ministeries en partijen als Logius. Er worden tot nu toe op deelgebieden audits en zelfevaluaties uitgevoerd:

---

[8] Zie Tactische BIG, item 13, Beheer van informatiebeveiligingsincidenten.
[9] Zie Tactische BIG, item 6.1.8, Beoordeling van informatiebeveiligingsbeleid; 15.2, Naleving van beveiligingsbeleid en –normen en technische naleving.

- tweejaarlijkse audits informatieveiligheid Basisregistraties Adressen & Gebouwen (BAG)
- jaarlijkse zelfevaluatie informatieveiligheid van de Basis Registratie Personen (BRP), gerapporteerd aan de Rijksdienst voor Identiteitsgegevens (voorheen agentschap BPR) en registratie van Paspoorten en Nederlandse IdentiteitsKaarten (PNIK)
- jaarlijks assessment informatieveiligheid digitale gemeentelijke loketten en WOZ-portalen, waar burgers met een DigID kunnen inloggen, gerapporteerd aan Logius.

Volgens de geïnterviewde ambtenaar is het de bedoeling dat er meer onderlinge samenhang tussen de audits wordt gerealiseerd.

Intern wordt gerapporteerd aan de colleges en de portefeuillehouder ICT & Communicatie in het Dagelijks Bestuur van de BEL-Combinatie. De raden krijgen sinds het jaar 2014 via de begroting en jaarrekening van de BEL Combinatie, in de paragraaf Bedrijfsvoering, op hoofdlijnen gerapporteerd over de voortgang en organisatie van informatieveiligheid. Zij kunnen hier hun zienswijzen over formuleren en bij het AB van de BEL-Combinatie indienen.

Met betrekking tot de informatievoorziening aan de gemeenteraden over voortgang op en functioneren van informatiebeveiliging verwijzen we naar aanbeveling 3.

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.[10]

De BIG stelt dat de beleidsuitgangspunten op informatieveiligheid risicogebaseerd moeten zijn. De risicoanalyse daarvoor vindt volgens de huidige planning van de organisatie plaats in het najaar van 2015. De risico's zoals deze nu zijn geformuleerd, zijn theoretisch van aard. Deze worden op basis van het self-assessment (GAP-analyse) getoetst en naar de praktijk gebracht.[11]

Uit het self-assessment volgt een integraal implementatieplan, met een prioritering, die afgestemd wordt op de beschikbare middelen en formatie. Hierbij verwijzen we naar aanbeveling 2.

---

[10] Zie Tactische BIG, item 5.1.2, Beoordeling van het informatiebeveiligingsbeleid.

[11] In het gesprek met de ambtenaar kwam het voorbeeld naar voren over de uitwijkmogelijkheid voor de bedrijfsvoering bij een calamiteit. Dat was theoretisch goed geregeld, maar een aantal zaken was praktisch nog niet adequaat genoeg geregeld. Er was nog geen gelegenheid dat in de praktijk te toetsen. Daarop wordt in het najaar van 2015 wel door middel van de risicoanalyse getoetst.

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.[12] *Als randvoorwaarde is in de BIG onder andere geformuleerd dat informatieveiligheid een verantwoordelijkheid is van het lijnmanagement en dat kennis en expertise essentieel zijn.*[13]

Volgens de CISO wordt BEL-breed de Plan-Do-Check-Act-cyclus (PDCA) gehanteerd als kwaliteits- en leerinstrument. Het Handboek Informatiebeveiliging werkt BEL-breed, en daarmee is de link met leren en verbeteren gelegd, volgens de geïnterviewde. De Rekenkamercommissie constateert dat informatie-beveiliging daarmee nog niet expliciet als item in de PDCA-cyclus is opgenomen.

In het kader van personeelsbeleid worden in Werk OntwikkelingsPlannen (WOP) individuele maatwerkafspraken gemaakt voor opleiding en ontwikkeling. Volgens de geïnterviewde ambtenaar is medio 2015 het onderwerp informatiebeveiliging nog niet ondergebracht bij HRM of integraal of strategisch personeelsbeleid dat BEL-breed is geïmplementeerd.

Aanbeveling 4. Aan de raden: Geef de colleges de opdracht informatieveiligheid tot expliciet aandachtspunt bij personeelsbeleid en verbetercycli (PDCA) te maken.

De verwachting is dat informatieveiligheid een belangrijk thema wordt binnen het Informatiebeleidsplan 2015-2018, dat voor het najaar wordt voorbereid. Volgens de geïnterviewde is het de bedoeling om extra formatie te creëren om een informatieveilige werkcultuur binnen de BEL-Combinatie en de aangesloten gemeenten te stimuleren en te borgen. Ook hiervoor verwijzen we naar aanbeveling 2.

---

[12] Zie Tactische BIG, item 13.2.2, Leren van informatiebeveiligingsincidenten.
[13] Zie Tactische BIG, 1.3, Randvoorwaarden.