Lelystad op weg naar BIG

Quick Scan- Informatiebeveiliging gemeente Lelystad

Nota van bevindingen

In opdracht van de rekenkamer Lelystad

Maart 2016
Drs. E.J.M. Lemmens, Prae Advies & Onderzoek

Inhoud

1 Samenvatting, conclusies en aanbevelingen

Met deze Quick Scan heeft de rekenkamer Lelystad een kort onderzoek uit laten voeren naar informatiebeveiliging in de gemeente Lelystad. Gemeenten en hun partners gaan met een toenemende hoeveelheid (vertrouwelijke) digitale gegevens om. Veel informatieprocessen verlopen digitaal. Dat is tegenwoordig zeer kwetsbaar en de beveiliging van gegevens en continuïteit van processen verdient de nodige aandacht.

Achtergrond van het onderzoek

In 2013 hebben gemeenten zich verplicht te werken aan verbetering van de digitale veiligheid. Gemeenten hebben daarom de Baseline Informatiebeveiliging Gemeenten (hierna: BIG) opgesteld. Zij werden daarbij ondersteund door VNG en het Rijk. De BIG formuleert op strategisch en tactisch niveau eisen, waaraan informatiebeveiliging bij gemeenten moet voldoen. De rekenkamer Lelystad heeft tien vragen voorgelegd aan de ambtelijke organisatie over de implementatie van de BIG. Deze vragen zijn gebaseerd op een vragenlijst van de rekenkamer van de gemeente Den Haag en de Taskforce Bestuur & Informatieveiligheid Dienstverlening (Taskforce BID) en gaan in op belangrijke aspecten van de BIG, zie hoofdstuk 3 p. 7-8. Op die manier wil de rekenkamer een globaal beeld krijgen van de manier waarop het beleid rond informatieveiligheid op papier in de organisatie van de gemeente Lelystad is ingevoerd. De vragen gaan niet in op de operationele situatie van de ICT bij de gemeente Lelystad, maar op het tactische en strategische niveau van de BIG.

Conclusies en aanbevelingen

In het algemeen concludeert de rekenkamer Lelystad, dat college en management van gemeente Lelystad op strategisch en tactisch niveau voldoende sturen op de afspraken uit de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'. De rekenkamer Lelystad kwalificeert de stand van zaken op het gebied van informatieveiligheid in de gemeente Lelystad, zoals op papier is aangetroffen, als goed. Ook in vergelijking met een viertal gemeenten waar de onderzoeker informatieveiligheid eerder heeft onderzocht.[1]

Op basis van een inventarisatie en risicoanalyse, waarbij het lijnmanagement is betrokken, zijn maatregelen geïdentificeerd die

- reeds genomen waren, of
- niet van toepassing zijn, of
- die nog genomen moesten worden.

De relevante nog te nemen maatregelen uit de BIG worden opgenomen in het Lelystadse implementatieplan[2] voor informatieveiligheid en de BIG-maatregelen, zoals in 2014 vastgesteld door college en directieteam. De maatregelen die niet van toepassing zijn, worden op basis van het ‘pas

[1] Het zijn vier gemeenten waar de onderzoeker van Prae Advies en onderzoek hetzelfde onderzoek heeft uitgevoerd. Het is geen officiële benchmark. De vier rekenkamer(commissie)s van deze gemeenten hebben geen expliciete toestemming gegeven voor een vergelijking van de onderzoeksresultaten. Vandaar dat de gemeenten niet bij naam worden genoemd.

[2] In het implementatieplan, of informatiebeveiligingsplan, neemt elke gemeente de maatregelen op die deze moet nemen om te voldoen aan de BIG. Dat gebeurt op basis van een risicoanalyse. In het implementatieplan prioriteert de gemeente de te nemen maatregelen.

toe of leg uit'-principe opgenomen in een 'Verklaring van Toepasselijkheid'. Daarmee stuurt de organisatie op strategisch niveau voldoende op implementatie van de maatregelen in de BIG.

Onder andere vanwege de nieuwe taken van gemeenten in het sociale domein verwerken de gemeente en zijn partners veel privacygevoelige informatie. De gemeente Lelystad heeft de partijen waarmee zij samenwerkt en informatie uitwisselt in beeld. De gemeente Lelystad communiceert haar eisen aan de beveiliging van de informatie aan deze partijen. De gemeente maakt afspraken met partijen, legt deze vast en monitort deze.

De maatregelen die de continuïteit en de integriteit van de gemeentelijke dienstverlening moeten garanderen, zijn op papier afdoende vastgelegd. Jaarlijks vinden audits door externen en self assessments plaats. Melding en opvolging van ernstige en minder ernstige incidenten zijn geregeld. De aansluiting op de Informatiebeveiligingsdienst voor gemeenten (hierna: IBD) is voor de eerste twee van de vier stappen afgerond. Volledige aansluiting op de IBD is echter geen eis vanuit de BIG. De Chief Information Security Officer (CISO) heeft vooralsnog bezwaren tegen volledige aansluiting. Deze bezwaren lijken de rekenkamer Lelystad gerechtvaardigd. Volledige aansluiting is op termijn wel het nastreven waard, omdat de IBD dan op maat toegesneden meldingen en adviezen kan geven.

Tweemaal per jaar moet namelijk de uitwijkprocedure worden getest. Dat is in 2015 niet gebeurd. Naar verluidt was dit gebaseerd op een bewuste keuze om de capaciteit anders in te zetten. Het niet testen is een mogelijk risico voor de effectiviteit van de uitvoering van de gemeentelijke dienst-verlening. Volgens de CISO is het de bedoeling, in 2016 het testen te hervatten. De rekenkamer spoort de gemeentelijke organisatie aan de opvolging te borgen van de maatregelen die de continuïteit van de gemeentelijke dienstverlening moeten garanderen. De gemeenteraad kan zich desgewenst hierover over een half jaar laten rapporteren.

De organisatie van de gemeente Lelystad besteedt de nodige aandacht aan de bewustwording bij medewerkers van de risico's op het gebied van informatieveiligheid. De gemeentelijke organisatie is van plan de bewustwordingscampagne van de IBD - 'Safe and Sound' - daarvoor in te zetten. Raadsleden worden in de campagne niet meegenomen, omdat zij niet of nauwelijks op het netwerk van de gemeentelijke organisatie zijn aangesloten. De rekenkamer geeft ter overweging om in de bewustwordingscampagne ook raadsleden te betrekken. Zij krijgen in hun raadswerk ook met vertrouwelijke informatie te maken.

De investering in de bewustwording van onder andere medewerkers van de risico's van informatie-veiligheid is niet eenmalig en zal continu herhaald en bijgehouden moeten worden. Of deze inspanningen ook in de praktijk de gewenste effecten hebben, was geen onderdeel van deze Quick Scan.

Informatieveiligheid krijgt de nodige aandacht van college en management. De wethouder Financiën, economie en wonen heeft informatieveiligheid in de portefeuille. Onderdelen, zoals Basisregistratie Personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK) en Suwinet vallen onder andere portefeuillehouders. Verdeling van onderdelen van een onderwerp over meerdere portefeuilles kan een risico op effectiviteit inhouden. Dat lijkt hier niet het geval, aangezien de wethouder Financiën, economie en wonen doorzettingsmacht op informatieveiligheid heeft.

De beleidsuitgangspunten voor informatieveiligheid zijn van eind 2014: dus relatief recente datum. Hoewel informatieveiligheid en de internetomgeving snel veranderen, zijn aanpassingen op basis van de bevindingen de beleidsuitgangspunten vooralsnog naar verwachting niet nodig.

College en management krijgen via de reguliere P&C-cyclus minimaal zes keer per jaar informatie over de uitvoering van het informatieveiligheidsbeleid. Dit is conform de BIG-normen. De gemeenteraad krijgt over informatieveiligheid gerapporteerd in de paragraaf bedrijfsvoering van het jaarverslag en de begroting. De informatie die in de bedrijfsvoeringsparagraaf is opgenomen is echter (te) summier.[3]
Hoewel de organisatie voldoet aan hetgeen in de BIG is afgesproken over informatievoorziening aan college en management, is de informatievoorziening aan de raad over informatiebeveiliging zowel kwalitatief als kwantitatief voor verbetering vatbaar. Dit kan en moet uitgebreider om de gemeenteraad voldoende bij het onderwerp aangesloten te laten zijn. Te meer omdat in het jaarverslag 2014 staat, dat met informatieveiligheid grote risico's gemoeid zijn. De kans op incidenten is weliswaar laag, maar als incidenten zich voordoen is de impact hoog. Daarmee is informatieveiligheid niet uitsluitend een uitvoeringsaangelegenheid en niet uitsluitend een thema op het gebied van bedrijfsvoering. Informatieveiligheid is een beleidskwestie, die van strategisch belang is. Een nadrukkelijker bestuurlijke en politieke borging en betere informatievoorziening aan de raad is daarom sterk aan te bevelen.

Aanbeveling: Geef het college opdracht informatieveiligheid aan te merken als een kritieke succesfactor[4] voor de gemeentelijke beleidsuitvoering en dienstverlening. En treedt met het college in overleg hoe (inhoud, frequentie en momenten in het jaar) de raad periodiek gerapporteerd wil krijgen over uitvoering en stand van zaken van het informatieveiligheidsbeleid.

<u>Toelichting op de aanbeveling</u>
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 om de raad op dit belangrijke thema voldoende aangesloten te laten zijn. Dit kan bijvoorbeeld verbeteren door opname van een aantal kerngegevens in de raadsrapportages in de reguliere P&C-cyclus. Zoals het aantal ernstige en minder ernstige incidenten op informatiebeveiliging, of de opvolging die is gegeven aan ernstige incidenten, of de audits en zelftesten afgehandeld zijn enz.

---

[3] Opgenomen in de Jaarstukken 2014, p. 117: "**Informatiebeveiliging** Veel overheidsinformatie is openbaar. Maar de gemeente heeft ook gegevens die beslist niet openbaar mogen worden zoals persoonlijke gegevens van burgers. Met de komst van de decentralisaties is de hoeveelheid privacygevoelige gegevens alleen maar groter geworden. Om de beveiliging van informatie te waarborgen heeft de gemeente informatiebeveiligingsbeleid en is er een functionaris belast met het controleren van de naleving ervan. Bij de organisatie brede risico-inventarisatie komt informatiebeveiliging wel naar boven als hoog risico. De kans op incidenten wordt als gevolg van het reeds bestaande beleid en maatregelen, klein geacht. Maar als een incident toch plaats zou vinden kan de impact daarvan hoog zijn."

[4] 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.

2 Inleiding

Informatieveiligheid is binnen gemeenten verscherpt op het netvlies gekomen na crises zoals die in het nieuws kwamen bij DigiNotar en door Lektober.[5] Deze hebben aangetoond dat gemeenten op digitaal gebied 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 aangesloten gemeenten in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' besloten de Baseline Informatiebeveiliging Gemeenten (BIG) als basisnorm te nemen voor hun beleid op informatieveiligheid. Deze baseline is opgesteld door Rijk en gemeenten. Hierin zijn maatregelen opgenomen die gemeenten kunnen nemen om de veiligheid van de door de gemeente beheerde informatie te verbeteren en te garanderen. Gemeenten hebben zich met deze resolutie een 'verplichte zelfregulering' opgelegd. Gemeenten zijn dus zelf aan zet.

De rekenkamer Lelystad heeft – gezien de risico's en het maatschappelijke en financiële belang van het onderwerp – besloten informatieveiligheid in de gemeente Lelystad aan een snel en globaal onderzoek te onderwerpen. Met deze Quick Scan wil de rekenkamer een inzicht geven in de stand van zaken rond de invoering van de BIG in de gemeente Lelystad. Het is een momentopname, omdat het beleidsterrein nog volop in ontwikkeling is. Prae Advies & onderzoek heeft het onderzoek voor de rekenkamerrekenkamer Lelystad uitgevoerd.

Leeswijzer

De onderzoeksaanpak voor deze Quick Scan is in hoofdstuk 3 geschetst. In dat hoofdstuk zijn de tien onderzoeksvragen opgenomen. Deze vragen gaan in op de belangrijkste aspecten van gemeentelijk informatieveiligheidsbeleid. In hoofdstuk 4 worden de onderzoeksvragen beantwoord. De conclusies uit de bevindingen en de aanbevelingen naar aanleiding van de conclusies, ter verdere verbetering van het informatieveiligheidsbeleid in de gemeente Lelystad, zijn weergegeven in hoofdstuk 1 'Samenvatting, conclusies en aanbevelingen'.

[5] 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 Aanpak

De rekenkamer Lelystad heeft zich voor dit onderzoek gebaseerd op een notitie van de rekenkamer van de gemeente Den Haag en de Taskforce Bestuur & Informatieveiligheid Dienstverlening (Taskforce BID).[6] De vragen uit de notitie gaan in op de belangrijkste aspecten van de BIG. Deze vragen zijn licht aangepast aan de situatie van Lelystad.

Dit onderzoek is een Quick Scan en richt zich op de implementatie van de tactische en strategische maatregelen van de BIG. De vragen in deze Quick Scan gaan vooral in op de situatie op informatieveiligheid op papier in de gemeente Lelystad. De vragen gaan niet in op de operationele aspecten van ICT, zoals bijvoorbeeld de Health Check ICT-omgeving gemeente Lelystad van mei 2015 dat doet. Overigens kunnen operationele aspecten risico's op informatieveiligheid inhouden, maar dat valt buiten de reikwijdte van deze Quick Scan.[7]

Op 28 oktober 2015 heeft de Chief Information Security Officer (CISO)[8] van de gemeente Lelystad de startnotitie voor het onderzoek ontvangen. In de startnotitie zijn tien vragen over informatieveiligheid en de uitvoering van de BIG-maatregelen opgenomen.

Deze tien 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?

---

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

7 Zo is in de Health Check ICT-omgeving gemeente Lelystad, mei 2015, geconstateerd dat 'het patchen van de server' als risico dient te worden opgepakt en er 'achterstanden op onderhoud' zijn. Deze kunnen een risico op informatie-beveiliging inhouden. Deze Quick Scan gaat in op de aanwezigheid en uitvoering van de maatregelen in de BIG op strategisch en tactisch niveau, die ervoor zorgen dat operationele risico's op informatieveiligheid worden geconstateerd en dat er opvolging aan wordt gegeven.

8 Doel van deze functie is het, op basis van de algemeen aanvaarde standaard BIG, zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente.

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?
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 rekenkamer heeft op 11 november 2015 antwoorden op de bovenstaande vragen ontvangen, met beleidsstukken als bijlagen. Naar aanleiding van de ontvangen reactie en stukken heeft de rekenkameronderzoeker aanvullende vragen gesteld. Daarop is op 26 november 2015 een gesprek gevoerd met de CISO. Naar aanleiding van het gesprek heeft de onderzoeker aanvullende relevante beleidsstukken toegestuurd gekregen. Voor een overzicht van de beleidsstukken: zie de bijlage op pagina 19. Aanvullend heeft de onderzoeker de jaarrekening 2014, de begroting 2015 van de gemeente Lelystad en de Health Check ICT-omgeving gemeente Lelystad van mei 2015 onderzocht. Tot slot heeft de CISO medio december 2015 en begin januari 2016 een beperkt aantal vragen via de telefoon en de mail beantwoord.

4 Vraag en antwoord

Hieronder wordt in tien paragrafen ingegaan op de gestelde vragen en antwoorden. Waar nodig worden conclusies getrokken. Onder elke vraag is in cursieve letters de norm weergegeven, wat in de BIG op dat punt is afgesproken.

4.1 Stuurt de organisatie 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?

Norm: 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 voor werknemers en relevante externe partijen. Het beleid is risico gebaseerd en een verantwoordelijkheid van het lijnmanagement. Deze stelt op basis van een analyse en assessments de risico's vast.[9]

Het college van B&W vat het onderwerp informatieveiligheid op als collegeambitie. Dit is opgenomen in de Kadernota 2014-2017. Het directieteam (DT) en het college hebben november 2014 de BIG als basis voor het informatiebeveiligingsplan van de gemeente Lelystad vastgesteld. Het implementatieplan is door college en directieteam goedgekeurd. Zij hebben zich volgens de CISO hierbij gebaseerd op een risicoanalyse, dat door de lijn is uitgevoerd. Dat is zoals de eerste twee uitgangspunten van de BIG voorschrijven: informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement en is gebaseerd op risicomanagement.[10] College en management laten zich rapporteren over de audits en self assessments, zoals die van de DigID, Basisregistratie Personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK) en Suwinet.

Het onderwerp informatieveiligheid valt onder gemeentelijke dienstverlening, ICT en nieuwe media & open data/digitale bereikbaarheid. Dat zit in de portefeuille van de wethouder Financiën, economie en wonen. Zaken die te maken hebben met informatieveiligheid en de implementatie van de BIG vallen onder deze portefeuillehouder.

De burgemeester heeft de BRP en PNIK in de portefeuille. Suwinet valt onder de portefeuillehouder Werk & inkomen, stads- en wijkbeheer en sport.[11] Over deze onderwerpen en op informatie-veiligheid in brede zin, wordt aan het gehele college gerapporteerd. Uiteindelijk is de wethouder Financiën, economie en wonen degene die verantwoordelijk voor informatieveiligheid, en deze heeft de doorzettingsmacht om maatregelen op dat terrein te nemen. Daarmee wordt een mogelijk risico op ineffectiviteit ondervangen. Verdeling van aspecten op informatieveiligheid over meerdere

---

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

10 Zie Strategische BIG, Randvoorwaarden, p. 8-9.
In de Health Check ICT-omgeving gemeente Lelystad, mei 2015, is geconstateerd dat er op securitymanagement geen actualisatie van de risicoanalyse is uitgevoerd. De risicoanalyse waar in de health check of ICT audit van sprake is, richt zich op de uitvoering van het zogenoemde securitymanagement. De risicoanalyse waarvan in de BIG sprake is, richt zich op de beleidsmatige component.

11 Suwinet is de elektronische infrastructuur, van onder andere persoonsgegevens op het gebied van werk en inkomen, die gemeenten en UWV bijhouden en raadplegen voor de uitvoering van de sociale zekerheid.

portefeuillehouders zou in theorie een gebrek aan doorzettingsmacht kunnen betekenen. Dat lijkt in dit geval in de praktijk niet aan de orde te zijn.

Op basis van de antwoorden van de CISO constateert de rekenkamer, dat op papier de borging van het informatiebeveiligingsbeleid gebeurt op basis van de Deming-cirkel (Plan-Do-Check-Act), die de CISO zelf coördineert.[12] De CISO rapporteert daarover aan het directieteam en het college.

Op basis van de antwoorden op de vragen uit dit onderzoek stelt de rekenkamer vast, dat de gemeente Lelystad in voldoende mate stuurt op de afspraken uit de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' volgens de vereisten van de BIG. Dat wordt bevestigd door de bevinding uit de ICT healthcheck/ICT audit van mei 2015: *'Informatiebeveiliging op strategisch niveau staat wel op de kaart en is in het strategisch beleid (STIP) als speerpunt benoemd."*[13]

4.2 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)?

Norm: Zie voor wat in de BIG is afgesproken de norm in de vorige paragraaf, §4.1 (p. 9).

In de vorige paragraaf is geconstateerd, dat de risico's op informatieveiligheid geïnventariseerd en geanalyseerd worden. Volgens voorschrift uit de BIG wordt deze analyse gemaakt door de lijn, met ondersteuning van:

- De Chief Information Security Officer (CISO),
- Algemene contactpersonen informatiebeveiliging (ACIB's)[14],
- Applicatiebeheerders,
- Teamleider ICT en ICT-ers,
- Afdeling P&O,
- Jurist,
- Inkoopmedewerker en
- Medewerker Facilitaire Zaken.

---

12 In de Health Check ICT-omgeving gemeente Lelystad (een ICT audit uit 2015), is geconstateerd dat security management als beheerproces zich pas op 'initieel' niveau bevindt. En dat de borging in een Plan-Do-Check-Act cyclus, op basis van een risicoanalyse en een daaraan gerelateerd beveiligingsontwerp niet is aangetroffen. Zoals we ook in voetnoot 9 hebben aangegeven richt deze audit zich op uitvoering van security management. Deze Quick Scan richt zich op de beleidsmatige implementatie van de BIG-maatregelen. Het valt dan ook buiten het bereik van deze scan om te constateren of de bevindingen uit de Health Check van mei 2015 afdoende zijn gepareerd. Een volgende ICT audit zal hierop het antwoord moeten geven.

13 Zie: Health Check ICT-omgeving gemeente Lelystad, mei 2015, p. 6.

14 De Algemeen contactpersoon informatiebeveiliging (ACIB) krijgt van IBD waarschuwingen en informatie met een niet vertrouwelijk karakter, over algemene bedreigingen en incidenten. De ACIB kan deze incidenten op informatieveiligheid melden bij de IBD. De Vertrouwde contactpersoon Informatiebeveiliging (VCIB) krijgt waarschuwingen en informatie met een vertrouwelijk karakter, en mag incidenten melden waarbij vertrouwelijke gegevens worden uitgewisseld.

De risicoanalyse is gedaan op basis van het 'comply or explain'-principe. Anders gezegd: 'pas de maatregel toe of leg uit waarom niet'. In de analyse is gekeken of er al voorzieningen waren getroffen op de maatregel uit de BIG. Reeds getroffen maatregelen en voorzieningen hoefden niet meegenomen te worden in het implementatieplan. Daarna is gekeken of de BIG-maatregel van toepassing is op de situatie van de gemeente Lelystad. Indien deze niet van toepassing is, is de maatregel opgenomen door de CISO in een Verklaring van Toepasselijkheid. Hierin geeft de CISO onder meer uitleg waarom de maatregel niet van toepassing is.[15] De andere aspecten uit de BIG die wel van toepassing zijn op de informatieveiligheidssituatie van de gemeente Lelystad, zijn opgenomen in het implementatieplan. De Verklaring van Toepasselijkheid en het implementatieplan zijn in november 2014 goedgekeurd door het directieteam en het college.

Op strategisch en tactisch niveau is dit conform hetgeen de BIG voorschrijft.

4.3 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?

*Norm: 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.*16 *In de BIG zelf staat niets over rapporteren aan waarstaatjegemeente.nl over het thema informatieveiligheid. 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.*

Directieteam (DT) en college krijgen op verschillende manieren gerapporteerd over de stand van zaken rond informatieveiligheid. Zo rapporteert de accountant jaarlijks aan het directieteam in het kader van de accountantscontrole over beheersmaatregelen op ICT, financiën en de belastingapplicatie. De CISO rapporteert zes tot zeven keer per jaar over informatieveiligheid aan het directieteam en college. Een van de jaarlijkse rapportages gaat over een evaluatie van het informatieveiligheidsbeleid en de voortgang op het implementatieplan. Daarnaast wordt jaarlijks gerapporteerd over de DigID-assessments, de tests op de Basisregistratie Personen (BRP), de Paspoorten en Nederlandse Identiteitskaarten (PNIK) en de Basisadministratie Adressen en

[15] Bijvoorbeeld, 11.7.1 van de BIG: "Beveiligingsmaatregelen op draagbare computers en communicatievoorzieningen." Dit is niet van toepassing verklaard omdat: "Hier is voor getekend door de ambtenaar, bovendien is het een onderdeel van de bewustwording van informatiebeveiliging. De verwachting is dat dit meer incidenten voorkomt dan het doorvoeren van technische maatregelen." Bij navraag hierover is door de CISO aangegeven dat er veel technische maatregelen genomen kunnen worden om mobiele apparaten te beveiligen. Dat kent zijn grenzen in verband met de gebruiksvriendelijkheid. Daarin hebben de medewerkers hun eigen verantwoordelijkheid. Namelijk toepassen van reguliere beveiligingsmaatregelen, zoals een valide password hanteren, deze niet met derden delen en het apparaat niet onbeheerd laten.

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

Gebouwen (BAG).[17] Ook over het gebruik van Suwinet wordt aan directieteam en college gerapporteerd.[18]

De DigID-assessments worden door Logius gemonitord, die dit in opdracht van het Ministerie van BZK uitvoert. Het Ministerie van SZW monitort het veilig gebruik van Suwinet.

De bevindingen uit dit onderzoek wijzen uit, dat de sturingsinformatie naar directieteam en college op orde is. De rekenkamer constateert dat de organisatie voldoet aan hetgeen in de BIG is afgesproken. Verantwoordingsinformatie naar de gemeenteraad kan echter beter afgestemd worden op het belang van het onderwerp en de wens van de raad om hierover voldoende geïnformeerd te zijn. De gemeenteraad krijgt over informatieveiligheid gerapporteerd via de bedrijfsvoeringsparagraaf van het jaarverslag en de begroting. De informatie die in de bedrijfsvoeringsparagraaf is opgenomen wordt door de rekenkamer als (te) summier aangemerkt.[19] De informatie over informatiebeveiliging aan de gemeenteraad kan en moet uitgebreider om hem voldoende bij het onderwerp betrokken te laten zijn. Zeker omdat in het jaarverslag staat vermeld dat het onderwerp informatieveiligheid als een hoog risico wordt opgevat. De kans op incidenten is weliswaar laag, maar als incidenten zich voordoen is de impact hoog. Daarmee is informatieveiligheid niet alleen een uitvoeringsaangelegenheid, maar een beleidskwestie en van strategisch belang. Betere bestuurlijke en politieke borging is gewenst op dit punt. Een manier om dat te realiseren is adequate informatievoorziening aan de raad.

De partijen waar de gemeente Lelystad informatie mee deelt kunnen zich op de hoogte stellen over informatieveiligheid van de gemeente Lelystad via waarstaatjegemeente.nl. Dat is in lijn met hetgeen de gemeenten in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' hebben afgesproken.

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

Norm: 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.[20]

---

17 Over de Basisadministratie Adressen en Gebouwen (BAG) wordt vooral gerapporteerd over de kwaliteit van de gegevens.

18 De laatste rapportage door het Ministerie van SZW over het 'Veilig gebruik Suwinet 2015' is op 8 december 2015 naar het college en de gemeenteraad gestuurd. Daarin is geconstateerd dat Lelystad voldoet aan 7 van de 7 normen uit het Normenkader behorende bij de Verantwoordingsrichtlijn Gezamenlijke elektronische Voorzieningen Suwi (GeVS).

19 Opgenomen in de Jaarstukken 2014, p. 117: "**Informatiebeveiliging** Veel overheidsinformatie is openbaar. Maar de gemeente heeft ook gegevens die beslist niet openbaar mogen worden zoals persoonlijke gegevens van burgers. Met de komst van de decentralisaties is de hoeveelheid privacygevoelige gegevens alleen maar groter geworden. Om de beveiliging van informatie te waarborgen heeft de gemeente informatiebeveiligingsbeleid en is er een functionaris belast met het controleren van de naleving ervan. Bij de organisatie brede risico-inventarisatie komt informatiebeveiliging wel naar boven als hoog risico. De kans op incidenten wordt als gevolg van het reeds bestaande beleid en maatregelen, klein geacht. Maar als een incident toch plaats zou vinden kan de impact daarvan hoog zijn."

20 Zie Tactische BIG, item 14, Bedrijfscontinuïteitsbeheer.

In oktober 2014 heeft het DT een uitwijkprocedure vastgesteld in geval van een grootschalige uitval of verstoring van de ICT. Deze procedure geldt ook voor de baliefunctie van de Stadswinkel, waar de publieksfuncties plaatsvinden. Met een uitwijkprocedure kan de organisatie de ICT op een andere locatie opstarten, zodat de dienstverlening zo spoedig mogelijk weer werkt. Lelystad garandeert dat binnen vier uur na een ernstige calamiteit of verstoring de centrale dienstverlening weer operationeel is. De continuïteit van de gemeentelijke dienstverlening is daarmee gewaarborgd, met een wachttijd van maximaal vier uur.

Tegelijk met de uitwijkprocedure is een testplan voor de uitwijk vastgesteld. Twee keer per jaar moet de uitwijk getest worden. Dat is in 2015 niet gebeurd. Uit de technische reactie blijkt, dat de daarvoor benodigde capaciteit in dat jaar bewust anders is ingezet. De tests zullen in 2016 weer worden opgepakt.

De organisatie heeft een uitgebreide back-up procedure opgesteld. Dagelijks, wekelijks en maandelijks worden back-ups gemaakt van de bestanden in de verschillende systemen. De back-ups worden met de regelmaat waarop ze worden gemaakt gecontroleerd op volledigheid. Lacunes worden alsnog geback-upt. Er wordt nagegaan waarom deze lacunes ontstonden en daar worden maatregelen op genomen, als dat nodig is.

De rekenkamer constateert dat procedures die de continuïteit van de gemeentelijke dienstverlening waarborgen zijn aangetroffen. In 2015 ontbraken de tests op de uitwijkprocedure.

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

Norm: 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.[21]

Gemeente Lelystad kent een contractenregister, waarin afspraken met partners en leveranciers van de gemeente zijn opgenomen. Dat zijn afspraken over bijvoorbeeld looptijd van het contract, voor welke afdeling een dienst of product wordt geleverd, contactpersonen enzovoort. De gemeente kent op die manier de leveranciers en partners waarmee ze samenwerkt.

Sinds begin 2015 hebben gemeenten nieuwe taken in het sociale domein gekregen. In de uitvoering van deze nieuwe taken wordt privacygevoelige informatie van burgers uitgewisseld met andere partijen, die deze beheren en/of bewerken. Als privacygevoelige gegevens van de gemeente door een andere partij worden verwerkt of opgeslagen, blijft de gemeente ervoor verantwoordelijk dat de regels van de Wet bescherming persoonsgegevens (Wbp) worden nageleefd. Om aan die verantwoordelijkheid invulling te geven sluit de gemeente een bewerkersovereenkomst met de externe partij die de gegevens bewerkt.[22] Daarin wordt onder andere geregeld dat de externe partij

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

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

de gegevens zorgvuldig opslaat en verwerkt. En dat voldoende maatregelen worden genomen om de gegevens technisch en organisatorisch te beveiligen.

Ter informatie heeft de CISO aan de partijen, waarmee de gemeente in het sociale domein samenwerkt op het gebied van Jeugdhulp en WMO, presentaties gegeven over informatiebeveiliging en privacy. De CISO heeft deze partijen een op de BIG gebaseerd normenkader Informatiebeveiliging toegestuurd. Partijen moeten in het eerste kwartaal van 2016 een zelftest uitvoeren en inzicht geven in hoeverre zij 'in control' zijn op informatieveiligheid.
Dat zullen andere – toekomstige – partners van de gemeente Lelystad ook moeten doen, voor zover dat relevant is voor de informatieveiligheid.

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

Norm: Aansluiting op de IBD is niet geregeld in de BIG zelf. De algemene en vertrouwde contactpersonen informatiebeveiliging (Algemene Contactpersoon Informatiebeveiliging [ACIB] en Vertrouwde Contactpersoon Informatiebeveiliging [VCIB]) van de gemeente kunnen aangesloten zijn bij de IBD. Dat is belangrijk, omdat de IBD meldingen van beveiligings-incidenten verzamelt en doorgeeft aan deze contactpersonen. En de IBD 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[23] en URL's[24] en doorgeven van de in gebruik zijnde hard- en software (de zogenoemde ICT-foto).

De gemeente Lelystad heeft twee algemene contactpersonen (ACIB) en twee vertrouwde contactpersonen (VCIB) op informatieveiligheid benoemd.[25] Daarmee zijn de eerste twee stappen gezet voor de aansluiting op de IBD. Daarmee krijgen deze functionarissen van de IBD meldingen over onder andere beveiligingsincidenten en softwarelekken. De contactpersonen kunnen incidenten en lekken die zich in Lelystad voordoen, ook doorgeven aan de IBD.

De CISO en een senior informatiemanager zijn de VCIB. Zij behandelen de informatieveiligheids-meldingen met een vertrouwelijk karakter. Twee systeembeheerders/ICT-ers zijn de ACIB. Zij handelen de meldingen met een algemeen karakter af. Gezien het feit dat deze contactpersonen twee systeembeheerders, een informatiemanager en de CISO zijn, constateert de rekenkamer dat zij over voldoende technische kennis beschikken om de meldingen van de IBD goed te kunnen inschatten en adequaat op te kunnen volgen.

De CISO geeft aan dat de stappen 3 en 4 van de aansluiting op de IBD bewust nog niet zijn gezet. Dat wil zeggen dat IBD geen inzage heeft in de IP-adressen en websiteadressen of url's (= stap 3) en de

---

[23] IP-adres (Internet Protocol): Elke computer die is aangesloten op het internet of een netwerk heeft een nummer (IP-adres) waarmee deze zichtbaar is voor alle andere computers op het internet. Men kan dit vergelijken met telefoonnummers.

[24] Url (Uniform Resource Locator): verwijst naar het unieke adres waarmee de locatie van een webpagina op internet wordt aangegeven of een e-mailadres.

[25] Zie voetnoot 13 voor de functies van de Algemene contactpersonen informatiebeveiliging (ACIB) en Vertrouwde contactpersonen informatiebeveiliging (VCIB).

hard- en software-omgeving die bij de gemeente Lelystad in gebruik zijn (= stap 4). Daarmee zou de IBD op maat gerichte adviezen en incidentmeldingen kunnen doorgeven aan de gemeente. Volgens de CISO is dat nog niet gebeurd, omdat de IBD nog geen zekerheid kon geven over de beveiliging van de bij de dienst bewaarde gegevens. De CISO denkt erover na om stap 3 van de aansluiting op IBD op korte termijn te zetten. Stap 4 vindt de CISO momenteel nog te prematuur, gelet op de gevoelige aard van de informatie over hard- en software die de gemeente gebruikt.

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

Norm: 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.[26]

De organisatie heeft een procedure opgesteld voor hoe te handelen bij incidenten op informatiebeveiliging en zwakke plekken in de beveiliging. Afdelingshoofden en teamleiders informeren de CISO over beveiligingsincidenten en in overleg met de CISO wordt de ernst van het incident bepaald. Alle meldingen worden geregistreerd in Topdesk, ongeacht de ernst van het incident.[27]

Minder ernstige incidenten worden aangemeld bij de helpdesk ICT. Tot de minder ernstige incidenten behoren meldingen dat medewerkers niet kunnen inloggen of dat apparaten de data niet goed synchroniseren. Indien uit de registratie in Topdesk blijkt dat meerdere lichte incidenten over hetzelfde onderwerp gaan, wordt dit probleem opgepakt door de afdeling ICT.

Tot de zware incidenten behoren lekken in de website, het niet naleven van beleid op informatiebeveiliging en cyberaanvallen door criminelen. Dit zijn ernstige incidenten, die een (ver)storing kunnen inhouden voor de continuïteit en/of integriteit van bedrijfsprocessen. Bij ernstige inbreuken op de beveiliging komt een team bijeen van CISO, teamleider ICT, lid MT, concerncontroller, experts en eventueel een communicatiemedewerker. De IBD wordt geraadpleegd over bekendheid met en aard van incident en over de juiste manier om daarop te handelen. Vanaf 1 januari 2016 geldt ook de meldplicht datalekken bij de Autoriteit Persoonsgegevens.[28]

De CISO monitort de afhandeling van de incidenten en rapporteert aan het management en het college. De CISO rapporteert minimaal eens per jaar over de beveiligingsincidenten aan het management en college. In 2015 zijn tot medio december geen ernstige incidenten geregistreerd.

---

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

[27] Topdesk is een applicatie (programma) waarmee incidenten op beveiligingsgebied bijgehouden kunnen worden. Onder andere worden aard, aantal en frequentie van de meldingen geregistreerd.

[28] 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.

4.8 Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatieveiligheid via peer reviews, audits of self assessments (zelf tests)? En wordt over het functioneren van de cyclus van informatieveiligheid gerapporteerd aan de raad?

Norm: 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 volgens de P&C-cyclus gerapporteerd aan het lijnmanagement. [29] *Voor rapportage aan gemeenteraden geeft de BIG geen richtlijnen.*

In §4.3, p. 11-12, heeft de rekenkamer geconstateerd, dat er jaarlijkse DigID-assessments worden uitgevoerd, audits op Suwinet en rapportages in het kader van de accountantscontrole op ICT, financiën en belastingapplicatie. Daarnaast zijn er de zelf tests Basisregistratie Personen (BRP), de Paspoorten en Nederlandse Identiteitskaarten (PNIK) en de Basisadministratie Adressen en Gebouwen (BAG). De audits worden uitgevoerd door een medewerker, die een post masteropleiding Internal Auditing (RO) en IT-auditing (RE) heeft gevolgd. Deze functionaris is ertoe geëquipeerd om de assessments adequaat uit te voeren.

Het directieteam en het college worden jaarlijks zes tot zeven keer gerapporteerd over de audits en zelf tests. De gemeenteraad krijgt over informatieveiligheid in de bedrijfsvoeringsparagraaf van het jaarverslag gerapporteerd. Zoals de rekenkamer reeds heeft geconstateerd is de informatievoorziening aan de raad (te) summier en voor verbetering vatbaar, zie p. 12.

4.9 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?

Norm: In de BIG hebben gemeenten afgesproken dat het informatiebeveiligingsbeleid eens in de drie jaar, of zodra zich belangrijke wijzigingen voordoen, wordt geëvalueerd.[30]

De beleidsuitgangspunten van het informatieveiligheidsbeleid zijn in 2014 geactualiseerd. Deze zijn van recente datum en volgens opgave van de CISO nog steeds valide. Na de renovatie van het stadhuis, heeft het Nieuwe Werken sinds 2011 zijn intrede gedaan. Vanaf toen zijn onder andere mobiele apparaten (smartphones en tablets) en verdergaande digitalisering in beleid en bedrijfsvoering opgenomen in het informatieveiligheidsbeleid. Naar aanleiding van de introductie van de BIG is dat beleid in 2014 geactualiseerd. De risicoanalyse, waarop de uitgangspunten van het informatieveiligheidsbeleid zijn gebaseerd, hoeft volgens de CISO voorlopig niet heroverwogen te worden.[31]

---

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

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

[31] Dat geldt in ieder geval het strategisch en tactisch niveau van het informatieveiligheidsbeleid. De audit van mei 2015, dus van recentere datum dan de actualisatie van de beleidsuitgangspunten van eind 2014, geeft aanleiding op operationeel niveau de risico's gestructureerd te actualiseren. Maatregelen daarop zijn reeds voorzien op de korte en middellange termijn. Zie daarvoor de presentatie 'Planning ICT audit'.

De CISO geeft aan dat een relevante recente ontwikkeling het sociaal domein is. Waarbij de gemeenten met externe partijen gevoelige informatie van burgers uitwisselt. Dat brengt grote risico's met zich mee. De gemeente pakt deze aan door met deze partijen bewerkersovereenkomsten te sluiten en presentaties te geven die het belang van informatiebeveiliging en privacy benadrukken. Ook moeten deze partijen vanaf 2016 zelf tests uitvoeren om de gemeente te laten zien dat zij in control zijn op informatieveiligheid. Zie hiervoor ook §4.4, p. 13-14.

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

Norm: In de BIG is afgesproken om te leren van beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren.[32] Als randvoorwaarde is in de BIG onder andere geformuleerd dat informatieveiligheid een verantwoordelijkheid is van het lijnmanagement en dat kennis en expertise essentieel zijn.[33]

Het informatieveiligheidsbeleid is uiteraard afhankelijk van de wijze waarop de medewerkers het in de dagelijkse praktijk uitvoeren. Enerzijds zijn er de protocollen. Anderzijds zullen medewerkers ervan doordrongen moeten zijn, dat deze daadwerkelijk toegepast moeten worden. De CISO geeft aan dat er werk wordt gemaakt van bewustwording op risico's op informatieveiligheid. Op basis van een risicoanalyse zijn Suwinet, Basisregistratie Personen (BRP) en de Paspoorten en Nederlandse Identiteitskaarten (PNIK) hierin tot speerpunten benoemd. De gegevens in deze registratiesystemen zijn zeer vertrouwelijk en fraude heeft direct grote gevolgen voor inwoners en gemeente.

Jaarlijks worden bewustwordingssessies georganiseerd voor specifieke groepen medewerkers. Zo geven de applicatiebeheerders Suwinet en de teamleiders van de afdeling Werk, Inkomen en Zorg (WIZ) jaarlijks een presentatie aan de medewerkers van deze afdeling. Deze presentaties zijn opgesteld door het Bureau Keteninformatisering Werk en Inkomen (BKWI). Voor de medewerkers van de Stadswinkel worden jaarlijks door de teamleiders presentaties gehouden over BRP en PNIK. Ook wordt naar aanleiding van incidenten of veranderende wet- en regelgeving aandacht besteed aan informatiebeveiligingsaspecten.
Bij de indiensttreding leggen alle medewerkers de eed of belofte af. In hun aanstellingsbrief staat een verwijzing naar informatiebeveiligingsbeleid en de gedragscode. In de gedragscode is informatie-beveiliging een aspect. Voor alle medewerkers is het belang van informatieveiligheid in 2014/2015 uitgedragen door vier integriteitscoaches. Dat zijn vier medewerkers die hiervoor een cursus hebben gevolgd. Zij zijn bij alle teams langs geweest, en hebben de gedragscode onder de aandacht gebracht. Hun taak is het uitdragen van de gedragscode, het management te ondersteunen bij integriteitskwesties en op afroep hierover te sparren met leidinggevenden.

Specifiek op informatieveiligheid zal vanaf het eerste kwartaal van 2016 gebruik worden gemaakt van 'Safe & Sound'. Dat is een bewustwordingscampagne die door IBD is ontwikkeld. Het ondersteunt

[32] Zie Tactische BIG, item 13.2.2, Leren van informatiebeveiligingsincidenten.
[33] Zie Tactische BIG, 1.3, Randvoorwaarden.

gemeenten bij het zelf uitrollen van een campagne om onder andere alertheid op informatie-veiligheid te promoten. De campagnemiddelen bestaan uit: posters, ansichtkaarten, banners voor intranet, een muismat, een notitieblok en stickers. Dat gebeurt gemeente breed, voor alle medewerkers die gebruik maken van het netwerk.
Raadsleden worden in de campagne niet mee genomen. Het argument daarvoor is dat zij niet op het netwerk zijn aangesloten. Raadsleden krijgen in hun raadswerk steevast ook met vertrouwelijke informatie te maken. Een punt ter overweging zou zijn raadsleden mee te nemen in een bewustwordingscampagne over informatieveiligheid, voor zover dat onderwerp niet reeds in de introductiecursus en/of gedragscode voor raadsleden wordt behandeld.

Om op de hoogte te blijven van nieuwe ontwikkelingen bezoeken de CISO, ICT-ers, systeem- en gegevensbeheerders en juristen van de gemeente zeven tot acht keer per jaar workshops, praktijkdagen en bijeenkomsten van VNG/IBD/KING. Ook is er een collegiale peergroup, van ambtenaren van verschillende gemeenten, die in specifieke gevallen geraadpleegd kan worden. De CISO is, tot slot, lid van de online community van de IBD. Daarmee houdt de organisatie de kennis op informatieveiligheid vast en bouwt deze verder uit.

Bijlage. Geïnterviewde en geraadpleegde literatuur

Interview

Pieter Poelstra, CISO, gemeente Lelystad

Geraadpleegde literatuur

- Health Check ICT-omgeving gemeente Lelystad, mei 2015
- Back up procedure
- Back up toets
- Collegebesluit Informatiebeveiligingsbeleid november 2014, nr. 141052238
- Informatiebeveiligingsbeleid gemeente Lelystad
- Informatiebeveiligingsplan 2015
- Jaarrekening Lelystad 2014
- Memo Uitwijk oktober 2014 v1.2
- Planning ICT audit, presentatie met maatregelen naar aanleiding van de Health Check ICT-omgeving gemeente Lelystad, mei 2015
- Presentatie Informatiebeveiliging BRP en PNIK – Stadswinkel
- Presentatie Informatiebeveiliging Privacy Jeugd
- Presentatie Informatiebeveiliging Suwinet – WIZ
- Testplan Uitwijk oktober 2014 v1.0
- Verklaring van toepasselijkheid