Vereniging van
Nederlandse Gemeenten

Visitatiecommissie Informatieveiligheid

180 dagen onderweg

Voorwoord

Met veel plezier ben ik samen met Maarten Ruys en Wim Blok in de zomer van 2015 in de Visitatiecommissie Informatieveiligheid gestapt. Ons doel is het vergroten van het handelingsperspectief van gemeenten bij het werken aan informatieveiligheid. Bewustwording van de risico's en kansen van informatie(veiligheid). De wereld verandert en gemeenten moeten mee veranderen. Gemeenten werken dan ook in een hoog tempo aan de digitalisering van hun dienstverlening. De samenleving verwacht van de overheid een professionele en bewuste houding ten opzichte van informatie. Gelukkig merken wij tijdens de gesprekken die wij met bestuurders van gemeenten mogen voeren, dat gemeenten het belang van informatieveiligheid inzien.

Met de Digitale Agenda 2020 geven gemeenten hier als collectief nog een extra impuls aan[1]. De voortgaande digitalisering brengt veel kansen met zich mee in de vorm van efficiëntere en kwalitatief betere dienstverlening, maar deze ontwikkeling kent ook risico's. Denk aan misbruik van (persoonlijke) gegevens en het niet kunnen leveren van kritieke dienstverlening door storingen van de ICT-voorzieningen. Naast risico's inzake kwaliteit van de dienstverlening kan het vertrouwen in de overheid zelf in het geding komen. Ook kunnen gemeenten aanzienlijke financiële risico's lopen als de informatieveiligheid niet goed geregeld is.

Door de verdere digitalisering raken gemeenten ook in toenemende mate 'vernetwerkt'. Denk aan gezamenlijke gestandaardiseerde voorzieningen als DigiD en het gezamenlijk gebruik maken van een Cloud-oplossing. Deze ontwikkelingen van standaardisatie en gezamenlijk gebruik van voorzieningen leiden tot grote voordelen, maar eisen tevens een adequate invulling van informatieveiligheid. Gemeenten zijn dus meer en meer afhankelijk van elkaar en van de manier waarop zij met informatieveiligheid om gaan. En hierbij geldt: de keten is zo sterk als de zwakste schakel.

Informatieveiligheid is een belangrijke randvoorwaarde om de digitale gemeente tot een succes te maken. In de Buitengewone Algemene Ledervergadering van de VNG op 29 november 2013 namen gemeenten vrijwel unaniem de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aan.

[1] Zie VNG ledenbrief 15/034.

Gemeenten erkenden hiermee de urgentie van het informatieveiligheidsvraagstuk en hebben besloten om werk te maken van informatieveiligheid met gelijke kaders en lokaal maatwerk.

Met de resolutie hebben gemeenten tevens aan de VNG en het Rijk gevraagd om aanvullende maatregelen om informatieveiligheid lokaal te kunnen verstevigen. Zo werd de Visitatiecommissie Informatieveiligheid als bestuurlijk en ambtelijk leerinstrument opgericht. Wij vinden het dan ook een 'eer' dat gemeenten met ons over dit zo belangrijke, maar ook vertrouwelijke onderwerp willen doorpraten. We willen bestuurders ondersteunen, als collega's onder elkaar. De Visitatiecommissie Informatieveiligheid is in het leven geroepen om de gemeente verder te helpen. Ons werk vanuit de Visitatiecommissie is met nadruk niet controlerend van aard. Wij zijn graag stimulerend en gericht op het vergroten van het handelingsperspectief van gemeenten.

Het VNG-bestuur heeft de Visitatiecommissie in het voorjaar van 2015 ingesteld. Sindsdien zijn wij met zijn drieën, ondersteund door de VNG, voortvarend aan het werk gegaan. We hebben in de afgelopen maanden meer dan 40 gemeenten mogen bezoeken én kunnen helpen. En gelukkig krijgen we dat ook terug: gemeenten geven aan dat zij het nuttig vinden om specifieke vraagstukken te bespreken en om samen met ons goed na te denken hoe de verschillende verantwoordelijkheden zijn belegd in de organisatie.

Wij danken alle gemeenten die wij tot nu toe hebben bezocht voor de open en constructieve manier waarop wij de gesprekken hebben kunnen voeren.

Tot medio 2017 blijven we als Visitatiecommissie Informatieveiligheid gesprekken voeren met gemeenten. In dit document leest u onze ervaringen tot nu toe.

Frans Backhuijs
Voorzitter van de
Visitatiecommissie Informatieveiligheid

Inhoudsopgave

Jantine Kriens, voorzitter directieraad VNG

“Gemeenten willen goede, snelle en correcte dienstverlening aan hun inwoners en ondernemers leveren. Ze werken daarom hard aan digitalisering. Daarbij is een correcte gegevensbescherming en het borgen van privacy van groot belang voor het vertrouwen. Dit goed blijven doen is complex en wordt steeds complexer door onder andere (nieuwe) Europese wetgeving, de groeiende technische mogelijkheden en de decentralisaties.

De VNG wil gemeenten blijven ondersteunen en stimuleren door van privacy een prioriteit te maken. Ik ben daarom ook blij dat de Visitatiecommissie Informatieveiligheid de aandacht voor informatieveiligheid en informatiebeveiliging vraagt en vasthoudt. Elke gemeente moet continu oog hebben voor informatieveiligheid en actie ondernemen als het beter moet.

Informatieveiligheid raakt (ook) de bedrijfsvoering van een gemeente en vraagt om een bestuurlijke visie, focus en draagvlak. Het is goed dat bestuurders dit onderling bespreken en elkaar helpen bij het op orde brengen en houden van informatieveiligheid en het waarborgen van de privacy van de inwoners.
Een gezamenlijke aanpak is essentieel om de rol van betrouwbare eerste overheid te kunnen blijven waarmaken. De gegevens die via Waarstaatjegemeente.nl beschikbaar zijn geven tevens een waardevol inzicht in ontwikkelingen op het gebied van informatieveiligheid.

Binnen de VNG gebruiken we de inzichten van de Visitatiecommissie bij de beleidsontwikkeling. Daarbij kijken we bijvoorbeeld of het systeem van verplichtende zelfregulering rondom informatieveiligheid voldoende werkt of dat aanpassing nodig is.

Doelen en uitgangspunten van de Visitatiecommissie

Incidenten als DigiNotar en Lektober hebben ons op scherp gezet. Deze incidenten toonden aan dat bestuurlijke aandacht voor informatieveiligheid en goede borging in de gemeentelijke organisatie essentieel zijn voor het informatieveilig handelen van een gemeente. Om de digitale gemeente tot een succes te maken is informatieveiligheid een randvoorwaarde. Gemeenten hebben met het aannemen van de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' in de BALV op 29 november 2013 de urgentie van het informatieveiligheidsvraagstuk erkend en besloten om deze opgave samen op te pakken.

Uitgangspunt daarbij is de zogenaamde verplichtende zelfregulering, waarbij iedere gemeente zelf verantwoordelijk is voor adequate informatieveiligheid. Op koepel- en landelijk niveau kunnen voorzieningen zoals de Informatiebeveiligingsdienst voor gemeenten (IBD) de gemeenten daarbij ondersteunen. In de Resolutie Informatieveiligheid staat het voornemen om een Visitatiecommissie Informatieveiligheid in te stellen om op bestuurlijk niveau stimulans en versterking van perspectief te organiseren. Ook kan deze commissie het (van elkaar) leren bevorderen. De hoofdopgave van de Visitatiecommissie Informatieveiligheid is om in de komende twee jaar in deze behoefte aan ondersteuning, versterken handelingsperspectief en van elkaar leren te voorzien.

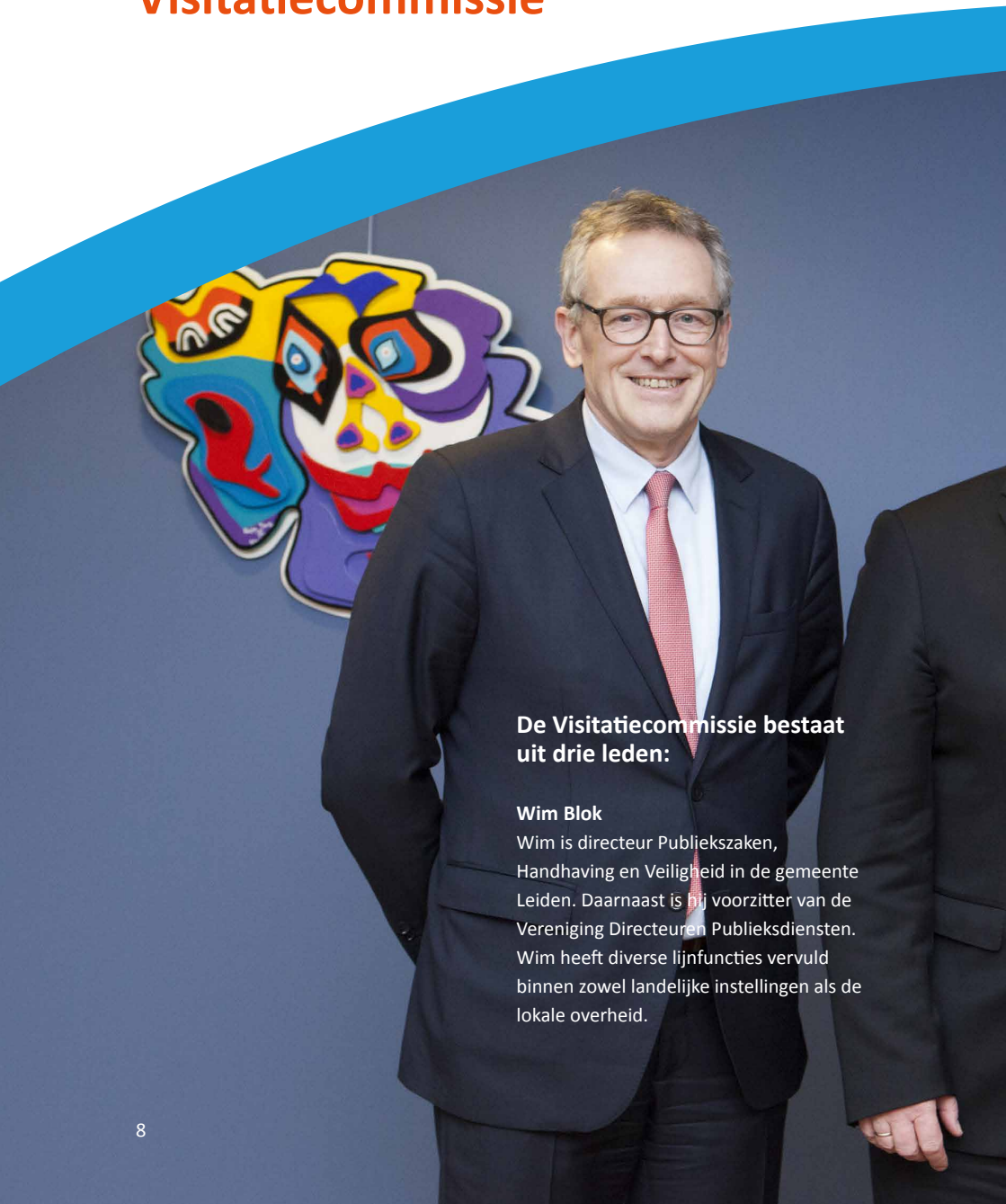
De Visitatiecommissie is in september 2015 met drie doelen van start gegaan:

1. Aandacht voor informatieveiligheid bij gemeenten vasthouden en stimuleren.
2. Vergroten van het handelingsperspectief van gemeenten op het vlak van informatieveiligheid.
3. Toetsen of het systeem van verplichtende zelfregulering werkt en hoe/waar het verbeterd kan worden.

De Visitatiecommissie hanteert de volgende uitgangspunten bij het realiseren van deze doelen:

- De Visitatiecommissie is als project onderdeel van de Digitale Agenda 2020.
- Informatieveiligheid is een voorwaarde voor digitalisering. Informatieveiligheid is vanuit dit perspectief altijd een onderdeel van het succes van de digitale overheid. Hier ligt ook de verbinding met de andere projecten die deel uitmaken van de Digitale Agenda 2020.
- Zelfbeeld van de gemeente vormt de basis.
- De Visitatiecommissie is gericht op stimuleren en bestuurlijk leren. De Visitatiecommissie oordeelt niet en biedt elke gemeenten een handelingsperspectief op maat waarmee een volgende stap kan worden gemaakt.
- De Visitatiecommissie heeft vertrouwelijkheid van informatie als uitgangspunt. Individuele rapportages worden niet gedeeld met derden zonder toestemming van de gemeenten. Informatie in de openbare rapportages is niet terug te geleiden naar individuele gemeenten.
- De Visitatiecommissie betrekt niet zelf de gemeenteraad bij haar visitatie, maar zal iedere gemeente die zij bezoekt sterk aanbevelen het verslag van de Visitatiecommissie te delen met de Raad en daarover een bindende afspraak proberen op te nemen in het verslag.

Samenstelling van de Visitatiecommissie



De Visitatiecommissie bestaat uit drie leden:

Wim Blok
Wim is directeur Publiekszaken, Handhaving en Veiligheid in de gemeente Leiden. Daarnaast is hij voorzitter van de Vereniging Directeuren Publieksdiensten. Wim heeft diverse lijnfuncties vervuld binnen zowel landelijke instellingen als de lokale overheid.

Frans Backhuijs
Frans is burgemeester van Nieuwegein en voorzitter van de Visitatiecommissie Informatieveiligheid. Eerder was hij respectievelijk wethouder in Eindhoven en burgemeester in Oldenzaal. Frans is als vicevoorzitter van de Commissie Dienstverlening & Informatiebeleid nauw betrokken bij de digitalisering van gemeenten.

Maarten Ruys
Maarten is voormalig gemeentesecretaris Groningen en eerder was Maarten onder meer Secretaris-Generaal bij het Ministerie van Sociale Zaken en Werkgelegenheid. Naast de activiteiten van de Visitatiecommissie is Maarten werkzaam als Ketenregisseur Persoonsgebonden Budget.

Werkwijze van de Visitatiecommissie

De werkwijze van de Visitatiecommissie sluit aan op de gedachte van verplichtende zelfregulering: cyclisch leren. In het kort gaat deze gedachte ervan uit dat een mens leert door het onderkennen van waarden (kennis) en het betrokken raken (emoties voelen, draagvlak creëren) bij een onderwerp, in dit geval informatieveiligheid. Is iemand betrokken en heeft hij een positieve associatie bij het onderwerp dan kunnen acties tot stand komen die informatieveiligheid verankeren in de organisatie. Door deze dynamiek systematisch te evalueren kan de organisatie blijven leren over haar eigen gedrag.

De Visitatiecommissie ziet het als de kern van haar opdracht om dit cyclisch leren te versterken. Zij beïnvloedt de gerichtheid op drie manieren:

- Door gerichte interactie met bestuurders en topmanagers over het belang van informatieveiligheid in termen van waarden en met name betrokkenheid;
- Door kennis te verhogen middels het formuleren van een concreet handelingsperspectief waarmee een volgende stap gemaakt kan worden;
- Door de deelname aan externe netwerken te stimuleren en verbindingen tussen gemeenten te leggen.

Daarnaast heeft de Visitatiecommissie ook als opdracht meegekregen om de werking van het systeem van verplichtende zelfregulering te beoordelen.

De Visitatiecommissie besteedt hiervoor in haar gesprekken specifiek aandacht aan de systeemcondities. Hierbij kan gedacht worden aan voorzieningen zoals de IBD of stroomlijning van de verantwoordingsverplichtingen rondom informatiebeveiliging.

De Visitatiecommissie heeft het volgende instrumentarium tot haar beschikking om uitvoering te geven aan haar opdracht:

Gesprekken inclusief voorbereiden via vragenlijst	Gesprekken met bestuur en hoger management over de wijze waarop informatieveiligheid aandacht krijgt en vertaald wordt naar acties.
Gespreksverslagen inclusief handelingsperspectief	Verscherpt beeld van de manier waarop de gemeente werkt aan informatieveiligheid, inclusief een beoordeling van positieve en verbeterpunten.
Communicatie	Communicatie over het werk en de werkwijze van de Visitatiecommissie en tussenresultaten

Waar is de Visitatiecommissie al geweest

De Visitatiecommissie is bij dit schrijven circa 180 dagen onderweg. In totaal zijn 45 gemeenten bezocht. In de kaart hieronder is weergegeven waar de Visitatiecommissie al is geweest.

Met gemeenten in de gebieden waar de Visitatiecommissie nog niet op bezoek is geweest, zijn al afspraken ingepland voor de komende tijd.

Legenda

1. Westland
2. Brummen
3. Putten
4. Nunspeet
5. Gouda
6. Zederik
7. Leusden
8. Vianen
9. Huizen
10. Geldermalsen
11. Culemborg
12. Tiel
13. Heerhugowaard
14. Zaanstad
15. Purmerend
16. Apeldoorn
17. Zutphen
18. Amersfoort
19. Landsmeer
20. Haarlemmermeer
21. Nijmegen
22. ’s Hertogenbosch
23. Geldrop
24. Nuenen
25. Son en Breugel
26. Breda
27. Bergen op Zoom
28. Goirle
29. Roermond
30. Gemert-Bakel
31. Oegstgeest
32. Noordwijk
33. Harderwijk
34. Renswoude
35. Druten
36. Venlo
37. Asten
38. Bergen (Limburg)
39. Dalfsen
40. Kampen
41. Raalte
42. Oostzaan
43. Wormerland
44. Amsterdam
45. Waterland

Gemeenten ervaren het bezoek van de Visitatiecommissie over het algemeen als zeer positief. Gemeenten werken graag mee aan een bezoek en onderkennen het belang en nut van de Visitatiecommissie. Ook de terugkoppeling naderhand is positief. De commissie kreeg meermaals als feedback dat de bezoeken zowel op bestuurlijk als ambtelijk niveau als leerzaam en nuttig worden ervaren.

Om het handelingsperspectief op informatieveiligheid van gemeenten te vergroten ontvangt een gemeente binnen twee weken na het gesprek een (concept)verslag. Dit verslag is altijd toegesneden op de specifieke situatie van de gemeente. Het verslag op maat aan gemeenten wordt als waardevol ervaren en is voor veel gemeenten aanleiding om hun activiteiten op het vlak van informatieveiligheid te herijken en/of te intensiveren.

Eerste bevindingen na bezoek aan ruim 40 gemeenten

De Visitatiecommissie constateert dat de bezochte gemeenten serieus werk maken van informatieveiligheid. Ook de trends die te zien zijn op Waarstaatjegemeente.nl wijzen op een positieve ontwikkeling op het vlak van informatieveiligheid. Deze gemeenten onderkennen daarbij het belang van blijvend leren. Vanzelfsprekend werkt iedere gemeente hierbij binnen haar lokale mogelijkheden in termen van (ook financiële) kaders, capaciteit en kennis. Het verrast dan ook niet dat er verschillen waarneembaar zijn tussen gemeenten. Het concreet vergroten van het handelingsperspectief van gemeenten valt of staat bij de aansluiting op de specifieke situatie in de gemeente. De commissie levert daarom een op maat gesneden advies. Dit neemt niet weg dat in alle adviezen generieke elementen zijn te herkennen die elke gemeente aanknopingspunten biedt om verder te werken aan informatieveiligheid.

Uitvraag via Waarstaatjegemeente.nl

Gemeenten kunnen hun eigen scores opzoeken op Waarstaatjegemeente.nl. Nog niet alle gemeenten hebben de uitvraag via Waarstaatjegemeente.nl ingevuld. Het spreekt voor zich dat hoe meer gemeenten informatie aanleveren, des te betrouwbaar de analyses zijn die daaruit volgen. Dit geldt zowel voor de analyses die gemeenten zelf kunnen maken ten behoeve van hun eigen ontwikkeling als analyses op het niveau van het gemeentelijk domein. Oproep aan gemeenten is daarom om gegevens aan te leveren. Zie hiervoor Waarstaatjegemeente.nl bij ‘Cijfers aanleveren’.

Zeven lessen

De Visitatiecommissie heeft haar bevindingen tot nog toe naar zeven algemene lessen voor gemeenten vertaald:

1. Zoek zoveel mogelijk de aansluiting tussen informatieveiligheid en actuele politiek-bestuurlijke vraagstukken om de aandacht in de breedte van het college en vast te houden.

   Informatieveiligheid is onderdeel van veruit de meeste vraagstukken waarmee gemeenten geconfronteerd worden. Denk aan de uitdagingen in het sociaal domein en (in de toekomst) de Omgevingswet. De kunst is om informatieveiligheid hierbij op een manier te framen dat de urgentie gevoeld wordt zonder de negatieve consequenties werkelijk te 'moeten' ervaren. Informatieveiligheid moet voor iedereen gaan voelen als voorwaarde voor succes. Hierbij kunnen de volgende adviezen helpen:

   - Maak duidelijk dat informatieveiligheid geen onderwerp is dat alleen bij anderen speelt. Sommige gemeenten communiceren via intranet bijvoorbeeld over phishingsmails of DDOS-aanvallen. Andere gemeenten dragen actief uit informatieveiligheid belangrijk te vinden door structureel ethische hackers (soms ook tegen beloning) uit te dagen om veiligheidslekken te vinden.
   - Versterk de urgentie van informatieveiligheid door de portefeuillehouder (of gemeentesecretaris) te positioneren als belangrijkste pleitbezorger. Door op dit niveau in de organisatie aandacht te vragen voor het onderwerp, wordt het belang en de urgentie onderstreept. Het 'verhaal' van de pleitbezorger is bij voorkeur niet herhalend, maar sluit aan bij de nieuwe ontwikkelingen en toekomstige uitdagingen. Denk aan een aankomende fusie met een buurgemeente, vragen rondom privacy in het sociaal domein of innovatieprogramma's rondom bijvoorbeeld de slimme stad en de slimme gemeente.
   - Houdt in de gaten welke (bijna) incidenten voorvallen. Zo kan de urgentie van informatieveiligheid beter aangetoond worden. Bij (bijna) incidenten kan altijd de helpdesk van de IBD gebeld worden. Gemeenten hebben eigenlijk elke dag te maken met pogingen om de informatieveiligheid te verstoren. Sommige gemeenten houden scherp in de gaten welke incidenten op gebied van informatieveiligheid (van klein tot groot) zich voordoen in de organisatie. De meeste gemeenten worden echter pas écht met informatieveiligheid geconfronteerd als het hun reguliere manier van werken verstoort.

2. Ga snel van onderkenning van het belang van informatieveiligheid naar actie.
   Dit kan door jaarlijkse actieplannen vast te stellen op basis van een informatieveiligheidsbeleidsplan en een inventarisatie van de risico's. De jaarplannen geven ruimte om in te spelen op nieuwe risico's en ontwikkelingen en maken tegelijkertijd concreet waarmee op korte termijn aan het werk te gaan. Het jaarplan vormt daarmee dé basis van de uitvoering. De Informatiebeveiligingsdienst voor Gemeenten (IBD) ondersteunt gemeenten bij het het implementeren van het gemeenschappelijk normenkader voor informatiebeveiliging (de baseline informatiebeveiliging gemeenten: de BIG) en hiermee de uitvoering en planning van het informatieveiligingsbeleid. Dit doet de IBD onder andere door het beschikbaar stellen van operationele kennisproducten en door het organiseren van regiosessies in het land.

3. Integreer informatieveiligheid in de reguliere sturingscyclus om scherp de uitvoering te kunnen volgen.
   Het jaarplan informatieveiligheid biedt houvast om gericht de voortgang te monitoren. Diverse gemeenten hebben informatieveiligheid inmiddels geïntegreerd in de reguliere sturingscyclus. Door de voortgang op het vlak van informatieveiligheid in kwartaalrapportages te beschrijven, kan (bij)gestuurd worden door de gremia die hiermee belast zijn in de organisatie. Ook verbeterpunten kunnen op deze manier snel gesignaleerd worden en meegenomen worden in volgende verbeterstappen. Hiermee krijgt het leren binnen de organisatie steviger ondergrond.

4. Leg actief verantwoording af over informatieveiligheid via het jaarverslag en periodieke besprekingen met de Raad.
   Door informatieveiligheid te integreren in de reguliere sturingscyclus kan ook de Raad periodiek goed geïnformeerd worden. Sec informeren wordt door veel gemeenten als onvoldoende ervaren. Het betrekken van de Raad bij de strategische vraagstukken die volgen uit de vorderingen en inspanningen is een manier om op periodieke basis de interactie aan te gaan. Eén van de bezochte gemeenten pakt dit systematisch aan door jaarlijks een nota te schrijven voor de Raad waarin de belangrijkste uitdagingen en beoogde besluiten op het vlak van informatieveiligheid zijn beschreven.

5. Werk op een systematische manier aan het leren en sluit daarbij aan bij het kennisniveau van de organisatie.

   De Visitatiecommissie komt in de praktijk een wisselend niveau van kennis op zowel bestuurlijk als topambtelijk niveau tegen. Vaak is het kennisniveau afhankelijk van persoonlijke interesse en achtergrond. In veel organisaties is het gedrag en de houding, naast de bewustwording van de medewerkers reeds een aandachtspunt. Hier wordt aan gewerkt door (vaak ludieke) bewustzijnsacties en campagnes. Tegelijkertijd constateren gemeenten zelf dat gedrag en houding blijvend om aandacht vragen. Valkuil voor gemeenten is dat als bewustzijnsacties worden herhaald het effect vermindert. Structurele aandacht is dus geen kwestie van een herhaling van stappen. Belangrijker is het systematisch voortbouwen op de kennis die medewerkers opdoen en de gedragsveranderingen die zichtbaar zijn. Dit vraagt om een leerbeleid waarin ook periodiek aandacht is voor het kennis- en bewustzijnsniveau in de organisatie. Door telkens na te denken over passende acties kan het leren vitaal worden gehouden. Dit gesteund door de durf in de organisatie elkaar aan te spreken op informatieonveilig gedrag.

6. Besteed in afspraken met leveranciers expliciet aandacht aan informatieveiligheid.

   De Visitatiecommissie adviseert gemeenten om in de relatie met leveranciers expliciet aandacht uit te laten gaan naar informatieveiligheid. De Visitatiecommissie doet de suggestie om dit te doen door lopende contracten te screenen op informatieveiligheid en alvast in beeld te brengen waar verbeteringen mogelijk zijn. Speciale aandacht wordt daarbij gevraagd voor de technische kant van informatieveiligheid, denk aan afspraken over patching en back-ups. Daarnaast heeft de Visitatiecommissie waargenomen dat in de inkoopprocedures het consulteren van de CISO een werkwijze is die helpt om informatieveiligheid vanaf het begin van de inkoopprocedure onder de aandacht te brengen. Ook na het sluiten van het contract kan de CISO een rol spelen door bijvoorbeeld controles te (laten) uitvoeren op de mate waarin afspraken worden gerealiseerd.

7. Pas de sturingsvorm voor het realiseren van verbeteringen aan op de situatie van de gemeente.

Voorgaande lessen kunnen gemeenten helpen om het inhoudelijk programma verder aan te scherpen. De gemeenten die de Visitatiecommissie tot nog toe heeft gesproken hebben stuk voor stuk aangegeven het advies te gaan gebruiken bij het verder vormgeven van informatieveiligheid. Hoe vervolgens sturing wordt gegeven op de realisatie van het verscherpte inhoudelijk programma is afhankelijk van de specifieke situatie per gemeente.

- Als de governance staat en werkt ligt het meest voor de hand om vanuit de reguliere lijn te sturen op de realisatie van het inhoudelijk programma.
- Als inhoudelijk een grote stap moet worden gezet, die tijdelijk extra aandacht vraagt en lastig is vrij te maken in de reguliere sturing, ligt het voor de hand om programmasturing te hanteren.
- Als het ontbreekt aan een goed werkend regulier sturingsmechanisme heeft het ook de voorkeur om het inhoudelijk programma (incl. governancevraagstuk) tijdelijk vanuit programmasturing vorm te geven.

Bevindingen ten aanzien van het systeem van verplichtende zelfregulering

Naast het vasthouden van de aandacht voor informatieveiligheid bij en het vergroten van het handelingsperspectief van gemeenten, kreeg de Visitatiecommissie ook als opdracht mee om te adviseren over de werking van het systeem van verplichtende zelfregulering. Op basis van de gevoerde gesprekken werden enkele barrières in de werking van het systeem duidelijk. Over de inrichting van het systeem van verplichtende zelfregulering zijn vier voorlopige adviezen gegeven aan VNG en het Ministerie van Binnenlandse Zaken:

1. Stroomlijn de auditverplichtingen op informatieveiligheid.
   Gemeenten geven aan veel tijd kwijt te zijn aan de uitvoering van de uiteenlopende audits op informatieveiligheid. Al bij het opstellen van de Resolutie Informatieveiligheid is aangegeven dat gestreefd wordt naar een vermindering van de auditlasten. De ministeries van BZK, I&M en SZW, VNG, verschillende gemeenten en andere partijen zoals de ADR werken nu aan deze vermindering door inhoudelijke en procesmatige stroomlijning van de verschillende verplichtingen via het project Eenduidige Normatiek Single Audit (ENSIA). Advies van de Visitatiecommissie is om dit project zowel ambtelijk als bestuurlijk te steunen en waar mogelijk versneld vorm te geven. Het vraagstuk speelt immers nú bij gemeenten.

Doelstelling ENSIA

Hoofddoel

Het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid dat in 2017 door alle gemeenten wordt gebruikt.

Subdoel

Verantwoording over BRP, PUN, BAG en BGT op aspecten anders dan informatieveiligheid, wordt op hetzelfde moment uitgevraagd als de verantwoording over informatieveiligheid. Daarnaast wordt waar mogelijk geharmoniseerd op taalgebruik, tooling en verantwoordingsafspraken.

Randvoorwaarden voor het verantwoordingsstelsel

Het verantwoordingsstelsel is erop gericht om horizontale en verticale verantwoording af te leggen over informatieveiligheidsaspecten zoals deze verwoord zijn in de BIG en de normensets van BRP, PUN, DigiD, SuwiNet, BAG en BGT.
Het horizontale verantwoordingsproces vormt de basis voor het verticale verantwoordingsproces. Bij het afleggen van verantwoording wordt het principe van single information audit toegepast; alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces. Onderdelen van het horizontale verantwoordingsproces zijn: het invullen een zelfevaluatievragenlijst, een In Control Verklaring (ICV), een IT- audit en opname van het onderwerp informatieveiligheid in de jaarverslag van de gemeente. In het horizontale verantwoordingsproces wordt aangesloten bij de P&C van gemeenten.

2. Zorg dat het gemeentebestuur actief aanstuurt op verdere aansluiting van de gemeente bij de IBD.

De Informatiebeveiligingsdienst voor Gemeenten (IBD) werkt voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen. Eén van de doelen van de IBD is het leveren van concrete ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging. De Visitatiecommissie merkt dat de IBD bij gemeenten als deskundig bekend staat. Gemeenten geven aan graag hun kennis en expertise te delen met andere gemeenten. Veel gemeenten nemen dan ook actief deel aan de IBD-community en maken gebruik van de helpdesk van de IBD. De Visitatiecommissie adviseert gemeenten om alle stappen in het aansluitplan van de IBD te doorlopen. Alleen indien de IBD over de juiste gemeentelijke informatie beschikt is zij in staat gemeenten direct te informeren en te helpen bij kwetsbaarheden of incidenten. Gemeenten vinden in het algemeen de IBD een voorziening die absoluut van toegevoegde waarde is in het gemeentelijk domein.

3. Werk aan verstevigen van informele gemeentelijke kennisnetwerken.

Het ontbreekt in de ogen van de Visitatiecommissie op dit moment aan een (informeel) kennisnetwerk die de gerichtheid en het leren op bestuurlijke en topambtelijk niveau structureel stimuleert. De Visitatiecommissie kan hieraan een impuls geven door gemeenten met elkaar in contact te brengen. Tegelijkertijd vinden de leden van de Visitatiecommissie het van belang om de aandacht, die nu wordt gecreëerd voor het onderwerp te borgen door bestuurlijke en topambtelijke kennisnetwerken op het vlak van informatieveiligheid te bouwen waarin kennis en kunde onderling kan worden uitgewisseld. Netwerken die ook in de toekomst het vasthouden van de aandacht en het verspreiden van de kennis ondersteunen. De Visitatiecommissie doet daarbij de suggestie om het onderwerp binnen bestaande netwerken meer en meer te agenderen, met de focus op toekomstgerichte onderwerpen, zoals: de data-gestuurde gemeente, de nieuwe Omgevingswet en smart cities.

4. Geef richting en handelingsperspectief

Gemeenten geven aan behoefte te hebben aan richting en handelingsperspectief in de conceptuele discussie over de relatie tussen dienstverlening, privacy, informatieveiligheid en integriteit. Gemeenten zijn dagelijks bezig met de privacybescherming van hun inwoners. Hierbij gaat het in de eerste plaats over de verwerking van persoonsgegevens op een juridisch juiste en technisch veilige manier. Maar privacy gaat over meer dan juridische vragen ("wat mag wel of niet?") of de technische mogelijkheden ("wat kan wel of niet/wat is veilig"). Privacy gaat in het gemeentelijke domein vooral ook over de relatie tussen burger en gemeente, en het vertrouwen van de burger in de gemeentelijke overheid. Gemeenten hebben er groot belang bij om collectief te werken aan de versterking en versteviging van hun denken en doen ten aanzien van privacy en privacybescherming. In de eerste plaats om een betrouwbare eerste overheid voor hun burgers en partners te zijn en blijven. Maar ook om omvangrijke bestuurlijke boetes te voorkomen, die met de invoering van de nieuwe Europese wetgeving mogelijk worden. De VNG wil de komende periode steviger inzetten op het stimuleren, faciliteren en ondersteunen van gemeenten.
In de afgelopen maanden zijn daarvoor een verkenning en een enquête gehouden. Op basis daarvan zal een samen met gemeenten gewerkt worden aan een bestuurlijke kader, een agenda en het ondersteuningsaanbod. De Visitatiecommissie adviseert om dit verder voort te zetten. Ook hiervoor geldt dat de gemeenten nú worstelen met dit vraagstuk.

Tot slot: een ongevraagd doch belangrijk advies

De Visitatiecommissie heeft als belangrijke meeropbrengst opgehaald dat gemeenten ‘last’ ondervinden van het sterk versnipperde ICT-landschap van Nederlandse gemeenten. De versnippering zorgt voor (onnodig sterke) complexiteit en bevordert dienstverlening én informatieveiligheid in het gemeentelijk domein niet. In het algemeen ervaren gemeenten hun positie ten opzichte van (grote) leveranciers als ongelijkwaardig in termen van kennis en expertise. Vanuit deze constatering heeft vrijwel iedere bezochte gemeente de wens uitgesproken naar het realiseren van meer centrale aansturing/coördinatie op het gebied van ICT en leveranciersmanagement.

Deze wens is eerder ook meer in algemene zin verwoord in de Digitale Agenda 2020 zoals vastgesteld tijdens de ALV 2015. In lijn met de wens van gemeenten heeft de VNG een verkenning uitgevoerd naar het organiseren van Collectieve Gemeentelijke Informatievoorzieningen en dienstverlening. De uitkomst van de verkenning bevestigt de lijn die de Visitatiecommissie in de gesprekken heeft geconstateerd. De problematiek van de I-voorzieningen is complex en gemeenten willen hierin worden ontzorgd. Standaardisering en collectief aanbod is onderdeel van het advies. Tijdens de ALV 2016 worden op basis van de uitkomsten van de verkenning voorstellen gedaan om de concrete uitwerking van het organiseren van de collectivisering in de tweede helft van 2016 te realiseren. Hierbij zullen de bovengenoemde uitkomsten van de bezoeken van de Visitatiecommissie als input voor de concretisering worden meegenomen.

Informatiebeveiligingsdienst voor gemeenten (IBD)

De IBD is een gezamenlijk initiatief van de VNG en KING en actief sinds 2013. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete (incident)ondersteuning aangaande informatiebeveiliging. Alle gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD. Om de gehele dienstverlening van de IBD af te kunnen nemen en elke gemeente gericht te kunnen helpen, heeft de IBD specifieke informatie nodig van elke gemeente. Hiervoor dient iedere gemeente zich 'officieel' aan te sluiten bij de IBD.

Verder aansluiten bij de IBD?

Alle gemeenten hebben inmiddels stappen 1 en 2 van het aansluitproces voltooid door het aanstellen van algemene (ACIB) en vertrouwde (VCIB) contactpersonen informatiebeveiliging. Het aansluitproces bevat twee aanvullende stappen om de complete dienstverlening van de IBD op maat te maken voor uw gemeente

Stap 3: het doorgeven van IP-adressen en URL's

Zodra de VCIB bij de IBD is vastgelegd, kunt u als gemeente uw IP-adressen en URL's doorgeven aan de IBD en hierdoor gebruik gaan maken van de dienstverlening behorende bij Incidentdetectie. De IBD controleert in samenwerking met het NCSC of uw IP-adressen of domeinen voorkomen in (internationale) lijsten met bekende kwetsbaarheden. Als dit het geval ontvangt u van de IBD gerichte informatie en kunt u direct passende maatregelen treffen.

Stap 4: Het aanleveren van in gebruik zijnde hard- en software

De IBD ontvangt op continue basis waarschuwingen over specifieke hard- en softwareproducten. Om deze waarschuwingen en adviezen gericht te kunnen verspreiden, moet de IBD inzicht hebben in de hard- en software die bij uw gemeente in gebruik is. Deze informatie kunt u met de IBD delen door het invullen van een gemeentelijke 'ICT-foto' en daarin aan te geven welke producten u gebruikt. Met behulp van deze 'ICT-foto' is de IBD in staat om uw gemeente gerichte adviezen te leveren.

Hoe nu verder

De Commissie is bijna halverwege haar doel: met 120 gemeenten het (bestuurlijk) gesprek voeren over informatieveiligheid. De planning is om de overige gesprekken te voeren tot en met medio 2017. Het plan is voor de periode tot en met zomer 2016 is inmiddels ingevuld. Ook veel gesprekken in de tweede helft van 2016 zijn reeds gepland.

Voor meer informatie over de Visitatiecommissie en haar werkzaamheden kunt u contact opnemen met de VNG via informatiecentrum@vng.nl. Of kijk op www.vng.nl.

Simone Roos, Directeur-generaal Overheidorganisatie

“Hier ligt een mooi jaarverslag van de visitatiecommissie. Deze commissie doet goed werk en dat blijkt ook. Steeds meer gemeenten, ook op bestuurlijk niveau, geven aandacht aan hun informatieveiligheid en nemen hun verantwoordelijkheid daarvoor. Informatieveiligheid is belangrijk en zal dat ook altijd blijven. Zonder adequate beveiliging bij de overheid kan het maatschappelijk functioneren en vertrouwen in de overheid worden geschaad. Daarmee kan bovendien de rechtszekerheid voor burgers en bedrijven in gevaar komen. Het is daarom heel positief dat gemeenten hun verantwoordelijkheid hier goed oppakken en hard aan het werk zijn met de implementatie van de gemeentelijke baseline informatieveiligheid. Kwetsbaarheden en ongelukken zijn echter nooit geheel uit te sluiten. Incidenten zullen er altijd zijn. We worden dan ook nog regelmatig geconfronteerd met incidenten, waar bestuurders erop aan kunnen dat hun organisatie snel en adequaat en maatregelen treft. Het is daarom belangrijk om daarvan te leren en daarmee de informatieveiligheid op een hoger plan te brengen. Bewustwording helpt daarbij, want ook bij informatieveiligheid gaat het heel vaak om mensenwerk.

De Visitatiecommissie levert in dat opzicht goed werk: bewustwording bij bestuurders over hun verantwoordelijkheid voor hun organisatie. Een van de doelstellingen van de Visitatiecommissie is immers het belang van informatieveiligheid onder de aandacht te houden van bestuurders, leidinggevenden en anderen in gemeenten.

Verantwoording houdt iedereen scherp. De gemeenteraad heeft hier een natuurlijke rol. Het is daarbij van belang hoe verantwoording wordt afgelegd. We willen graag de administratieve lasten beperkt houden. Om daarin te voorzien is project ENSIA opgezet: de verticale verantwoording kan worden gebaseerd op de integrale horizontale verantwoording over de gemeentelijke baseline. Zo kunnen we ons blijven concentreren op de essentie: informatieveiligheid.”

Vereniging van
Nederlandse Gemeenten

Colofon
Publicatiedatum: mei 2016
Eindredactie: Communicatie KING
Ontwerp: Smidswater, Den Haag