Verslag Visitatiecommissie Informatieveiligheid

Gemeente	Papendrecht Zwijndrecht Sliedrecht
Tijd	20 april 2016, 9:30 uur
Aanwezig gemeente	Roelof van Netten (Papendrecht) Karen van Rijswijk (Papendrecht) Richard Korteland (Papendrecht) Eric Lam (Papendrecht) Rita van Breugel (Sliedrecht) Henk-Willem Langhorst (Sliedrecht) Jannes Blokstra (Zwijndrecht) Dominic Schrijer (Zwijndrecht) Peter de Nooijer (Zwijndrecht) Henk van Beelen (Zwijndrecht) Bas Verheijen (Drechtsteden) Nico Noorland (Drechtsteden)
Aanwezig Visitatiecommissie Informatieveiligheid	Frans Backhuijs (voorzitter) Wim Blok Jeroen Boot (secretaris)

Algemene opmerking over samenwerking in de GR Drechtsteden

De gemeenten Papendrecht, Sliedrecht en Zwijndrecht maken met drie andere gemeenten deel uit van de Gemeenschappelijke Regeling Drechtsteden (GRD). De GRD is sinds 8 maart 2006 de uitvoeringsorganisatie die zorgt voor een efficiënte en effectieve uitvoering van taken die door de Drechtstedengemeenten zijn opgedragen of overgedragen.

Daarnaast behartigt de GRD gemeenschappelijke belangen daar waar dossiers een duidelijk regionaal of bovenregionaal karakter hebben en waarbij een regionale aanpak meerwaarde heeft.

De GRD begon relatief klein in omvang, maar is inmiddels een professionele en resultaatgerichte organisatie met in totaal zo'n 800 medewerkers.

De taken van de GRD worden uitgevoerd door zes dochterorganisaties, waaronder Servicecentrum Drechtsteden (biedt diensten op het gebied van personeel & organisatie, financiën, communicatie, inkoop, juridische zaken en ICT). Informatieveiligheid is uitdrukkelijk een onderwerp dat op GR niveau wordt aangepakt, overigens zonder dat daarbij de verantwoordelijkheid is verlegd: deze ligt bij de individuele gemeenten.

Inleiding

De Commissie informatieveiligheid dankt de gemeenten Papendrecht, Sliedrecht en Zwijndrecht, alsmede GR Drechtsteden, hartelijk voor haar gastvrijheid. De Commissie heeft een open gesprek kunnen voeren, wat zij zeer heeft gewaardeerd. Ze denkt een goed beeld te hebben gekregen van de wijze waarop de gemeenten Papendrecht, Sliedrecht en Zwijndrecht werken aan informatieveiligheid en wat de grootste uitdagingen zijn.

De Commissie heeft het beeld dat de gemeenten Papendrecht, Sliedrecht en Zwijndrecht op een realistische manier werken aan informatieveiligheid. Daarbij viel de Commissie specifiek de volgende zaken positief op:

- De gemeenten hebben in GR Drechtstedenverband een professionele en leuke bewustwordingscampagne opgezet waarbij door middel van onder meer posters de aandacht op informatieveiligheid wordt gevestigd. De Commissie moedigt aan dat nieuwe initiatieven in de planning staan (*mystery guests*; *phishing* e-mails). Ter sprake is geweest dat mogelijkheden liggen in het verbinden van informatieveiligheid met integriteitsvraagstukken. De Commissie onderschrijft dat hierin een kans ligt om informatieveiligheid meer structureel en organisatiebreed op de agenda te krijgen en te houden.
- Het kennisniveau is dankzij samenwerking in de GR Drechtsteden op een hoog niveau.
- Tijdens het gesprek kwam aan de orde dat door middel van subtiele onderlinge competitie en benchmarking in GR verband effectieve stimulansen gegeven worden om bepaalde thema's naar een hoger plan te trekken. De Commissie meent dat dit een aardige manier is om ook informatieveiligheid verder te verstevigen en te stimuleren.

In dit verslag beschrijven we achtereenvolgens ons verkregen beeld, een aantal aanbevelingen voor het handelingsperspectief van de gemeente voor de komende periode en enkele slotnoties. Het beeld van de Commissie is gecategoriseerd in vijf onderdelen: 1. Digitalisering algemeen; 2. Gerichtheid; 3. Verankering; 4. Extern leren en 5. Werking.

Handelingsperspectief

Ga verder op de ingeslagen weg en maak de vervolgstap naar een structureel beleid op het gebied van informatieveiligheid

In GR Drechtstedenverband zal in dit jaar de GAP-analyse uitgevoerd worden. De Commissie verwacht dat deze analyse nader momentum zal geven voor het onderwerp informatieveiligheid en de mogelijkheid geeft om in de nabije toekomst concrete en significante vervolg stappen te zetten. De Commissie onderschrijft de ambitie om deze aandacht niet *ad hoc* of op basis van incidenten maar op basis van een structurele agenda en actieplannen om te zetten naar concrete acties. De Commissie roept op om hierbij ook oog te hebben voor (eventuele) verschillen tussen de individuele gemeenten.

Daarnaast beveelt de Commissie aan om een expliciete afweging te maken over prioriteit en intensiteit waarmee de veelheid aan risico's op het vlak van informatieveiligheid beheerst worden. De Commissie beveelt aan om de concrete keuzes en de volgorde waarin de gemeenten de risico's gaan adresseren, in nauwe dialoog tussen de ambtelijke organisatie en bestuur/portefeuillehouder tot stand te laten komen.

Benadruk het belang van informatieveiligheid voor politiek-urgente thema's richting de Colleges en de Raden

De Commissie beveelt aan om het gesprek met de Colleges en de Raden van de individuele gemeenten concreet vorm te geven door aandacht te vragen voor informatieveiligheid als onderdeel van politiek-urgente vraagstukken of door het organiseren van themasessies. Op structurele basis zijn dit onderwerpen zoals financiën en de veranderingen in het sociaal domein. Door informatieveiligheid te framen als een randvoorwaarde voor het realiseren van haar ambities biedt het handvatten om een toekomstgericht gesprek met de Colleges en Raden aan te knopen over informatieveiligheid.

Systematiseer het leren; werk aan een leerprogramma

De gemeenten geven al uitvoering aan diverse leer- en bewustzijnsacties (in de planning staan: *mystery guest*, phishing mails). De Commissie doet de suggestie om dit als basis te gaan gebruiken voor verdere systematisering van het leren. Door leeracties als i-Bewustzijn te verbinden met opleidingsplannen en systematische aandacht voor het kennisniveau in de organisatie wordt het leren binnen de organisatie steviger ondergrond geboden. Concreet kan het kennisniveau in beeld worden gebracht met een periodieke kennispeiling via een game of een enquête. Periodieke interactie met het lijnmanagement (verantwoordelijke teamleiders) over het verder systematiseren van het leerbeleid is daarbij wenselijk. Dit geeft de mogelijk om heel gericht te blijven zoeken naar de best werkende mix van interventies en acties. De VNG kan daarbij, desgevraagd, behulpzaam zijn om de verbinding tussen gemeenten te leggen. Ten slotte beveelt de Commissie aan om de samenhang met het integriteits- en privacybeleid te zoeken.

Sluit tot en met stap 4 aan bij IBD

De gemeenten zijn tot en met stap 3 aangesloten bij IBD. De Commissie benadrukt het belang om tot en met stap 4 (het aanleveren van in gebruik zijnde hard- en software: de gemeentelijke ICT-foto) aan te sluiten bij de IBD. Aansluiting tot en met stap 4 stelt de IBD in staat om gericht te waarschuwen bij concrete incidenten/dreigingen. Gemeenten krijgen zo meer inzicht in incidenten die zich bij collega-gemeenten hebben voorgedaan. Dit kan bovendien het bewustzijn verder vergroten.

Sturen op het blijven verbeteren vanuit de lijn

Zoals de gemeenten hebben benadrukt tijdens het gesprek, is informatieveiligheid een onderwerp dat permanente en structurele aandacht verdient. Tot op heden hebben de gemeenten in GR Drechtstedenverband geïnvesteerd om een inhoudelijk grote stap te zetten. De Commissie acht het mogelijk bovenstaande aanbevelingen te realiseren door vanuit de GR Drechtsteden te sturen op de realisatie van de overkoepelende agenda. Gelet op de structuur waarin de gemeenten samenwerken in GR Drechtsteden is het wenselijk dat daarbij het gesprek in de lijn van de individuele gemeenten wordt geïntensiveerd.

1. Digitalisering algemeen

Drechtsteden en de gemeenten hebben het digitale beleid (strategie/ambities) weergegeven in visiedocumenten. In het informatiebeveiligingsbeleid is aansluiting gezocht bij de BIG. Dit beleid is vastgesteld door de gemeentesecretarissen en de colleges. De gemeenten kampen met uitdagingen op het gebied van organisatie brede betrokkenheid, gedrag en effectuering van het beleid.

Op het niveau van de GR Drechtsteden en het de CIO-office is de ambitie op het gebied van digitalisering vastgelegd in een visiedocument voor het werken in de Drechtsteden (horizon 2018). Dit zal in 2016 worden geactualiseerd.

Jaarlijks wordt een regionaal projectportfolio (RPP) opgesteld in GR Drechtstedenverband. Dit wordt vastgesteld door het ONS-D (de gemeentesecretarissen gezamenlijk). In dit RPP staan de uit te voeren digitaliserings-projecten (bv vervanging zaaksysteem, invoering stelsel basisregistraties, BGB, enz.).

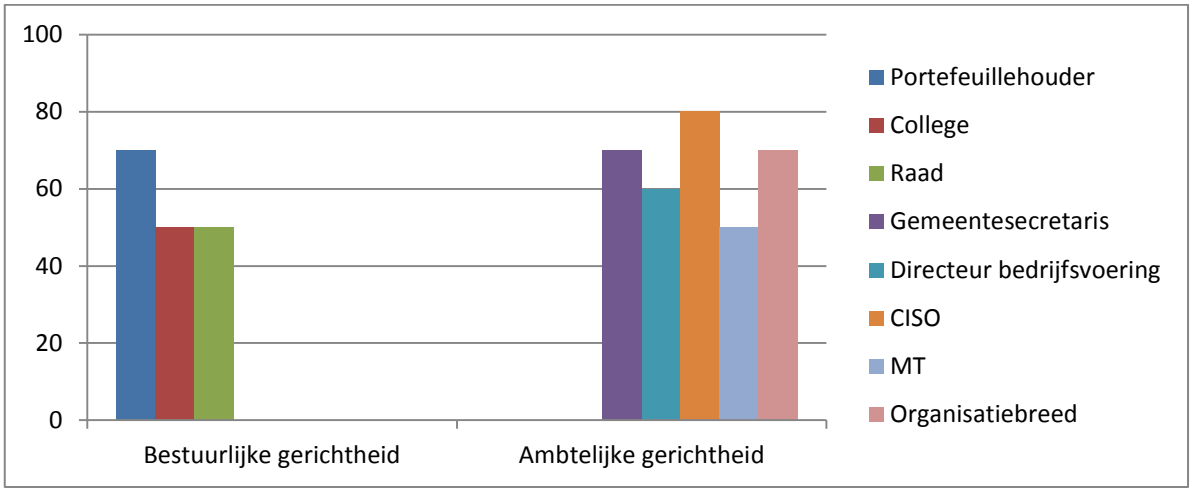
De visie op / het strategisch Raamwerk voor Informatiebeveiliging is vastgesteld door de gemeentesecretarissen (september 2014) en door de Colleges. In december 2015 is door de gemeentesecretarissen en de Colleges het strategisch/tactisch beleid vastgesteld. Er is een 3-jarig bewustwordingscampagne in uitvoering (2015-2017). Het informatiebeveiligingsbeleid sluit volledig aan bij de BIG. Voor dit jaar staat het uitvoeren van de GAP-analyse gepland, welke ondersteund zal worden vanuit de GR Drechtsteden. Uit deze analyse zal ook moeten blijken in hoeverre er verschillen zitten tussen de individuele gemeenten.

De belangrijkste uitdaging voor de gemeenten is i) kennis en bewustzijn bij alle betrokkenen vergroten en behouden, ii) het daadwerkelijke gedrag (organisatiebreed) en iii) het effectueren van het beleid. De afgelopen maanden is dit onder controle gebracht. Het komende jaar staat de GAP-analyse op het programma. Concrete incidenten in het afgelopen jaar bestonden uit virus uitbraken, welke in relatie stonden tot de vervanging van het technische netwerk. De lopende uitdagingen hebben betrekking op hoe organisatiebreed om te gaan met (openbaar) Wi-Fi, het delen van wachtwoorden (ook voor management) en het beheer van mobiele apparaten.

2. Besef van het belang van werken aan informatieveiligheid (gerichtheid)

Het belang van informatieveiligheid wordt op bestuurlijk en topambtelijk niveau gevoeld en er zijn organisatiebrede (op het niveau van de GR) initiatieven om de gerichtheid op medewerkersniveau te bewerkstelligen. Binnen het GR-verband is op de diverse niveaus aandacht voor het thema informatieveiligheid. Het algehele beeld is dat deze aandacht minder structureel is binnen de individuele gemeenten. Tegelijkertijd zijn er diverse initiatieven om de vertaling naar de individuele gemeenten te maken, bijvoorbeeld door het Periodiek Informatiebeveiligings Overleg Drechtsteden (PIO-D). De CISO speelt hierin ook een belangrijke rol door GR-breed informatie en voorlichtingsmateriaal ter beschikking te stellen.

Met behulp van de figuren in het vervolg van dit verslag illustreert de Commissie haar beeld van de huidige situatie ten opzichte van de groeipotentie (100) die is waargenomen. Dit houdt in dat de figuren *geen* norm voor de ideale gemeente verbeelden, maar de ruimte voor verbetering per specifieke gemeente weergeeft.



De portefeuillehouders (van elke gemeente één) nemen zitting in het PFO-middelen en spreken elkaar periodiek. Informatieveiligheid staat tijdens deze PFO-overleggen met regelmaat op de agenda. De portefeuillehouders hebben zich geconformeerd aan het informatieveiligheidsbeleid en zijn eerst verantwoordelijk om dit uit te dragen naar de Colleges, de organisaties en de raden.

De Colleges stellen de beleidsplannen vast en worden betrokken gehouden via de portefeuillehouder. In géén van de drie gemeenten wordt met het college in een vast ritme

gesproken over informatieveiligheid. De gemeenten hebben informatieveiligheid niet als onderdeel van de collegeambities opgenomen.

In de gemeenteraden is geen structurele aandacht voor het onderwerp informatiebeveiliging. Ook hebben de Raden zich niet expliciet over informatieveiligheid uitgesproken.

In de Drechtraad (het Algemeen Bestuur), waarin diverse raadsleden van de individuele gemeenten zitting hebben, is in maart 2016 een themasessie over informatieveiligheid georganiseerd. Op basis van deze sessie zal nu worden bezien hoe (vervolg)acties in de richting van de individuele gemeenteraden worden vormgegeven. Digitalisering is in de Drechtraad in algemene zin een onderwerp van belang omdat recent hoge (vervangings)investeringen in ICT zijn gepleegd.

De gemeentesecretarissen en de directeuren bedrijfsvoering spreken elkaar periodiek tijdens het ONS-D-overleg respectievelijk Netwerk MT-middelen; waarbij het onderwerp informatieveiligheid desgewenst (ad hoc) op de agenda staat.

Er zijn twee beleidsadviseurs voor informatiebeveiliging binnen de CIO-office (waarvan één CISO) aangesteld op het niveau van de GR Drechtsteden. Zij zijn dagelijks met informatieveiligheid bezig ten behoeve van de GR en de individuele gemeenten en zijn zeer betrokken.

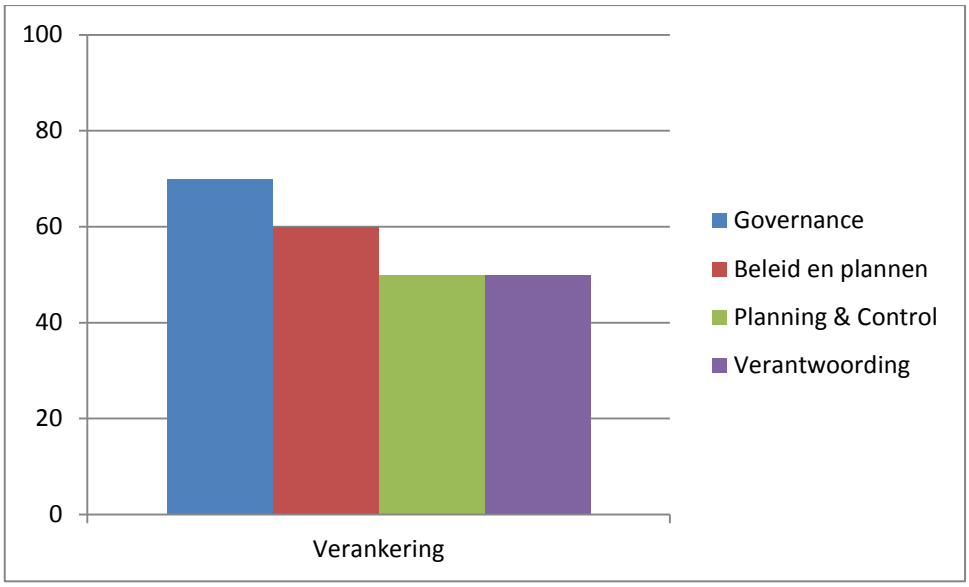
Aan de MT's van de individuele gemeenten worden terugkoppelingen gegeven door de gemeentesecretarissen/directeuren bedrijfsvoering. De gemeenten geven aan dat de MT leden zich verantwoordelijk voelen voor informatieveiligheid maar dat het onderwerp niet met een vast ritme wordt besproken tijdens de MT's.

Er is een maandelijks overleg in de Drechtsteden via een door de gemeentesecretarissen ingesteld platform: het Periodiek Informatiebeveiligings Overleg Drechtsteden (PIO-D). In dit overleg nemen medewerkers ('informatiemanagers' en ICT-contactpersonen) van alle gemeenten deel. De CISO rapporteert in dit PIO-D en tijdens deze overleggen wordt stilgestaan bij relevante ontwikkelingen (bv Internet of Things, etc).

Medewerkers doen (verplicht) mee aan e-learning over informatieveiligheid en worden via posters geïnformeerd. Er is een 3-jarige bewustwordingscampagne. Hierbij wordt e-learning ingezet en worden er posters opgehangen, berichten op intranet geplaatste en zijn er mogelijkheden om workshops te volgen. Deze bewustwordingscampagnes zullen worden opgevolgd (bv door middel van *mystery guests* en phishing e-mails).

3. Formele positionering in bestuur, organisatie en in P&C-cyclus (verankering)

De governance structuur is sterk gerelateerd aan de samenwerking van de gemeenten in GR Drechtsteden. De verplichte audits/controles worden uitgevoerd. In het jaarverslag wordt informatieveiligheid nog niet afzonderlijk uitgelicht, maar dit is wel de ambitie voor aankomend jaar.



De *governance* structuur is sterk gerelateerd aan de samenwerking van de gemeenten in de GR Drechtsteden.

- De portefeuillehouders zijn verantwoordelijk op bestuurlijk niveau in hun gemeenten en stemmen af in het kader van PFO-middelen (GR-niveau). De portefeuillehouders zijn de verbindende factor met de individuele Colleges.
- De individuele Colleges stellen de beleidsplannen vast.
- De gemeentesecretarissen zijn eindverantwoordelijk op ambtelijk niveau en overleggen in GR verband in het ONS-D-overleg.
- Diverse raadsleden hebben zitting in het AB van de GR Drechtsteden (Drechtraad), maar dit gremium heeft geen verantwoordelijkheden op het vlak van informatieveiligheid.
- Er is een regionaal CIO-office met twee beleidsadviseurs informatiebeveiliging (waarvan één CISO); de gemeenten hebben géén eigen (C)ISO.

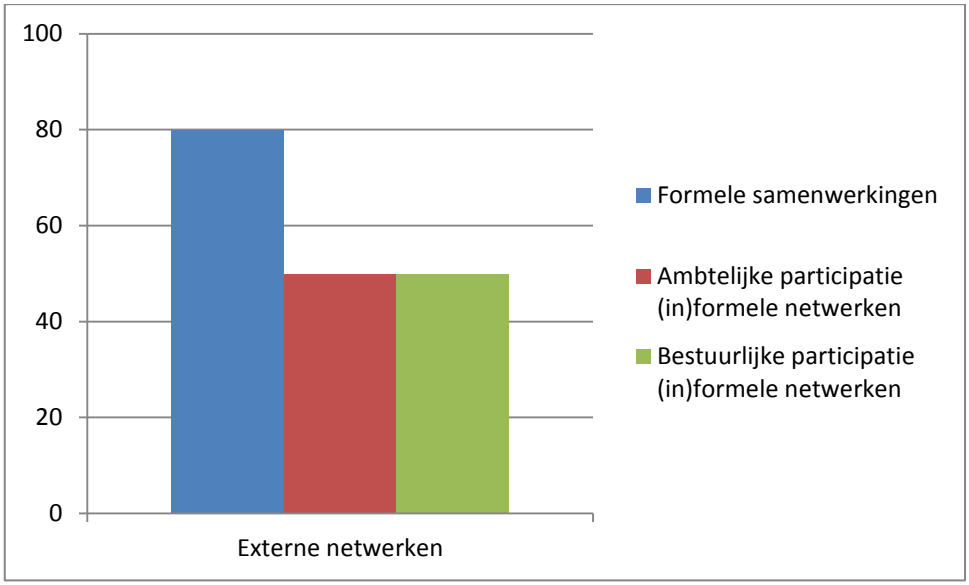
Ter ondersteuning van de hierboven vermelde structuur is er een regionaal overleg (PIO-D), waarin de CISO, de ICT-medewerkers en 'informatiemanagers' van de gemeenten zitting hebben. De beleidsadviseurs in de CIO-office zijn tevens verantwoordelijk voor het concipiëren van beleidsstukken/beleidsvoorbereiding, op basis van input door het PIO-D en onder leiding van de gemeentesecretarissen (ONS-D-overleg).

Audits en controles vinden plaats aan de hand van verplichte audits en deels door accountantscontrole. De GR Drechtsteden vervult een coördinerende rol. Voor dit jaar staat het uitvoeren van de GAP-analyse, per gemeente, op het programma.

Op dit moment is informatieveiligheid wel al opgenomen in de afzonderlijke jaarverslagen tbv de Raden maar nog niet in een aparte paragraaf. Informatieveiligheid zal vanaf komend jaar wel een aparte plek gaan krijgen.

4. Extern leren

De gemeenten werken samen in de GR Drechtsteden. Binnen deze GR wordt ook het regionale informatieveiligheidsbeleid ontwikkeld waarbij ruimte is voor lokale invulling (per gemeente). De gemeenten zijn tot stap 3 aangesloten bij het IBD. Van deelname aan bestuurlijke/ambtelijke (informele) initiatieven buiten GR verband is niets gebleken.



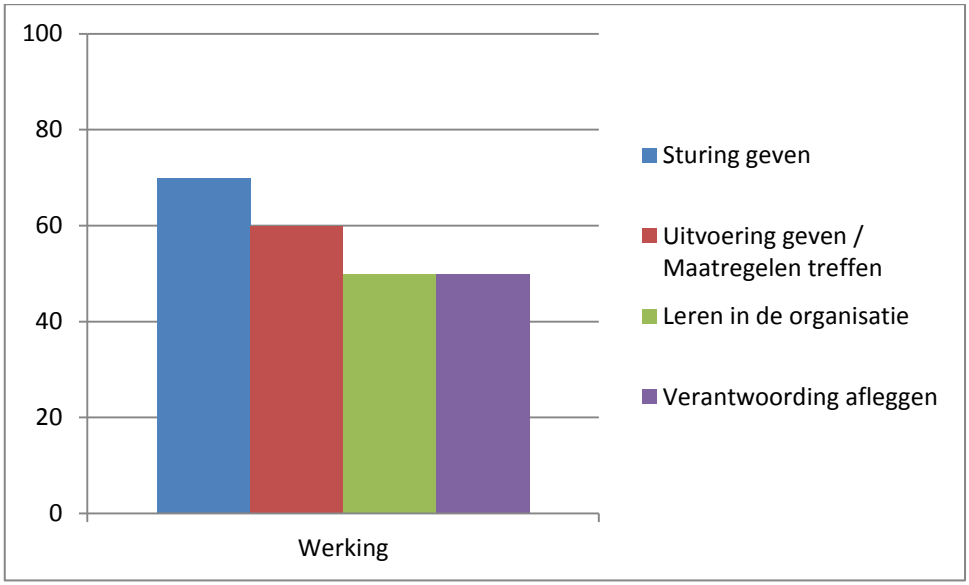
Formeel werken zes gemeenten, waaronder Papendrecht, Sliedrecht en Zwijndrecht, samen in de GR Drechtsteden. Deze gemeenten ontwikkelen gezamenlijk regionaal informatieveiligheidsbeleid, met lokale toepassing (waar nodig aangepast aan de lokale omstandigheden). Op dit moment is nog geen GAP-analyse uitgevoerd, zodat er nog geen goed beeld is hoe de individuele gemeenten (in verhouding tot elkaar) ervoor staan. Het algehele beeld is dat er geen grote verschillen zijn, maar dit dient nog geverifieerd te worden. Er zijn thans, behalve collegiale contacten, geen voornemens ten aanzien van samenwerking met andere gemeenten dan in het verband met de GR Drechtsteden (uitgezonderd Hardinxveld-Giessendam gezien de aansluiting in 2018).

De gemeenten zijn tot en met stap 3 aangesloten bij het IBD. Dit houdt in dat er een Vertrouwd Contactpersoon is aangesteld en IP-adressen / URL-adressen zijn doorgegeven. Binnen GR Drechtstedenverband zijn er 3 VCIB-ers, waarvan één de bestuurlijk portefeuillehouder en de twee beleidsadviseurs informatiebeveiliging binnen de CIO-office. Twee ACIB-ers zijn aangesteld bij de technische ICT-afdeling van SCD.

De CIO-office van de GR Drechtsteden organiseert bijeenkomsten op regionaal niveau over informatieveiligheid, bijvoorbeeld voor de Drechtraad (AB GR Drechtsteden en in PIO-D verband). Bestuurlijke en ambtelijke participatie in netwerken met betrekking tot informatieveiligheid vindt volledig in het kader van de GR Drechtsteden plaats. Van deelname aan overleggen daarbuiten is thans geen sprake.

5. Daadwerkelijk leren, daadwerkelijk beleid uitvoeren (werking)

De werking van de governance is sterk gerelateerd aan de GR Drechtsteden. In dit verband zijn op de diverse niveaus (bestuurlijk, topambtelijk en medewerkers niveau) regelmatig overleggen. In het komende jaar zal de informatie uit ISMS op de PDCA-cyclus worden aangesloten en een GAP-analyse worden uitgevoerd.



De werking van de governance is sterk gerelateerd aan de GR Drechtsteden. In dit verband zijn op de diverse niveaus (bestuurlijk, topambtelijk en medewerkers niveau) regelmatig overleggen. Daardoor is toch een gevoel van 'nabijheid'. In het PIO-D-overleg staat informatieveiligheid permanent op de agenda. In het PFO-middelen en ONS-D-overleg is dit op *ad hoc* basis, waarbij korte lijnen bestaan met de CIO-office. Via deze gremia wordt de vertaling naar de individuele gemeenten vormgegeven, welke formeel verantwoordelijk zijn en blijven voor informatieveiligheid.

De gemeenten geven aan dat de leden van het PIO-D ('informatiemanagers' en ICT-contactpersonen op medewerkersniveau) het meest betrokken zijn bij het bevorderen van de informatieveiligheid in de organisatie(s).

De gemeenten geven aan dat de informatiebeveiligingsonderwerpen deels zijn belegd in hun werkprocessen. Op de werkvloer komt een en ander samen, maar er is nog geen volledig zicht op hoe de individuele gemeenten zich onderling verhouden doordat de GAP-analyse nog niet is uitgevoerd.

Voor het komend jaar staat aansluiting van managementinformatie uit ISMS op de PDCA-cyclus (via ENSIA) en het uitvoeren van de GAP-analyse in de planning. Deze analyse zal worden vertaald naar een (gezamenlijk) beleidsplan, waarbij er ruimte is om voor verschillende gemeenten om een op maat gesneden focus te kiezen.

De gemeenten geven aan voldoende te scoren op de audits BRP, DigiD en Suwinet.

De bevindingen op basis van de (verplichte) audits en accountantscontrole worden zoveel mogelijk opgelost of opgenomen in jaarplannen. De CIO-office en SCD-ICT analyseren de incidenten en komen met concrete voorstellen voor verbetering.

De contracten met leveranciers zijn uniform voor alle deelnemers in de GR Drechtsteden. Aanbestedingen worden vanuit het shared service centrum (SCD) in GR verband georganiseerd waarbij gebruik wordt gemaakt van IBD-informatie/voorwaarden. Een terugkerend thema is dat leveranciers (bv Centric) actief aangespoord moeten worden om zwakheden in de beveiliging van software te repareren en te voorkomen.

De gemeenten geven aan dat zij investeren in het kennisniveau van de organisatie door middel van opleidingen, workshops en campagnes. Er is een 3-jarige bewustwordingscampagne. Hierbij wordt e-learning ingezet en worden er posters opgehangen, berichten op intranet geplaatst en zijn er mogelijkheden om workshops te volgen. Deze bewustwordingscampagnes zullen worden opgevolgd (bv door middel van *mystery guests* en phishing e-mails). De verantwoordelijkheid voor deze campagnes ligt bij de individuele gemeenten maar zij worden hierin door twee beleidsadviseurs binnen de CIO-office op GR Drechtsteden niveau ondersteund.

6. Slot

- De gemeenten zouden het op prijs stellen om, naar aanleiding van een melding, ook terugkoppeling van de IBD te krijgen over hoe deze melding is opgevolgd.
- De gemeenten zouden het op prijs stellen als de visitatiecommissie concrete en praktische handreikingen zou willen doen om informatieveiligheid naar een nog hoger plan te trekken.
- Big data en privacy zijn op dit moment (andere) belangrijke thema's die op ICT gebied spelen. Enerzijds zijn dit andere thema's dan informatieveiligheid maar er wordt ingezien dat verbinding op onderdelen wel degelijk mogelijk is (bv. bij het bepalen hoe/op welk niveau de functionaris gegevensbescherming vorm gaat krijgen).