

Verslag Visitatiecommissie Informatieveiligheid

Gemeente	Zwolle
Tijd	21 september 2016, 12:00 uur.
Aanwezig gemeente	Dhr. Jan Brink, wethouder bedrijfsvoering (inclusief IB en privacy) Dhr. Bernard Mencke, hoofd domein dienstverlening (loco secretaris, verantwoordelijk voor ICT) Mevr. Marrie Hol, informatiemanager (CISO)
Aanwezig Visitatiecommissie Informatieveiligheid	Frans Backhuijs (voorzitter) Wim Blok Maarten Ruys Jeroen Boot (secretaris)

Inleiding

De Commissie Informatieveiligheid dankt de gemeente Zwolle 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 gemeente Zwolle werkt aan informatieveiligheid en wat de grootste uitdagingen zijn.

De Commissie heeft het beeld dat de gemeente Zwolle op een realistische manier werkt aan informatieveiligheid.

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

Houd oog voor de actuele ontwikkelingen en deel kennis

Zwolle werkt professioneel aan informatieveiligheid, terwijl de omgeving continue en snel verandert. Dit betekent onder meer het belang om te investeren op de benodigde (technische) kennis en applicaties. Daarbij kan gedacht worden aan het *realtime* monitoren en analyseren van het dataverkeer, zoals Zwolle dat op dit moment al doet. De Commissie raadt Zwolle aan om dergelijke initiatieven voort te zetten om technisch bij te kunnen blijven. Tegen de achtergrond dat informatieveiligheid een randvoorwaarde is om de privacy van haar inwoners te borgen, is het belang toenemend om cyberdreigingen te kunnen duiden, tegenmaatregelen te kunnen adviseren en inzicht te houden in actuele risico's. Desgewenst kan Zwolle samenwerking en aansluiting zoeken met andere gemeenten (bijvoorbeeld in de regio, in het geval van Zwolle bijvoorbeeld in het shared service center met Kampen en de Provincie Overijssel), overigens zonder dat dit haar van haar individuele verantwoordelijkheid onder de BIG ontslaat. De Commissie roept Zwolle op om haar analyses en inzichten op basis van *realtime* monitoring te delen in IBD-verband. Langs deze weg kan Zwolle een voortrekkersrol (blijven) vervullen op het gebied van informatieveiligheid.

Sluit tot en met stap 4 aan bij de IBD

Zwolle is tot en met stap 2 aangesloten bij de IBD. De Commissie benadrukt het belang om tot en met stap 4 aan te sluiten bij de IBD, hetgeen Zwolle onderschrijft. 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. Ten slotte benadrukt de Commissie dat, na aansluiting tot en met stap 4, de ICT-foto periodiek dient te worden geüpdatet, omdat de ICT omgeving bij de gemeente continue zal blijven veranderen. De Commissie raadt aan om het periodiek updaten van de ICT foto te borgen in de werkprocessen van de gemeente Zwolle.

Werk in nog sterkere mate op systematische wijze aan informatieveiligheid

Zwolle geeft aan dat zij het informatieveiligheidsbeleid op dit moment herzielt en een hoog ambitieniveau heeft. De Commissie benadrukt om vanuit het beleid en haar ambitie de bijbehorende concrete acties en prioriteiten te benoemen. Door een structurele agenda en actieplannen kan Zwolle scherp voor ogen te houden wat zij in een bepaalde periode beoogt te realiseren. Het is bovendien van belang om het sturen op de realisatie/voortgang (door middel van Plan-Do-Check-Act) te verankeren in de organisatie door de verbinding te leggen tussen managementinformatie uit ISMS en de P&C cyclus. Dit is een belangrijke stap naar een verdere, nog meer systematische, manier van werken aan informatieveiligheid binnen de gemeente Zwolle. Dit voorkomt dat het werken van aan informatieveiligheid te veel ad hoc of op basis van concrete incidenten is georganiseerd.

1. Digitalisering algemeen

Zwolle werkt aan een omvangrijke digitaliserings-agenda. Zwolle heeft daarbij oog voor informatieveiligheid op zowel het technische als het gedragsaspect.

Op dit moment loopt in Zwolle het programma “Digitaal werken”. Het resultaat moet zijn dat eind 2017 80% van de organisatie digitaal werkt. Concreet betekent dit de introductie van zaakgericht werken, de doorontwikkeling van (digitale) dienstverlening, ontwikkeling en aansluiting GDI, het werken aan de omgevingswet en het ontwikkelen van slimme sturingsinformatie. Zwolle is zich ervan bewust dat al deze ontwikkelingen ook een zekere ‘digivaardigheid’ van haar medewerkers vraagt.

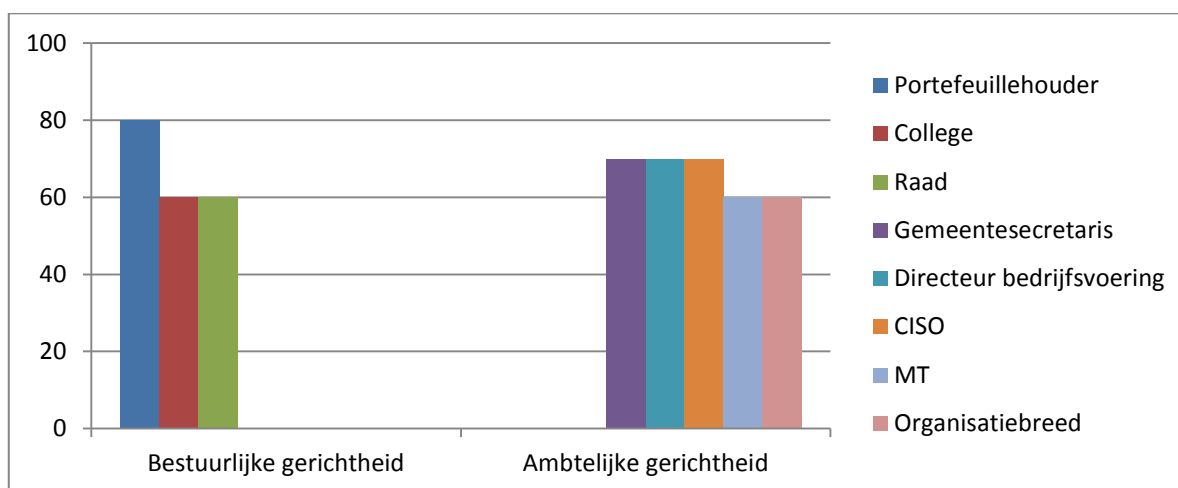
Zwolle wil een betrouwbare en integere overheid zijn, waar burgers en bedrijven hun gegevens veilig mee kunnen delen. De gegevens van burgers en bedrijven zijn als het ware in ‘bruikleen’. Hierbij gaat het om allerlei technische aspecten, maar ook om de houding en gedragskant. Door de diverse veranderingen wordt dit ook duidelijk: bij het introduceren van het nieuwe werken betekent dit ook dat je moet uitloggen en een clean desk moet hebben. Zwolle maakt van deze wisselwerking dankbaar gebruik bij het werken aan informatieveiligheid.

Zwolle ervaart uitdagingen op het vlak van outsourcing versus informatieveiligheid alsmede big en open data versus informatiebeveiliging en privacy. Zwolle geeft aan dat er budget beschikbaar is, en dat haar ambities mede worden bepaald door beschikbare middelen en haalbaarheid.

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

De portefeuillehouder is zeer betrokken bij het onderwerp informatieveiligheid. De structurele betrokkenheid van het college en de raad kan verder worden versterkt. Het MT is betrokken bij het vaststellen van beleid en uitvoeringsplannen. In de breedte van de organisatie kan het belang van werken aan informatieveiligheid nog meer aandacht krijgen.

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 portefeuillehouder is zeer betrokken bij de onderwerpen informatiebeveiliging en privacy. Bij nieuwe projectvoorstellen wordt aandacht gevraagd voor informatiebeveiliging. Portefeuillehouder stelt kritische vragen met betrekking tot informatiebeveiliging en heeft dit direct bij zijn aantreden als wethouder naar voren gebracht als een belangrijk aandachtspunt en gestuurd op verscherping vanuit het perspectief van persoonlijke integriteit.

In het college worden vragen gesteld over informatieveiligheid en het college wordt op de hoogte gehouden van resultaten van audits. Collegeleden zijn vanzelfsprekend ook gebruiker van de systemen en worden bijvoorbeeld geconfronteerd met een wachtwoordbeleid. Het belang hiervan wordt door het college begrepen en onderschreven.

In de raad zitten een aantal specialisten op het gebied van ICT/informatieveiligheid. De betrokkenheid van de raad bestaat uit het stellen van vragen als er berichtgeving is over mogelijk onveilig gebruik van gegevens van burgers en bedrijven. De raad vindt het belangrijk dat informatieveiligheid op orde is.

Het MT is betrokken bij het vaststellen van het informatiebeleid en –plan en laat zich informeren door middel van voortgangsrapportages.

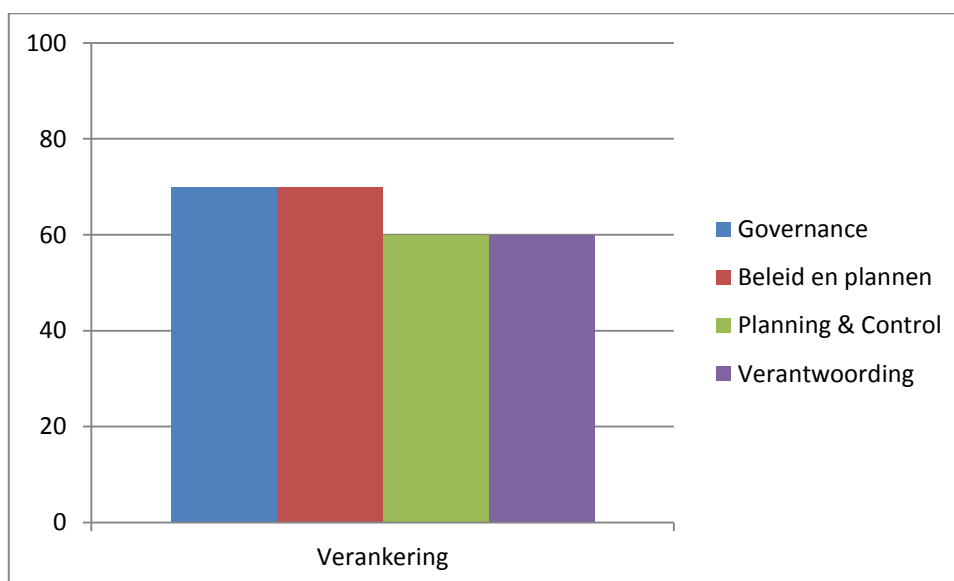
Bij de uitvoering van projecten is er een verplichte BIG-toets. Er wordt prioriteit gegeven aan het beschikbaar stellen van middelen voor informatiebeveiliging.

Bij specifieke groepen medewerkers leeft het onderwerp informatieveiligheid, wat blijkt uit vragen over verbeteringen in processen en het elkaar aanspreken op gedrag.

Zo is er voor de privacy kant bij transities in het sociaal domein veel aandacht voor informatieveiligheid geweest, waaronder door het doen van pilots in samenwerking met het ministerie van Binnenlandse Zaken. In het kader van de wijkteams is een privacy impact analyse gedaan. Zwolle geeft echter aan dat de organisatie als geheel gemiddeld genomen nog weinig met informatieveiligheid bezig is.

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

De taken/rollen op het gebied van informatieveiligheid zijn belegd. Op dit moment werkt Zwolle aan een nieuw uitvoeringsplan en ook het beleid zal in de komende periode worden herzien. Informatieveiligheid komt terug in de reguliere P&C cyclus.



Informatieveiligheid is opgenomen als onderdeel de collegeambities in het kader van de dienstverlening naar burgers en bedrijven en voor het Sociaal Domein.

De gemeentesecretaris is opdrachtgever voor beleid en plannen. De CISO is verantwoordelijk voor de realisatie en voor de uitvoering is een functionaris benoemd. CISO rapporteert aan hele MT en kan direct naar de wethouder stappen. De lijn is verantwoordelijk voor het gedrag van de medewerkers en wordt daarop eventueel geattendeerd door de informatiebeveiligingsmedewerker. Clean desk policy etc. is verantwoordelijkheid van de lijn.

Er is informatieveiligheidsbeleid op basis van de BIG met als looptijd tot en met 2017, dat is vastgesteld door het bestuur.

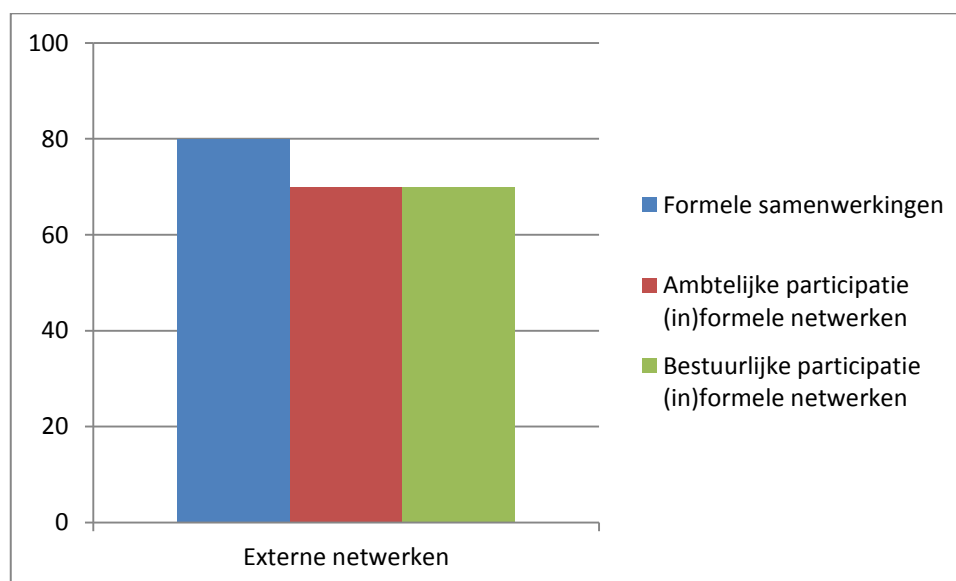
Aanpassing van dit beleid staat voor eind dit jaar, begin volgend jaar op de planning. Het informatieveiligheidsplan ligt op dit moment voor bij het MT en zal enkel ambtelijk vastgesteld worden. Er is enige vertraging opgetreden omdat het integraal opzetten van het plan (dus inclusief BIG, BRP, Suwinet, DigiD) meer tijd vergde.

Rondom accounts zijn er controles door de Accountant, EDP-auditor kijkt naar Suwinet, Suwinet-accounts worden periodiek gecontroleerd door IC'er. Er is een jaarlijkse digid audit met verbeterplan. Op dit moment wordt een ISMS ingevoerd met bijbehorende controls op BIG, BRP etc. In Zwolle neemt de interne auditor, ondergebracht bij de afdeling advies eveneens informatieveiligheidsaspecten mee.

Informatieveiligheid is onderdeel van de IT-paragraaf en komt terug in de reguliere P&C cyclus.

4. Extern leren

Zwolle werkt nauw samen met Kampen en de Provincie en neemt deel in Dimpact. Zwolle is tot stap 2 aangesloten bij IBD en neemt deel in informele netwerken.



Zwolle participeert in Dimpact en werkt samen met de gemeente Kampen en provincie Overijssel in een gezamenlijk shared service centrum.

Het SSC heeft een beperkt taakgebied: technisch beheer, inkoop en personeels/salaris administratie. Voor systemen is Zwolle afhankelijk van wat het SSC levert aan technisch beheer. Er is samenwerking op het gebied van kennisuitwisseling en samenwerking in audit, pentesten en beleid. Bij het aanschaffen van nieuwe applicaties gaat Zwolle in overleg met Kampen en de provincie of zij ook willen meedoen. Dit heeft er bijvoorbeeld in geresulteerd dat één applicatie gedeeld wordt op het gebied van veilig mailen en delen van gegevens.

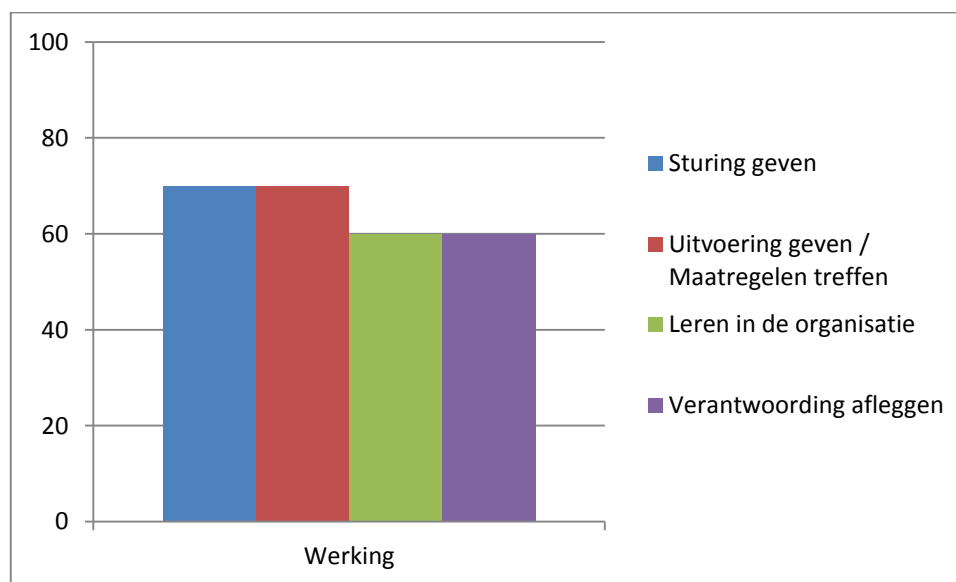
De samenwerking met de Provincie verloopt goed, maar de Provincie heeft iets andere voorwaarden, invulling en applicaties vanwege haar (andere) taken: de Provincie heeft bijvoorbeeld geen Suwi. In de uitvoering trekt Zwolle dus iets meer op met Kampen, waarbij de Provincie op iets meer afstand staat.

Zwolle is aangesloten bij IBD tot en met stap 2. Incidentafhandeling loopt via servicedesk(algemeen) of via vertrouwd persoon naar incident / changeproces. Zwolle geeft aan dat zij waarstaatjegemeente.nl nog niet netjes ingevuld heeft. Zwolle verwacht in november tot en met stap 4 bij de IBD aan te sluiten en waarstaatjegemeente.nl te hebben ingevuld.

Ten slotte wisselt Zwolle regelmatig kennis uit met IBD en ook met andere gemeenten zoals Enschede en Deventer.

5. Daadwerkelijk leren, daadwerkelijk beleid uitvoeren (werking)

De CISO en FG weten elkaar te vinden en werken samen. Er zijn diverse ontwikkelingen, bijvoorbeeld in het Sociaal Domein waarin informatieveiligheidsaspecten een belangrijke plaats innemen. Zwolle is zich bewust van het belang van het controleren/monitoren van haar externe leveranciers en heeft hierop specifieke maatregelen ingesteld. Het organisatiebrede leren en het gesprek met de raad kan nog verder verstevigd en gestructureerd worden in de toekomst.



De CISO functie is bemenst met 1,2 fte. Op strategisch niveau voor 0,2 fte en op operationeel/tactisch niveau voor 1 fte. Formeel is geen CIO benoemd, het hoofd domein dienstverlening heeft als taak een goed informatiebeleid te voeren. De FG is werkzaam bij juridische zaken. De CISO en FG trekken veelal samen op bij voorkomende vraagstukken. In Zwolle is er een gemeentebrede informatieveiligheidswerkgroep opgericht om het werken aan informatieveiligheid verder te structureren bestaande uit de CISO, Projectleider IB, de adviseur IB en de FG.

In de uitvoering is op dit moment veel aandacht voor het Sociaal Domein, waarbij de klant ook regisseur moet zijn van zijn eigen dossier en daarvoor over toegang moet beschikken. Ook de mogelijkheden van big/open data worden in het Sociaal Domein verkend. De ervaring is dat hiermee veel inzichten zijn te behalen, maar het roept ook allerlei vragen op met betrekking tot privacy/informatieveiligheid. Een andere uitdaging is het continue blijven bij de technische ontwikkelingen.

Alle bewerkingsovereenkomsten met externe leveranciers zijn zorgvuldig onder de loep genomen. Het proces van inkopen is daarop aangepast. Dit is naar tevredenheid van Zwolle afgerond, waarbij zij profiteert van de gezamenlijke kracht die via Dimpact kan worden gegenereerd. Op dit moment voert Zwolle realtime monitoring uit omdat er veel veranderingen worden doorgevoerd in de ICT-omgeving. Zwolle kijkt waar veel dataverkeer optreedt en waar eventuele verstoringen zitten. Dit heeft Zwolle waardevolle inzichten opgeleverd.

Zwolle heeft geïnvesteerd in de aanschaf van een tool om de implementatie van de BIG te monitoren (ISMS). Uit de controles blijkt dat formeel nog veel meer geregeld moet worden, maar dat in de praktijk er al een hoop gebeurt, onder meer vanuit de professionaliteit van de individuele applicatiebeheerders

Zwolle is voornemens te gaan werken met een mystery guest en probeert incidenten ten goede te benutten door deze te gebruiken om het bewustzijn in de organisatie te vergroten. Gepoogd wordt om organisatiebreed te informeren, maar Zwolle is zich ervan bewust dat hier nog stappen te maken zijn. Het resultaat is wel dat als gevolg van de incidenten informatieveiligheid nu hoger op de agenda staat. Zwolle heeft verder geëxperimenteerd met hackatons, in het sociaal domein en met parkeergegevens. Dit heeft veel inzichten opgeleverd.

Het gesprek met de raad krijgt vorm via het formele P&C circuit maar ook informeel. Raadsleden kunnen met feitelijke vragen direct bij de ambtenaren terecht. Zwolle informeert de raad actief in het geval van incidenten.