Verslag Visitatiecommissie Informatieveiligheid

Gemeente Oegstgeest

Tijd en datum	12.00-13.30 17 februari 2016
Aanwezig gemeente Oegstgeest	• Marien den Boer, wethouder • Harro Leegstra, (waarnemend) gemeentesecretaris • Henriëtte Tans, informatieadviseur gemeente Oegstgeest
Aanwezig Visitatiecommissie Informatieveiligheid	• Frans Backhuijs (voorzitter) • Wim Blok • Eric Warners (secretaris)

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

De Commissie heeft het beeld dat de gemeente Oegstgeest zich het belang van informatieveiligheid voor haar dienstverlening beseft. Daarbij viel de Commissie specifiek de volgende zaken positief op:

- Op bestuurlijk en topambtelijk niveau is men doordrongen van het belang van informatieveiligheid en ziet de Commissie de motivatie om stappen voorwaarts te gaan maken. Tegelijkertijd ziet de Commissie dat Oegstgeest zich realiseert dat niet alle stappen tegelijk genomen kunnen worden. Men werkt aan een uitvoerbaar programma dat op korte termijn eerste resultaten oplevert.
- De Visitatiecommissie ziet de nadrukkelijke aandacht voor de verbinding tussen informatieveiligheid als onderdeel van het primaire proces als een sterk perspectief op het vraagstuk. Dit perspectief sluit aan bij een benadering waarbij gezocht wordt naar de waarde die informatieveiligheid toevoegt aan de dienstverlening. Dit is de benadering waar ook de Commissie voor staat.

In dit verslag beschrijven we achtereenvolgens het handelingsperspectief voor de gemeente Oegstgeest, ons verkregen beeld 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

Voor informatieveiligheid is pas echt in de breedte aandacht als het concreet en tastbaar is

Het beeld van de Commissie is dat Oegstgeest vooral een uitdaging ziet in de aandacht realiseren en vasthouden voor het onderwerp in de organisatie en bij de Raad. Om de betrokkenheid bij het onderwerp in de breedte van de organisatie te versterken en vast te houden is het advies van de Commissie om het onderwerp ook heel nadrukkelijk op tactisch en operationeel niveau te verbinden aan lopende ontwikkelingen en het reguliere werk. Het grote verhaal over informatieveiligheid bestaat uit allemaal kleinere verhalen die de aanpak diep in de organisatie een plek geven. Door informatieveiligheid op alle niveaus van de organisatie concreet en tastbaar te maken wordt voorkomen dat het onderwerp 'verdwijnt' in algemeniseringen van het belang. Denk aan de vele voorbeelden over identiteitsfraude als het verhaal voor de medewerkers van burgerzaken, het confronteren van medewerkers van ruimtelijke ordening met informatie*on*veilig gedrag door een mystery guest, (nieuwe) medewerkers doordringen van het belang bij integriteitsworkshops.

Systematiseer het vertalen van beleid naar actie

Na vaststelling van het informatieveiligheidsbeleid heeft de gemeente Oegstgeest een kader waarbinnen zij aan het werk kan met informatieveiligheid. De Visitatiecommissie acht het belangrijk om het kader snel te vertalen naar uitvoerbare acties. Oegstgeest geeft aan dat vooral het lijnmanagement baat heeft bij het formuleren van de acties. De Visitatiecommissie onderkent dat het lijnmanagement een belangrijke rol heeft bij de realisatie van en sturing op informatieveiligheid. Maar ziet tegelijkertijd een belangrijke rol voor de aanstaande CISO bij het formuleren van een jaarlijks actieplan. Vanuit de gedachte dat niet 'alle acties tegelijk' kunnen worden uitgevoerd, ziet de Commissie bij andere gemeenten dat behoefte is aan een expert op het vlak van informatieveiligheid om, op basis van een risicoanalyse, een slimme volgorde aan te brengen in de uit te voeren acties. Daarnaast helpt het werken met één jaarlijks actieplan bij het sturen op de lopende acties. Dit neemt niet weg dat lijnmanagers een verantwoordelijkheid toebedeeld kunnen krijgen bij het uitvoeren van specifieke maatregelen.

Een stevige governance-structuur geeft grip op ontwikkeling

Oegstgeest werkt aan verdere concretisering en formalisering van de governance-structuur voor het onderwerp informatieveiligheid. De Visitatiecommissie acht een dergelijke structuur belangrijk om als gemeente goed te kunnen sturen op de ontwikkeling. Op basis van de ervaring van andere gemeenten doet de Visitatiecommissie de volgende suggesties:

- Zet de rol van CISO stevig neer. Dit houdt in ieder geval in dat de CISO een directe rapportagelijn heeft naar de gemeentesecretaris.
- Zorg voor periodieke interacties tussen de CISO-gemeentesecretaris en gemeentesecretaris-portefeuillehouder over het onderwerp informatieveiligheid.
- Deze overleggen kunnen gestructureerd worden door bijvoorbeeld te werken met kwartaalrapportages over de voortgang.
- Werk met een projectteam / coördinerend team informatieveiligheid onder voorzitterschap van de CISO met daarin de belangrijkste uitvoerende krachten binnen de organisatie om op tactisch-operationeel niveau snelle stappen te kunnen maken.

Aan het werk met een (leuk!) leerprogramma

Het beeld is dat Oegstgeest in de voorbereidende fase is om een stevige impuls te geven aan houding en gedrag, door diverse leer- en bewustzijnsacties te benoemen. De Commissie doet de suggestie om de aandacht voor houding en gedrag in de organisatie ook op langere termijn te borgen door dit momentum te gebruiken om het leren te systematiseren. Door leeracties als I-bewustzijn te verbinden met opleidingsplannen en systematische aandacht voor het kennisniveau in de organisatie (bijvoorbeeld een periodieke uitvoering van een peiling van de kennis) wordt het leren binnen de organisatie stevige ondergrond geboden. Periodieke interactie met het lijnmanagement over het verder inrichten van het leerbeleid is daarbij wenselijk. Dit geeft de mogelijkheid om heel gericht te blijven zoeken naar de best werkende mix van interventies en acties. Het campagnemateriaal van I-bewustzijn kan het ontwikkelen van houding en gedrag binnen de organisatie verder ondersteunen (zie; https://www.vngacademie.nl/e-learning/ibewustzijn-overheid-.aspx). Daarnaast kan de VNG Oegstgeest helpen om in contact te komen met gemeenten die op dit vlak goede stappen hebben gemaakt.

Daarnaast is het belangrijk om het leren vooral ook leuk en vitaal te houden. De Commissie heeft hiervoor in andere gemeenten diverse werkvormen opgehaald: denk aan een jaarlijkse oefening, een mystery guest of het spelen van een informatieveiligheidsgame. Via de VNG zijn verdere suggesties op te halen over leuke werkvormen die gemeenten hiervoor kunnen gebruiken.

Haal kennis en inspiratie uit externe netwerken

De Commissie doet de suggestie kennis en inspiratie op het vlak van informatieveiligheid op te halen bij andere gemeenten en uit de landelijke netwerken van de VNG. Denk aan deelname I-Bewustzijnsessies, landelijke congressen of het initiëren van kennisuitwisseling over dit onderwerp in de regio met andere gemeenten, private organisaties en/of de wetenschap.

Geef vorm aan een veranderprogramma om de stap voorwaarts te maken

Oegstgeest heeft de ambitie om volgend jaar een stap voorwaarts te zetten waar het gaat om informatieveiligheid. Hiervoor lopen al diverse initiatieven en is extra capaciteit beschikbaar. Bovenstaande aanbevelingen kunnen verder richting geven aan de ontwikkeling. De realisatie van de ambitie kan verder versterkt worden door de uitvoering van de activiteiten vorm te geven als tijdelijk veranderprogramma. De ‘arena’ voor zo’n intensivering van het lopende programma zou kunnen bestaan uit een aanpassing van de huidige actie naar wat de gemeente zinvol vindt en een vertaling in een aantal concrete doelen. Het realiseren hiervan kan tot inzet van specifieke afspraken gemaakt worden tussen portefeuillehouder en gemeentesecretaris, programmaverantwoordelijken en van de verantwoording tegenover College en Raad. Het vereist betrokkenheid en sturing van bestuur en de ambtelijke top om een dergelijk programma succesvol te maken.

1. Digitalisering algemeen (context)

Gemeente Oegstgeest heeft de ambitie om in de breedte te werken conform het principe ‘click, call, face’ en heeft deze ambitie vastgelegd in de Visie op Dienstverlening. Oegstgeest heeft flinke stappen gezet waar het gaat om digitalisering, maar ziet in dat op onderdelen ook nog stappen te zetten zijn.

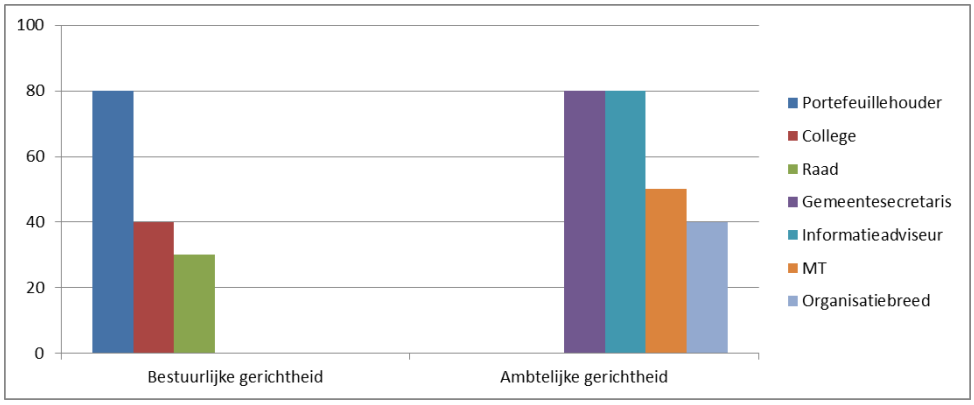
Oegstgeest ziet de samenwerking met Servicepunt 71 als een manier om (samen) stappen te nemen op het vlak van digitalisering. In de organisatie heeft Oegstgeest ook extra capaciteit vrijgemaakt om te werken aan digitalisering. Concreet werkt men momenteel aan diverse acties: het verbeteren van dienstverlening aan inwoners en ondernemers, het herontwerp van diverse werkprocessen en de implementatie daarvan en het gebruik van de generieke basisinfrastructuur.

Informatieveiligheid is één van de onderwerpen waar in de komende periode extra in geïnvesteerd gaat worden. Concreet wil de gemeente Oegstgeest in samenwerking met de gemeenten Leiden, Leiderdorp en Zoeterwoude in de komende jaren de Baseline gaan implementeren. Dit houdt in dat regionaal de kaders worden bepaald voor het werken aan informatieveiligheid om deze vervolgens lokaal vast te stellen en te vertalen naar besluiten.

Grootste uitdaging op het vlak van informatieveiligheid is en blijft het creëren en vasthouden van het gevoel van urgentie in de organisatie. Daar is sinds medio 2015 flink in geïnvesteerd.

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

Bestuurlijk en topambtelijk is sprake van gerichtheid op informatieveiligheid. Het beeld van de Commissie is dat het vooral gaat om het verspreiden van de aandacht voor het onderwerp in de breedte van de organisatie. Oegstgeest wil hieraan werken door onder meer het MT hierbij een belangrijke rol te laten vervullen.



Figuur 1: mate van bestuurlijke en ambtelijke gerichtheid

De betrokken portefeuillehouder onderkent het belang van informatieveiligheid. De portefeuillehouder ziet daarbij specifiek het belang van informatieveiligheid als onderdeel van de primaire processen en draagt zijn perspectief op het onderwerp ook uit in besprekingen over informatieveiligheid.

Het College onderkent het belang van informatieveiligheid. Tegelijkertijd is het onderwerp in het College vooral nog aan de orde bij besprekingen van specifieke thema's. Informatieveiligheid staat nog niet zelfstandig als onderwerp op de College-agenda. Dit gaat voor het eerst gebeuren met de vaststelling van het informatieveiligheidsbeleidsplan.

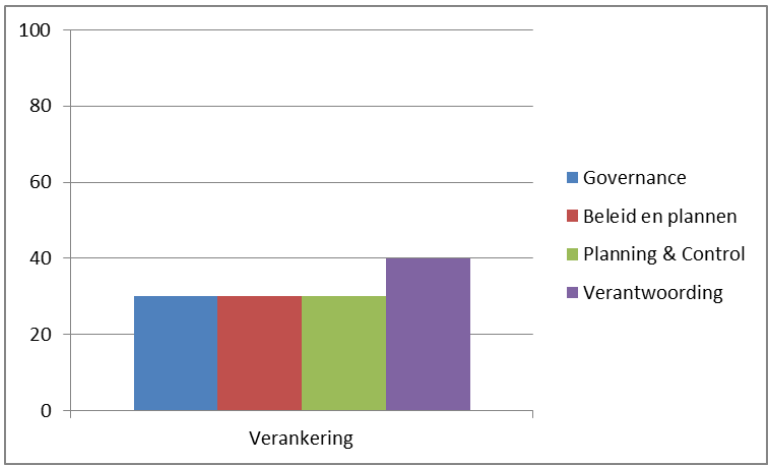
In de Raad richt de aandacht zich vooral op informatievoorziening in de brede zin. Men is vooral betrokken bij informatieveiligheidsvraagstukken rondom specifieke vraagstukken, zoals het sociaal domein. De aandacht richt zich daarbij specifiek op het privacyvraagstuk.

Topambtelijk wordt de urgentie om te werken aan informatieveiligheid onderkend. Aandacht voor en kennis van het onderwerp is in het MT in ontwikkeling. Hier wordt onder meer aan gewerkt door het MT hierbij mee te nemen via presentaties over het belang van informatieveiligheid.

In de breedte van de organisatie wordt het belang in verschillende mate onderkend. In het algemeen geldt dat hier nog een stap is te maken. De Commissie is positief over de ambitie van Oegstgeest om parallel aan het bewustzijn ook te investeren in het geven van handelingsperspectief aan de medewerkers.

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

Oegstgeest is op dit moment aan het werk met de formele positionering van informatieveiligheid in de organisatie. In de uitwerking is specifiek aandacht voor het formuleren van een beleidsplan, een passende governance-structuur en verantwoording aan de Raad.



Figuur 2: mate van bestuurlijke en ambtelijke verankering

(let op: de scores geven de huidige situatie weer. Er is veel in ontwikkeling!)

Op het moment is sprake van een organisch gevormde structuur:

- Het team bedrijfsondersteuning bewaakt of wordt voldaan aan de wettelijke eisen op het vlak van informatieveiligheid.
- Indien daar geen sprake van is, wordt hierover gerapporteerd aan de gemeentesecretaris. De gemeentesecretaris informeert hierover het College.

Op dit moment wordt gewerkt aan een formele governance-structuur waarbij de taken en rollen in de organisatie expliciet zijn belegd. De governance-structuur is nog niet definitief.

In ieder geval zal in deze structuur:

- De rol van CISO en de Functionaris Gegevensbescherming (FG) worden geformaliseerd
- De rol van het lijnmanagement waar het gaat om de realisatie van maatregelen is hierin verder uitgewerkt.
- Er een gremium komen dat de sturing op informatieveiligheid in de organisatie gaat ondersteunen.

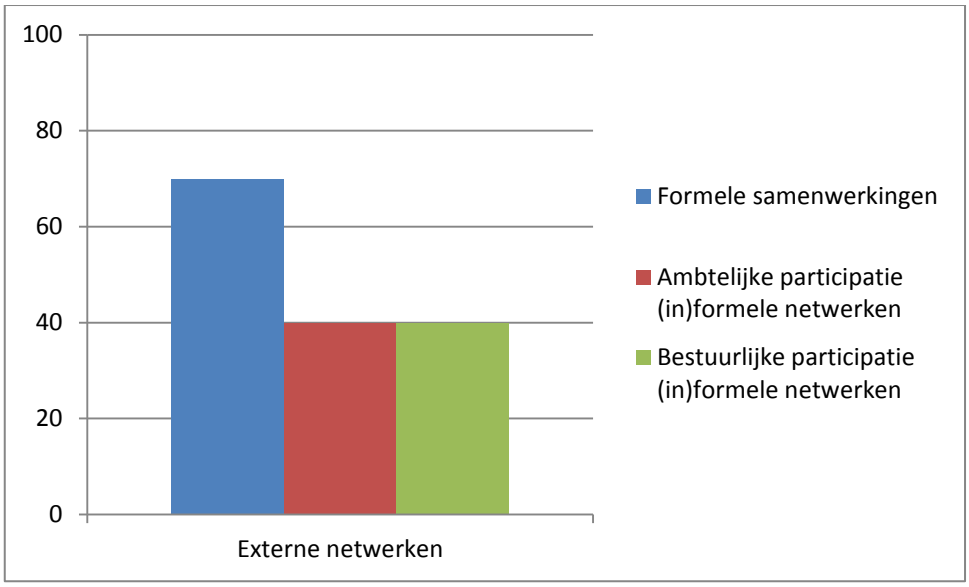
Het informatieveiligheidsbeleidsplan is in ontwikkeling. In het beleidsplan is aandacht voor de uitwerking van de governance-structuur, organisatorische maatregelen en ook het leren van de medewerkers. De ambitie van Oegstgeest is nu om de lijnmanagers een rol te laten vervullen bij het vertalen van het beleid naar concrete acties in de organisatie.

Controles en verplichte audits worden nu gecoördineerd door het team bedrijfsondersteuning.

In de paragraaf bedrijfsvoering is een korte passage opgenomen over informatieveiligheid. De ambitie is nu om hier in komende jaarverslagen meer uitgebreid en expliciet aandacht aan te besteden.

4. Extern leren

In de samenwerking Servicepunt71 is informatieveiligheid een belangrijk onderwerp. In de andere samenwerkingen komt het onderwerp wisselend ter sprake. Zowel bestuurlijk als ambtelijk participeert Oegstgeest voorzichtig in informele netwerken waar informatieveiligheid op de agenda staat.



Figuur 3: mate van participatie in netwerken

Het belangrijkste formele netwerk waarin Oegstgeest participeert is het Servicepunt 71. Dit is sinds 1 januari 2012 formeel de bedrijfsvoeringsorganisatie. In zowel het Dagelijks Bestuur als het Algemeen Bestuur is informatieveiligheid regelmatig een gespreksonderwerp. Met name in het Algemeen Bestuur is nadrukkelijk aandacht voor het gezamenlijk werken aan de kaders voor een informatieveiligheidsbeleidsplan.

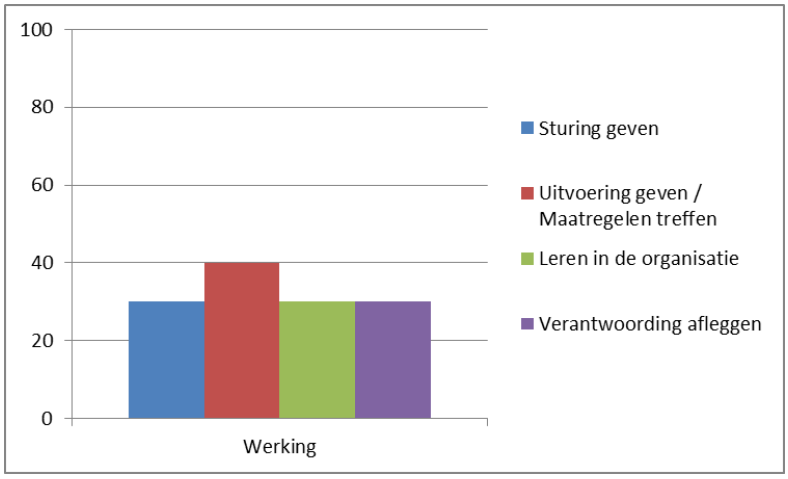
In andere samenwerkingen is wisselend aandacht voor informatieveiligheid. Vaak komt het onderwerp thematisch ter sprake.

Oegstgeest is aangesloten bij de IBD

In de informele netwerken wordt door de gemeente Oegstgeest nog voorzichtig geparticipeerd. Op ambtelijk niveau is men wel bekend met de IBD-bijeenkomsten. Bestuurlijk lijkt men nog niet te participeren in de informele netwerken waar informatieveiligheid op de agenda staat.

5. Daadwerkelijk leren, daadwerkelijk beleid uitvoeren (werking)

Uit voorgaande passages blijkt dat veel acties in ontwikkeling zijn. De werking beperkt zich op dit moment tot het uitvoeren van verplichte audits en controles en de daaruit volgende verbeteringen. Oegstgeest is zich aan het voorbereiden op een inhaalslag op het vlak van informatieveiligheid.



Figuur 4: mate van werking van de verankering en het leren

(let op: de scores geven de huidige situatie weer. Er is veel in ontwikkeling!)

Oegstgeest bereidt zich voor op het maken van een inhaalslag waar het gaat om informatieveiligheid. In deze fase van de voorbereiding gaat het vooral om het urgentiebesef creëren binnen de organisatie en de Raad. Het recente SUWI-rapport helpt daarbij om informatieveiligheid concreet te maken.

In de voorbereiding van de inhaalslag wordt het belangrijk gevonden om tijdig de Raad te betrekken. Belangrijk perspectief op het werken aan informatieveiligheid is het realiseren van een sterke koppeling tussen primaire processen en informatieveiligheid. In de woorden van de gemeente Oegstgeest: ‘informatieveiligheid moet waarde toevoegen aan de diensten die we leveren’.

De huidige werking beperkt zich op dit moment tot de uitvoering van technische en organisatorische maatregelen die volgen uit de audits. In de afspraken met leveranciers is informatieveiligheid nog maar beperkt een onderwerp.

6. Tot slot

- Gemeente Oegstgeest geeft aan erg geholpen te zijn met inzichten die helpen om de verbinding tussen het primaire proces en informatieveiligheid te versterken in de aanpak.
- De voorbereiding aan de hand van de vragenlijst heeft erg geholpen. Daarbij kan het helpen om in de communicatie duidelijker aan te geven hoe het gesprek beoogt te verlopen.
- In het format is het handig om nummers toe te voegen aan de vragen.