

Bestuursdienst

Directie MID/CIM/Wouters

Onderwerp Raadsvoorstel Informatiebeveiliging



Bezoekadres
Waagstraat 1

Postadres
Postbus 20001
9700 PB Groningen

Wij zijn met het openbaar
vervoer bereikbaar,
buslijnen
1, 2, 3, 5, 6, 11, 13, 16

Informatie over
vertrektijden krijgt u via
0900-92 92

In uw antwoord graag datum
en kenmerk vermelden.

E-mailadres
bestuursdienst@bsd.
groningen.nl

Website
www.groningen.nl

GRIFFIE
reg.nr. 9ROG.1879232
ingek. - 2 APR 2009
class. - 2.07.51
te beh. door: GR
kopie gez. aan:

De leden van de raad van de gemeente Groningen
te
GRONINGEN

Telefoon 050 367 76 92

Bijlage(n) 2

Ons kenmerk BD 09.1848559

Datum - 2 APR 2009

Uw brief van

Uw kenmerk

Geachte mevrouw/heer,

Inleiding.

Medio 2007 heeft u ingestemd met een voorstel voor het op een acceptabel niveau brengen van de informatiebeveiliging ("de basis op orde", raadsvoorstel BD 07.1381493). Gezien de aard van onze organisatie en de gegevens en informatie die deze tot zich krijgt, opslaat, verwerkt en beschikbaar stelt is dat een forse opgave. Hier lagen ook adviezen van de accountant aan ten grondslag. In bijlage 1 treft u een overzicht aan van de accountantsaanbevelingen in relatie tot de uitgevoerde acties en gerealiseerde doelen.

In de eerste fase van de uitwerking van dit voorstel – over de jaarschijven 2007 en 2008 – werden conform het voorstel de werkzaamheden projectmatig uitgevoerd. Daarna zou bepaald worden hoe deze werkzaamheden structureel in de organisatie belegd worden en welke middelen daarvoor nodig zijn.

Zoals toegezegd ontvangt u hierbij over deze eerste fase een rapportage over wat er bereikt is en hoe wij met het op orde brengen van onze informatiebeveiliging verder om denken te gaan.

Hierbij wordt met name ingegaan op de verdere structurele inbedding van informatiebeveiliging binnen onze organisatie en de (organisatorische en financiële) consequenties die dit met zich meebrengt.

Om u goed te kunnen informeren over de verbeteringen op het gebied van de informatiebeveiliging in de afgelopen jaren en u een beeld te geven hoe de gemeente er nu voorstaat ten opzichte van de start van het project, hebben wij een onderzoek uit laten voeren (een zogenaamde 1-meting die het verschil laat zien ten opzichte van de start van het project: de 0-meting).

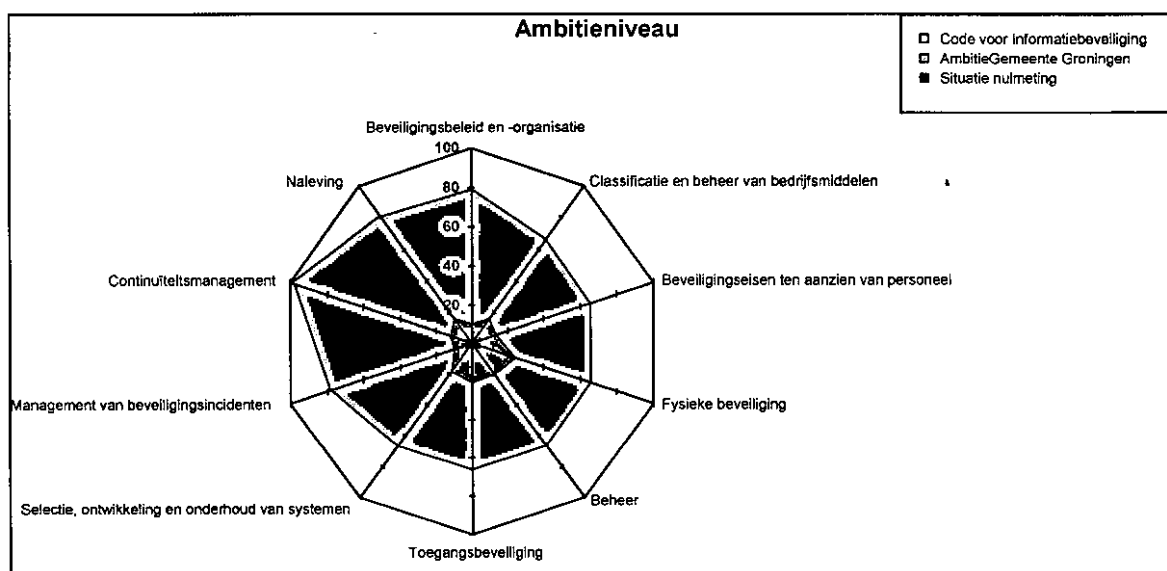
De afgelopen jaren heeft zich een aantal ontwikkelingen voorgedaan die om extra inspanning op het gebied van de informatiebeveiliging vragen. Deze ontwikkelingen hebben met name betrekking op de interactie tussen gemeente en buitenwereld (burger en bedrijf, maar ook bijvoorbeeld onze ketenpartners). Ook hier zullen wij nader op ingaan.

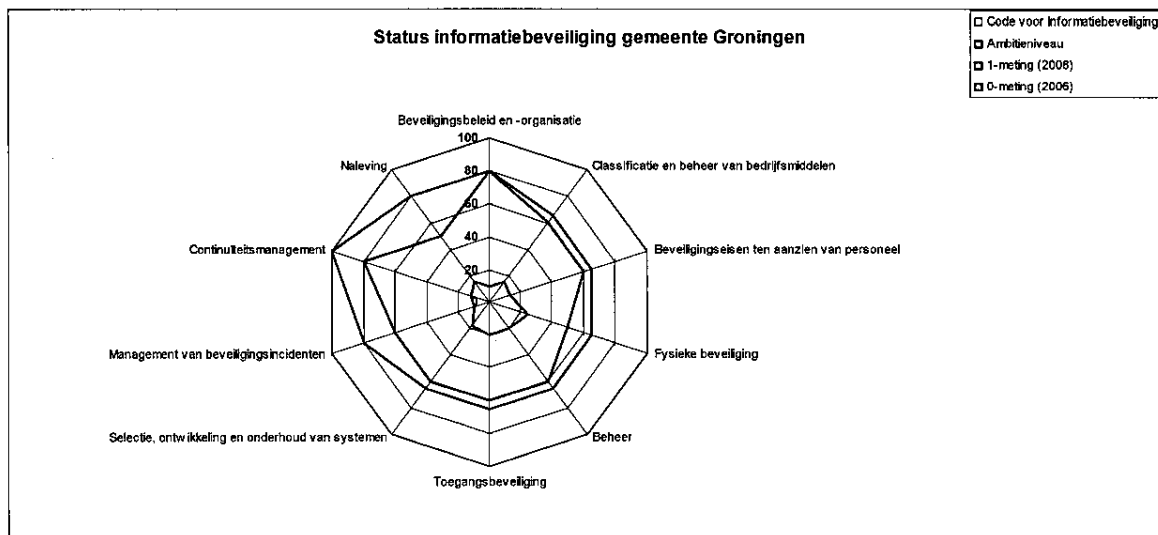
Wat is er bereikt.

Doelstelling van het project was "de basis op orde" te brengen voor wat betreft onze informatiebeveiliging. Door de accountant was in de jaren 2004-2005 reeds geadviseerd om een concernbreed informatiebeveiligingsbeleid op te stellen. In 2006 heeft de accountant aanbevolen om de dienstuitvoeringsplannen zo spoedig mogelijk uit te voeren. Op dat gebied is er de afgelopen twee jaar veel gerealiseerd. Er is nu sprake van concernbreed informatiebeveiligingsbeleid en alle diensten hebben een dienstuitvoeringsplan opgesteld. In bijlage 1 is een overzicht opgenomen van de daarnaast nog gerealiseerde doelen.

Uitkomsten van de 1-metingen.

In de voorgaande paragraaf hebben wij geschetst welke voortgang er de afgelopen twee jaar is gemaakt. Om dit ook visueel inzichtelijk te maken zetten wij in de figuur ons ambitieniveau ten opzichte van de code voor informatiebeveiliging (figuur 1), naast de resultaten van de onlangs uitgevoerde 1-meting (figuur 2) die de status van eind 2008/begin 2009 weergeeft (deze figuur is, omdat deze mogelijk lastig leesbaar is, in de bijlage vergroot weergegeven):





Uit de figuur van de 1-meting blijkt dat we de afgelopen jaren al veel bereikt hebben, maar dat we er met name op het onderdeel "naleving" nog niet zijn. Dit kan worden verklaard doordat in het project nog onvoldoende gewerkt is aan "bewustwording" bij de medewerkers van de gemeente. Met name hier valt nog een slag te maken.

De resultaten van de 1-meting zullen ook aan de accountant worden aangeboden.

Beoordeling informatiebeveiliging.

In navolging van de uitgevoerde 0-meting in 2006 zijn er in 2008 verschillende beoordelingen van het niveau van informatiebeveiliging uitgevoerd. Naast de 1-meting is er begin 2008 een aantal beveiligingstesten uitgevoerd op de e-loketten van de gemeente.

Essentie van deze beoordelingen is dat het niveau van informatiebeveiliging is gestegen van onacceptabel in 2006 naar voldoende in 2008. In onderstaand schema wordt dit grafisch weergegeven.

De gemaakte vorderingen in de afgelopen twee jaren rechtvaardigen echter niet dat het niveau "voldoende" geconsolideerd kan worden; er moeten nog stappen worden gemaakt. Met name op het vlak van communicatie, risico-analyses, bewustwording van medewerkers en melding van beveiligingsincidenten moeten nog vorderingen worden gemaakt.

Ontwikkelingen die extra aandacht vragen op het gebied van informatiebeveiliging.

Het betreft hier geen ontwikkelingen op het gebied van informatiebeveiliging zelf, maar ontwikkelingen die op de gemeente af komen en een (forse) claim doen op de beschikbare IB-capaciteit. Ook noodzaken deze externe ontwikkelingen tot bijstelling van het informatiebeveiligingsbeleid.



De belangrijkste ontwikkeling is dat er steeds meer "externe" partijen zijn (zoals onze "ketenpartners") die op gecontroleerde wijze toegang willen of die op wettelijke basis (bijvoorbeeld de Wet Algemene Bepalingen Omgevingsrecht en de Wet Basisregistraties) toegang moeten krijgen tot gegevens die binnen de gemeentelijke organisatie opgeslagen zijn c.q. door de gemeente onderhouden worden. Deze ontwikkelingen en de impact op de gemeentelijke informatiebeveiligingsvoorzieningen konden bij het starten van het project niet worden voorzien. Ook de invloed van die ontwikkeling op het informatiebeveiligingsbeleid en de bijbehorende infrastructuur zijn veel groter dan wij hadden kunnen voorzien.

Financieel overzicht.

Over de jaren 2007 en 2008 is het budget (groot € 385.000,-- per jaar) vrijwel volledig aangewend voor de hiervoren beschreven activiteiten. Hieronder worden de uitgaven van 2008 weergegeven.

Raadsvoorstel	
Omschrijving	2008
Extra capaciteit (CFIB) incl. ondersteuning van de diensten	245.000
Uitvoeren jaarlijkse beveiligingstesten	25.000
Communicatie / bewustzijn e.d.	15.000
Investerings in technische beveiligingsmaatregelen / licentiekosten (bv. monitoren software, firewall e.d.)	0
Versterking informatiebeveiliging in lopende informatieprojecten	60.000
Totaal	345.000
Begroot	385.000
Saldo	40.000



Over 2009.

Over 2009 ramen wij de kosten als volgt:

Post:	Kosten:
Inhuur Concern Functionaris InformatieBeveiliging (CFIB)	€ 105.000
Aanpassen beveiliging zodat ketenpartners gecontroleerd toegang kunnen krijgen tot gemeentelijke informatie/gegevens	€ 100.000
Ondersteuning van de diensten bij het vergroten van de bewustzijn en het uitvoeren van risicoanalyses	€ 90.000
Het uitvoeren van jaarlijkse beveiligingstesten	€ 90.000
Totaal:	€ 385.000

Bij deze vier posten geven we een korte toelichting.

- De vacature van CFIB is nog steeds niet structureel ingevuld. Dit heeft er deels mee te maken dat het een vacature voor 0,5 fte betreft. Omdat de provincie Groningen met een vergelijkbare vacature zit wordt getracht gezamenlijk een functionaris aan te trekken die voor 50% van zijn/haar tijd voor beide organisaties werkt. Als dit op korte termijn lukt, dan zullen de kosten naar verwachting lager uitvallen. Vooralsnog gaan wij ervan uit dat we (zeker voor een deel van 2009) de capaciteit extern in moeten huren.
- De kosten voor het aanpassen van onze (beveiligings)infrastructuur, zodat ketenpartners op gecontroleerde wijze toegang kunnen krijgen tot onze gegevens (IAA), ramen wij op € 100.000,--. De exacte (incidentele en structurele) kosten zullen tijdens de uitvoering van het project (in de loop van 2009) inzichtelijk moet worden.
- Zoals uit de 1-meting bleek, moet er nog een en ander gedaan worden aan met name de bewustwording bij de gebruikers. Omdat wij verwachten dat de diensten dit niet allemaal helemaal zelf kunnen doen, reserveren we € 90.000,-- van het budget om de diensten hierbij waar nodig te ondersteunen.
- Conform uw raadsbesluit van 2007 reserveren wij € 90.000,-- voor het uitvoeren van beveiligingstesten.

De kosten voor 2009 kunnen volledig gedekt worden uit het budget dat daarvoor (als onderdeel van het programma BO+SS) beschikbaar is.

Structureel.

De totale structurele kosten zullen naar verwachting eind 2009 inzichtelijk zijn. Van een aantal posten weten wij dat deze structureel op de begroting zullen blijven drukken. Het gaat hierbij om de salarislasten van de CFIB en het uitvoeren van jaarlijkse beveiligingstesten (geraamd op € 90.000,--). Een grote onzekerheid zit in de (structurele) kosten die het bijgestelde ambitieniveau van de gemeente met zich



meebrengt voor wat betreft de elektronische dienstverlening en de eerder genoemde toegang van onze gegevens voor ketenpartners.

Hoe verder.

Omdat de uitkomsten van de 1-meting laten zien dat de gemeente haar ambitie voor wat betreft de informatiebeveiliging nog niet helemaal gehaald heeft en gelet op de geschetste externe ontwikkelingen die met effect op onze organisatie afkomen, willen wij de informatiebeveiliging ook dit jaar (2009) nog projectmatig aanpakken.

Eind 2009 moet dit zover gevorderd zijn dat wij u een voorstel kunnen voorleggen hoe de informatiebeveiliging structureel in de organisatie belegd kan worden en welke middelen daarvoor benodigd zijn. Het "Uitvoeringsplan I&A organisatie", dat momenteel wordt opgesteld als gevolg van de uitkomsten van het "Bedrijfskundig onderzoek I&A (BOIA)", is daarvoor het geëigende medium, waar het de concern-brede organisatie betreft.

Met vriendelijke groet,
burgemeester en wethouders
van Groningen,

de burgemeester,

de secretaris,

Bijlage 1: Overzicht accountantsaanbevelingen in relatie tot uitgevoerde akties

Aanbevelingen accountants	Jaar	Huidige stand van zaken
Opstellen van concerninformatiebeveiligingsbeleid (ML 2005)	2003-2005	Er is gemeentebreed Informatiebeveiligingsbeleid opgesteld. Dit beleid is ook door de diensten onderschreven, waardoor het gesignaleerde risico van verschillende uitwerking en interpretatie per dienst wordt ondervangen. Tevens is een (tijdelijke) Concern Functionaris Informatie Beveiliging aangesteld
Uitvoering van Dienstuitvoeringsplannen (DUP's)	2006	Alle diensten hebben een dienstuitvoeringsplan opgesteld. Ook is er een concernuitvoeringsplan informatiebeveiliging opgesteld. Belangrijke activiteiten zijn verificatie van kritische autorisaties (loopt), communicatie en interne controle.
Overig gerealiseerde doelen (op basis van nota Informatiebeveiliging BD 07.1381493)		
<i>Organisatorisch</i>		
<ul style="list-style-type: none"> – Alle diensten hebben risicoanalyses uitgevoerd om te bepalen of er ten opzichte van het in het beveiligingsbeleid gedefinieerde minimum beveiligingsniveau aanvullende maatregelen dienen te worden getroffen. Op concernniveau wordt op dit moment daarnaast een aantal risicoanalyses uitgevoerd. – De beveiligingsorganisatie is op concern- en dienstniveau ingericht, en er is binnen de CIO een security manager aangesteld. De fysieke beveiliging wordt gecoördineerd door de Centrale Veiligheidscoördinator. – De DIA en de Bestuursdienst hebben een geïntegreerd Intern Controleplan ICT opgesteld. – Alle diensten hebben een continuïteitsplan opgesteld. Tevens is dat op concern-niveau gebeurd. – Er is een Informatiebeveiligingsraad (IB-raad) in het leven geroepen met daarin alle beveiligingsfunctionarissen om de tafel zitten. Doel is afstemming, het wiel niet opnieuw uitvinden en communicatie. 		
<i>Technisch</i>		
<ul style="list-style-type: none"> – Er is een blauwdruk voor de (toekomstige) beveiligingsarchitectuur opgesteld. – De beveiliging van de laptops die binnen de gemeente worden gebruikt is -dan wel wordt- aangescherpt. – Op dit moment wordt de software van de standaardwerkplek gefaseerd en per dienst bijgewerkt. Onderdeel van deze update is de invoering van een groot aantal technische beveiligingsmaatregelen uit het basispakket beveiligingsmaatregelen. 		

Bijlage 2: Status per ultimo 2008/begin 2009:

Status informatiebeveiliging gemeente Groningen

