RAADSVOORSTEL:
2006-2007
Ons kenmerk: BD 07.1381493

Registratienummer : GR 07.
Ingekomen op :

Onderwerp: Informatiebeveiliging.

Groningen,

Aan de raad,

Als gemeente hebben wij een schat aan gegevens en informatie in huis, zowel in onze computersystemen als op papier. Dat zijn gegevens over burgers en bedrijven, informatie over onze bedrijfsvoering, plannen voor de stad, etc. Gegevens en informatie die soms vertrouwelijk is en waar derden heel wat voor over hebben om erover te kunnen beschikken. Tegelijkertijd hebben wij als overheidsorgaan de verplichting tot openbaarheid. Onze burgers verwachten terecht van ons dat hun gegevens bij ons in veilige handen zijn. Daarom vinden wij de beveiliging van onze informatie van groot belang. Dat is niet alleen een kwestie van techniek. Natuurlijk moet de techniek op orde zijn. Door het nemen van maatregelen op technisch gebied wordt de beveiliging enorm vergroot. Maar informatiebeveiliging is zo sterk als de zwakste schakel. Kijken we naar beveiligingsincidenten – situaties waarin schade werd geleden omdat de beveiliging niet op orde was – dan is niet zelden menselijk falen de oorzaak: een computer die aan de straat wordt gezet zonder de gegevens die erop staan afdoende te verwijderen; een geheugenstick met vertrouwelijke informatie die in een huurauto is blijven liggen. Het nemen van technische maatregelen alleen is dus niet voldoende. Van even groot belang zijn het bewustzijn van management en medewerkers, goede procedures en controle op de naleving ervan, de fysieke beveiliging van gebouwen, etc.
Het belang van informatiebeveiliging neemt bovendien om verschillende redenen toe. Binnen Stad en Stadhuis zijn we druk bezig onze dienstverlening ook elektronisch aan te bieden. Dat doen we omdat we daarmee een hogere servicegraad kunnen aanbieden aan onze burgers en tevens een hogere efficiency kunnen bereiken. Maar we worden door deze ontwikkelingen wel steeds afhankelijker van een betrouwbare werking van ICT. En juist omdat we internet als communicatie-medium gebruiken, staan we bovendien in toenemende mate bloot aan allerlei bedreigingen die samenhangen met gebreken in de beveiliging van informatie-systemen. De snel voortschrijdende technologische ontwikkelingen en de onbegrensde omgeving, waarin de bedreigingen zich kunnen manifesteren, spelen hierbij een belangrijke rol. Dat is geen reden om dan maar af te zien van elektronische dienstverlening en communicatie, maar wel om extra te investeren in informatiebeveiliging.

Een aantal van onze processen vereist een hoge beschikbaarheid, foutloze informatie en bovendien kunnen de bedrijfsbelangen ernstig geschaad worden, als ongeautoriseerden toegang krijgen tot de informatie in en rond deze processen. Het gaat hierbij bijvoorbeeld om de Meldkamer, het verstrekken van uitkeringen, de gemeentelijke basisadministratie, het innen van belastingen, het loket Burgerzaken en het eLoket. De betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking is in belangrijke mate afhankelijk van maatregelen op het gebied van informatiebeveiliging. De accountant is verplicht om als onderdeel van de jaarrekeningcontrole te rapporteren over de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking.
Ook in wet- en regelgeving komt steeds meer aandacht voor informatiebeveiliging. Zo stelt de Wet Bescherming Persoonsgegevens normen voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens (bijvoorbeeld gegevens van burgers). De wet vereist dat wij passende organisatorische en technische maatregelen treffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

Het niet op orde hebben van onze informatiebeveiliging kan grote gevolgen hebben:
- financiële schade (bijvoorbeeld herstelkosten, maar financiële schade die ontstaat als een wijziging van een bestemmingsplan vroegtijdig openbaar wordt);
- imagoschade (gevolg van het niet-beschikbaar, niet integer dan wel niet-vertrouwelijk zijn van informatie);
- juridische schade (aansprakelijkheid/rechtmatigheid).

We zijn van mening dat onze informatiebeveiliging op een aantal punten kan verbeteren. Deze mening is bevestigd door een aantal tests die we hebben laten uitvoeren. Deze zogenaamde nulmeting bestond uit een test van de beveiliging van het eLoket en het concernnetwerk alsmede een test van de getroffen fysieke en organisatorische beveiligingsmaatregelen. Uit deze tests is gebleken dat de informatiebeveiliging ook daadwerkelijk verbetering behoeft. Ook onze accountant heeft ons meermalen gewezen op de noodzaak tot het hebben van een adequaat informatiebeveiligingsbeleid en een goede calamiteitenplanning.
Tegelijkertijd willen we echter een open en transparante organisatie zijn. We willen onze informatiebeveiliging goed op orde hebben zonder daarmee een onneembare vesting voor onze burgers te worden.

Voorstel.
Uitgangspunt is dat onze werkprocessen en informatie voldoende beveiligd moeten zijn. Dat betekent dat onze informatie aan de volgende eigenschappen moet voldoen:

- **beschikbaarheid**: het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfs-middelen;
- **integriteit**: het waarborgen van de juistheid en volledigheid van informatie;
- **vertrouwelijkheid**: het waarborgen dat de informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

Om dit te bereiken stellen we voor een integraal beleidskader te hanteren (zie bijlage I). Eén van de uitgangspunten van dit kader is dat we als basis de Code voor

Informatiebeveiliging nemen. De Code voor Informatiebeveiliging is een breed geaccepteerde internationale standaard voor het ontwikkelen, implementeren, onderhouden en continu verbeteren van (het niveau van) informatiebeveiliging en omvat praktische maatregelen en richtlijnen. De Code voor Informatiebeveiliging wordt ook binnen andere vergelijkbare gemeenten veelvuldig toegepast.
Om de verbetering van onze informatiebeveiliging verder vorm te geven stellen we voor om aan de hand van een "gezond verstand" scenario maatregelen te treffen. Dat wil zeggen: openheid waar het kan, grondige beveiliging waar het moet.
In de praktijk betekent "gezond verstand" dat we een keuze maken, welke maatregelen uit de Code voor Informatiebeveiliging voor de gemeente Groningen relevant zijn. Dit pakket bestaat uit drie delen. Het 1e deel is het minimum pakket, waar alle diensten en onderdelen van de gemeente aan moeten voldoen. Het 2e deel is het pakket maatregelen die de Centrale ICT Organisatie (CIO) moet nemen. Het 3e deel bevat aanvullende maatregelen die alleen voor sommige diensten van belang zijn. Op basis van risicoanalyses per dienst wordt bepaald, welke van deze aanvullende maatregelen voor die dienst noodzakelijk zijn. Dit kan bijvoorbeeld zijn omdat die wettelijk zijn voorgeschreven of voor een bepaald werkproces noodzakelijk zijn.

We hebben o.a. de volgende maatregelen in ons pakket opgenomen:

Algemene informatiebeveiligingsmaatregelen.
- Het jaarlijks uitvoeren van risicoanalyses, het opstellen van een beveiligingsplan en het testen van o.a. de beveiliging van het netwerk en de gebouwen.
- Continuïteitsmanagement op dienst- en concernniveau.
- Control op de naleving van de maatregelen.

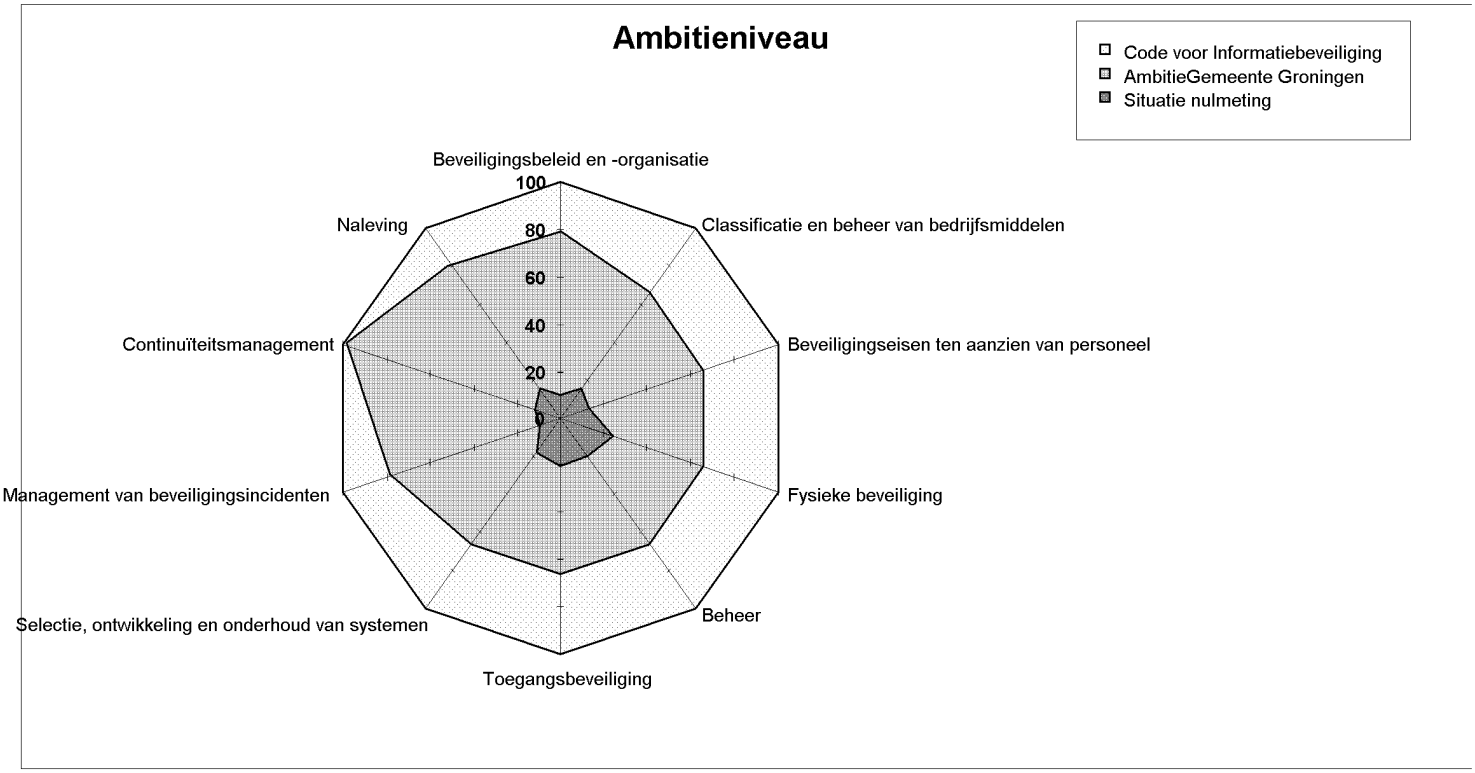
Personele informatiebeveiligingsmaatregelen.
- Diverse richtlijnen voor indiensttreding van personeel (o.a. vaststelling identiteit, echtheid van diploma's, verklaring van goed gedrag, ambtseed), tijdens het dienstverband (o.a. communicatie over informatiebeveiliging) en bij beëindiging van het dienstverband (o.a. het innemen van bedrijfsmiddelen, toegangsrechten deregistreren).

Gebouwgebonden informatiebeveiligingsmaatregelen.
- Indeling van alle ruimten van gebouwen van de gemeente in een zonecategorie, waarmee het bijbehorende beveiligingsniveau is vastgelegd. Zonecategorieën zijn: publieksruimten, dienstruimten en beveiligde ruimten.
- Adequate toegangscontrole en bezoekersprocedure.

ICT gerelateerde informatiebeveiligingsmaatregelen.

- Er dienen formele procedures en beleid te zijn voor o.a. de installatie van bedrijfsmiddelen, het beheer en de bediening van alle informatiesystemen, wijzigingen in informatiesystemen en de IT-infrastructuur, aanvraag en beheer van toegang en autorisaties, het testen, acceptatie en in gebruikname van nieuwe systemen en wijzigingen van bestaande systemen en het omgaan met testgegevens.
- Inventarisatie en classificatie van alle informatiesystemen en informatie.
- Voorzieningen ter beveiliging van gevoelige informatie tijdens vervoer.
- Normen voor toegang tot en autorisaties van de technische infrastructuur van de CIO en informatiesystemen.

Wanneer we de complete Code voor Informatiebeveiliging afzetten tegen het ambitieniveau (ons "gezond verstand" scenario) en tegen de situatie, zoals die uit de nulmeting naar voren komt, dan krijgen we grofweg het volgende beeld.



Sinds de nulmeting hebben we overigens al de nodige activiteiten op het gebied van informatiebeveiliging uitgevoerd, zodat bovenstaand beeld in feite al verbeterd is.

Ook hebben we onze accountant Ernst & Young gevraagd een mening te geven over het beleidskader en de maatregelen. De accountant is van mening dat het een goede aanzet is tot een adequate informatiebeveiliging en pleit voor een spoedige verdere implementatie van de maatregelen. Daarnaast doet E&Y een aantal zinvolle suggesties die we in het vervolgtraject zullen meenemen.

Uitvoering.

Informatiebeveiliging is niet nieuw voor de gemeente Groningen. Om de risico's te beheersen zijn in het verleden reeds diverse maatregelen getroffen. Echter, de maatregelen zijn onvoldoende en worden vanuit de verschillende diensten onafhankelijk van elkaar opgepakt. Een integrale benadering ontbreekt.
De beveiliging van werkprocessen en informatie is een verantwoordelijkheid van de lijn. Omdat een aantal verbeteringen noodzakelijk is, zal voor het op orde brengen van de beveiliging van werkprocessen en informatie een concernbreed project ingericht worden. Gedurende het project zullen de diensten ondersteund worden, maar uiteraard moeten zij ook zelf het nodige werk verrichten. We verwachten dat het project ca. 2 jaar duurt (tot eind 2008). Op dat moment moet de basis op orde zijn. Na afronding van het project wordt het niveau van de informatiebeveiliging geborgd in de lijn en worden eventuele extra's, waar later voor gekozen kan worden, geïmplementeerd.

Financiële paragraaf.
Bij de uitvoering van het project is extra capaciteit nodig. Deze capaciteit wordt ingezet om het beleid en de procedures op orde te brengen, informatiebeveiliging over de diensten heen te coördineren, de maatregelen van de verschillende diensten op elkaar af te stemmen, control vorm te geven, materiaal en tools voor diensten te ontwikkelen voor die aspecten die voor alle diensten gelijk zijn (bv. bewustzijn, communicatie, formats). Daarnaast zijn er bij de diensten veel vragen en is er behoefte aan specifieke ondersteuning.
Aangezien de tests niet uitputtend zijn geweest en we de vorderingen van de diensten willen monitoren, wordt in de projectfase rekening gehouden met kosten voor het uitvoeren van nog een aantal beveiligingtests. Medewerkers zijn zich onvoldoende bewust van (de risico's op het gebied van) informatiebeveiliging, zodat bovendien een investering in communicatie en het vergroten van het bewustzijn noodzakelijk is.
Tenslotte verwachten we nog geld nodig te hebben voor extra investeringen in de techniek.
Momenteel werken we aan een aantal projecten die de samenhang in de informatiehuishouding vergroten. We willen het aspect van de informatiebeveiliging sterker in deze projecten verankeren, wat extra kosten met zich mee brengt.
We gaan ervan uit dat de maatregelen die de CIO moet treffen in het kader van informatiebeveiliging, die voortvloeien uit de kaders, bekostigd kunnen worden door de CIO zelf en dat dit niet leidt tot kostenverhoging bij de diensten. Indien dit niet het geval is, zullen wij in een later stadium een voorstel aan u voorleggen.
Samengevat verwachten wij in de projectfase de volgende financiële middelen nodig te hebben.

Omschrijving	**2007**	**2008**
Extra capaciteit voor o.a. projectleiding en coördinatie; ontwikkelen beleid, procedures en richtlijnen; ontwikkelen materiaal en tools; ondersteunen diensten bij risicoanalyses en implementatie; control	140.000	140.000
Uitvoeren jaarlijkse (technische) beveiligingstesten, o.a. inbraak eloket; applicatietest webapplicatie; test beveiliging concernnetwerk; inventarisatie en testen beveiliging internetkoppelingen; fysieke inbraaktest.	90.000	90.000
Communicatie / bewustzijn e.d.	15.000	15.000
Investeringen in technische beveiligingsmaatregelen / licentiekosten (bv. monitoren software, firewall e.d.)	50.000	50.000
Versterking informatiebeveiliging in lopende informatieprojecten	90.000	90.000
Totaal	**385.000**	**385.000**

Bij de begroting 2007 is € 385.000,-- nieuw beleid structureel gereserveerd voor informatiebeveiliging. Wij stellen voor om de gereserveerde middelen voor nieuw beleid 2007 a € 385.000,-- structureel beschikbaar te stellen en toe te voegen aan het programma Bedrijfsvoering en Organisatie Ontwikkeling / Stad en Stadhuis, conform de volgende begrotingswijziging.

	Financiële begrotingswijziging	**Lasten**	**Baten**	**Saldo**	**- Reserve**	**+ Reserve**	**Saldo**
9.03	Concernstelposten	-385		385			385
9.01	Bestuursdienst	385		-385			-385
	Totalen begrotingswijziging	**0**		**0**	**0**	**0**	**0**

Als het project eind 2008 afgerond is, dan kunnen de inspanningen verminderen. Eind 2008 zullen wij een definitief voorstel doen voor de benodigde structurele middelen met ingang van 2009.

Bijlage.
- Bijlage I: Informatiebeveiliging: de kaders d.d. 6 maart 2007.

Wij stellen u voor te besluiten:

I. de kaders en aanpak voor "Informatiebeveiliging" vast te stellen;
II. een structurele bijdrage van € 385.000,-- beschikbaar te stellen en toe te voegen aan het programma Bedrijfsvoering en Organisatie Ontwikkeling/Stad en Stadhuis;
III. dit bedrag te dekken uit de gereserveerde middelen voor nieuw beleid 2007;
IV. de gemeentebegroting 2007 dienovereenkomstig te wijzigen.

Burgemeester en wethouders
van Groningen,

De burgemeester, De secretaris,

Jacq. Wallage. H.P. Bakker.