Collegebesluit

Onderwerp: Informatiebeveiligingsbeleid 2014 - 2018
BBV nr: 2014/467799

1. Inleiding

In 2011 zorgde een aantal incidenten rond de beveiliging van overheidsinformatie er voor dat met andere ogen werd gekeken naar informatieveiligheid bij gemeenten. De DigiNotar-crisis toonde aan dat de gemeentelijke ICT-infrastructuur kwetsbaar is, en een reeks publicaties[1] over aan informatiebeveiliging gerelateerde incidenten bij gemeenten legde een structureel probleem bloot: De informatieveiligheid was onvoldoende gegarandeerd.

Na 2011 is een duidelijke omslag zichtbaar in het denken over informatieveiligheid. Onderkend is dat waar informatie in steeds meer processen en ketens een steeds grotere rol speelt, de zorg voor de veiligheid van deze informatie niet mag achterblijven. De gemeenten hebben gekozen voor een gezamenlijke aanpak in VNG verband.

In het coalitieprogramma 2014-2018 ‘Samen Doen!’ ligt vast dat informatiebeveiliging de aandacht krijgt zoals in VNG verband is afgesproken. Dit verwijst naar de VNG resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ van november 2013, een forse aanzet voor het verbeteren van lokale informatiebeveiliging. De Informatiebeveiligingsdienst, onderdeel van KING en door de VNG in het leven geroepen om gemeenten te ondersteunen, heeft een Baseline Informatieveiligheid Gemeenten (BIG) opgeleverd. Deze Baseline is in Haarlem gebruikt om het in 2011 vastgestelde ‘Gemeentelijk InformatiebeveiligingsBeleid’ volledig te herzien.

Het college heeft de gemeentelijke organisatie aangepast aan de afspraken in de VNG-resolutie door beveiligingsfunctionarissen aan te stellen en informatiebeveiliging te positioneren in het ondersteuningsteam van de CIO.

Het nieuwe Informatiebeveiligingsbeleid 2014-2018 is in december 2013 reeds vastgesteld in een directiebesluit. Invulling gevend aan het normenkader van de VNG en als deel van de uitvoering van dit beleid wordt de vaststelling ervan voortaan belegd bij het college. Het beveiligingsplan voor SZW is herzien om aan te sluiten bij het nieuwe beleid.

[1] O.a. het initiatief ‘Lektober’ van Webwereld: http://webwereld.nl/tag-lektober-2011

2. Besluitpunten college

Het college besluit:

1. het Gemeentelijk Informatiebeveiligingsbeleid 2014-2018 inclusief de Basis beveiligingsrichtlijnen Sociale Zaken en Werkgelegenheid vast te stellen;

2. de Baseline Informatiebeveiliging Gemeenten vast te stellen als basisnormenkader voor informatiebeveiliging;

3. informatieveiligheid expliciet te benoemen in de portefeuille waarin ook Bedrijfsvoering is opgenomen;

4. de CIO opdracht te geven informatiebeveiliging inclusief financiële en personele impact uit te werken in een integrale strategische nota Informatievoorziening.

3. Beoogd resultaat

Informatie moet beschikbaar en betrouwbaar zijn, en alleen toegankelijk voor bevoegden. Dit is de kern van informatieveiligheid.

Het informatiebeveiligingsbeleid beoogt:

- Het managen van de informatiebeveiliging;
- Adequate bescherming van bedrijfsmiddelen;
- Het minimaliseren van risico's van menselijk gedrag;
- Het voorkomen van ongeautoriseerde toegang;
- Het garanderen van correcte en veilige informatievoorzieningen;
- Het beheersen van de toegang tot informatiesystemen;
- Het waarborgen van veilige informatiesystemen;
- Het adequaat reageren op incidenten;
- Het beschermen van kritieke bedrijfsprocessen;
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers;
- Het waarborgen van de naleving van dit beleid.

De belangrijkste doelen voor de korte termijn zijn het verhogen van het bewustzijn rond informatieveiligheid in de gehele organisatie (menselijk gedrag), het voorkomen van ongeautoriseerde toegang door verbeteren en uniformeren van processen rond gebruikersautorisaties, het beschermen van kritieke bedrijfsprocessen door o.a. verdere professionalisering van wijzigingsprocessen en het realiseren van een goed continuïteits- en herstelplan.

Met het oog op alle wijzigingen rond de 3 decentralisaties is het beschermen van persoonsgegevens een specifiek doel waar de komende tijd veel aandacht naar uit gaat. Met de herziene Basis beveiligingsrichtlijnen SZW wordt het Informatiebeveiligingsbeleid toegepast op taken binnen het Sociaal Domein.

4. Argumenten

1. Vaststellen Informatiebeveiligingsbeleid en Basis beveiligingsrichtlijnen SZW

Volgende stap op ingeslagen weg
Na vaststelling van het Informatiebeveiligingsbeleid 2014-2018 door de directie is reeds een aantal stappen gezet op weg naar het beoogde resultaat. In de Concernstaf is op een onafhankelijke positie de Coördinator Informatiebeveiliging (Engels: Chief Information Security Officer / CISO) aangesteld. De CISO adviseert de directie op het gebied van informatieveiligheid, stelt het beveiligingsbeleid op en ziet toe op naleving van het beleid. Bij Middelen & Services is de Information Security Officer (ISO) aangesteld. De ISO stelt op basis van het beleid jaarlijks een plan op en implementeert aan de hand hiervan het beleid verder in de organisatie. Daarnaast is de afhandeling van informatiebeveiligingsincidenten belegd bij een functioneel team van technisch specialisten met een escalatielijn via de CIO, directie en portefeuillehouder.

Bestuur raakt meer direct betrokken bij informatieveiligheid
Door de normen uit de Baseline Informatiebeveiliging Gemeenten (BIG) te implementeren wordt geborgd dat de informatieveiligheid op orde is. Het Informatiebeveiligingsbeleid is gebaseerd op de BIG. Tenminste eenmaal per vier jaar wordt het beleid herzien en opnieuw vastgesteld door het college. Jaarlijks stelt de Security Officer op basis van het beleid een Informatiebeveiligingsplan op. Over de voortgang van de uitvoering wordt jaarlijks gerapporteerd aan het college. Een belangrijk te verbeteren aspect van Informatieveiligheid is de menselijke factor. Het bewustzijn rond informatieveiligheid moet in de gehele organisatie worden verhoogd, ook bij het college als bestuurlijk verantwoordelijke. De verantwoordelijkheid voor het Informatiebeveiligingsbeleid wordt om die reden door het college van B&W gedragen.

Verbeterpunten accountant in het beleid vastgelegd
Na het uitkomen van de management letter 2012 is in 2013 door de directie het geactualiseerde beveiligingsbeleid vastgesteld. Daarmee wordt invulling gegeven aan de volgende punten:
- Het op orde brengen van (het proces rond) de gebruikersautorisaties;
- Het verhogen van het beveiligingsbewustzijn binnen de organisatie;
- Het integreren van de testprocedure in het wijzigingsbeheer;
- Het opstellen van een continuïteits- of herstelplan, met name voor kritieke systemen.

Richtlijnen SZW aansluiten op nieuw beleid
De Basis beveiligingsrichtlijnen van SZW zijn volledig gereviseerd om aan te sluiten op het nieuwe Informatiebeveiligingsbeleid. Vaststellen van de Basis beveiligingsrichtlijnen SZW heeft geen financiële consequenties.

2. Baseline Informatiebeveiliging Gemeenten als basisnormenkader

Samenwerking door breed gedragen uniforme aanpak
Door het normenkader uit de Baseline Informatiebeveiliging Gemeenten over te nemen kunnen gemeenten efficiënt samenwerken rond informatieveiligheid. Dit uit

zich bijvoorbeeld in de eenduidige eisen die worden gesteld aan leveranciers van software, maar ook in het kunnen uitwisselen van handreikingen en best practices binnen de BIG. De Baseline is bedoeld als hulpmiddel om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen. Wanneer de informatievoorziening wordt ingericht volgens deze normen geeft dit voldoende garantie dat de informatieveiligheid op orde is. Het voldoen aan de Baseline Informatiebeveiliging Gemeenten maakt de gemeente een betrouwbare partner richting andere overheden.

Op termijn vermindering van extern opgelegde audits
De Baseline heeft ten doel de auditlast bij gemeenten te verminderen. Waar het aantal verplichte IT audits in de achterliggende jaren voortdurend toenam (Suwinet, DigiD, GBA, etc.) wordt middels de Baseline aangestuurd op het consolideren van normen en uiteindelijk audits. Door nu de normen van de Baseline te hanteren zal op termijn het aantal verschillende uit te voeren IT audits worden beperkt.

3. Opnemen van informatieveiligheid in portefeuille met bedrijfsvoering

Uitvoering van resolutie
Het opnemen van informatieveiligheid in de portefeuille van een lid van het college van B&W geeft invulling aan een afspraak in de VNG resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’.

Borging betrokkenheid bestuur
Het college van B&W is integraal verantwoordelijk voor de beveiliging van informatie die de gemeente gebruikt bij het vervullen van haar maatschappelijke taken. Door informatieveiligheid als onderwerp expliciet onder te brengen in een portefeuille wordt de betrokkenheid van het bestuur geborgd.

Aansluitend bij huidige praktijk
In de praktijk is informatieveiligheid tot nu toe als onderdeel van informatievoorziening belegd geweest bij de portefeuillehouder bedrijfsvoering. Er is geen aanleiding dit nu te wijzigen. De ontwikkelingen rond de strategische kaderstelling op de informatievoorziening pleiten ervoor deze koppeling in stand te houden. Binnen het ondersteuningsteam van de CIO en met de bevoegdheden van de CIO kan informatieveiligheid integraal worden meegenomen bij ontwikkelingen in de informatievoorziening.

4. Uitwerken informatiebeveiliging in strategische nota informatievoorziening

Financiële en personele impact afhankelijk van strategische keuzes
De uitvoering van het beleid heeft een structureel effect op de organisatie. Er zal invulling worden gegeven aan een aantal nieuwe taken en processen. Deze taken en processen zijn te veelomvattend om in de bestaande uitvoeringsorganisatie onder te brengen. Bovendien zullen investeringen in de infrastructuur nodig zijn specifiek met het doel de informatieveiligheid te verbeteren. Welke consequenties dit heeft valt nog niet in te schatten, omdat deze sterk afhankelijk zijn van een aantal strategische keuzes die gemaakt moeten worden. Deze keuzes worden in de komende maanden uitgewerkt.

Kaders voor het geheel aan informatievoorziening
In het voorjaar wordt voor de kadernota een strategische nota Informatievoorziening opgesteld, waarin het geheel aan informatievoorziening wordt beschouwd en van kaders voorzien. Deze nota zal richting geven aan de ontwikkeling van informatievoorziening in de komende jaren. Informatieveiligheid is daarbij een belangrijk aspect. In deze nota wordt tevens uitgewerkt wat de financiële en personele impact is. Te verwachten is dat het college bij de kadernota zal voorstellen extra middelen voor informatiebeveiligingsbeleid ter beschikking te stellen.

Routekaart voor verbetering informatieveiligheid
Het Informatiebeveiligingsbeleid is veelomvattend. Volledige realisatie van het beoogd resultaat zal meerdere jaren in beslag nemen en ook daarna zal het op peil houden van de informatieveiligheid een doorlopende activiteit blijven. Een routekaart is nodig om te komen van de huidige situatie naar het volledig voldoen aan het normenkader zoals voorgeschreven in de BIG. Als voorbeeld: De organisatie moet de kans krijgen om zich nieuwe normen eigen te maken en deze te implementeren alvorens hierop audits worden losgelaten: implementatie van nieuwe normen vraagt om een traject van steeds afnemende vrijblijvendheid.

Voortdurend veranderende dreiging
Informatiebeveiliging evolueert in hoog tempo. Bedreigingen op het gebied van informatieveiligheid veranderen voortdurend en nemen toe in aantal en potentiële impact. Vanuit de Rijksoverheid wordt de komende jaren sterk ingezet op het onder controle krijgen van deze dreigingen. Om de informatieveiligheid te waarborgen beweegt de gemeente Haarlem daarin mee. Flexibiliteit in de aanpak is ingebouwd door jaarlijks opnieuw te analyseren wat met het Informatiebeveiligingsplan moet worden gerealiseerd.

5. Kanttekeningen

Relatie informatieveiligheid en privacy
Privacy wordt, ook binnen de gemeente Haarlem, vaak in één adem genoemd met informatieveiligheid. De onderwerpen hebben een duidelijke relatie, immers informatiebeveiliging is een randvoorwaarde voor vertrouwelijke verwerking van privacygevoelige gegevens. Overwogen is om de onderwerpen informatieveiligheid en privacy gezamenlijk in een portefeuille onder te brengen. Privacy is echter naar haar aard een ander onderwerp. Dit gaat over ethische afwegingen in de vertaling van wet- en regelgeving naar richtlijnen en procedures. Niet alles wat binnen het wettelijk kader is toegestaan is ook wenselijk wanneer het gaat om privacy. Over deze specifieke dilemma's en de bescherming van persoonsgegevens bij ons handelen als overheid volgt 1e kwartaal 2015 een nota Privacy.

Balans informatieveiligheid en efficiëntie
Een kanttekening kan worden geplaatst bij het effect op processen en werkwijzen. De meest efficiënte werkwijze is niet altijd de beste uit oogpunt van informatieveiligheid. Met het vaststellen van de baseline kiest het college voor het stevig plaatsen van beveiligingsaspecten in de afwegingen die daarover bij het inrichten van onze geautomatiseerde processen genomen moeten worden.

Absolute veiligheid onmogelijk
Ook bij een zeer goed informatiebeveiligingsbeleid blijft een risico bestaan op incidenten. Absolute zekerheid kan niet worden geboden. De genoemde voortdurend veranderende dreiging maakt van Informatiebeveiliging een soort wapenwedloop. Nieuwe bedreigingen zijn niet altijd bekend en nieuwe maatregelen kunnen niet altijd zo snel worden getroffen als wenselijk op basis van een nieuwe dreiging. Met ondersteuning van de Informatiebeveiligingsdienst zullen de doelen van het informatiebeveiligingsbeleid zo goed als redelijkerwijs mogelijk worden gerealiseerd.

6. Uitvoering

Uitvoering reeds gestart
Het Informatiebeveiligingsbeleid 2014 - 2018 is reeds van kracht sinds vaststelling door de Directie. De uitvoering is in volle gang. Vaststelling van beleid en normenkader door het college en het opnemen van informatieveiligheid in de portefeuille met bedrijfsvoering zijn deel van de uitvoering van het beleid.

Concrete punten naar aanleiding van brief VNG
Vanuit de VNG wordt gestuurd op een aantal concrete resultaten. Per brief dd. 19 november 2014 (reg.nr. 2014443052) wordt college en gemeenteraad door de VNG geïnformeerd over voortgang informatieveiligheid. Ook wordt gevraagd invulling te geven aan de resolutie door de gemeente aan te laten sluiten bij de Informatiebeveiligingsdienst, transparant te zijn over de voortgang door de uitvraag op waarstaatjegemeente.nl in te vullen en gebruik te maken van het beschikbare leeraanbod I-Bewustzijn.

- De gemeente Haarlem is sinds november 2013 aangesloten bij de IBD. Deze aansluiting bestaat uit meerdere stappen. In januari 2015 worden de laatste stappen afgerond. Dit leidt ertoe dat de gemeente meer op de Haarlemse situatie toegesneden adviezen en waarschuwing kan ontvangen van de IBD;
- De uitvraag op waarstaatjegemeente.nl is ingevuld;
- Het leeraanbod I-Bewustzijn wordt overwogen als deel van de voor 2015 geplande interne campagne ter bevordering van veiligheidsbewustzijn.

Vervolg
Voor de kadernota 2015 worden de financiële en personele consequenties van de nieuwe taken die voortvloeien uit het Informatiebeveiligingsbeleid uitgewerkt in een strategische nota Informatievoorziening.

Iedere vier jaar, of zoveel eerder als nodig, zal een vernieuwd Informatiebeveiligingsbeleid worden vastgesteld door het college. Op basis van dit beleid wordt jaarlijks een Informatiebeveiligingsplan opgesteld aan de hand waarvan de organisatie de informatieveiligheid op peil houdt en verbetert.

7. Bijlagen

1. Informatiebeveiligingsbeleid 2014 - 2018
2. Basis beveiligingsrichtlijnen Sociale Zaken en Werkgelegenheid
3. Strategische Baseline Informatiebeveiliging Gemeenten (BIG)
4. Brief VNG: ‘Voortgang Informatieveiligheid’ (reg.nr. 2014443052)

Het college van burgemeester en wethouders

de secretaris de burgemeester