Hoe kunnen Nederlandse gemeenten aan BIG voldoen?

LinkedIn, Nov 13, 2014

De VNG heeft op 29 november 2013 een resolutie aangenomen waarin de Nederlandse gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG) als normenkader onderschrijven en bij het Rijk en ketenpartners zullen bevorderen. De BIG beschrijft eisen waaraan een gemeente dient te voldoen, op straffe van bijvoorbeeld het afsluiten van DigiD.

In andere branches is een vergelijkbare ontwikkeling waar te nemen:

- In de financiële sector is informatiebeveiliging een basisvereiste. Daar heeft De Nederlandsche Bank (DNB) een set van 54 practices (controls/eisen/maatregelen) voorgeschreven o.b.v. COBIT en ISO27002. Deze controls zijn rechtstreeks overgenomen uit de betreffende normdocumenten. COBIT zelf bevat 201 practices.
- In de zorg is patiëntveiligheid en –privacy een hot item; daar werden in 2010 de informatiebeveiligingseisen door de Inspectie voor de Gezondheidszorg (IGZ) ingevuld door een sectie van 33 controls uit de Nederlandse standaard NEN7510 voor te schrijven aan de zorginstellingen. De norm NEN7510 zelf bevat 151 controls, en is grotendeels gebaseerd op de internationale norm ISO27001, en de bijbehorende concretisering in ISO27002. Per medio juli 2014 is het voor zorginstellingen bij wet verplicht om de integrale NEN7510-eisen te voldoen als ze in hun elektronisch patiëntendossier (EPD) gebruik willen maken van het burgerservicenummer.

Zowel DNB als de IGZ zouden graag zien dat de betrokken instellingen zelfstandig kunnen bepalen wat belangrijk voor hen is, en een voortdurende, gestructureerde verbetering in werking zetten. Ze hebben dus een voorkeur voor een *principle based benadering* in plaats van de huidige *rule based benadering*. De praktijk laat helaas nog zien dat dit zowel aan de kant van de toezichthouder als aan de kant van de uitvoerende partij veelal blijft steken in wishful thinking.

Hoe pakt de toezichthouder van de Nederlandse gemeenten dit nu aan? Is daar al sprake van een *principle based* benadering? Heeft men daar al geleerd van de ervaringen in de zorg en de financiële sector, en de *rule based* benadering achter zich gelaten? De rol van toezichthouder ligt in dit geval bij de staat, maar de aansturing wordt vanuit de sector zelf ondersteund door een combinatie van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). Deze ondersteuning is concreet gemaakt in de vorm van een resolutie waarin de BIG wordt onderschreven door de VNG, en het instellen van een centraal ondersteunend orgaan van KING: de Informatiebeveiligingsdienst voor gemeenten (IBD). De BIG bestaat uit:

Een strategische BIG, waarin het belang van het herstel van veiligheidsincidenten centraal staat. Dit document benadrukt de schade die kan ontstaan bij veiligheidsincidenten, voor de burger, voor de overheid zelf, en het bedrijfsleven.

- Een tactische BIG, een richtlijn met een totaalpakket aan informatiebeveiligingsmaatregelen die voor iedere gemeente geldt. Deze tactische BIG is opgezet rondom ISO 27001 en ISO 27002.
- Een set van 303 controls als operationele uitwerking van de BIG

Wat valt op aan deze benadering:

- Er is in de operationele controls geen zichtbare referentie gelegd naar een onderliggende formele norm.
- Er is sprake van een *enorm* groot aantal, zeer gedetailleerd uitgewerkte controls: 303 stuks.
- Deze controls zijn sterk gericht op technische uitvoering: werkzaamheden ("*Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels*") en voorzieningen ("*Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen*") worden in detail voorgeschreven.
- Er is zeer weinig aandacht voor het managementsysteem waarmee die werkzaamheden en voorzieningen beheerd en geborgd worden.

De BIG is dus een typische *rule based* benadering.

Technocratie
Gemeentes die enthousiast beginnen met het realiseren van deze 303 controls lijken daarmee een *technocratische aanpak* te gaan volgen: gedetailleerde technische voorschriften en gedragsregels vormen het hoofdbestanddeel van de aanpak. Die technocratische benadering is al jaren één van de hoofdoorzaken voor de uiterst complexe en moeilijk beheersbare situatie waar de gemeentes zich (net als een groot deel van het bedrijfsleven) momenteel in bevinden: er is jarenlang vooral gekoerst op de "T" van *technologie*, waarbij de aandacht voor het managementsysteem ver achter bleef. Als nu opnieuw eenzelfde benadering wordt gevolgd, ligt het voor de hand dat je dezelfde resultaten krijgt als voorheen: veel inspanningen die weinig borging in een managementsysteem hebben, zodat er veel energie wordt besteed waar slechts weinig blijvende resultaten uit voortkomen. Een technocratische aanpak lost het probleem tijdelijk op maar leert de organisaties niet omgaan met soortgelijke situaties. Er is onvoldoende sprake van *borging*. Het invoeren van de 303 BIG-controls leidt dus niet tot een *principle based benadering* die de borging en de continue verbetering centraal stelt. En daar zijn we nu toch zo langzamerhand wel aan toe….

Gebrek aan processturing
Een procesmatige onderbouwing van alle in de BIG opgesomde activiteiten ontbreekt. Er is wel een zwakke verwijzing naar het *herstellen* en *wijzigen* van de informatiesystemen, maar daarmee is het ook wel zo'n beetje gedaan. Processen zoals *afspreken* en

voorkomen komen slechts fragmentarisch in beeld, en *informeren* en *leveren* worden al helemaal niet in een procesmatige context aangesproken. Veruit het grootste deel van de eisen gaat over technische voorzieningen of gedragsregels. Maar, stel je voor dat je die allemaal een keer geregeld hebt, hoe zorg je er dan voor dat je bij een volgende ontwikkeling in de markt de dan noodzakelijke voorzieningen of gedragsregels signaleert en invoert? Daar heb je toch een onderliggend proces voor nodig? Dat proces is hier duidelijk niet de grondslag geweest voor de ontwikkeling van het eisenpakket. Actuele technologie en actuele praktijk wel. Die technologie en praktijk zijn echter voortdurend in beweging, dus deze aanpak lijkt een garantie om op afzienbare termijn *weer* achter de feiten aan te lopen.

Wat kan een gemeentelijke I&A-organisatie met de BIG-controls?
Zoals altijd met dit soort eisenpakketten vindt slechts een deel van de informatiebeveiliging (IB) plaats binnen de scope van de IT-beheerafdeling (I&A). Wat er buiten valt is vooral te scharen onder de noemer **Personeelszaken (PZ)** en **Facilitair beheer (FACB)**. Die twee moeten dus hoe dan ook worden gedekt als je aan de BIG wil voldoen. Dat kan op twee manieren:

1. Door 3 gescheiden servicedomeinen te hanteren: I&A, PZ, en FACB. Elk van die domeinen probeert z'n eigen zaken uit het eisenpakket op eigen houtje te regelen, en de Chief Information Security Officer (CISO) treedt op als externe aanjager. De CISO is meestal ondergebracht in een stafafdeling, dus buiten I&A, PZ en FACB, soms zelfs in een bovengemeentelijk samenwerkingsverband.
2. Door de IB-targets vanuit één domein te managen. Omdat veruit de meeste eisen binnen het domein I&A vallen is dat het voor de hand liggende sturingsdomein. De PZ- en FACB-taken op het gebied van de IB kunnen dan vanuit dat I&A-domein worden aangestuurd. Een CISO kan dan (functioneel binnen de groep I&A) het integrale eisenpakket en de bijbehorende projectmatige realisatie onder één sturing brengen.

Optie 1 leidt tot sturing vanuit een zijlijn, in een gefragmenteerd project met 3 uitvoerende domeinen. Die situatie komt in de praktijk vaak voor. De CISO moet dan mandaat genoeg hebben om alle 3 domeinen aan te kunnen sturen. Dat mandaat is in de praktijk vaak slechts beperkt aanwezig.

Als die drie domeinen elk een gestructureerd managementsysteem hanteren, dan heeft de CISO daar groot voordeel van: hij kan veel beter schakelen met elk domein, omdat elk domein alle taken binnen haar grenzen kan aansturen in haar managementsysteem. Deze situatie wordt in de zorg en in de financiële sector door een aantal organisaties ingevuld met de ISM-methode, vooral in de I&A-hoek. ISM voorziet in het Information Security Management System (ISMS), biedt tooling voor de planning, aansturing, voortgangsbewaking en compliancy-meting van de betreffende controls, en brengt deze in een eenvoudige en integrale managementaanpak onder. ISM ondersteunt bij uitstek een *principle based* benadering. De CISO kan zich in zo'n geval vooral concentreren op de overige domeinen, en op de integratie tussen de 3 domeinen. Vanuit een zijlijnpositie zonder formeel mandaat is dat een forse opgaaf. Deze aanpak vergt dus een stevige visie en leiderschap op bestuurlijk niveau binnen de gemeente.

Optie 2 heeft als voordeel dat er vanuit het domein waar de *meerderheid* van het werk ligt centraal kan worden gestuurd op de uitvoering van taken in beide ondersteunende domeinen (PZ/FACB), in eerste instantie vanuit een projectmatige aanpak. Ook in die andere domeinen kunnen organisaties de ISM-methode inzetten, in een 'algemene' vorm, zonder verbijzondering naar IT.

Optie 2 kan in de praktijk echter tegen dezelfde autoriteitsproblemen aanlopen: het vergt de medewerking van de manager PZ en de manager FACB, alsmede van hun

medewerkers. Deze optie vergt dus feitelijk de sturing vanuit de eersthogere managementlaag: de manager die verantwoordelijk is voor zowel I&A als PZ en FACB. En ook dat vereist weer een stevige visie en leiderschap.

Een derde factor die feitelijk buiten beeld is vanuit de positie van I&A is de gebruiker. Een deel van de BIG-controls komt voor rekening van die gebruiker, waar I&A geen managementverantwoordelijkheid heeft: dat valt immers onder de lijntaak van de gemeentelijke organisatie. I&A kan wel *eisen* stellen, om de sturing op de activiteiten van die gebruiker te voeden. Zulke eisen vinden dan hun plek in de SLA (als die er is), in de servicecatalogus (als die er is), en in gemeentelijke richtlijnen die voor alle medewerkers gelden (als die er zijn). Dat vergt opnieuw de actieve inzet van de verantwoordelijke lijnmanager op het eersthogere niveau. Omdat die rol boven PZ, FACB, I&A en de gebruikers ligt zal dat veelal de gemeentesecretaris zijn. Die gemeentesecretaris heeft echter z'n handen vol aan de komende decentralisatie, en IT stond toch al niet zo hoog op de agenda. Een centrale afdeling Bedrijfsondersteuning o.i.d. zou hier soelaas kunnen bieden, mits het mandaat goed belegd wordt en er (alweer) leiderschap en visie aanwezig is.

Centrale, procesmatige aanpak is onontkoombaar
Om op een efficiënte en effectieve wijze te voldoen aan de doelstellingen van de BIG is dus centrale sturing in de organisatie een vereiste. Oftewel, als de gemeentesecretaris niet het voortouw neemt bij de invoering van de BIG, en de sturing daarop in het gemeentelijk apparaat managet of delegeert aan een gemandateerde afdeling Bedrijfsondersteuning, dan gaat de betreffende gemeente niet zo erg ver komen met de BIG. Of dat dan komt door problemen met leiderschap, visie, tijd, kennis van IT, of aandacht, maakt in de praktijk niet veel uit.

Een tweede minimale vereiste is dat de gemeente werkt vanuit een efficiënte procesmatige managementaanpak zoals in het bedrijfsleven al lang gebruikelijk is, en niet verzeild raakt in een technocratische benadering. Anders kun je de gevolgen wel weer uittekenen.

Het is vijf voor twaalf, en gegeven de enorme druk die er door de komende decentralisatie op gemeentes ligt, zal er snel en hard gewerkt moeten worden om te voorkomen dat die klok straks toch het volle uur slaat.