Een tweesporenaanpak voor informatiebeveiliging

Risicomanagement is een cruciaal onderdeel van de bedrijfsvoering. Het managen van de risico's die de informatievoorziening loopt, oftewel informatiebeveiliging, heeft echter nogal wat voeten in de aarde. Te weinig beveiliging leidt tot onverantwoorde risico's, maar te veel beveiliging frustreert de organisatie. Het is de kunst om hierin evenwicht te vinden en informatiebeveiliging effectief te organiseren. Dit artikel gaat in op een tweesporenaanpak waarmee dat gerealiseerd kan worden.

Auteurs: **Dr. Marcel E.M. Spruit** en **drs. Martin de Graaf**, zijn beiden verbonden aan Het Expertise Centrum. Marcel Spruit is tevens lector Informatiebeveiliging aan de Haagse Hogeschool en TH Rijswijk.

Voor iedere organisatie is het van belang dat er verantwoord wordt omgaan met risico's, oftewel dat er aan risicomanagement wordt gedaan. Er zijn personele, materiële, en financiële risico's, maar ook risico's met betrekking tot de informatievoorziening. Informatiebeveiliging richt zich op het managen van de risico's die betrekking hebben op de betrouwbaarheid van de informatievoorziening. Daarmee is informatiebeveiliging een onderdeel van risicomanagement en dus van de bedrijfsvoering.

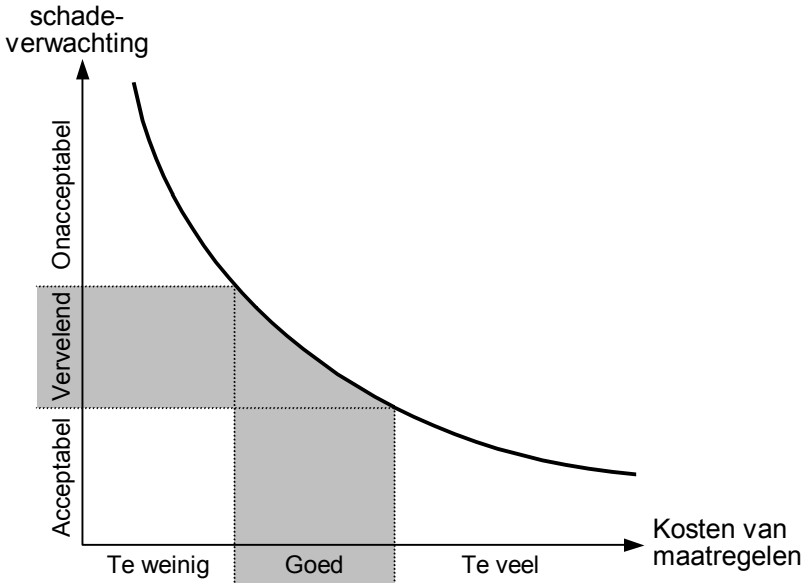
De risico's waar informatiebeveiliging zich op richt, ontstaan doordat de al dan niet geautomatiseerde informatievoorziening getroffen kan worden door een grote verscheidenheid aan bedreigingen, variërend van natuurrampen tot apparatuurstoringen en al dan niet opzettelijke menselijke fouten. De risico's kunnen beperkt worden door het nemen van maatregelen. De vraag is alleen welke maatregelen nodig en voldoende zijn. Het is duidelijk dat niemand baat heeft bij te weinig maatregelen en al helemaal niet bij de verkeerde maatregelen. Aan de andere kant leidt een overmaat aan maatregelen tot hoge kosten en het onnodig hinderen van het normale werk. Het is dus zaak om hierin een evenwicht te vinden.

Risico's en maatregelen

Om te bepalen tegen welke bedreigingen iets moet worden ondernomen, moet niet zozeer naar de *bedreigingen* gekeken worden als wel naar de *risico's*, oftewel de te verwachten schade door de bedreigingen (Overbeek e.a., 2000). Het begrip *schade* moet daarbij breed geïnterpreteerd worden: financiële schade, derving van omzet, imagoverlies, kwaliteitsvermindering, et cetera.

Tot een bepaald niveau kunnen risico's zonder veel problemen geaccepteerd worden. Het gaat dan om 'kleine' problemen, bijvoorbeeld storingen die zonder veel impact opgelost kunnen worden en fouten die zonder noemenswaardige schade te corrigeren zijn. Er zijn echter

ook risico's waarbij de schade zo groot is dat de bedrijfsprocessen of zelfs de continuïteit van de organisatie ernstig in gevaar gebracht worden. Hieronder valt bijvoorbeeld het afbranden van het computercentrum. Dergelijke risico's zijn onacceptabel. Tussen deze twee niveaus ligt een gebied waarin de te verwachten schade kan leiden tot een weliswaar vervelende, maar niet fatale, verstoring van bedrijfsprocessen (zie Figuur 1).



Figuur 1: Schadeverwachting versus kosten van maatregelen

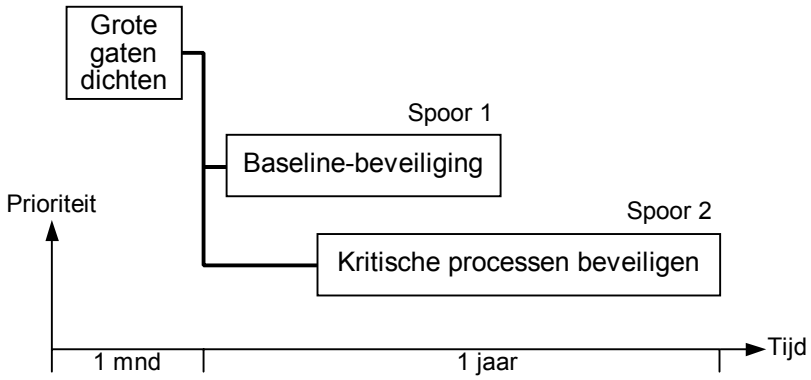
Door maatregelen te treffen is het mogelijk de risico's te verkleinen. Maar vanzelfsprekend zijn hier kosten aan verbonden. Het betreft de initiële kosten voor het ontwerpen, realiseren en implementeren van de maatregelen, maar ook de terugkerende kosten voor het onderhoud en de bewaking ervan. Een beperking van de functionaliteit van de informatievoorziening is ook een kostenpost.
Figuur 1 laat zien dat hoe meer uitgegeven wordt aan de maatregelen, des te lager de te verwachten schade is. De kunst is om wel maatregelen te treffen tegen de bedreigingen die tot onacceptabele risico's leiden, maar niet tegen de bedreigingen die geen noemenswaardige risico's met zich meebrengen. Het is bovendien belangrijk dat de getroffen maatregelen een samenhangend geheel vormen. Dit betekent dat binnen een bedrijfsproces de maatregelen op elkaar afgestemd moeten worden en dat bedrijfsbrede coördinatie nodig is voor de maatregelen die de verschillende bedrijfsprocessen overstijgen (Overbeek & Roos Lindgreen, 2002).

Tweesporenaanpak

In het kader van risicomanagement dient de directie te bepalen welke risico's voor de organisatie te hoog zijn en welke maatregelen daarvoor nodig zijn. In principe moet men er van uit kunnen gaan dat de directie heel goed weet wat de belangrijkste risico's voor de eigen organisatie zijn en welke maatregelen daarvoor nodig zijn. Als één of meer van deze maatregelen nog niet getroffen zijn, dan bestaat er dus een belangrijk risico, waarop de directie

urgent actie moet ondernemen. In Figuur 2 wordt deze stap aangeduid als ‘grote gaten dichten’. Voorbeelden hiervan zijn de maatregelen tegen hackers die getroffen dienen te worden naar aanleiding van een penetratietest van een internetbankiersysteem, en het aanpassen van de uitwijkfaciliteit na een configuratieverandering van een zeer tijdkritisch boekingssysteem.

Voor de verschillende bedrijfsprocessen[1] heeft de directie als het goed is ‘eigenaren’ aangewezen. Bovendien dient de directie te bepalen welke bedrijfsprocessen grote risico’s in zich dragen voor de organisatie, oftewel welke processen ‘kritisch’ zijn. De eigenaar van een proces is verantwoordelijk voor het betreffende proces en de daarin gebruikte informatiesystemen; in het algemeen is een eigenaar een lijnmanager of een hoofd van een stafdienst. Iedere eigenaar dient voor ‘zijn’ proces te bepalen welke risico’s te hoog zijn, welke maatregelen daarvoor nodig zijn en welke daarvan urgent zijn. De eigenaren van de bedrijfsprocessen worden geacht zelf deze inschatting te kunnen maken, rekening houdend met het feit dat hun proces al dan niet kritisch is voor de organisatie. Mocht een eigenaar dat toch niet kunnen of willen, dan kan daarvoor de hulp ingeroepen worden van een deskundige. Deze kan met behulp van een checklist eenvoudig en snel bepalen welke maatregelen geen uitstel kunnen velen. Ook hier geldt: als één of meer van deze maatregelen ontbreken, zijn belangrijke risico’s nog niet afgedekt en heeft de betreffende proceseigenaar dus nog een urgente actie uitstaan. Ook dit valt nog onder de noemer ‘grote gaten dichten’.



Figuur 2: Tweesporenaanpak

De volgende stap in de tweesporenaanpak beoogt het goed op de rails zetten van de informatiebeveiliging. Hierin zijn twee ‘sporen’ te onderkennen (Glashouwer e.a., 2002). Het eerste spoor richt zich op het creëren van een zogenaamde *baseline* voor de informatiebeveiliging. Het tweede spoor beoogt de processen die kritisch zijn voor de organisatie nog eens grondig onder de loep te nemen om te bepalen of daarvoor nog aanvullende maatregelen nodig zijn. Vanwege praktische redenen, zoals onder meer de beschikbare menskracht, start het tweede spoor veelal later dan het eerste spoor, hoewel dat in principe niet noodzakelijk is.

[1] Het kan ook groepen, afdelingen, of projecten betreffen.

Baseline-beveiliging

Voor het inrichten van informatiebeveiliging wordt gezocht naar een samenhangende set maatregelen. Veel maatregelen kunnen het best (bedrijfs)breed ingevoerd worden. Hiervoor kunnen verschillende argumenten zijn:

- De maatregelen werken van zichzelf al (bedrijfs)breed (bijvoorbeeld huisregels en gedragsrichtlijnen, inbraakbeveiliging van het pand, noodaggregaat tegen stroomstoring).
- De maatregelen gelden voor (bijna) iedereen in de organisatie (bijvoorbeeld classificatierichtlijnen voor informatie, clear-desk voor vertrouwelijke stukken, beveiliging van berichtenverkeer met externe partijen).
- De effectiviteit of de efficiëntie van de maatregelen verbetert als ze breed toegepast worden (bijvoorbeeld centraal incidentmanagement, centrale firewall, standaard antivirus-programmatuur).

De (bedrijfs)breed geldende maatregelen vormen een minimumbeveiligingsniveau voor de gehele organisatie. De set maatregelen waarmee deze minimumbeveiliging wordt geboden, duidt men veelal aan met de term *baseline*.

Bij het samenstellen van een baseline-beveiliging blijkt dat in verschillende situaties toch meestal dezelfde maatregelen nodig zijn. Vandaar dat men voor het samenstellen van een baseline gebruik kan maken van een standaardlijst van maatregelen voor informatiebeveiliging. In Nederland is de bekendste en meest gebruikte standaardlijst de *Code voor Informatiebeveiliging*, ook wel afgekort tot ‘de Code’ (NNI, 2000; Oud, 2002). De Code kan gebruikt worden als een checklist, waarmee men afvinkt of alle relevante maatregelen genomen zijn. Voor iedere maatregel geeft de Code een korte toelichting over het belang ervan. Op basis daarvan kan de directie zonodig beslissen dat bepaalde maatregelen in de gegeven situatie niet relevant zijn, of dat er juist een paar maatregelen toegevoegd moeten worden.

Organisaties die voor hun baseline-beveiliging gebruik maken van de Code profiteren van het bijkomende voordeel dat ze een beveiligingsniveau realiseren dat vergelijkbaar is met dat van andere organisaties die ook de Code gebruiken. Zeker in situaties waarin (elektronische) informatie tussen organisaties wordt uitgewisseld, is dit aspect niet onbelangrijk.

Kritische processen beveiligen

Bepaalde bedrijfsprocessen dragen grote risico’s in zich voor de organisatie zelf (bijvoorbeeld het primaire productieproces) of voor de omgeving (bijvoorbeeld de verkeersleiding van het vliegverkeer boven Nederland). Deze kritische processen stellen zulke hoge eisen aan de beveiliging dat men er niet zonder meer van uit mag gaan dat de maatregelen van de baseline-beveiliging alle risico’s voor deze processen voldoende reduceren. Het is daarom nodig om de risico’s voor alle kritische processen in de organisatie grondig te analyseren door middel van (kwalitatieve) risicoanalyse. De in Nederland meest gebruikte methode hiervoor is de *Afhankelijkheids- & Kwetsbaarheidsanalyse*, oftewel *A&K-analyse* (ACIB, 1995).

Een andere veel gebruikte methode is *CCTA Risk Analysis and Management Method*, oftewel *CRAMM* (Insight, 1996). Beide methoden voldoen, maar vergen wel een aanzienlijke inspanning. Vandaar dat er ondersteunende hulpmiddelen ontworpen zijn, maar de ultieme hulpmiddelen zitten daar nog niet bij. Vooralsnog blijft het nodig om specialisten in te zetten voor het doen van risicoanalyses.

Voor elk kritisch proces dient een risicoanalyse uitgevoerd te worden. Daarin wordt met name ook gekeken naar de informatiesystemen die in het betreffende proces gebruikt worden en de informatiestromen naar andere systemen en/of partijen. Elke risicoanalyse resulteert in een lijst met benodigde maatregelen. Deze lijst wordt vergeleken met de maatregelen die al voor de baseline-beveiliging ingevoerd zijn. De maatregelen die nog niet gerealiseerd zijn, moeten alsnog ingevoerd worden. Het is zinvol om de additionele maatregelen voor de verschillende kritische processen op elkaar af te stemmen.

Wanneer meer dan circa tien kritische processen onderkend zijn, dan is het zinvol om hierin categorieën te onderscheiden. Voor een grote overheidsorganisatie zoals het Ministerie van Verkeer en Waterstaat kan bijvoorbeeld onderscheid gemaakt worden tussen maatschappelijk vitale processen (bijvoorbeeld de besturing van de stormvloedkering) en interne kritische processen (bijvoorbeeld de financiële administratie). Hierdoor valt het tweede spoor, kritische processen beveiligen, in feite uiteen in een aantal subsporen met verschillende prioriteiten.

Randvoorwaarden

De tweesporenaanpak heeft alleen kans van slagen als aan enkele randvoorwaarden wordt voldaan. Ten eerste dienen de verantwoordelijkheden ten aanzien van informatiebeveiliging in de organisatie belegd te zijn, en moet ook de motivatie aanwezig zijn om te werken aan de informatiebeveiliging. Hiervoor is onder meer nodig dat het management voldoende sturing aan informatiebeveiliging geeft en ook in zijn gedrag het goede voorbeeld geeft. Ten tweede dient informatiebeveiliging niet beperkt te blijven tot een eenmalige inspanning, maar moet het een doorlopend proces worden waarbinnen plaats is voor aanpassingen in de beveiligingsmaatregelen en onderhoud aan de beveiligingsmiddelen. Bovendien dient de werking van informatiebeveiliging getoetst te worden, onder meer door de inzet van audits.

Organisatie

De verantwoordelijkheden ten aanzien van informatiebeveiliging dienen in de organisatie belegd te zijn. Dit betekent in de eerste plaats dat de eindverantwoordelijkheid voor informatiebeveiliging ligt op de plaats waar deze ook moet liggen, namelijk bij de directie. De directie dient informatiebeveiliging te beschouwen als een onlosmakelijk onderdeel van de bedrijfsvoering, specifiek gericht op het beheersen van de risico's ten aanzien van de betrouwbaarheid van de informatievoorziening. En net als de andere onderdelen van de bedrijfsvoering heeft informatiebeveiliging regelmatig wat aandacht van de directie nodig.
Overigens wordt het leeuwendeel van de aansturing en uitvoering van informatiebeveiliging gedelegeerd naar anderen in de organisatie. Twee partijen spelen hierbij een hoofdrol, na-

melijk de eigenaren van de bedrijfsprocessen en de informatiebeveiligingsfunctionaris(sen). Als de informatiebeveiliging projectmatig op een hoger plan getild moet worden, dan kan er tijdelijk nog een derde hoofdrol nodig zijn, namelijk de projectorganisatie voor informatiebeveiliging (Glashouwer & Wielaard, 2002).

De eigenaren van de bedrijfsprocessen zijn ieder verantwoordelijk voor één of meer bedrijfsprocessen en de daarin gebruikte informatiesystemen. Iedere eigenaar moet er onder meer voor zorgen dat 'zijn' informatiesystemen (en de informatie daarin) goed beveiligd zijn. Dit omvat de verantwoordelijkheid voor de implementatie en de bewaking van alle maatregelen die nodig zijn voor beveiliging, maar ook het houden van toezicht op het gebruik van de betreffende systemen.

De informatiebeveiligingsfunctionaris(sen), ook wel aangeduid als security manager en security officer, vervullen een belangrijke rol in het coördineren en ondersteunen van beveiligingsactiviteiten (Goor, 2002; Overbeek & Roos Lindgreen, 2002). Hierbij valt onder meer te denken aan het uitvoeren van risicoanalyses, het installeren en onderhouden van beveiligingsapparatuur (bijvoorbeeld de firewall), het registreren van beveiligingsincidenten, en het overleggen met externe beveiligingspartijen.

Naast de juiste belegging van de verantwoordelijkheden voor informatiebeveiliging moet er ook voldoende motivatie voor informatiebeveiliging zijn (Spruit, 1998; Van Noord, 2001). Hiervoor is het bijvoorbeeld nodig dat de directie en het lijnmanagement het belang van informatiebeveiliging uitdragen. Bovendien dienen medewerkers die een zekere autoriteit bezitten, te worden overtuigd van de noodzaak van informatiebeveiliging, zodat ze naar hun collega's als 'ambassadeur' van informatiebeveiliging op kunnen treden.
Verder hebben de te nemen maatregelen voldoende draagvlak nodig. Dit betekent onder meer dat de maatregelen zo veel mogelijk geïntegreerd moeten worden in de beheer- en bedrijfsvoeringsprocessen binnen de organisatie. De maatregelen moeten bovendien zodanig ingericht worden dat de medewerkers zich in het kader van informatiebeveiliging niet heel anders moeten gaan gedragen dan ze gewend zijn. De inhoud en de reden van elke in te voeren maatregel moeten redelijk gevonden worden door de medewerkers die ermee in aanraking komen. De directie en lijnmanagers dienen zelf het goede voorbeeld te geven. Bovendien vergroot het draagvlak voor maatregelen als de medewerkers zelf participeren in het selecteren en invoeren van de maatregelen.

Borging en onderhoud

Het op peil brengen van informatiebeveiliging mag niet beschouwd worden als een eenmalige inspanning. Sterker nog: de voornaamste inspanning om een goede informatiebeveiliging te krijgen en te houden, wordt geleverd nadat de beveiligingsmaatregelen geïmplementeerd zijn. De aandacht en daarmee de motivatie voor informatiebeveiliging zal na verloop van tijd sterk teruglopen, temeer daar er juist door de betere beveiliging weinig tot geen ernstige beveiligingsincidenten meer zullen optreden. Toch zal het aantal optredende bedreigingen niet noemenswaard afnemen (Spruit & Looijen, 1995). Het is dus zaak om informatiebeveiliging

continu onder de aandacht te houden, door iedereen binnen de organisatie regelmatig te informeren over de bedreigingen die opgetreden zijn en hoe ze afgeslagen zijn. Een goede registratie van opgetreden bedreigingen en (bijna-)incidenten is daarvoor wel noodzakelijk, evenals goede communicatie hierover naar de medewerkers. Naast de aandacht voor informatiebeveiliging moet ook de motivatie hiervoor continu gevoed worden. Hiervoor is het nodig dat de directie en het lijnmanagement steeds het goede voorbeeld blijven geven en dat de ambassadeurs van informatiebeveiliging de inspanningen hiervoor ook niet moe worden.

Een ander belangrijk punt waar terdege rekening mee gehouden moet worden is het feit dat organisaties en hun omgeving voortdurend veranderen. Daarom moeten de verschillende aspecten van de bedrijfsvoering, waaronder de informatiebeveiliging, regelmatig geëvalueerd en zonodig aangepast worden. Voor elke aanpassing in de informatiebeveiliging moet weer voldoende draagvlak bestaan, waar de eerder genoemde redelijkheid en participatie door de medewerkers weer om de hoek komen kijken. Ook moeten de maatregelen zo veel mogelijk geïntegreerd worden in de andere processen. Bovendien is het belangrijk om erop te letten wie de noodzaak voor aanpassingen naar de medewerkers communiceert. Hier is weer een schone taak weggelegd voor de ambassadeurs van informatiebeveiliging.

En zelfs als de organisatie niet verandert, dan is er regelmatig onderhoud nodig aan de middelen die voor informatiebeveiliging ingezet worden. Hierbij valt onder meer te denken aan het toewijzen van accounts aan nieuwe medewerkers en het blokkeren van accounts van vertrekkende medewerkers, het actueel houden van antivirus-programmatuur en firewall-tabellen, het analyseren en archiveren van audit-logs, het legen van papierversnipperaars, et cetera. Daarnaast dient ook andere apparatuur en programmatuur zodanig onderhouden te worden dat ze niet kwetsbaarder wordt voor bedreigingen. Hieronder valt bijvoorbeeld het installeren van *patches* om gesignaleerde beveiligingslekken in programmatuur te dichten.

Ten slotte

In de praktijk wordt de verantwoordelijkheid voor informatiebeveiliging nog vaak belegd bij een specialistische groep. Gezien het voorgaande is dat niet verstandig; een aanpak waarbij het management het voortouw neemt, verdient de voorkeur. Het is overigens wel mogelijk om een specialistische groep in te zetten voor informatiebeveiliging, maar dan voor het uitvoeren van coördinerende en technische beveiligingstaken.
De directie en de proceseigenaren zijn verantwoordelijk voor het beheersen van de bedrijfsrisico's. Het gaat hierbij om risico's met betrekking tot de betrouwbaarheid van de informatievoorziening, maar ook risico's met betrekking tot andere aspecten van de bedrijfsvoering. Het beheersen van al deze risico's is gebaat bij een geïntegreerde aanpak. Temeer daar het dan mogelijk is om risico's met betrekking tot verschillende bedrijfsaspecten in onderlinge relatie te beschouwen en op basis daarvan prioriteiten te stellen. Het aanpakken van risico's in het kader van informatiebeveiliging dient dan ook hand in hand te gaan met het aanpakken van andere risico's voor de bedrijfsvoering. Onder de vlag van integraal management is een dergelijke geïntegreerde aanpak ook volstrekt normaal.

Noot: De auteurs willen hun dank uitspreken voor de inbreng van Boudien Glashouwer en Paul Wielaard.

Literatuur

ACIB, *Handboek Informatiebeveiliging Rijksdienst*, Ministerie van Binnenlandse Zaken, Den Haag (1995)

B. Glashouwer, M. de Graaf, J. Meij, P. Mettau & P. Wielaard, *Informatiebeveiliging voor de overheid; een praktische aanpak*, HEC, Den Haag (2002)

B. Glashouwer & P. Wielaard, 'Informatiebeveiliging bij de overheid: een veranderproces', *Informatiebeveiliging*, nr. 2, pag. (2002)

A.D. van Goor, 'Informatiebeveiliging: 'grenzeloos'', *Informatiebeveiliging*, nr. 5, pag. 18-21 (2002)

Insight, *Logic behind CRAMM's assessment of measures of risk and determination of appropriate countermeasures*, Insight, Walton-on-Thames (1996)

NNI, *Code voor Informatiebeveiliging*, Nederlands Normalisatie Instituut, Delft (2000)

F. van Noord, 'Beveiliging: gepland veranderen van gedrag', *Informatiebeveiliging*, nr. 4, pag. 20-23 (2001)

E. Oud, 'Code voor Informatiebeveiliging: een decennium aan ervaring', *Informatiebeveiliging*, nr. 7, pag. 24-26 (2002)

P. Overbeek & E. Roos Lindgreen, 'Informatiebeveiliging: wat mag u ervan verwachten?', *Management & Informatie*, nr. 1, pag. 50-56 (2002)

P. Overbeek, E. Roos Lindgreen & M. Spruit, *Informatiebeveiliging onder controle*, Pearson, Amsterdam (2000)

M. Spruit, 'De falende mens en informatiebeveiliging', *Informatiebeveiliging praktijkjournaal*, nr. 1, pag. 12-15 (1998)

M. Spruit & M. Looijen, 'Beveiliging van informatievoorziening', *Informatie*, nr. 5, pag. 328-336 (1995)