

## Vir-bi: interessant voorbeeld voor beveiliging informatie

Kees Louwerse  
Leo Valentijn  
Jaap van der Wel

*Informatiebeveiliging is een lastige en dure operatie en daarom niet voor iedereen weggelegd. De Code voor Informatiebeveiliging en het Voorschrift Informatiebeveiliging Rijksdienst (Vir) zouden hulp moeten bieden, maar beide stukken zijn tamelijk abstract en moeilijk toe te passen. Sinds het voorjaar echter bestaat het Vir-bijzondere informatie (Vir-bi): een voorbeeld van hoe het wel kan. De auteurs van dit artikel inventariseren de resultaten.*

Alleen grote organisaties zijn in staat om specialisten vrij te maken om aan informatiebeveiliging te werken. Voor kleinere organisaties is informatiebeveiliging niet minder belangrijk maar daar is men vaak door gebrek aan kennis en mogelijkheden gedwongen tot amateurisme. Op menige basisschool is de beveiliging afhankelijk van een handige leerkracht of ouder. Bij afwezigheid daarvan kan een beetje hacker simpel bij de gegevens van het leerlingvolgsysteem. Ouders online

([www.ouders.nl](http://www.ouders.nl)) publiceerde daarvan op 17 september j.l. een leuk voorbeeld onder de titel "Een vechtpartijtje in de zandbak kan je tot het HBO blijven achtervolgen". Ook bij menige huisarts of streekziekenhuis zou de beveiliging wel beter mogen maar ontbreekt het aan kennis om uit te zoeken hoe. Waar management en medewerkers van kleinere organisaties zich de risico's realiseren, hoedt men zich ervoor om te afhankelijk te worden van ICT. Geen voordeel voor de economische ontwikkeling van ons land.

De oorzaak ligt deels bij de opzet van de Code voor Informatiebeveiliging en het Voorschrift Informatiebeveiliging Rijksdienst. Beide stukken zijn geschikt voor iedere situatie maar daardoor ook abstract.

Concreet maken voor de eigen organisatie blijkt in de praktijk een behoorlijk karwei waarvoor alleen de grotere organisaties de benodigde middelen kunnen vrijmaken. En dan nog verzanden ook die vaak in te diepgravende risicoanalyses waarna het geld op is om de aangetroffen risico's te bestrijden. Dit is ook de oorzaak van de problemen met de invoering van het Voorschrift Informatiebeveiliging Rijksdienst (Vir). Dit voorjaar nog meldde deze krant dat de Algemene Rekenkamer de problemen met de invoering zelfs uitzonderlijk vond.

### Voorbeeld

Dit alles maakt het extra interessant dat er dit voorjaar in het publieke domein een voorbeeld is gepubliceerd dat concreet maakt hoe je aan beveiliging vorm kunt

geven: het Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie of kortweg: Vir-bi.



Met dank aan de Automatisering Gids

Het Vir-bi vervangt een uit 1989 stammend voorschrift voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst. Het Vir-bi beperkt zich dan ook tot de exclusiviteitsbescherming en laat de andere aspecten van informatiebeveiliging, integriteit en beschikbaarheid, voor wat het is. Deze beperkte invalshoek doet echter niets af aan het belang van dit voorschrift als voor-beeldaanpak voor andere sectoren. Het voorbeeld kan namelijk gemakkelijk worden verbreed naar de integriteits- en beschikbaarheidsaspecten van informatiebeveiliging.

Het Vir-bi vat informatie op als kennis die in welke vorm dan ook uitgewisseld kan worden. Ook 'materiaal' waarin deze kennis is opgeslagen, zoals bijvoorbeeld een document of communicatieapparatuur, wordt aangemerkt als informatie. Om te komen tot beveiligingsmaatregelen voor informatie, beschrijft het Vir-bi een voor de hand liggend procédé:

- 1) Classificeer de schade die het gevolg kan zijn van een beveiligingsprobleem.
- 2) Leid de rubricering van de informatie hieruit af.
- 3) Leid de beveiligingsmaatregelen af uit deze rubricering.

De voorbeelden uit de bijlagen van het Vir-bi illustreren deze aanpak en het zijn die voorbeelden die het Vir-bi interessant maken. Zo zijn er schadecategorieën beschreven zoals 'Schade voor de Nederlandse Staat' of 'Ongerechtvaardigde verrijking of voordeel voor natuurlijke personen of bedrijven' waarmee veel departementen goed uit de voeten kunnen. Aan die schadecategorieën worden vier rubriceringen verbonden variërend van 'Staatsgeheim - Zeer Geheim' aan de ene kant tot 'Departementaal Vertrouwelijk' aan de andere kant. Aan die rubriceringen zijn vergaand uitgewerkte voorbeeldlijsten van concrete beveiligingsmaatregelen verbonden zoals een gebod om in een aantal gevallen informatiedragers niet alleen te wissen maar ook te vernietigen en om alle gegevensopslag en -communicatie te versleutelen.

Het geheel wordt gecompleteerd met een goedkeuringsprocedure voor ICT-beveili-

gingsproducten die het ministerie van Binnenlandse Zaken uitvoert. Dit is een uitwerking van het 'autorisatieproces voor IT-voorzieningen' uit de Code voor Informatiebeveiliging voor wat betreft de beschermende werking van die beveiligingsproducten.

Al met al wordt zo de implementatie van een werkende informatiebeveiliging gemakkelijker gemaakt. De secretarissen-generaal van ministeries kunnen de voorbeelden zo overnemen en als regelgeving verplicht stellen voor de eigen organisatie, hooguit is wellicht enige modificatie nodig. Bovendien hoeven ze zelf geen uiterst gespecialiseerd personeel aan te trekken om de beveiligingskracht van hardware- of software te beoordelen.

De concretiseringsaanpak van het Vir-bi werkt doordat de beveiligingsproblemen binnen de departementale overheid min of meer vergelijkbaar zijn (kader Inspectie voor de Gezondheidszorg). De aanpak heeft ook een keerzijde: het toepassingsgebied versmalt. Sectoren buiten de departementale overheid zullen de concrete voorbeelden niet of alleen na een vertaalslag kunnen overnemen. Zo is ook in de zorgsector geheimhouden van informatie belangrijk maar bij huisartsen zal men niet snel de netwerkbeheerder van het Vir-bi aantreffen die 'toezicht houdt op de netwerkstatus om ongecontroleerd gebruik te detecteren' en in de ziekenhuizen zal men niet snel het bewakingspersoneel de rondes zien lopen die het Vir-bi voorstelt.

Voor sectoren met veel zelfstandige organisaties - bijvoorbeeld onderwijs of zorg - is de aanpak van het Vir-bi een interessant voorbeeld. Met een vergelijkbare aanpak kunnen brancheorganisaties veel toegevoegde waarde voor hun sector genereren. Zolang dat niet gebeurt moeten kleine organisaties zich blijven behelpen met de zeer generieke voorschriften zoals die van Code voor Informatiebeveiliging. Uiteindelijk levert dat leuke systemen op of, erger nog, geen systemen.

## De Inspectie voor de Gezondheidszorg

De informatie die door de Inspectie voor de Gezondheidszorg (de IGZ) wordt verzameld, is soms zeer vertrouwelijk. Dan gaat

het om concurrentiegevoelige informatie (productie van medicijnen) of opsporingsinformatie (tuchtzaken). Maar ook om per-

soonsgevoelige informatie over gedwongen opnames van patiënten in de psychiatrie. Geregeld haalt de IGZ de kranten over tekortschietende zorg of dreigende misstanden. Beveiliging van de informatie in welk stadium van verwerking dan ook is noodzaak. Soms spelen politieke risico's mee en worden adviezen speelbal van politieke opinievorming. De IGZ is daarin niet de enige rijksdienst met dit profiel. Zo werken ook de Voedsel en Waren Autoriteit of Algemene Inspectiedienst (AID) met gevoelige informatie voor belanghebbenden.

De IGZ werkt vanuit zeven regiolocaties en met ongeveer 150 inspecteurs. Voor de kantoorautomatisering en gegevensverwerking maakt de IGZ gebruik van een systeem gebaseerd op serverbased computing onder Citrix. Consequentie daarvan is dat het dataverkeer van de regiolocaties via een centrale serverfarm in Den Haag verloopt.

Buiten de kantoren is de Citrixfarm via Internet benaderbaar met een token, een nummegeratorpje dat synchroniseert met de servers en toegang verleent als ook een wachtwoord en een pincode zijn ingevoerd. Als de gebruiker wordt herkend, dan kan het netwerk worden gebruikt.

Voor het kantoorgebruik is geen token te nodig. Het lokale - en het wide area network transporteren namelijk gegevens beveiligd vanuit Den Haag naar de gebruikers en vice versa.

Omdat de IGZ de infrastructuur door derden laat beheren - KPN en facilitaire dienst van VWS - zijn daar de beveiligingsmaatregelen getroffen. De IGZ moet op grond van het Voorschrift Informatiebeveiliging Rijksdienst (VIR), zich er wel van verzekeren dat passende beveiligingsmaatregelen zijn genomen.

Voor staatsgeheime of departementaalgeheime informatie maakt het VIR-BI concreet wat onder passende maatregelen wordt verstaan. Departementaalgeheime informatie is de informatie waarvan kennisname door niet gerechtigden nadelig kan zijn voor het belang van één of meer ministeries. En dat is bij veel rijksdiensten waarschijnlijk al vlot van toepassing, zeker bij inspecties. Daar gaat het namelijk nogal eens om bijvoorbeeld informatie over vertrouwelijke onderzoeken waaronder opsporingsonderzoeken.

De vaste maatregellijsten die het Vir-bi suggereert, hebben als voordeel dat de risicoanalyse- en ontwerptrajecten van het VIR niet of beperkt meer nodig zijn. Het ligt voor departementen namelijk voor de hand om de maatregellijsten die het Vir-bi suggereert maar over te nemen.

Voorbeelden: Routing van printers moet geborgd zijn, Sleutelbeheer moet worden geadministreerd. Sterkte van opbergmiddelen moet in overeenstemming zijn met de aard. Voor uitvoering van reparaties door externen moet door de beveiligingsambtenaar (BVA) procedures worden opgesteld. Verwisselbare gegevensdragers moeten worden voorzien van de hoogste rubricering van de erop voorkomende gegevens. Dit laatste voorbeeld laat zien dat de maatregelsets niet alle vragen oplossen. Moeten bijvoorbeeld ook de hot-swappable (=verwisselbaar) harde schijven uit servers worden voorzien van de hoogste rubricering van de erop voorkomende gegevens? Hoe moet het dan met de Citrixfarms van de IGZ waar alle gegevens door elkaar staan? Moeten er nu aparte schijven voor departementaal-geheime informatie worden ingericht?

Systeemontwikkeling en -beheer is ook aan explicietere spelregels gebonden. Zaken als wachtwoordgebruik, schermbeveiliging, autorisatie moeten aangescherpt. Functiebeschrijvingen van iedereen die met gerubriceerde informatie in aanraking kan komen moet worden aangepast. En alles moet kunnen worden getoetst door BVA of Algemene Inlichtingen en Veiligheidsdienst (AIVD).

Concluderend zijn de maatregelen in het Vir-bi stuk voor stuk begrijpelijk en acceptabel. Wat echter niet uit het Vir-bi blijkt, is hoe je de weging moet uitvoeren als je alles in samenhang bekijkt. Hebben we meer nodig dan het nu al zeer restrictieve toegangsbeleid tot de rekencentra? Moeten we daarnaast ook nog alle file-servers met staatsgeheime gegevens apart gaan zetten? Evenals de backupservers? Al het personeel screenen dat met beheer en onderhoud te maken heeft? Inclusief de leden van externe organisaties? Onze systeemontwikkelaars "heropvoeden" in de trant van het Vir-bi? Kostbaar al met al. Voordat de IGZ hiertoe overgaat, moeten eerst de risico's goed in kaart worden gebracht om tot een afweging te komen of het nou echt wel zo redelijk is om de investeringen te doen die het Vir-bi adviseert.

Voor implementatie van het Vir-bi heeft de overheid vier jaar de tijd. Tijd genoeg dus om te zien of we toekunnen met een lichter regime. In de tussentijd kan de marktwerking voor de tools die we nodig hebben, bijvoorbeeld encryptie van alle gegevens, ook zijn werk doen en zijn we straks minder duur uit.

Als systeem om alles te wegen en de maatregelen er bij te zoeken, is het Vir-bi mak-

kelijker en sneller dan het VIR. De verleiding is dus groot om de maatregelsets van Vir-bi te pakken en in ieder geval die voor het laagste beveiligingsniveau te nemen. Voor de zekerheid. Maar zelfs deze aanpak kan al leiden tot hoge kosten. Bezint eer ge begint, gebruik de komende vier jaar die het Vir-bi toelaat voor een inhaalslag, goed.

## Norm voor Informatiebeveiliging in de Zorg

Dat zorgverleners zorgvuldig om moeten gaan met de informatie die ze van en over hun patiënten te weten komen, is geen nieuws: de eed van Hippocrates is daar al zeer duidelijk over. Het ministerie van VWS bereidt wetgeving voor over het gebruik van een identificatienummer in de zorg. Doel van dit nummer is het ondersteunen van een betrouwbare en doelmatige (elektronische) uitwisseling van gegevens over de zorgcliënt. Daarbij is van belang dat de gegevensuitwisseling goed en veilig functioneert. Dat geldt ook voor opslag en toegang tot gegevens.

Het ministerie van VWS heeft na gereedkomen van de Norm voor Informatiebeveiliging in de zorg (NEN7510) het Nederlands Normalisatie Instituut (NEN) de opdracht gegeven om toetsbare voorschriften uit te werken waarmee zorginstellingen in staat zijn om zelf hun informatiebeveiliging te implementeren.

Het Nederlands Normalisatie-instituut, NEN, heeft recentelijk de Norm voor Informatiebeveiliging in de Zorg (NEN 7510) gepubliceerd. De opzet van deze norm is, om aan de zorgverleners ondersteuning te bieden bij het implementeren van informatiebeveiliging in de praktijk. De norm is direct afgeleid van de bekende Code voor Informatiebeveiliging, maar is specifiek gericht op de gezondheidszorg. In een set bijbehorende handreikingen is veel praktische informatie opgenomen. Deze handreikingen zijn toegesneden op de verschillende soorten organisaties die in de zorg een rol spelen (er is bijvoorbeeld een set voor de alleen werkende huisarts, en een voor de groepspraktijk, maar ook een voor de grote organisaties als de ziekenhuizen).

Ondanks deze handreikingen zal de norm nog door veel zorginstanties als veel te abstract worden ervaren. NEN en de normcommissie 'Informatiebeveiliging in de zorg' proberen dan ook om de concretiseringslag voor het zorgveld zo groot mogelijk te maken, en roepen daarbij de hulp in van de beroepsorganisaties die dit veld vertegenwoordigen. Gezien het verplichtende karakter dat VWS wil hanteren, worden de handreikingen bij de norm voor de verschillende beroepsgroepen in de zorg voorzien van een voorschrijvend karakter. Dit proces verloopt in nauw overleg met die beroepsgroepen, zodat er een zelfregulerend mechanisme optreedt. Beoogd wordt daarnaast een toetsingsmechanisme op te starten, waarbij de Inspectie voor de Gezondheidszorg de beroepsgroepen zal toetsen op de regels die ze zelf hebben opgesteld.

De normcommissie denkt dat certificering op dit gebied uiteindelijk een mooie aanvulling zou kunnen zijn op de marktwerking die op dit moment zijn intrede doet in de zorgsector. Met bijvoorbeeld een certificaat van de Inspectie kan de zorgorganisatie aantonen dat patiëntgegevens bij hen in goede handen zijn. Een mooi predikaat voor het immer nastreven van het bieden van het gewenste niveau van dienstverlening aan de patiënt.

Jaap van der Wel is directeur van Comfort-IA ([jvdwel@comfort-ia.nl](mailto:jvdwel@comfort-ia.nl)). Kees Louwerse is voorzitter van de NEN Normcommissie Informatiebeveiliging in de zorg ([c.p.louwerse@lumc.nl](mailto:c.p.louwerse@lumc.nl)). Leo Valentijn (op persoonlijke titel) is senior-adviseur ICT bij de Inspectie voor de Gezondheidszorg ([lq.valentijn@iqz.nl](mailto:lq.valentijn@iqz.nl)). Met dank aan Eline Loomans, M.Sc, Standardization consultant NEN-Health Care