VIR en Code: een paar apart?

Dr. E.E.O. Roos Lindgreen RE, J.C. van Praat RE RA en dr. ir. P.L. Overbeek

Het VIR en de Code zijn beide – steeds sterker – de-factostandaarden op het gebied van informatiebeveiliging. Twee standaarden op één terrein impliceert echter conflict of diversiteit. Het nut van beide wordt aangegeven, mede aan de hand van certificering als toepassing.

Inleiding

Het vakgebied informatiebeveiliging staat de laatste jaren volop in de belangstelling. Elk jaar lijken er meer conferenties, seminars en vaktijdschriften aan het onderwerp te worden gewijd. Daarnaast is informatiebeveiliging een vast agendapunt op menige directievergadering geworden.

Al deze aandacht roept de vraag op of het met al die informatiebeveiliging inmiddels niet een beetje te veel van het goede is. De wens om betrouwbare informatie uit te wisselen dan wel geheimen te bewaren is immers al zo oud als de mensheid zelf. In sectoren als defensie, research en financiële dienstverlening maakt de beveiliging van informatie en informatiesystemen sinds jaar en dag deel uit van het primaire proces. Is er eigenlijk wel iets nieuws onder de zon?

Het antwoord op deze vraag luidt natuurlijk: ja, er is voortdurend veel nieuws onder de zon. Het huidige vakgebied richt zich immers op 'fast-moving targets': informatiesystemen en IT-infrastructuren die zich al jaren in een steeds hoger tempo ontwikkelen en inmiddels tot in de haarvaten van onze organisaties zijn doorgedrongen. Het vakgebied informatiebeveiliging holt noodgedwongen voortdurend achter die ontwikkelingen aan. Beveiligingsspecialisten weten er wonder boven wonder steeds voor te zorgen dat de afstand niet te groot wordt.

Beleid of baselines?

Twintig jaar geleden. Informatiebeveiliging heet nog computerbeveiliging. Het vakgebied leidt een sluimerend bestaan. Afgezien van een enkele wetenschapper, een paar accountants, een handvol verlichte managers en een iets groter aantal automatiseerders lijken maar weinigen zich werkelijk bewust te zijn van de kwetsbaarheid van de informatiesystemen van dat moment. En wie het probleem durft aan te roeren, mag als brenger van het slechte nieuws zelden op een warm onthaal rekenen. De PC-golf maakt het er in eerste instantie niet beter op. De pas verworven vrijheid van de ontketende eindgebruiker, die vóór het PC-tijdperk was aangewezen op de diensten van het rekencentrum, mag immers niet in gevaar worden gebracht door zoiets negatiefs als computerbeveiliging.

Kortom, beveiliging is nauwelijks in beeld. Tot Nederland midden jaren tachtig wordt opgeschrikt door een aantal spraakmakende beveiligingsincidenten. De eerste computervirussen steken de kop op. Studenten breken in op de systemen van enkele gerenommeerde organisaties. Morris' worm legt grote delen van het juist in opkomst zijnde Internet plat. Hackers verzamelen zich en organiseren spraakmakende conferenties waar op zich weinig nieuws verteld wordt, maar die zich wel in een enorme aandacht van de media mogen verheugen.

Al snel groeit bij managers binnen en buiten de overheid het besef dat de beveiliging van informatie en informatiesystemen niet langer kan worden uitgesteld tot de noodzaak zich voordoet. De snelle ontwikkeling van informatietechnologie (IT) en de toepassingen daarvan maken een structurele en proactieve aanpak noodzakelijk.

Dit besef leidt tot tal van initiatieven op strategisch en tactisch niveau, die in twee categorieën kunnen worden onderverdeeld. De eerste categorie bestaat uit beleid, richtlijnen, directieven, voorschriften en memoranda op een relatief hoog abstractieniveau, waarin vooral meer aandacht voor de beveiligingsproblematiek wordt gevraagd. De tweede categorie bestaat uit checklists en baselines met concrete maatregelen die binnen een organisatie of binnen een informatiesysteem kunnen worden ingevoerd.

Beleid ...

Een voorbeeld uit de eerste categorie is het 'Memorandum omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking in het bankwezen', in 1988 gepubliceerd door De Nederlandsche Bank, na uitvoerig overleg met vele partijen in de markt. Geparafraseerd stelt het Memorandum dat de betrouwbaarheid en continuïteit van informatiesystemen voor het bankwezen van essentieel belang zijn, dat kredietinstellingen al het nodige in het werk moeten stellen om deze kwaliteitsaspecten te waarborgen, en dat toezicht zal worden uitgeoefend door De Nederlandsche Bank. Het Memorandum wordt zeer positief ontvangen en geldt tien jaar na dato nog steeds als bindend voorschrift.

De overheid publiceert in 1994 het besluit Voorschrift Informatiebeveiliging Rijksdienst. Het VIR maakt in beveiligingsland nogal wat tongen los. Dat de overheid zo doortastend het voortouw neemt bij het aanpakken van de beveiligingsproblematiek doet veel managers even schrikken. Hetzelfde geldt voor de inhoud en kwaliteit van het boekje zelf. In een beperkt aantal pagina's wordt helder uiteengezet hoe de departementen het beveiligingsvraagstuk ter hand zouden moeten nemen. De impliciete boodschap daarbij is luid en duidelijk: wij vertellen u niet wat u moet doen; u moet er zelf over

nadenken! Wel reiken de samenstellers van het VIR de lezer daarbij enkele praktische instrumenten ter ondersteuning van dit denkproces aan: de afhankelijkheidsanalyse, waarbij wordt onderzocht in hoeverre de organisatie afhankelijk is van informatie en informatiesystemen, en de kwetsbaarheidsanalyse, waarbij wordt onderzocht in hoeverre deze systemen – en daarmee ook de processen – beschermd zijn tegen bedreigingen. Het VIR markeert het begin van een groot aantal beveiligingsprojecten bij de Rijksoverheid én daarbuiten, waarover elders in dit boek meer te lezen is.

... of baselines?

Naast de ontwikkeling van de noodzakelijkerwijs relatief abstracte richtlijnen in overheidskringen ontstaat in het bedrijfsleven een andere trend, die voortkomt uit een sterke behoefte aan praktische standaarden: de ontwikkeling van security baselines. Een aanzet hiertoe is in 1988 al gegeven door het Nederlands Instituut voor Registeraccountants in de vorm van NIVRA-geschrift 43, getiteld *Automatisering en controle*: een praktische lijst algemene en specifieke 'organisatorische maatregelen en controletechnieken die kunnen worden toegepast bij de automatisering van de informatieverzorging'. In 1989 verschijnt NIVRA-geschrift 53, getiteld *Kwaliteitsoordelen over informatievoorziening*, waarin onder andere wordt ingegaan op de criteria die worden aangelegd bij het vormen van een kwaliteitsoordeel.

Iets later ontwikkelt het Stanford Research Institute (SRI) een nog meer op de praktijk ingestelde baseline, die via het International Information Integrity Institute (I4) wordt verspreid onder grote bedrijven en instellingen over de hele wereld. Kort daarop neemt Shell in Engeland het initiatief en schrijft samen met een aantal andere ondernemingen de Code of Practice for Information Security Management, ofwel de Code. De Code waait over naar Nederland, waar hij door het Nederlands Normalisatie Instituut onder auspiciën van het Ministerie van Economische Zaken wordt uitgebracht als de 'Code voor Informatiebeveiliging'. Kort daarop wordt de Code in Engeland tot officiële standaard geslagen; British Standard 7799 is een feit.

De Code nu

De Code was en is tamelijk revolutionair. Het is een 'best practice'-document, waarin de beste beveiligingsmaatregelen van een groot aantal grote organisaties zijn beschreven. De Code definieert de volgende tien categorieën van beveiligingsmaatregelen die door de samenstellers noodzakelijk worden geacht om te voldoen aan het principe van minimumzorgplicht:

1 Beleid;
2 Organisatie;
3 Classificatie en beheer;
4 Personeel;
5 Fysieke beveiliging;
6 Computer- en netwerkbeheer;
7 Toegangsbeveiliging voor systemen;
8 Ontwikkeling en onderhoud van systemen;
9 Continuïteitsplanning;
10 Toezicht.

De maatregelen in de Code voor Informatiebeveiliging vertonen nauwe raakvlakken met andere beveiligingsdisciplines, zoals de beveiliging van gebouwen en terreinen, maatregelen in de personele sfeer en EDP-audit.

De structuur van de Code is niet altijd even logisch, en sommige hoofdstukken overlappen elkaar behoorlijk, maar deze bezwaren zijn zeker niet onoverkomelijk. In de praktijk blijkt de Code een zeer bruikbaar instrument voor het uitvoeren van beveiligingstrajecten te zijn. De toenemende acceptatie van de Code in de markt is daarbij een belangrijke succesfactor.

Inmiddels wordt de laatste hand gelegd aan een nieuwe versie van BS 7799, die meer toegesneden zal zijn op de huidige IT-praktijk en die meer zal aansluiten bij normen en standaarden voor specifieke deelonderwerpen.

De Code vormt inmiddels de basis voor een aantal standaard-'methoden' voor het uitvoeren van beveiligingstrajecten, zoals het hieronder beschreven Corporate Information Security-programma.

Figuur 1. De fasering van het Corporate Information Security-programma.

Corporate Information Security

Het Corporate Information Security-programma bestaat uit de volgende acht deelstappen (zie figuur 1):

Fase 1 - Business risk analysis
In deze fase worden de bedrijfsprocessen en informatiesystemen binnen de organisatie geanalyseerd, alsmede de hieraan verbonden zijnde afhankelijkheden en kwetsbaarheden. Hiertoe worden gesprekken gevoerd met vertegenwoordigers van verschillende organisatieonderdelen en wordt gebruikgemaakt van bestaande procesbeschrijvingen. De resultaten van deze fase worden samengevat in een beknopte notitie.

Fase 2 - Policy formulation
In deze fase wordt een informatiebeveiligingsbeleid opgesteld, waarin het gewenste niveau van informatiebeveiliging wordt beschreven. Het beveiligingsbeleid bevat naast een heldere formulering van de strategie en architectuur inzake informatiebeveiliging ook een beschrijving van de organisatorische en technische beveiligingsmaatregelen die door de organisatie als minimaal noodzakelijk worden beschouwd. Deze 'baseline' is afge-

leid van de Code voor Informatiebeveiliging en wordt afgestemd op de specifiek wenselijk geachte situatie. Het beleid wordt in een aantal workshops met vertegenwoordigers van de diverse organisatieonderdelen afgestemd. Deze fase resulteert in een beknopt beveiligingsbeleid, dat voor akkoord aan de leiding van de organisatie wordt voorgelegd. De fase wordt afgesloten met een go/no go-moment, waarbij wordt besloten over de voortgang van het project.

Fase 3 - Assessment
In deze fase wordt op basis van interviews met vertegenwoordigers van de verschillende organisatieonderdelen onderzocht in hoeverre het huidige stelsel van maatregelen voldoet aan het in de vorige fase geformuleerde baselineniveau. De resultaten worden centraal verwerkt en geconsolideerd en worden in een beknopte presentatie weergegeven. Essentieel is dat deze presentatie de stand van zaken in één oogopslag inzichtelijk kan maken. Het grote aantal relevante beveiligingsmaatregelen kan er snel toe leiden dat de betrokken managers, die vaak niet de tijd hebben zich intensief in de materie te verdiepen, door de bomen het bos niet meer zien. Een vereenvoudigde grafische weergave van de ist-situatie in de vorm van een stoplichtendiagram of een spinnenweb kan wonderen doen, maar moet altijd met het nodige voorbehoud worden gepresenteerd.

Fase 4 - Intermediate evaluation
In deze fase worden de resultaten van het assessment geëvalueerd en besproken met het hoogste management. Een moment van reflectie en discussie is noodzakelijk om de resultaten van het assessment tot alle betrokkenen door te laten dringen en consensus te verkrijgen over de implicaties ervan.

Fase 5 - Information security plan
In deze fase wordt een beveiligingsplan opgesteld, waarin wordt beschreven op welke wijze eventuele achterstallige beveiligingsmaatregelen kunnen worden ontwikkeld en geïmplementeerd. Het beveiligingsplan omvat ten minste een beschrijving van de te verrichten werkzaamheden, doorlooptijden en benodigde capaciteit, alsmede van het managementkader dat nodig is om het beveiligingsbeleid gestalte te kunnen geven. Doel van het beveiligingsplan is het bieden van heldere uitgangspunten voor de realisatie van het informatiebeveiligingsbeleid door de verschillende organisatieonderdelen.

Bij het opstellen van het plan kan onderscheid worden gemaakt tussen maatregelen die zonder overmatige inspanning binnen relatief korte tijd getroffen kunnen worden (de 'quick wins') en maatregelen die aanzienlijk meer tijd zullen vergen (de zogenaamde 'slow gains'). Door dit onderscheid te maken en de quick wins als eerste aan te pakken, kunnen snel zichtbare resultaten worden bereikt.

Daarnaast dient te worden aangegeven welke maatregelen een hoge prioriteit hebben en welke maatregelen minder urgent zijn. Het kan voorkomen dat de resultaten van het assessment aanleiding geven tot het initiëren van 'crash actions', maatregelen die onmiddellijk dienen te worden gerealiseerd omdat de organisatie is blootgesteld aan onaanvaardbare risico's.

Als blijkt dat de beveiligingsachterstand zo groot is dat de invoering van achterstallige maatregelen de beschikbare tijd, geld en mankracht te boven gaat, kan gekozen worden voor een evolutionair ontwikkelingsmodel. Hierbij wordt een meerjarenplan opgesteld, waarbij niet alle maatregelen in één keer worden gerealiseerd, maar stapsgewijs wordt toegewerkt naar de uiteindelijke situatie. Hierbij wordt gebruikgemaakt van plateaus. Een plateau is daarbij gedefinieerd als een stabiele situatie die zichzelf in de praktijk bewezen heeft. De overgang naar een volgend plateau wordt pas in gang gezet als het huidige plateau naar tevredenheid functioneert. Hiervoor is recent een variant van het Capability Maturity Model (CMM) ontwikkeld, waarbij vier fasen van volwassenheid worden onderscheiden, analoog aan het bekende groeimodel van Nolan. Het Capability Maturity Model houdt rekening met het feit dat informatiebeveiliging in veel organisaties een gestage ontwikkeling doormaakt, waarbij een volgende groeifase pas kan aanvangen als de voorgaande groeifasen achter de rug zijn.

Fase 6 - Development
In deze fase worden de organisatorische en technische maatregelen die in fase 4 als achterstallig zijn aangemerkt, ontwikkeld op basis van het in fase 5 opgestelde beveiligingsplan.

De ontwikkeling van *organisatorische maatregelen* bestaat uit het definiëren van procedures en richtlijnen, die kunnen worden vastgelegd in een Handboek Informatiebeveiliging, maar evengoed kunnen worden opgenomen in een bestaand Handboek Administratieve Organisatie. Daarnaast is het toewijzen van verantwoordelijkheden een essentiële stap in deze fase. Ten slotte moet aandacht worden besteed aan het opstellen van 'security agreements': afspraken over informatiebeveiliging met derden, zoals toeleveranciers, IT service providers, afnemers en andere zakenpartners.

De ontwikkeling van *technische maatregelen* bestaat veelal uit de ontwikkeling of de selectie en aanschaf van specifieke beveiligingsproducten voor bijvoorbeeld logische toegangsbeveiliging, noodstroomvoorzieningen, netwerkbeveiliging of encryptie. Hierbij moet rekening worden gehouden met het feit dat de onderhoudskosten en beheerkosten van zulke producten de aanschafkosten in de regel flink te boven gaan; de totale eigendomskosten vallen hierdoor vele malen hoger uit.

Het te ontwikkelen stelsel van maatregelen dient toekomstvast te zijn en zichzelf zoveel mogelijk in stand te kunnen houden. Merk op dat de benodigde capaciteit voor deze fase pas kan worden vastgesteld na het opstellen van het beveiligingsplan.

Fase 7 - Implementation
In deze fase worden de ontwikkelde maatregelen formeel geaccepteerd en binnen de organisatie geïmplementeerd conform het in fase 5 ontwikkelde beveiligingsplan. De implementatie omvat onder meer training en opleiding van gebruikers en beheerders alsmede een breed awarenessprogramma. Essentieel in deze fase is dat de beveiligingsboodschap wordt overgebracht aan alle managers en medewerkers die niet betrokken zijn geweest bij de voorgaande fasen. Daarom wordt in deze fase altijd

nauw samengewerkt met de organisatorische eenheid die verantwoordelijk is voor de interne bedrijfscommunicatie, zodat een gericht communicatieprogramma kan worden uitgevoerd. Daarbij wordt in toenemende mate gebruikgemaakt van intranetoplossingen, die inmiddels binnen de meeste organisaties een essentiële rol in de bedrijfscommunicatie spelen.

Fase 8 - Evaluation and certification
In deze fase wordt het beveiligingstraject formeel afgerond, geëvalueerd en, indien gewenst, gecertificeerd tegen de Code voor Informatiebeveiliging.

Het Corporate Information Security-programma is in een aantal varianten door een groot aantal organisaties uitgevoerd. De belangrijkste conclusie die uit deze trajecten kan worden getrokken, is dat het programma een effectieve aanpak van de beveiligingsproblematiek mogelijk maakt. Door het gebruik van een standaardnormenset (de Code), de eenvoudige projectfasering, de eenduidigheid en de uniformiteit is het Corporate Information Security-programma voor het management herkenbaar. Bovendien wordt elke fase van het traject steeds afgesloten met een tastbaar bewijs van de effectiviteit van de geleverde inspanning.

Vergelijking

Wie het VIR en de Code met elkaar vergelijkt, ziet opmerkelijke verschillen:

Denken versus doen
Het VIR legt de nadruk op de eigen verantwoordelijkheid: een organisatie moet zelf nadenken over de risico's die men loopt en de maatregelen die men zou moeten treffen. De Code daarentegen is zeer praktisch opgezet en definieert een kleine honderd concrete maatregelen, waaronder het regelmatig uitvoeren van een risicoanalyse.

Abstract versus concreet
Het VIR is vrij abstract in termen van de maatregelen die getroffen moeten worden; het VIR biedt daardoor de vrijheid om maatregelen af te stemmen op de specifieke situatie, maar mist tegelijkertijd een directe aansluiting op de praktijk. De Code is veel concreter – al is de Code volgens sommigen nog lang niet concreet genoeg!

Maatwerk versus confectie
Het VIR bepleit het treffen van maatregelen die specifiek zijn afgestemd op de uitkomsten van een afhankelijkheids- en kwetsbaarheidsanalyse. De Code pretendeert geschikt te zijn voor alle organisaties en alle informatiesystemen.

Ook in de bereikte resultaten zijn verschillen zichtbaar. Beide benaderingen zijn met succes in de praktijk toegepast; andersom is het ook zo dat beide benaderingen wel eens met minder succes zijn uitgevoerd. Omdat concrete cijfers ontbreken, is het moeilijk een objectieve vergelijking te maken. Toch willen wij een poging wagen.

In het algemeen kan worden gesteld dat een aanpak op basis van het VIR weliswaar zeer effectief kan zijn, maar tegelijkertijd het risico in zich draagt pas in een laat stadium tot concrete maatregelen te leiden. Het uitvoeren van A-analyses en K-analyses vergt in de regel veel tijd en mankracht. Het te lang uitblijven van concrete resultaten kan managers een ongemakkelijk gevoel geven, waardoor het project het risico loopt te worden beëindigd nog voordat er resultaten geboekt zijn.

Een aanpak op basis van de Code leidt vrijwel altijd tot tastbare resultaten. Ook de Code draagt echter een risico in zich, namelijk dat het verantwoordelijke management onvoldoende tijd en energie aan de zo noodzakelijke risicoafweging besteedt. Door het simpelweg invoeren van maatregelen op basis van de Code ontstaat het gevoel dat alles vanzelf goed geregeld is. We zijn toch immers gecertificeerd? Dit gevoel is echter in de meeste gevallen onterecht. Het certificaat is allesbehalve een veiligheidsgarantie; het geeft aan dat de organisatie een minimumniveau aan maatregelen getroffen heeft, en biedt zo enige mate van zekerheid. Een certificaat sluit echter niet uit dat voor bepaalde omgevingen en systemen aanvullende maatregelen moeten worden getroffen. Welke omgevingen en systemen dat zijn, kan alleen aan de hand van een risicoafweging worden bepaald.

Twee worden één

En zo zijn we terug bij het VIR. Een voorschrift kan niet zonder concrete maatregelen, maar concrete maatregelen kunnen ook niet zonder risicoafweging. Een integratie van beide benaderingen – in de praktijk betekent dit: een vorm van integratie van het VIR en de Code – zou daarom van harte moeten worden toegejuicht en ligt zelfs zozeer voor de hand, dat zij als onvermijdelijk mag worden beschouwd. Het doel van zo'n integratie is niet het hermetisch dichttimmeren van de informatievoorziening, maar het verantwoord beheersen van de daarmee samenhangende risico's. De organisatie die in staat is op een snelle en effectieve wijze met de inherente kwetsbaarheden van IT om te gaan heeft daarbij een streepje voor. Leve het VIR, en leve de Code!