COMPACT

TIJDSCHRIFT EDP-AUDITING

INFORMATIE(BEVEILIGINGS)-BELEID

1998/5

KPMG EDP Auditors

Bezoekadres
Beneluxlaan 43
3526 KK Utrecht

Correspondentie-adres
Postbus 3222
3502 GE Utrecht

Telefoon (030)2810210
Telefax (030)2896714

KPMG Peat Marwick LLP
Victoria Street 685
Mr R. Koorn
CA 94127 San Francisco
USA

Utrecht, 16 november 1998

Onderwerp: **Compact 1998/5**

Geachte heer Koorn,

Het nummer van Compact, dat wij u hierbij toezenden, is geheel gewijd aan het onderwerp informatiebeveiliging. Een actueel onderwerp nu steeds meer organisaties zich realiseren dat informatiebeveiliging en informatiebeveiligingsbeleid een conditio sine qua non vormen om de kwaliteit van de geautomatiseerde informatieverzorging adequaat te kunnen beheersen. Immers, informatiebeveiligingsbeleid dient ten aanzien van beschikbaarheid/continuïteit, betrouwbaarheid en vertrouwelijkheid de kaders te scheppen waarbinnen informatiebeveiliging daadwerkelijk kan worden gerealiseerd.

In dit nummer van Compact (1998/5) gaan verschillende auteurs in op de onderhavige problematiek.
De auteurs Coumou en Schoemaker besteden uitgebreid aandacht aan de inhoud van het informatiebeveiligingsbeleid, waarna de heer Roos Lindgreen aandacht besteedt aan de maatregelen die vanuit het informatiebeveiligingsbeleid kunnen worden geformuleerd en vervolgens moeten worden geïmplementeerd. In het derde artikel, van de hand van de auteurs Buren, Van der Meer, Shahim, Barnhoorn en Roos Lindgreen, wordt een toelichting gegeven op een concreet hulpmiddel voor het verstekken van informatie over de kwaliteit van de informatiebeveiliging: de securometer, waarna tot slot de auteur Overbeek in het laatste artikel aandacht besteedt aan de certificatie van de informatiebeveiliging in organisaties.

Wij vertrouwen erop dat dit nummer van Compact u opnieuw uitnodigt tot een grondige bestudering van de problematiek. Wij zijn gaarne bereid de problematiek van informatiebeveiligingsbeleid en informatiebeveiliging met u te bespreken en/of toe te lichten.

Hoogachtend,

J.C. Boer

Bijlage: Compact 1998/5

xamco
JCB/jdh

Compact ®
Jaargang 25, nummer 5
Een uitgave van KPMG EDP Auditors NV en ten Hagen & Stam BV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
Drs. P.P.M.G.G. Brouwers RE RA
Ir. J.A.M. Donkers RE
W. de Korte RE RA
J.C. van Praat RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Mr. P. van Dijken
G. van Essen RA
Prof.mr. H. Franken
Dr. K.IJ. Mollema RA
Prof. H.B. Mooren RE RA
Prof.dr.ir. R. Paans RE
Bureauredactie
Drs. Q.C.H.J. Hünteler, ten Hagen & Stam, Postbus 34, 2501 AG Den Haag
Tel.: 070 – 304 57 74
Fax: 070 – 304 58 17
e-mail: q.hunteler@wkths.nl
Basisvormgeving
Bureau Karakter, Delft
Opmaak
AlphaZet bv, Waddinxveen
Abonnementen
f 165,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom BedrijfsInformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax: 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.
Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij de uitgeefassistent. Prijs per overdruk per artikel (inclusief omslag) f 5,-.

Uitgever
I.J. van Haren

Nederlands Uitgeversverbond
Groep vaktijdschriften

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals:
• beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG, KPMG EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij ten Hagen & Stam BV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij de uitgeef-assistent verkrijgbaar is.

Met het toenemende gebruik van de mogelijkheden van de informatie- en communicatietechnologie (ICT) in organisaties ontstaat tegelijkertijd behoefte aan een structurele en systematische aandacht voor het onderwerp informatiebeveiliging. Als organisaties aan de beveiliging van de informatievoorziening in de eigen organisatie onvoldoende aandacht besteden, dan is het risico aanwezig dat soms wezenlijke informatie over het eigen reilen en zeilen bij een veel grotere groep bekend wordt dan men eigenlijk zou willen. Ook de informatie-uitwisseling tussen organisaties is een punt van aandacht. Dit laatste blijkt uit een aantal recente problemen met betrekking tot de beveiliging rond het gebruik van Internet. Ook zijn in de publiciteit concrete voorbeelden genoemd rond het gebruik van een toonaangevend product als Windows/NT.

Vanwege het grote belang van de informatiebeveiliging wordt in dit nummer van Compact een aantal aspecten van dit fenomeen aan de orde gesteld. Het gaat hierbij om het beveiligingsbeleid, de invoering van een bedrijfsbrede informatiebeveiliging, het gebruik van hulpmiddelen om de informatiebeveiliging concrete inhoud te geven en ten slotte het proces dat gevolgd moet worden om door middel van certificatie een vertrouwensbasis te bieden voor de beveiliging van informatie.

Het eerste artikel besteedt uitgebreid aandacht aan de inhoud van het informatiebeveiligingsbeleid. De auteurs stellen dat een goede informatiebeveiliging begint met het formuleren van het beleid. Op deze stelling is weinig af te dingen. Als het topmanagement van een organisatie niet weet wat het wil, kan het van de werkvloer niet verwachten dat daar gestructureerd en systematisch aandacht wordt besteed aan de beveiligingsaspecten rond het dagelijks gebruik van de ICT. Daarom geven de auteurs in het artikel ook de nodige richtlijnen voor de zogenaamde 'probleemeigenaar'. Om tot een goed informatiebeveiligingsbeleid te komen is een procesmatige aanpak noodzakelijk. Deze aanpak wordt in het artikel uitgebreid beschreven. Ten slotte geven de auteurs aan dat informatiebeveiliging een continu en cyclisch proces is, waarbij de voortdurende veranderingen in de ICT ook de voortdurende aandacht van het management vragen voor het fenomeen informatiebeveiliging.

De maatregelen die vanuit het informatiebeveiligingsbeleid kunnen worden geformuleerd en vervolgens moeten worden geïmplementeerd, vormen de kern van het volgende artikel. Hoewel niet voorkomen kan worden dat ook in dit artikel even stil wordt gestaan bij het informatiebeveiligingsbeleid, wordt al snel het vizier gericht op het transformatieproces dat moet leiden tot een werkende beveiligingsorganisatie. Centraal hierin staat het Corporate Information Security-programma van KPMG EDP Auditors. Deze methodiek is tot nu toe al op verschillende plaatsen met succes toegepast. Opvallend in het artikel is ook de opmerking dat het beveiligingsbewustzijn steeds meer aandacht krijgt (ook van het management), doch dat de beschikbaarheid van goed opgeleide en ervaren mensen een steeds groter probleem gaat worden. Naar mijn mening verdient dit punt bijzondere aandacht.

In het derde artikel wordt een toelichting gegeven op een concreet hulpmiddel voor het verstrekken van informatie over de kwaliteit van de informatiebeveiliging: de Securometer®. Naast de toelichting op de werking van dit product is het belangrijk op te merken dat de inzet van dergelijke hulpmiddelen alleen verantwoord is wanneer zij gebruikt worden door deskundig personeel. De uitkomsten die het gebruik van de Securometer® oplevert, vormen een belangrijke bron van informatie voor het management dat, zoals aangegeven in het eerste artikel, deze informatie kan gebruiken voor het al of niet bijstellen van het informatiebeveiligingsbeleid.

Het laatste artikel besteedt de nodige aandacht aan de certificatie van de informatiebeveiliging in organisaties. Daartoe in staat gesteld door de nieuwste ontwikkelingen op het vlak van ICT wisselen organisaties steeds meer informatie uit. Organisaties worden steeds afhankelijker van elkaar en hebben belang bij een goede beveiliging van de informatiestromen, niet alleen in het openbare verkeer, maar ook binnen organisaties zelf. Als organisaties gecertificeerd zijn, ontstaat een basis voor een toenemend vertrouwen tussen organisaties, zodat ze ook minder problemen zullen hebben met het uitwisselen van informatie. Dat de Code voor Informatiebeveiliging hierbij een belangrijke basis is, is vanzelfsprekend gezien de plaats die deze Code inmiddels heeft gekregen.

Ten slotte rest de redactie nog te wijzen op een ingezonden bijdrage van prof. J.H. Blokdijk RE, die reageert op het artikel van J.C. Boer RE RA opgenomen in Compact 1998/3. In dit artikel besteedde Boer aandacht aan de ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking. Deze reactie is belangrijk omdat, zoals Blokdijk ook al aangeeft, er eindelijk weer eens een artikel is verschenen dat aanleiding geeft tot discussie en zo de inbedding van de ICT in de accountantscontrole opnieuw onder de aandacht brengt.
De redactie van Compact is blij met de doordachte en helder gestructureerde bijdrage van Blokdijk en ruimt daar dan ook graag een plaats voor in. Wellicht dat deze reactie aanleiding is tot verdere discussie, hetgeen de redactie uiteraard apprecieert.

De redactie van Compact wenst u het nodige leesplezier over het onderwerp informatiebeveiliging en hoopt dat dit nummer bijdraagt tot een beter beveiligingsbewustzijn in organisaties.

Jan van Praat

Hoe helpen we de probleemeigenaar?

Ondersteuning bij het opstellen van een informatiebeveiligingsbeleid

Drs. C.J. Coumou en drs. J.W.R. Schoemaker

Dit artikel gaat in op de wijze waarop de organisatie ondersteund kan worden bij het opstellen van een informatiebeveiligingsbeleid. De rol van de adviseur staat daarbij centraal, zoals blijkt uit de titel: 'Hoe helpen we de probleemeigenaar?'

INLEIDING

De aanleiding voor het besteden van aandacht aan het opstellen van een informatiebeveiligingsbeleid ligt in het feit dat dit de basis vormt voor alle activiteiten die samenhangen met informatiebeveiliging. Is het informatiebeveiligingsbeleid onjuist of onvolledig dan zijn de werkzaamheden die samenhangen met informatiebeveiliging gebaseerd op drijfzand. Al in de oudheid werd de noodzaak van beleid ingezien en de rol van de adviseur op zijn waarde geschat, zoals blijkt uit Spreuken 11, vers 14: 'Als beleid ontbreekt, komt het volk ten val; maar er is redding als er vele raadgevers zijn.' ([Bijb51]).

De opzet van dit artikel is als volgt. Allereerst worden enkele definities gegeven teneinde duidelijkheid te scheppen in de gehanteerde terminologie. Vervolgens wordt aandacht besteed aan de 'probleemeigenaar'. Wie is deze figuur en wat houdt hem bezig? Als er een 'probleemeigenaar' is, zal er ook een 'probleem' zijn. Dus wordt in dit artikel ook aangegeven welk probleem wordt opgelost met het opstellen van een informatiebeveiligingsbeleid. De kern van dit artikel bevat de beschrijving van een procesmatige aanpak voor informatiebeveiliging. Hierbij wordt met name ingegaan op het formuleren van een informatiebeveiligingsbeleid. Vervolgens wordt ook aangegeven wat een zinvolle inhoud van een informatiebeveiligingsbeleid zou kunnen zijn. Het artikel wordt afgerond met een samenvatting en enkele conclusies.

DEFINITIES

Alvorens in te gaan op de centrale vraag van dit artikel, 'Hoe helpen we de probleemeigenaar?', is het nuttig enige definities te geven van enkele termen die in dit artikel worden gehanteerd.

De eerste term die nadere toelichting vereist is *informatiebeveiliging*. Het Voorschrift Informatiebeveiliging Rijksdienst definieert informatiebeveiliging als 'het treffen van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van een informatiesysteem.'([BiZa94]). In deze definitie wordt het informatiesysteem dus als object van beveiliging aangemerkt. Het Voorschrift geeft aan dat het proces van informatievoorziening in het kader van beveiliging drie kenmerken bevat: beschikbaarheid, integriteit en exclusiviteit.

Een andere bron voor een definitie van informatiebeveiliging is de Code voor Informatiebeveiliging. De Code voor Informatiebeveiliging geeft aan dat het doel van informatiebeveiliging is 'het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van de schade voor het bedrijf door het trachten te voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.'([NNI94]). Evenals het Voorschrift Informatiebeveiliging Rijksdienst noemt de Code drie basisprincipes:

- vertrouwelijkheid: het beschermen van gevoelige informatie tegen onbevoegde kennisname;
- integriteit: het waarborgen van de correctheid en volledigheid van informatie en computerprogrammatuur;
- beschikbaarheid: zeker stellen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers.

De elementen van informatiebeveiliging zijn vergelijkbaar. Alleen gebruikt het Voorschrift de term exclusiviteit en de Code de term vertrouwelijkheid. Verder valt op dat de Code de bedrijfsvoering als object van beveiliging kiest. Bij de toelichting van de basisprincipes wordt in de Code gesproken over informatie, computerprogrammatuur en diensten als elementen die beveiliging vereisen.

Op grond van deze bronnen wordt informatiebeveiliging gedefinieerd als:

het geheel aan maatregelen dat gericht is op de bevordering van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en de informatieverwerking.

De tweede term die nader moet worden toegelicht, is *informatiebeveiligingsbeleid*. Een beleid heeft in het algemeen tot doel een richting aan te geven. Zo geeft het ondernemingsbeleid aan hoe de doelstellingen van de organisatie zullen worden gerealiseerd.

Volgens de Code voor Informatiebeveiliging dient het management in het informatiebeveiligingsbeleid aan te geven welke richting de organisatie wenst uit te gaan met betrekking tot informatiebeveiliging en te demonstreren dat zij informatiebeveiliging ondersteunt ([NNI94]). Verder dient het beleid volgens de Code als een hulpmiddel om aan te tonen dat het management informatiebeveiliging serieus neemt.

In de praktijk blijkt dat managementaandacht voor informatiebeveiliging een essentiële voorwaarde is voor een succesvolle implementatie van informatiebeveiliging.

Het Voorschrift Informatiebeveiliging Rijksdienst geeft als definitie van het informatiebeveiligingsbeleid de vastlegging van de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert ten aanzien van informatiebeveiliging, waarbij aandacht wordt besteed aan de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid ([BiZa94]). Het Voorschrift wijst dus op een goede coördinatie tussen het informatiebeveiligingsbeleid, het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. In het algemene beveiligingsbeleid wordt aandacht besteed aan de beveiliging van algemene middelen, zoals materieel en personen. Deze beveiliging heeft raakvlakken met informatiebeveiliging, bijvoorbeeld bij de beveiliging van kritische ruimten waarin IT-hulpmiddelen staan opgesteld. Het beleid voor de informatievoorziening geeft aan welke rol de informatiesystemen spelen binnen de bedrijfsprocessen. Verandert deze rol fundamenteel, bijvoorbeeld in geval van de implementatie van een nieuwe infrastructuur, dan zal ook de informatiebeveiliging opnieuw onder de aandacht moeten worden gebracht.

Op grond van deze bronnen wordt het informatiebeveiligingsbeleid gedefinieerd als:

de vastlegging van de doelstellingen, uitgangspunten, randvoorwaarden en prioriteiten van het management ten aanzien van informatiebeveiliging.

In het vervolg van dit artikel zal onder andere aandacht worden besteed aan de inhoud van een informatiebeveiligingsbeleid.

WIE IS DE PROBLEEMEIGENAAR?

In het kader van een adviestraject is het belangrijk inzicht te krijgen in de verdeling van het krachtenveld binnen de organisatie. Stokpaardjes, verborgen agenda's en onduidelijkheid over de verdeling van verantwoordelijkheden kunnen belemmerend werken bij het opstellen van een informatiebeveiligingsbeleid en het uitvoeren van werkzaamheden met betrekking tot informatiebeveiliging.

Wie kan als de probleemeigenaar worden aangewezen? In het algemeen is dat diegene die verantwoordelijk is (of zich verantwoordelijk voelt) voor de bedrijfsvoering. Dit geldt niet alleen voor de organisatie als geheel maar ook voor bedrijfsonderdelen of afdelingen. De rol van probleemeigenaar kan dus door diverse geledingen binnen de organisatie worden vervuld. De Raad van Commissarissen kan bijvoorbeeld aandacht vragen voor het onderwerp informatiebeveiliging vanuit de zorg voor de algemene continuïteit van het bedrijf.

Het (top)management van de organisatie kan de behoefte hebben aan beleid op dit terrein. Volgens de Code voor Informatiebeveiliging is het van belang dat het topmanagement aandacht besteedt aan in-

formatiebeveiliging ([NNI94]). Hierbij wordt aangegeven dat om deze aandacht structuur te geven hiervoor een stuurgroep voor informatiebeveiliging kan worden opgericht. Dit managementforum kan er volgens de Code voor zorgen dat de koers duidelijk is en dat er aantoonbare ondersteuning van het management is voor het nemen van beveiligingsmaatregelen. Aandacht in de pers voor het onderwerp informatiebeveiliging, bijvoorbeeld in het geval van incidenten met computervirussen of inbraak in computersystemen, kan bij het management de vraag oproepen hoe het op dit punt bij de eigen organisatie is geregeld.

Het lijnmanagement van een afdeling of businessunit kan zelf initiatieven nemen om informatiebeveiliging op een hoger plan te krijgen. Indien dit uit onvrede met het gebrek aan aandacht van het topmanagement is, kan dit in de praktijk tot problemen leiden. Wanneer het beleid moet worden vertaald in maatregelen ontbreken in een dergelijke situatie vaak de middelen om een en ander concreet vorm te geven. Dit is natuurlijk wel afhankelijk van de mate van decentralisatie en de budgettaire verantwoordelijkheid van de lokale eenheid.

Ten slotte kan ook de afdeling Automatisering haar eigen verantwoordelijkheid nemen en met de beveiliging van de informatievoorziening aan de slag gaan. In de praktijk blijkt dat het bewustzijn voor de noodzaak van informatiebeveiliging bij dit organisatieonderdeel het meest aanwezig is. Medewerkers van de afdeling Automatisering komen direct in aanraking met het beheer van informatiesystemen en de infrastructuur voor informatietechnologie (IT). Hierdoor hebben deze medewerkers zicht op de risico's die samenhangen met het gebruik van IT. Indien dit bewustzijn niet door het (top)management wordt gedeeld, kan dat leiden tot frustratie en ongenoegen bij deze functionarissen.

In de praktijk blijkt overigens vaak dat een incident de aanleiding vormt om serieus aandacht te gaan besteden aan informatiebeveiliging. Voorbeelden hiervan zijn sabotage aan een computersysteem, computerinbraak of fraude bij het gebruik van financiële informatiesystemen.

Vaak vormt een incident de aanleiding om serieus aandacht te besteden aan informatiebeveiliging.

WAT IS HET PROBLEEM?

Alvorens aan de slag te gaan met het ondersteunen van de probleemeigenaar is het van belang het probleem helder te krijgen. Dit is een belangrijke stap in het adviestraject die in de praktijk maar al te vaak wordt overgeslagen. Met als gevolg dat de adviseur en de probleemeigenaar aan de slag gaan met het oplossen van het verkeerde probleem of dat gedurende het adviestraject het helder krijgen van de probleemstelling een storende factor blijft in de werkzaamheden.

Wat is het probleem in relatie met dit artikel? In het kader van informatiebeveiliging wordt ervan uitgegaan dat er bedreigingen zijn die de continuïteit van de bedrijfsprocessen kunnen verstoren. De hiervoor genoemde drie aspecten van informatie en informatieverwerking – beschikbaarheid, integriteit en vertrouwelijkheid – kunnen door bedreigingen worden aangetast. Vaak heeft dat direct of indirect ook gevolgen voor de continuïteit van de bedrijfsvoering. Teneinde een logische indeling van bedreigingen te krijgen kan naast het gebruik van deze drie aspecten ook onderscheid worden gemaakt naar opzettelijke en onopzettelijke ongewenste gebeurtenissen ([Neis98]). Computeruitval door het optreden van fysieke dreigingen (zoals stroomuitval en brand) is een voorbeeld van een onopzettelijke gebeurtenis met gevolgen voor de beschikbaarheid. Ongeautoriseerde ontsluiting van gegevens is een opzettelijke daad die de vertrouwelijkheid van de informatie schaadt.

Kern van de probleemstelling voor informatiebeveiliging is dat het desbetreffende beleid zich zal richten op het voorkomen van bedreigingen en het beperken van de schade in het geval een bedreiging zich desondanks voordoet. Bij het beschrijven van het probleem is het van belang ghoststories en doemverhalen te filteren en een helder zicht te krijgen op de echte problematiek. Het uitvoeren van een risicoanalyse kan hierbij een nuttig hulpmiddel zijn.

De verantwoordelijke probleemeigenaar zou dus de volgende vragen moeten kunnen beantwoorden:
- Welke risico's hangen samen met de bedrijfsprocessen waarvoor ik verantwoordelijk ben?
- Welke maatregelen heb ik getroffen om de risico's het hoofd te bieden?
- Welke risico's zijn acceptabel?
- Hoe heb ik de verantwoordelijkheden met betrekking tot informatiebeveiliging toegewezen?
- Heb ik voldoende maatregelen getroffen en zijn die effectief?
- Welk programma ter verbetering van maatregelen en ter vermindering van risico's heb ik opgesteld?

HOE HELPEN WE DE PROBLEEMEIGENAAR?

Deze vraag wordt beantwoord vanuit de rol van de adviseur. De adviseur als deskundige op het gebied van informatiebeveiliging ondersteunt de probleemeigenaar bij de vormgeving en realisatie van het beleid voor specifieke bedrijfsprocessen. Het bieden van inzicht op grond waarvan beslissingen kunnen worden genomen, staat daarbij voorop. Het bedrijfsproces blijft centraal staan zodat informatiebeveiliging geen 'l'art pour l'art' wordt. Bovendien is het van belang dat de adviseur gedurende het adviestraject helder voor ogen blijft houden dat het probleem niet *voor* de klant maar *met* de klant wordt opgelost. Het is tenslotte de klant die na de afronding van het adviestraject met de voorgestelde oplossing aan de slag moet gaan.

Procesmatige aanpak voor informatiebeveiliging

Een eerste antwoord op de gestelde vraag kan zijn dat een structurele aanpak beter werkt dan ad-hocmaatregelen. Zoals eerder in dit artikel aangegeven, blijkt de probleemeigenaar vaak aandacht te willen besteden aan informatiebeveiliging na het optreden van een beveiligingsincident. Dan bestaat de neiging om de aandacht te richten op het incident en hiertegen ad-hocmaatregelen te treffen. Gaat het om een brandje, dan moet natuurlijk allereerst het brandje geblust worden. In alle andere gevallen kan beter worden gewerkt aan een structurele oplossing om te voorkomen dat op één plek te veel maatregelen worden getroffen, terwijl op een ander deelterrein ontoelaatbare risico's blijven bestaan.

Een procesmatige werkwijze kan dienen als structurele aanpak voor informatiebeveiliging. Dit is gebaseerd op de gedachte dat informatiebeveiliging een continu en cyclisch proces is dat bestaat uit bewust worden, beleid opstellen, plannen maken, maatregelen voorbereiden en implementeren, en vervolgens weer bewust worden van nieuwe risico's, beleid opstellen, enz. Hierbij wordt ervan uitgegaan dat de organisatie eerst als geheel met informatiebeveiliging aan de slag gaat. Vervolgens kunnen programma's voor specifieke risico's of voor onderdelen van de organisatie worden uitgekozen. In figuur 1 wordt deze procesmatige aanpak voor informatiebeveiliging schematisch weergegeven.

De procesmatige aanpak voor informatiebeveiliging is gebaseerd op de terminologie die wordt gehanteerd bij Total Enterprise Risk Management (TERM) binnen KPMG. De Engelse termen van deze aanpak worden ter referentie in de onderstaande toelichting vermeld. Deze aanpak omvat de volgende stappen:

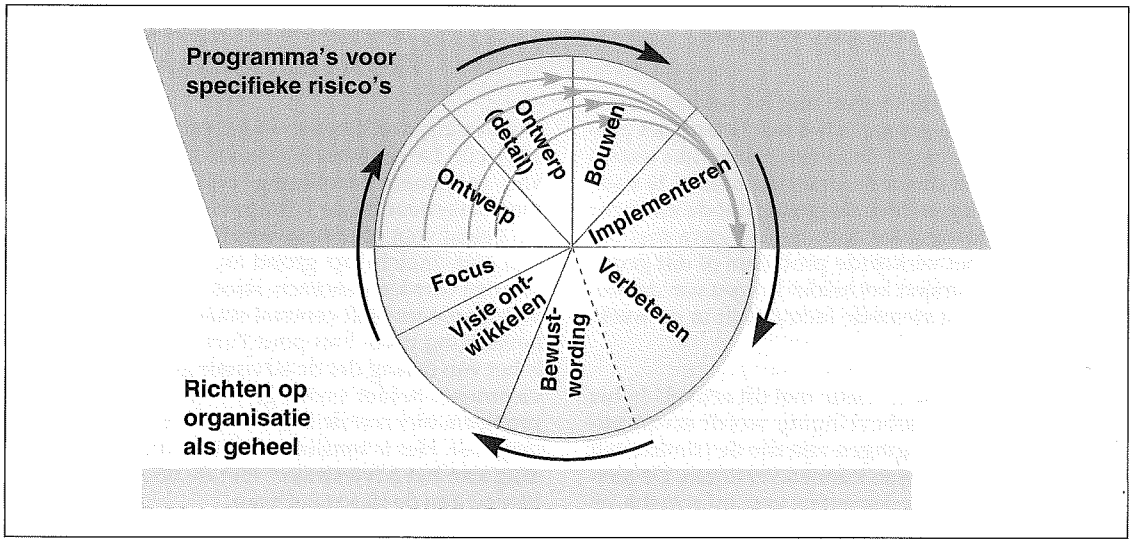
1. Bewustwording (Awaken);
2. Visie ontwikkelen (Envision);
3. Focus (Focus);
4. Ontwerp – breed (Design High Level);
5. Ontwerp – detail (Design Details);
6. Bouwen (Build);
7. Implementeren (Implement);
8. Verbeteren (Enhance).

De eerste stap binnen de procesmatige aanpak voor informatiebeveiliging is *Bewustwording*. De verantwoordelijken binnen de organisatie dienen zich allereerst bewust te worden van de risico's die samenhangen met het gebruik van IT en van de wenselijkheid van het treffen van beveiligingsmaatregelen. Om in het kader van dit artikel te spreken: 'de probleemeigenaar moet zich bewust worden van het probleem'. Ontbreekt die bewustwording (nog) bij de probleemeigenaar, dan kan zij worden bereikt door te wijzen op de aanwezige risico's of door het creëren van een gesimuleerd incident. Wanneer het probleem voor alle betrokkenen helder is, kan worden overgegaan tot de volgende stap van de voorgestelde aanpak.

De tweede stap heeft als titel *Visie ontwikkelen*. Deze stap omvat in het kader van informatiebeveiliging het opstellen van een informatiebeveiligingsbeleid. In dit beleid legt de organisatie vast welke visie de leiding heeft met betrekking tot informatiebeveiliging. Zoals eerder aangegeven in dit artikel geeft het management hiermee de richting aan die men wenst te gaan bij het treffen van beveiligingsmaatregelen.

Tijdens de volgende stap bepaalt de organisatie op welke onderdelen van informatiebeveiliging de aandacht zal worden gevestigd. Deze stap wordt daarom omschreven als *Focus*. De in de vorige stap bepaalde visie dient hierbij als basis. Aangezien de organisatie beschikt over beperkte tijd en gelimiteerde middelen moet een keuze worden gemaakt uit beveiligingsonderwerpen en -doelen die in het beleid zijn vastgelegd.

Bij de stap *Ontwerp* worden de beveiligingsmaatregelen ontworpen. Hiertoe wordt een beveiligingsplan opgesteld. In dit plan wordt aangegeven welke doelstellingen bepaalde (groepen van) maatregelen hebben, welke functionarissen en onderdelen van de organisatie bij deze maatregelen worden betrokken en welke middelen hiervoor noodzakelijk zijn. Daarnaast bevat het beveiligingsplan een inschatting van de kosten en een planning van de realisatie van de maatregelen. Het beveiligingsplan vormt de marsroute om de gewenste beveiligings-



Figuur 1. Procesmatige aanpak voor opzetten en uitvoeren van informatiebeveiliging.

situatie te kunnen bereiken. De stap Ontwerp kan twee onderdelen bevatten, allereerst een ontwerp op hoofdlijnen en daarna een uitwerking in detail.

De volgende stap is genaamd *Bouwen*. De maatregelen worden op basis van het beveiligingsplan gerealiseerd. Dit omvat het opstellen van richtlijnen en procedures en het selecteren van de benodigde middelen. Indien voor het eerst wordt gestart met een projectmatige aanpak van informatiebeveiliging betekent dit veelal dat tegelijkertijd verschillende maatregelen worden gebouwd. Voorbeelden van maatregelen zijn het verbeteren van de fysieke beveiliging van kritische ruimten (computerruimte, telefooncentrale, etc.), het opstellen van richtlijnen en procedures voor de logische beveiliging van informatiesystemen of het realiseren van uitwijk voor de primaire informatiesystemen.

De stap *Implementeren* betreft het daadwerkelijk invoeren van de in de vorige fase gerealiseerde maatregelen. Ook bij dit onderdeel heeft een projectmatige aanpak de voorkeur. Van belang hierbij is tijdige opleiding en training voor alle betrokkenen, waaronder zij die de maatregelen zullen moeten naleven.

De geïmplementeerde maatregelen kunnen vanwege allerlei oorzaken voor verbetering vatbaar zijn. Bijvoorbeeld door veranderingen in de organisatie of gebruikte hulpmiddelen. Tijdens de stap *Verbeteren* wordt dus onderhoud uitgevoerd zodat de maatregelen actueel kunnen blijven. Dit onderhoud kan geïnitieerd worden door het uitvoeren van controles. Tijdens deze controles kan worden geconstateerd dat maatregelen niet volledig of correct zijn, niet meer in samenhang met het beleid zijn of in de praktijk niet of niet geheel worden nageleefd. Indien het onderhoud van grote omvang is, zullen de stappen Ontwerp, Bouw en Implementatie doorlopen worden.

Vervolgens kan opnieuw worden begonnen met de eerste fase Bewustwording voor nieuwe onderdelen van informatiebeveiliging. Dit kan bijvoorbeeld het geval zijn voor de introductie van nieuwe technologieën, zoals Internet, electronic commerce en dergelijke. Hieruit blijkt dat informatiebeveiliging een continu proces is dat om blijvende aandacht van het management vraagt.

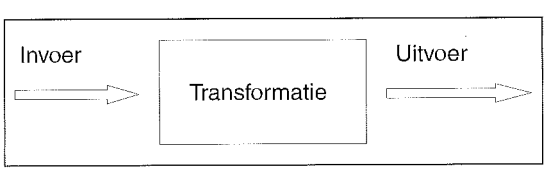
Gebruik van risicoanalyse

Tijdens de eerste drie stappen van de voorgestelde procesmatige aanpak kan een risicoanalyse of een Afhankelijkheids- en Kwetsbaarheidsanalyse (A&K-analyse) worden uitgevoerd. Risicoanalyse is een hulpmiddel voor besluitvorming met betrekking tot informatiebeveiliging omdat zij inzicht biedt in de relevante bedreigingen en in de mogelijke schade die daardoor kan ontstaan, en zicht biedt op de effectiviteit van maatregelen ([Coum93]). De Code voor Informatiebeveiliging wijst ook op het nut van het uitvoeren van een risicoanalyse voor het bepalen van de te nemen maatregelen en het stellen van prioriteiten ten aanzien van het beheer van risico's en het implementeren van de maatregelen die in de Code zijn beschreven ([NNI94]). Het Voorschrift Informatiebeveiliging Rijksdienst geeft aan dat voor ieder informatiesysteem en voor ieder verantwoordelijkheidsgebied een zogenaamde afhankelijkheidsanalyse moet worden uitgevoerd ([BiZa94]). Onder een verantwoordelijkheidsgebied wordt een geheel van voorzieningen verstaan dat ter beschikking staat aan één of meer informatiesystemen en waarvoor de verantwoordelijkheid eenduidig is toe te wijzen aan één organisatorische eenheid. De afhankelijkheidsanalyse dient uit te monden in aan het informatiesysteem te stellen betrouwbaarheidseisen. Tevens geeft het Voorschrift aan dat voor elk informatiesysteem en voor elk verantwoordelijkheidsgebied door middel van een zogenaamde kwetsbaarheidsanalyse moet kunnen worden aangetoond dat aan de betrouwbaarheidseisen wordt voldaan. Dit wordt gedaan door in de kwetsbaarheidsanalyse een afweging te maken tussen de risico's en de getroffen maatregelen. Daar waar ter dekking van de risico's onvoldoende maatregelen zijn genomen om de betrouwbaarheidseisen te kunnen waarborgen, worden aanvullende maatregelen voorgesteld, welke worden vastgelegd in een beveiligingsplan.

Bij de eerste stap, Bewustwording, kan risicoanalyse of A&K-analyse als hulpmiddel dienen om het management te overtuigen van de noodzaak van informatiebeveiliging. Tijdens de volgende twee stappen, Visie en Focus, biedt het uitvoeren van een risicoanalyse of een A&K-analyse de mogelijkheid om prioriteiten te stellen. De beperkte middelen kunnen hierdoor worden ingezet op de bestrijding van de risico's die om de meeste aandacht vragen.

Bedrijfsprocessen als uitgangspunt

Bij de toepassing van bovengenoemde aanpak verdient het aanbeveling om de bedrijfsprocessen als uitgangspunt te nemen. Een bedrijfsproces kenmerkt zich door de in figuur 2 weergegeven elementen.



Figuur 2. Elementen van een bedrijfsproces.

Allereerst biedt de invalshoek van de bedrijfsprocessen de mogelijkheid om het lijnmanagement verantwoordelijk te stellen voor de informatiebeveiliging van de bedrijfsprocessen die onder hun verantwoordelijkheid vallen. In het Voorschrift Informatiebeveiliging Rijksdienst ([BiZa94]) wordt het belang van een eenduidige en volledige toewijzing van verantwoordelijkheden onderstreept. Hierbij wordt aangegeven dat dit bij een complexe infrastructuur geen eenvoudige zaak is. Het vinden van aansluiting bij de bestaande verdeling van taken en verantwoordelijkheden voor de informatievoorziening kan hiervoor een oplossing bieden.

Het vereenvoudigde overzicht van een bedrijfsproces, bestaande uit invoer, transformatie en uitvoer, kan bij informatiebeveiliging van nut zijn. Aan de *invoerkant* kunnen afhankelijkheden van leveranciers bestaan. Daar waar ten behoeve van het bedrijfsproces gebruik wordt gemaakt van geavanceerde IT kan deze afhankelijkheid bijzonder groot zijn. Denk aan de toepassing van Internet-technieken, zoals electronic commerce. Het is hierbij zaak de eisen voor de beschikbaarheid van de diverse

componenten van de IT scherp te bepalen en deze in contracten met de leverancier vast te leggen.

De kern van het bedrijfsproces wordt gevormd door de *transformatie*. Hierbij wordt een waarde toegevoegd aan de geleverde producten of diensten. Uit het oogpunt van risico's dient er dus op te worden gelet dat die toevoeging van waarde ook daadwerkelijk kan plaatsvinden op de daarvoor aangegeven wijze. Zo kunnen maatregelen voor interne controle en administratieve organisatie worden getroffen om de transformatie correct te laten verlopen.

Aan de *uitvoerkant* zijn de afspraken met de afnemers van belang. Welke afspraken zijn gemaakt en welke bedreigingen kunnen ertoe leiden dat het nakomen van deze afspraken in gevaar komt? Hier gaat het dus over de gevolgen die ontstaan als bedreigingen optreden die tot gevolg hebben dat de afnemer de producten en diensten niet volgens de afgesproken specificaties ontvangt. Tot die gevolgen behoren onder meer schadeclaims, verlies van omzet en klanten, en imagoschade. Voorbeelden van uitval, waarbij er een directe relatie met de klant is, zijn uitval van een pinautomaat op zaterdagochtend of het niet-beschikbaar zijn van een computersysteem bij het inchecken op een vliegveld. Naast het schaden van beschikbaarheid kunnen er ook problemen ontstaan met de integriteit of de vertrouwelijkheid van de uitvoer. Met name daar waar het product of de dienst gebaseerd is op vertrouwelijke omgang met gegevens, zal dit snel aanleiding geven tot imagoschade en klantverlies.

Het is dus van belang voor de drie elementen van elk bedrijfsproces – invoer, transformatie en uitvoer – een helder beeld te hebben van de risico's, zodat beveiligingseisen kunnen worden gesteld. Enerzijds kunnen deze eisen worden vastgelegd in contracten met leveranciers en afnemers. Anderzijds zal de lijnmanager van het desbetreffende bedrijfsproces ervoor moeten zorgen dat de eisen in een beveiligingsbeleid worden opgenomen zodat maatregelen kunnen worden getroffen.

INHOUD VAN EEN INFORMATIEBEVEILIGINGSBELEID

Wat zou een informatiebeveiligingsbeleid moeten bevatten? Voor de beantwoording van deze vraag kunnen diverse bronnen worden geraadpleegd.

Een eerste antwoord op de vraag naar de inhoud van het informatiebeveiligingsbeleid wordt gegeven door de Code voor Informatiebeveiliging ([NNI94]). Deze spreekt over het opnemen van de volgende richtlijnen:
- een definitie van de term informatiebeveiliging;
- een verklaring van de betrokkenheid van het management;
- een toelichting op beleidsmaatregelen, principes, normen en eisen ten aanzien van informatiebeveiliging;
- een omschrijving van algemene en specifieke verantwoordelijkheden inzake informatiebeveiliging;
- een beschrijving van een procedure voor het rapporteren van beveiligingsincidenten.

Volgens een publicatie van de afdeling Beveiliging van het Nederlands Genootschap voor Informatica ([NGI92]) omvat een beveiligingsbeleid het volgende:
- de te bereiken doelen;
- het onderkennen van risico's;
- het inventariseren van de te beveiligen gebieden;
- de beveiligingsuitgangspunten die in maatregelen moeten worden omgezet;
- het benoemen van de maatregelen (in hoofdlijnen);
- de randvoorwaarden;
- de wijze van vaststelling van de realisatie van de doelen, de implementatie en de effectiviteit van de maatregelen.

Het Voorschrift Informatiebeveiliging Rijksdienst ([BiZa94]) doet eveneens een uitspraak over de mogelijke inhoud van het informatiebeveiligingsbeleid. In artikel 3 van dit Voorschrift wordt aangegeven dat het informatiebeveiligingsbeleid de volgende onderdelen zou moeten bevatten:
- de strategische uitgangspunten en randvoorwaarden, waaronder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;
- de organisatie van de beveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;
- de eenduidige en volledige indeling in informatiesystemen en verantwoordelijkheidsgebieden en de toewijzing van de verantwoordelijkheden daarvoor aan lijnmanagers;
- de wijze waarop het beleid vertaald wordt naar concrete maatregelen en de wijze waarop deze gefinancierd worden;
- de gemeenschappelijke betrouwbaarheidseisen en maatregelen die voor de gehele organisatie van toepassing zijn;
- de wijze waarop inbreuken op de informatiebeveiliging gemeld en afgehandeld worden;
- de wijze waarop en de frequentie van evaluatie van het informatiebeveiligingsbeleid en van de beoordeling van de toereikendheid van het beleid, de implementatie en de uitvoering daarvan door een onafhankelijke deskundige;
- de wijze waarop het beveiligingsbewustzijn wordt bevorderd.

Op grond van deze bronnen kan worden geconcludeerd dat de doelstellingen, uitgangspunten, prioriteiten en randvoorwaarden voor informatiebeveiliging als kernpunten in het informatiebeveiligingsbeleid kunnen gelden. Daarnaast verdient het aanbeveling aandacht te besteden aan de beveiligingsorganisatie in de vorm van de verdeling van taken, verantwoordelijkheden en bevoegdheden, aan de normen en eisen die gelden ten aanzien van de beveiliging van informatiesystemen en aan de wijze van evaluatie en beoordeling van de realisatie van het informatiebeveiligingsbeleid.

Steekwoorden bij de beschrijving van de *doelstellingen* van informatiebeveiliging zijn beschikbaarheid, integriteit en vertrouwelijkheid van de informatieverwerkende processen van de organisatie. Dit betekent dat het management in het informatiebeveiligingsbeleid vastlegt dat het ernaar streeft om zorg te dragen dat:

- de informatievoorziening er zal zijn op de afgesproken tijdstippen (beschikbaarheid);
- de informatievoorziening zal functioneren volgens de daarvoor vastgestelde specificaties (integriteit);
- de omgang met de informatie zodanig beveiligd zal zijn dat ongeautoriseerde ontsluiting van gegevens wordt voorkomen (vertrouwelijkheid).

Uitgangspunten hebben betrekking op de houding van het management ten aanzien van risico's en maatregelen. Zo kan het management van de organisatie risicomijdend gedrag vertonen, hetgeen tot uitdrukking komt in de getroffen maatregelen. Een voorbeeld van een uitgangspunt is dat bij het treffen van beveiligingsmaatregelen het belang en de veiligheid van het personeel voorop staan.

In het informatiebeveiligingsbeleid moeten ook *randvoorwaarden* ten aanzien van informatiebeveiliging worden vastgelegd. Dit biedt de mogelijkheid voor afbakening en schept duidelijkheid ten aanzien van wat wel en wat niet onder informatiebeveiliging valt te scharen. Een voorbeeld van een randvoorwaarde is dat beveiligingsmaatregelen altijd worden geselecteerd op basis van een risicoanalyse of A&K-analyse, waarbij een afweging wordt gemaakt tussen de kosten van de beveiligingsmaatregel en de verwachte vermindering van het risico.

Het beleid behoort ook een vastlegging van *prioriteiten* te bevatten. Deze hebben veelal betrekking op de verbetering van de kwaliteit van de beveiligingsmaatregelen. Zo'n verbetering kan gebaseerd zijn op de bij de risicoanalyse of A&K-analyse geconstateerde hiaten.

Informatiebeveiliging is in eerste instantie een verantwoordelijkheid van het lijnmanagement. Ook andere disciplines vanuit de organisatie zullen bij de realisatie van het informatiebeveiligingsbeleid worden ingezet. Daarom is het goed in het informatiebeveiligingsbeleid aandacht te besteden aan de beschrijving van de beveiligingsorganisatie. Een juiste en volledige verdeling van *taken, verantwoordelijkheden en bevoegdheden* schept duidelijkheid naar alle betrokkenen en biedt de mogelijkheid van decharge van de betrokken functionaris voor de door hem verrichte werkzaamheden.

De *normen en eisen* die gelden ten aanzien van de beveiliging van informatiesystemen behoren ook in het informatiebeveiligingsbeleid te worden vastgelegd. Het betreft hier de normen en eisen die algemeen geldend zijn voor de organisatie en de gebruikte informatiesystemen. Eventuele specifieke eisen voor individuele informatiesystemen kunnen op basis van aparte risicoanalyses of A&K-analyses worden bepaald. De Code voor Informatiebeveiliging noemt drie bronnen voor het opstellen van beveiligingseisen ([NNI94]):

1. De eerste bron wordt gevormd door de beveiligingsrisico's en de consequenties hiervan voor de organisatie. Door het uitvoeren van een algemene risicoanalyse of A&K-analyse voor de gehele organisatie kunnen de risico's en de hieruit voortvloeiende eisen boven tafel komen.

Informatiebeveiliging is in eerste instantie een verantwoordelijkheid van het lijnmanagement.

2. De tweede bron bestaat uit de wettelijke eisen en contractuele voorwaarden. In Nederland bestaat de Wet computercriminaliteit. Daarnaast is er de Wet persoonsregistraties die naar verwachting nog dit jaar zal worden vervangen door nieuwe wetgeving. Deze en andere wet- en regelgeving kunnen als bron dienen voor het bepalen van beveiligingseisen. Hetzelfde geldt voor de contractuele voorwaarden die met derden worden afgesloten. Zoals aangegeven bij de bespreking van de invalshoek van de bedrijfsprocessen dwingen afspraken met afnemers tot het formuleren van heldere beveiligingseisen.

3. De principes, doelstellingen en eisen voor het verwerken van informatie, die de organisatie heeft ontwikkeld ter ondersteuning van de bedrijfsvoering, vormen de derde bron voor de beveiligingseisen. De Code geeft aan dat de implementatie van beveiligingsmaatregelen een efficiënte bedrijfsvoering niet in de weg mag staan. In de praktijk blijkt er vaak een spanningsveld te bestaan tussen informatiebeveiliging en een efficiënte bedrijfsvoering. Hierbij komt het erop aan juiste keuzen te maken, waardoor enerzijds een acceptabel niveau van beveiliging ontstaat en anderzijds ook rekening wordt gehouden met een efficiënte bedrijfsvoering.

Als laatste element mag de *wijze van evaluatie en beoordeling van de realisatie van het informatiebeveiligingsbeleid* in het beleid niet ontbreken. Zoals eerder in dit artikel is aangegeven, is informatiebeveiliging een continu proces. Het regelmatig evalueren en beoordelen van de realisatie van de informatiebeveiliging biedt de organisatie de mogelijkheid om te controleren of men op de goede weg is. Is dit niet het geval dan is bijsturing noodzakelijk. Door hieraan in het informatiebeveiligingsbeleid expliciet aandacht te besteden kan dit onderdeel van het proces van informatiebeveiliging praktisch vorm krijgen.

Baseline

In het informatiebeveiligingsbeleid kan ook aandacht worden besteed aan een zogenaamde baseline. Indien de organisatie bestaat uit meerdere onderdelen, die ieder een bepaalde eigen verantwoordelijkheid hebben voor informatiebeveiliging, kan een baseline een goed hulpmiddel vormen voor de realisatie van een optimaal beveiligingsniveau voor alle onderdelen van de organisatie. Een baseline omvat een minimumset van beveiligingsmaatregelen die, ongeacht de specifieke omstandigheden of risico's van het onderdeel van de organisatie, aanwezig dienen te zijn. Indien wordt gekozen voor een uitgebreid beveiligingsdocument kan de baseline in het beleid worden opgenomen. Wordt gekozen voor een beleid van beperktere omvang dan kan de baseline in een apart document worden vastgelegd en kan in het informatiebeveiligingsbeleid worden volstaan met een verwijzing naar het separate document.

De baseline kan worden samengesteld door alle mogelijke beveiligingsmaatregelen, bijvoorbeeld die uit de Code van Informatiebeveiliging, de revue te laten passeren en per maatregel te bepalen in hoeverre deze onderdeel dient uit te maken van de baseline. De meest beperkte vorm van een baseline wordt gevormd door de zogenaamde sleutelmaatregelen van de Code. Dit zijn tien essentiële maatregelen die volgens de opstellers van de Code voor Informatiebeveiliging van toepassing zijn op elke organisatie en omgeving. Criteria bij het bepalen van de relevantie van de maatregel voor de baseline zijn:

- invloed van de maatregel op de elementen beschikbaarheid, integriteit en/of vertrouwelijkheid;
- invloed van de maatregel op risico's;
- aard van de maatregel (generiek versus specifiek);
- relevantie van het toepassingsgebied van de maatregel.

SAMENVATTING

In dit artikel is getracht een antwoord te geven op de vraag: 'Hoe helpen we de probleemeigenaar?' Vastgesteld is allereerst dat de probleemeigenaar kan variëren per organisatie en per probleemstelling. Voorop staat dat het lijnmanagement verantwoordelijk is voor de beveiliging van de eigen informatiesystemen. De eerste stap hierbij is het vaststellen van de relevante beveiligingseisen.

Vervolgens is aandacht besteed aan de vraag wat het probleem van de probleemeigenaar nu eigenlijk zou moeten zijn. In het kader van informatiebeveiliging is het probleem dat bedreigingen de continuïteit van de bedrijfsprocessen van de probleemeigenaar kunnen verstoren. Hierbij dienen de drie aspecten van informatie en informatieverwerking – beschikbaarheid, integriteit en vertrouwelijkheid – in ogenschouw te worden genomen.

Een structurele aanpak biedt de beste basis voor een effectieve en efficiënte informatiebeveiliging. Hierdoor kan worden voorkomen dat op één plek te veel maatregelen worden getroffen, terwijl op een ander deelterrein ontoelaatbare risico's blijven bestaan.

Een mogelijke aanpak uitgaande van een procesmatige invalshoek bestaat uit de acht stappen gehanteerd bij Total Enterprise Risk Management. Deze stappen omvatten het bewust worden van de noodzaak van informatiebeveiliging en de risico's die samenhangen met IT-gebruik, het opstellen van een informatiebeveiligingsbeleid, het uitwerken van beleidsprincipes in een beveiligingsplan, het voorbereiden, implementeren en verbeteren van concrete beveiligingsmaatregelen. Aangezien het een continu proces betreft, kan de cyclus weer opnieuw beginnen met het bewust worden van nieuwe risico's.

Het uitvoeren van een risicoanalyse of A&K-analyse kan als hulpmiddel dienen om het management te overtuigen van de noodzaak van informatiebeveiliging en biedt de mogelijkheid om prioriteiten te stellen. De beperkte middelen voor informatiebeveiliging kunnen hierdoor worden ingezet op de bestrijding van de risico's die om de meeste aandacht vragen.

Bij de toepassing van een structurele aanpak voor informatiebeveiliging verdient het aanbeveling om de bedrijfsprocessen als uitgangspunt te nemen. Dit biedt de mogelijkheid om het lijnmanagement verantwoordelijk te stellen voor de informatiebeveiliging van zijn bedrijfsprocessen. Tevens kunnen de beveiligingseisen op een heldere manier worden vastgesteld door een eenvoudig model van het bedrijfsproces als uitgangspunt te hanteren.

In een informatiebeveiligingsbeleid behoren doelstellingen, uitgangspunten, prioriteiten en randvoorwaarden voor informatiebeveiliging als kernpunten terug te komen. Daarnaast verdient het aanbeveling aandacht te besteden aan de verdeling van taken, verantwoordelijkheden en bevoegdheden, aan de normen en eisen die gelden ten aanzien van de beveiliging van informatiesystemen en aan de wijze van evaluatie en beoordeling van de realisatie van het informatiebeveiligingsbeleid.

In het informatiebeveiligingsbeleid kan ook aandacht worden besteed aan een zogenaamde baseline. Indien de organisatie bestaat uit meerdere onderdelen die ieder een bepaalde eigen verantwoordelijkheid hebben voor informatiebeveiliging, kan een baseline een goed hulpmiddel vormen voor de realisatie van een optimaal beveiligingsniveau voor alle onderdelen van de organisatie.

CONCLUSIES

De probleemeigenaar wordt het meest geholpen als hij tijdens de stappen die leiden tot een werkend stelsel van maatregelen voor informatiebeveiliging, steeds het inzicht heeft dat nodig is voor het nemen van beslissingen. Op een structurele wijze de weg bewandelen van bewustwording tot controle en evaluatie, is de beste garantie voor een doeltreffend informatiebeveiligingsbeleid.

Het helder krijgen van de probleemstelling is ook bij informatiebeveiliging belangrijk voor een succesvol adviestraject. Het vaststellen van de probleemstelling behoort dan ook bij de aanvang van het adviestraject aan de orde te komen.

In de praktijk blijkt de probleemeigenaar vaak aandacht te willen besteden aan informatiebeveiliging na het optreden van een beveiligingsincident. Hierbij bestaat de neiging om de aandacht te concentreren op het incident en hiervoor ad-hocmaatregelen te treffen. Het is echter beter om te werken aan een structurele oplossing om te voorkomen dat op één plek te veel maatregelen worden getroffen, terwijl op een ander deelterrein ontoelaatbare risico's blijven bestaan.

Het informatiebeveiligingsbeleid vormt de basis voor alle activiteiten die samenhangen met informatiebeveiliging. Daarom behoort het opstellen van

een dergelijk beleid ruime aandacht te krijgen binnen het proces van informatiebeveiliging.

Informatiebeveiliging is een continu en cyclisch proces. Veranderende omstandigheden, zoals de introductie van nieuwe technologieën (Internet, electronic commerce en dergelijke), vragen om blijvende aandacht van het management voor het vormgeven van het informatiebeveiligingsbeleid.

LITERATUUR

[Bijb51] Nederlands Bijbelgenootschap, *Bijbel, NBG-vertaling*, Derde druk, Haarlem 1951.

[BiZa94] Ministerie van Binnenlandse Zaken, *Voorschrift Informatiebeveiliging Rijksdienst*, 1994.

[Coum93] Drs. C.J. Coumou, *Using Risk-Analysis as a Tool for Decision making. Experiences from Real Life, in Facing the Challenge of Risk and Vulnerability in an Information Society*, IFIP North-Holland, 1993.

[NGI92] Nederlands Genootschap voor Informatica, afdeling Beveiliging, *Beveiligingsbeleid en beveiligingsplan*, 1992.

[NNI94] Nederlands Normalisatie Instituut, *Code voor Informatiebeveiliging*, 1994.

[Neis98] Prof. A.W. Neisingh RE RA, *Informatie- en communicatietechnologie en accountants: een verstandshuwelijk?*, Compact 1998/3.

Drs. C.J. Coumou en drs. J.W.R. Schoemaker zijn beiden werkzaam als senior manager bij KPMG EDP Auditors.

Corporate Information Security

Geen halve maatregelen

Dr. E.E.O. Roos Lindgreen RE

Door de snelle ontwikkelingen in de IT is naast de vele voordelen het gebruik ervan een toenemende bedreiging voor organisaties. Met name kunnen beveiligingsproblemen ontstaan die dringend om een oplossing vragen. Hierbij is het van groot belang een bedrijfsbrede aanpak te volgen. Hoe aan deze aanpak inhoud moet worden gegeven, wordt in dit artikel beschreven.

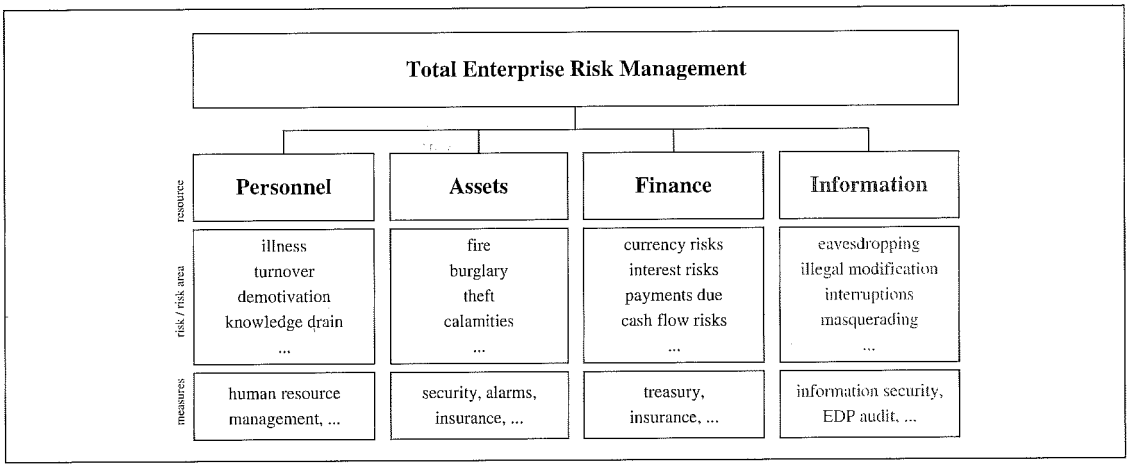
INLEIDING

Informatiebeveiliging is niet langer het domein van specialisten. Onder invloed van de toenemende integratie van informatietechnologie (IT) in onze bedrijfsprocessen wordt beveiliging steeds vaker verankerd in de taken en verantwoordelijkheden van de staande organisatie. Informatiesystemen zijn onmisbaar geworden voor het kunnen aanbieden van producten en diensten aan de markt. Ook buiten de informatie-industrie werkt vrijwel elke werknemer tegenwoordig met IT. Dit heeft consequenties voor de manier waarop het beveiligingsvraagstuk moet worden aangepakt. Van een specialisme is informatiebeveiliging uitgegroeid tot een gemeenschappelijke verantwoordelijkheid voor managers en medewerkers, een verantwoordelijkheid die in veel gevallen met twee woorden is samen te vatten: zorg en zorgvuldigheid. Zorg en zorgvuldigheid alleen zijn echter niet voldoende. De snelle veranderingen in de IT en de toepassing daarvan maken een proactieve houding en een voortdurende herbezinning op dreigingen en maatregelen noodzakelijk. Daarnaast worden informatiesystemen steeds vaker aan elkaar gekoppeld, waardoor de situatie ontstaat dat de beveiliging van het ene systeem afhankelijk is van de beveiliging van vele andere. Ten slotte zijn de meeste organisaties voortdurend aan verandering onderhevig. Deze veranderingen kunnen variëren van normaal personeelsverloop – zeer actueel in de huidige IT-arbeidsmarkt – tot ingrijpende processen als reorganisaties, fusies en overnames. Organisatorische veranderingen hebben niet zelden een aanzienlijke impact op de wijze waarop de informatiebeveiliging binnen een organisatie is ingericht. Informatiebeveiliging is dus een permanent proces, dat is gericht op het beheersen van veranderingen – management of change. In dit artikel wordt beschreven hoe dit proces structureel kan worden ingericht. De inhoud is als volgt.

In de eerste paragraaf wordt de relatie tussen informatiebeveiliging en integraal risicomanagement behandeld. Daarnaast wordt aandacht besteed aan het procesmatige karakter van beveiligingsmaatregelen. Ten slotte komt de relatie tussen maatwerk en confectie in informatiebeveiliging ter sprake.

Vervolgens komt één van de belangrijkste instrumenten voor het inrichten van het beveiligingsproces aan de orde: het *informatiebeveiligingsbeleid*. In het informatiebeveiligingsbeleid legt de hoogste leiding van een organisatie vast welke beveiligingskoers zij de komende jaren wil varen. Het opstellen en naleven van een beveiligingsbeleid is een must voor elke organisatie die het beveiligingsvraagstuk serieus neemt. In dit artikel zal aandacht worden geschonken aan de doelstellingen, de vorm, de inhoud en de totstandkoming van een informatiebeveiligingsbeleid. Daarbij wordt gekeken naar de verschillen tussen grote en kleine organisaties en tussen bedrijfsleven en overheid. Speciale aandacht zal worden besteed aan de valkuilen die men bij het opstellen en het invoeren van een informatiebeveiligingsbeleid kan tegenkomen.

Het opstellen van het informatiebeveiligingsbeleid is een belangrijke eerste stap bij het inrichten van een duurzaam stelsel van beveiligingsmaatregelen.



Figuur 1. Informatiebeveiliging als onderdeel van integraal risicomanagement.

Maar met een informatiebeveiligingsbeleid is men er natuurlijk nog niet. Papier is gewillig, wordt wel gezegd, en papieren tijgers bijten niet. Veel beleidsdocumenten slijten hun levensdagen helaas in de spreekwoordelijke bureaulade, dan wel beëindigen die in het ronde archief. De volgende stap is daarom het transformeren van het beleid naar een werkende *beveiligingsorganisatie*. Dit komt onder 'De beveiligingsorganisatie' aan de orde. Ingegaan wordt onder meer op de taken, verantwoordelijkheden en bevoegdheden van managers en medewerkers; de rol van de security manager; de aansturing van de organisatie door het management en het afleggen van verantwoording door de organisatie aan het management; en het realiseren van beveiligingsmaatregelen inzake contacten met derden. In de slotparagraaf wordt ingegaan op manieren waarop een duurzaam stelsel van beveiligingsmaatregelen kan worden gerealiseerd. Daarbij wordt aandacht besteed aan een structurele aanpak die beide benaderingen in zich verenigt: het Corporate Information Security-programma van KPMG EDP Auditors.

INFORMATIEBEVEILIGING IS...

Niet barsten, maar buigen

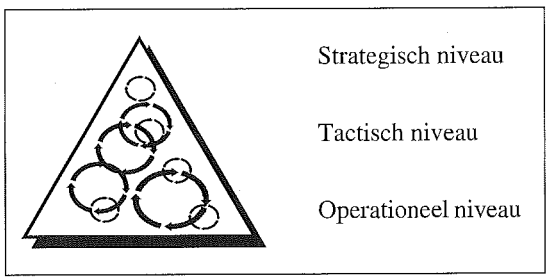
Iedere organisatie heeft haar eigen, unieke strategische doelstellingen, maar wat vrijwel alle organisaties gemeen hebben, is dat zij bij het realiseren van deze doelstellingen verantwoord willen omgaan met de risico's die daarbij optreden. De doelstelling van risicomanagement is deze risico's tot een aanvaardbaar niveau terug te brengen, in elk geval tot een niveau waarop het voortbestaan van de organisatie niet onnodig op het spel wordt gezet. De continuïteit van de bedrijfsvoering is immers voor elke organisatie van primair belang. Het volledig wegnemen van risico's is in de meeste gevallen niet haalbaar en ook niet wenselijk. Risico's nemen is nu eenmaal onlosmakelijk verbonden met ondernemen.

Risicomanagement is een activiteit die op zeer veel verschillende plaatsen binnen de organisatie plaatsvindt. Maatregelen voor risicomanagement kunnen op vele manieren worden geclassificeerd, bijvoorbeeld op basis van de productiemiddelen die een onderneming aanwendt om haar strategische doelstellingen te bereiken: Man, Matter, Money en ... Information. Essentieel is dat voor elk van deze productiemiddelen adequate maatregelen getroffen moeten worden. Informatiebeveiliging is in deze optiek niet meer en niet minder dan een normaal onderdeel van risicomanagement in algemene zin (zie figuur 1).

Geen halve maatregelen

Informatiebeveiliging is een breed vakgebied en omvat een heel scala van maatregelen. Sommige van deze maatregelen bestaan al sinds jaar en dag; een voorbeeld is het laten tekenen van een geheimhoudingsverklaring door het personeel. Andere maatregelen zijn zeer technologiegebonden, zoals het installeren van een firewall voor Internet-toegang. Het classificeren van beveiligingsmaatregelen is een aardig tijdverdrijf. Literatuuronderzoek wijst uit dat er vele manieren zijn om beveiligingsmaatregelen in te delen. Belangrijker is dat elke beveiligingsmaatregel altijd volgens het regelkringmodel dient te worden ingericht. Controle en bijsturing zijn noodzakelijk om te voorkomen dat maatregelen aan effectiviteit verliezen. Ook voor informatiebeveiliging geldt: stilstand is achteruitgang. De term beveiligingsmaatregel is dan ook enigszins misleidend; hij suggereert dat de beveiligingsproblematiek kan worden opgelost door een eenmalig ingrijpen, waar in feite voortdurende aandacht en zorg vereist zijn. Beveiligingsproces is om die reden een betere benaming.

Informatiebeveiliging is dus te beschouwen als een stelsel van maatregelen – of liever: processen – op alle niveaus in de organisatie (zie figuur 2). Al deze processen komen in de top van de organisatie bij elkaar. De hoogste leiding van een organisatie dient sturing te geven aan de doelstellingen en de uitvoe-



Figuur 2. Informatiebeveiliging als stelsel van processen op strategisch, tactisch en operationeel niveau.

ring van de beveiligingsprocessen. Bovendien zal de leiding steeds een getrouw beeld moeten hebben van de kwaliteit van de beveiligingsprocessen, liefst in verhouding tot het relatieve belang van elk proces voor de bedrijfsvoering en de continuïteit van de organisatie.

Confectie op maat

Hoe weet een topmanager nu welke beveiligingsmaatregelen zijn organisatie moet treffen? Over deze vraag hebben zich de afgelopen tientallen jaren vele deskundigen het hoofd gebroken. Daarbij lijkt een tegenstelling te ontstaan tussen voorstanders van een maatwerkbenadering en voorstanders van een standaardbenadering.

De eerste groep propageert het uitvoeren van een uitgebreide kwantitatieve risicoanalyse, op basis waarvan minutieus bepaald kan worden welke maatregelen wel en welke maatregelen niet getroffen moeten worden. Het uitvoeren van een risicoanalyse heeft als groot voordeel dat de organisatie een goed inzicht krijgt in de afhankelijkheden en kwetsbaarheden van IT. Risicoanalyses kennen ook nadelen: zij zijn niet alleen kostbaar, maar kunnen ook leiden tot een teveel aan informatie, waardoor het nemen van beslissingen niet makkelijker, maar juist moeilijker wordt.

De tweede groep maakt zich er heel wat gemakkelijker van af en vertrouwt op standaardmaatregelen, die zijn vastgelegd in uitgebreide checklists. Van zulke checklists zijn al heel wat waardevolle exemplaren verschenen. Denk aan de uitgaven van de afdeling Beveiliging van het Nederlands Genootschap voor Informatica (NGI) en het Nederlands Instituut voor de Registeraccountants (NIVRA), aan de Normbladen voor Informatiebeveiliging, aan de baselinebenadering van SRI International, of aan de Code voor Informatiebeveiliging. De laatste tijd doen organisaties in toenemende mate een beroep op deze laatste standaard, in 1994 uitgegeven door het Ministerie van Economische Zaken en het Nederlands Normalisatie Instituut.

Sommige deskundigen zijn van mening dat het intelligent gebruik van checklists als de Code voor Informatiebeveiliging de toepassing van risicoanalyses geheel overbodig zal maken ([Solm97]). Het is de vraag of het zo'n vaart zal lopen. Aan het gebruik van checklists kleeft een aantal bezwaren ([Roos95]), waarvan de belangrijkste is samen te vatten onder de noemer 'one size does not fit all'. De beveiligingsbehoeften van verschillende organisaties vertonen onderling vaak minder gelijkenis dan men op grond van andere overeenkomsten zou verwachten. Zelfs binnen één branche kunnen de bedrijfsprocessen van verschillende organisaties sterk uiteenlopen. Hetzelfde geldt voor de risico's die samenhangen met de automatisering van deze processen. Ten slotte is de toepasbaarheid van specifieke maatregelen mede afhankelijk van de omvang, de externe omgeving en de bedrijfscultuur van een organisatie. Zo kunnen maatregelen die zijn gebaseerd op een verregaande controletechnische functiescheiding, niet worden gerealiseerd in kleine of onderbemande organisaties.

Ook bij een intelligent gebruik van checklists moet altijd zorgvuldig worden afgewogen welke maatregelen wel en welke maatregelen niet moeten worden getroffen, afhankelijk van het belang van het te beschermen informatiesysteem voor de organisatie en de dreigingen waaraan dit systeem is blootgesteld. Een dergelijke afweging impliceert het uitvoeren van een risicoanalyse. Het gebruik van checklists is daarom noodzakelijk, maar niet voldoende; informatiebeveiliging is en blijft maatwerk, waarbij checklists buitengewoon nuttig kunnen zijn.

BEVEILIGINGSBELEID

Het beveiligingsbeleid is een essentieel instrument voor de aansturing en coördinatie van de verschillende beveiligingsprocessen binnen een organisatie. Het uiteindelijke doel is daarbij: het inrichten van een duurzaam stelsel van beveiligingsmaatregelen in de organisatie en in de IT, gericht op een adequate beheersing van de risico's. Het beleid biedt daarvoor een uniforme basis. Het beleid is derhalve primair een communicatie-instrument.

Een ander doel van het beleid is ook: laten zien dat de organisatie voldoet aan eisen die worden gesteld door diverse partijen uit het maatschappelijk verkeer. Zo worden impliciet of expliciet beveiligingseisen gesteld door aandeelhouders, zakenpartners, fusiepartners, een branchevereniging, een beroepsorganisatie en toezichthouders. Het opstellen en invoeren van een informatiebeveiligingsbeleid past daarbij in ontwikkelingen als het waarborgen van de waarde van de organisatie voor aandeelhouders en andere belanghebbenden (*shareholder value*, respectievelijk *stakeholder value*) en het inrichten van heldere bestuursvormen en juridische constructies, zodat eenduidig verantwoording over het reilen en zeilen van de organisatie kan worden afgelegd (*corporate governance*). Daarnaast worden in de wet expliciete eisen gesteld aan de beveiliging van gegevens en informatiesystemen. Voorbeelden hiervan zijn te vinden in de Wet persoonsregistraties en het voorstel van de Wet Bescherming Persoonsgegevens, en in de Wet computercriminaliteit, maar ook in het Burgerlijk Wetboek, de Telecommunicatiewet en het Wetboek van Strafvordering.

Inhoud en vorm

Bij het opstellen van een beveiligingsbeleid is de eerste vraag: wat komt erin te staan? Het beleid definieert allereerst de koers van de organisatie inzake de informatiebeveiliging en definieert het organisatorische en bestuurlijke raamwerk. Het beleid moet daarom zeker een koppeling met processen en organisatieonderdelen kennen, maar mag niet te zeer gefixeerd zijn op de staande organisatie. Elke organisatie is immers aan verandering onderhevig.

Een andere vraag is: moet het beleid ook inhoudelijk ingaan op concrete beveiligingsmaatregelen? Een voordeel hiervan is dat organisatieonderdelen direct aan de slag kunnen met de implementatie; een nadeel is dat het beleid snel zal verouderen. Het verdient daarom aanbeveling geen concrete maatregelen in het beleid op te nemen als deze maatregelen zeer technologiespecifiek zijn. In dat geval kan beter worden verwezen naar bestaande standaarden en

best practices. Volgens het Voorschrift Informatiebeveiliging Rijksdienst 1994 dient een informatiebeveiligingsbeleid ten minste de volgende onderwerpen te bevatten:
- strategische uitgangspunten en randvoorwaarden;
- organisatie van de beveiligingsfunctie;
- toewijzing van verantwoordelijkheden;
- vertaling naar concrete maatregelen;
- gemeenschappelijke betrouwbaarheidseisen;
- melding van incidenten;
- toetsing en evaluatie;
- bevordering van het beveiligingsbewustzijn.

Daarnaast kan worden gedacht aan onderwerpen als het maken van afspraken met derden, een calamiteitenplan of een organisatiebrede aanpak voor risicoanalyse.

Voor wat betreft de vorm kàn worden opgemerkt dat het beleidsdocument ondanks bovenstaande eisen niet te dik mag zijn en in heldere taal gesteld moet zijn. Een beleidsdocument moet altijd worden afgestemd op de doelgroep, dat wil zeggen: de managers en medewerkers die betrokken zijn bij de invoering ervan.

Het olievlekeffect – Op verzoek van de Stuurgroep Informatiebeleid van een grote organisatie stort een werkgroep zich op het formuleren van een informatiebeveiligingsbeleid. Tijdens het schrijven ontdekt de werkgroep dat er steeds weer nieuwe maatregelen opduiken waaraan gedacht zou moeten worden. Bovendien ontstaat over sommige maatregelen een verhitte discussie, waarbij duidelijk wordt dat voor sommige beveiligingsmaatregelen uitzonderingen op de regel gelden, uitzonderingen die in het beleid vastgelegd moeten worden. Het beleidsdocument groeit en groeit. Een extra correctieslag die wordt uitgevoerd om het stuk iets compacter te maken, brengt alleen maar meer lacunes en uitzonderingen aan het licht, die met verve in de tekst worden verwerkt. Het resulterende document telt 86 kantjes en geeft een redelijk volledige opsomming van maatregelen die door de organisatie getroffen zouden moeten worden. In een bijlage worden de maatregelen nader uitgewerkt. Trots presenteert de werkgroep het beleid aan de Stuurgroep, die het op hoofdlijnen goedkeurt, maar wel enige kanttekeningen plaatst bij de omvang van het stuk. Het document wordt in de organisatie verspreid en verdwijnt daar geruisloos in stapels papier, archiefkasten en bureaulades...

Product én proces

Beveiliging is natuurlijk geen doel op zich, maar een middel; de kosten en andere lasten van dit middel moeten opwegen tegen de baten, die zeer moeilijk meetbaar zijn. Dit zakelijke uitgangspunt vereist een voortdurende afweging, die al in het beleid tot uitdrukking zal komen. Het opstellen van een beveiligingsbeleid is een uitstekende kans om lijnmanagers te betrekken bij het maken van deze afweging. Aangezien het denkproces toch moet plaatsvinden en de bijbehorende discussies toch gevoerd moeten worden, verdient het aanbeveling deze obstakels reeds in een vroeg stadium te nemen. Dit kan worden bereikt door het beveiligingsbeleid te laten opstellen door een team van betrokken lijnmanagers uit de staande organisatie. Deze aanpak heeft als groot voordeel dat het resulterende beleid, indien dit door alle leden van het team wordt onderschreven, direct sponsors heeft in de verschillende organisatieonderdelen die het beleid zullen moeten invoeren. Sponsors die weten dat het beleid er is, die het kunnen verdedigen en die het waar nodig kunnen toelichten. Een ander voordeel is dat een op deze wijze ontwikkeld beleid nauw zal aansluiten op de bedrijfsprocessen, de organisatie, de organisatiecultuur en de binnen de organisatie gehanteerde terminologie. Dit zal de acceptatie van het beleid binnen de organisatie sterk verhogen. Bij het opstellen van een informatiebeveiligingsbeleid gaat het dus niet alleen om het *product*, maar ook om het *proces*.

Penny wise, pound foolish – Een grote onderneming met vestigingen in meerdere landen heeft de pers gehaald met een klein, maar vervelend beveiligingsincident. De concernleiding besluit het beveiligingsvraagstuk nu eens goed aan te pakken en geeft de stafafdeling Corporate Information Management opdracht een beveiligingsbeleid voor alle divisies te ontwikkelen. De stafafdeling besluit geen eigen informatiebeveiligingsbeleid te schrijven, maar het beleidsdocument van een branchegenoot over te nemen, op punten aan te passen en uit te vaardigen. Waarom het wiel zelf uitvinden? Het beleid wordt in conceptvorm verspreid, maar de opzet mislukt. Managers hebben scherpe kritiek op het stuk. 'Dit is typisch zo'n oekaze uit de ivoren toren van het hoofdkantoor,' moppert een hunner. 'Dit komt uit de lucht vallen. Ik kan hier niets mee.' Het beveiligingsproject loopt al in de eerste fase vertraging op, de stafafdeling Corporate Information Management verliest een stukje van haar geloofwaardigheid, en aan het woord informatiebeveiliging kleeft nog lang een smet.

Kortom, het draagvlak en dus de acceptatie van het beleid kunnen worden verhoogd door het instellen van een (tijdelijke) projectgroep, die de formulering van het beleid op zich neemt. Deze projectgroep dient bij voorkeur te bestaan uit 'key players' uit de staande organisatie – invloedrijke en enthousiaste personen, die zich bewust zijn van de risico's van IT en die beveiliging een warm hart toedragen.

De omvang van zo'n projectgroep is vanzelfsprekend aan een maximum gebonden. De praktijk leert dat men met zeven personen nog wel een beveiligingsbeleid kan ontwikkelen, maar dat de effectiviteit en efficiency sterk afnemen naarmate de groep groter wordt. De wet van de verminderde meeropbrengst geldt ook bij beveiliging. Vergist u zich niet in het enthousiasme waarmee managers kunnen debatteren over de noodzakelijke lengte van een wachtwoord!

De werkwijze van de projectgroep zal van geval tot geval verschillen, maar moet altijd aansluiten op de manier van werken die binnen de organisatie gebruikelijk is. De projectgroep kan bijvoorbeeld vier keer bij elkaar komen, om met tussenpozen van twee à drie weken steeds een onderdeel van het informatiebeveiligingsbeleid op te stellen en af te ronden. Een deugdelijke voorbereiding, waarbij voor elke bijeenkomst steeds een concept-onderdeel van

het beleid ter bespreking aan de deelnemers wordt toegezonden, en een bekwame eindredacteur, die het beleid zowel qua inhoud als qua vorm kan schuren en polijsten, kunnen de efficiency en de effectiviteit van dit proces zeer ten goede komen.

Het resulterende beleidsdocument zal ter goedkeuring moeten worden voorgelegd aan de hoogste leiding of een door die leiding gemandateerd orgaan. Daarna kan het beleid door de organisatie worden ingevoerd – een operatie die niet zonder slag of stoot zal verlopen.

DE BEVEILIGINGSORGANISATIE

Voordat werkelijk een aanvang kan worden gemaakt met het invoeren van het beleid, zal een beveiligingsorganisatie moeten worden ingericht. Dit is noodzakelijk om te voorkomen dat tijdens het invoeringstraject onduidelijkheden ontstaan over de taken, verantwoordelijkheden en bevoegdheden. In dat geval is de kans groot dat concrete maatregelen bij gebrek aan een 'probleemeigenaar' in het luchtledige blijven zweven, ook al is dit natuurkundig gezien onmogelijk. Dit risico wordt verhoogd door het gegeven dat informatiebeveiliging vaak wordt gezien als een hete aardappel, die zo snel mogelijk op het bordje van een ander geschoven dient te worden. Het duidelijk vaststellen van taken, verantwoordelijkheden en bevoegdheden is daarom van het grootste belang.

Inrichting van de beveiligingsorganisatie

Al eerder is gesteld dat informatiebeveiliging de verantwoordelijkheid is van elke manager en medewerker van een organisatie. In de praktijk kan de verdeling van taken, verantwoordelijkheden en bevoegdheden vrij eenvoudig zijn, zoals het in tabel 1 gegeven voorbeeld laat zien.

Daarnaast zullen onder meer taken zijn weggelegd voor:
- de *automatiseringsorganisatie*, voor het treffen van vele noodzakelijke organisatorische en technische maatregelen;
- de *gebruikersorganisatie*, voor het uitoefenen van zorgvuldigheid en discipline bij het omgaan met IT;
- de *helpdesk*, inzake het beantwoorden van vragen over informatiebeveiliging en het registreren van incidentmeldingen;
- *personeelszaken*, inzake het voorlichten van nieuwe medewerkers, het laten ondertekenen van geheimhoudingsverklaringen en het opstellen van een sanctiebeleid bij overtreding van de voorschriften;
- *inkoop*, inzake het afsluiten van overeenkomsten met derden;
- *facilitair beheer*, inzake de beveiliging van gebouwen en terreinen.

In sommige gevallen kan het lonend zijn een Stuurgroep Informatiebeveiliging in te stellen, die de totstandkoming van beveiligingsvoorschriften en de invoering daarvan bewaakt. In deze Stuurgroep kunnen verschillende organisatorische eenheden en functionarissen vertegenwoordigd zijn, zoals de security manager, informatiemanagers van organisatieonderdelen, automatiseringsmanagers, manager personeelszaken, en lijnmanagers.

Uitzonderingen op dit voorbeeld zijn zeer wel mogelijk; de feitelijke invulling van de beveiligingsorganisatie zal van organisatie tot organisatie verschillen.

De Security manager

Reeds eerder is aangevoerd dat het aanstellen van een security manager of zelfs het inrichten van een stafafdeling Security management noodzakelijk kan zijn voor de beheersing van het beveiligingsproces. Tot zijn taken behoren onder meer (met dank aan André Buren):
- het opstellen en actualiseren van het beveiligingsbeleid;
- het toezicht houden op de implementatie en naleving van beveiligingsbeleid, en het onderhouden en actualiseren van de aanwezige kennis hierover;
- het onderhouden van interne en externe contacten binnen dit kader;
- het optreden als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen organisatorische eenheden;
- het afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie;
- het uitvoeren of initiëren van risicoanalyses en kleine interne audits;

Tabel 1.
Verdeling van taken, verantwoordelijkheden en bevoegdheden.

Directie	eindverantwoordelijk
Security manager	houdt toezicht op de algehele werking van het beveiligingsbeleid en faciliteert de implementatie van dit beleid
Afdeling EDP-audit	toetst en rapporteert aan de directie
Lijnmanagers	verantwoordelijk voor de implementatie en uitvoering van het beveiligingsbeleid binnen de desbetreffende organisatorische eenheid
Projectleiders	verantwoordelijk voor het opstellen en implementeren van beveiligingseisen die specifiek zijn voor het desbetreffende project
Leidinggevenden	verantwoordelijk voor een adequate beveiliging binnen de desbetreffende organisatorische eenheid
Medewerkers	verantwoordelijk voor alle aspecten van beveiliging met betrekking tot de functie

- het organiseren van en deelnemen aan een coördinerend overleg Informatiebeveiliging;
- het opstellen van criteria, normen en standaarden voor en het coördineren van de werkzaamheden van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het beveiligingsbeleid;
- het verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen;
- het uitwerken van beveiligingsplannen ten aanzien van de maatregelen, alsmede het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen;
- het geven van gevraagd en ongevraagd advies aan de leiding van de organisatie en het lijnmanagement over de te nemen maatregelen;
- het verzorgen en coördineren van interne opleidingen van het personeel op het gebied van informatiebeveiliging;
- het stimuleren van het beveiligingsbewustzijn en het opstellen, uitvoeren en onderhouden van een communicatieplan;
- het afhandelen van opgetreden beveiligingsincidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten;
- het opstellen van een controleplan;
- het rapporteren aan de leiding van de organisatie over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles;
- het op de hoogte blijven van nieuwe ontwikkelingen op het gebied van beveiliging en wetgeving met betrekking tot beveiliging.

De security manager zal in de praktijk als gelijkwaardig gesprekspartner van het hoger lijnmanagement moeten functioneren. In noodsituaties moet de security manager beheerst, maar daadkrachtig kunnen ingrijpen. De functie van security manager is een zware vertrouwensfunctie, waarbij wordt omgegaan met zeer gevoelige informatie. Een positionering op hoger managementniveau, waarbij direct wordt gerapporteerd aan de leiding van de organisatie, ligt daarom voor de hand.

IMPLEMENTATIE VAN HET BELEID

Is het beleid opgesteld en de bijbehorende beveiligingsorganisatie ingericht, dan kan een aanvang worden genomen met de invoering van het beleid in de organisatie. Het uiteindelijke doel hiervan is het inrichten van een duurzaam stelsel van beveiligingsmaatregelen in de organisatie, dat is gericht op een adequate beheersing van de risico's. Op papier ziet dit eruit als een eenvoudige, rechtlijnige operatie, die te vergelijken is met het monteren van dievenklauwen, pensloten en ander hang- en sluitwerk in uw eigen woning. De praktijk leert echter dat de implementatie van een informatiebeveiligingsbeleid aanzienlijk meer voeten in de aarde heeft. Hiervoor zijn – helaas – enkele fundamentele faalfactoren aan te wijzen.

Beveiliging 'scoort' niet
Waar dievenklauwen en pensloten een zichtbare en tastbare bijdrage aan de beveiliging van uw huis leveren, zijn de meeste informatiebeveiligingsmaatregelen niet zichtbaar voor het management. Het gaat in veel gevallen om nogal specialistische maatregelen in en rondom de informatiesystemen, maatregelen die voor een buitenstaander niet zichtbaar zijn en waar dus weinig goede sier mee te maken is.

Beveiliging is lastig
Waar beveiligingsmaatregelen wel zichtbaar zijn, leveren zij voor de gebruiker doorgaans ongemak op. Dit ongemak kan betekenen dat eens genoten privileges voorgoed geblokkeerd worden, of dat voor ogenschijnlijk eenvoudig functies opeens omslachtige handelingen moeten worden verricht.

Beveiliging is duur
Sommige beveiligingsmaatregelen hebben meer voeten in de aarde dan oorspronkelijk was gedacht, waardoor de kosten kunnen tegenvallen. Daarbij komt dat de kosten van informatiebeveiliging vóór het implementatietraject meestal verborgen gebleven zijn. Als de totale kosten van informatiebeveiliging tijdens het traject inzichtelijk worden gemaakt, zal weerstand bij het management ontstaan.

De aanwezigheid van deze constante faalfactoren maakt elk beveiligingstraject tot een uitdagende onderneming, waarbij een zeer zorgvuldige aanpak en een zeer zorgvuldige voorbereiding noodzakelijk zijn. Daarbij zijn ten minste drie kritische succesfactoren aan te wijzen:

Commitment van de hoogste leiding
Om een beveiligingstraject tot een succes te maken dient de hoogste leiding zich volledig en actief achter het beleid op te stellen. Gebeurt dit niet, dan zal het lijnmanagement concluderen dat beveiliging geen hoge prioriteit heeft.

Communicatie
Voor, tijdens en na het traject is een optimale communicatie met alle betrokkenen van het grootste belang. Een gebrekkige communicatie zal snel leiden tot een afnemend gevoel van betrokkenheid en een verhoging van de weerstand binnen de organisatie.

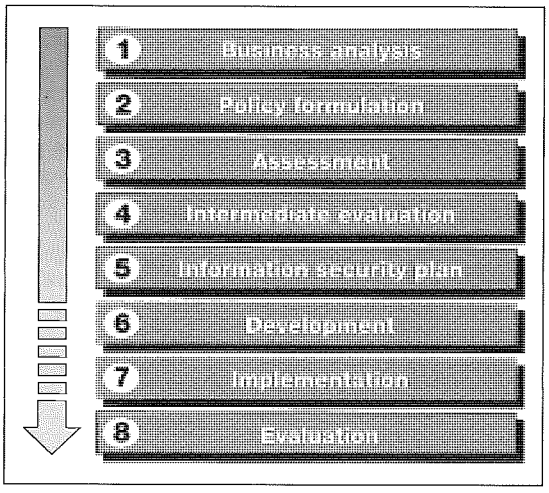
Gestructureerde aanpak
Het implementatietraject dient volgens een gestructureerde, projectmatige aanpak te worden uitgevoerd. Waar nodig dient per organisatieonderdeel een beveiligingsplan te worden opgesteld, waarin staat aangegeven welke maatregelen wanneer worden geïmplementeerd. Een voorbeeld van deze aanpak is het Corporate Information Security-programma van KPMG EDP Auditors, dat navolgend zal worden behandeld.

Corporate Information Security

Het Corporate Information Security-programma is opgebouwd uit een aantal deelstappen. Deze deelstappen zijn weergegeven in figuur 3.

De acht fasen uit het Corporate Information Security-programma zijn hieronder samengevat.

Fase 1 – Business analysis
In deze fase worden de bedrijfsprocessen en informatiesystemen binnen de organisatie geanalyseerd,



Figuur 3.
De fasering van het KPMG Corporate Information Security-programma.

alsmede de hieraan verbonden afhankelijkheden en kwetsbaarheden. Hiertoe worden korte 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, al dan niet op basis van een beknopte risicoanalyse en al dan niet op basis van een bestaande baseline, zoals de Code voor Informatiebeveiliging. 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 afgeleid 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 concept-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 'spider web' kan wonderen doen, maar moet altijd met een duidelijk voorbehoud worden gepresenteerd.

Fase 4 – Intermediate evaluation
In deze fase worden de resultaten van de assessment geëvalueerd en besproken met het hoogste management. Een moment van reflectie en discussie is noodzakelijk om de resultaten van de 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 de 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. KPMG heeft hiervoor recent 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 ontwikkelingsfase richt zich zowel op organisatorische als op technische maatregelen.

De ontwikkeling van *organisatorische maatregelen* bestaat uit het definiëren van procedures en richtlijnen, die kunnen worden vastgelegd in een Handboek Informatiebeveiliging, maar even goed kunnen worden opgenomen in een bestaand Handboek Organisatie of 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 beheerskosten van zulke producten de aanschafkosten in de regel sterk overschrijden; 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 awareness-programma. 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
In deze fase wordt het beveiligingstraject formeel afgerond, geëvalueerd en, indien gewenst, gecertificeerd tegen de Code voor Informatiebeveiliging.

Ervaringen

Het Corporate Information Security-programma is in enkele 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 de eenvoudige projectfasering, de eenduidigheid en de uniformiteit is het Corporate Information Security-programma voor het management herkenbaar. Bovendien wordt het traject steeds afgesloten met een tastbaar bewijs van de effectiviteit van de geleverde inspanning.

De Code voor Informatiebeveiliging blijkt in de praktijk zeer bruikbaar te zijn. De toenemende acceptatie van de Code in de markt is daarbij een belangrijke succesfactor. De structuur van de Code is niet altijd even logisch, en sommige hoofdstukken overlappen elkaar behoorlijk, maar deze bezwaren blijken in de praktijk niet onoverkomelijk te zijn. 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. Het is dan ook noodzakelijk de hiervoor verantwoordelijke afdelingen zeer nauw bij het beveiligingstraject te betrekken.

Naast de eerdergenoemde algemene faalfactoren is op dit moment slechts één specifiek knelpunt aan te wijzen. Commitment is het probleem niet; beveiligingsbewustzijn is vandaag de dag aanwezig op alle niveaus in de organisatie. Ook het budget vormt slechts in een klein aantal gevallen een beperkende factor. Een zwaarwegender beperking is dat vrijwel alle organisaties op dit moment kampen met een nijpend gebrek aan gekwalificeerd personeel en een zeer hoge mobiliteit op de IT-arbeidsmarkt, waardoor beveiligingstrajecten soms onbedoeld vertraging oplopen. Deze problematiek wordt versterkt door de huidige activiteiten op het gebied van het millennium en de euro, waarvan de prioriteit evident is.

Een organisatie die een Corporate Information Security-programma initieert, uitvoert en met een certificering bekroont, dient zich te realiseren dat haar informatiesystemen nog steeds kwetsbaarheden zullen kennen, kwetsbaarheden die mogelijk pas in de toekomst aan het licht zullen komen. Dat is gegeven de huidige stand van de IT onvermijdelijk en bovendien op zich geen ramp. Het doel is immers niet het 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.

Dr. E.E.O. Roos Lindgreen RE Is manager bij KPMG EDP Auditors.

EEN WOORD VAN DANK

Cees Coumou, Paul Overbeek, Ronald Paans en Jan Willem Schoemaker zijn de geestelijke co-ouders van het Corporate Information Security-programma. Bijzondere bijdragen zijn geleverd door André Buren, Gerben Nelemans, Neltsje van Nieuwpoort, Danny Onwezen, Abbas Shahim, Piet Veltman, Marleen Vorstenbosch, Ruben de Wolf en Arjen van Zanten. Bovenal is grote dank verschuldigd aan de personen en organisaties die het Corporate Information Security-programma of onderdelen ervan uitvoeren en hun ervaringen met ons delen.

LITERATUUR

[Solm97] R. von Solms, *Can security baselines replace risk analysis?* Proceedings of the IFIP/SEC Conference 'Information Security in Research and Business', Kopenhagen, 1997, pp. 91-101.

[Roos95] E. Roos Lindgreen en C.S. Schönfeld, *Maatwerk past informatiebeveiliging*, Compact 1995/3.

Informatiebeveiliging voor topmanagers

Securometer® stroomlijnt managementinformatie

Drs. A.M. Buren, drs. B. van der Meer, ing. A. Shahim M.sc., W. Barnhoorn, dr. E.E.O. Roos Lindgreen

Informatiebeveiliging wordt als onderdeel van de totale bedrijfsvoering steeds belangrijker. Informatiebeveiliging mag zich dan ook in toenemende mate in de aandacht van het topmanagement verheugen. In tegenstelling tot prestaties van financiële en logistieke processen worden de prestaties van het beveiligingsproces vaak niet op een efficiënte en evenwichtige manier onder de aandacht van het topmanagement gebracht. In dit artikel wordt een werkwijze en toepassing beschreven om de rapportage over beveiligingsprocessen aan de hoogste leiding van de organisatie te verbeteren.

INLEIDING

De beveiliging van informatie en informatiesystemen wordt steeds vaker gezien als een normaal onderdeel van risicomanagement in algemene zin en daarmee als een normale verantwoordelijkheid van de hoogste leiding van elke organisatie. Net als bij alle andere aspecten van risicomanagement is bij informatiebeveiliging geen sprake van een enkele en eenmalige activiteit, maar van een stelsel van processen dat zich uitstrekt over alle geledingen binnen de organisatie. Al deze processen komen in de top van de organisatie bij elkaar. Om over een goed inzicht in de daadwerkelijke veiligheid van informatie en informatiesystemen te kunnen beschikken, zal het verantwoordelijk management immers een getrouw beeld moeten hebben van de kwaliteit van elk beveiligingsproces, liefst in verhouding tot het relatieve belang van dat proces voor de bedrijfsvoering en de continuïteit van de organisatie.

Informatiebeveiliging mag zich op dit moment in de aandacht van het topmanagement verheugen. Men is zich bewust van de risico's van informatietechnologie (IT) en van de noodzaak verantwoord met deze risico's om te gaan. Er is één maar: topmanagers kunnen doorgaans slechts een beperkte hoeveelheid tijd en aandacht besteden aan het onderwerp informatiebeveiliging. Dat is nauwelijks verwonderlijk als men bedenkt dat de kosten voor informatiebeveiliging hooguit enkele procenten van de omzet bedragen.

Als gevolg hiervan beperkt de aandacht van het topmanagement zich vaak tot een kleine verzameling acute bedreigingen en tegenmaatregelen die op dat moment toevallig tot de waan van de dag behoren. De overige beveiligingsmaatregelen krijgen daarbij vaak niet de aandacht die zij noodzakelijkerwijs verdienen. Deze situatie is niet alleen onwenselijk, maar ook onnodig. Net als de prestaties van financiële en logistieke processen kunnen immers ook de prestaties van beveiligingsprocessen op een efficiënte en evenwichtige manier onder de aandacht van het topmanagement worden gebracht.

In dit artikel wordt beschreven hoe de informatievoorziening inzake informatiebeveiliging kan worden gestroomlijnd. De inhoud is als volgt. De eerste paragraaf beschrijft een algemeen raamwerk voor managementinformatie over informatiebeveiliging. De paragraaf 'Webtechnologie' geeft een algemene beschrijving van webtechnologie en de toepassing daarvan voor het meten van de prestaties van beveiligingsprocessen. De slotparagraaf gaat in op de algemene specificaties van zo'n toepassing, de Securometer®. Het artikel wordt afgesloten met een korte samenvatting.

MANAGEMENTINFORMATIE

Voor de inrichting van de informatiebeveiliging binnen organisaties wordt steeds vaker een beroep gedaan op de Code voor Informatiebeveiliging. Deze standaard definieert tien categorieën van beveiligingsmaatregelen die door de opstellers van de standaard als minimaal noodzakelijk worden beschouwd.

De Code voor Informatiebeveiliging vormt op zijn beurt weer de basis voor een gestructureerde benadering van de beveiligingsproblematiek. Een voorbeeld van deze benadering is KPMG's Corporate Information Security-programma, dat elders in deze Compact is beschreven. De essentie van dit programma is dat beveiligingsmaatregelen op basis van een heldere normstelling en een pragmatische analyse van de actuele situatie projectmatig worden ontwikkeld en geïmplementeerd.

Om een duurzame werking en naleving van de noodzakelijke maatregelen te waarborgen, voorziet het Corporate Information Security-programma in een gelaagd controlemodel, dat is weergegeven in figuur 1.

In dit model wordt de eerste controle op de effectiviteit van de maatregelen uitgevoerd door de verantwoordelijke functionaris zelf. Door middel van een self assessment rapporteert deze functionaris periodiek over de kwaliteit van de beveiligingsmaatregelen die vallen binnen zijn verantwoordelijkheidsgebied. Naast een toegenomen doelmatigheid heeft deze aanpak ook als voordeel dat door het erkennen van de autonomie van de verantwoordelijke functionaris een belangrijke psychologische barrière wordt weggenomen, die de acceptatie van een beveiligingstraject in de weg kan staan. Want wie vindt het nu werkelijk leuk voortdurend op de vingers gekeken te worden?

Een nadeel van de self assessment als controle-instrument is natuurlijk dat mensen hun zaken vaak rooskleuriger voorstellen dan ze in werkelijkheid zijn. De resultaten van de self assessment dienen dan ook in een tweede controletrap te worden getoetst, bijvoorbeeld door een internecontroleafdeling. In de praktijk blijkt bij de gecontroleerden voldoende begrip te bestaan voor de noodzaak van deze extra controle.

Ten slotte wordt een overkoepelende controle uitgevoerd door een externe deskundige, zoals een EDP-auditor. Deze controle kan plaatsvinden in het kader van de jaarrekeningcontrole, maar kan ook gericht zijn op het verstrekken van een third-party mededeling ([Velt95]) of een officieel beveiligingscertificaat ([Over97]).

Managementinformatie

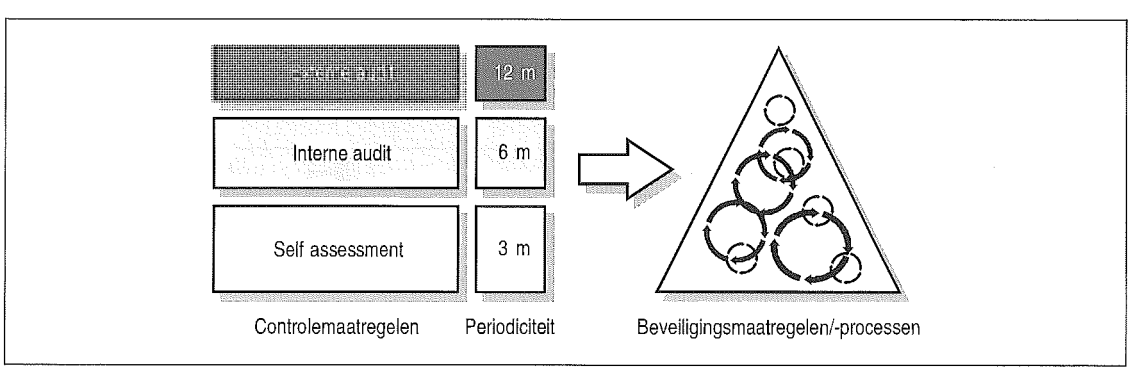
Het hierboven geschetste controlemechanisme valt of staat met de beschikbaarheid van goede managementinformatie over de talrijke beveiligingsprocessen. Idealiter moet de topmanager in één oogopslag kunnen zien hoe het met de kwaliteit van de beveiligingsmaatregelen is gesteld. Dit stelt op zijn beurt zekere eisen aan de vorm en inhoud van de managementinformatie over informatiebeveiliging.

In de praktijk blijkt dat deze managementinformatie vaak te wensen overlaat. Niet alleen vanwege het grote aantal beveiligingsmaatregelen – dat zelfs voor een middelgrote organisatie al vele tientallen, zo niet honderden zal bedragen – maar ook vanwege het uiteenlopende karakter van deze maatregelen, die veelal in verschillende organisatorische eenheden belegd zullen zijn en langs verschillende wegen, in verschillende vormen en met verschillende frequenties zullen worden gerapporteerd.

Om de managementinformatie over informatiebeveiliging te verbeteren kunnen verschillende technieken worden toegepast. Twee daarvan vormen de essentie van dit artikel.

In de eerste plaats is dat het gebruik van de Code voor Informatiebeveiliging voor het inrichten van een uniforme en gestructureerde standaardrapportage. De vaste en voor velen inmiddels bekende hoofdstukindeling van de Code blijkt de toegankelijkheid en herkenbaarheid van de gepresenteerde informatie aanmerkelijk te bevorderen en vormt bovendien een goede waarborg voor de volledigheid van de rapportage. In de tweede plaats kan een integraal controlemechanisme op basis van self assessments de kwaliteit van de managementinformatie sterk verbeteren. Met zo'n mechanisme beschikt de topmanager over een instrument waarmee de prestatie van de talrijke beveiligingsprocessen effectief, efficiënt en betrouwbaar kan worden gemeten.

De wijze waarop de self assessments worden afgenomen, blijkt medebepalend voor de effectiviteit ervan. In veel organisaties is het rondsturen, verzamelen en consolideren van papieren vragenlijsten nog steeds een gebruikelijke gang van zaken. Andere organisaties zijn overgestapt op het rondsturen



Figuur 1.
Gelaagd controlemodel.

van diskettes met geautomatiseerde vragenlijsten, maar deze aanpak lijkt het logistieke probleem in veel gevallen alleen maar erger te maken. Nieuwe media en technologieën bieden ons heden ten dage mogelijkheden self assessments op een snellere en efficiëntere wijze uit te voeren.

WEBTECHNOLOGIE

Nieuwe media als Internet, intranet en het World Wide Web zijn inmiddels algemeen geaccepteerd. Webtechnologie biedt de mogelijkheid om informatie op een uniforme, heldere wijze aan de doelgroep te presenteren. Het laagdrempelige en gebruikersvriendelijke grafisch georiënteerde interface van het World Wide Web is een krachtige eigenschap, die in toenemende mate wordt toegepast bij het realiseren van nieuwe informatiesystemen ([Bure97]).

Webtechnologie is bij uitstek geschikt voor het realiseren van een geautomatiseerd hulpmiddel voor het uitvoeren en presenteren van self assessments. In deze paragraaf worden hiervan de karakteristieken en onderliggende bouwstenen beschreven.

Bouwstenen

TCP/IP, HTTP en HTML vormen de technologische bouwstenen voor het World Wide Web, kortweg web genoemd, momenteel de meeste gebruikte Internet-toepassing. Deze technologie laat zich het best beschrijven aan de hand van een eenvoudig gelaagd model, afgebeeld in figuur 2, dat is ontleend aan de OTB-studie Internet ([OTBI97]).

Op het laagste niveau van dit model bevinden zich de twee generieke protocollen die de routering en het transport van gegevens over het netwerk mogelijk maken. Deze protocollen, Internet Protocol (IP) en Transmission Control Protocol (TCP), zijn elders in detail beschreven. TCP biedt een betrouwbare transportdienst aan tal van applicaties, die daar dankbaar gebruik van maken. Klassieke voorbeelden zijn e-mail (SMTP) en login op afstand (TELNET). Veel belangrijker is op dit moment het protocol dat wordt gebruikt voor het opvragen van hypertextpagina's: HTTP. Op de computer van de gebruiker draait een clientapplicatie – de webbrowser – die eenvoudige verzoekjes indient bij een serverapplicatie. De server reageert hierop door ofwel de opgevraagde pagina te retourneren, ofwel de ingevoerde gegevens te verwerken.

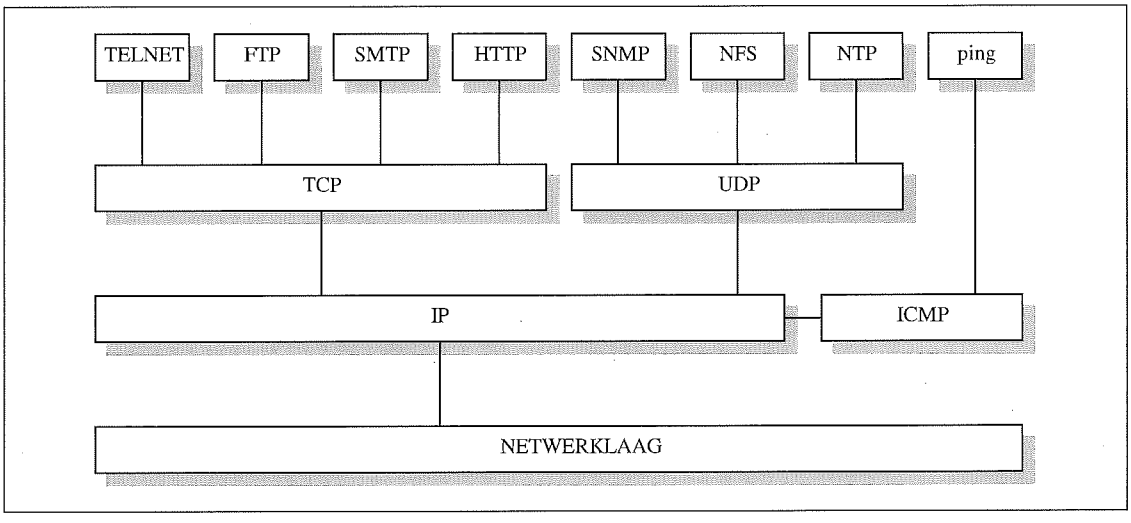
Kenmerkend voor het ontsluiten van informatie in een webomgeving is het hypertextprincipe. Volgens dit principe vindt de gebruiker op interactieve en associatieve wijze zijn weg door de enorme hoeveelheden gegevens. Deze gegevens zijn gegroepeerd in pagina's, die met behulp van links aan elkaar zijn gekoppeld. De muis is het belangrijkste wapen. Het intranet kan niet alleen worden gebruikt voor het opvragen van gegevens, maar ook voor het invoeren van gegevens. Hierbij valt te denken aan het stellen van vragen, het uitvoeren van zoek- en speuracties of het invullen van elektronische standaardformulieren.

De hypertextpagina's zijn opgebouwd volgens een vast formaat, de HyperText Markup Language (HTML). Hierbij worden verwijzingen naar andere pagina's in de tekst opgenomen, waarvoor een specifieke adresseringswijze wordt gebruikt: de Uniform Resource Locator (URL). Een URL voor HTTP bestaat uit de karakters 'http://', gevolgd door het Internet-adres van de computer waar de pagina zich fysiek bevindt, aan de hand van het Domain Name System (DNS), bijvoorbeeld 'www.asz.nl', gevolgd door een aanduiding van de locatie waar de pagina op deze computer is opgeslagen.

Naast tekst kunnen webpagina's ook informatie bevatten in de vorm van afbeeldingen, geluid, animatie en videobeelden. De multimediale presentatie van webpagina's heeft haar meerwaarde voor gebruikers inmiddels bewezen ([Bure95]). Mede hierdoor is het gebruik van de webtechnologie de afgelopen jaren explosief gestegen.

Intranet

Eerder beschreven technologieën kunnen behalve voor het publieke Internet ook worden gebruikt om informatie op kleinere schaal te distribueren via een zogeheten intranet. De groeiende populariteit van het Internet voor zakelijke en particuliere toepassin-



Figuur 2.
Internet-architectuur.

gen heeft het afgelopen jaar geleid tot een stormachtige opmars van intranettoepassingen.

Veel bedrijven beschikken inmiddels over geavanceerde intranettoepassingen. In sommige gevallen is het intranet niet meer dan een toegankelijke opslagplaats voor een beperkte verzameling algemene interne bedrijfsinformatie, zoals formulieren, regelingen, handboeken, de telefoonlijst en een wie-is-wie. Andere organisaties gaan veel verder en exploiteren het intranet voor de opslag en beschikbaarstelling van alle mogelijk denkbare gegevens, waarbij koppelingen worden gemaakt met bestaande applicaties voor de ondersteuning van primaire en secundaire bedrijfsprocessen, maar ook met externe informatiebronnen.

Een intranet is relatief eenvoudig te realiseren. Omdat het intranet op een bestaande LAN-omgeving draait, kunnen de initiële kosten laag blijven. Een groot voordeel van een intranet is dat door gebruikmaking van 'active content', zoals Java of ActiveX, de informatieoverdracht onafhankelijk van het onderliggende clientplatform wordt gemaakt. Hierbij wordt wel onderscheid gemaakt tussen scripts en applets. Een script is een verzameling instructies waarbij de broncode in de HTML-pagina is opgenomen. Een script wordt bij uitvoering geïnterpreteerd door de browser. Een applet is een verzameling instructies die in gecompileerde vorm met een HTML-pagina wordt meegestuurd, waarna de instructies door de webbrowser worden uitgevoerd. Een Java-applet wordt niet vertaald in machinecode, zoals normaliter het geval is bij applicaties, maar wordt vertaald naar een platformonafhankelijk bytecodeformaat. Om deze bytecode uit te kunnen voeren dient de browser te beschikken over een ingebouwde Java-interpreter. De Java-interpreter vormt de vertaalslag naar het onderliggende besturingssysteem.

Vrijwel alle browsers beschikken tegenwoordig over een ingebouwde Java-interpreter, waardoor de uitvoering van een Java-applet onafhankelijk is van zowel het besturingssysteem als het hardwareplatform. Ook voor het ontsluiten van managementinformatie hoeft de gebruiker daarom slechts over een browser te beschikken. Een welkome eigenschap voor organisaties met doorgaans meerdere hardwareplatformen, besturingssystemen en verschillend ingerichte werkplek-PC's.

Securometer®

Door de eerder beschreven karakteristieken als laagdrempeligheid, gebruikersvriendelijkheid, platformonafhankelijkheid en de relatief lage kosten is webtechnologie bij uitstek geschikt voor het realiseren van een tool voor het uitvoeren en presenteren van self assessments. Hierdoor kunnen de gewenste prestatiemeting van beveiligingsmaatregelen en de rapportage daarvan aan het topmanagement vergaand worden geautomatiseerd en daarmee efficiënt en duurzaam worden ingericht. Een uitwerking van dit principe heeft geresulteerd in de Securometer®, die in de volgende paragraaf wordt beschreven.

Webtechnologie is bij uitstek geschikt voor het realiseren van een tool voor het uitvoeren en presenteren van self assessments.

SECUROMETER®

De Securometer® is een intranetapplicatie voor het afnemen van self assessments ter inventarisatie van de kwalitatieve status van de getroffen beveiligingsmaatregelen en het verzorgen van de bijbehorende rapportage aan het topmanagement. De Securometer® is ontwikkeld door Automatisering Sociale Zekerheid (ASZ), huisleverancier van informatiediensten aan de GAK Groep, in samenwerking met KPMG EDP Auditors ([Meer97]). Achtereenvolgens worden de functionaliteit en de technische implementatie van de Securometer® beschreven.

Functionaliteit

De kwalitatieve status van de getroffen beveiligingsmaatregelen dient te worden ingevuld door respondenten die verantwoordelijk zijn voor de opzet en werking van deze beveiligingsmaatregelen.

De Securometer® werkt op basis van het client-serverprincipe en is onafhankelijk van de lokale computerinrichting van de eindgebruiker en eventuele randapparatuur. De gebruiker dient slechts te beschikken over een browser en toegang tot het intranet. Een installatieprocedure van de Securometer® aan de gebruikerskant komt hierdoor te vervallen; een welkome bijkomstigheid voor toch al vaak overbezette managers.

De Securometer® beschikt over een aantal basisfuncties, die achtereenvolgens zullen worden beschreven.

Starten
Bij het opstarten bepaalt het systeem aan de hand van de combinatie user-id en password wat de identiteit van de gebruiker is en stelt de daarbij horende autorisaties vast. Laatstgenoemde hebben betrekking op het uitvoeren van functies en het al dan niet bevoegd zijn self assessments van andere gebruikers op te vragen. Indien de gebruiker voor het systeem bekend is, controleert het de invulstatus van eerder ingevoerde self assessments, en geeft het de laatste nog in te vullen self assessment weer, al dan niet vergezeld van schermboodschappen dat voorgaande self assessments nog niet zijn ingevuld of verstuurd.

Self assessment
Om inzicht te krijgen in hoeverre beveiligingsmaatregelen binnen de organisatie zijn getroffen, zullen deze maatregelen periodiek moeten worden geïnventariseerd. Hiertoe worden door het systeem vragen geformuleerd, waarop gebruikers antwoord dienen te geven.

Het systeem bevat een centrale database waarin alle vragen zijn opgeslagen. Deze vragenlijst is opge-

bouwd volgens de structuur van de Code voor Informatiebeveiliging, maar kan op eenvoudige wijze worden aangepast voor andere baselines. Een manager zal gezien zijn functie in de regel verantwoordelijk zijn voor slechts een deel van de totale beveiligingsmaatregelen. Afhankelijk van de identiteit van de gebruiker distribueert het systeem daarom alleen de voor de gebruiker relevante vragen naar zijn of haar werkplek.

Het systeem presenteert de vragen aan de hand van omschrijving en kenmerken als de groep en het type van de vraag: betreft het een baselinevraag of een aanvullende vraag? Iedere respondent dient per deelonderwerp – het 'derde niveau' uit de Code – aan te geven of een specifieke maatregel wel, gedeeltelijk of niet geïmplementeerd is. Het antwoord op de vragen wordt daarbij gegeven door het aanklikken van de bij het antwoord behorende button. De vragen die in de desbetreffende invulperiode al zijn beantwoord, zijn daarbij gemarkeerd en kunnen afhankelijk van de gekozen menuoptie ('invullen onbeantwoorde vragen') bij verder invullen door de gebruiker worden genegeerd. Vragen worden doorgelopen door middel van navigatiebuttons. Met behulp van een zoekbutton kan daarbij worden gesprongen naar beschikbare vraagcategorieën (zoals bijvoorbeeld gebaseerd op de hoofdstukindeling van de Code van Informatiebeveiliging). Indien meer uitleg is gewenst over gestelde vragen dan wel de besturing van het systeem, voorzien helpbuttons in meer toelichtende informatie.

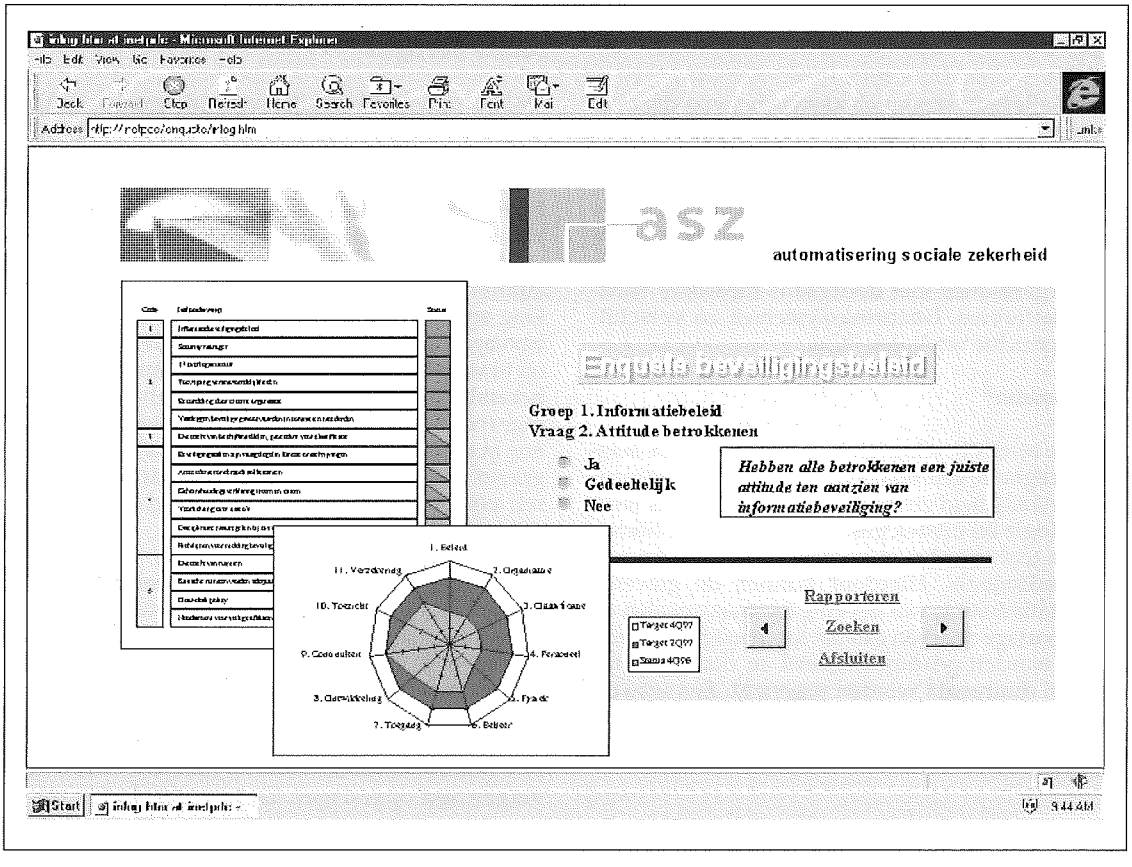
Een compleet ingevulde self assessment dient door de respondent te worden bevestigd, alvorens de antwoorden in de centrale database worden verwerkt. Hiertoe besluit de gebruiker door middel van het aanklikken van de bevestigingsbutton. Verwerkte self assessments kunnen daarbij door de gebruiker niet meer worden gewijzigd.

Voor de communicatie tussen client en server is gekozen voor een informatie-uitwisseling op transactiebasis. Het systeem kan hierdoor te allen tijde worden verlaten zonder verlies aan informatie.

Rapportage

De Securometer® verwerkt geregistreerde antwoorden tot geaggregeerde grafische meerdimensionale overzichten. De status van de getroffen beveiligingsmaatregelen wordt daarbij weergegeven door middel van een zogeheten stoplichtendiagram, waarin het niveau van informatiebeveiliging als rood, oranje of groen wordt afgebeeld. 'Rode' maatregelen zijn hierbij in onvoldoende mate aanwezig; 'oranje' maatregelen zijn hetzij onderwerp van discussie, hetzij slechts gedeeltelijk aanwezig; 'groene' maatregelen worden door alle respondenten als voldoende beoordeeld.

In een zogeheten spinnenwebdiagram kan het geïnventariseerde stelsel van beveiligingsmaatregelen worden gerelateerd aan de vooraf gestelde normen (in dit geval de Code voor Informatiebeveiliging). In dit diagram kan in één oogopslag worden afgelezen of deze normen worden nageleefd; het diagram geeft daarmee een snelle indicatie van het algemene beveiligingsniveau. Figuur 3 geeft hiervan een impressie; de feitelijke schermopmaak kan eenvoudig worden aangepast aan de huisstijl van de organisatie.



Figuur 3. Impressie van de vormgeving van de Securometer®.

Trendanalyse
Naast het opvragen en grafisch weergeven van actuele self assessments biedt het systeem ook diverse functies voor het weergeven van voorgaande self assessments. In het verleden ingevulde self assessments kunnen door de daartoe geautoriseerde gebruikers per invulperiode worden geaggregeerd en in een tijdslijn worden geplaatst. Hieruit ontstaat voor het topmanagement een goed inzicht in de progressieve dan wel regressieve ontwikkeling van het niveau van informatiebeveiliging.

Beheer
Behalve deze functionaliteit voor de eindgebruiker bevat de Securometer® een afzonderlijke beheermodule die de beheerder in staat stelt gebruikersnamen aan te maken en te wijzigen, permissies in te stellen, voortgangscontrole uit te oefenen, back-ups van de centrale database te maken en de vragenlijst te onderhouden.

Technische implementatie

De Securometer® opereert in een webomgeving en maakt gebruik van op Internet gebaseerde technologieën als TCP/IP en HTTP voor de communicatie tussen client en server. Door middel van TCP/IP en het HTTP-protocol communiceert het systeem de informatieoverdracht via het intranet aan de gebruiker. De opmaak en de inhoud van de informatieoverdracht zijn daarbij opgebouwd volgens het HTML-formaat. Voor elke vraag-antwoordsessie wordt een nieuwe verbinding tussen de client en de server opgezet en weer verbroken.

Webbrowsers interpreteren de HTML-pagina's en laten de gebruiker deze pagina zien in de beschreven opmaak. Bij de ontwikkeling van de Securometer® is gekozen voor een zogeheten 'dunne client'-architectuur, waarbij de clientapplicatie beperkt blijft tot navigatiefuncties met behulp van een webbrowser. Daardoor is de Securometer®-programmatuur gecentraliseerd op de server, wat zich vertaalt in efficiënter uit te voeren beheer- en onderhoudswerkzaamheden. Bovendien maakt deze architectuur het installeren van de Securometer® aan gebruikerskant overbodig.

De server is gekoppeld aan een relationele database, waarin de vragen zijn opgeslagen. De server fungeert als een communicatiepoort tussen de webbrowser en de Securometer®-database. De server gebruikt scripts om vragen en diagrammen – vertaald in HTML-pagina's – te communiceren naar de webbrowser en de binnengekomen antwoorden te verwerken. In figuur 4 is de technische architectuur van de Securometer® weergegeven.

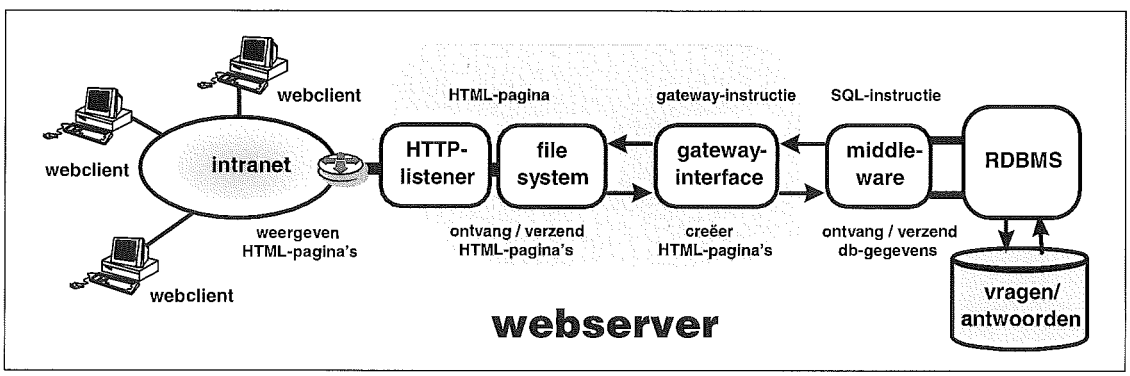
SAMENVATTING

Informatiebeveiliging wordt steeds belangrijker als onderdeel van de totale bedrijfsvoering. De noodzaak tot structurele verbetering maakt daarbij een integrale aanpak noodzakelijk. Om een integrale aanpak succesvol te maken, dient het topmanagement te beschikken over adequate managementinformatie over de prestaties van de beveiligingsprocessen binnen de organisatie.

Deze managementinformatie laat doorgaans te wensen over door de veelheid en diversiteit van beveiligingsmaatregelen. Beveiligingsmaatregelen zijn veelal in verschillende organisatorische eenheden belegd en worden hierdoor vaak langs verschillende wegen, in verschillende vormen, en met verschillende frequenties aan de hoogste leiding gerapporteerd.

Als onderdeel van een integrale aanpak kan een gelaagd rapportage- en controlemodel worden ingericht, dat bestaat uit self assessments, internecontrolemaatregelen en externecontrolemaatregelen. Door het decentrale management periodiek te laten rapporteren over de kwaliteit van de beveiligingsmaatregelen, kan de aggregatie van deze rapportage fungeren als managementinformatie voor de hoogste leiding van de organisatie. Voor het kunnen aggregeren van deze informatie is het van belang een uniforme inhoudsvorm te hanteren. De hoofdstukindeling van de Code voor Informatiebeveiliging vormt hiervoor een geschikt uitgangspunt.

Nieuwe technologieën bieden uitstekende mogelijkheden om het genereren en verstrekken van managementinformatie op basis van self assessments te stroomlijnen – ook omtrent informatiebeveiliging. Door gebruik te maken van intranettechnologie kan de logistiek van het controlemodel worden vereenvoudigd; een intranet biedt de mogelijkheid om self assessments op een snellere en efficiëntere wijze uit te voeren. De laagdrempeligheid en gebruikersvriendelijkheid van webtechnologie zijn daarbij krachtige eigenschappen, die zijn toegepast in de Securometer®.



Figuur 4.
Technische architectuur van de Securometer®.

Drs. A.M. Buren
Is als EDP-auditor werkzaam bij KPMG EDP Auditors en gespecialiseerd in technologische ontwikkelingen op het gebied van informatieoverdracht en multimedia. Zijn aandachtsgebieden liggen bij ondernemingsbrede beveiligingsvraagstukken en advies voor en audit van daaraan gerelateerde technologieën.

Drs. B. van der Meer
Is reeds geruime tijd werkzaam in de automatisering als systeemontwerper en technisch projectleider. De laatste jaren behoren technologieën als objectoriëntatie, RAD, Java, database- en Internet-technologie tot zijn werkterrein. Momenteel is hij werkzaam binnen het Competence Center Internet van ASZ, waar hij als technisch projectleider en medeontwerper verantwoordelijk is voor de ontwikkeling van de Securometer®.

Ing. A. Shahim M.Sc.
Is adviseur bij KPMG EDP Auditors en houdt zich bezig met advisering en projectmanagement op het gebied van informatiebeveiliging, cryptografie en systeemontwikkeling.

W. Barnhoorn
Is geruime tijd werkzaam in de automatisering als projectleider. Als IT security manager bij ASZ is hij verantwoordelijk voor de interne organisatie van informatiebeveiliging en het onderhouden van externe contacten ter zake.

Dr. E.E.O. Roos Lindgreen RE
Is manager bij KPMG EDP Auditors.

De Securometer® verwerkt ingevulde self assessments tot geaggregeerde grafische meerdimensionale overzichten. De status van de getroffen beveiligingsmaatregelen wordt daarbij afzonderlijk weergegeven. Het geïnventariseerde stelsel van beveiligingsmaatregelen kan bovendien worden gerelateerd aan vooraf gestelde kwaliteitsniveaus, waardoor het topmanagement in één oogopslag kan aflezen of de beleidsnormen in voldoende mate worden nageleefd. Ten slotte verschaft de Securometer® inzicht in de progressieve dan wel regressieve ontwikkeling van het niveau van informatiebeveiliging.

In een artikel in een volgende Compact zal worden ingegaan op de ervaringen die in de praktijk met dit hulpmiddel zijn opgedaan.

ASZ	Automatisering Sociale Zekerheid
DNS	Domain Name System
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transaction Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
NFS	Network File System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TPP	Thrusted Third Party
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WWW	World Wide Web

Tabel 1.
Afkortingen.

LITERATUUR

[Bure95] A.M. Buren, *Multimedia nader bekeken*, Compact 1995/2.

[Bure97] A.M. Buren, *Multimedia in open omgevingen, de mogelijkheden van het World Wide Web*, Compact 1997/6.

[OTBI97] Overlegorgaan Technische Beveiligingsstandaarden, OTB-studie Internet, 1997.

[Over97] P.L. Overbeek, *Certificering tegen de Code voor Informatiebeveiliging*, Compact 1997/6.

[Meer97] Drs. B. van der Meer, *Strategisch Plan Securometer®* en *Functioneel Ontwerp Beveiligingsenquête Deelproject 8.7*, 1997.

[Velt95] P. Veltman, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact 1995/3.

Een vertrouwensbasis voor informatie-beveiliging

Certificatie op basis van de Code voor Informatiebeveiliging

Dr.ir. P.L. Overbeek

Een audit op het adequaat toepassen van informatiebeveiliging kan zekerheid geven over de vraag of die beveiliging juist is geïmplementeerd. Zo'n audit kan leiden tot certificeren, waarbij het certificaat weer gebruikt kan worden naar derden om aan te tonen dat men de informatiebeveiliging in de greep heeft. Dit artikel behandelt de wijze waarop aan het certificeringsproces inhoud wordt gegeven.

INLEIDING

Beveiliging van informatie is essentieel voor alle organisaties. Niet alleen vanwege de groeiende afhankelijkheid van die informatie die voor de organisatie zelf geldt, maar ook vanwege het vertrouwen van (elektronische) handelspartners en het publiek. Immers, steeds meer informatie wordt uitgewisseld en is op steeds meer plaatsen toegankelijk. Informatie moet niet alleen nauwkeurig en volledig zijn, maar moet ook op het gewenste moment beschikbaar zijn. En natuurlijk moet de informatie alleen toegankelijk zijn voor degenen die toegang mogen hebben.
Om te voorkomen dat de kwetsbaarheid van de organisatie toeneemt, moet binnen een organisatie een stelsel uniforme spelregels voor de informatiebeveiliging worden gehanteerd. De Code voor Informatiebeveiliging voorziet hierin in de vorm van een managementraamwerk en een evenwichtig stelsel maatregelen die een 'baseline' vormen voor informatiebeveiliging. Veel bedrijven hanteren de Code als uitgangspunt voor hun informatiebeveiliging.

Sinds 1995 hebben bedrijven in Nederland de beschikking over de Code als een praktijkgericht hulpmiddel voor het opzetten van hun maatregelen voor informatiebeveiliging. De Code voor Informatiebeveiliging is de Nederlandse versie van de 'Code of Practice for Information Security Management', British Standard 7799. De Code is gebaseerd op maatregelen die zich bij tal van bedrijven in de praktijk hebben bewezen.
Naast een hulpmiddel om in eigen huis orde op zaken te stellen, geeft de Code voor Informatiebeveiliging ook aan zakenpartners, IT-gebruikers en hun IT-service providers een gemeenschappelijk referentiekader dat kan worden gebruikt als basis voor afspraken over de beveiliging.

Sinds eind 1997 is het mogelijk de beveiliging van een organisatie te laten certificeren door erkende certificatieorganisaties (momenteel KPMG Certification en Kema) op basis van de Code voor Informatiebeveiliging. Het certificatieschema is ontwikkeld door het ICIT (Stichting Instituut voor de bevordering van de keuring en Certificatie van Informatie Technologie), met steun van het Ministerie van Economische Zaken, VNO/NCW, FENIT en toonaangevende bedrijven waaronder IBM, Philips, Shell, AKZO, Unilever, ABN AMRO, RABO en de ING Bank.
De ontwikkeling van dit certificatieschema heeft in nauw overleg plaatsgevonden met partijen in het Verenigd Koninkrijk en enkele Scandinavische landen. Hoewel het ieder land vrij staat eigen schema's te ontwikkelen, is de verwachting dat dit certificatieschema spoedig internationale erkenning zal krijgen.

Certificatie kan een belangrijk managementinstrument zijn voor zowel grote als kleine organisaties. Het certificatieschema is dusdanig opgezet dat certificatie eerder als stimulans wordt ervaren dan als belasting. Daarmee helpt certificatie tevens het niveau van informatiebeveiliging omhoog te brengen.

Dit artikel geeft een indruk van de mogelijkheden van certificatie op basis van de Code voor Informatiebeveiliging om hiermee in eigen huis orde op zaken te stellen en ook de vertrouwensbasis tussen handelspartners te versterken.

ZORG VOOR INFORMATIEBEVEILIGING

Informatiebeveiliging is geen doel op zich, maar staat ten dienste van de bedrijfsbelangen. Informatiebeveiliging zorgt ervoor dat de continuïteit van de organisatie zeker wordt gesteld en dat schade door incidenten wordt beperkt of, waar mogelijk, wordt voorkomen.

Een goede aanpak van de beveiliging maakt het mogelijk optimaal gebruik te maken van informatie en van de steeds groeiende mogelijkheden van informatietechnologie (IT), met een beheersing van de risico's.

Informatiebeveiliging bestrijkt de volgende drie aspecten:
- vertrouwelijkheid: inzage in informatie wordt beheerst;
- integriteit: informatie en software zijn correct, volledig en actueel;
- beschikbaarheid: informatie en -diensten zijn binnen een gewenste tijd beschikbaar.

Een certificaat maakt het bedrijven mogelijk aan derden te laten zien dat zij voldoen aan de Code voor Informatiebeveiliging. Conformiteit met de Code wordt vastgesteld door een door de Raad voor Accreditatie geaccrediteerde certificatieorganisatie. Het schema legt een vertrouwensbasis voor bedrijven en hun klanten bij het zakelijke gebruik van computers en netwerken. Bedrijven worden in staat gesteld publiekelijk uitdrukking te geven aan het feit dat serieuze inspanning wordt verricht op het vlak van informatiebeveiliging. Dit kan leiden tot een intensiever gebruik van IT in het zakelijk verkeer. En dat past goed bij de huidige inspanningen van het bedrijfsleven rond electronic commerce.

In de beveiliging van vandaag vormt de techniek slechts één component.

Groeiende behoefte aan informatiebeveiliging

De behoefte aan informatiebeveiliging groeit sterk. In de eerste plaats vanwege de steeds prominentere rol van informatie in iedere organisatie. Immers, informatie speelt een essentiële rol in vrijwel alle organisatieprocessen: productie, administratie, distributie, ontwikkeling; alle processen 'draaien' op informatie.

Een andere reden voor onze toenemende behoefte aan informatiebeveiliging vormen de veranderingen in de organisatie van het werk. Bedrijven gaan steeds vaker relaties met elkaar aan waarbij bedrijfsinformatie, of computers, mede voor deze derde partijen toegankelijk (moeten) zijn.

Ook de nieuwe technische mogelijkheden brengen nieuwe bedreigingen met zich mee. Informatie wordt op veel meer plaatsen verwerkt dan voorheen. Daardoor is informatie niet langer slechts kwetsbaar in één centrale locatie, maar is deze informatie ook kwetsbaar op de vele laptops, de lokale netwerken en het Internet. Ook is de informatie kwetsbaar door het groeiend aantal plaatsen waar de informatie beschikbaar moet zijn en verwerkt moet kunnen worden: op kantoor, onderweg, bij de klanten en zelfs bij de medewerkers thuis. De mogelijkheden voor blootstelling van de informatie van de organisatie en haar klanten, en van privacygevoelige gegevens nemen hierdoor belangrijk toe.

Deze ontwikkelingen leiden tot een aanzienlijk hoger verwachtingspatroon van wat in redelijkheid aan beveiligingsmaatregelen moet zijn getroffen. Hoe kan aan die hoge verwachtingen tegemoet worden gekomen?

Nieuwe oplossingen

Informatiebeveiliging stond vroeger in feite gelijk aan fysiek beveiligde gebouwen en ruimten. De computers en netwerken bleven daarbinnen, en zo ook de informatie. De toegang tot de informatie werd op deze wijze inderdaad effectief beperkt tot de 'eigen' gebruikers. Een volgende stap was al de afscherming van de nog sporadische verbindingen met de buitenwereld, nog steeds langs de fysieke grenzen, door bijvoorbeeld inbelbeveiliging en firewalls. Deze wijze van beveiliging is echter niet geschikt voor de hierboven beschreven behoefte aan het delen van informatie met partners en het toegankelijk maken van informatie voor de (vaste of flexibele) medewerkers die niet langer gebonden zijn aan een fysieke locatie.

In de beveiliging van vandaag vormt de techniek slechts één component. Beveiliging vraagt een meer evenwichtige benadering waarbij de bijdrage aan de informatiebeveiliging van de componenten mensen, (organisatie)processen en IT opnieuw wordt bezien.

Voor wat de component mensen betreft gaat het hier om aspecten als cultuur en houding ten opzichte van informatiebeveiliging, organisatie van de informatiebeveiliging, taken en verantwoordelijkheden, opleiding en training.

Voor wat betreft de bedrijfs- of organisatieprocessen gaat het hier om aspecten als werkwijzen, procedures en gevolgde standaarden, het 'meten' van de prestaties op beveiligingsgebied en natuurlijk toetsing.

De component IT dient de processen en de mensen te ondersteunen. Daartoe is een realistisch beeld nodig ten aanzien van de (on)mogelijkheden van de techniek op het gebied van software, computers en netwerken.

De IT dient een strategisch hulpmiddel te zijn voor het bereiken van de bedrijfsdoelstellingen. De toegepaste beveiligingsmaatregelen dienen dit doel te ondersteunen en de noodzakelijke waarborgen te geven. Beveiliging mag geen onnodige belemmering vormen bij de uitvoering van werkzaamheden of in de samenwerking met relaties.

De Code voor Informatiebeveiliging geeft bij het opzetten en implementeren van beveiliging een praktisch handvat.

DE CODE VOOR INFORMATIEBEVEILIGING

Informatiebeveiliging vraagt om een stelsel uniforme spelregels. De Code voor Informatiebeveiliging voorziet hierin in de vorm van een managementraamwerk en een evenwichtig stelsel maatregelen die een basisniveau (*baseline*) vormen voor informatiebeveiliging. Veel bedrijven hanteren de Code inmiddels als uitgangspunt voor hun informatiebeveiliging.

De Code voor Informatiebeveiliging is een leidraad voor praktische informatiebeveiliging. In de eerste plaats is het de opzet van de Code in eigen huis orde op zaken te kunnen stellen. De Code verschaft de basis om zelf beveiligingsplannen te ontwikkelen, te implementeren, de uitvoering te 'meten' en bovenal dit geheel goed te managen.

Bovendien is de Code bedoeld als referentiekader, als *gemeenschappelijke* basis, voor (elektronische) zakenpartners. In zaken moet men op elkaar kunnen vertrouwen. Dat geldt ook wanneer organisaties afhankelijk worden van (de beveiliging bij) partners waarmee elektronisch zaken worden gedaan, bijvoorbeeld bij electronic commerce (EDI) of elektronische post.

Door de opkomst van outsourcing neemt bovendien de afhankelijkheid van service providers belangrijk toe. De Code is inmiddels een veelgebruikt referentiedocument tussen zakenpartners onderling (gebruik van de Code in convenanten en interchange agreements) en tussen service providers en hun klanten (gebruik van de Code in service level agreements – SLA's).

Ter versterking van het vertrouwen tussen de partners is het nu mogelijk een uitspraak over het voldoen aan de Code te onderbouwen met een certificaat. KPMG Certification is een van de instanties die een dergelijk certificaat mag afgeven; zij doet dit na uitvoering van een gedegen audit in samenwerking met KPMG EDP Auditors.

Wat is de Code voor Informatiebeveiliging

De Code voor Informatiebeveiliging is een inmiddels breed geaccepteerde samenbundeling van *best practices* voor informatiebeveiliging. De Code steunt op twee principes. Ten eerste zal iedere organisatie die structureel aandacht besteedt aan informatiebeveiliging hier een managementstructuur voor nodig hebben. Dit benadrukt het uitgangspunt dat ook informatiebeveiliging een normale managementtaak is. Ten tweede is er een verzameling maatregelen die men redelijkerwijs mag verwachten in een organisatie. In tabel 1 staan de categorieën waarin deze maatregelen vallen, samengevat. Met de Code kan relatief eenvoudig een evenwichtig pakket maatregelen op maat van de organisatie worden gemaakt, en dat is precies de kracht van de Code.

Niet iedere maatregel uit de Code zal nodig zijn voor iedere organisatie. Anderzijds zullen er organi-

Beveiligingscategorieën	Trefwoorden uit de categorie
Beveiligingsbeleid	Doelstellingen voor informatiebeveiliging vastleggen in het beleidsdocument: beschrijving van de te bereiken of na te streven situatie in termen van de bedrijfsbelangen. Het beleid wordt goedgekeurd en uitgedragen door het management.
Organisatie van de beveiliging	Beveiligingsfuncties, taken en verantwoordelijkheden, coördinatie, samenhang en rapportagelijnen. Verantwoordelijkheid voor afspraken over samenwerking met derden.
Classificatie en beheer van de bedrijfsmiddelen	Overzicht van de bedrijfsmiddelen en hun verantwoordelijke 'eigenaar'. Gebruik van classificatieschema's voor informatie; bijbehorende beveiligingsmaatregelen.
Personeel	Training, security awareness, veilig gedrag op de werkvloer, aannamebeleid en functioneringsbeoordeling. Reageren op en melden van beveiligingsincidenten.
Fysieke beveiliging en omgeving	Beveiliging van en in de infrastructuur. Toegangscontrole bij de poort, fysieke beveiliging van computerruimten en decentrale computers. Clean desk policy. Stroomvoorziening, datacommunicatielijnen, koeling. Bescherming van diskettes, tapes en documentatie.
Computer- en netwerkbeheer	Bedieningsprocedures, beheer van de technische beveiliging en verantwoordelijkheden voor dit beheer. Antivirusmaatregelen, incidentafhandeling en -rapportage, beveiliging bij uitwisseling van gegevens, e-mail, EDI. Kortom: veilige systemen ook veilig *houden*.
Toegangsbeveiliging	Toegangsbeheersing en -autorisatie voor informatiesystemen.
Ontwikkeling en onderhoud van systemen	Aandacht voor de nodige beveiligingsfunctionaliteit en veilige ontwikkel- en onderhoudsmethoden leiden 'zeker' tot veilige systemen, die ook veilig blijven.
Continuïteitsplanning	Calamiteitenopvang, rampenplannen, uitwijk.
Toezicht	Naleving van wettelijke en contractuele voorschriften, beveiligingscontrole op IT-systemen, EDP-audit, interne controle.

Tabel 1.
De tien categorieën van beveiligingsmaatregelen in de Code voor Informatiebeveiliging.

saties zijn die nog specifieke maatregelen toe willen voegen. Het management selecteert dus die maatregelen die van belang zijn voor zijn organisatie en zijn IT-omgeving, afhankelijk van de eisen die het stelt en de risico's.

De tien sleutelmaatregelen vormen een goed vertrekpunt

De eerste stap op weg naar selectie van maatregelen wordt extra eenvoudig gemaakt doordat de Code de zogenaamde sleutelmaatregelen (*key controls*) heeft gedefinieerd. Deze tien maatregelen zijn gebaseerd op essentiële vereisten (bijvoorbeeld voortkomend uit contracten of wettelijke voorschriften) of worden beschouwd als fundamentele bouwstenen voor beveiliging (bijvoorbeeld training en opleiding). Deze tien sleutelmaatregelen vormen samen de basis voor de managementcyclus: planning, implementatie, auditing en bijsturen. De tien sleutelmaatregelen zijn:

- opstellen van een beleidsdocument voor informatiebeveiliging;
- toewijzen van verantwoordelijkheden voor informatiebeveiliging;
- training en opleiding voor informatiebeveiliging;
- rapportage van beveiligingsincidenten;
- antivirusmaatregelen;
- continuïteitsplanning;
- voorkomen van illegaal kopiëren;
- beveiliging van de meest essentiële documenten en registraties;
- naleving van wetgeving, in het bijzonder de Wet Bescherming Persoonsgegevens (privacywet);
- controle op naleving (auditing) van het beveiligingsbeleid.

CERTIFICATIE OP BASIS VAN DE CODE

Een certificaat geeft zowel binnen een organisatie als tussen organisaties meer vertrouwen in de opzet en het bestaan van het managementsysteem voor de informatiebeveiliging en het getroffen stelsel van maatregelen. Het feit dat de Code uitgaat van een managementcyclus en het certificaat alleen geldig blijft bij periodieke controleaudits, rechtvaardigt het vertrouwen dat het beoogde niveau van beveiliging ook *blijvend* wordt geboden.

De 'Eigen vereisten'

Het vertrekpunt wordt gevormd door de 'Eigen vereisten'. Dit is het stelsel normen die door en voor de organisatie zijn afgeleid van de Code voor Informatiebeveiliging, ofwel de Code die op maat gemaakt is voor de eigen organisatie. Het certificatieonderzoek vindt plaats in twee stappen (deze worden later nog in detail toegelicht): het documentatie- en het implementatieonderzoek. In het documentatieonderzoek wordt gevalideerd dat dit normenstelsel inderdaad een juiste en voor de organisatie passende 'vertaling' van de Code vormt. In het implementatieonderzoek wordt onderzocht of de 'Eigen vereisten' daadwerkelijk zijn geïmplementeerd.

Twee sporen en twee niveaus

Het certificatieschema kent verschillende mogelijkheden voor evaluatie en certificatie. Allereerst zijn er twee sporen, namelijk de 'Eigen verklaring' en het 'Certificaat'. Ten tweede zijn er twee niveaus: de 'Basisbeveiliging' en de 'Geavanceerde beveiliging'.

De twee sporen: Eigen verklaring en Certificaat
De *Eigen verklaring* wordt uitgegeven door de organisatie zelf. De Eigen verklaring is een *conformiteitsverklaring* waarin het verantwoordelijke management verklaart te voldoen aan de relevante categorieën uit de Code, zoals gespecificeerd in de 'Eigen vereisten'. De Eigen verklaring wordt uitgegeven op basis van een door de organisatie zelf uitgevoerde interne review, de 'Eigen beoordeling'. De Eigen verklaring wordt geheel onder verantwoordelijkheid van de organisatie zelf uitgegeven. Wel zijn er voorwaarden gesteld aan het proces dat door de organisatie wordt gevolgd bij het uitgeven van deze verklaring. Er zijn geen beperkingen aan deze Eigen verklaring, hoewel de gedachte uiteraard wel is de Eigen verklaring te laten volgen door een echt Certificaat.

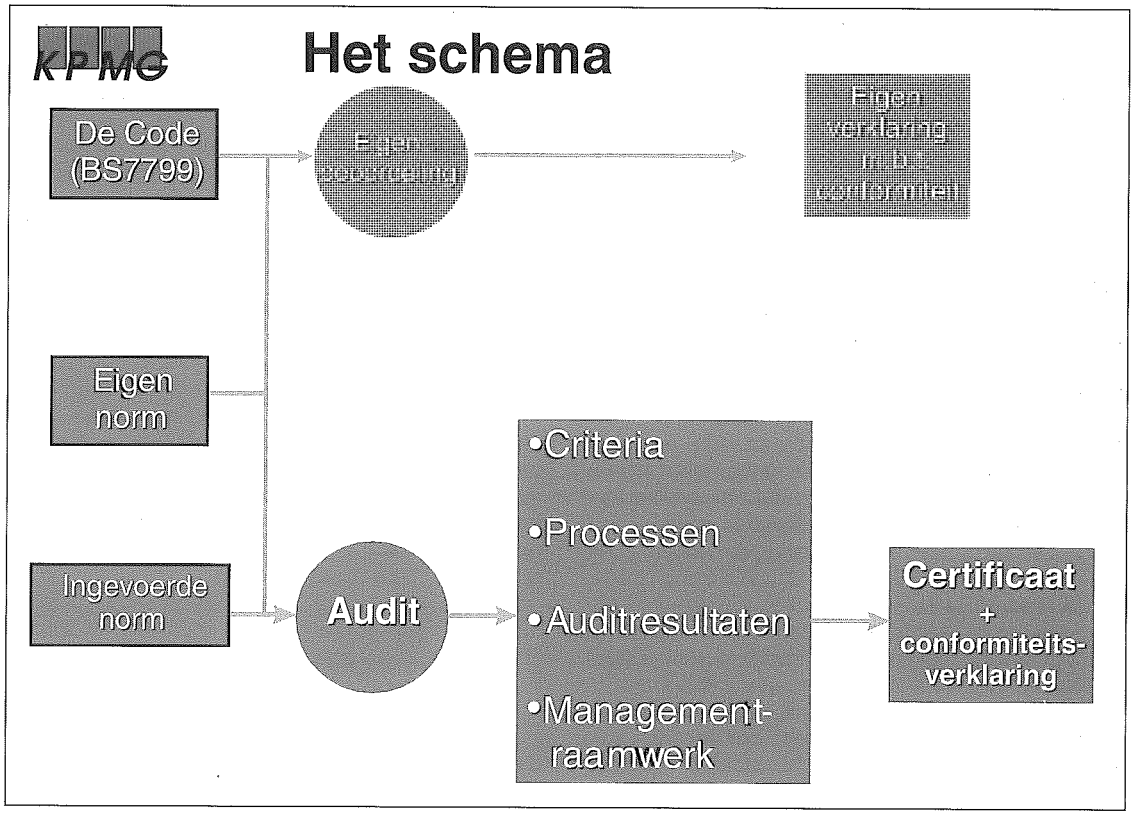
Het *Certificaat* wordt afgegeven door een certificatieorganisatie, die daarvoor is geaccrediteerd door de Raad voor Accreditatie (RvA) en daartoe aan de criteria van de Raad moet voldoen. Het Certificaat wordt afgegeven op basis van een audit van het managementsysteem voor informatiebeveiliging van de organisatie. Ook voor het certificatietraject stelt het management een conformiteitsverklaring op. In het certificatieonderzoek kan, zo de organisatie dit wenst, mede worden gesteund op de zelfbeoordelingen of interne audits die mogelijk reeds binnen de organisatie plaatsvinden. Het (zelf) beoordelen van de naleving van de eigen regels is namelijk een onderdeel van de Code.

Indien het onderzoek positief wordt afgesloten, wordt een Certificaat verleend. Op verzoek van de organisatie wordt het Certificaat vermeld in het openbare register dat het ICIT hiervoor bijhoudt. Het Certificaat heeft een geldigheid van drie jaar. Ieder jaar vindt een controleaudit plaats.

De twee niveaus: Basisbeveiliging en Geavanceerde beveiliging
Het schema onderscheidt twee niveaus, namelijk de Basisbeveiliging en de Geavanceerde beveiliging. Op beide niveaus is zowel een Eigen verklaring als een Certificaat mogelijk.

Voor het niveau *Basisbeveiliging* dient de organisatie ten minste de bekende sleutelmaatregelen (*key controls*) uit de Code te hebben geïmplementeerd. Voor het niveau *Geavanceerde beveiliging* dient de organisatie voor alle maatregelen uit de Code aan te geven welke van toepassing zijn en deze selectie te onderbouwen door middel van een risicoanalyse of vergelijkbare methode.

Het staat organisaties vrij zelf het bij de complexiteit en het ambitieniveau van de organisatie passende niveau te kiezen. Het is bijvoorbeeld goed denkbaar dat kleinere organisaties zullen volstaan met de Basisbeveiliging en nooit zullen doorgroeien naar de Geavanceerde beveiliging.



Figuur 1. Schema voor Eigen verklaring en Certificatie van informatiebeveiliging op basis van de Code voor Informatie-beveiliging (BS7799).

Het groeipad van Eigen verklaring naar Certificaat

Het in figuur 1 weergegeven certificatieschema is opgesteld met de volgende oogmerken:
- het moet inspelen op de behoeften van een breed scala van organisaties, van handel en industrie tot overheden;
- certificatie moet als stimulans worden ervaren en er moet een positieve balans zijn tussen de lusten en de lasten van de certificatie;
- er dient een weg te zijn voor stapsgewijze opbouw naar een geavanceerd niveau bij toenemende volwassenheid van de informatiebeveiliging binnen de organisatie.

Een tweesporenschema, bestaande uit een Eigen verklaring en een Certificaat, gebaseerd op twee niveaus, namelijk Basisbeveiliging en Geavanceerde beveiliging, voldoet aan de genoemde oogmerken.

De Code voor Informatiebeveiliging omvat meer dan honderd maatregelen voor informatiebeveiliging, verdeeld in tien categorieën met daarbinnen 33 doelstellingen. Organisaties met complexe IT-systemen waarin zeer gevoelige of veiligheidskritische gegevens worden verwerkt, zullen mogelijk na analyse tot de vaststelling komen dat alle categorieën, doelstellingen en maatregelen van belang zijn voor hun bedrijfsvoering. Zo nodig kunnen additionele, niet in de Code genoemde doelstellingen en maatregelen aan het stelsel worden toegevoegd. Andere organisaties met wellicht minder gevoelige gegevens kunnen die zaken uit de Code kiezen die passen bij hun bedrijfsproces en beveiligingsbehoeften. Organisaties kunnen eveneens zelf bepalen welke organisatieonderdelen worden betrokken in het beveiligingsbeleid. De afbakening van organisatieonderdelen en geselecteerde categorieën, doelen en maatregelen, alsmede de verantwoording daarvan, wordt vastgelegd in de Conformiteitsverklaring.

Na invoering van het stelsel voor informatiebeveiliging kan de organisatie een eigen beoordeling uitvoeren om zich ervan te verzekeren dat de fysieke, logische en organisatorische maatregelen adequaat functioneren. Als de informatiebeveiliging werd opgezet en geïmplementeerd in overeenstemming met de BS 7799-criteria, kan het management besluiten dit extra te onderstrepen door het uitgeven van een Eigen verklaring. De Eigen verklaring kan in het ICIT-register worden ingeschreven. Hiermee geeft de organisatie publiekelijk uitdrukking aan het feit dat serieuze inspanning werd verricht op het vlak van informatiebeveiliging. Dit kan voordeel bieden uit diverse gezichtspunten: klantvriendelijkheid, concurrentiepositie, versterking van vertrouwen met handelspartners, bescherming van belangen, doeltreffendheid van de eigen processen.

Een volgende stap kan zijn het laten certificeren van het stelsel door een certificatieorganisatie. Het voordeel voor de organisatie ligt vooral in het versterken van het vertrouwen tussen handelspartners en in een betere bescherming van de belangen van klanten.

Het certificatieproces zelf

Indien de organisatie besluit 'op te gaan' voor het Certificaat is de eerste stap in het certificatieproces de aanvraag tot certificatie. De organisatie stelt dan de conformiteitsverklaring op. De certificatie-instelling stelt een auditteam samen met auditors die ten minste vier jaar IT-ervaring hebben en ten minste twee jaar ervaring met informatiebeveiliging. Bovendien moeten de auditors aantoonbare auditerva-

Vast onderdeel van de controleaudit vormt de beoordeling van het 'veranderingsmanagement'.

Dr.ir. P.L. Overbeek
Is Senior manager bij KPMG EDP Auditors te Amstelveen.

ring hebben. Hoewel de audit sterk leunt op de kennis en ervaring van de auditors, is de tweejarige postdoctorale EDP-auditopleiding voor hen niet verplicht. De tweede, optionele, stap is de uitvoering van een proefbeoordeling. Hierin wordt een globale indruk verkregen en wordt een beeld gevormd van de haalbaarheid van een Certificaat. De derde stap is het documentatieonderzoek. In dit onderzoek wordt vastgesteld of de conformiteitsverklaring en de bijbehorende documentatie voldoen aan de gestelde eisen, met name de selectie van categorieën uit de Code met een verantwoording. Indien non-conformiteiten (grote afwijkingen) worden vastgesteld, wordt de audit niet eerder voortgezet dan nadat deze zijn verholpen. De vierde stap is de implementatiebeoordeling. Zoals gezegd zijn hier voor de organisatie en de certificatie-instelling in onderling overleg verschillende benaderingen te kiezen. Indien de organisatie een goede interne managementstructuur kent met goede interne controles of zelfbeoordelingen, bestaat het grootste deel van het werk van de certificatie-instelling uit het beoordelen van deze werkzaamheden. Daarnaast zal de certificatie-instelling ook onafhankelijke waarnemingen uitvoeren (interviews en verwerven van 'evidence'). De verdeling van werkzaamheden tussen organisatie en certificatie-instelling is dus niet vastgelegd, er zijn hier de nodige vrijheidsgraden. De laatste stap is de beslissing tot certificatie. Indien geen non-conformiteiten zijn blijven bestaan en de onvermijdelijke tekortkomingen niet te ernstig zijn, kan het certificaat worden verleend. Bij de eerstvolgende periodieke controleaudit worden uiteraard met name de geconstateerde tekortkomingen opnieuw onder de loep genomen. Vast onderdeel van de controleaudit vormt ook de beoordeling van het 'veranderingsmanagement': zijn de wijzigingen in de organisatie en in de informatiesystemen adequaat beheerst en welke aanpassingen zijn daartoe getroffen in de beveiliging.

Reikwijdte van het Certificaat

De opzet van het certificatieproces op basis van de Code is het vertrouwen tussen de interne en externe partners te bevorderen. Niet meer en niet minder. De werkwijze in het certificatieproces kent een aantal inperkingen. Aangezien een groot deel van de werkzaamheden op steekproeven en door de organisatie door middel van self assessments aangedragen 'evidence' gebaseerd is, is de werkwijze niet bestand tegen boze opzet of fraude. Ook is de beoordeling van de technische implementatie indirect: de uitvoering van de benodigde technische audits wordt geverifieerd en niet de implementatie zelf. Hier zijn aanvullende audits voor nodig. Er is echter wel sprake van een volledige audit, binnen het opgegeven toepassingsgebied. Dit toepassingsgebied wordt vermeld op het certificaat.

Sterk punt is het accent op het managementraamwerk voor informatiebeveiliging: de organisatie stelt van de Code afgeleide normen, implementeert deze, houdt toezicht op de implementatie, stuurt zo nodig de implementatie, en analyseert periodiek of een bijstelling van de normen nodig is.

TOT SLOT

Certificatie op basis van de Code voor Informatiebeveiliging is een relatief nieuwe ontwikkeling. Twee voorheen gescheiden werelden, namelijk die van auditing in de definitie van de EDP-auditing en die van certificatie met de bijbehorende audits in de definitie van de Raad voor Accreditatie, kunnen hier naar elkaar toe groeien. Dat zal ongetwijfeld enige tijd nodig hebben. Het certificatieschema stelt ervaringseisen aan de auditors: ten minste vier jaar IT-ervaring, ten minste twee jaar ervaring met informatiebeveiliging en aantoonbare auditervaring. Hoewel de audit dus sterk leunt op de kennis en ervaring van de auditors, is de postdoctorale EDP-auditopleiding voor hen nog niet verplicht. Toch zou een vaste rol van de EDP-auditor hier van belangrijke betekenis kunnen zijn: het kwaliteitsniveau van de auditor staat dan niet ter discussie, hetgeen ook zijn positieve effecten heeft op de acceptatie van certificatie bij de gebruikers.

EDP AUDITORIUM

ICT-ASPECTEN BIJ DE ACCOUNTANTSCONTROLE VAN DE ROUTINEMATIGE TRANSACTIEVERWERKING

Reactie op het artikel van J.C. Boer RE RA

Prof. J.H. Blokdijk RA

Het artikel van Boer in Compact 1998/3 is mij door een relatie aangereikt; ik moet bekennen dat ik geen regelmatige lezer van Compact meer ben. Ik vond het artikel zeer leesbaar, zelfs nu ik al een poosje wat verder van de accountantscontrolepraktijk afsta. Aan de beginselen van de door Boer behandelde problematiek is in de laatste tien jaren kennelijk niet veel veranderd, want ik kon zijn betoog helemaal volgen. Dat ligt waarschijnlijk aan het door Boer gesignaleerde feit dat er de laatste tijd niet veel aan theorievorming is gedaan. Hij doet een poging daartoe, en vraagt uitdrukkelijk om reacties. Bij dezen!

Ik heb zijn betoog met veel plezier gelezen, en ik vind het ook overtuigend. Eindelijk een analytische theoretische benadering! Vergeten wordt nog wel eens dat de in de tachtiger jaren gepropageerde 'analytische controle', met name ANACONDA, slechts half analytisch was, en wel alleen met betrekking tot de informatie. Ten aanzien van de organisatie was ANACONDA zéér synthetisch, hetgeen bijvoorbeeld leidde tot ellenlange internecontrolevragenlijsten, met vele vragen die eigenlijk niets met de controle van de jaarrekening te maken hadden. Boer gaat uit van de doelstelling van de controle, en vraagt zich af wat daarvoor nodig is; dat is echt analytisch!
Voorts stapt Boer impliciet af van het dogma van de systeemgerichte controle. Immers, de betrouwbare werking van het systeem wordt door de gebruikers doorlopend vastgesteld door gebruikerscontroles; dat zijn informatiecontroles, en dat zijn weer gegevensgerichte controles!
Boer dringt dus door versteende standpunten heen, en gaat weer denken. Daarin wil ik hem graag volgen, maar ik heb nog wat vragen, met name: wat doet de controlerend accountant nu precies?

Boer gaat kennelijk uit van een reeds geïmplementeerd systeem. Dat lijkt mij, zeker als begin van theorievorming, erg praktisch, want de fasen vóór de implementatie laat de controlerend accountant toch meestal aan specialisten over.
Vanuit het gezichtspunt van de controle zijn de kernelementen van een dergelijk systeem: 1) geprogrammeerde controles, die 2) gebruikerscontroles mogelijk maken. Door de gebruikerscontroles wordt de betrouwbaarheid van de werking vastgesteld. Dit alles moet gewaarborgd worden door General Controls, en dat zijn bij een geïmplementeerd systeem 3) de change controls en 4) de logische toegangsbeveiliging.

Wat doet de controlerend accountant hier nu aan, en mee? Allereerst heb ik getracht mij precies voor te stellen wat nu geprogrammeerde controles en wat gebruikerscontroles zijn. Ik heb een piepklein B.V.-tje, en de boekhouding, met een handvol posten per maand, houd ik zelf bij met EXACT. Ik denk dat de geprogrammeerde controles die maatregelen zijn, die mij verhinderen een niet-sluitende memoriaalpost in te geven, en een post niet in een subadministratie te verwerken. Dat blijkt regelmatig heel nuttig, maar het enige effect van een fout is dat ik het systeem niet uit kan; ik krijg geen print-out die zegt: 'Sukkel, nu heb jij alwéér....'. Een dergelijke boodschap kan ik dus ook niet voor mijn accountant bewaren, als ik die al nodig zou hebben. Ik zie dat ook niet als een bezwaar, zelfs niet als accountant. Maar als dit algemene geldigheid zou hebben, dan kunnen wij het reeds in NIvRA-geschrift 13 geïntroduceerde onderscheid tussen geprogrammeerde controles die wel en niet regelmatig tot signalen leiden, naar de schroothoop van de achterhaalde theorie verwijzen. Als het grootboek sluit en de subadministraties aansluiten, is de betrouwbare werking van die geprogrammeerde controles vastgesteld, als wij ten minste de saldibalans en de saldilijsten uit de subadministratie hebben nageteld, maar dat is met auditsoftware geen probleem.
Dan zijn er geprogrammeerde controles die gebruikerscontroles mogelijk maken, en met name de opsporing van boekingen op verkeerde rekeningen. Bij EXACT zijn dat er in elk geval twee: na de invoering van de boekingen kan ik een boekingsverslag krijgen, maar als ik onmiddellijk doorga met de verwerking van de boekingen in het grootboek krijg ik ongevraagd een verwerkingsverslag. Mijn gebruikerscontrole bestaat uit het controleren van het boekingsverslag of het verwerkingsverslag met de bescheiden waarvan ik geboekt heb.
Als degene die de boekingen heeft ingevoerd dat verslag zelf controleert, lijkt mij dit voor de accountant weinig waarde te hebben. Het is al beter als de chef van betrokkene, de (hoofd)boekhouder, deze controle uitvoert en daarvoor parafeert; de accountant kan dan nagaan of dit regelmatig geschiedt. Ook hierbij kan de vraag rijzen of de hoofdboekhouder qua functiescheiding zodanig is geplaatst dat aan deze – vervangbare – interne controle veel waarde kan worden gehecht: vooral bij kleine ondernemingen kan hieraan terecht twijfel bestaan. In dat geval zou de accountant zelf de boekingsverslagen met de bescheiden moeten controleren, maar dan zij wij terug bij de ouderwetse synthetische controle, via de dagboeken. Die is niet echt efficiënt; daarvoor in de plaats hebben wij allang de analytische gegevensgerichte controle uitgevonden. Dan zijn wij terug bij AF! Maar: is dat erg? Met goede auditsoftware moet die controle heel sluw en efficiënt uit te voeren zijn.
Ten aanzien van de volledigheid zijn twee problemen te onderscheiden: 1) boekingen zijn wel ingevoerd, maar daarna niet in het grootboek verwerkt, en 2) boekingen zijn helemaal niet gemaakt. Als boe-

kingen worden ingevoerd, worden in EXACT de boekingsposten automatisch per dagboek doorgenummerd. Uit de boekingsverslagen is dus de doorlopende nummering vast te stellen; hetzelfde geldt voor de verwerkingsverslagen. Maar wie doet dit, intern? Moet de accountant de doorlopende nummering van de memoriaalposten vaststellen, omdat deze het domein van de (hoofd)boekhouder vormen? Het komt mij voor dat ook hier auditsoftware een praktische oplossing kan bieden.
Als boekingen helemaal niet zijn gemaakt, dan is hiervan in het financiële systeem geen spoor te ontdekken. Daarvoor moeten gewone ouderwetse controlemaatregelen worden toegepast, al dan niet door vergelijking met gegevens uit andere systemen.
Misschien moet ten aanzien van het financiële systeem de theorie nog verder uitgesponnen worden; het lijkt mij zinnig daarbij in praktische details af te dalen, omdat daarin meestal de duivel schuilt. Toch lijkt er één conclusie mogelijk: er zijn geen doorslaggevende redenen voor een afzonderlijk onderzoek naar de werking van de interne controle op de gegevensverwerking. Het ongelijk van Boer is dus – gelukkig – nog niet bewezen.

Er zijn echter nog andere systemen, en wel systemen waarin 'transacties worden gegenereerd', zoals de – slechtgekozen – vakterm luidt. Ik denk daarbij aan systemen voor de goederenbeweging inclusief de facturering, aan salarissystemen, en aan het klassieke voorbeeld: het rekening-courantsysteem bij banken, waarin interestberekeningen worden uitgevoerd. De gedachten van Boer zullen op elk van deze soorten systemen afzonderlijk losgelaten moeten worden, waardoor een ander soort typologie van de accountantscontrole kan ontstaan. Zo ver ben ik zelf echter nog niet.

Ten slotte: de algemene waarborgen waarmee de systemen moeten worden omringd, en wel de change controls en de logische toegangsbeveiliging. Ik acht het niet ondenkbaar dat uit een diepgaande en gedetailleerde analyse zou blijken dat het onderzoek door de accountant van de change controls en/of de logische toegangsbeveiliging niet altijd nodig is; dat zal dan afhangen van de inhoud van de gebruikerscontroles. Maar *als* de noodzaak bestaat, dan zal de werking van de interne controle op deze punten moeten worden onderzocht. En dat kan niet met informatiecontrole.
Bij change controls kan het bovendien niet steekproefsgewijs: alle protocollen of soortgelijke goedkeuringsdocumenten zullen moeten worden bekeken, met inbegrip van de documentatie van spoedeisende aanpassingen. Dit lijkt mij ook in een ander opzicht nuttig: de accountant actualiseert zo zijn kennis over 'wat het systeem doet'; dat kan vast geen kwaad.
Met betrekking tot de logische toegangsbeveiliging voel ik mij op wat gladder ijs. In elk geval lijkt het mij wenselijk af en toe de systeembeheerder of een soortgelijke functionaris te vragen om te laten zien wie mutatiebevoegdheid tot een bepaald systeem hebben. Dat heeft ongeveer hetzelfde effect als de standaardbankverklaring ten aanzien van de tekeningsbevoegdheden; kennis daarvan is ook menigmaal nuttig gebleken. Twijfel heb ik aan de haalbaarheid van het volledig napluizen van logs en dergelijke, om incidentele, tijdelijke wijzigingen op te sporen. Als echter de wijziging van een bevoegdheid onder de procedure van de change controls zou vallen, zouden twee vliegen in één klap geslagen kunnen worden.

Al met al vind ik het artikel van Boer een belangwekkende, misschien zelfs historische, aanzet tot een verdere uitbouw van de theorie, op een wijze die ook steun kan bieden aan de praktijk. Ik heb mij niet willen beperken tot veilige kritiek vanuit een pantserwagen; daarmee heb ik wellicht enige onwetendheid op het gebied van de automatisering geëtaleerd. Als dat zo is, moet dat maar blijken uit de verdere discussie. Daar zie ik met belangstelling naar uit!

CUMULATIEF

OVERZICHT VAN EERDER VERSCHENEN ARTIKELEN IN COMPACT

5 23e jaargang 96/5

Corporate governance; de betekenis voor de EDP-auditor
Drs. R.M. Renes RA, prof. dr. P. Wallage RA, J.C. Boer RE RA en ir. J.A.M. Donkers RE

Management control en accountantscontrole – Veranderende inzichten?
Drs. R.M. Renes RA

Het vaststellen van de management-informatiebehoefte; de rol van de tol
Dr. O.C. van Leeuwen RA, drs. R.H.I. van Schoubroeck en drs. P.J.A. Kazius

Management control over informatietechnologie
Ir. J.A.M. Donkers RE, drs. R. Oudega RE en ir. J.A. Verstelle RE

6 23e jaargang 96/6

Een beheersbaar verandertraject voor rekencentrummanagers
P. Teeuwen

Van rekencentrum naar infocentrum
Dr. ing. H.T.M. van der Zee

Informatiebeveiliging in outsourcing-trajecten
H.R.D. Janus, G. Hulst CISA, ing. A. Shahim en dr. E. Roos Lindgreen

Methoden en technieken van logische toegangsbeveiliging
Drs. ing. E. Beijer

Surfen met de AS/400
Drs. R.Ch.T. Ewals RE

Het einde van Halons
G. Doddrell

1 24e jaargang 97/1

Een overzicht van Y2K-problemen
Ir. drs. J. van der Vlugt

Testen en de Millennium-conversie
Drs. T. Koomen en drs. E. Broekman CISA

'2000', een millennium om naar toe te werken
O. Venhuis

2 24e jaargang 97/2

Succesvol selecteren van logistieke standaardpakketten
Drs. E.P.R. van Vroenhoven RE RA

Standaardpakketten in de retail
Drs. ing. S.R.M. van den Biggelaar, drs. J.A.C. van Geel RE en drs. P. Fluitsma

Implementeren van ERP-pakketten is modelleren
Mw. drs. M.E. Koopmans en ir. E. Joustra CPIM

What's in a number? Nummering in een competitieve omgeving
Mr. drs. E.F. Clarkson en prof. mr. dr. J.M. Smits

3 24e jaargang 97/3

Maximaal rendement uit een geïntegreerd standaardpakket
Drs. M.A.A. Jongen, R.L.M. Essers en drs. E.P.R. van Vroenhoven RE RA

IT-trends en ERP-pakketwaarde
Drs. M.J.H. Giesbers RE, dr. G.J. van der Pijl RE en drs. E.P.R. van Vroenhoven RE RA

Pakketmededeling: de vlag moet de lading dekken
Drs. H.E. Sijbring RE RA

Voorschrift Informatiebeveiliging Rijksdienst
Mw. drs. M.C.C. van der Burg RI en J.M.W. van de Garde RE

Audit en beheer van Jaar 2000-projecten
Prof. W. Van Grembergen

4 24e jaargang 97/4
Beheersing van de informatietechnologie in midden- en kleinbedrijf

Typologie van een kleinschalige automatiseringsomgeving
J.C. van Praat RE RA

Beheer en beveiliging van Client/Servers
Ir. drs. J. van der Vlugt

Informatietechnologie en management control in het algemeen en voor het MKB in het bijzonder
E.F. Heck RA, mw. drs. M.J.A. Koedijk RA en mw. W.A. de Munck RA

Elektronisch bankieren in het MKB
Drs. R. Oudega RE en mw. M. Pieper

Certificering van software
Drs. H.G.Th. van Gils RE RA en drs. A.R.J. Basten

5 24e jaargang 97/5

De euro

De accountant en de euro: ontwikkelingen op Europees niveau
Mw. drs. S. Slomp RA

Met de euroanalyse worden onaangename verrassingen voorkomen
Mw. drs. E.C.J. Aendekerk en mw. drs. M.A.G. Runderkamp

Euro: beheersing en de rol van de EDP-auditor
Drs. J.J. van Beek RE RA, mw. S. van der Werve en drs. F.R. Schut

Systemen en mensen: veranderkundige aspecten van de euro-overgang
Ir. A. van Buuren MBA en drs. E.J. Hermans

Euro, Y2K, IT
Ir. drs. J. van der Vlugt

6 24e jaargang 97/6

Ontwikkelomgevingen

Softwaremetingen binnen het Capability Maturity Model
Drs. C.M. Piek

Selectie van CASE-hulpmiddelen: een casebeschrijving
Drs. ing. R.F. Koorn CISA en J.C.J.M. Vrakking

Benchmarking van systeemontwikkeling
Drs. J.C. de Boer, ir. J.A.M. Donkers RE en ir. K.M. Lof

Multimedia in open omgevingen; de mogelijkheden van het World Wide Web
Drs. A.M. Buren

1 25e jaargang 98/1

Platformen

Common Criteria voor evaluatie van beveiliging van IT-producten
Dr. ir. P.L. Overbeek en ir. G.N. Nelemans

Beheer en beveiliging van Unix-omgevingen
Ir. P. Kornelisse RE

NT en (veilig) netwerken
Ir. drs. J. van der Vlugt

Beveiligingsaspecten van Novell NetWare
Drs. M.J. van Beek RE

2 25e jaargang 98/2

Management van informatietechnologie

De EDP-auditor en de veranderende ICT-organisaties
Drs. J.C. de Boer en drs. J.R.M. Vandecasteele

Strategie en informatietechnologie
Drs. M.W. van Aalst en drs. ing. P. Olieman

Inzicht in de kosten van informatietechnologie
Ir. W.J. Neuteboom, mw. ir. E.R. van Sommeren en drs. R.J.J. Weerts

Inzicht in procescontrol
Drs. J.J. van Beek RE RA en drs. A.R.J. Basten

4 25e jaargang 98/3

Accountantscontrole en ICT

Informatie- en communicatietechnologie en accountants: een verstandshuwelijk?
Prof. A.W. Neisingh RE RA

ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking
J.C. Boer RE RA

EDP-auditor en jaarrekeningcontrole van vergaand geautomatiseerde organisaties
W. de Korte RE RA

Het beheersen van risico's op het gebied van informatiebeveiliging: de visie van een klant
Mr. P. van Dijken

Accountantscontrole, COSO en CobiT
Mw. drs. A.J.M. Koopman

4 25e jaargang 98/4

Electronic commerce

Stand van zaken en ontwikkelingen rond electronic commerce
Drs. A.J. Biesheuvel RA RE en drs. C.F. Olde Olthof

Oplossingen voor veilige electronic commerce over Internet
R.L. Moonen

Als u dan hier even wilt tekenen, op de stippellijn? Enkele juridische aspecten van electronic commerce
Mw. mr. A.M.Ch. Kemna MBA

De Trusted Third Party als enabler voor electronic commerce
Mw. mr. drs. A.W. Duthler en mw. mr. M.J. Dontje

Electronic commerce en TTP-dienstverlening, een praktijkvoorbeeld uit de bouwbranche
Ing. J.A.M. Hermans en A. Bruggeman

KPMG EDP Auditors
ten Hagen & Stam Uitgevers