Is er een accountant in de zaal?

Prof. dr. E.E.O. Roos Lindgreen RE en dr. ir. P.L. Overbeek RE

Beveiliging is belangrijk, maar de kwaliteit ervan is weer afhankelijk van andere factoren, zoals de kwaliteit van het beheer van de informatievoorziening. In de praktijk blijkt er vaak nogal wat te schorten aan de kwaliteit van de beveiliging, in het bijzonder op het niveau van de applicatie en van de technische infrastructuur. Welke gevolgen dit heeft voor de jaarrekeningcontrole is geen eenvoudig te beantwoorden vraag.

Dit artikel is mede gebaseerd op de tekst van de oratie ter gelegenheid van de aanvaarding van het hoogleraarsambt door Edo Roos Lindgreen ([Roos02]) en het boek *Informatiebeveiliging onder controle* van beide auteurs ([Over00]).

Inleiding

Het is genoegzaam bekend dat elke organisatie van enige omvang intensief gebruikmaakt van informatietechnologie voor de ondersteuning of zelfs de volledige realisatie van de belangrijkste bedrijfsprocessen en de communicatie met klanten, toeleveranciers, zakenpartners en dergelijke. Niet voor niets wordt wel gesproken van informatiesystemen als het zenuwstelsel van onze economie. Sinds de jaren zeventig heeft menig prominent accountant betoogd dat deze informatiesystemen tijdens de jaarrekeningcontrole moeten worden onderzocht om een uitspraak te kunnen doen over de betrouwbaarheid van de daarin opgeslagen gegevens – die immers de basis vormen voor die jaarrekening – en de effectiviteit van de daarin ingebedde maatregelen op het gebied van administratieve organisatie en interne controle ([Neis99]). Daarbij dient onder meer te worden ingegaan op de risico's die aan de toepassing van informatietechnologie verbonden kunnen zijn en welke maatregelen de onderneming dient te treffen om die risico's te beheersen. Een deel van deze maatregelen wordt tegenwoordig samengevat onder de noemer informatiebeveiliging. Volgens een algemeen aanvaarde definitie wordt met informatiebeveiliging bedoeld: het stelsel van processen dat een organisatie inricht om de vertrouwelijkheid, de betrouwbaarheid en de beschikbaarheid van haar informatie en informatiesystemen te waarborgen. Maar evengoed staat het woord informatiebeveiliging voor een onderwerp dat zich de afgelopen tien jaar heeft ontwikkeld van een obscuur specialisme tot een volwassen vakgebied met eigen opleidingen, eigen standaarden, eigen beroepsorganisaties en eigen literatuur. Een onderwerp ook dat zeer in de belangstelling staat als gevolg van een sterk toenemend aantal incidenten en veel publiciteit daarover. Beveiliging is voor de accountant een belangrijk onderwerp, omdat een goede beveiliging een voorwaarde is voor de betrouwbaarheid van financiële gegevens en de effectiviteit van maatregelen op het gebied van administratieve organisatie en interne controle. Daarnaast kan de beschikbaarheid van deze systemen van invloed zijn op de continuïteit van de bedrijfsvoering.

Een breder pakket

Beveiliging is dus belangrijk, maar dan wel als onderdeel van het veel bredere pakket aan beheersingsmaatregelen dat een onderneming dient te treffen. Die beheersingsmaatregelen kunnen worden geadresseerd aan de hand van de twee hoofdstadia in de levenscyclus van een informatiesysteem: het ontwikkelingsstadium en het productiestadium. In elk van beide stadia is sprake van specifieke risico's en de bijbehorende maatregelen. De accountant dient in de jaarrekeningcontrole dan ook een inventarisatie te maken van lopende ontwikkelingsprojecten en operationele productiesystemen en deze projecten en systemen aan een beknopte risicoanalyse bloot te stellen. Bij zo'n risicoanalyse worden onder meer de volgende vragen beantwoord: Welke systemen en projecten zijn relevant voor de informatie in de jaarrekening? Welke systemen en projecten zijn relevant voor de continuïteit van de onderneming? Hoe groot is het risico dat gegevens in operationele systemen worden gewijzigd of dat het systeem anderszins onbetrouwbare informatie oplevert? Voor de werkelijk risicovolle projecten en systemen kan vervolgens een beoordeling van de getroffen beheersingsmaatregelen plaatsvinden. Die beoordeling kan de accountant in sommige gevallen zelf uitvoeren. In veel gevallen zal hij echter een beroep moeten doen op deskundige derden, zoals IT-auditors. Deze laatste beroepsgroep heeft zich verenigd in de Nederlandse Orde van Register EDP-Auditors (NOREA); de bijna duizend leden van de NOREA zijn onder meer werkzaam bij accountantskantoren, interne accountantsdiensten, automatiseringsbedrijven en adviesbureaus. Door hun lidmaatschap onderwerpen zij zich aan strenge regels ten aanzien van hun deskundigheid, hun gedrag en de uitoefening van hun beroep.

Informatiebeveiliging en standards of due care

Bij het beoordelen van beheersingsmaatregelen maken accountants en IT-auditors steeds vaker gebruik van 'standards of due care': normen, methodieken, richtlijnen en dergelijke die door de markt zelf zijn ontwikkeld en die in de loop der jaren als de-factostandaarden voor het inrichten van dit soort maatregelen zijn gaan gelden.

Een bekend voorbeeld hiervan is de Code voor Informatiebeveiliging ([Code00]). Deze standaard is begin jaren negentig door een groep bedrijven en instellingen ontwikkeld op initiatief van Shell, werd vervolgens tot officiële British Standard geslagen, kreeg ook in Nederland voet aan de grond, werd na zes jaar grondig gerenoveerd en is inmiddels uitgeroepen tot officiële ISO-standaard, nummer 17799 ([ISO01]). De Code beschrijft meer dan honderd beveiligingsmaatregelen die door de opstellers ervan als minimaal noodzakelijk worden beschouwd. De maatregelen zijn ingedeeld in tien hoofdstukken, die gaan over beleid, organisatie, classificatie, personeel, fysieke beveiliging, beheer, logische toegangsbeveiliging, ontwikkeling en onderhoud, continuïteit en toezicht. Veel organisaties hebben de Code gekozen als basis voor het inrichten van hun beveiliging. Zij hebben zonder uitzondering ervaren dat deze standaard niet zomaar kan worden ingevoerd, maar eerst op maat gesneden moet worden. Op dit moment ligt de Code enigszins onder vuur. Canada, Frankrijk en Duitsland hebben bij ISO formeel bezwaar gemaakt tegen de aanvaarding van deze Engelse standaard. Het Amerikaanse National Institute for Standards and Technology (NIST) kwam eind vorig jaar met een officiële publicatie waarin fel van leer wordt getrokken tegen ISO 17799 en waarin en passant de eigen standaarden worden aangeprezen, standaarden die inhoudelijk weinig van de ISO-standaard verschillen ([NIST01]). Deze schermutselingen doen niets af aan het feit dat ISO 17799 een zeer goede en nuttige standaard is, waarmee elke organisatie haar voordeel kan doen.

De Code voor Informatiebeveiliging wordt sinds een aantal jaren ook gebruikt als basis voor certificering. De opzet daarvan is simpel. Een certificerende organisatie voert een documentatieonderzoek en een implementatieonderzoek uit. In het documentatieonderzoek wordt getoetst of de eigen normen die de organisatie hanteert in voldoende mate overeenkomen met de Code voor Informatiebeveiliging; in het implementatieonderzoek wordt onderzocht of de eigen normen ook daadwerkelijk worden nageleefd. Als beide deelonderzoeken een positief resultaat opleveren, draagt de certificerende organisatie het onderzoeksdossier over aan de Raad voor de Accreditatie. De Raad voor de Accreditatie controleert op basis van dit dossier of het onderzoek naar behoren is uitgevoerd. Als dit het geval is, kan het certificaat worden uitgereikt.

Voor sommige organisaties heeft certificering voordelen. Een certificaat is een duidelijk doel, waar naartoe gewerkt kan worden. Het maakt beveiliging tastbaar. Sommige grote organisaties gebruiken certificering als instrument voor het coördineren van interne verbetertrajecten. Voor andere organisaties heeft een certificaat commerciële waarde; zij gebruiken het certificaat om aan te tonen dat de beveiliging op orde is. Hierin schuilt een zeker risico. Een certificaat wil zeggen dat een organisatie op het moment van onderzoek in materiële zin voldoet aan de normen in de Code voor Informatiebeveiliging. Niet meer, maar ook niet minder. We weten dat de normen in de Code voor Informatiebeveiliging samen een minimumniveau voor informatiebeveiliging beschrijven; we weten ook dat die normen niet bepaald spijkerhard zijn en enige ruimte laten voor interpretatie. Hiermee is direct aangegeven welke beperkingen er aan zo'n certificaat verbonden zijn. Wie een certificaat presenteert als het harde bewijs van een waterdichte beveiliging draait zichzelf en anderen een rad voor ogen.

> Certificering op basis van de Code voor Informatiebeveiliging is geen spijkerhard bewijs van waterdichte beveiliging.

Beheren en uitbesteden

In de praktijk blijkt de kwaliteit van de beveiliging sterk afhankelijk te zijn van de kwaliteit van het beheer van de informatievoorziening. Ook hiervoor bestaat een relevante standard of due care: de Information Technology Infrastructure Library (ITIL), een verzameling richtlijnen voor het beheer van informatiesystemen, opgesplitst in modules voor de meest uiteenlopende beheerprocessen, zoals configuratiebeheer, wijzigingsbeheer, probleembeheer en netwerkbeheer ([ITIL02]). Inmiddels zijn er meer dan tachtig modules verschenen. ITIL is een best practice: de procesbeschrijvingen zijn gebaseerd op de manier waarop een groot aantal bedrijven en instellingen het beheer van de informatievoorziening heeft ingericht. ITIL is inmiddels algemeen geaccepteerd en wordt in tal van varianten toegepast. Aan ITIL is twee jaar geleden een belangrijke ontbrekende schakel toegevoegd: de module Security Management, een Nederlands initiatief, gebaseerd op de Code voor Informatiebeveiliging ([ITIL00]). Veel automatiseringsafdelingen en serviceorganisaties werken op dit moment volgens ITIL. Voor de accountant kan een standaard als ITIL van belang zijn omdat de kwaliteit van de beveiliging in de praktijk sterk afhankelijk is van de manier waarop het beheer is ingericht.

Als het beheer van de informatievoorziening is uitbesteed aan een serviceorganisatie – hetgeen tegenwoordig vaak het geval is – kan bij de uitbestedende organisatie, maar ook bij haar accountant behoefte bestaan aan het verkrijgen van zekerheid over de opzet en de werking van de beheersingsmaatregelen bij de serviceorganisatie ([Velt95]). Die zekerheid kan worden geboden door het uitvoeren van een audit. Veel serviceorganisaties hebben meer dan één klant en vinden het niet praktisch om elke klant een eigen audit te laten uitvoeren. In dat geval kan een onderzoek door een onafhankelijke partij uitkomst bieden; dit type onderzoek staat bekend onder de naam third party review. Bij zo'n onderzoek wordt de serviceorganisatie getoetst aan een vooraf overeen te komen normenkader. Het onderzoek resulteert in een mededeling, de zogeheten third-partymededeling, die door de serviceorganisatie aan haar klanten kan worden overgelegd.

De praktijk leert dat het uitvoeren van third party reviews en het verstrekken van de bijbehorende mededelingen nog lang geen volwassen vakgebied is. Kenmerkend voor deze onvolwassenheid is de verwarring rond het begrip third party zelf, waarmee soms de con-

trolerende partij en dan weer de klant van de serviceorganisatie wordt bedoeld. Daarnaast verschillen de gehanteerde normenkaders onderling sterk; ze zijn gebaseerd op varianten van ITIL, op de Code voor Informatiebeveiliging, op eigen normen, of op een combinatie daarvan, en de onderzoeken zelf vinden met verschillende scope en diepgang plaats. Rond third party reviews worden dan ook vaak discussies gevoerd die sterk doen denken aan vergelijkbare discussies in aanpalende vakgebieden. Een terugkerend thema bijvoorbeeld is 'substance over form'. Over het algemeen doet die discussie zich voor als de auditor een formele aanpak heeft gevolgd en netjes alle normen heeft getoetst, afgevinkt en voorzien van scores die samen leiden tot een eindcijfer, maar waarbij de serviceorganisatie het niet eens is met dat cijfer en vindt dat de auditor zich veel te formeel opstelt en te weinig oog heeft voor de dagelijkse praktijk, of waarbij de klant van de serviceorganisatie juist vindt dat de formele aanpak leidt tot een veel te rooskleurig beeld van de werkelijkheid. Het eerste komt overigens vaker voor dan het laatste. Andere discussiepunten hebben betrekking op de scope, de diepgang, de mate van zekerheid, de onderzoeksaspecten en de wijze van rapportage, waarbij de serviceorganisatie doorgaans op het standpunt staat dat zo weinig mogelijk informatie over de interne processen mag worden verstrekt, terwijl de gebruiker van de mededeling wil weten wat er nu precies gecontroleerd is.

Duidelijk is dat de third party review nog wel wat regelgeving kan gebruiken en door zulke regelgeving ook aan kracht zou winnen. In dit verband kan worden gewezen op initiatieven als WebTrust en SysTrust, door de AICPA ontwikkelde standaarden voor het uitvoeren van IT-audits en het verstrekken van mededelingen in zegelvorm, die ook in Nederland ingang vinden en waarbij beveiliging een belangrijke plaats inneemt ([AICP02]).

Beveiliging: de stand van zaken

En daarmee komen we terug op het onderwerp beveiliging. De Delftse hoogleraar Bob Herschberg, in menig opzicht de grondlegger van het vakgebied Informatiebeveiliging in Nederland, testte in de jaren tachtig samen met zijn docenten en studenten de beveiliging van computersystemen bij uiteenlopende bedrijven en instellingen in Nederland. Als verklaard aanhanger van de wetenschapsfilosoof Popper ([Popp59]) stelde hij zich naar eigen zeggen ten doel op empirische gronden de hypothese te verwerpen dat de beveiliging van systemen in orde was. Hoopte Herschberg aanvankelijk wellicht nog dat zijn publicaties ([Hers89]) tot een verbetering zouden leiden, aan het einde van zijn carrière had hij die hoop laten varen. In zijn afscheidsrede schreef hij: 'De doordringbaarheid is totaal. ... Nu mijn emeritaat is ingegaan, kan ik na een half leven omgang met software, mompelen: het is al goed. ... Wie uit de uitspraak 'het is al goed' zou willen lezen dat ik het bestaande goedkeur, is een slecht verstaander. Een goed verstaander hoort met mij al onze software en al onze intiemste gegevens kraken in hun voegen' ([Hers98]). Was Herschberg te somber of had hij gelijk? Laten we, om dit verhaal passend af te ronden, eens kijken naar de wijze waarop informatiebeveiliging in de praktijk vorm krijgt, waarbij wij voor het moment onderscheid maken tussen de beveiliging van de applicatie en de beveiliging van de technische infrastructuur.

Beveiliging van de applicatie

In tegenstelling tot verwachtingen die nog maar tien jaar geleden werden uitgesproken, is het aantal tegelijk in gebruik zijnde applicaties niet afgenomen, maar toegenomen. Naast de centrale, op maat gemaakte 'legacy'-toepassingen uit de vorige eeuw, die vaak nog tot volle tevredenheid worden gebruikt, hebben we nu ook wijdvertakte client-serverapplicaties, ERP-systemen, webomgevingen en kantoorapplicaties. De daarbij gebruikte beveiligingstechnieken hebben de afgelopen tien jaar een snelle ontwikkeling doorgemaakt. Authenticatie en autorisatie blijven daarbij centraal staan. De manier waarop deze essentiële functies in de huidige informatiesystemen invulling krijgen, verschilt opmerkelijk genoeg niet wezenlijk ten opzichte van vroeger.

Neem authenticatie: de gebruiker legitimeert zich met een gebruikersnaam en een wachtwoord, waarna het systeem op basis van een autorisatietabel beslist welke functionaliteit de gebruiker ter beschikking staat. Dat deze aanpak ernstige beperkingen kent, is al lang bekend, maar het mechanisme is kennelijk zo efficiënt en zo algemeen ingeburgerd dat nieuwe technieken bijna geen voet aan de grond krijgen. De laatste tien jaar is zeer veel geïnvesteerd in de ontwikkeling van nieuwe technieken voor authenticatie op basis van digitale certificaten, al dan niet in combinatie met smartcards en biometrie, technieken die razend interessant zijn maar die wij hier niet in detail met u zullen doornemen. Wij volstaan met de constatering dat het gebruik van digitale certificaten nog lang geen gemeengoed is en dat het ook nog jaren zal duren voordat medewerkers, laat staan burgers zich door middel van één of meer digitale certificaten kunnen legitimeren. Dat is misschien maar goed ook; aan het gebruik van digitale certificaten zijn aspecten verbonden die nog niet de aandacht krijgen die zij verdienen, onder andere op het gebied van privacy ([Bran99]) en identiteitsfraude ([Grij99]).

Dan autorisatie. De invoering van ERP-systemen heeft het autorisatievraagstuk zowel lastiger als gemakkelijker gemaakt. Lastiger, omdat het aantal te controleren autorisaties in een centraal opgezette ERP-omgeving kan oplopen tot vele tienduizenden, zodat het inzetten van speciale hulpmiddelen noodzakelijk is; gemakkelijker, omdat de dominantie van een klein aantal leveranciers betekent dat de auditor daarbij steeds dezelfde aanpak kan volgen. De praktijk leert dat de autorisaties in ERP-omgevingen nogal eens afwijken van de formele functiescheidingen waar de accountant op steunt tijdens zijn jaarrekeningcontrole.

Het alomtegenwoordig gebruik van openbare en besloten computernetwerken – al dan niet draadloos – betekent dat bijzondere aandacht moet worden besteed aan de vertrouwelijkheid van de gegevens die over zulke netwerken worden getransporteerd, waaronder wachtwoorden. Versleuteling biedt daarbij uitkomst. De afgelopen jaren is versleuteling uitgegroeid van 'one-off' tot 'commodity'; jarenlang moesten programmeurs zich in allerlei bochten wringen en speciale modules ontwikkelen om versleuteling te kunnen toepassen, maar sinds een

paar jaar kun je de benodigde standaardmodules op basis van standaardprotocollen gewoon van internet halen ([Dier99]). De huidige generatie internetsoftware, maar ook de huidige generatie mobiele apparaten heeft versleuteling dan ook standaard ingebouwd; we gebruiken het elke dag, meestal zonder het te weten.

Ten slotte het wereldomspannend gebruik van kantoorapplicaties. Van alle applicaties is e-mail wel de meest gevoelige. Het versturen van vertrouwelijke documenten via internet is bij de meeste organisaties de gewoonste zaak van de wereld, met alle risico's van dien. E-mail blijkt bovendien een ideaal vehikel voor de verspreiding van virussen, wormen, Trojaanse paarden en andere schadelijke software; virussen staan niet voor niets boven aan de lijst van meest schadelijke beveiligingsincidenten, zowel in aantal als in schadeomvang. Vooral hier wreekt zich de dominantie van een enkele leverancier. Kwetsbaarheden in de producten van zo een leverancier zijn onmiddellijk over de hele wereld bekend. Het exploiteren van deze kwetsbaarheden kan in zeer korte tijd leiden tot een schade die wereldwijd in de miljarden kan lopen. Uit het oogpunt van beveiliging zou een iets grotere diversiteit in onze informatiesystemen geen slechte zaak zijn. Dat geldt ook voor de infrastructuur.

Beveiliging van de technische infrastructuur

Het is geen geheim dat die infrastructuur tegenwoordig bestaat uit een groot aantal componenten, waaronder langdradige en draadloze netwerkverbindingen, servers, routers, printers, intelligente kopieermachines, bureaucomputers, draagbare computers en mobiele telefoons. Al die componenten worden bestuurd door besturingsprogrammatuur waar u de fouten en beveiligingslekken gratis bij krijgt, die doorgaans zijn geconfigureerd op maximaal gebruiksgemak – lees: minimale beveiliging – en die worden geleverd door een zeer klein aantal leveranciers. De componenten van onze infrastructuur zijn dus inherent onveilig; op zich is dit niet zo erg, als we er maar in slagen die onveiligheid te beheersen en tot een aanvaardbaar niveau terug te brengen. Dat dit geen sinecure is, ondervinden organisaties dagelijks aan den lijve, zoals blijkt uit onderstaand voorbeeld.

Een kijkje in de kruipruimte

Een jonge IT-auditor krijgt van zijn collega's van de afdeling Forensic accounting het verzoek in het computernetwerk van een cliënt op zoek te gaan naar de digitale sporen van een fraudezaak. Bij zo'n digitaal sporenonderzoek worden servers, databases en andere op het netwerk aangesloten systemen op specifieke gegevens onderzocht. Omdat het aantal servers in een middelgrote organisatie gemakkelijk in de tientallen kan lopen, is het van belang om voor aanvang van zo'n onderzoek eerst te bepalen welke servers wel en welke servers niet moeten worden onderzocht. De auditor meldt zich hiertoe bij het hoofd van de afdeling die verantwoordelijk is voor het netwerkbeheer. Deze verwijst de auditor door naar twee verantwoordelijke functionarissen die hem precies kunnen vertellen hoe het netwerk eruit ziet: de netwerkbeheerder en de configuratiemanager. De eerste is verantwoordelijk voor het tactisch en operationeel beheer van het netwerk; de tweede is verantwoordelijk voor de registratie van alle zogeheten IT-middelen.

De netwerkbeheerder blijkt een externe functionaris die nog maar net in zijn huidige detacheringsopdracht werkzaam is. Hij verwijst naar 'het netwerkplaatje' dat aan de muur in de rookruimte hangt en door zijn voorganger is opgesteld. Het netwerkplaatje geeft de structuur van het netwerk weer en bevat ook informatie over netwerkadressen, besturingssystemen en aangesloten servers. De auditor maakt een kopie van het schema en meldt zich bij de configuratiemanager. Ook deze functionaris blijkt een externe medewerker die enkele weken geleden is begonnen en zich naar eigen zeggen nog aan het inwerken is. Hij verwijst naar de configuratiedatabase, een bestand met informatie over alle aangeschafte en geïnstalleerde hardware en software; de database bevat voor elk configuratie-item onder meer de datum van aanschaf, de datum van installatie, de huidige locatie, de eigenaar, het serienummer en eventueel een aantal versienummers. Dankbaar maakt onze auditor een uitdraai van de database. Maar als hij op kantoor het eerdergenoemde netwerkschema vergelijkt met de uitdraai van de configuratiedatabase vindt hij meer verschillen dan overeenkomsten: in het netwerkplaatje staan tal van componenten die in de configuratiedatabase niet voorkomen, en omgekeerd.

> Uit het oogpunt van beveiliging zou een iets grotere diversiteit in onze informatiesystemen geen slechte zaak zijn.

Een tweede gesprek met het hoofd van de afdeling levert weinig op en onze auditor besluit het heft in eigen handen te nemen. Op zijn laptop installeert hij een paar simpele beheerprogramma's om het gegevensverkeer op een netwerk te analyseren. Hij sluit zijn laptop aan op het netwerk van de cliënt en volgt een middag lang al het netwerkverkeer. Dat netwerkverkeer bestaat uit kleine pakketjes die behalve de gegevens van de gebruiker – zeg, de tekst van een e-mailbericht – ook netwerkadressen bevatten. De netwerkadressen geven aan van welk systeem een pakketje afkomstig is en ook voor welk systeem het pakketje bestemd is. Op basis van de netwerkadressen krijgt onze auditor langzaam een beeld van het netwerk zoals dat er werkelijk uitziet. Met andere tools probeert hij te achterhalen welke systemen er schuilgaan achter de adressen die hij uit het netwerkverkeer filtert. Na een middag scannen komt de auditor tot de conclusie dat het netwerk vermoedelijk veel omvangrijker en complexer is dan het hoofd van de afdeling, de netwerkbeheerder en de configuratiemanager vermoeden. Niet alleen blijkt uit de scans dat het netwerk veel meer servers en andere systemen bevat dan het netwerkschema en de configuratiedatabase suggereren, maar bovendien dat het netwerk tal van vertakkingen heeft naar andere netwerken. Dit lijkt een nader onderzoek waard. Het hoofd van de afdeling raakt geïnteresseerd en geeft de auditor opdracht het gehele netwerk in kaart te brengen.

Na een maand geeft de auditor een tussenrapportage, met daarin een aantal opmerkelijke bevindingen. Het netwerk bevat een groot aantal servers die nergens geregistreerd staan. Van die servers draait een aantal onder

Prof. dr. E.E.O. Roos Lindgreen RE
is partner bij KPMG Information Risk Management en hoogleraar IT en Auditing aan de Universiteit van Amsterdam. Hij adviseert bedrijfsleven en overheid bij de inzet van informatietechnologie, onder meer op het gebied van beheersing, beveiliging, auditing en kosten.

Dr. ir. P.L. Overbeek RE
is werkzaam als director bij KPMG Information Risk Management en houdt zich onder andere bezig met beveiliging en cryptografie. Tevens doceert hij techniek aan de KUB (TIAS).

besturingssystemen die niet worden ondersteund, noch door de organisatie zelf, noch door enige leverancier. Op een aantal servers is een grote hoeveelheid niet-zakelijk en zelfs illegaal materiaal van zeer recente datum gevonden. In de scans zijn systemen aangetroffen die niet fysiek gelokaliseerd konden worden. Een aantal van deze systemen blijkt zich achter een loos gipswandje in één van de computerruimten te bevinden. Het netwerk heeft vertakkingen met tientallen andere netwerken; sommige van die netwerken blijken toe te behoren aan klanten, toeleveranciers en andere zakenpartners, maar van een aantal andere netwerken kan de eigenaar niet worden vastgesteld. Van vrijwel alle aangesloten systemen blijkt de beveiliging niet te voldoen aan gangbare normen. Dat betekent dat willekeurige gebruikers zich op deze systemen alle rechten kunnen toe-eigenen.

Conclusies

Eén van de conclusies van dit waar gebeurde verhaal is dat informatiebeveiliging voor de accountant heden ten dage van materieel belang is. Materieel, omdat tekortkomingen in de beveiliging kunnen leiden tot materiële fouten in de jaarrekening en de continuïteit van de organisatie kunnen bedreigen. Een andere conclusie is dat de beveiliging van de infrastructuur die de basis vormt voor onze informatiesystemen, vaak materiële gebreken vertoont. Gebreken die hun oorsprong vinden in tekortkomingen in het tactisch en operationeel beheer, waardoor we er niet in slagen de inherente onveiligheid van de componenten van die infrastructuur te beheersen, maar haar juist verergeren. Heeft Herschberg nu al gelijk gekregen? Zoveel kunnen wij niet zeggen. Laten wij het erop houden dat zijn hypothese van totale doordringbaarheid nog niet is verworpen.

En daarmee komen we op een belangrijke vraag in de driehoek informatietechnologie, accountancy en informatiebeveiliging. De vraag is deze: gesteld dat de accountant tijdens de jaarrekeningcontrole voldoende aandacht besteedt aan de toepassing van informatietechnologie, en daarbij constateert dat de functiescheidingen op het niveau van de organisatie wellicht in orde zijn, maar dat zij op het niveau van de applicatie veelal te wensen overlaten, en dat zij op het niveau van de technische infrastructuur meestal eenvoudig doorbroken kunnen worden, wat betekent dit dan voor de accountantsverklaring bij de jaarrekening? Dit is geen gemakkelijke vraag. Wellicht is er een accountant in de zaal die het antwoord weet.

Literatuur

[AICP02]
www.aicpa.org
[Bran99]
S.A. Brands, *Rethinking public key infrastructures and digital certificates – building in privacy*, proefschrift, Technische Universiteit Eindhoven, 1999.
[Code00]
Code voor Informatiebeveiliging, Nederlands Normalisatie-instituut, 2000.
[Dier99]
T. Dierks and C. Allen, *RFC 2246, The TLS protocol, version 1.0*, The Internet Society, 1999.
[Grij99]
J. Grijpink, *Identiteit als kernvraagstuk in een informatiesamenleving*, in: Handboek Fraudepreventie, Samsom, Alphen aan den Rijn 1999, hoofdstuk Fraude en integriteit, nr. E 4010.
[Hers89]
I.S. Herschberg, *The Hacker's Comfort*, Computers & Security, 1989, Vol. 8.
[Hers98]
I.S. Herschberg, *Al Goed*, in: Bewaar Me (eds. H.J. van den Herik en E. Roos Lindgreen), afscheidsrede, Technische Universiteit Delft, 1998, pp. 201-216.
[ISO00]
ISO/IEC 17799:2000, *Code of Practice for Information Security Management*, 2000.
[ITIL00]
ITIL Security Management, The Stationery Office, Office of Government Commerce, 2000.
[ITIL02]
www.itil.co.uk
[Over00]
P.L Overbeek, E. Roos Lindgreen en M. Spruit, *Informatiebeveiliging onder controle*, Pearson Education, Financial Times / Prentice Hall imprint, 2000.
[Neis99]
A.W. Neisingh, *Van automatisering en controle tot IT-audit*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999, pp. 4-8.
[NIST01]
National Institute for Standards and Technology, *International Standard ISO/IEC 17799:2000, Information Security Management, Code of Practice for Information Security Management, Frequently Asked Questions*, December 2001.
[Popp59]
K.R. Popper, *The logic of scientific discovery*, Unwin Hyman, 1959.
[Roos02]
E. Roos Lindgreen, *Over informatietechnologie, accountancy en informatiebeveiliging*, oratie, Vossiuspers/AUP, 2002.
[Velt95]
P. Veltman, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact, herfst 1995.