De accountant en de kruipruimte

Hoe relevant is informatiebeveiliging voor de accountantscontrole?

Edo Roos Lindgreen, Paul Overbeek en Ruben de Wolf

SAMENVATTING De intensieve toepassing van informatietechnologie door bedrijven en instellingen heeft niet alleen voordelen, maar brengt ook risico's met zich mee. In dit artikel gaan de auteurs in op enkele verborgen risico's van informatietechnologie. Zij gunnen de lezer daarbij een blik in de kruipruimte van onze informatiesystemen. De situatie die daar wordt aangetroffen, kan het daglicht niet altijd verdragen. Wat betekent dit voor de accountantscontrole?

1 Inleiding

Ach, informatietechnologie. Wat valt hierover nog te zeggen? Elke accountant weet zo langzamerhand wel dat bedrijven en instellingen intensief gebruikmaken van informatietechnologie: voor het invoeren van orders, het vastleggen van transacties, het bijhouden van klantgegevens, het beheren van voorraden, het sturen van facturen, het communiceren met klanten en natuurlijk voor de boekhouding. En elke accountant weet dat geautomatiseerde informatiesystemen het zenuwstelsel vormen van onze economie, die al jaren vergaand gedigitaliseerd is. Ook in de Richtlijnen voor de Accountantscontrole (NIVRA, 2002) wordt het belang van informatietechnologie onderkend. Richtlijn 401 geeft expliciete aanwijzingen voor het uitvoeren van een controle in een omgeving waarin gebruik wordt gemaakt van geautomatiseerde informatiesystemen.

Prof. Dr. E.E.O. Roos Lindgreen RE is partner bij KPMG en hoogleraar IT & Auditing bij de Postdoctorale Opleiding Accountancy aan de Universiteit van Amsterdam.
Dr. Ir. P.L. Overbeek RE is director bij KPMG en docent bij de TIAS EDP-Audit opleiding aan de Universiteit van Tilburg.
Ir. R. de Wolf RE is manager bij KPMG en docent bij de Postdoctorale EDP-Audit opleiding aan de Vrije Universiteit.

Sinds de jaren zeventig betogen vooraanstaande accountants dat hun vakbroeders de informatiesystemen van hun opdrachtgevers grondig zouden moeten onderzoeken om een uitspraak te kunnen doen over de betrouwbaarheid van de daarin opgeslagen gegevens – die immers de basis vormen voor de jaarrekening – en over de effectiviteit van de in die systemen ingebedde maatregelen op het gebied van administratieve organisatie en interne controle (Neisingh, 1999). De accountant zou daarbij scherp moeten letten op de risico's die het gebruik van informatietechnologie met zich meebrengt en naar de maatregelen die zijn opdrachtgever heeft getroffen om deze risico's te beheersen. Een deel van deze beheersingsmaatregelen wordt tegenwoordig samengevat onder de noemer informatiebeveiliging. In dit artikel gaan wij in op enkele verborgen risico's van informatietechnologie en op de relevantie van informatiebeveiliging voor de accountant. Aan de orde komen achtereenvolgens: informatiebeveiliging (paragraaf 2), de Code voor Informatiebeveiliging (paragraaf 3), beheer en uitbesteden van de informatievoorziening (paragraaf 4) en ten slotte de huidige situatie in de praktijk (paragraaf 5). Die situatie is voor de accountant zo relevant, dat aan de Universiteit van Amsterdam een onderzoek is gestart naar de kwaliteit van de beveiliging van de technische infrastructuur bij bedrijven en instellingen in Nederland.

2 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 (Overbeek, Roos Lindgreen en Spruit, 2000). Maar tegelijk staat het woord informatiebeveiliging voor een onderwerp dat zich de afgelopen tien jaar heeft ontwikkeld van een obscuur specialisme tot een

min of meer volwassen vakgebied met eigen opleidingen, eigen standaarden, eigen beroepsorganisaties en eigen literatuur. Een onderwerp ook dat zeer in de belangstelling staat door de vele beveiligingsincidenten en alle publiciteit daarover, van virusuitbarstingen tot al dan niet geslaagde inbraakpogingen.
Informatiebeveiliging is voor de accountant een relevant onderwerp. Een goede beveiliging is immers een noodzakelijke voorwaarde voor het waarborgen van de betrouwbaarheid van financiële gegevens en de effectiviteit van maatregelen op het gebied van administratieve organisatie en interne controle. Daarnaast is een goede beveiliging nodig om de beschikbaarheid van kritische informatiesystemen – en daarmee de continuïteit van de bedrijfsvoering – te waarborgen.
Informatiebeveiliging staat niet op zichzelf. Het maakt deel uit van een breed pakket aan maatregelen voor het beheersen van risico's die met informatietechnologie te maken hebben. Het kan zinvol zijn om bij het in kaart brengen van deze risico's onderscheid te maken tussen 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 specifieke beheersingsmaatregelen. De risico's die optreden in het ontwikkelingsstadium zijn vooral van belang voor de onderneming zelf en liggen primair op het vlak van efficiency: slechts één op de vier automatiseringstrajecten wordt binnen de begroting uitgevoerd en resulteert in een informatiesysteem dat werkt volgens de specificaties. De accountant zal zich bij een ontwikkelingstraject hooguit zorgen maken over de activering van het opgeleverde systeem of onderdelen daarvan, en wellicht ook nog over mogelijke gevolgen voor de continuïteit van de onderneming als het project mislukt. Voor de accountant zijn toch vooral de risico's in het productiestadium van een informatiesysteem van belang. Deze risico's kunnen de accountantscontrole direct raken; zij worden gedeeltelijk genoemd in artikel 7 van Richtlijn 401, en bestaan onder meer uit het ontbreken van vastleggingen van transacties, het ontbreken van functiescheidingen, het optreden van fouten en onjuistheden en het bedreigen van de continuïteit van de organisatie (NIVRA, 2002).
Eigenlijk zou de accountant jaarlijks een inventarisatie moeten maken van lopende ontwikkelingsprojecten en operationele systemen bij zijn opdrachtgever, om deze projecten en systemen vervolgens aan een beknopte risicoanalyse te onderwerpen. Daarbij zouden ten minste de volgende vragen aan de orde moeten komen: Welke projecten en systemen zijn relevant voor de jaarrekening? Welke projecten en systemen 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? Wat betekent dit voor de posten in de jaarrekening? Voor de werkelijk risicovolle projecten en systemen kan de accountant vervolgens een beoordeling van de getroffen beheersingsmaatregelen uitvoeren. In een aantal gevallen zal de accountant daarbij een beroep doen op deskundige derden, zoals IT-auditors. Deze laatste beroepsgroep heeft zich verenigd in de Nederlandse Orde van Register EDP-Auditors (NOREA); de ruim 1000 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.

3 De Code voor Informatiebeveiliging

Bij het beoordelen van beheersingsmaatregelen maken accountants en IT-auditors steeds vaker gebruik van 'standards of due care': normen, methodieken en richtlijnen die door de markt zelf zijn ontwikkeld en die in de loop der jaren als de-facto-standaarden voor het inrichten van dit soort maatregelen zijn gaan gelden.
Een bekend voorbeeld hiervan is de Code voor Informatiebeveiliging (NEN, 2000). 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 (ISO, 2001). 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 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 (NIST, 2001). Deze schermutselingen doen niets af aan het feit dat ISO 17799 een nuttige standaard is, waarmee elke organisatie en elke accountant zijn 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 kan worden gewerkt. 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. De normen in de Code voor Informatiebeveiliging beschrijven samen een minimumniveau voor informatiebeveiliging; zij zijn echter niet spijkerhard en laten behoorlijk wat ruimte 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.

4 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 – configuratiebeheer, wijzigingsbeheer, probleembeheer, netwerkbeheer enzovoort (ITIL, 2003). 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 uitgegeven door de Engelse overheid, is inmiddels algemeen geaccepteerd in het Verenigd Koninkrijk en Nederland en wordt in tal van varianten toegepast. Aan ITIL is enkele jaren geleden een belangrijke ontbrekende schakel toegevoegd: de module Security Management, een Nederlands initiatief, gebaseerd op de Code voor Informatiebeveiliging (ITIL, 2000). Veel automatiseringsafdelingen en serviceorganisaties werken op dit moment volgens ITIL.
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 diens accountant behoefte bestaan aan het verkrijgen van zekerheid over de opzet en de werking van de beheersingsmaatregelen bij de serviceorganisatie (Veltman, 1995). Richtlijn 402 geeft expliciete aanwijzingen voor accountants waarvan de opdrachtgever gebruikmaakt van een serviceorganisatie (NIVRA, 2002). De gevraagde zekerheid kan worden geboden door het uitvoeren van een IT-audit. Veel serviceorganisaties hebben tientallen klanten en vinden het niet wenselijk om elke klant een eigen IT-audit te laten uitvoeren. In dat geval kan een onderzoek door een onafhankelijke partij uitkomst bieden, bijvoorbeeld door de accountant van de serviceorganisatie; 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-party-mededeling, die door de serviceorganisatie aan haar klanten kan worden overlegd. 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, afhankelijk van de kringen waarin men verkeert, soms de controlerende 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, 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 het American Institute of Certified Public Accountants (AICPA) ontwikkelde standaarden voor het uitvoeren van IT-audits en het verstrekken van mededelingen in zegelvorm die ook in Nederland beperkte ingang vinden en waarbij beveiliging een belangrijke plaats inneemt (AICPA, 2003).

5 Informatiebeveiliging in de praktijk

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. Als verklaard aanhanger van de wetenschapsfilosoof Karl Popper (Popper, 1959) 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 (Herschberg, 1989) 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' (Herschberg, 1998). 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 toepassingsprogrammatuur en de beveiliging van de technische infrastructuur.

Over de beveiliging van onze toepassingsprogrammatuur kunnen we kort zijn: die is al dertig jaar min of meer onveranderd. Goed, we beschikken naast onze oude, centrale, op maat gemaakte toepassingen uit de vorige eeuw – die vaak nog tot volle tevredenheid worden gebruikt – nu ook over wereldwijde hypermoderne ERP-systemen met geavanceerde webinterfaces, maar de manier waarop authenticatie en autorisatie geregeld worden, verschilt niet wezenlijk ten opzichte van vroeger: de gebruiker legitimeert zich nog altijd met een gebruikersnaam en een wachtwoord, waarna het systeem op basis van een autorisatietabel beslist welke functionaliteit de gebruiker ter beschikking staat. Dat aan het gebruik van wachtwoorden nogal wat nadelen kleven, 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. 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 een 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 (Brands, 1999) en identiteitsfraude (Grijpink, 1999).

Ook autorisatie is niet wezenlijk anders dan vroeger. De invoering van ERP-systemen heeft het autorisatievraagstuk zowel lastiger als gemakkelijker gemaakt. Lastiger, omdat het aantal autorisaties in een centraal opgezette ERP-omgeving kan oplopen tot vele tienduizenden, zodat bedrijven speciale hulpmiddelen moeten inzetten om die autorisaties te beheren en te controleren; gemakkelijker, omdat de dominantie van een klein aantal leveranciers betekent dat deze bedrijven daarbij steeds dezelfde aanpak kunnen volgen. Maar een heidens karwei blijft het, en de praktijk leert dat de autorisaties in grootschalige informatiesystemen nogal eens afwijken van de formele functiescheidingen

waar de accountant tijdens zijn controle op denkt te kunnen steunen.
Dan de technische infrastructuur. Met deze term worden de technische componenten bedoeld waaruit onze informatiesystemen zijn opgebouwd: servers, databases, PC's, laptops, schijven, taperobots, draadloze en langdradige netwerkverbindingen, routers, switches en allerlei andere apparaten. De technische infrastructuur is te beschouwen als de kruipruimte van onze informatiesystemen. Maar wat heeft die kruipruimte nu te maken met accountantscontrole? Meer dan u denkt, zoals blijkt uit onderstaand voorbeeld (Roos Lindgreen, 2002).

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 opdrachtgever 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 detacheringopdracht 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 eerder genoemde 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. 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 opdrachtgever 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 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 computerruimtes 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 personen zich op deze systemen eenvoudig alle rechten kunnen toe-eigenen en daarmee kunnen beschikken over alle vertrouwelijke bedrijfsgegevens, elke functiescheiding kunnen doorbreken en de systemen naar wens voor langere tijd kunnen uitschakelen…

6 Conclusies

Bovenstaand voorbeeld is met zorg gekozen. Maar is het ook representatief? Laten wij eens aannemen van wel. Onze eigen praktijkervaringen geven in elk geval geen directe aanleiding om die aanname in twijfel te trekken.

De eerste conclusie zou dan zijn dat informatiebeveiliging voor de accountant heden ten dage van materieel belang is. Materieel, omdat tekortkomingen in de beveiliging de betrouwbaarheid en vertrouwelijkheid van gevoelige gegevens, de binnen de organisatie gedefinieerde functiescheidingen en zelfs de continuïteit van de organisatie in gevaar kunnen brengen. Een beoordeling van de beveiliging van informatie en informatiesystemen zou dan, om deze reden, een verplicht bestanddeel van nagenoeg elke accountantscontrole moeten zijn.

Een tweede conclusie zou zijn dat de beveiliging van het fundament van onze informatiesystemen nogal eens materiële gebreken vertoont; gebreken die hun oorsprong vinden in tekortkomingen in het tactisch en operationeel beheer, waardoor we er niet in slagen de inherente kwetsbaarheid van de componenten in die infrastructuur te beheersen, maar haar juist verergeren. Heeft Herschberg nu al gelijk gekregen? Zoveel kunnen wij niet zeggen. Laten wij het er op houden dat zijn hypothese van totale doordringbaarheid nog niet is verworpen.

En daarmee komen we op de slotvraag van dit artikel. De vraag is deze: als de accountant constateert dat de functiescheidingen op het niveau van de organisatie in orde zijn, maar dat zij op het niveau van de applicatie nog te wensen overlaten, en dat zij op het niveau van de technische infrastructuur eenvoudig doorbroken kunnen worden, wat betekent dit dan voor de accountantscontrole? Deze vraag is niet eenvoudig te beantwoorden. Het ligt voor de hand te stellen dat de accountant in dat geval meer gegevensgerichte werkzaamheden dient uit te voeren. Maar hiermee is de vraag nog niet beantwoord. De bestanden die de accountant in het kader van zijn gegevensgerichte werkzaamheden analyseert om zo aanvullende controle-informatie te verkrijgen, bevinden zich immers mogelijk in dezelfde onveilige infrastructuur en kunnen dus niet zonder meer als betrouwbaar worden aangemerkt. Hoe met dit probleem moet worden omgegaan, verdient naar onze mening een bredere discussie. In elk geval lijkt de kwaliteit van de beveiliging van de technische infrastructuur bij bedrijven en instellingen in Nederland een nader onderzoek waard. Aan de Universiteit van Amsterdam is zo'n onderzoek inmiddels gestart; wij hopen de lezer hierover op korte termijn nader te kunnen informeren. ■

Literatuur

AICPA, (2003), www.aicpa.org, on-line informatie over Webtrust en Systrust.

Brands, S.A., (1999), *Rethinking public key infrastructures and digital certificates – building in privacy*, proefschrift, Technische Universiteit Eindhoven.

NEN, (2000), Code voor Informatiebeveiliging.

Grijpink, J., (1999), Identiteit als kernvraagstuk in een informatiesamenleving, in: *Handboek Fraudepreventie*, Samson, Alphen aan den Rijn, hoofdstuk Fraude en integriteit, nr. E 4010.

Herschberg, I.S., (1989), The Hacker's Comfort, in: *Computers & Security,* Vol. 8, pp. 168-183.

Herschberg, I.S., (1998), Al Goed, in: *Bewaar Me* (red. H.J. van den Herik en E. Roos Lindgreen), afscheidsrede, Technische Universiteit Delft, pp. 201-216.

ISO, (2000), ISO/IEC 17799:2000, *Code of Practice for Information Security Management.*

ITIL, (2003), www.itil.co.uk.

ITIL, (2000), *ITIL Security Management*, The Stationery Office, Office of Government Commerce.

Overbeek, P.L., E. Roos Lindgreen en M. Spruit, (2000), *Informatiebeveiliging onder controle,* Pearson Education, Financial Times / Prentice Hall imprint.

Neisingh, A.W., (1999), Van automatisering en controle tot IT-audit, in: *Compact ICT en Auditing*, Neisingh et. al. (red.), pp. 4-8.

NIST, (2001), 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.*

Popper, K.R., (1959), *The logic of scientific discovery*, Unwin Hyman.

NIVRA, (2002), *Richtlijnen voor de Accountantscontrole,* Koninklijk NIVRA, Amsterdam.

Roos Lindgreen, E., (2002), *Over informatietechnologie, accountancy en informatiebeveiliging,* oratie, Vossiuspers / AUP.

Veltman, P., (1995) Third-party-review en -mededeling bij uitbesteding van IT-services, in: *Compact*, september, pp. 14-23.