Over informatietechnologie, accountancy en informatiebeveiliging

Vossiuspers UvA is een imprint van Amsterdam University Press.
Deze uitgave is totstandgekomen onder auspiciën van de Universiteit van Amsterdam.

Omslag: Colorscan, Voorhout
Opmaak: JAPES, Amsterdam
Foto omslag: Carmen Freudenthal, Amsterdam

ISBN 90 5629 258 7
©Vossiuspers UvA, Amsterdam, 2002

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voorzover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j° het Besluit van 20 juni 1974, St.b. 351, zoals gewijzigd bij het Besluit van 23 augustus 1985, St.b. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 882, 1180 AW Amstelveen). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

Over informatietechnologie, accountancy en informatiebeveiliging

Rede

Uitgesproken bij de aanvaarding van het ambt
van hoogleraar IT en Auditing
aan de Universiteit van Amsterdam
op woensdag 16 oktober 2002

door

Edo Roos Lindgreen

Vossiuspers UvA

Mijnheer de rector magnificus,
Geachte aanwezigen,

Het nu volgende verhaal gaat over informatietechnologie, accountancy en informatiebeveiliging – drie onderwerpen die op het eerste gezicht weinig met elkaar van doen hebben, maar schijn bedriegt, en ik zal u vandaag vertellen waarom. Laten we eerst teruggaan naar een periode die voor elk van deze onderwerpen van bepalend belang is geweest. Het is een periode die al lang achter ons lijkt te liggen.

Een blik terug

We bevinden ons in de tweede helft van de jaren negentig van de twintigste eeuw. De gouden jaren, worden ze wel genoemd. En gouden jaren zijn het: voor huiseigenaren, voor beleggers, en vooral voor leveranciers van informatietechnologie, het eerste onderwerp van dit verhaal. De economie draait op volle toeren. Ondernemingen investeren miljarden in informatiesystemen voor toepassingen met klinkende namen als *workflow management*, *enterprise resource planning* en *e-business*. Het vermeende millenniumprobleem en de komst van de euro leiden alleen al in Nederland tot extra investeringen van tientallen miljarden guldens voor het aanpassen, repareren en versneld vervangen van informatiesystemen. De opkomst van internet is aanleiding voor het ontstaan van een geheel nieuwe bedrijfstak, waar kleine bedrijfjes met geinige ideetjes tientallen miljoenen guldens aan durfkapitaal kunnen krijgen van financiers die hun investering zowaar dubbel en dwars terugverdienen als ze diezelfde bedrijfjes naar de beurs brengen en daarbij een enorme koerswinst incasseren. De aandelenkoersen van bedrijven die iets met internet, telecommunicatie of informatietechnologie te maken hebben, stijgen tot niet eerder vertoonde hoogten.

Met de accountancy, ons tweede onderwerp, gaat het intussen ook niet slecht. Kleine en grote accountantskantoren groeien mee op het tij van de hoogconjunctuur. Fusies zijn aan de orde van de dag – ook in de accountancy zelf, waar grote kantoren kleine kantoren overnemen en de *big six*, zoals de zes grootste accountantskantoren worden genoemd, overgaan in de *big five*. Accountants genieten een hoog maatschappelijk aanzien. De naam van een groot accountantskantoor is voor velen voldoende om aan verklaringen, onderzoeksrapporten en andere documenten een universeel waarheidsgehalte toe te dichten. Op verzoek van hun veeleisende en snel groeiende klantenkring breiden de accountantskantoren hun dienstenaanbod in hoog tempo uit met diensten als managementadvies, financieel advies, forensisch accountantsonderzoek, milieucertificering of de implementatie van grote softwarepakketten. Het gaat de accountant voor de wind en de wereld mag het weten.

Ook voor het derde onderwerp van dit verhaal, informatiebeveiliging, zijn het bijzondere tijden. Bedrijven en instellingen worden geconfronteerd met een toenemend aantal incidenten die mogelijk worden gemaakt door gebreken in de beveiliging van hun informatiesystemen.[1] Virussen en andere kwaadaardige programma's duiken in steeds weer andere gedaanten op; zij nestelen zich in onschuldig ogende bestanden, verspreiden zichzelf via elektronische post, vernietigen gegevens en richten voor miljarden euro's schade aan. Het aantal gevallen van diefstal en verlies van draagbare computers en de informatie die zich daarop bevindt, stijgt zo snel dat verzekeraars zich genoodzaakt zien speciale maatregelen te treffen. Jonge hackers breken in op websites van internetwinkels en bemachtigen daarbij honderdduizenden creditcardnummers die zij op internet publiceren. Websites van grote ondernemingen zijn het slachtoffer van *distributed denial of service*-aanvallen, waarbij een aanvaller eerst met behulp van geautomatiseerde scripts een groot aantal slecht beveiligde computers binnendringt – liefst bij universiteiten, want die zijn het gemakkelijkst te kraken – en die computers daarna voorziet van speciale aanvalsprogrammatuur. Vervolgens lanceren de aldus geprepareerde computers – soms gaat het om duizenden systemen – onder regie van de aanvaller een massale, georkestreerde aanval op een website om die zo snel mogelijk uit te schakelen.

Er gaat geen week voorbij zonder dit soort beveiligingsincidenten, die vaak breed in de pers worden uitgemeten. Het zijn tastbare symptomen van de toenemende kwetsbaarheid van onze informatiemaatschappij.[2] Toch leiden al deze symptomen, in tegenstelling tot achteraf gezien minder reële dreigingen zoals het millenniumprobleem, in de praktijk zelden tot daadkrachtig ingrijpen door managers,

laat staan door leveranciers. Is het omdat iedereen het te druk heeft met investeren en innoveren? Of is het de zorgeloosheid die lijkt te horen bij een bruisende economie en aandelenkoersen die alleen maar stijgen? Feit is dat informatiebeveiliging ondanks alle incidenten aan het eind van de jaren negentig geen prominent agendapunt is, of zoals een manager bij een grote semi-overheidsinstelling met de gegevens van ten minste tien miljoen Nederlanders in de databases ten overstaan van zijn voltallige management team glimlachend bevestigt: beveiliging heeft wel de aandacht, maar geen prioriteit.

Kortom, het is een bloeiende, zorgeloze periode; maar aan alles komt een eind, en deze periode eindigt met drie gebeurtenissen die elk een keerpunt vormen voor de drie onderwerpen van dit verhaal.

De eerste van deze gebeurtenissen vindt plaats in het voorjaar van het jaar 2000. Niet het gevreesde millenniumprobleem, maar het alom gevierde internet zorgt voor een wezenlijke verandering van het klimaat in de informatietechnologiesector. Na een reeks negatieve berichten over de resultaten en perspectieven van de dotcomsector verliezen beleggers het vertrouwen in de nieuwe economie en nemen afstand van hun aandelen. Scherpe koersdalingen zijn het gevolg. In de maanden daarna volgen internetbedrijven, informatietechnologieleveranciers, telecommunicatiebedrijven en financiële instellingen. De economie begint te stagneren. Investeringen in informatietechnologie nemen sterk af. Leveranciers en dienstverleners zien hun omzet dalen en zijn gedwongen een groot aantal werknemers te ontslaan. Informatietechnologie, eerder geprezen als bron van innovatie en motor achter de economische groei, verliest zijn glans en wordt weer gewoon een productiemiddel waarvan de baten moeten opwegen tegen de kosten.

De tweede gebeurtenis vindt plaats in het najaar van 2001. Malversaties door het management van energiegigant Enron leiden uiteindelijk tot het faillissement van deze voormalige beurslieveling. De accountant van Enron, het gerenommeerde kantoor Andersen, wordt na vermeende obstructie van de rechtsgang door het vernietigen van dossiers meegesleurd in de val van het energiebedrijf. De *big five* worden gereduceerd tot de *final four*, zoals de grote accountantskantoren na het gebeurde optimistisch worden genoemd. Na Enron komen meer boekhoudschandalen aan het licht; zij brengen in de zomer van 2002 een wereldwijde daling van de aandelenkoersen teweeg. De accountant, eerder geprezen als de onfeilbare rekenmeester en het financieel geweten van de top van het zakenleven, geniet niet langer het van-

zelfsprekende vertrouwen van de rest van de samenleving. Ook de serieuze pers spreekt van een crisis in de accountancy.[3]

De derde gebeurtenis vindt plaats op 11 september 2001: de terreuraanslag op het World Trade Center in New York. Ik volsta hier met de opmerking dat het maatschappelijk gevoel van onveiligheid en van de prijs die de maatschappij lijkt te willen betalen om die veiligheid te verbeteren na de aanslag sterk stijgen.[4] In elk geval worden de beschikbare middelen voor opsporing, veiligheid en defensie en de bevoegdheden van de hiervoor verantwoordelijke instanties na de aanslag sterk uitgebreid. Hieronder vallen ook de bestrijding van computercriminaliteit en het doen van onderzoek naar de kwetsbaarheid van informatie-infrastructuren. Informatiebeveiliging staat hoger op de agenda dan ooit tevoren.

Drie gebeurtenissen markeren zo het einde van een periode; drie gebeurtenissen zorgen elk voor een schokgolf in een specifiek vakgebied. Voor mensen die zich bezighouden met informatietechnologie, accountancy of informatiebeveiliging ziet de wereld er op dit moment anders uit dan drie jaar geleden. Het leek me goed deze omstandigheid te schetsen alvorens het echte verhaal te laten beginnen.

Een van de doelstellingen van dit verhaal is u iets meer te vertellen over een nieuwe leerstoel, IT en Auditing. De naam van deze leerstoel kunt u op twee manieren interpreteren. De eerste, enge interpretatie is de oorspronkelijk bedoelde: informatietechnologie en accountantscontrole. Sommige collega's van de postdoctorale accountantsopleiding houden mij voor dat de volgorde anders moet zijn: eerst accountantscontrole, dan pas informatietechnologie. Want het gaat in deze opleiding om de accountant, zeggen ze, en informatietechnologie is op zijn best een bijkomend ongemak. Ik ben het wel met ze eens. De tweede interpretatie heeft echter mijn voorkeur: informatietechnologie en toetsing in bredere zin. Die interpretatie geeft mij, maar ook de betrokken docenten en studenten, de mogelijkheid om niet alleen stil te staan bij de relatie tussen de activiteiten van de registeraccountant en het verschijnsel informatietechnologie, maar vooral om dieper in te gaan op onderwerpen die samenhangen met de beheersing van risico's rond informatietechnologie en de onafhankelijke toetsing daarvan. En zo komen we op de drie onderwerpen in de titel van dit verhaal – informatietechnologie, accountancy en informatiebeveiliging – die ik graag in deze volgorde met u zou willen bespreken.

Informatietechnologie

Het eerste onderwerp is dus informatietechnologie. Hier ligt mijn achtergrond. Een jaar of zeventien geleden probeerde ik een studie informatica aan deze universiteit te combineren met een parttime baan als systeemprogrammeur bij SARA, het rekencentrum van de Amsterdamse universiteiten. Het waren twee verschillende werelden met verschillende opvattingen over informatietechnologie. 's Ochtends volgde je het college complexiteitstheorie of schreef je een werkstuk over dataflow-computers, 's middags testte je een nieuwe versie van een besturingssysteem of schreef je een script om back-ups te maken. Met andere woorden, tijdens je studie leerde je dingen waarvan de praktische relevantie niet helemaal duidelijk was, tijdens je werk loste je zonder theoretische onderbouwing allerlei praktische problemen op. Dat vulde elkaar dus goed aan. Inmiddels zijn theorie en praktijk iets dichter bij elkaar gekomen. Er zijn zelfs boeken waarin zowel de praktische toepassingen als de onderliggende beginselen van de informatica op een aanvaardbare en actuele manier worden behandeld.[5]

Zeventien jaar geleden was een computer nog wel iets bijzonders. Tegenwoordig gebruikt bijna elke Nederlander dagelijks een computer die tien keer zo goedkoop en duizend keer zo snel is als de exemplaren van toen, en maakt elke organisatie van enige omvang intensief gebruik van informatietechnologie voor de ondersteuning of zelfs de volledige realisatie van de belangrijkste bedrijfsprocessen en de communicatie met klanten, toeleveranciers, zakenpartners en dergelijke. In die toepassing is voortdurend sprake van allerlei trends waarnaar door universiteiten, maar ook door adviesbureaus en accountantskantoren, onderzoek wordt gedaan.[6] Naar mijn mening is een vijftal van deze trends in bijzondere mate bepalend geweest voor de manier waarop organisaties op dit moment gebruikmaken van informatietechnologie: de implementatie van standaardpakketten, het gebruik van standaardomgevingen voor kantoorautomatisering, het gebruik van internettechnologie, de explosieve groei van gegevensopslag en het uitbesteden van de informatievoorziening. Op elk van deze trends wil ik hieronder kort ingaan.

1. Standaardpakketten

De eerste trend is de grootschalige invoering van standaardpakketten die ook bekend staan onder de noemer Enterprise Resource Planning (ERP).[7] ERP-systemen

zijn oorspronkelijk ontwikkeld voor de ondersteuning van logistieke processen in productiebedrijven; later zijn aan deze systemen ook modules toegevoegd voor processen als financieel beheer, personeelszaken en relatiebeheer, en zijn er versies ontwikkeld die zijn toegesneden op specifieke sectoren, zoals handelsondernemingen of energiebedrijven. Typerend voor de huidige generatie ERP-systemen is de automatische koppeling tussen de verschillende bedrijfsprocessen, waardoor het voor de onderneming eenvoudiger wordt zulke processen op een standaardwijze in te richten, op elkaar aan te laten sluiten en de prestaties van deze processen te bewaken. In de markt voor ERP-systemen is een beperkt aantal leveranciers actief, waarvan één de onbetwiste marktleider is. Bij de invoering van een ERP-systeem wordt een basissysteem op maat gemaakt door het te configureren en indien nodig aan te passen. De afgelopen jaren hebben veel ondernemingen ondervonden dat aan de invoering van een ERP-systeem nogal wat haken en ogen kunnen zitten. Een Rotterdams tankopslagbedrijf kondigde eerder dit jaar aan rigoureus te stoppen met de invoering van een nieuw informatiesysteem voor zijn Europese distributieactiviteiten; de gedane investering bedroeg op dat moment 75 miljoen euro.[8] Als reden noemde het bedrijf de nog te maken implementatiekosten die niet zouden opwegen tegen de verwachte opbrengsten.

2. Kantoorautomatisering

Een trend die vrijwel geen werknemer onberoerd heeft gelaten, is de wereldwijde invoering van kantoorapplicaties. In dit segment domineert één leverancier de markt op een manier die het best als totalitair gekenmerkt kan worden. Het gaat om een leverancier die tegen relatief lage prijzen goedgevulde applicaties op de markt brengt voor tekstverwerking, presentaties, rekenbladen, elektronische post, internettoegang en wat dies meer zij. Vrijwel elke onderneming gebruikt de applicaties van deze leverancier, die eigenlijk alleen goed werken in combinatie met de besturingssystemen van dezelfde leverancier. Mede om deze reden is de leverancier verwikkeld in een nu al vier jaar slepende rechtszaak in de Verenigde Staten.[9] Aan het gebruik van kantoorautomatisering zijn beveiligingsvraagstukken verbonden die later nog aan de orde zullen komen.

3. Internettechnologie

De derde trend is de wereldwijde invoering van internettechnologie, een trend die gelijktijdig verliep met de invoering van standaardpakketten en kantoorapplicaties. Onderdeel van deze technologie is een stapel communicatieprotocollen uit de jaren zeventig. Deze protocollen zijn inmiddels standaard ingebouwd in elk gangbaar besturingssysteem en worden toegepast in apparaten waarmee bedrijfsnetwerken kunnen worden gebouwd (routers). Boven op deze stapel draaien weer andere protocollen, onder meer voor het versturen van e-mail en het navigeren in informatienetwerken op basis van hyperlinks met een interface dat iedereen tegenwoordig kent als een browser. Zonder in te gaan op de ontwikkeling van internet en alles wat daarmee samenhangt, kunnen we hier constateren dat inmiddels elke onderneming gebruikmaakt van de internetprotocollen, dat vrijwel elke onderneming één of meer websites onderhoudt – hetzij voor extern, hetzij voor intern gebruik – en dat vrijwel elke werknemer tegenwoordig gebruikmaakt van internet voor zakelijke en recreatieve doeleinden. De markt voor routers en de markt voor internetsoftware worden beiden gedomineerd door één leverancier.

4. Gegevensopslag

Een vierde trend is de sterke stijging van de hoeveelheid opgeslagen gegevens. Uit informele gegevens van gebruikers en leveranciers van opslagtechnologie blijkt dat de hoeveelheid gebruikte opslagruimte de afgelopen tijd elk jaar met ruwweg een factor twee is gestegen. Waar deze stijging vandaan komt, is niet geheel duidelijk. Er moet voor de meeste ondernemingen toch wel een bovengrens zijn aan de hoeveelheid informatie die nog relevant is voor de bedrijfsvoering en in veel gevallen lijkt die bovengrens wel bereikt. Toch blijven de databases maar groeien en moet de opslagcapaciteit steeds opnieuw worden uitgebreid. Automatiseerders noemen als mogelijke oorzaken van de geconstateerde stijging onder meer het toenemend gebruik van gedigitaliseerde afbeeldingen in tekstbestanden en presentaties, de stijging van het aantal gebruikte applicaties waarbij voor elke applicatie een nieuwe server wordt geïnstalleerd, en de toename van het niet-zakelijk gebruik van de infrastructuur; we kunnen inderdaad niet voorbijgaan aan het naakte feit dat werknemers dagelijks vele terabytes aan filmpjes, muziekbestanden en Dilbert-cartoons via e-mail uitwisselen en opslaan op de systemen van hun werkgever. Die niet-zake-

lijke gegevens worden doorgaans bewaard op dezelfde servers als de kritieke bedrijfsgegevens, en daarmee heeft de explosieve stijging van het aantal opgeslagen gegevens onvermoede gevolgen voor de continuïteit van de informatievoorziening. Het terugladen van 20 terabyte aan gegevens die verspreid zijn over 80 servers is een wezenlijk probleem, zeker als dat binnen 24 uur moet gebeuren.

5. Uitbesteden

De vijfde en laatste trend die ik hier wil noemen, is het uitbesteden van het beheer van de informatievoorziening aan hierin gespecialiseerde serviceorganisaties. Uitbesteden heeft een hoge vlucht genomen, mede onder invloed van de stagnerende economie waarin ondernemingen naar mogelijkheden zoeken om kosten te besparen en waarin het uitbesteden van niet-kernactiviteiten, zoals het beheer van de informatievoorziening, een snelle en eenvoudige manier lijkt om dat doel te bereiken. In veel gevallen gaat deze uitbesteding gepaard met de overdracht of verkoop van de interne automatiseringsorganisatie aan een belangstellende aanbieder.[10] Aan uitbesteden zijn ook vraagstukken rond beveiliging en continuïteit verbonden; ik zal hier later nog op ingaan.

We laten deze trends even voor wat ze zijn en gaan naar een volgende vraag. Hoeveel geld geven organisaties eigenlijk uit aan informatietechnologie? Ook hiernaar wordt al jaren onderzoek gedaan, maar de onderzoeksresultaten divergeren sterk. Dit zal wel het gevolg zijn van verschillen in de onderzoeksaanpak en de onderzochte populatie. Toch kunnen we rustig aannemen dat ondernemingen een substantieel deel van hun omzet aan informatietechnologie spenderen.

Ik geef u een zorgvuldig geanonimiseerd voorbeeld: een zeker accountantskantoor had in het jaar 2001 een omzet in Nederland van ongeveer één miljard gulden. Ongeveer tien procent hiervan, een slordige, maar niettemin keurig verantwoorde 100 miljoen gulden, werd – in de vorm van kosten en afschrijvingen op investeringen – uitgegeven aan informatietechnologie. Dragen al deze kosten en investeringen nu op de een of andere manier bij aan de doelstellingen van de onderneming? Met andere woorden, levert informatietechnologie ons iets op? Ook over deze vraag – dat het een vraag is, zegt natuurlijk al iets – breken wetenschappers zich reeds jaren het hoofd, en ook op dit gebied verschillen de deskundigen van mening, niet alleen onderling, maar ook met zichzelf.[11]

OVER INFORMATIETECHNOLOGIE, ACCOUNTANCY EN INFORMATIEBEVEILIGING

Wat levert informatietechnologie een accountant eigenlijk op? Laten we het eerder genoemde voorbeeld nemen. Voor de 100 miljoen gulden per jaar kreeg het niet nader genoemde accountantskantoor het volgende terug: 170 relationele databases op 30 servers; een uren- en kostenregistratiesysteem met 4.600 gebruikers; een systeem voor de registratie van onderhanden werk en facturering met 2.700 gebruikers; een personeelsinformatiesysteem met 273 gebruikers en 6.550 tabellen, waarin circa 20.000 arbeidsrelaties zijn vastgelegd; een financieel-administratief systeem met 123 gebruikers, 12.000 tabellen, ruim 1,9 miljoen journaalpostregels, 1,3 miljoen grootboekregels en evenveel factuurregels; draagbare computers voor circa 4.000 professionals en bureaucomputers voor circa 1.000 interne medewerkers; een landelijk netwerk met aansluitingen op het wereldwijde netwerk; toegang tot een wereldwijd kennismanagementsysteem; inbelmogelijkheden voor 4.000 gebruikers; 120 inbellijnen die gelijktijdig beschikbaar zijn tegen lokaal tarief; gemiddeld 44.000 inbelverbindingen per maand met een gemiddelde connectietijd van 22 minuten en 22 seconden; in totaal 900.000 inbelminuten per maand; circa 13.000 netwerkpoorten op 30 kantoren; bijna 76 miljoen internet-hits per maand, waarbij ongeveer 182.000 websites werden bezocht; gemiddeld 20.000 mailberichten via internet per dag, waarbij alle mailberichten op virussen worden gecontroleerd. Bij de interne afdeling die verantwoordelijk is het voor het leveren van deze diensten werken 150 professionals, worden in totaal 180 servers beheerd, zijn 4.000 backuptapes in omloop en wordt 13 terabyte aan schijfruimte beheerd. De infrastructuur voor telecommunicatie bestaat uit 31 telefooncentrales, 1.200 netlijnen en 12.500 poorten in Nederland. Die infrastructuur wordt gebruikt voor 25.000 externe gesprekken en 75.000 interne gesprekken per dag, waarbij sprake is van 1.500 aansluitwijzigingen per maand. Het callcenter, dat is uitbesteed, verwerkt een luttele 5.000 probleemmeldingen per maand.

Duizelt het u inmiddels? Laat mij u dan vertellen dat deze cijfers redelijk marktconform lijken te zijn en in grote lijnen ook zullen gelden voor andere grote accountantskantoren. De vraag daarbij is niet zozeer of al die investeringen uiteindelijk productiviteitsverhogend werken; de vraag is of die kantoren het zich kunnen permitteren die investeringen *niet* te doen. Het antwoord op die vraag luidt ten enenmale ontkennend.

Accountancy

Hiermee komen we op het tweede onderwerp in dit drieluik: accountancy, te beschouwen in relatie tot het vorige onderwerp, informatietechnologie. Sommige accountants in opleiding vragen zich openlijk af waarom een accountant iets van informatietechnologie zou moeten weten. Wij zagen zojuist één reden: het kost hem handen vol geld en hij kan niet meer zonder. Maar wat is nu het belang van informatietechnologie voor zijn dagelijkse werkzaamheden? Om deze vraag te kunnen beantwoorden, is het noodzakelijk stil te staan bij wat een accountant precies doet.

Die accountant is er in de eerste plaats om jaarrekeningen te controleren; iets formeler gesteld, om als onafhankelijke deskundige financiële verantwoordingen te certificeren. Dit wordt dan ook de certificerende functie genoemd.[12] Simpel gezegd stelt de accountant vast of de jaarrekening van een onderneming, die onder meer bestaat uit een winst- en verliesrekening en een balans, een getrouw beeld geeft van het resultaat en de financiële positie van de organisatie. Essentieel hierbij is het begrip materialiteit. Een goedkeurende accountantsverklaring betekent niet dat de jaarrekening volkomen foutloos is; het gaat er bij de jaarrekeningcontrole om vast te stellen dat de jaarrekening geen materiële fouten bevat, waarbij een materiële fout is gedefinieerd als een fout die van invloed kan zijn op beslissingen die op basis van de jaarrekening worden genomen door de gebruikers ervan. Die gebruikers vormen een breed en divers gezelschap dat bestaat uit aandeelhouders, toezichthouders, vermogensverschaffers, zakenpartners, leveranciers, klanten, werknemers en andere partijen in het maatschappelijk verkeer.[13] In de accountantsverklaring dient de accountant ten slotte melding te maken van gerede twijfel over de continuïteit van de organisatie.

Naast zijn primaire functie als controleur van de jaarrekening heeft de accountant een aantal andere functies die weliswaar secundair genoemd worden, maar die in de praktijk niet minder belangrijk zijn. Zo fungeert de accountant vaak als gesprekspartner van de leiding van de organisatie, bijvoorbeeld over strategische of financiële aangelegenheden. Ook verstrekt de accountant op verzoek van de leiding van de organisatie advies, bijvoorbeeld over de inrichting van de administratieve organisatie. Het zal u niet ontgaan zijn dat de adviesfunctie van de accountant de laatste tijd – en na het Enron-schandaal in verhevigde mate – ter discussie wordt gesteld, omdat zij strijdig zou zijn met het geven van een onafhankelijk oordeel over de getrouwheid van de jaarrekening. Critici vinden dat een accountant geen onaf-

hankelijk oordeel kan vellen over zaken waarover hij zelf geadviseerd heeft; bovendien wijzen ze op het risico dat de accountant die zowel controleert als adviseert in de verleiding kan komen een goedkeurende accountantsverklaring bij een slechte jaarrekening te geven omdat hij anders zijn lucratieve adviesopdracht zou kwijtraken. Deze kritiek is naar mijn mening gerechtvaardigd, en het is onvermijdelijk dat de certificerende functie en de adviesfunctie van de accountant de komende jaren strikter zullen worden gescheiden.[14] Sommigen spreken zelfs de verwachting uit dat accountants in de nabije toekomst hun advieswerk geheel zullen staken. Die verwachting deel ik niet.

Tot slot zij opgemerkt dat accountants worden ingeschakeld voor het uitvoeren van activiteiten die met enige goede wil zowel tot de certificerende functie als tot de adviesfunctie gerekend kunnen worden, of tot geen van beide, en die wel worden samengevat onder de noemer 'aan controle verwante opdrachten', zoals reviews, samenstellingsopdrachten en andere overeengekomen specifieke werkzaamheden. Een voorbeeld daarvan is het boekenonderzoek bij fusies en overnames (*due diligence*), waarbij de overnemende partij zoveel mogelijk te weten wil komen over de over te nemen partij – vooral dingen die niet deugen – en een accountant in de arm neemt om zo'n onderzoek uit te voeren onder condities die vooraf tussen beide partijen zijn overeengekomen.

Hoe belangrijk is informatietechnologie nu voor al deze functies? Laten we eerst eens kijken naar de certificerende functie ofwel de jaarrekeningcontrole. Een jaarrekening wordt samengesteld op basis van allerlei gegevens over het reilen en zeilen van de organisatie: gegevens over inkoop- en verkooptransacties, geleverde en ontvangen goederen, ontvangsten en betalingen, vorderingen en schulden, prijzen en kortingen, orders en onderhanden werk, voorraden, bezittingen, deelnemingen, saldi, overboekingen en nog veel meer zaken die zowel voor de bedrijfsvoering als voor de jaarrekeningcontrole van belang zijn. Naast deze primaire registraties is er ook aanvullende documentatie die van invloed kan zijn op posten in de jaarrekening, zoals begrotingen, contracten of investeringsplannen. Kan een accountant een jaarrekening goedkeuren als hij niet met een redelijke mate van zekerheid kan vaststellen dat de gegevens die aan deze jaarrekening ten grondslag liggen daadwerkelijk betrouwbaar zijn? Neen. Dus zal de accountant óf de betrouwbaarheid van de gegevens zelf moeten verifiëren, óf moeten verifiëren of de organisatie effectieve maatregelen getroffen heeft om de betrouwbaarheid van die gegevens te waarborgen. En daarmee komen we natuurlijk bij de kern van de zaak: letterlijk alle

gegevens die worden gebruikt om een jaarrekening samen te stellen, zijn tegenwoordig opgeslagen in digitale informatiesystemen. Als die systemen niet goed worden gebruikt of als de gegevens in die systemen niet betrouwbaar zijn, kunnen materiële fouten in de jaarrekening ontstaan.

Hetzelfde geldt voor de maatregelen die een organisatie kan treffen om de betrouwbaarheid van de administratie te waarborgen en die sinds jaar en dag worden samengevat onder de noemer 'administratieve organisatie en interne controle'.[15] Ook deze maatregelen vormen tegenwoordig een integraal onderdeel van de informatiesystemen. Neem een van de pijlers van de administratieve organisatie: het principe van controletechnische functiescheiding. Uitgangspunt van deze functiescheiding is de organisatorische taken zo te verdelen dat een belangentegenstelling ontstaat; opzettelijke of onopzettelijke onjuistheden in de werkzaamheden van de ene functionaris worden ogenblikkelijk opgemerkt door het resultaat van die werkzaamheden systematisch te vergelijken met het resultaat van de werkzaamheden van een andere functionaris met een tegengesteld belang. Waar vroeger vaak sprake was van gescheiden papieren vastleggingen die werden geparafeerd door verschillende functionarissen en uiteindelijk werden gecontroleerd door een centrale administratieve afdeling, is tegenwoordig sprake van centrale systemen waarbij verschillende functionarissen toegang hebben tot verschillende functies in het systeem. Het systeem bepaalt daarbij wie toegang heeft tot welke functies op basis van twee gegevens: de identiteit van de gebruiker en een autorisatietabel.[16] Niet alleen de gegevens, maar ook de maatregelen die de betrouwbaarheid van deze gegevens moeten waarborgen, vormen dus een integraal onderdeel van de informatiesystemen. Dit maakt het controleren van de informatiesystemen en de onderliggende infrastructuur tot een onmisbaar onderdeel van elke jaarrekeningcontrole. Een bijzonder geval doet zich voor bij het controleren van de jaarrekening van een onderneming die informatietechnologiegebonden diensten levert, zoals telecommunicatiediensten, internetdiensten of de verkoop van gegevens via internet; hierbij dient de accountant per definitie te beschikken over kennis van informatietechnologie omdat dit een wezenlijk onderdeel is van het primaire proces van de onderneming.

Eveneens van belang voor de primaire functie van de accountant zijn vraagstukken inzake de activering, waardering en afschrijving van investeringen in informatietechnologie zelf. Lang niet altijd is duidelijk of de euro's die worden uitgegeven aan informatietechnologie moeten worden gezien als kosten die direct ten laste van de winst- en verliesrekening moeten worden genomen of als investeringen die als

activa op de balans kunnen worden opgenomen, waarna afschrijving plaatsvindt. Nu is activeren en afschrijven, mede op grond van het voorzichtigheidsbeginsel,[17] alleen gepast als van de investering in kwestie een reële bijdrage aan de omzet en de winst mag worden verwacht. Helaas voldoen lang niet alle investeringen in informatietechnologie aan dit criterium. Uit wetenschappelijk en quasi-wetenschappelijk onderzoek blijkt keer op keer dat grote automatiseringsprojecten vaker mislukken dan slagen.[18] In maar liefst een kwart van de gevallen leiden automatiseringsprojecten niet tot het beoogde resultaat en moet het resulterende systeem letterlijk als waardeloos worden beschouwd. Voor omvangrijke projecten zijn deze cijfers nog ongunstiger; vaak is er al in een vroeg stadium sprake van gerede twijfel over het succes van het project. Duidelijk is dat in die gevallen niet zonder meer mag worden overgegaan tot activering, maar hoe zit het met een situatie waarbij zo een mislukt systeem wordt ontmanteld, waarna uit de componenten van dat systeem een nieuw, werkend systeem wordt opgebouwd? Activering lijkt hier gerechtvaardigd, maar vanaf welk moment, tegen welke waarderingsgrondslag, voor welk bedrag en met welke afschrijvingstermijn? Bedenk in relatie tot het begrip materialiteit dat het hier bij grote ondernemingen kan gaan om strategische investeringen met een omvang van tientallen of zelfs honderden miljoenen guldens.

Een derde, maar minstens zo belangrijk aspect ten slotte is dat risico's met betrekking tot informatietechnologie een direct gevaar kunnen vormen voor de continuïteit van een organisatie. Ik noem twee voorbeelden:

1. Een adviesbureau laat een nieuw systeem ontwikkelen voor de registratie van werkzaamheden. Medewerkers van het kantoor kunnen dit systeem gebruiken om bij te houden aan welk project ze werken; op basis hiervan worden facturen verstuurd aan de opdrachtgevers van het kantoor. Het nieuwe systeem wordt in zes maanden ontwikkeld door een extern automatiseringsbedrijf. Bij de ontwikkeling wordt op initiatief van het automatiseringsbedrijf gebruikgemaakt van zeer geavanceerde, maar nog niet geheel beproefde technieken. Na oplevering wordt het nieuwe systeem ingevoerd; tegelijkertijd wordt het oude systeem afgeschaft. Bij de invoering van het nieuwe systeem ontstaan grote problemen. Het systeem is vaak uit de lucht en bepaalde functies werken niet naar behoren. Bovendien veroorzaakt het systeem een te hoge netwerkbelasting, waardoor veelvuldig storingen in het netwerk ontstaan. Het oplossen van de problemen neemt maanden in beslag. In die periode vindt een zeer gebrekkige registratie van de uitgevoerde werkzaamheden

plaats en kan feitelijk niet gefactureerd worden. Een dreigend liquiditeitsprobleem kan alleen worden afgewend door een papieren noodadministratie in te voeren en handmatig te factureren.

2. Een producent van fornuizen start met de implementatie van een ERP-systeem ter vervanging van het bestaande informatiesysteem, waarvan niet minder dan zeventien verschillende versies operationeel zijn. De implementatie wordt uitbesteed aan een gerenommeerd automatiseringsbedrijf. Doordat de verschillende bedrijfsonderdelen van de producent elk hun eigen eisen stellen aan de functionaliteit van het nieuwe systeem en die eisen ook door de projectgroep worden ingewilligd, ontstaat een systeem dat voor meer dan de helft uit maatwerk bestaat. Er raken steeds meer consultants betrokken bij het project; de kosten lopen op tot het dubbele van de begrote 25 miljoen gulden en het project loopt een jaar uit. Het resulterende systeem blijkt na oplevering zo traag te werken en nog zoveel fouten te bevatten dat het primaire proces van de onderneming ernstig verstoord raakt. Het bedrijf kan niet meer leveren en veel klanten stappen over naar de concurrent. 'Het imago dat we in al die jaren hadden opgebouwd, werd in drie maanden tijd om zeep geholpen', aldus een oud-medewerker. Faillissement volgt.[19]

Het spreekt voor zich dat dergelijke situaties voor de accountant, gezien vanuit diens primaire functie, van materieel belang zijn.

Dan de secundaire functie, die van sparring partner en adviseur van de leiding van de onderneming. Cliënten vertellen dat informatietechnologie een onderwerp is waar ze wel eens wakker van liggen. Dat heeft te maken met de hoogte van de aan informatietechnologie gerelateerde kosten en investeringen en het feit dat die kosten en investeringen lang niet altijd direct leiden tot een meetbare verbetering van het resultaat en de financiële positie van de organisatie, om van situaties als hierboven beschreven maar niet te spreken. We kunnen rustig stellen dat de accountant op zijn minst enige kennis moet hebben van informatietechnologie, haar toepassingen en haar beperkingen om als adviseur serieus genomen te worden.

Dan nog de accountant als leverancier van aan controle verwante opdrachten. Neem als voorbeeld het *due-diligence*-onderzoek. Als eerder gezegd, is het bij zo'n onderzoek in het belang van de koper om zoveel mogelijk risico's bloot te leggen die de waarde van de over te nemen partij, en daarmee de overnameprijs, in negatieve zin kunnen beïnvloeden. Juist aan de informatiesystemen en aan de technische in-

frastructuur van een over te nemen partij kunnen zulke risico's verbonden zijn. Hierbij gaat het niet alleen om 'lijken in de kast' zoals instabiele systemen, uitgestelde investeringen of ernstige overschrijdingen in budget en doorlooptijd bij lopende automatiseringsprojecten, maar ook om zaken als de kwaliteit van de automatiseringsorganisatie, de lopende contracten met aanbieders en leveranciers of de mate van compatibiliteit van de informatiesystemen van de over te nemen partij met de systemen van de koper en, hiermee samenhangend, de verwachte integratiekosten.[20] Een bijzonder geval doet zich voor bij de overname van een aanbieder van diensten die gerelateerd zijn aan informatietechnologie, zoals systeembeheer of systeemontwikkeling; hierbij hangen de overnamerisico's direct samen met de mate waarin de over te nemen partij de technologie beheerst. Enig inzicht in deze technologie en de bijbehorende beheersingsmaatregelen zal de *due-diligence*-onderzoeker wel van pas komen.

Wij kunnen dus vaststellen dat de accountant in zijn secundaire functie als sparring partner en adviseur en ook in zijn rol als *due-diligence*-onderzoeker enig verstand van informatietechnologie moet hebben en informatietechnologie actief in zijn werkzaamheden moet adresseren.

Maar dan de praktijk. In hoeverre besteden accountants nu werkelijk aandacht aan informatietechnologie? Deze vraag zullen wij voor het moment beantwoorden door te kijken naar de manier waarop informatietechnologie in de accountantsopleiding wordt behandeld, naar de positie van informatietechnologie in nationale en internationale wet- en regelgeving voor de accountantscontrole, naar de inbedding van informatietechnologie in de controlemethodieken van accountantskantoren, en ten slotte naar de mate waarin de accountant het geleerde in de praktijk brengt, de richtlijnen volgt en handelt volgens de controlemethodiek van zijn kantoor.

1. Informatietechnologie in de accountantsopleiding

In hoeverre wordt op dit moment in de postdoctorale accountantsopleiding aandacht gegeven aan informatietechnologie? Enkele jaren geleden is door collega Fijneman geformuleerd welke onderwerpen in de postdoctorale accountantsopleidingen behandeld zouden moeten worden; vervolgens is onderzocht in hoeverre de universiteiten deze *common body of knowledge* ook daadwerkelijk in het opleidingsaanbod hadden opgenomen.[21] Het voert te ver om hier diep in te gaan op het onderzoek

en de resultaten daarvan, maar een van de conclusies was dat er grote verschillen bestonden tussen de mate waarin opleidingen aan de in het kader van het onderzoek geformuleerde minimumeisen voldeden. Een korte inventarisatie van de programma's van de Nederlandse accountantsopleidingen leert dat er sinds het onderzoek van Fijneman nog niet bijzonder veel veranderd is. Ook met de positie van informatietechnologie in de veelal internationale literatuur die in de opleidingen wordt gebruikt, is het nog wat mager gesteld. Messier besteedt enige aandacht aan informatietechnologie,[22] Knechel in het geheel niet.[23]

Dan nog wat internationale ontwikkelingen. De Education Committee van de International Federation of Accountants (IFAC) kwam ongeveer een jaar geleden met een conceptversie van een richtlijn met de veelzeggende titel 'Information Technology for Professional Accountants'.[24] In dit concept stelt de IFAC onder meer: 'Information technology is one of the core competencies of professional accountants and requires special attention due to its explosive growth and rapid rate of change.' Het concept bestaat uit een nogal lijvige opsomming van de kennis op het gebied van informatietechnologie waarover elke accountant in zijn verschillende functies zou moeten beschikken en die in de accountantsopleidingen aangeboden zou moeten worden. Zover zijn we in Nederland nog niet.

2. Informatietechnologie en regelgeving

In hoeverre komt informatietechnologie in nationale en internationale regelgeving voor de accountantscontrole aan bod? Nu, dat valt niet tegen. Ik volsta met een kleine selectie, te beginnen met de wet. Volgens artikel 393, lid 4 van het Burgerlijk Wetboek is de accountant verplicht zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking te melden aan de Raad van Commissarissen en aan het bestuur.[25] Dat lijkt duidelijke taal, maar wie het desbetreffende artikel goed leest, ziet hierin geen verplichting om onderzoek te doen, maar een verplichting om eventuele bevindingen te melden; wie geen onderzoek doet, heeft geen bevindingen, en wie geen bevindingen heeft, heeft niets te melden. Een accountant die geen onderzoek doet naar de betrouwbaarheid en continuïteit van de informatiesystemen van zijn cliënt handelt dus niet in strijd met de wet. Overigens is de vraag gerechtvaardigd of commissarissen en bestuur het niet aan hun stand verplicht zijn de accountant om zo'n onderzoek te vragen.

Dan de Richtlijnen voor de Accountantscontrole (RAC) waaraan elke accountant in Nederland zich dient te houden. Deze richtlijnen worden uitgegeven door het Koninklijk Nederlands Instituut van Registeraccountants (NIVRA) en zijn direct afgeleid van de internationaal erkende International Standards on Auditing (ISA) van de IFAC. Met betrekking tot het onderwerp informatietechnologie zijn drie specifieke richtlijnen van belang. De eerste daarvan is RAC400. Volgens deze richtlijn dient de accountant voldoende inzicht te krijgen in de administratieve organisatie en interne controle. In een recent artikel constateert De Koning dat administratieve organisatie en interne controle vandaag de dag zeer sterk verweven zijn met geautomatiseerde informatiesystemen; hij concludeert dat direct uit de RAC mag worden afgeleid dat de accountant aandacht moet besteden aan de informatiesystemen binnen de te controleren huishoudingen en dan vooral aan de maatregelen van interne controle die daar in zijn opgenomen of daarop betrekking hebben.[26] Naast RAC400 is er een aanvullende richtlijn, RAC401, voor situaties waarbij de controle wordt uitgevoerd in een omgeving waarin gebruik wordt gemaakt van geautomatiseerde informatiesystemen.[27] De Koning merkt op dat zulks tegenwoordig altijd het geval is en pleit ervoor RAC400 en RAC401 samen te voegen. Ik ben het op dit punt met hem eens. RAC402 geeft ten slotte overwegingen bij controles van organisaties die gebruikmaken van serviceorganisaties en stelt dat de accountant ten minste moet vaststellen wat de betekenis is van de activiteiten van de serviceorganisaties voor de controle. Als de accountant tot de conclusie komt dat die activiteiten belangrijk voor de organisatie en relevant voor de controle zijn, dient hij voldoende inzicht te krijgen in de administratieve organisatie en interne controle bij de serviceorganisatie; daarbij kan hij gebruikmaken van eventuele rapporten van de accountant van de serviceorganisatie.[28]

Het NIVRA is ook op andere gebieden actief. Zo publiceerde het reeds jaren geleden een studierapport waarin een normenkader voor de beoordeling van de algemene beheersingsmaatregelen is opgenomen.[29] Tot slot gelden er in Nederland ook richtlijnen die specifiek zijn voor een bepaalde sector. Een bekend voorbeeld hiervan is de Regeling Organisatie en Beheersing (ROB) van De Nederlandsche Bank.[30]

En wat gebeurt er in het buitenland? Vooral in de Verenigde Staten lijkt men op dit moment iets verder te zijn dan hier te lande. De Auditing Standards Board (ASB) van het American Institute of Chartered Public Accountants (AICPA), de Amerikaanse tegenhanger van het NIVRA, heeft in april 2001 een Statement of Auditing Standards (SAS) uitgebracht waarin de effecten van informatietechnologie op de

beoordeling van de interne beheersingsmaatregelen wordt beschreven.[31] SAS 94 is niet alleen bedoeld voor grote organisaties, maar stelt expliciet dat informatietechnologie van invloed is op de jaarrekeningcontrole van organisaties van elke omvang. Het document gaat in op de invloed van informatietechnologie op de bedrijfsvoering, op het initiëren en verwerken van transacties, en op de administratieve organisatie en interne controle, en stelt dat de accountant zich moet afvragen of een puur gegevensgerichte controle in een hooggeautomatiseerde omgeving wel voldoende effectief is, of dat ook een beoordeling van de opzet en de werking van de aan informatietechnologie gerelateerde beheersingsmaatregelen moet plaatsvinden. Daarbij wordt opgemerkt dat de accountant bijzondere aandacht dient te besteden aan de werking van deze maatregelen om voldoende zekerheid te krijgen dat specifieke uitspraken (bijvoorbeeld over de juiste en volledige vastlegging van transacties) geen materiële onjuistheden bevatten.[32] SAS 94 maakt onderscheid tussen specifieke en algemene beheersingsmaatregelen en geeft richtlijnen voor het beoordelen en testen van geautomatiseerde beheersingsmaatregelen. Ten slotte gaat SAS 94 in op wat de accountant moet weten over de geautomatiseerde en handmatige procedures die zijn cliënt hanteert bij het samenstellen van de jaarrekening, inclusief procedures voor het invoeren van transactietotalen in het grootboek, het verwerken van journaalposten en het verwerken van wijzigingen in de financiële verantwoording. SAS 94 schrijft hiermee gedetailleerder voor wat er van de accountant wordt verwacht dan zijn Nederlandse tegenhanger RAC401. Naast SAS 94 kennen de Amerikanen onder meer een richtlijn voor het beoordelen van de beheersingsmaatregelen bij serviceorganisaties, waarbij wordt gebruikgemaakt van het rapport van de accountant van de serviceorganisatie, SAS 70.[33]

3. Informatietechnologie in controlemethodieken

Interessant is de vraag hoe de accountantskantoren met informatietechnologie omgaan. Een oppervlakkige beschouwing van de controlemethodieken van de grote accountantskantoren leert dat informatietechnologie daarin wel een plaats heeft gekregen. Die methodieken zijn doorgaans gebaseerd op een *topdown*-benadering, waarbij de accountant eerst een strategieanalyse uitvoert, daarna de bedrijfsprocessen analyseert en vaststelt binnen welke bedrijfsprocessen risico's spelen die van materieel belang kunnen zijn voor posten in de jaarrekening, en vervolgens binnen die processen gerichte controles uitvoert. Bij de gehanteerde methodieken vormt

het beoordelen van de automatisering een integraal onderdeel van elk van deze processtappen, zij het dat de uitwerking van de manier waarop de accountant daadwerkelijk met informatietechnologie moet omgaan soms wel erg summier is. De methodieken worden ondersteund door geautomatiseerde hulpmiddelen, zoals elektronische dossiers, vragenlijsten en analyseprogrammatuur.

4. Informatietechnologie in de praktijk

Dan informatietechnologie in de accountantspraktijk. Hoeveel aandacht besteedt de accountant werkelijk aan informatietechnologie in zijn primaire en secundaire werkzaamheden? Het wetenschappelijke antwoord op deze vraag luidt: het is nooit echt onderzocht, dus officieel weten we het niet. Maar laten we er geen doekjes om winden: de praktijk leert dat het wel iets beter zou kunnen, of zwaarder aangezet, dat er accountants zijn die zich wat informatietechnologie betreft noch aan de internationale richtlijnen, noch aan de voorschriften van het eigen accountantskantoor houden. Ik geef direct toe dat dit een weinig oorspronkelijke constatering is. Sinds het midden van de jaren zeventig is er bijna elk jaar wel een prominent accountant geweest die een constatering van deze aard heeft gedaan in een goed onderbouwd artikel in een gerenommeerd tijdschrift dat door alle accountants gelezen zou moeten worden. Toch hebben al die constateringen in al die artikelen in al die tijdschriften nog niet geleid tot een ideale situatie.

Er zou een promotieonderzoek kunnen worden gewijd aan het blootleggen en analyseren van de oorzaken van dit fenomeen. Volgens een hooggeplaatste interne accountant van een beursgenoteerde financiële instelling is het een kwestie van desinteresse – hij gebruikte iets andere bewoordingen – maar dat is te gemakkelijk gedacht; er is meer aan de hand.

Neem eerst de financiële kant. In theorie zou het controleren van een klein aantal informatiesystemen efficiënter moeten zijn dan het controleren van grote hoeveelheden gegevens. De ervaring leert echter dat de systeemgerichte controle niet in de plaats komt van, maar een aanvulling vormt op de gegevensgerichte controle en dat zelfs een oppervlakkige controle van de systemen en de daaraan gerelateerde aspecten een substantieel beslag kan leggen op het beschikbare controlebudget. Dit budget is gebaseerd op een offerte waarin het controleren van informatiesystemen vaak niet expliciet is opgenomen. Het beoordelen van informatiesystemen wordt door veel accountants nog gezien als onbetaald meerwerk. Zo zijn er in elk geval

financiële, of liever gezegd commerciële redenen die de soms beperkte aandacht voor informatietechnologie kunnen verklaren.

Andere redenen zijn niet-financieel van aard. Verplaatst u zich voor de aardigheid eens in de verantwoordelijk vennoot. U leidt de jaarrekeningcontrole, u bent verantwoordelijk voor het eindresultaat en u geeft uiteindelijk ook de accountantsverklaring af; u heeft dan ook een bepalende invloed op de samenstelling en de uitvoering van het controleprogramma. Als we uw omstandigheden in ogenschouw nemen, is het geenszins verwonderlijk dat informatietechnologie in dit controleprogramma niet altijd een prominente plaats krijgt. Want wat wil het geval? In de eerste plaats heeft u waarschijnlijk geen bijzondere affiniteit met informatietechnologie – als dat wel zo was, had u vast een andere studie gekozen en was u geen accountant geworden. In de tweede plaats bent u evenals de andere vennoten van uw generatie opgeleid in een periode waarin informatiesystemen nog niet zo belangrijk waren als zij tegenwoordig zijn; hiervoor hoeven we niet eens zo ver terug te gaan in de tijd. Misschien heeft u het vak nog geleerd van vennoten die het vak hebben geleerd van vennoten die het vak hebben geleerd toen er nog helemaal geen computers waren. In de derde plaats heeft u net als de meeste mensen een stevig vertrouwen in gegevens die worden geproduceerd door geautomatiseerde informatiesystemen en ziet u de noodzaak van het controleren van dit soort gegevens niet direct in. In de vierde plaats constateert u terecht dat uw cliënten er niet om vragen en hun rekening gewoon betalen. En ten slotte weet u zich gesteund door het feit dat de meeste van uw collega's dezelfde benadering volgen.

Zo zijn er ook niet-financiële redenen die een integrale benadering van informatietechnologie in de jaarrekeningcontrole nog belemmeren. En wat is een beter moment om deze redenen weg te nemen dan tijdens de basisvorming van elke toekomstige vennoot, de accountantsopleiding?

Informatiebeveiliging

De tussentijdse conclusie is duidelijk: informatietechnologie zou een elementair onderdeel van elke accountantsopleiding moeten vormen. Aan deze universiteit is dat ook zo; tijdens de opleiding wordt onder meer ingegaan op de risico's die aan de toepassing van informatietechnologie verbonden kunnen zijn en welke maatregelen men zou kunnen treffen om die risico's te beheersen. Een deel van deze maatrege-

len wordt tegenwoordig samengevat onder de noemer informatiebeveiliging, het derde onderwerp van dit verhaal. Volgens een algemeen aanvaarde definitie wordt hiermee 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.[34] Een onderwerp ook dat zeer in de belangstelling staat, om redenen die aan het begin van dit verhaal aan de orde kwamen. We zagen al dat beveiliging voor de accountant een belangrijk onderwerp is, 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. Ook zagen wij dat de beschikbaarheid van deze systemen van groot belang kan zijn voor de continuïteit van de bedrijfsvoering. In de colleges besteedt ons docententeam de nodige aandacht aan informatiebeveiliging, maar dan wel als onderdeel van het veel bredere pakket aan beheersingsmaatregelen dat een organisatie kan treffen en dat voor de accountant van belang kan zijn. In de colleges worden die beheersingsmaatregelen behandeld 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. Wij leren aanstaande accountants om in de jaarrekeningcontrole 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 riskante projecten en systemen vindt vervolgens een beoordeling van de getroffen beheersingsmaatregelen plaats. 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, auto-

matiseringsbedrijven en adviesbureaus. Door hun lidmaatschap onderwerpen zij zich aan strenge regels ten aanzien van hun deskundigheid, hun gedrag en de uitoefening van hun beroep.

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-facto-standaarden voor het inrichten van dit soort maatregelen zijn gaan gelden.

Een bekend voorbeeld hiervan is de Code voor Informatiebeveiliging.[35] 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.[36] 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.[37] Deze schermutselingen doen niets af aan het feit dat ISO 17799 een zeer goede en nuttige standaard is, waarmee elke organisatie 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 gewerkt kan worden. Het maakt beveiliging tastbaar. Een aantal grote organisaties gebruikt 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.

Een andere relevante *standard of due care* is 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.[38] 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 .[39] 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 diens accountant behoefte bestaan aan het verkrijgen van zekerheid over de opzet en de werking van de beheersingsmaatregelen bij de serviceorganisatie.[40] Die zekerheid kan worden geboden door het uitvoeren van een *au-*

dit. 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-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 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 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, netjes alle normen heeft getoetst en die normen heeft 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 vaker voor dan het laatste. Andere discussiepunten hebben betrekking op de omvang, 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.[41]

En daarmee komen we terug op het onderwerp beveiliging. De Delftse hoogleraar Bob Herschberg, in menig opzicht de grondlegger van het vakgebied informa-

tiebeveiliging 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 stelde hij zich naar eigen zeggen ten doel op empirische gronden de hypothese te verwerpen dat de beveiliging van systemen in orde was.[42] Hoopte Herschberg aanvankelijk wellicht nog dat zijn publicaties tot een verbetering zouden leiden,[43] 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.'[44] 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 applicaties en de beveiliging van de technische infrastructuur.

1. De beveiliging van applicaties

In tegenstelling tot verwachtingen die nog maar tien jaar geleden werden uitgesproken, is het aantal tegelijkertijd in gebruik zijnde applicaties de laatste jaren niet afgenomen, maar sterk 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/server-applicaties, ERP-systemen, webomgevingen en kantoorapplicaties. De daarbij gebruikte beveiligingstechnieken hebben de afgelopen tien jaar een snelle ontwikkeling doorgemaakt. Authenticatie en autorisatie bleven echter 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. Ik volsta 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[45] en identiteitsfraude.[46]

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 steeds dezelfde aanpak kan volgen. De praktijk leert overigens 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 om versleuteling te kunnen toepassen, maar sinds een paar jaar kun je de benodigde standaardmodules op basis van standaardprotocollen gewoon van internet halen.[47] 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. Wat kunnen we hierover nog zeggen? Gevoelige bestanden zijn tegenwoordig vrij toegankelijk voor elke medewerker, het versturen van vertrouwelijke documenten via het inherent onveilige internet is de gewoonste zaak van de wereld, en de digitale kantoortuin blijkt een ideale omgeving voor de verspreiding van virussen, wormen, Trojaanse paarden en andere schadelijke software. Vooral hier wreekt zich de dominantie van een enkele leverancier. Kwetsbaarheden in de producten van zo'n leverancier zijn onmiddellijk over de hele wereld bekend en het exploiteren van deze kwetsbaarheden kan in zeer korte tijd leiden tot een schade die wereldwijd in

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

2. Beveiliging van de technische infrastructuur

Wij concluderen dat er in de beveiliging van onze applicaties nog wel iets te verbeteren valt. Al deze applicaties maken gebruik van een technische infrastructuur die u in veel opzichten kunt vergelijken met de kruipruimte onder uw huis. Er is één verschil: in een echte kruipruimte is meestal niet zoveel te beleven, maar in de digitale kruipruimte vindt u een groot aantal actieve componenten, waaronder langdradige en draadloze netwerkverbindingen, servers, mainframes, routers, printers, intelligente kopieermachines, bureaucomputers, draagbare computers en mobiele telefoons. Al die componenten worden bestuurd door systeemprogramma's waar u de fouten gratis bij krijgt, die doorgaans geconfigureerd zijn op maximaal gebruiksgemak en die worden geleverd door een zeer klein aantal leveranciers. Met andere woorden, de componenten in onze infrastructuur zijn inherent onveilig. Op zich is dit niet zo erg, als we er in zouden slagen die onveiligheid te beheersen en tot een aanvaardbaar niveau terug te brengen. Dat dit geen sinecure is, blijkt uit onderstaand voorbeeld.

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 doorzocht; 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 voor de registratie van alle zogeheten IT-middelen. De netwerkbeheerder blijkt een externe functionaris te zijn 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 in-

formatie 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 te zijn 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 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-mail bericht – 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 de gangbare normen. Dat betekent dat willekeurige gebruikers zich op deze systemen alle rechten kunnen toe-eigenen.

Een van de conclusies van dit waar gebeurde verhaal 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? Laten wij het er op 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: als de accountant tijdens de jaarrekeningcontrole voldoende aandacht besteedt aan de toepassing van informatietechnologie, dan zal hij constateren 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.

Een blik vooruit

Zo tegen het einde van dit verhaal lijkt het passend een korte blik vooruit te werpen. Informatietechnologie zal zich de komende decennia verder ontwikkelen en zal ook de komende jaren een voedingsbodem vormen voor nieuwe toepassingen die kunnen leiden tot een wezenlijke verandering in de manier waarop organisaties werken. Ook voor accountants zullen deze ontwikkelingen veranderingen met zich meebrengen: standaarden als eXtensible Business Reporting Language (XBRL) ma-

ken nieuwe vormen van verslaggeving mogelijk, waarbij ondernemingen niet alleen een papieren jaarverslag uitbrengen, maar ook via elektronische kanalen continu op maat rapporteren aan specifieke groepen belanghebbenden.[48] Diezelfde accountants zullen als gevolg van de recente boekhoudschandalen de komende jaren ongetwijfeld strenger gaan controleren. Zij zullen niet alleen dieper moeten spitten in de boekhouding zelf, zij zullen vanuit hun primaire functie ook meer aandacht moeten besteden aan zaken die een directe of indirecte invloed op de jaarrekening kunnen hebben, waaronder informatietechnologie. Tegelijkertijd zal hun kennis over informatietechnologie vanzelf toenemen. De huidige generatie opgroeiende accountants krijgt informatietechnologie immers met de paplepel ingegoten – tijdens de opleiding, in de dagelijkse werkzaamheden en als recreatief gebruiker. Het is mijn stellige verwachting dat het beoordelen van informatiesystemen op korte termijn een standaardonderdeel zal vormen van elke controleofferte. De accountant zal dit soort werkzaamheden in toenemende mate zelf uitvoeren, maar zal bij specialistische vraagstukken rond de beveiliging van de technische infrastructuur altijd een beroep op de IT-auditor blijven doen.

Dan de leerstoel IT en Auditing. De gedachte om deze leerstoel in te stellen, is ontstaan in de gouden jaren aan het eind van de vorige eeuw, toen sommige mensen nog dachten dat informatietechnologie eeuwige groei zou brengen, dat accountants alles konden en dat het @-teken hip was. Op grond van dit gegeven zou u tot de slotsom kunnen komen dat deze leerstoel niet meer is dan het verlate product van een hype die al lang en breed is overgewaaid. En eerlijk gezegd is dat ook wel zo. Maar zie hoe de zaken kunnen lopen: de hype is over, maar het product ervan lijkt actueler te zijn dan ooit.

Ook over de toekomst van deze leerstoel kan ik kort zijn. Mijn horizon beperkt zich hier tot een jaar of drie. In die periode ga ik gewoon doen wat een deeltijdhoogleraar wordt geacht te doen. Dat is onder meer het geven en organiseren van colleges over informatietechnologie en accountancy als onderdeel van de postdoctorale accountantsopleiding. Ik zal gastdocenten bij deze colleges blijven betrekken omdat ik vind dat zij studenten veel kunnen leren, bijvoorbeeld door in het college hun eigen praktijkervaringen met de studenten te delen of door ze inzicht te geven in hun eigen specialisme. Ik zie ook uit naar het begeleiden van studenten en promovendi; het verrijkt je kennis en verschaft je nieuwe inzichten, bijvoorbeeld over de manier waarop grote ondernemingen reageren op beveiligingsincidenten,[49] over de verschillen en overeenkomsten tussen ITIL en Cobit,[50] over de relatie tussen strate-

gisch en operationeel beveiligingsbeheer, of juist het ontbreken daarvan,[51] over de kwaliteit van de algemene beheersingsmaatregelen bij ondernemingen die indirecte e-commerce bedrijven[52] of over de toepasbaarheid van standaarden als de Code voor Informatiebeveiliging in netwerkorganisaties.[53] Fundamenteel onderzoek zal ik niet verrichten – daarvoor is mijn aanstelling te beperkt. Wel zal ik samen met een aantal collega's, ook van andere universiteiten, nadenken over het opzetten van een postdoctorale opleiding risicomanagement. Hieraan lijkt op dit moment een zekere maatschappelijke behoefte te ontstaan.

Dankwoord

Geachte aanwezigen, aan het einde gekomen van mijn rede zou ik nog een kort woord van dank willen uitspreken tot degenen die mij de afgelopen jaren in bijzondere mate hebben voorzien van inspiratie, ondersteuning, advies en kritiek.

Beste collega's aan de Universiteit aan Amsterdam,

Jullie ben ik grote dank verschuldigd. Philip Wallage, Hans Leenaars, Arnold Schilder, Martin Hoogendoorn: het is een eer en genoegen met jullie samen te mogen werken. De wijze waarop jullie een niet-accountant in jullie midden hebben opgenomen, getuigt van bijzondere klasse. Cynthia van Leeuwen, Regina Meijer en Miranda Branje, dank voor jullie inzet. Peter de Wolff en Ad van Engelen ben ik erkentelijk voor hun prikkelende commentaar. De docenten IT en Auditing dank ik voor de vele colleges die zij de afgelopen jaren hebben verzorgd.

Beste collega's bij KPMG,

Dank voor jullie inzet en enthousiasme. In het bijzonder dank ik Debby Uitermarkt voor haar professionele ondersteuning, Ruben de Wolf voor zijn snelheid van schakelen, Abbas Shahim voor zijn gedrevenheid, Paul Overbeek voor de telepathische samenwerking, Piet Veltman voor zijn kritische blik, Cees Coumou voor de zwakke signalen, Dries Neisingh voor de bemiddeling, Ronald Paans voor een goede leerschool, Henk Bronts voor de aanmoediging en de partners en medewerkers van

KPMG Information Risk Management voor het vormen van een sterk en slagvaardig team.

Lieve familie,

Wim Lindgreen, Atie Bolsenbroek en Bep Wolthuis, dank voor jullie stille, maar zeer gewaardeerde steun. Daphne en Rinske, dank voor de draadloze communicatie en de goede zorgen. Bo, je bent meer dan een broer voor me. Herl, fantastische vader, dank voor alles. Ten slotte dank ik Marianne Bauman, mijn toekomstige echtgenote, en Erik, Marijn en Lucas, mijn grote helden.

Beste studenten,

Op uw schouders rust straks de verantwoordelijkheid de eer van de stand hoog te houden. Daarin zult u alleen slagen als u in de praktijk weet te brengen wat deze universiteit – geen hogeschool – u probeert te leren: het stellen van vragen en het zoeken naar antwoorden. Ik wens u veel nieuwsgierigheid.

Ik heb gezegd.

Noten

1. www.security.nl.
2. *Kwetsbaarheid op internet, Samen werken aan meer veiligheid en betrouwbaarheid*, Ministerie van Verkeer en Waterstaat, Directoraat-Generaal Telecommunicatie en Post, juli 2001.
3. Kat, M., Crisis in de accountancy, *Intermediair*, nummer 24, 13 juni 2002.
4. Centraal Bureau voor de Statistiek, *CBS Persbericht PB02-125*, 24 juni 2002.
5. Zie bijvoorbeeld Stair, R.M. en Reynols, G.W., *Principles of information systems*, 4th Edition, Course Technology, 1999, ISBN 0-7600-1079-X.
6. Noordam, P., Van der Vlist, A., en Derksen, B., *Trends in IT 2002*, ten Hagen Stam, ISBN 90-440-0494-8.
7. Meuldijk, A.M., De rol van de accountant in ERP-implementatieprojecten, *Compact 2000/2*, pp. 32-40.
8. Vopak stopt acuut met ERP-project, *ITlogistiek*, maart 2002.
9. Krim, J., Microsoft, States Hold Firm As Case Enters Final Stages, *Washington Post*, 20 juni 2002.
10. Delen, G.P.A.J., Verhaar, J., en Wesselman, H.J., Outsourcing, insourcing – de sourcing-cyclus, *World Class IT*, Tutein Nolthenius, 's-Hertogenbosch, 2000, pp. 83-105, ISBN 90-72194-61-6.
11. Brynjolfsson, E., en Hitt, L.M., Beyond The Productivity Paradox, *Communications of The ACM*, volume 41:8 (August 1998), pp. 49-55.
12. Wallage, Ph., Auditing Theory, *Handboek Accountancy*, Samsom Bedrijfsinformatie, Alphen aan den Rijn, 1993.
13. Wallage, Ph., *Corporate governance en de rol en functie van de accountant*, Vossiuspers AUP, Amsterdam, 1995.
14. In het voorjaar van 2002 hebben de Nederlandse beroepsorganisaties voor accountants NIVRA en NOvAA gezamenlijk aanvullende onafhankelijkheidsvoorschriften voor accountants ontwikkeld. De aanvullende regelgeving, die onder meer ingaat op conflicterende combinaties van controle en adviesdiensten, is gebaseerd op de aanbevelingen voor onafhankelijkheid die in mei 2002 werden uitgegeven door de Europese Commissie.
15. Starreveld, R.W., De Mare, H.B., en Joëls, E.J., *Bestuurlijke Informatieverzorging deel 1*, 4e druk, Samsom Bedrijfsinformatie, Alphen aan den Rijn/Brussel, 1994.
16. Het vaststellen en verifiëren van de identiteit van een entiteit wordt in beveiligingsjargon aangeduid met het Anglicisme *authenticatie*. Het toekennen van bevoegdheden op basis van die identiteit heet *autorisatie*.
17. Zie Burgerlijk Wetboek, artikel 365 e.v.
18. Zie bijvoorbeeld The Standish Group, www.standishgroup.com.

19. Beerens, H., De kille jaren voorbij, in: *ITlogistiek*, december 2001.
20. Van Beek, J.J., Donkers, J.A.M., en Lof, K.M., Het belang van ICT binnen due diligence onderzoeken, *Compact 1999/4*, pp. 13-21.
21. Fijneman, R.G.A., *De betekenis en inhoud van 'jaarrekening ICT-auditing' als onderdeel van de jaarrekeningcontrole, 'Common body of knowledge'- Consequenties voor de accountantsopleiding*, proefschrift, Tilburg University Press, 1999, ISBN 90-361-9989-1.
22. Messier, W.F., *Auditing, a systematic approach*, McGraw-Hill, ISBN 0-07-041575-7.
23. Knechel, W.R., *Auditing, Assurance & Risk*, South-Western College Publishing, 2nd edition 2001, ISBN 0-324-02213-1.
24. International Federation of Accountants, Education Committee, *Information Technology for Professional Accountants, Exposure Draft IEG-11*, september 2001.
25. Burgerlijk Wetboek, artikel 393, lid 4.
26. De Koning, F., Beoordeling van de interne controle in het kader van de jaarrekeningcontrole, *Maandblad voor Accountancy en Bedrijfskunde*, juni 2002, pp. 272-280.
27. Nederlands Instituut van Registeraccountants, RAC 401, Controle in een omgeving waarin gebruik wordt gemaakt van geautomatiseerde informatiesystemen, *Richtlijnen voor de Accountantscontrole*, 2000.
28. Nederlands Instituut van Registeraccountants, RAC 402, Overwegingen bij controles van huishoudingen die gebruikmaken van serviceorganisaties, *Richtlijnen voor de Accountantscontrole*, 2000.
29. Nederlands Instituut van Registeraccountants, *Studierapport 34 - Normatieve maatregelen voor de geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole*, 1995.
30. De Nederlandsche Bank, *Regeling Organisatie en Beheersing*, 2001.
31. American Institute for Certified Public Accountants, *SAS no. 94: The Effect of Information Technology on the Auditor's Consideration of Internal Consideration of Internal Control in a Financial Statement Audit*, april 2001.
32. Tucker, G.H., IT and the Audit, *Journal of Accountancy*, september 2001, pp. 41-43.
33. American Institute of Certified Public Accountants, Reports on the Processing of Transactions by Service Organisations, Statement on Auditing Standards No. 70, 1992.
34. Zie bijvoorbeeld Overbeek, P.L., Roos Lindgreen, E. en Spruit, M., *Informatiebeveiliging onder controle*, Pearson Education, Financial Times / Prentice Hall imprint, 2000, ISBN 90-430-0289-5.
35. *Code voor Informatiebeveiliging*, Nederlands Normalisatie-instituut, 2000.
36. ISO/IEC 17799:2000, *Code of Practice for Information Security Management*, 2000.
37. 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.
38. www.itil.co.uk.
39. *ITIL Security Management*, The Stationery Office, Office of Government Commerce, 2000, ISBN 011330014X.

40. Veltman, P., Third party review en -mededeling bij uitbesteding van IT-services, *Compact*, september 1995.
41. www.aicpa.org.
42. Popper, K.R., *The logic of scientific discovery*, Unwin Hyman, 1959, ISBN 0-04-44-5934.
43. Zie Herschberg, I.S., The Hacker's Comfort, *Computers & Security*, 1989, Vol. 8. ISSN 0167-4048.
44. Herschberg, I.S., Al Goed. In: *Bewaar Me* (eds. H.J. van den Herik en E. Roos Lindgreen). Afscheidsrede, Technische Universiteit Delft, pp. 201-216, 1998, ISBN 90-901-1372-X.
45. Brands, S.A., *Rethinking public key infrastructures and digital certificates – building in privacy*, proefschrift, Technische Universiteit Eindhoven, 1999.
46. Grijpink, J., Identiteit als kernvraagstuk in een informatiesamenleving, in: *Handboek Fraudepreventie*, Samson, Alphen aan den Rijn, 1999, hoofdstuk Fraude en integriteit, nr. E 4010.
47. Dierks, T., en Allen, C., *RFC 2246, The TLS protocol, version 1.0*, The Internet Society, 1999.
48. De Haas, M., eXtensible Business Reporting Language: e-Reporting?, *Maandblad voor Accountancy en Bedrijfskunde*, april 2002, pp. 183-187.
49. Hafkamp, W.H.M., De 'mission impossible' van Computer Emergency Response Teams, *Informatiebeveiliging* (nog te verschijnen), 2002.
50. Leicester, E.F., *In welke mate sluiten ITIL en Cobit op elkaar aan?*, afstudeerscriptie, Universiteit van Amsterdam, 2001.
51. Koot, A., *Enhanced Security Management, informatiebeveiliging verankerd in een dynamische Business Alignment theorie*, afstudeerscriptie, Universiteit van Amsterdam, 2002.
52. Stramrood, J., *Administratieve organisatie en interne controle bij indirecte e-commerce ondernemingen*, afstudeerscriptie, Universiteit van Amsterdam, 2001.
53. Van Mierlo, S., *Informatiebeveiliging binnen netwerkorganisaties*, afstudeerscriptie, Universiteit van Amsterdam, 2002.