Prof. L. C. van Zutphen RA

Een beveiligingsverklaring in het jaarverslag?

Een commentaar op het rapport van de Commissie-Franken inzake Computercriminaliteit vanuit het gezichtsveld van de accountant en de EDP-auditor

Inleiding

In april j.l. verscheen het rapport Informatietechniek en Strafrecht van de Commissie computercriminaliteit. De commissie werd in november 1985 ingesteld door de Minister van Justitie en stond onder voorzitterschap van de Leidse hoogleraar in het strafrecht prof. mr. H. Franken. Uitgaande van de aanhoudende technische ontwikkelingen op het gebied van computer- en datacommunicatiesystemen had de commissie tot opdracht te onderzoeken of het bestaande materiële en formele strafrecht nog toereikend is, om passend te kunnen optreden tegen gedragingen met betrekking tot deze apparatuur met schadelijke gevolgen.
Het rapport is ook voor niet-juristen een interessant document. En wel in het bijzonder vanwege de opvattingen van de commissie ter zake van computerbeveiliging en de rol die ter bevordering daarvan ook aan accountants wordt toebedacht.
Een eerste vraag die bij de lezer zou kunnen opkomen is wat een accountant eigenlijk met strafrecht te maken heeft. Maar wie kennis neemt van het rapport en met name hoofdstuk V (Bijzondere onderwerpen) zal ontdekken dat de relatie met de accountancy dan ook niet via het strafrecht, maar via het burgerlijk recht tot stand komt.

Samenvattend komen de redeneringen van de commissie op het volgende neer. De noodzaak tot beveiliging, als preventiemiddel tegen computercriminaliteit en -misbruik, krijgt in het rapport een centrale plaats toebedeeld. Maar 'het primaat daarvan moet worden gegeven aan de eigen verantwoordelijkheid van bedrijven en instellingen' (t.a.p. blz. 97). Heeft de overheid dan in het geheel geen taak tot het afdwingen van beveiligingsmaatregelen, of op zijn minst het bevorderen daarvan? De commissie ziet, gelet op de reeds bestaande (ontwerp) regulering en de praktische omstandigheden 'noch de noodzaak, noch de wenselijkheid om door middel van wetgeving terzake van beveiliging, *die met behulp van straffen te handhaven is*, een verplichting tot, en eisen ten aanzien van, beveiliging in te voeren' (t.a.p. blz. 98).

Wordt aldus het strafrecht uitgeschakeld, aan het burgerlijk recht wordt wel een functie in de beveiligingssector toegekend en wel als volgt. Gelet op het algemeen belang, door de Commissie-Franken nader aangeduid als het belang van de maatschappij bij een ongestoorde gegevensverwerking, dient er toch een drempel tegen nonchalance en nalatigheid te worden opgeworpen. En wel door:

1 een meer algemeen werkende regulering, die aansluit bij de wettelijke regels met betrekking tot de jaarverslaggeving (Boek 2, titel 8 BW);
2 regulering in bijzondere als vitaal beoordeelde sectoren (bijvoorbeeld de financiële sector).

Het eerste voorstel uitwerkend wordt gepleit voor het opnemen van een verklaring van het bestuursorgaan in het jaarverslag inhoudende dat de beveiliging conform een door haar ingesteld reglement is uitgevoerd, zodat het bestuur 'instaat voor de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking' (t.a.p. blz. 99).
De door de commissie gehanteerde begrippen: betrouwbaarheid en continuïteit zijn gelijk aan de definities van NIvRA geschrift 26.[1] De accountant zou deze beveiligingsverklaring van het bestuur vervolgens dienen te toetsen aan het reglement en publiekelijk moeten uitspreken of deze al dan niet terecht is afgegeven.

Bij het tweede voorstel wordt onder meer in overweging gegeven toezichthoudende instanties in de financiële sector een rol te geven bij de beoordeling van de kwaliteit van de beveiliging.
In dit verband wordt opgemerkt dat De Nederlandsche Bank in het recent verschenen jaarverslag over 1986[2] een standpunt inneemt dat qua bedoeling overeenstemt met de ideeën van de Commissie-Franken, maar waarbij het zwaartepunt toch meer verlegd wordt naar het accountantsoordeel.
De Nederlandsche Bank acht vanuit haar toezichthoudende rol met het oog op een mogelijke bedreiging van de continuïteit van kredietinstellingen twee aspecten relevant te weten de handhaving van de betrouwbaarheid (het frauderisico) en van de continuïteit (het uitvalrisico).

'In a nutshell' komen de voorstellen van de Commissie-Franken hierop neer:

- Computerbeveiliging moet;
- het bestuur is hiervoor verantwoordelijk;
- opname van verantwoordingsinformatie over de kwaliteit van de beveiliging in het jaarverslag;
- de accountant dient deze informatie te toetsen en hierover publiekelijk te rapporteren.

Als geheel spreken deze voorstellen mij aan; zij vormen een weldoordacht en sluitend geheel. Maar met welke praktische problemen zal de uitwerking

ervan gepaard gaan? Vooral als we daarbij letten op de twee hoofdrolspelers: het management en de accountant?

Computerbeveiliging; enkele stellingen en uitgangspunten

De beheersing van informatievoorziening en automatisering is in de praktijk een zeer ingewikkeld management-proces. Het ontwikkelen en operationeel houden van geautomatiseerde systemen moet voldoen aan eisen van effectiviteit, efficiency, beheersbaarheid, betrouwbaarheid, continuïteit en controleerbaarheid. Geen van deze eisen mag als zodanig worden verabsoluteerd. Voor het management zal het altijd gaan om het realiseren van een optimale mix van deze eisen in de eigen organisatorische omgeving. Zo kan er bijvoorbeeld spanning ontstaan tussen de vereiste service-graad van een systeem (effectiviteit) en een rigoureus doorgevoerde toegangscontrole (betrouwbaarheid). In het algemeen zullen de organisatorische omstandigheden en de kostenverhoudingen de doorslag geven bij de keuze van een haalbare en betaalbare oplossing.
Vanuit deze context staan de - in de vorm van een tiental uitgangspunten en stellingen - kerngedachten zoals deze bij de schrijver leven ten aanzien van de beveiliging tegen computercriminaliteit weergegeven in het onderstaande schema.

1 Managers worden bij geautomatiseerde gegevensverwerking geconfronteerd met een samenstel van risico's:
   - ontwikkelingsrisico;
   - foutenrisico;
   - continuïteitsrisico;
   - risico schending privacy en bedrijfsgeheim;
   - risico van computercriminaliteit.
2 De kansen op computercriminaliteit nemen toe naarmate de kwaliteit van de beveiliging afneemt.
3 Het topmanagement draagt de primaire verantwoordelijkheid voor een haalbaar en betaalbaar beveiligingsbeleid en de uitvoering daarvan.
4 Naast managers dragen ook anderen een gedelegeerde of eigen verantwoordelijkheid;
   te noemen zijn: de automatiseringsstaf, gebruikers van systemen, beveiligingsfunctionarissen, adviseurs, computerleveranciers, software-houses, accountants, EDP-auditors, beroepsorganisaties, normalisatie-instituten en de overheid.
5 Er ontstaat eerst dan een adequaat bestrijdingspotentieel tegen computercriminaliteit en -misbruik als het probleem op brede schaal, met inschakeling van alle in stelling 4 genoemde participanten wordt aangepakt.
6 Toezicht en controle zijn onmisbare componenten van een sluitend beveiligingssysteem.
7 Bij de beoordeling van enig beveiligingssyteem in relatie tot de risico's van computercriminaliteit dient het zwaartepunt te worden gelegd op de in redelijkheid daaraan te stellen eisen (reasonable assurance).
8 Zolang er geen duidelijke beveiligingsnormen zijn bestaat de neiging zeer (of té) hoge eisen te stellen.
9 Risico's van computercriminaliteit zullen er altijd bestaan.
10 Bij materiële schade als gevolg van computercriminaliteit blijkt achteraf de beveiliging altijd onvoldoende te zijn geweest.

De beveiligingsverklaring in het jaarverslag

Het meest intrigerende deel van de voorstellen betreft de inhoud van de beveiligingsverklaring in het jaarverslag alsmede de aard en betekenis van de accountantstoets. In het rapport wordt over beide zaken betrekkelijk weinig gezegd en er worden nauwelijks praktische aanwijzingen gegeven. De directie zou in een reglement moeten regelen aan welke eisen de beveiliging in het bedrijf moet voldoen. In het jaarverslag zou vervolgens moeten worden aangegeven dat de beveiliging conform het reglement is uitgevoerd, zodat de directie *instaat* voor de betrouwbaarheid en continuïteit van de gegevensverwerking. Dit betekent uiteraard een zware opgave: gedurende de verslagperiode *instaan* voor een permanente goede naleving van de gegeven voorschriften. Maar er zijn meer onderwerpen die de aandacht vragen zoals:

- Op welke risico's - en derhalve categorieën van beveiliging - moet de managementverklaring betrekking hebben?
- Wat verwachten gebruikers van het jaarverslag terzake? Zowel wat betreft de te verstrekken informatie als de toetsing door de accountant.
- Dient elk jaar een beveiligingsverklaring te worden opgenomen?
- Aan welke onderwerpen en bewoordingen voor de beveiligingsverklaring wordt gedacht?
- Wanneer kan gesproken worden van voldoende beveiliging?

Vooral de beantwoording van de laatste vraag is mijns inziens cruciaal. Elke organisatie of zelfs onderdeel daarvan kent zijn eigen specifieke risico's en de leiding zal een daarop afgestemd beveiligingssysteem moeten inrichten. De praktijk leert dat algemene beveiligingsrichtlijnen voor de organisatorische omgeving en computertoepassingen (general en application controls), hoe gedetailleerd ook opgesteld, altijd een vertaalslag behoeven naar de concrete situatie. Bij dit alles staat het management voor de moeilijke taak risico's en belangen alsook kosten en baten af te wegen. Wat de inhoud van de beveiligingsverklaring betreft gaan mijn gedachten uit naar de volgende onderwerpen waarover informatie zou kunnen worden verschaft:

- een beknopte weergave van de kwaliteit van het beveiligingssysteem;
- het aangeven van de gronden waarop dit oordeel is gebaseerd;
- het aangeven van eventuele correctieve acties naar aanleiding van de accountantstoets.

Als voorbeeld - en niet meer dan dat - zou voor een grote organistie de volgende tekst kunnen dienen:

'Voorbeeld van een beveiligingsverklaring in het jaarverslag van een grote organisatie

Onze vennootschap onderhoudt zodanige systemen van beveiliging en interne controle dat de informatiesystemen en gegevens in redelijke mate gewaarborgd zijn tegen ongeautoriseerd of toevallig gebruik c.q. wijziging, vernietiging en/of openbaarmaking daarvan. De beveiligings- en controlesystemen voorzien in adequate taakverdelingen en verantwoordelijkheidsstellingen en daaraan aangepaste procedures. Alle daarbij betrokken medewerkers zijn dienovereenkomstig geïnstrueerd. Zonodig vinden systeemaanpassingen plaats als gevolg van technische ontwikkelingen, organisatie-wijzigingen en dergelijke.
Regelmatig vinden er controles plaats op de werking van het systeem. Daarenboven worden zowel opzet als werking systematisch onderzocht en getest door onze interne accountantsafdeling en het externe accountantskantoor XYZ & Co. Alle bevindingen zijn door de directie overwogen en hebben - indien de kosten/baten-verhouding dit rechtvaardigde - tot aanpassingen geleid. De directie is van mening dat op het moment van publikatie van dit jaarverslag het bij de NV ABC werkzame beveiligings- en controlesysteem aan in redelijkheid te stellen eisen voldoet.'

Zoals uit de tekst blijkt krijgen de beveiliging, alsook de controle en het toezicht op de goede werking van het systeem in deze grote organisatie kennelijk veel aandacht. Maar, hoe te handelen in het middelgrote of kleinere bedrijf? Ook in ons land kan een explosieve groei worden waargenomen van de automatisering juist in deze sector.
Kleinschaligheid in organisatie en automatisering beperken de beveiligingsmogelijkheden in het algemeen sterk. Zowel in de organisatorische sfeer (bijv. gebrekkige functiescheidingen), maar evenzeer in de sfeer van procedures, software (standaardpakketten) en apparatuur (diskettes, utilities en dergelijke).

De toets door de accountant en de EDP-auditor

De accountantsfunctie, zoals wij die nu kennen, vloeit in essentie voort uit de behoefte aan controle bij de gebruikers van verantwoordingen. Deze willen de zekerheid dat het verantwoordingsverslag dat zij onder ogen krijgen een getrouwe weergave is van de uitkomsten van het gevoerde bedrijfsbeleid en van de transacties zoals deze door de verantwoordende partij zijn verricht. Niet gunstiger of ongunstiger en vrij van materiële fouten.
De behoefte aan accountantscontrole blijkt het sterkst bij te publiceren jaarrekeningen. De wetgever heeft accountantscontrole voor een groot aantal huishoudingen in onze samenleving verplicht gesteld.
In onze tijd nemen de controlebehoeften op velerlei terreinen toe. Niet alleen financiële verantwoordingen, maar ook andere objecten en aspecten staan in de belangstelling. De processen van informatievoorziening en automatisering zijn daarvan een duidelijk voorbeeld en vormen het werkgebied van de EDP-auditor.

Electronic Data Processing Auditing kan kernachtig worden omschreven als een onafhankelijke en onpartijdige beoordeling van de betrouwbaarheid, continuïteit, effectiviteit en efficiency van operationele en in ontwikkeling zijnde geautomatiseerde systemen, van de organisatie van de automatisering en van de bijbehorende technisch-organisatorische infrastructuur.[3]

In de praktijk van de EDP-auditing ziet men al bepaalde specialistische accenten zoals op apparatuur en architectuur, organisatie en toepassingssystemen, besturingsprogrammatuur en dergelijke.
Accountants en EDP-auditors werken vaak nauw samen in accountantskantoren en -diensten, zowel in het bedrijfsleven als bij de overheid, vooral in meer complexe automatiseringsomgevingen.

De Commissie-Franken stelt voor om de hiervoor besproken beveiligingsverklaring in het jaarverslag door de accountant te laten toetsen aan het reglement en hem bovendien publiekelijk te laten rapporteren of deze verklaring al dan niet terecht is afgegeven. In essentie dus controle op de juistheid en toereikendheid van de beveiligingsparagraaf in het jaarverslag.

Het is onmiskenbaar dat vele van de hiervoor aangeduide problemen ten aanzien van keuze, inrichting en onderhoud van het beveiligingssysteem ook op het toetsingswerk van de accountant zullen terugslaan. Maar daarnaast wordt de accountant geconfronteerd met enkele additionele vragen zoals:

1 Welke extra toetsing is nodig in vergelijking tot de jaarrekeningcontrole, of met andere woorden welke zijn precies de doelstellingen van de beveiligingstoets?
2 Welke toetsingsnormen en -methoden moeten daarbij worden gehanteerd? Is een toets aan de hand van het (interne) reglement voldoende, of dient de beveiliging ook op (minimale) algemeen aanvaarde richtlijnen te worden getest?
3 Wanneer kan worden gesproken van een beveiligingsniveau dat voldoet aan 'redelijke eisen'? Zoals hiervoor betoogd kan dit per organisatieeenheid verschillen. De eindconclusie van de accountant zal in ieder geval gebaseerd zijn op een zekere mate van subjectieve oordeelsvorming (professional judgement).
4 Hoe rapporteert de accountant het toetsingsresultaat?

Wat deze laatste vraag betreft zijn in NIvRA geschrift 26 voor een nadere gedachtenvorming nuttige praktische voorbeelden opgenomen.[1] In principe staan de accountant alle rapportage-vormen ten dienste behoudens de standaard accountantsverklaring die gereserveerd dient te blijven als verklaring van getrouwheid bij jaarrekeningen. In de vorm van accountantsrapporten, managementletters, rapporten van bevindingen en separate mededelingen beschikt de accountant over voldoende communicatiemiddelen om zowel bestuursorganen, toezichthouders als het publiek te informeren.

Slotopmerking

Managers en accountants krijgen in de voorstellen van de commissie belangrijke taken en verantwoordelijkheden toebedeeld bij het organiseren en handhaven van adequate beveiligingssystemen bij bedrijven en instellingen. Hoewel de gedachtengangen van de commissie in principe logisch en sluitend zijn, moeten voor de uitvoering ervan nog vele praktische problemen worden opgelost. Dit artikel heeft hieraan een bijdrage willen leveren.

Literatuur

1 Mededelingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking, *NIvRA geschrift* no. 26, Kluwer Deventer 1982.

2 *De Nederlandsche Bank Jaarverslag 1986*, pagina's 110 en 111. Kluwer Deventer april 1986.

3 L. C. van Zutphen, EDP-auditing, een poging tot verduidelijking. *Maandblad voor Accountancy en Bedrijfshuishoudkunde*, november 1985.