compact

COMPUTER EN ACCOUNTANT

Klynveld Kraayenhof & co
ACCOUNTANTS

NUMMER 21 7E JAARGANG VOORJAAR/ZOMER 1980

compact

VAN DE REDACTIE

In dit lentenummer 1980 zijn de volgende hoofdartikelen opgenomen:

- Het gebruik van de computer in de accountantscontrole — door A.H.C. Koedijk.
- Privacy-problematiek en geautomatiseerde gegevensverwerking — door drs. H.C. Kocks en A.W. Neisingh.

  Dit artikel is geschreven om te worden opgenomen in het septembernummer van het "Tijdschrift voor sociale geneeskunde". Duidelijk een andere lezerskring dan die van Compact.
  Toch heeft de redactie gemeend dit artikel, alsmede de "samenvatting" van het "Advies inzake registratie van medische en psychologische gegevens en de bescherming van de persoonlijke levenssfeer, uitgebracht door een commissie van de Gezondheidsraad", in Compact te moeten opnemen aangezien KKC cliënten heeft in de medische sector.

De vaste rubrieken zijn - na de onderbreking bij het voorgaande Compact-nummer - weer opgenomen.
A.B.C.-Nieuws verzameld door drs. H.C. Kocks en het literatuuroverzicht samengesteld door H.J.M. van der Wielen.

De redactie stelt graag ruimte in dit blad beschikbaar voor reacties op bovengenoemde bijdragen.

Compact is een uitgave van de Automatisering en Controle Groep van Klynveld Kraayenhof & Co.

Het doel van deze uitgave is informatie te verstrekken over ontwikkelingen op het gebied van automatisering en controle in binnen- en buitenland.

Deze informatie is in de eerste plaats bestemd voor diegenen, die in de algemene controlepraktijk werkzaam zijn.

Redactie:
Prof. D. Steeman, A.W. Neisingh, J. Philippo en H.J.M. van der Wielen (plv. lid).

Adres:
Pr. Irenestraat 59,
1077 WV Amsterdam.

HET GEBRUIK VAN DE COMPUTER IN DE ACCOUNTANTSCONTROLE

door A.H.C. Koedijk

Inleiding

Door een toenemend gebruik van computers bij de administratieve gegevensverwerking, waarbij (eveneens in toenemende mate) gebruik wordt gemaakt van beeldschermen en andere technische hulpmiddelen ten behoeve van invoervastlegging en uitvoerpresentatie, wordt papier als informatiedrager teruggedrongen. Niet alleen wordt informatie steeds meer opgeslagen in niet direct voor de mens leesbare vorm, het is ook steeds meer de vraag of informatie op voor de accountant bruikbare wijze periodiek zichtbaar wordt gemaakt.
De computer biedt de accountant evenwel ook mogelijkheden om in zijn informatiebehoefte te voorzien. Het gebruik van de computer in de accountantscontrole is bovendien doelmatig te achten indien sprake is van omvangrijke gegevensverzamelingen. Dit laatste is steeds meer het geval ten gevolge van in omvang gegroeide ondernemingen.
In dit artikel zal worden ingegaan op het gebruik van de computer in de accountantscontrole met betrekking tot verificatie en beoordeling van gegegevens (het onderzoek van gegevensverzamelingen). Op het door de accountant inschakelen van de computer bij de beoordeling van de handhaving en naleving van de organisatorische maatregelen in en rond de geautomatiseerde processen zal hier niet worden ingegaan. Benadrukt moet echter worden, dat de accountant ook hierbij technieken ten dienste staan.

Bewerkingen

Met betrekking tot de wensen die bij de accountant ten aanzien van de uit te voeren werkzaamheden kunnen leven, kunnen de volgende voorbeelden worden gegeven. Deze bewerkingen zijn met behulp van de computer vrij eenvoudig uit te voeren.

a. Het zichtbaar maken van op media als banden en schijven vastgelegde informatie.

b. Het maken van een selectie (bijvoorbeeld een steekproef) uit een gegevensverzameling.

c. Het op een andere wijze sorteren van gegevens, bijvoorbeeld omdat de bestaande volgorde niet overeenstemt met de archivering van documenten.

d. Het uitvoeren van controleberekeningen.

e. Het toetsen van gegevens aan normen (zoals een gemiddeld opslagpercentage op verkopen).

f. Het bijhouden van eigen totalen (bijvoorbeeld grootboeksaldi).

Mogelijkheden

De accountant kan met betrekking tot het inschakelen van de computer bij zijn controle-activiteiten een keuze doen uit een drietal mogelijkheden:

a. standaard audit packages;

b. eigen, per geval, te ontwikkelen programmatuur;

c. voorzieningen op (laten) nemen in toepassingsprogrammatuur van de gecontroleerde.

Altijd zal de controleprogrammatuur zodanige totalen moeten opleveren, dat de volledigheid van de te controleren bestanden vastgesteld kan worden door middel van aansluiting met totalen bij de gecontroleerde.

Ad a. Standaard audit packages

Aan het ontwerp van audit packages lag de algemene doelstelling ten grondslag, dat ze eenvoudig hanteerbaar moesten zijn voor gebruikers die slechts over enige algemene computerkennis beschikken.
Audit packages zijn dan ook zeer geschikt voor accountants die niet kunnen beschikken over eigen automatiseringsspecialisten. Een ander voordeel van audit packages is, dat ze zijn uitgetest; door de accountant zelf ontwikkelde programmatuur zal altijd (soms zeer uitgebreide) testinspanningen vergen, om de juiste werking van de programmatuur aan te tonen. (Ter handhaving van de onafhankelijkheid zal de accountant ook bij het gebruik van een pakket tests moeten uitvoeren; deze tests hebben echter een eenmalig karakter.)
Nadat oorspronkelijk alleen Amerikaanse accountantskantoren deze pakketten offreerden, richten thans ook softwarehouses (programmatuurleveranciers) zich op deze markt.
Audit packages kunnen bruikbaar worden geacht indien de probleemstelling (de wensen van de accountant) eenvoudig kan worden ontleed in elementaire handelingen (zoals die globaal beschreven zijn onder het hoofd "Bewerkingen").

Ad b. Eigen programmatuur

In dit geval zal meestal gebruik gemaakt worden van een "hogere" programmeertaal zoals COBOL of RPG. Bij het gebruik van deze talen hoeft niet tegemoet te worden gekomen aan beperkingen die wel vaak gelden bij het gebruik van audit packages. Voordelen zijn bovendien, dat kennis van deze talen toegepast kan worden op vele computersystemen en dat de uitvoering op de computer vaak efficiënter geschiedt dan bij een audit package toepassing.
Tegenover deze voordelen staan als nadelen de hoge kosten van het ontwikkelen van deze programmatuur. Bovendien is de inzet van automatiseringsspecialisten noodzakelijk.
Deze (overigens niet alleen voor accountants, maar algemeen geldende) nadelen leiden ertoe, dat steeds meer zogenaamde gebruikersvriendelijke talen worden aangeboden. De retrieval-talen zijn hiervan voorbeelden. Deze talen beogen een grote flexibiliteit en tevens een relatief eenvoudig gebruik. Binnen ons kantoor wordt ten behoeve van de accountantscontrole gebruik gemaakt van de retrieval-taal CA/EARL. Door het gebruik van deze taal kunnen veelal relatief goedkope toepassingen worden gerealiseerd.
In het kader van de samenwerking in KMG-verband') kunnen wij inmiddels beschikken over een tweetal andere retrieval-pakketten, te weten EDP-Auditor en CARS IV.

') KMG staat voor Klynveld Main Goerdeler.

Ad c. Voorzieningen in programmatuur van de gecontroleerde

Een voorbeeld van deze derde mogelijkheid is het in een grootboekmutatie-programma opnemen van een routine die een steekproefselectie vervaardigt van de mutaties.
Bij deze methode komt de onafhankelijkheid van de uitvoering van het controleprogramma van de accountant in het geding, doordat de "wandel" van de programmatuur, waarin de controleroutine is geïntegreerd, zich goeddeels aan zijn waarneming onttrekt.
Er kan een aantal maatregelen worden genomen om dit bezwaar te ondervangen, maar de methode is niet te prefereren, ook omdat de gecontroleerde bekend raakt met een deel van het controleprogramma. De methode kan echter wel nuttig zijn met betrekking tot interne controledoeleinden.

Het opzetten van de controletoepassing

Indien de accountant bij het opstellen van een nieuw controleprogramma, respectievelijk het herbeoordelen van een bestaand controleprogramma, mogelijkheden ziet tot geautomatiseerde uitvoering van bepaalde onderdelen, zal hij (na overlegd te hebben met de administratie van de gecontroleerde), indien mogelijk, contact opnemen met een op automatisering en controle gespecialiseerde collega-accountant of met een edp-auditor. Vastgesteld zal moeten worden of lonende toepassingen kunnen worden gerealiseerd. Indien de uiteindelijke ontwikkeling van de toepassing door een programmeur zal worden verzorgd (zoals bij de AC-Groep van KKC doorgaans het geval is), is het zaak, gezien de bij deze functionaris aanwezige ervaring met en gedetailleerde kennis van de mogelijkheden van de computer, deze in een vroeg stadium in het overleg te betrekken.

Vervolgens zal bij de gecontroleerde informatie moeten worden verkregen over de bestanden, informatiedragers en dergelijke. Indien de toepassing mettertijd op de computer van de gecontroleerde zal worden uitgevoerd, dient eveneens informatie te worden verkregen over de computerconfiguratie en de beschikbare programmeertalen. Verder zullen met de gecontroleerde afspraken moeten worden gemaakt inzake het aan de accountant beschikbaar stellen van kopieën van de benodigde bestanden. Hierna zal de toepassing ontwikkeld kunnen worden.

Plaats van verwerking

Ook met betrekking tot de plaats waar met de controleprogrammatuur zal worden gewerkt, heeft de accountant de keuze uit een drietal mogelijkheden:

a. indien aanwezig, de eigen computer;

b. een computerservicebureau;

c. de computer van de gecontroleerde.

In geval a. bereikt de accountant maximale onafhankelijkheid. Informatie afkomstig van vele computersystemen kan worden verwerkt, hoewel een conversie van bestanden soms noodzakelijk is.

Indien de accountant niet beschikt over een eigen computer, dient hij, ten einde een voldoende mate van onafhankelijkheid te bereiken, te overwegen de verwerking te laten geschieden bij een servicebureau (leverancier van computerbeschikbaarheid).
Soms wenst de gecontroleerde, dat bestanden het bedrijf niet verlaten. Ook kan het zijn, dat een vereiste bestandsconversie moeilijk of onmogelijk is. In dergelijke gevallen zal uitvoering van de controlehandelingen met behulp van de controleprogrammatuur op de computer van de gecontroleerde noodzakelijk zijn.

In het laatste geval dient de accountant maatregelen te nemen om zoveel mogelijk te voorkomen dat

- controleprogrammatuur (die immers een deel van het controleprogramma bevat) door de gecontroleerde wordt gekopieerd;
- de uitvoering van de programmatuur door de gecontroleerde wordt beïnvloed;
- de betrokken bestanden op enigerlei wijze worden veranderd ten einde de resultaten van de verwerking te beïnvloeden.

Hoewel de accountant voor dit doel maatregelen ter beschikking staan, geldt als nadeel toch wel de geringere onafhankelijkheid.
Indien de gegevensverwerking ten behoeve van de accountant bij een "derde" (bijvoorbeeld een servicebureau) plaatsvindt, dient de accountant de geheimhouding van de gegevens van de gecontroleerde te waarborgen.

Documentatie en beveiliging

De documentatie van de controletoepassing alsmede de beveiliging van programmatuur, documentatie en bestanden, moet, net als bij "gewone" toepassingen

- een soepel verloop van de produktie waarborgen;
- wijzigingen in de toepassing op eenvoudige wijze mogelijk maken;
- reconstructie mogelijk maken;
- het beheer van de toepassing eenvoudig overdraagbaar maken.

De bestandsbeveiliging krijgt een extra dimensie, omdat het gaat om gegevens van een gecontroleerde.

Ten behoeve van het kunnen afleggen van verantwoording, moeten in de documentatie tevens worden vastgelegd:

- uitvoeringsverslagen;
- informatie omtrent geldigheidsperioden van programmatuurversies en de inhouden van deze versies.

Nawoord

Veel controletoepassingen zijn binnen onze maatschap reeds ontwikkeld. Naast de, meest voorkomende, grootboekcontroles zijn onder meer computerprogramma's ontwikkeld ten behoeve van de controle op:

- debiteuren (saldobiljetten; afloopcontrole);
- verkopen (verantwoorde winst);
- inkopen;
- lonen en salarissen;
- effecten;
- pensioenen;
- inventarisaties;
- kosten;
- interest (nacalculatie);
- concernconsolidaties.

(Bovenstaand artikel is gebaseerd op de gelijknamige publikatie in het Handboek Accountancy, een coproduktie van A.W. Neisingh en de schrijver van deze bijdrage aan Compact.)

COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.

PRIVACY-PROBLEMATIEK EN GEAUTOMATISEERDE GEGEVENSVERWERKING IN DE GEZONDHEIDSZORG

door drs. H.C. Kocks en A.W. Neisingh

Inleiding

Vele vrije beroepsbeoefenaren leggen - al dan niet wettelijk verplicht - dossiers aan van door hen verrichte werkzaamheden en/of onderzoekingen. Gesteld kan worden dat de medische stand eveneens dossiervorming kent. Hierbij dient vooral gedacht te worden aan de ontstane patiëntendossiers, welke een grote hoeveelheid en verscheidenheid aan medische gegevens kunnen bevatten met betrekking tot de gezondheidstoestand van personen. Het systeem van verwijzen van patiënten door de (huis)arts naar specialisten enz. heeft met zich gebracht dat van één patiënt op meerdere plaatsen een dossier wordt aangelegd, waardoor slechts moeilijk een totaalbeeld van de gezondheidstoestand van de patiënt wordt verkregen. Met andere woorden een centraal actueel dossier ontbreekt. Dit probleem is ten dele ondervangen doordat artsen en specialisten patiëntengegevens onderling uitwisselen. Deze uitwisseling kon echter (en kan in vele gevallen thans nog) niet à la minute plaatsvinden.

Zoals in bijna alle sectoren van de samenleving is de automatisering ook aan de medische wereld niet voorbijgegaan. Door de invloed van de automatisering is de termijn van gegevensuitwisseling weliswaar verkort, doch het probleem van de multipele dossiervorming en het niet beschikken over een actueel dossier niet opgelost. De vraag blijft of in de toekomst de multipele dossiervorming geheel zal verdwijnen.

Afgezien van het al of niet up-to-date zijn van gegevensverzamelingen met medische (patiënt)gegevens zijn er twee aspecten die in deze tijd - waarin de gedachte van de bescherming van de persoonlijke levenssfeer opgeld doet - bijzonder in de belangstelling staan, namelijk:

- welke informatie over personen mag worden opgeslagen in gegevensverzamelingen;
- de beveiliging van die opgeslagen informatie tegen onrechtmatige inzage en gebruik.

Gezien het feit dat vooral in de gezondheidszorg wordt gewerkt met gegevens, die de persoonlijke levenssfeer raken, heeft een Commissie van de Gezondheidsraad zich met voornoemde aspecten beziggehouden. Dit heeft geresulteerd in richtlijnen dienaangaande welke als bijlage bij dit artikel zijn opgenomen.
In dit artikel wordt nader ingegaan op die voorstellen, echter nadat eerst de meer algemene aspecten met betrekking tot de automatisering en bestaande privacy-opvattingen zijn belicht.

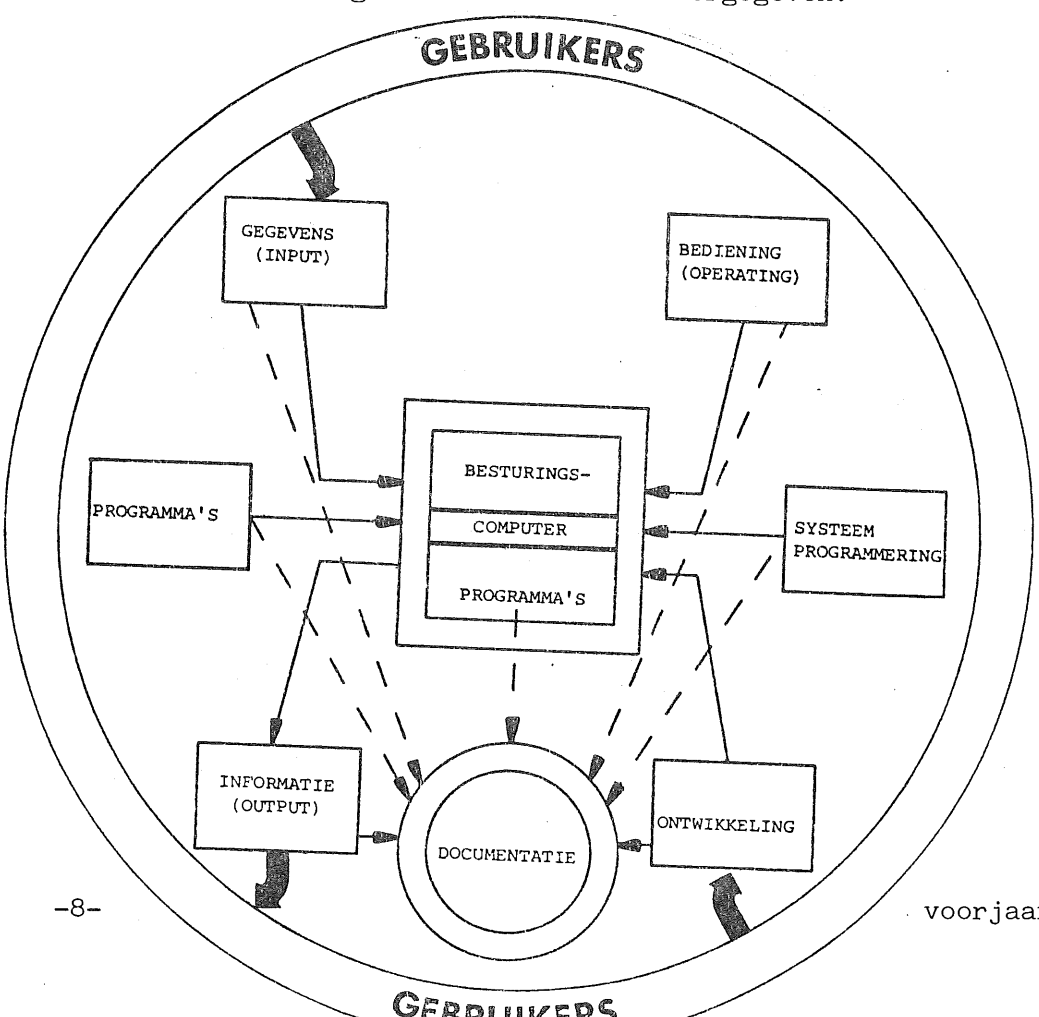
In de literatuur met betrekking tot de bescherming van de persoonlijke levenssfeer worden twee belangrijke begrippen gehanteerd die een nadere toelichting verdienen: privacy en data security.

Privacy omvat de bescherming van personen. Hierbij dient bescherming te worden gezien als het slechts vastleggen van noodzakelijke informatie omtrent personen met betrekking tot een bepaald doel. Als over privacyregels wordt gesproken dienen deze aan te geven: welke gegevens over personen mogen worden vastgelegd, wie daarin inzage mag hebben, wie vastgelegde informatie mag verspreiden en hoe vertrouwelijke gegevens moeten worden bewaard.

Data security handelt over de beveiliging van gegevens die met betrekking tot personen worden vastgelegd, waarbij onder beveiliging dient te worden verstaan de maatregelen die genomen (kunnen) worden tegen ongeautoriseerde toegang tot, modificatie en gebruik van gegevens.

Organisatie van de automatisering

Meestal gaat aan de aanschaf van een computer een onderzoek (feasibility study = toepasbaarheidsonderzoek) vooraf. Op grotendeels economische gronden/motieven wordt bepaald of automatisering voordelen biedt. Op die onderzoekfase wordt niet nader ingegaan.
Het zal echter duidelijk zijn dat met alleen een computerinstallatie niet veel kan worden gedaan. Het is een stuk elektronisch vernuft dat zonder "bijbehoren" geen enkel economisch nut heeft. Naast de reeks instructies die essentieel zijn voor de werking en het onderhoud van de installatie (besturingsprogramma's) moet de apparatuur door iemand worden bediend (operator). Om gegevens te laten verwerken om een bepaald resultaat (informatie) te verkrijgen dient een reeks instructies of opdrachten te worden geschreven, gecodeerd in een voor een computer aanvaardbare vorm (programma). Het schrijven van een programma kan pas plaatsvinden als door een persoon/afdeling (gebruiker) is geïnventariseerd wat moet worden geautomatiseerd (systeemeisen) en op welke manier (systeemontwerp). Van voornoemde activiteiten dienen op een uniforme voorgeschreven wijze vastleggingen te worden gemaakt (documentatie) om het onderhoud (maintenance) aan systemen en programma's mogelijk te kunnen maken. In de volgende figuur is een en ander nog eens schematisch weergegeven.



Terug naar de gezondheidszorg. In het simpelste geval gaat een zelfstandig praktizerend arts tot automatisering over. Hij/zij ziet er zodanige voordelen in dat tot aanschaf van een kleine computer wordt overgegaan om het patiëntenbestand te automatiseren. Hij/zij vervult alle functies van systeemontwerper tot operator toe. Daarnaast is de arts de enige gebruiker. De patiëntendossiers worden zogenaamd "op de computer" gebracht waardoor gegevensverzamelingen (bestanden) ontstaan. De inhoud van die verzamelingen is door de arts (gebruiker) bepaald. Ten aanzien van gegevens, die de persoonlijke levenssfeer van de patiënt raken, heeft de arts eigen (privacy-)normen aangelegd. Bovendien heeft de arts maatregelen genomen opdat geen vertrouwelijke gegevens in verkeerde handen terecht kunnen komen (data security). Immers alleen hij/zij is gebruiker en alleen hij/zij mag inzage hebben in de geautomatiseerde patiëntengegevens (dossiers).
Uit oogpunt van privacy en data security zal het duidelijk zijn dat deze situatie niet afwijkt van die van een praktizerend arts die zijn/haar patiëntendossiers op een conventionele manier bijhoudt. Hiermee zij aangetoond dat de aspecten privacy en data security reeds bestonden vóórdat automatisering haar intrede deed.
Uit het volgende zal duidelijk worden waarom privacy en data security, vooral als het om automatisering gaat, meer nadruk hebben gekregen.

Na het simpele geval van alleen praktizerend arts wederom een gestileerde situatie, doch dichter bij de realiteit liggend.
Een aantal specialisten in een ziekenhuis besluit om gezamenlijk een computer aan te schaffen om hun patiëntendossiers te automatiseren.

Elke specialist houdt zijn eigen bestand waarvan gegevens aan hem/haar beschikbaar worden gesteld door middel van eigen programma's. Voor de bediening van de computer en de ontwikkeling van systemen en programmatuur worden gespecialiseerde medewerkers aangetrokken die in een apart deel van de organisatie worden ondergebracht. De automatiseringsorganisatie is ontstaan met de twee belangrijke functies ontwikkeling en produktie.

In deze situatie bepaalt elke specialist als gebruiker wat in zijn/haar bestand opgenomen wordt, waarbij weer de eigen privacy-normen gelden. Bepaald is dat de specialist alleen informatie uit zijn/haar eigen patiëntenbestand mag kunnen krijgen. Binnen de automatiseringsafdeling dienen nu zodanige maatregelen te worden genomen, dat dàt ook alleen maar mogelijk is. De data security ligt dus niet meer bij de enkele specialist doch is gedelegeerd aan de automatiseringsafdeling. Doordat het risico is toegenomen dat data security leemten kan vertonen, zodat vertrouwelijke informatie bij onbevoegden terecht kan komen, dienen de privacy-normen aangepast te worden.

De derde situatie, die zal worden geschetst, is reeds in een bepaalde mate realiteit. De verwachting is dat dergelijke situaties in de toekomst steeds meer zullen ontstaan.
De situatie is identiek aan de voorgaande met de volgende verschillen.

Elke specialist houdt geen eigen gescheiden bestand en om de informatie in/uit de bestanden op te nemen/te verkrijgen wordt gebruik gemaakt van gezamenlijke programmatuur. Hoewel elke specialist zelf wenst te bepalen wat hij/zij inhoudelijk in het bestand wil opnemen, is het risico van onbevoegd gebruik van gegevens sterk toegenomen vanwege het feit dat met dezelfde programmatuur verschillende gebruikers uit één en hetzelfde bestand dezelfde soort gegevens/informatie wensen te verkrijgen.
Binnen de automatiseringsorganisatie dienen ook hier zodanige maatregelen te zijn genomen dat inzage in gegevens door onbevoegden niet mogelijk mag zijn.

Gezien het feit dat - in casu - gebruikers (specialisten) inzage (kunnen) verkrijgen in gegevens, die mede door anderen zijn vastgelegd, ontstaat behoefte aan een gemeenschappelijke privacy-norm (norm ten aanzien van vastleggen van privacy-gevoelige gegevens). Er dient voorzichtiger te worden omgesprongen met gegevens die de persoonlijke levenssfeer van de patiënt raken.

De ontwikkeling om te komen tot een gemeenschappelijke privacy-norm in de medische wereld is gezien de aanbevelingen van de commissie in een gevorderd stadium. De behoefte aan een wetgeving echter kan gestalte krijgen indien:

- in de praktijk een algemeen aanvaardbare norm is ontstaan/gegroeid die om een wettelijke status vraagt; en/of
- de overheid als objectief vertegenwoordiger van de gemeenschap (de patiënten) van mening is dat een wet nodig is opdat een ieder duidelijk is welke normen/regels dienen te gelden.

Gesteld kan worden dat in casu van beide punten aspecten terug te vinden zijn in "het advies" van de commissie, waarbij als belangrijk motief naar voren komt de uitbanning van het gevaar van rechtsongelijkheid.

Tot nu toe is alleen gesproken over de geautomatiseerde verwerking van persoonsgegevens. Eén van de volgende - logisch te verwachten - stappen in het gehele proces van automatisering van de (medische) gegevensverwerking zal (kunnen) zijn de koppeling van patiëntengegevens (resultaten onderzoek, opnamegegevens, enz.) met facturering aan patiënt of ziekenfonds (eventueel gevolgd door de uitwisseling van factuurgegevens op magneetband c.q. online tussen bijvoorbeeld ziekenhuis en ziekenfonds).
Uit het voorgaande blijkt dat - gezien de concentratie van activiteiten en de te verwachten ontwikkelingen in de toekomst - de automatiseringsorganisatie een zo belangrijke rol speelt in het geheel, dat daaraan bepaalde eisen dienen te worden gesteld. Optimale privacy-bescherming en betrouwbare verwerking van (medische) gegevens is zonder een goede automatiseringsorganisatie niet mogelijk. In een achttal (0 t/m 7) punten wordt weergegeven welke eisen aan een automatiseringsorganisatie moeten worden gesteld. De eerste drie eisen zijn van algemene aard, de volgende hebben betrekking op de systeemontwikkeling (3 t/m 5), de produktie (6) en de beveiliging (7).

Algemeen

0. De organisatorische plaats van de automatiseringsafdeling binnen de totale organisatie dient zodanig te zijn dat ze onafhankelijk is van beschikkende en bewarende functies (bij voorkeur hiërarchisch rechtstreeks onder de hoogste leiding).

1. De organisatie van de automatiseringsafdeling dient in grote lijnen duidelijk vast te liggen.

2. De verdeling van de functies binnen de automatiseringsafdeling dient zodanig te zijn dat de ontwikkeling en de verwerking gescheiden zijn. Indien aanwezig dient de systeemprogrammering gescheiden te zijn van ontwikkeling en produktie.

Algemene voorschriften met betrekking tot de ontwikkeling enz. van systemen

3. Er moeten algemene voorschriften zijn met betrekking tot de ontwikkeling en het in gebruik nemen van nieuwe systemen. Deze voorschriften moeten betrekking hebben op:

   - systeemontwerp en -analyse,
     programmering,
     testen,
     acceptatie,
     conversie;
   - actieve participatie van degenen die uiteindelijk gebruik zullen maken van de gegevens die door deze systemen worden opgeleverd;
   - beoordeling en goedkeuring na elke belangrijke fase in de ontwikkeling (onder andere door de leiding van de automatiseringsafdeling, gebruiker(s), controlefunctionarissen).

4. Er moeten algemene voorschriften zijn met betrekking tot het wijzigen van systemen (inclusief programma's). Deze voorschriften dienen dezelfde componenten te bevatten als is aangegeven onder punt 3.

5. Er moeten algemene voorschriften zijn met betrekking tot het documenteren van systemen en individuele programma's.

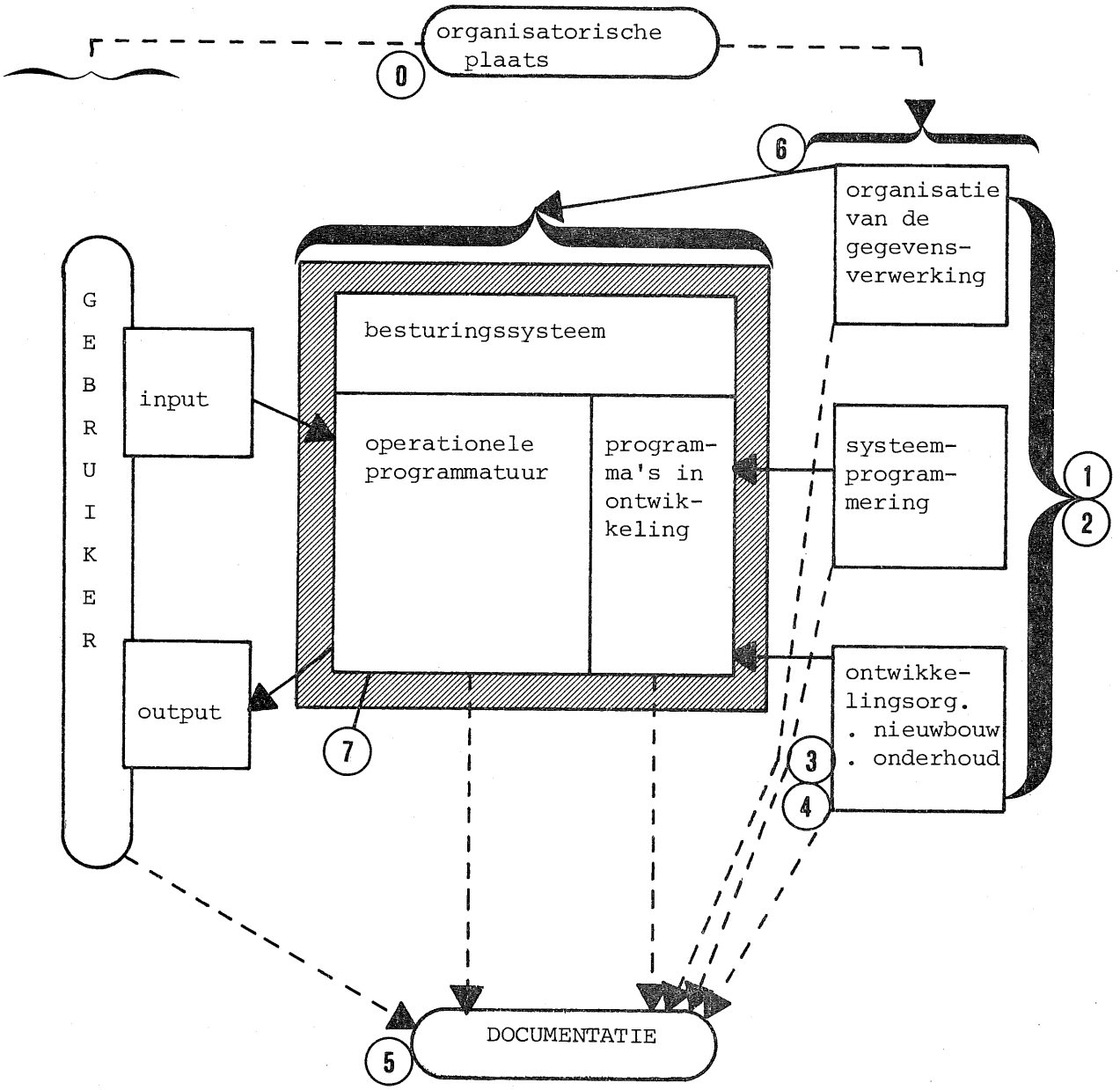
Algemene voorschriften en maatregelen met betrekking tot de verwerking

6. Er moeten zodanige voorschriften en procedures zijn dat de gegevensverwerking betrouwbaar kan worden geacht.

Algemene voorschriften en maatregelen met betrekking tot de beveiliging

7. De algemene voorschriften en maatregelen met betrekking tot de beveiliging dienen zodanig te zijn dat de continuïteit van de gegevensverwerking en -verstrekking is gewaarborgd.

De punten geven schematisch het volgende te zien:



Geautomatiseerde systemen

Geautomatiseerde systemen staan niet op zichzelf. Zij vormen een onderdeel van een informatiesysteem voor de gehele organisatie. Bij elk geautomatiseerd systeem is een zogenaamd voor- en natraject aanwezig, dat buiten de automatiseringsorganisatie ligt.
In het voor- en natraject dienen voldoende maatregelen van administratief-organisatorische aard (inclusief maatregelen van interne controle en beveiliging) te worden getroffen, waardoor het mogellijk is de invoerverzorging correct te laten plaatsvinden en de uitvoerverzorging op dienovereenkomstige wijze.
Evenals aan de automatiseringsorganisatie dienen aan geautomatiseerde systemen eisen te worden gesteld ten aanzien van de betrouwbaarheid en beveiliging. (Betrouwbaarheid, dat wil zeggen de mate van interne controle [inclusief privacy-bewaking] en beveiliging, dat zijn de maatregelen die in redelijke mate waarborgen dat de continuïteit van de gegevensverwerking verzekerd is.)

Ten aanzien van de betrouwbaarheid en beveiliging van systemen dienen de volgende eisen te worden gesteld:

1. Het geautomatiseerde systeem moet de mogelijkheid bieden om te kunnen constateren, dat de ingevoerde gegevens juist, tijdig, volledig en geautoriseerd zijn.
2. Het geautomatiseerde systeem dient de mogelijkheid te bieden om te kunnen vaststellen dat alle ingevoerde gegevens juist en volledig zijn verwerkt.
3. Een bevredigende controle moet mogelijk zijn op de door het geautomatiseerde systeem opgeleverde gegevens welke niet direct voortvloeien uit de ingevoerde gegevens.
4. Het systeem moet de mogelijkheid bieden om te kunnen constateren dat de gegevensverzamelingen juist en volledig blijven en dat de verbanden tussen de gegevensverzamelingen, indien aanwezig, gehandhaafd blijven.
5. Het systeem moet die gegevens vasthouden, welke voor controle achteraf noodzakelijk kunnen zijn.

Opgemerkt dient te worden dat, ingeval wordt voldaan aan één van de eisen ter zake van de beveiliging (bijvoorbeeld het bewaren van kopieën van gegevensverzamelingen op een andere lokatie), deze maatregelen kunnen confligeren met de eisen die uit hoofde van privacy-bescherming worden gesteld. Immers het extern bewaren ten behoeve van reconstructiedoeleinden van een kopie van een belangrijk "privacy-gevoelig" bestand roept een privacy-risico op!
Echter ook van de omgekeerde situatie kan sprake zijn: privacy versus data security.

Uit het oogpunt van privacy-bescherming verdient het aanbeveling de geautomatiseerde gegevensverwerking van de diagnoses, medicijnverstrekking en dergelijke altijd door dezelfde operator te laten uitvoeren (geheimhouding gemakkelijker te waarborgen en te controleren).

Uit oogpunt van interne controle is een dergelijke situatie echter ongewenst te achten (mogelijkheid van ongeoorloofd ingrijpen en onopzettelijke fouten in de verwerking, discontinuïteit in de bezetting bij ziekte en dergelijke).

Wil men komen tot een adequate bescherming van persoonsgebonden gegevens bij geautomatiseerde gegevensverwerking, dan kan bij de ontwikkeling van deze systemen worden gedacht aan de volgende mogelijkheden[3]:

1. Verplicht gebruik van data encryption-technieken, ter voorkoming van ongeoorloofde kennisneming van de vertrouwelijke gegevens. Deze technieken ook te gebruiken bij - uit beveiligingsoverwegingen - extern te bewaren kopieën van verzamelingen die persoonsgegevens bevatten.
2. Toekennen van classificatiecodes aan de uitvoer, zowel op papier als op andere informatiedragers. Hierbij behoren tevens voorschriften met betrekking tot de vernietiging van geclassificeerde stukken.
3. De implementatie van technieken gericht op de controle van de bevoegdheden en de identificatie van de gebruiker:
   Bijvoorbeeld het gebruik van wachtwoorden ter bescherming tegen ongeautoriseerde toegang tot (delen van) bestanden, eventueel gecombineerd met een automatisch log-off-mechanisme indien terminals gedurende een bepaalde periode niet zijn gebruikt.
   Vastleggingen dienen te worden opgebouwd van pogingen tot ongeautoriseerde toegang tot beschermde/geclassificeerde bestanden.
4. Het gebruik van waarschuwingen die in de desbetreffende toepassingsprogramma's worden opgenomen en zichtbaar op de uitvoer worden afgedrukt (papier en beeldscherm), bijvoorbeeld:

> "Attentie! Openbaarmaking van deze gegevens is in strijd met art. ... Wet Privacy-bescherming."

Het is uit velerlei oogpunten van belang een privacy-reglement te definiëren. Kuitenbrouwer[2] geeft een lijstje van aandachtpunten, te weten:

1. een nauwkeurige beschrijving van het doel van de persoonsregistratie;
2. een nauwkeurige beschrijving welke soorten gegevens mogen worden opgenomen over welke soorten van personen;
3. een voorziening voor het periodiek verwijderen van geregistreerde gegevens;
4. een beschrijving van de organisatie van het registratiesysteem met nadruk op het beheer;
5. een beschrijving van de afnemers van persoonsgegevens, onder vermelding welke soorten informatie elk van hen ten hoogste mag krijgen;
6. een regeling van het recht op inzage en correctie van geregistreerde personen met betrekking tot over hen vastgelegde gegevens.

Risicofactoren bij automatisering

Uit het voorgaande valt op te maken dat in geval van automatisering eveneens risico's worden gelopen, doch dat deze anders van aard zijn.
In onderstaand schema zijn deze risico's voor zover in het kader van dit artikel van belang (in categorieën ingedeeld) weergegeven. Tevens is vermeld welke schade kan worden veroorzaakt en welke preventieve maatregelen ter zake kunnen worden getroffen.

	Schade voor het bedrijf	Preventieve maatregelen
1. Gebruik computer door personeel voor eigen, c.q. malafide doeleinden:		
a. verwerken eigen programma's	- daaraan verbonden kosten - de toegenomen kansen op storingen in apparatuur ("spelen")	- motivatie van personeel - procedures m.b.t. planning en werkvoorbereiding, voortgangscontrole
b. gebruik aanwezige programmatuur voor eigen doeleinden	- daaraan verbonden kosten - afdrukken van (eventueel geheime) persoonsgegevens	- 2 operators per shift - speciale beveiliging van geheime en vertrouwelijke gegevens
c. verwerken eigen programma's om persoonsgegevens t.b.v. derden af te drukken (informatie inzake fysieke toestand)	- daaraan verbonden kosten - aantasting privacy - andere vormen van schade door bekend worden van niet voor derden bestemde gegevens	- procedures m.b.t. uitgifte van bestanden - afhaalsysteem voor output - datacommunicatiesystemen beveiligen met toegangscontrole - functiescheiding óók buiten normale werktijden - antecedentenonderzoek
2. Manipulaties met, resp. ongeautoriseerd gebruik van gegevens, besturingssysteem, programma's en formulieren	- niet meer juist functioneren van de programmatuur - verstrekken van onjuiste gegevens - werken met verminkte bestanden - verloren gaan van beveiligingskopieën - claims in kader van privacy-wetgeving	- motivatie personeel - antecedentenonderzoek - altijd 2 operators in computercentrum - geen systeem- en programmadocumentatie onder bereik van operating - gebruik maken van beveiligingsmaatregelen die door bibliotheekpakketten worden geboden

	Schade voor het bedrijf	Preventieve maatregelen
		- bewaring gescheiden van operating - kopieën aanhouden - strikte procedure m.b.t. programmawijzigingen
3. Moedwillige vernieling, diefstal a. apparatuur b. informatiedragers	- materiële schade - stilstand informatieverwerking - materiële schade - verlies bestanden - verlies programmatuur - stilstand informatieverwerking	- motivatie van personeel - reconstructiemogelijkheden - bewaarder informatiedragers als aparte functie - uitwijkmogelijkheid - opberging bestanden - administratie - tijdens ontslagperiode niet zonder meer op computercentrum toelaten - betrouwbaarheid operators - toegangsbeveiliging - closed shop - alarm - controle op inhoud van bestanden
4. Beïnvloeden van de goede werking van de apparatuur	- vertraging/verstoring van de gegevensverwerking	- motivatie van personeel

Een bijzonder probleem ontstaat bij het gebruik van datacommunicatiemiddelen met betrekking tot de toegang tot gegevensverzamelingen (inzage, wijzigen en dergelijke).
Op verschillende fronten wordt aan de oplossing van deze problematiek gewerkt. In de eerste plaats kunnen worden genoemd de identificatieprocedures, dat wil zeggen degene die achter de terminal plaatsneemt dient aan het systeem mede te delen wie hij is, terwijl (in een aantal gevallen) de terminal zich via een zogenaamde hardware-identificatie aan het computersysteem kenbaar maakt. Ten tweede dient er een autorisatieprocedure te zijn, die in gang wordt gezet nadat de identificatieprocedure met goed gevolg is doorlopen.
De terminalgebruiker dient slechts die programmatuur beschikbaar te krijgen waarover hij mag beschikken. In deze programmatuur dienen bepaalde functies te zijn opgenomen, zoals toevoegen van gegevens, bijwerken, opvragen en dergelijke.
In het besproken geval dient de autorisatie in de afzonderlijke toepassingsprogrammatuur te worden geregeld. Een andere mogelijkheid is ontstaan bij het gebruik van data bases. Met behulp van zogenaamde subschema's kan nu centraal worden vastgelegd wie tot welke gegevenselementen toegang heeft en tot welke acties hij is gerechtigd.

Alhoewel in vergaande mate maatregelen kunnen worden getroffen tegen ongeautoriseerde toegang tot gegevens dient toch eerlijkheidshalve te worden opgemerkt, dat mogelijkheden tot het doorbreken van de beveiligingsmaatregelen aanwezig zijn.
Bedacht dient te worden dat systeemprogrammeurs en data base administrators toegang moeten hebben - uit hoofde van hun functie - tot de toegangsbeveiligingssystemen respectievelijk de beschrijvingen van de data base. Hierin schuilt het gevaar dat zij van deze situatie misbruik kunnen maken, terwijl systeemprogrammeurs als specialisten van besturingsprogrammatuur van computers uiteraard in staat zijn de sporen van hun werkzaamheden uit te wissen!

Het Eindrapport van de Commissie Koopmans

Na de publikatie van het Eindrapport van de "Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties (zogenaamde Commissie Koopmans)" in 1976 is in de pers met een zekere regelmaat gerefereerd aan het Eindrapport.
Met betrekking tot dit Eindrapport zijn enige opmerkingen te maken.

In buitenlandse wetten en (voor)ontwerpen is voorzien in een inzage- en correctierecht voor degene van wie persoonlijke gegevens zijn opgeslagen en een recht te weten wie in een bepaalde periode persoonsgegevens heeft opgevraagd.
In artikel 69 lid 2 van het in het Eindrapport opgenomen ontwerp van wet wordt vermeld: "indien gegevens betreffende de persoon van de verzoeker in het registratiesysteem zijn opgenomen stelt de houder hem, desverlangd in schriftelijke vorm een volledig en eenvoudig te begrijpen overzicht van deze gegevens ter beschikking".
De consequentie hiervan kan zijn dat speciale maatregelen in systemen nodig zullen blijken. Dit recht op inzage en verbetering zal in vele reeds bestaande systemen kunnen leiden tot uitbreidingen van deze systemen. Programmatuur zal moeten worden ontwikkeld om aan de wet te voldoen ("in schriftelijke vorm een volledig en eenvoudig te begrijpen overzicht") en op grond van andere in de artikelen 69 t/m 74 genoemde condities[5].

Advies inzake privacy uitgebracht door een commissie van de Gezondheidsraad

Tot slot van dit artikel een aantal opmerkingen met betrekking tot het "Advies inzake registratie van medische en psychologische gegevens en de bescherming van de persoonlijke levenssfeer" (verder "Advies"), dat is uitgebracht door een commissie van de Gezondheidsraad (verder commissie).

- De gehanteerde terminologie kan (spraak)verwarring teweeg brengen. Belangrijke, inhoudelijk duidelijk verschillende, begrippen worden door elkaar gebruikt (onder andere verzameling, bestand en systeem). Automatisering verdraagt dit niet. Zij eist exacte definiëring van begrippen, die consistent dienen te worden gebruikt en slechts voor eenduidige uitleg vatbaar mogen zijn.

- Jammer genoeg heeft de commissie een term overgenomen van "de Staatscommissie Koopmans" die tot veel misverstand en onduidelijkheid aanleiding zal geven, namelijk "de houder". Deze houder wordt gedefinieerd als: degene die de zeggenschap heeft over de gegevens (pag. 54). Een definitie zonder inhoud omdat in het "Advies" door de commissie niet wordt aangegeven wat onder zeggenschap dient te worden verstaan. De commissie is het probleem "houder" uit de weg gegaan door hier en daar aan te geven wie de houder zou moeten zijn in specifieke situaties. Ze heeft nagelaten een duidelijke beschrijving van de functie van de "houder" te geven.
  Kernvragen als:

  . welke (gedelegeerde) bevoegdheden kan, mag of moet de houder, gezien zijn functie, (niet) hebben,
  . waarvoor kan, mag of moet de houder, gezien zijn funcie, verantwoordelijk worden gesteld,

  zullen bij de ontwikkeling van een functiebeschrijving niet eenvoudig te beantwoorden zijn.

- De commissie heeft geen splitsing aangebracht in privacy en data security. Daardoor komt ze tot de te algemeen gestelde conclusie: "Naar het oordeel van de commissie zouden geautomatiseerde en conventionele gegevensverzamelingen ') tot grote hoogte aan dezelfde regels kunnen worden onderworpen" (einde citaat pag. 44).
  Gezien de gedefinieerde begrippen privacy en data security in de inleiding van dit artikel gaat dat grotendeels wel op voor privacy doch niet voor data security. Hoewel - zoals reeds gezegd - data security niet aan automatisering gebonden is krijgt ze bij (toenemende) automatisering wel een andere dimensie. Daardoor zullen de privacy-normen wellicht weer worden beïnvloed waardoor een toch niet te verwaarlozen verschil in nuancering zal gaan ontstaan tussen regels voor wel en niet geautomatiseerde gegevensverzamelingen.

- In het "Advies" heeft de commissie zich helaas beperkt tot richtlijnen inzake privacy met betrekking tot gegevensverzamelingen. De organisatie van de automatisering is geheel buiten beschouwing gelaten. Daarom is in dit artikel met opzet de organisatie van de automatisering wel aan de orde gesteld. Het belang van een goede organisatie is door de commissie (?) wellicht niet onderkend voor de privacy en de data security. De regels ten aanzien van gegevensverzamelingen mogen nog zo goed zijn, als de organisatie waarbinnen die regels gestalte moeten krijgen en moeten worden geëffectueerd niet aan de eisen voldoet die in het voorgaande zijn aangegeven, zijn de regels als een huis gebouwd op drijfzand.
  Het is aanbevelenswaardig, zo niet noodzakelijk, regels en voorschriften te ontwerpen waaraan een automatiseringsorganisatie minimaal moet voldoen. Ongetwijfeld zal daarin duidelijk moeten worden aangegeven wat zeggenschap over de gegevens is, waar die moet liggen en wie die mag/moet hebben. Binnen dit totale spanningsveld zal het niet eenvoudig zijn een - noodzakelijke - functiebeschrijving voor "de houder" te ontwikkelen.

') Gewijzigd van bestanden in gegevensverzamelingen.

Enige afrondende punten

In het in het Eindrapport opgenomen voorontwerp van wet is vanzelfsprekend ook voorzien in een toezichthoudend staatsorgaan. In Nederland wordt hiertoe gedacht aan een Registratiekamer, die "bevoegd is inlichtingen in te winnen, apparatuur, programmatuur, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen vertonen, voor zover dit redelijkerwijs voor de vervulling van zijn taak nodig is" (art. 9 lid 1). Van deze stellingname zal een positieve invloed uitgaan op de organisatie.
Onafhankelijke registeraccountants moeten zeer wel in staat worden geacht het bedoelde toezicht uit te oefenen en ten behoeve van het bevoegde gezag verklaringen te geven omtrent het voldoen aan de eisen, respectievelijk het op bepaalde aangegeven onderdelen niet voldoen[6].
Immers de apparatuur die voor de persoonsgegevensverwerking wordt gebruikt, zal goeddeels dezelfde zijn die in ruime mate reeds voor de - onder accountantscontrole vallende - administratieve vastlegging wordt gebruikt.

Er is een tendens waarneembaar minicomputers in te schakelen bij de geautomatiseerde gegevensverwerking. Deze minicomputers bieden over het algemeen op bescheiden schaal dezefde mogelijkheden ten aanzien van dataccommunicatie en data base als "gewone" computers.
Probleem bij gebruik van deze mini's is dat deze in het algemeen niet zullen (kunnen) worden ingepast in een afzonderlijke automatiseringsorganisatie, omdat zij nu eenmaal juist in een kleinschaliger omgeving zullen worden gebruikt (dus ontstaan er leemtes in de organisatie).
Een ander aspect betreft de zogenaamde gebruikersvriendelijkheid van de mini's, die er de oorzaak van kan zijn dat leemtes in de beveiligingsorganisatie ontstaan, die moeilijk of in het geheel niet door compenserende controlemaatregelen elders kunnen worden opgeheven.

Literatuur

1a NIvRA-geschrift nr. 1: de automatisering en controle

1b Computer Control Guidelines

2. Het privacy-reglement en andere beleidsaspecten van gegevensregulering
mr. F. Kuitenbrouwer (Informatie nr. 10/1979)

3. De invloed van de privacy-wetgeving op de organisatie en op de geautomatiseerde informatiesystemen
A.W. Neisingh RA (Informatie nr. 10/1979)

4. EDP Audit Doelmatig instrument bij het beoordelen van de automatisering
J.H. Urbanus RA en J.M. Verheul RA (Handboek Accountancy)

5. Eindrapport Commissie Koopmans art. 69 t/m 74

6. Brief Nederlands Instituut van Registeraccountants
zie pag. 200 e.v. van het Eindrapport Commissie Koopmans

Bijlage

Samenvatting

1. Het rapport is geschreven tegen de achtergrond van het rapport van de Staatscommissie Koopmans. De Staatscommissie heeft in haar rapport van 1976 een voorontwerp van wet op de persoonsregistraties gepresenteerd. De Commissie Privacy van de Gezondheidsraad is gevraagd daarop te reageren en na te gaan in hoeverre het voorontwerp voor medische en psychologische gegevens is aan te bevelen.

2. Medische en psychologische gegevens worden verzameld in een bonte verscheidenheid, door zeer verschillende personen en instanties, op zeer verschillende manieren, voor uiteenlopende doeleinden. Omdat het - naar de Commissie zelf ondervond - moeilijk is zicht te krijgen op wat, waarvoor, hoe, door wie, wordt bewaard, heeft de Commissie een inventarisatie in het rapport opgenomen. Men vindt in één van de eerste paragrafen van het rapport een korte beschrijving van een aantal belangrijke geautomatiseerde systemen die medische gegevens bevatten. Men vindt in een volgende paragraaf een korte karakteristiek van de bewaring van diverse conventionele bestanden.

3. Het voorontwerp van de Staatscommissie Koopmans is in de eerste plaats gericht op geautomatiseerde systemen. De Commissie Privacy is er voorstandster van een wettelijke bescherming - ten aanzien van medische en psychologische gegevens - van meet af aan te laten gelden èn voor computerbestanden èn voor conventionele gegevens. De vraagstelling aan de Commissie had overigens ook betrekking op conventionele gegevens.
De Commissie heeft een aantal richtlijnen voor het beheer van medische en psychologische gegevens opgesteld die in het rapport uitvoerig zijn toegelicht. De richtlijnen zullen, hopelijk, van nut zijn bij het voorbereiden en uitwerken van het definitieve wetsontwerp.
De Commissie heeft daarnaast voor ogen gehad dat organisaties en beroepsbeoefenaren die bij het beheer van medische en psychologische gegevens betrokken zijn, rechtstreeks van het rapport zouden kunnen profiteren.

4. De laatste jaren is de behoefte aan informatie enorm gegroeid. Daartegenover (en waarschijnlijk vooral: als gevolg daarvan) is het verlangen naar meer bescherming van privacy sterk toegenomen. De Commissie vond het niet altijd eenvoudig in dit spanningsveld een keuze te doen. Men kan immers - ook als Commissie die privacy in haar naam voert - niet eenvoudigweg die oplossingen kiezen die het maximum aan privacy-bescherming voor de patiënt/cliënt bieden. Men moet steeds privacy-belangen afwegen tegen andere belangen die door een grotere en snellere beschikbaarheid van informatie gediend worden. Die andere belangen zijn bepaald niet alleen die van de gemeenschap en van organisaties en beroepsbeoefenaren, maar ook andere belangen van de betrokken persoon zelf. De spanning tussen de informatiebehoefte en de privacy is wellicht juist in de gezondheidszorg bijzonder groot omdat ook de patiënten zelf enerzijds privacy willen, maar anderzijds vaak verlangen dat de informatie in ruime mate, soms snel, beschikbaar is, bijvoorbeeld bij een spoedopname in een andere hoek van het land.

De lastige belangenafweging gecombineerd met de grote verscheidenheid van verzamelingen van medische en psychologische gegevens, maken dat de oplossingen en overwegingen van de Commissie nogal eens genuanceerd moesten zijn.

5. Mede vanwege die grote verscheidenheid van de gegevens kon de Commissie niet de pretentie hebben in haar rapport alle medische en psychologische privacy-problemen op te lossen. Men kan, bijvoorbeeld, de gegevensverzameling van een psycholoog, een ziekenhuisinformatiesysteem, en een computerbestand van de Stichting Medische Registratie bepaald niet in elk opzicht over één kam scheren. Het rapport bevat een aantal hoofdregels die (voor zover zij uitgewerkt moeten worden) voor sommige soorten bestanden tot zekere hoogte zijn toegelicht. Uitwerking zal echter voor een groot deel moeten plaatsvinden in reglementen en andere deelregelingen die voor de verschillende soorten bestanden van medische en psychologische gegevens moeten tot stand komen.

6. Hieronder zijn de door de Commissie geformuleerde richtlijnen afgedrukt. Er zij op gewezen dat voor een volledig begrip daarvan kennisname van het rapport zelf en met name de toelichting bij de richtlijnen onontbeerlijk is.

   1. Een verzameling moet een duidelijke doelstelling hebben. De houder mag gegevens niet opslaan en gebruiken voor andere doeleinden.

   2. Er mag niet meer bewaard worden dan voor het doel van de verzameling nuttig is.

   3. Gegevens mogen niet langer bewaard worden dan nodig is. Per soort verzameling dienen bewaartermijnen te worden gesteld.

   4. Wanneer het voor het doel van de verzameling niet nodig is gegevens op naam (of anderszins tot een persoon herleidbaar) te bewaren, moeten zij geanonimiseerd worden dat wil zeggen dat mogelijkheden tot herleiding ongedaan moeten worden gemaakt.

   5. In verzamelingen die worden gehouden door instellingen die niet rechtstreeks bij de curatieve gezondheidszorg betrokken zijn worden, indien de verzameling geautomatiseerd is of wordt gehouden door een organisatie die meer dan 25 personen omvat, de gegevens per persoon op nummer en niet op naam bewaard. De sleutel tot herleiding van nummers tot namen wordt door de houder (of een afzonderlijke sleutelbewaarder), apart en met bijzondere veiligheidsvoorzorgen, bewaard.

   6. Met het registreren van subjectieve indrukken, voorlopige meningen en waardeoordelen dient men zeer terughoudend te zijn, in het bijzonder wanneer het gaat om opslag in een geautomatiseerd systeem.

7.1 Het is gewenst bij het opslaan van gegevens van meet af aan met verschillen in relevantie in de tijd rekening te houden, zodat het schonen van een verzameling bijvoorbeeld vóór het opbergen in een archief, niet te veel moeite kost.

7.2 Het is gewenst bij het opzetten van een verzameling met verschillen in toegankelijkheid voor verschillende groepen gebruikers rekening te houden.

7.3 In een conventioneel bestand dienen subjectieve indrukken en, indien genoteerd, voorlopige meningen, neer te leggen in persoonlijke werkaantekeningen, zoveel mogelijk gescheiden te worden bewaard van de meer objectieve gegevens. Het verdient steeds overweging objectieve, maar zeer privacy-gevoelige gegevens slechts op te nemen in de persoonlijke werkaantekeningen.

8. Van elke verzameling moet duidelijk zijn wie de houder is. De houder dient aansprakelijk te zijn voor schade geleden door de patiënt/ cliënt ten gevolge van overtreding van de voor de verzameling geldende regels.

9.1 Een afzonderlijk reglement dient te gelden en een vergunning dient te worden vereist, voor elke verzameling die
a) geautomatiseerd is, of
b) gehouden wordt door een organisatie die meer dan 25 personen omvat.

9.2 Voor verzamelingen die niet vallen onder 9.1 dienen collectief, per soort verzameling, regels te worden gesteld.

9.3 In de reglementen en regels dient met deze richtlijnen (en natuurlijk tevens met huidige en toekomstige wettelijke regels) te worden rekening gehouden. Het reglement en de in 9.2 bedoelde regels zullen in elk geval regels moeten inhouden over: doel; houder; op te nemen gegevens; toegang; beveiliging; commissie van toezicht (indien van toepassing); gegevensverstrekking aan derden; bewaartermijn; uitoefening rechten tot weigering, inzage, correctie en vernietiging.

10. Door houders van verzamelingen van gegevens als bedoeld in 9.1 wordt òf per verzameling òf per categorie verzamelingen, een onafhankelijke commissie van toezicht ingesteld.
In de commissie hebben (mede) één of meer personen van buiten de organisatie van de houder zitting.

11. Wanneer een verzameling wordt gehouden binnen een organisatie moeten regels worden gesteld welke tot de organisatie behorende personen op welke wijze toegang tot die verzameling hebben. Daarbij dient toegang slechts te worden verleend indien en voor zover dit voor het doel van de verzameling nodig is. Uitgangspunt van de Commissie is hierbij dat het behoren tot eenzelfde functionele eenheid het wezenlijke criterium is en niet het behoren tot eenzelfde organisatie.
De toegangsregels kunnen voor verschillende groepen gebruikers verschillend zijn.

12. De patiënt/cliënt/geregistreerde heeft de volgende rechten:

    a. Voordat zijn gegevens opgenomen worden moet (behoudens uitzonderingen) duidelijk zijn, of door een kennisgeving duidelijk worden gemaakt, dat gegevens in een verzameling zullen worden opgenomen en voor welk doel dit geschiedt. De geregistreerde heeft, behoudens bij de wet bepaalde uitzonderingen, het recht opname in de verzameling te weigeren.

    b. De geregistreerde heeft recht op inzage van over hem geregistreerde gegevens. Dit recht wordt niet rechtstreeks uitgeoefend maar via een door de geregistreerde aan te wijzen vertrouwensman. De vertrouwensman moet een persoon zijn die is onderworpen aan een tuchtrecht of een beroepscode en die ten opzichte van derden een beroepsgeheim in acht moet nemen. Van het inzagerecht zijn uitgesloten persoonlijke werkaantekeningen mits degene die de aantekeningen maakt deze strikt onder zich houdt.

    c. Gegevens die onjuist zijn dienen op verzoek van de geregistreerde te worden gecorrigeerd.

    d. De houder van gegevens bewaard in het kader van de gezondheidszorg, is, behoudens bij de wet bepaalde uitzonderingen, verplicht onder een aantal in paragraaf 9.5.2 genoemde voorwaarden gegevens op verlangen van de patiënt te vernietigen of anonimiseren. Ten aanzien van gegevens bewaard voor andere doeleinden heeft de geregistreerde het recht vernietiging c.q. anonimisering te verlangen indien door de bewaring het doel waarvoor de gegevens verzameld werden niet meer gediend kan worden of wanneer de voor de bewaring gestelde termijn is verstreken.

    e. Verstrekking van gegevens aan derden is, behoudens de in paragraaf 10 aangegeven uitzonderingen, niet geoorloofd zonder uitdrukkelijke schriftelijke gerichte toestemming van de geregistreerde.

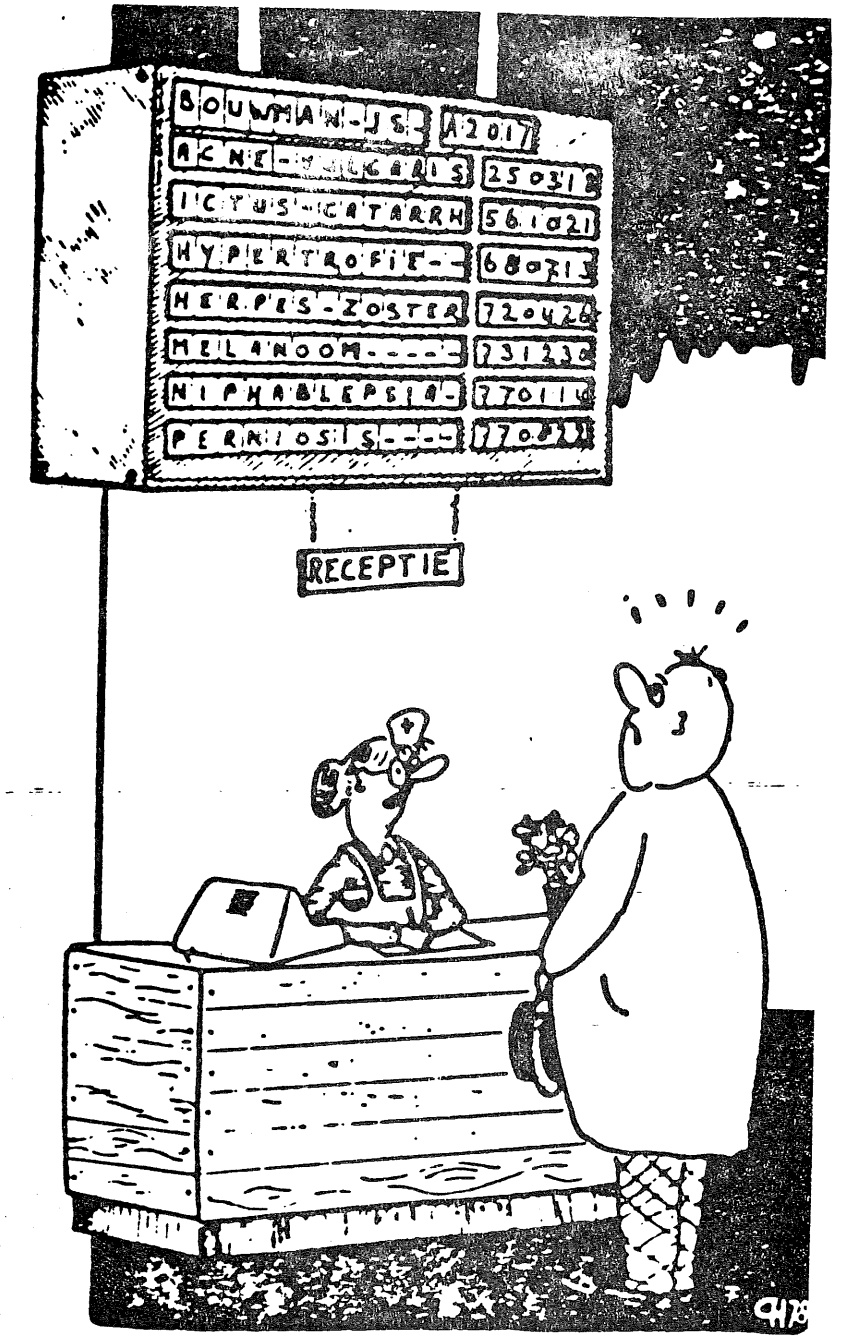
13. Aan de beveiliging van medische en psychologische gegevens dient grote zorg te worden besteed.

14. Ook geautomatiseerde systemen die medische of psychologische gegevens bevatten die niet direct tot de persoon herleidbaar zijn dienen goed beveiligd te zijn, vooral tegen personen die met behulp van thans of in de toekomst beschikbare technische middelen daaruit toch persoonsgegevens zouden willen verkrijgen. Deze systemen behoren een reglement te hebben waarin tenminste regels zijn gesteld omtrent toegang, beveiliging en gegevensverstrekking aan derden.

Namens de Commissie,

De Secretaris-rapporteur, De Voorzitter,

(mr. B. Sluyters) (dr. D. Wolvius)



"KLOPT DAT ?....."

COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.

Automatisering Beveiliging Controle NIEUWS

door H.C. Kocks

Automatisering

De automatisering en de gevolgen daarvan hebben een grote invloed op de maatschappij. De veranderingen gaan zo snel, dat het in veel gevallen aanpassingsmoeilijkheden geeft. Eén van de sectoren, die moeilijkheden heeft met de computer is de rechtspraak, en wel in het bijzonder in Engeland. De Engelse rechtspraak is er niet in geslaagd gelijke tred te houden met het fenomeen automatisering.

Aldus de inleiding van het artikel "Het gebruik van de computeroutput in de rechtszaal" in De Automatisering Gids van 5 juni 1980 dat bijna integraal is overgenomen. Naast de situatie in Engeland wordt ingegaan op de Nederlandse situatie, alsmede op die in België, Frankrijk en Duitsland.

In science-fiction-literatuur kwam de combinatie rechtbank en computer jaren geleden al voor. Een typisch voorbeeld hiervan is een verhaal van Sir Alan Herbert, waarin een computer in het getuigenbankje plaatsnam. De machine werd onder ede geplaatst en het proces verliep vlekkeloos. Echter, toen dezelfde situatie zich in werkelijkheid voordeed, verliep de zaak niet zo gladjes. De wet was op deze situatie niet voorbereid en het gevolg was dan ook, dat de door de computer verstrekte getuigenis in tweede instantie nietig werd verklaard. Het proces waar het hier om gaat speelde begin dit jaar in Groot-Brittanië. Bij een inbraak in het noorden van Engeland was een stapel bankbiljetten ontvreemd.
In het bezit van de vermoedelijke dader werden enkele van deze biljetten aangetroffen. Identificatie van de biljetten was mogelijk, aangezien het hier ging om splinternieuwe biljetten van 5 pond. Het aan de bestolene uitbetaalde bedrag was naar zijn bank gestuurd, te zamen met een computerlijst van alle serienummers. Tijdens de rechtszaak werd deze computerlijst dan ook aangevoerd als bewijsmateriaal. De advocaat van de verdachte maakte bezwaar tegen dit bewijs, op grond van het feit dat "computeroutput" in een bepaald wetsartikel niet werd genoemd als zijnde een handelsdocument. De rechter verklaarde de bezwaren echter niet ontvankelijk en de verdachte werd veroordeeld. De veroordeelde was het met de gevolgde gang van zaken niet eens en ging in hoger beroep bij het "Court of Appeal".
Tijdens de behandeling van de zaak door het "Court of Appeal" bracht de verdediging nog een extra argument naar voren. De advocaat stelde dat de computerprint niet was vervaardigd door "een persoon die persoonlijke kennis had van de inhoud, of van wie redelijkerwijze mag worden aangenomen, dat hij deze kennis had". Het is namelijk zo, dat in de Angelsaksische rechtspraak alleen bewijs dat door personen is geleverd, rechtsgeldigheid heeft. Het gevolg van de protesten van de verdediging was, dat een intensief onderzoek werd ingesteld naar de wijze, waarop de computerlijst tot stand was gekomen.

De lijst was samengesteld door een computer van de Bank of England. Het apparaat werd gevoed met stapels nieuwe bankbiljetten, die daarna werden afgetast. Tijdens dit aftasten las het apparaat de serienummers, terwijl tevens de onvolkomen biljetten werden uitgeselecteerd. Het enige wat de mens (in dit geval de operator) deed, was de stapels in de machine leggen en het serienummer van het bovenste biljet noteren. Omdat de lijst dus eigenlijk helemaal door de machine was geproduceerd waren de drie rechters van het court of appeal unaniem van mening, dat het hier geen persoonlijke getuigenis betrof. Het gevolg hiervan was, dat de lijst zijn bewijskracht verloor en de verdachte dus moest worden vrijgesproken. Bij het bekrachtigen van het eerste vonnis verklaarde rechter Bridge, die het onderzoek leidde, wel dat men hier te maken had met een maas in de Engelse wetgeving. Anders gezegd komt deze maas neer op het verschijnsel "hearsay evidence", dat wil zeggen getuigenverklaringen "van horen zeggen". De Engelse rechtbank heeft dit soort bewijs nooit geaccepteerd.

Men is druk bezig de wet te moderniseren, door ook gegevens van een computer als wettig bewijs te accepteren. De ambtelijke molens werken ook in Engeland traag, zodat het nog wel enige tijd zal duren voordat de wetgeving voldoende is ingespeeld op de huidige technische maatschappij. In 1972 werd reeds een wetsvoorstel ingediend, om ook computerprints te beschouwen als wettig bewijsmateriaal. Men is bereid om dit wetsvoorstel aan te nemen, doch dit kan pas, nadat het rapport klaar is van de "Royal Commission on Criminal Procedures.".
Zelfs al zou het wetsontwerp worden aangenomen, dan zit er nog een addertje onder het gras. In het ontwerp wordt namelijk uitsluitend gesproken van "output die is samengesteld uit aan de computer verstrekte gegevens (door de mens, dus)". Nergens wordt gerept over informatie, die het apparaat zelf vergaard heeft. Waarschijnlijk is dit te wijten aan de technologische kennis van 1972. In dat jaar was het namelijk erg onwaarschijnlijk, dat een computer zelf zijn gegevens kon verzamelen. Computers uit die tijd werkten voornamelijk met ponskaarten en ponsbanden, die werden geproduceerd door de operators. De laatste jaren zijn de computers zo perfect geworden, dat zij in staat zijn voor het grootste gedeelte zelf hun gegevens te vergaren. Dit verzamelen van gegevens gebeurt onder meer door het optisch lezen van formulieren of door meten en wegen.

Het blijkt dus, dat het wetsontwerp, van nauwelijks een decennium oud, alweer verouderd is. Het probleem wordt des te urgenter, doordat veel bedrijven en instellingen apparatuur in gebruik nemen, die is voorzien van een microprocessor. Ook deze apparatuur is in staat om output op papier te leveren en de vraag is dan in hoeverre dit als bewijsmateriaal kan dienen. Deze vraag speelt vooral een rol, als de geleverde informatie niet meer in klare tekst is gesteld, maar bijvoorbeeld in bar-code.
Het wordt tijd, dat de Britse regering zo snel mogelijk stappen gaat ondernemen, om computeroutput tot wettig bewijsmateriaal te bestempelen. Doet zij dit niet, dan is de kans zeer groot, dat computermisdaden ongestraft gepleegd kunnen worden. Hierbij komt ook nog, dat een slechte wetgeving een aantasting kan zijn van de vrijheid van het individu.

Nederlandse situatie

In het Nederlands Burgerlijk Wetboek wordt in artikel 1903 een opsomming gegeven van mogelijke bewijsmiddelen. Algemeen wordt echter aanvaard, dat deze opsomming niet limitatief is, wat wil zeggen, dat ook niet genoemde middelen als wettig bewijs kunnen dienen. In die zin is artikel 1903 dus geen belemmering voor de toelaatbaarheid van computerbewijs. Indien we ervan uitgaan, dat alle bewijsmiddelen toegelaten zijn, is de rechter normaal gesproken ook vrij in de waardering ervan. Deze vrijheid van de Nederlandse rechter staat in scherpe tegenstelling tot het Angelsaksische rechtssysteem, waar die vrijheid ten enenmale ontbreekt.

We spreken hier over computerbewijs, de vraag is wat we ons hierbij moeten voorstellen. Computerbewijs valt uiteen in een aantal categorieën, te weten: prints van de gegevens zonder meer, magnetische opslagmedia zoals schijven en banden, afdrukken van verwerkingen van de opgeslagen gegevens en tenslotte een verslag van een expert, waarin hij bepaalde bevindingen weergeeft, die hij heeft gedaan met een computer. Bij het gebruik van computerbewijs komen enkele specifieke problemen naar voren, zoals daar zijn:

Objectieve beoordeling van het systeem en zijn werking
Hierbij dient men te letten op de gekozen methode van verwerking, en op de juiste logische en technische verwerking daarvan. Beide vragen dienen door experts te worden onderzocht.

Controle van de input
De Amerikanen hanteren hiervoor het gevleugelde begrip "garbage-in, garbage out" (GIGO). Dit betekent, dat wil de output betrouwbaar zijn, dan moet ook de input juist zijn.

Juiste beoordeling van de output
Vaak is een print uit een computer slechts voor deskundigen begrijpelijk. De gegevens zullen moeten worden geïnterpreteerd, waarbij manipulatie zeer eenvoudig mogelijk is.

Privacy
Als computeroutput gebruikt wordt als bewijsmateriaal dan kan dit een inbreuk betekenen op de privacy van hen, die in het bestand zijn opgenomen. In zo'n geval zou de rechter kunnen besluiten het computerbewijs niet te gebruiken.

Uit de hiervoor gegeven opsomming blijkt, dat computerbewijs gelijkgesteld mag worden met ofwel een geschrift, of met een deskundigenrapport. Volgens de doctrine (dat wil zeggen de rechtsleer) is het deskundigenrapport geen bewijsmiddel, maar een advies aan de rechter. Deze laatste is vrij om aan het rapport rechtswaarde toe te kennen.
De vraag die nu nog rest is of computerbewijs onder "geschriften" valt te classificeren. De wettelijke definitie van een geschrift, zoals die ligt vastgelegd in artikel 1904 en verder van het Burgerlijk Wetboek, luidt: "Iedere drager van verstaanbare leestekens, die een gedachteninhoud vertolkt, waarbij het materiaal waarop niet relevant is". Uitgaande van deze definitie is een lijst met gegevens wel in wettelijke zin een geschrift, een ponskaart of magneetschijf daarentegen niet.

Dit bleek uit een geding voor de strafkamer van het Gerechtshof te Amsterdam, op 18 februari 1972. Een citaat uit het verslag toont dit aan: "Het hof acht met name telkens niet bewezen dat de ponskaart was een geschrift, waaruit enig recht, enige verbintenis of enige bevrijdenis van schuld kon ontstaan (...) derhalve is een ponskaart geen geschrift in de zin van artikel 225 van het Wetboek van Strafrecht".
Of computergegevens al dan niet gelijkgesteld mogen worden met een geschrift is niet zo belangrijk. Volgens de criteria van de Hoge Raad is computerbewijs geen akte, en het heeft daardoor een vrije bewijskracht, met andere woorden, de rechter zelf mag bepalen welke zwaarte hij aan computerbewijs toekent.

Laten we het Engelse geval eens overzetten naar de Nederlandse situatie. Iemand haalt bij zijn bank een bedrag van 10.000 gulden, in coupures van 100 gulden. Zijn bank heeft van De Nederlandsche Bank een lijst gekregen met alle serienummers. Bij de persoon wordt ingebroken, waarbij het bedrag van 10.000 gulden wordt ontvreemd. Vervolgens wordt in het bezit van de verdachte een aantal bankbiljetten aangetroffen, waarvan de serienummers op de lijst voorkomen.
Tijdens de rechtszaak is dus als bewijs een computerprint voorhanden, met daarop alle serienummers van de ontvreemde bankbiljetten.
De rechter kan nu een onderzoek gelasten naar de juiste werking van het gebruikte computersysteem. De lijst met gegevens bevat leesbare tekst (serienummers), die niet geïnterpreteerd hoeft te worden door een deskundige.
Afhankelijk van de uitslag van het onderzoek, het deskundigenrapport, kan de rechter bepalen of de computerlijst wettig bewijsmiddel is, of niet.
Laten we aannemen, dat het computersysteem feilloos functioneert. In dat geval zal de rechter besluiten, de lijst als wettig bewijs te accepteren. Het gevolg hiervan is, dat de verdachte wordt veroordeeld. (Eventueel tegenbewijs of een sluitend alibi van de verdachte zijn in dit voorbeeld buiten beschouwing gelaten, het gaat ons in dit geval louter om de geldigheid van computerbewijs.)

Andere landen

Het is wellicht interessant, de situatie te bekijken in de ons omringende landen. Bij navraag bleek, dat een situatie zoals hiervoor geschetst, niet te achterhalen was in de juridische historie van Frankrijk, België en Duitsland. Dit houdt in, dat er dus geen specifieke voorbeelden te geven zijn over de geldigheid van deze vorm van computerbewijs.
Frankrijk heeft zijn "Code Civil", het Burgerlijk Wetboek, waarin staat, dat in theorie ieder aangehaald bewijs op schrift gesteld dient te zijn. In het Franse Handelsrecht staat onder meer, dat een boekhouding moet zijn bijgehouden op gewaarmerkt papier, met andere woorden, dat het ook hier moet gaan om een geschrift. Nergens in de wetteksten wordt gesproken van computeroutput, doodeenvoudig omdat die nog niet bestond ten tijde van het ontstaan van de wetten. De Franse wetten dateren voor het grootste gedeelte nog uit de Napoleontische tijd. Hoewel computeroutput nergens wordt genoemd in de wet, worden computerprintings de facto wel als bewijs aanvaard. Eventueel kan een rechter eisen, dat de lijst wordt gepresenteerd, te zamen met een grondige analyse van de verhouding tussen invoer en uitvoer.

Op die manier voorkomt men, dat een lijst, die volgens het GIGO-principe is gefabriceerd, wordt aanvaard als wettig bewijs. Naast de samenhang van in- en uitvoer, zal ook de betrouwbaarheid van het computersysteem vastgesteld moeten worden.

Het Belgische recht neigt zeer sterk naar het Franse, dus mogen we verwachten, dat ook bij onze zuiderburen computeroutput als wettig bewijs kan dienen. De Belgische wet accepteert bijvoorbeeld een boekhouding, die met behulp van een computer is samengesteld. Bij deze acceptatie is echter wel een eis aanwezig: van alle gevoerde transacties dient een officieel journaal te worden bijgehouden. Dit journaal dient handgeschreven te zijn, op genummerde en gewaarmerkte bladen. Het journaal mag echter worden samengesteld uit "verscheidene bronnen, ongeacht hun aard, mits betrouwbaar".
Hieronder vallen dus ook computerlijsten.

In Duitsland gelden iets andere voorwaarden, hier wordt computeroutput niet altijd zonder meer als bewijsmiddel aanvaard. Dit houdt in, dat alleen op grond van een computerlijst geen veroordeling plaats kan vinden. In ons voorbeeld (de dief, die aan de hand van een lijst met serienummers wordt gearresteerd) zou de Duitse rechtspraak een nadere controle eisen van het tot stand komen van genoemde lijst. In dat geval wordt de verantwoordelijke beambte (in het voorbeeld de directeur van de bank) gedagvaard. Zijn getuigenis, samen met de lijst met serienummers vormt dan het bewijs.
Er is in het Duitse recht wel een mogelijkheid, om de computerlijst zonder meer als bewijs te accepteren, doch dit komt alleen voor bij civielrechtelijke procedures. Een diefstal is namelijk een strafrechtelijke zaak.
In Duitsland geldt bij een civielrechtelijke procedure, dat ieder bewijs dat een partij naar voren brengt en dat niet door de tegenpartij wordt aangevochten, geldig is. Om een zeer extreem voorbeeld te noemen: als de ene partij verklaart dat gras een rode kleur heeft en de tegenpartij bestrijdt dit niet, dan is gras voor wat de rechtbank betreft inderdaad rood.

Resumerend kunnen we dus zeggen, dat in Nederland en de ons omringende landen computerlijsten zeer vaak als wettig bewijsmiddel kunnen gelden. Behalve voor lijsten geldt dit in de meeste gevallen ook voor andere vormen van computeroutput, zoals ponskaarten, ponsbanden, magneetschijven en magneetbanden.

Over op IBM-4300? Uit: Ditem (Pakhoed)

De aankondiging van de 4300-serie van IBM, heeft bij vele gebruikers van kleine en middelgrote systemen ruime aandacht getrokken.
Het verkoopsucces van de aangekondigde 4331 en 4341 is zoals bekend zeer groot, waarvoor meerdere redenen zijn aan te wijzen.
Wanneer wij afzien van meer modieuze argumenten, zoals "nieuwe technologie" zijn voor dit artikel twee hoofdargumenten relevant:

a. zeer gunstige prijs/prestatieverhouding;
b. simpelheid van het systeem.

Het eerste argument heeft aantrekkingskracht voor die gebruikers die aan de topcapaciteit van hun (kleine) computersysteem zitten en waar het management zorgelijk de uitbreidingsbudgetten bekijkt.
Simpelheid van het systeem, vooral bij 4331 is een argument dat zeer relevant is voor kleinere gebruikers, zoals van 370/115 en /125 systemen, van System/3 en /34 en natuurlijk ook voor de groep die voor het eerst een computer in huis haalt. Simpelheid betekent tenslotte dat men zijn bestaande computerstaf niet behoeft uit te breiden en voor de "low-budget" nieuwe gebruikers, dat men zijn personeelskosten laag kan houden.
Laten wij enkele opmerkingen maken over onderdelen van de 4300.

Hardware
Naast de 64K chips, geïntegreerde controller en andere zijn de vaste schijven (3310 en 3370) het opvallendst. Fixed Block Architecture maakt snellere toegang mogelijk, maar is inefficiënter in ruimtebenutting. Door de vaste schijven is men praktisch gedwongen zijn systeembeveiliging opnieuw te overdenken, wat vooral bij bestaande rekencentra problemen kan geven.

Systeemgeneratie
Deze wordt gedaan met "System Installation Productivity Options". Dit zijn standaardpakketten van systeemsoftware-modules, globaal vooraf gegenereerde operating systemen. Aanbevelenswaardig is personeel ervaring te laten opdoen met de SIPO's alvorens men de machine in huis heeft. Installatie is eenvoudig, de nieuwelingen doen er echter 4 à 5 maal zo lang over. Zoals reeds uit de naam blijkt, zijn SIPO's gestandaardiseerd. Is de SIPO voor de gebruiker te gering in omvang, dan moet hij zelf systeemcomponenten inbrengen ("tuning"). De installatietijd stijgt dan tot het veelvoudige, zeker in het begin. Systeem-tuning moet zorgvuldig gebeuren, moet goed worden voorbereid en vergt systeemkennis. Men moet zich verder realiseren dat elke SIPO-versie die IBM levert, een aparte tuning vergt en dat men moet hopen, dat de nieuwe SIPO geen invloed heeft op de bestaande tuning-parameters.

Monitorsysteem
Nieuwe software geeft in het begin relatief veel fouten. Heeft men een standaardmonitorsysteem (IBM verkoopt graag CICS), dan kan men op het ogenblik verwachten dat er meer storingen optreden dan op de 370-serie.
Analyse van storingen vergt systeemkennis. Dump-lezen is niet voor elke programmeur een genoegen; en voor de telefonische stand-by verwacht IBM een adequate gesprekspartner.

Applicatiesoftware
Conversie van DOS/VS-programma's (ook TOTAL) naar DOS/VSE is niet noodzakelijk als men de beschikking heeft over oude (3340) schijven. Problematischer wordt het echter, wanneer slechts de FBA-schijven ter beschikking staan. De gebruiker is gedwongen de oude schijven te emuleren op de nieuwe, of zijn applicaties te herschrijven op VSAM-basis (TOTAL support VSAM). Vooronderstelling is dat men VSAM vooraf bestudeert, waarvoor een redelijke systeemkennis aanwezig moet zijn. Dat de conversieslag groter is bij een gebruiker die van een System/3 of System/34 overgaat spreekt vanzelf.

Wil een gebruiker overgaan op een 4331 dan zal hij zich moeten realiseren, dat er enerzijds zeker in het begin aanloopmoeilijkheden zijn door onkunde ten aanzien van het systeem en anderzijds er tenminste een deskundige aanwezig moet zijn op het gebied van de systeemsoftware. Het parallel draaien van het te vervangen systeem en de 4331 voor een zekere tijd lijkt ons aan te bevelen, terwijl voor de nieuwe gebruiker helaas moet worden geconstateerd dat een deskundige op het gebied van systeemsoftware voor een klein budget niet te vinden is.

System/34-TOTAL

TOTAL Data Base Management System is nu ook beschikbaar voor IBM S/34 gebruikers.

Cullinane overbrugt stap van DL/1 naar IDMS data base

Cullinane ziet haar klantenkring voor het data base management systeem IDMS voortdurend groter worden. Veelal gaat dit ten koste van het IBM-alternatief IMS of DL/1 en vandaar dat het ook niet onlogisch is, dat Cullinane met een soort brugsysteem tussen haar produkt en dat van IBM is gekomen, waaraan de naam Escape is gegeven. Hoewel de eerste releases hiervan pas in het najaar op de markt zullen komen zijn er toch al enige bijzonderheden van het pakket bekendgemaakt. Met Escape richt Cullinane zich op twee groepen data base gebruikers, namelijk die welke reeds IDMS in combinatie met IBM-"hardware" toepassen maar die daarnaast ook onder DL/1 draaiende programmatuur willen gaan toepassen en die, welke alleen beschikken over DL/1 of IMS data base en naar IDMS willen converteren. Met behulp van Escape worden de Call's in DL/1-toepassingsprogramma's omgebouwd naar IDMS, waarbij de gebruiker dan uiteraard wel de equivalenten in de diverse "control blocks" moet hebben gedefinieerd. Omgekeerd kunnen ook IDMS-toepassingsprogramma's met behulp van Escape gebruik maken van een data base volgens de DL/1-structuur. Op deze manier is het natuurlijk ook mogelijk om zowel DL/1- als IDMS-applicatieprogramma's van dezelfde data base gebruik te laten maken.

Computable, 23 mei 1980

Beveiliging

Het volgende is overgenomen uit het tijdschrift Computer-markt van maart 1980. Aan de voor zich sprekende tekst is weinig toe te voegen.

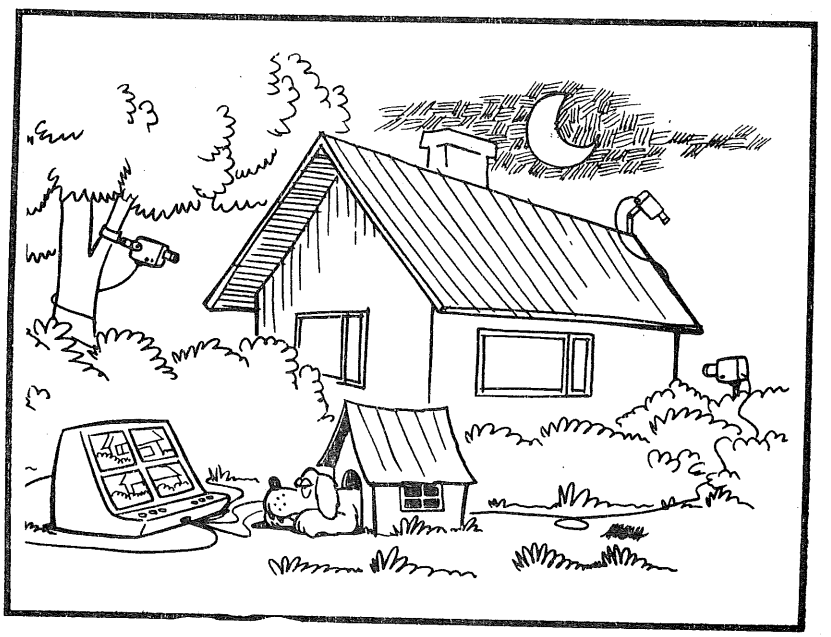
Ten geleide

Computerbeveiliging is in. Diverse seminars, bijeenkomsten, artikelen, enz. worden thans aan dit onderwerp gewijd. In veel gevallen behartigt het hoofd van het rekencentrum deze kwestie zelf, maar in toenemende mate zien we gespecialiseerde functionarissen en zelfs afdelingen ontstaan. Sophisticated benaderingen onder de vlag van Data Risk Management Methoden maken thans een noodzakelijk onderdeel uit van het complete dienstenpakket van automatiseringsadviesbureaus.

In de publiciteit rondom dit onderwerp staan gevallen van fraude, brand, sabotage, aftappen van datatransmissielijnen, enz. meestal centraal. Dat is jammer omdat daardoor de aandacht wordt afgeleid van de meer alledaagse risico's die praktisch iedere organisatie loopt.

Automatisering brengt een aantal nevenverschijnselen met zich mee waar meestal weinig aandacht aan wordt besteed. Ook al kent men de risico's wel degelijk, dan ziet men in de praktijk toch dat er onvoldoende maatregelen worden getroffen om bepaalde calamiteiten het hoofd te bieden. Een sprekend voorbeeld is de verwaarlozing van documentatie. Hoe vaak komt het niet voor dat enkele sleutelmedewerkers of soms alle medewerkers van een automatiseringsafdeling vertrekken en het systeem onvoldoende gedocumenteerd is?

Sommige deskundigen betreuren het dat er zo weinig bekend is over gevallen van fraude. Maar zou het niet veel nuttiger zijn als er meer gegevens bekend zijn over de kosten van vertrek van computerpersoneel? Moet men zich daar ook niet tegen beveiligen?



Weergave in een aantal punten welke security-problemen kunnen ontstaan als bepaalde beveiligingsmaatregelen niet zijn genomen.

Security problems for computer centers

1. *No access protection*
   There is no enforced access control; employees other than operating personnel may wander through the computer room.

2. *The glass palace*
   The data centre is in effect a fish-bowl for everyone to see.

3. *No back-up*
   Duplicates of data files, programmes, documentation, etc. are not maintained on a current basis at a location far enough away to be out of the disaster area.

4. *Centralised processing*
   Data processing is consolidated into one large computer centre.

5. *No outside audit*
   There is no independent evaluation group to test the security procedures and to monitor the security programme.

6. *No personnel security programme*
   There is little background check of new personnel, computer security is not conducted.

7. *No protection system*
   The computer center is not equipped with a basic protection system for fire, smoke detection, and fire-fighting.

Accountancy, May 1980

In Edpacs van februari 1980 is onder de titel Computer Access Control Software een artikel verschenen waarin L.L. Vetter de mogelijkheden en beperkingen beschrijft van de standaardpakketten voor toegangsbeveiliging RACF (Resource Access Control Facility), ACF2 (Access Control Facility) en SECURE. Deze mogelijkheden en beperkingen zijn aan het slot van het artikel samengevat in een overzicht dat hierna wordt weergegeven.

OVERVIEW OF THREE ACCESS CONTROL SOFTWARE PACKAGES

	ACF2
TYPE OF PROTECTION	Protection by default
GENERAL	
Nature of package	Privileged program, data base (extension of MVS)
Operating system needed	MVS (only)
PROTECTED RESOURCES	
Control method	User's identity
Basic type of control	Access to computer system and resources
Resources protected	Data sets (DASD and/or tape), volumes (DASD and/or tape), TSO commands, selected programs by name, terminals and RJE's, IMS transactions, others, as locally defined
Where does control occur?	Operating system
When does control occur?	OPEN, END OF VOLUME, ALLOCATE, SCRATCH, CATALOG, RENAME
Types of access differentiated	READ WRITE (update only) EXECUTE ONLY ALLOCATE (CREATE, DELETE, etc.)

RACF	SECURE
Protected if specified	Protected if password protection bit set
Privileged program, data base (extension of MVS)	Program - a replacement for the IBM open-security routines and password maintenance SVC
MVS (only)	Any IBM operating system
User's identity	Knowledge (JCL format)
Access to computer system and resources	Access to data sets
Data sets (DASD), volumes (DASD and/or tape), terminals, IMS transactions, others, as locally defined	Data sets, VTOC's
Operating system	Operating system
OPEN, END OF VOLUME, ALLOCATE, SCRATCH	OPEN, END OF VOLUME, SCRATCH, RENAME
READ UPDATE ALTER (CREATE, DELETE, etc.)	READ READ/WRITE SCRATCH EXECUTE ONLY

Controle

Ongetwijfeld kan gesteld worden dat de minicomputer nog volledig in de belangstelling staat. In een aantal publikaties is getracht aan te geven welke invloed de komst van de minicomputer heeft en nog zal hebben op de accountantscontrole. Gesuggereerd is reeds in de literatuur dat het tijdperk van controle around de computer is teruggekeerd waarbij de vraag kan worden gesteld of dat tijdperk ooit is afgesloten.
Het volgende artikel Auditing "Micro" Systems van Robert D. Hodge, dat is overgenomen uit Edpacs van maart 1980, signaleert eerst de problemen voor de accountant bij microsystemen. Vervolgens worden een aantal through-the-computer benaderingen genoemd die volgens Hodge in een "micro"-omgeving niet bruikbaar zijn, waarna die paragraaf wordt besloten met de uitspraak: "Micro systems, because of their limited capacity, are often impractical to use for through-the-computer auditing".
Er zal dus naar andere wegen moeten worden gezocht. Hodge ziet als één van de mogelijkheden "The audit minicomputer". Voor hetgeen hij hieronder verstaat en waarom hij dat als mogelijkheid ziet wordt U naar het hieronder volgende artikel verwezen. Of de visie van Hodge werkelijkheid zal worden zal de toekomst leren.

Auditing "Micro" Systems

by Robert D. Hodge

Many devices used by businesses are being given "intelligence" by means of microcomputers and associated software. Some very small microcomputer-based systems are quite advanced and have extensive capabilities. Coping with these developments requires a more dynamic, computer-oriented audit. This article covers some of the technical aspects of micros and describes the use of an audit minicomputer.

THE NEW COMPUTER ENVIRONMENT

A review of data processing literature shows that advanced systems often utilize smaller, not larger, computers. Applications that have always been done manually are now being computerized. Hardwired and mechanical business machines are being replaced by small computers which can emulate many different devices. There are numerous examples of these changes:

1. Physical security based on locks and keys is being replaced by magnetic badge readers connected to intelligent door controllers and recording devices.
2. Personal identification based on signature comparison is giving way to personal identification codes that serve as input to algorithms in desk top microcomputers.
3. Data entry based on hardcopy forms processed at a central site is being replaced by interactive input entered directly into portable microcomputers which contain the related data base, application software, and printing capability.

The range is enormous. In many banks, mechanical posting machines are being supplanted by teller machines which support four CRT's and keyboards, two printers, two floppy disk drives, two magnetic card readers and personal identification devices, and are online to a central computer.
The entire terminal is controlled by one microcomputer, and each device relies on its own microcomputer to make it function.

AUDIT RAMIFICATIONS OF SMALL INTELLIGENT DEVICES

The use of microcomputers as a basic component of a wide range of commercial devices will require a change in audit responsibility at all levels from the general staff auditor to the EDP auditor. For example, an EDP auditor was once able to perform an audit without leaving the building containing the mainframe, but now he must go the user site(s).

An EDP audit of small systems must overcome some new obstacles:

1. The programs are often stored in read only memory (ROM), so they are inaccessible for audit or user review.
2. The programs supplied with the device are usually proprietary products of the vendor. As a result, the source code is seldom made available.
3. A direct interface between the small system and a larger mainframe is usually not feasible because it would be an inefficient use of the mainframe's resources.
4. Most generalized audit software will run only on mainframe computers.
5. Although they are really general-purpose computers, most micros are implemented in systems, that treat them as "black boxes". This results in little, if any, design effort being devoted to using the microcomputer's power to implement error control or security protection.
6. An audit trail of system activity is usually not available.

MICROSYSTEM AUDIT METHODS

While small computer systems have created barriers to EDP auditing, they do not necessarily require new audit methods. The initial problem appears to be developing ways to apply existing EDP audit methods to new areas of technology.

What methods can be employed? Around-the-computer audit approaches should not be influenced by the physical or logical size of the computer, although the lack of audit trails makes such approaches difficult to apply.
Some of the through-the-computer approaches which can be applied include:

- Simulation/modeling
- Test data
- Parallel operations
- Parallel simulation
- Generalized audit software
- Terminal audit software
- Special purpose audit programs (See "Use of Computer Audit Practices", Edpacs, November 1978).

These through-the-computer approaches are usually implemented on the computer that is used to process the applications being tested.
Micro systems, because of their limited capacity, are often impractical to use for through-the-computer auditing. Other means of getting into the system must be employed.

THE AUDIT MINICOMPUTER

One approach involves the use of the audit computer: a general-purpose hardware system capable of interfacing with both large and small computers. An audit computer offers several general advantages:

1. Increased auditor control over EDP audit programs and program development creates greater auditor independence.
2. Small computers are often more easily interfaced to micro systems because of the similarities in peripherals and interface methods.
3. The risk of audit processing affecting other users of a large computer is eliminated. This is especially important if some of the proposed audit steps are implemented.
4. There is no competition with other users for the use of scarce mainframe computer resources.

To summarize, a small audit computer can be used to apply existing through-the-computer audit practices to micro systems.

SYSTEMS INTERFACE

Several methods can be used to interface an audit computer to a small system:

1. Transferring floppy disks (diskettes) or tape cassettes between computers provides access to the micro system data base without requiring a rewriting of the audit software.
2. Direct connection to the circuits of the microcomputer allows direct monitoring of or interaction with the system.
3. Peripheral devices or the micro system itself can be emulated to test the other components of the system.

These interface alternatives are explored below.

FLOPPY DISKS AND CASSETTES

Many small systems use floppy disks or tape cassettes for data and program storage. Audit reviews and tests of data can often be accomplished without a physical connection between the device to be tested and the audit computer. Data can simply be transferred to the audit computer. Audit software can be written solely for the audit computer instead of for each device to be tested.

A major obstacle to overcome is the different disk recording formats used by the various micro- and minicomputer manufacturers. Disks may be physically, but not logically, compatible. This obstacle is usually eliminated

if the computers are from the same vendor. In addition, many vendors use the IBM format as a standard. Compatibility between systems is probable, but the situation will become more complex as new drives, recording formats and recording densities are introduced. If the formats are different, a conversion effort will be necessary. Direct conversion often requires the writing of special software.

Some systems can use their own disk format or the IBM format, depending on the option selected at "write" time. In such cases, the IBM format can be used by both systems, or may be used as an intermediary between the systems. This would allow the audit software on the audit computer to be used in its native format. At least three major manufacturers supply utilities which can convert their disk format to the IBM format and back again.

DIRECT CONNECTION TO A COMPUTER BUS

A "bus" is a conductor or group of conductors serving as a common connection for three or more circuits. In the power panel in your home, for example, all the neutral circuit wires are connected together by a bus bar.

A computer may have many busses. The power bus distributes voltage to the various circuit boards. The address bus allows the processor to communicate with the other circuit boards. The data bus is used to transfer data between the processor and the different circuit boards, such as for memory or video display. Finally, the control bus allows the processor to "tell" the other circuit boards what it is doing; e.g., writing to memory or waiting for input. Relatively widely used small system busses include the Intel Multibus, DEC LSI-11 bus, and the Altair S100 bus. The S100 has become an unofficial industry standard.

Highly technical questions can be answered by inserting probes or a "monitor" circuit board into a bus while operating the device under test conditions. For instance, what would a reduction from 120 to 93 volts do to a point-of-sale (POS) terminal? Would the machine simply begin to produce errors? Would it stop because it lost its program in memory? Etc. Monitoring the control bus or data bus could provide exact answers to these questions.

EMULATION OF COMPONENTS

When a peripheral device is to be tested, it may be linked to the audit computer bus via a local peripheral communcations board (port) or a remote communications modem board. The audit computer can then emulate the computer to which the peripheral device is attached.

Where the microcomputer itself is to be tested, the audit computer could be linked to a micro bus via the micro's peripheral device communications board. The audit computer could then be used to emulate a variety of input or output devices.

Component emulation might be applied to a POS network that utilizes programmable POS devices, customer identification devices, store controllers,

regional controllers, and a switching computer accessing various hosts. By the use of emulation, it is possible to test the controls throughout the network. The audit computer might, for example, emulate portions of the POS devices to test customer identification, code encryption, and key management processing. Such tests could be used to determine if the specifications have been followed for each programmable device to provide for the proper protection of the encryption key.

The RS-232 interface gives the auditor the easiest way to access a small intelligent device. RS-232 is a standard communications bus that can be used to interconnect terminal equipment and communications equipment that employ a serial data interchange. The data communications equipment is not concerned about character length, bit codes, bit sequences, or restrictions on message formats. Since all RS-232 communications are treated as unstructured strings or streams of bits, none of these factors need be considered. This interface is extensively used to connect computers to peripheral devices.

Direct connection to a computer bus (as previously described) does not utilize an RS-232 interface. RS-232 is similar to the direct bus connection, but it is more flexible and requires less technical knowledge of the device to be tested.

The RS-232 interface was primarily designed to make peripherals plug-compatible with their controlling computers. As such, use of the interface can make connection to an audit computer much simpler. The auditor has to write code to either drive or emulate the peripheral, depending upon the device to be tested. In either case, the audit computer must be able to check for even, odd, or no parity; differing numbers of bits per character; different bit codes; and varying message formats. Specifications for these ables can be found in the technical manuals for the component to be tested or emulated.

STANDARDS ARE NOT STANDARD

As with most "standards", in the real world there are variations in some of the areas described or discussed in this article. In most cases, these are recognizable and can be avoided, or at least allowed for, in the audit. Discovery of these variations should be viewed as part of the audit to be performed. For example:

1. Experience has shown that data recorded on floppy disks will conform to the standard under which it was recorded. Tape cassettes recorded on commercial systems under the same standard are readily transferable, but are not as reliable as disks. Some systems use less expensive, lower quality cassette drives which are meant for use in the hobbiest market.

2. Experience with the audit utilization of computer busses has shown that variations from the S100 standard are common between circuit boards. A given board may work by itself, but it may fail when used in combination with other boards. These variations can usually be traced to timing requirements.

3. RS-232 variations are frequent, but not usually fatal. RS-232-B uses logic levels of ± 25 volts while RS-232-C uses levels of ± 15 volts. An overload potential exists if systems are mismatched, but no real problems have been encountered to date.
4. Cable connector assignments and types of physical connectors required vary on RS-232 boards. Simple mechanical changes can solve these problems.
5. RS-232 is designed to allow one device to control another. Two "masters" trying to communicate, where a master/slave relationship should exist, may require some juggling.

WHO CAN/SHOULD AUDIT MICROS?

Initial audits of microprocessor-based peripherals and computers have been intentionally informal and low budget. Expert technical information and advice, as well as required small parts, have been readily available at personal computer stores.

At the Ninth Conference on Computer Audit, Control and Security, some participants questioned the responsibility or need for the EDP auditor to get involved in the "guts" of a microcomputer. As a rule of thumb, if there was a need to audit a function performed on a mainframe, then it is necessary to audit in on a microcomputer. As one consideration, there are the extra exposures present when the function is distributed to many computers in different physical environments.
The need to audit program controls and logic does not decrease with the size of a computer. Clearly, the auditor can and should be involved in the audit of microcomputer-based systems.

CONCLUSION

Micro systems are tremendous innovations. They are being applied in imaginative ways to many new applications. By present auditing conventions, the responsibility for the audit of these new applications is moving from the general staff auditor to the EDP auditor. The EDP auditor must be imaginative in using existing audit practices to overcome some of the challenges created by microcomputers.

The audit computer provides one way to cope with these challenges. It is a practical way of applying effective through-the-computer audit practices to small systems.

LITERATUUROVERZICHT

door H.J.M. van der Wielen

Bespreking van enkele boeken en artikelen uit tijdschriften die in de A.C.-bibliotheek zijn opgenomen

1. IMS-Guide

AC 167 In deze bundel zijn de rapporten van IMS-Guide opgenomen

AC 167.1 Rapport Werkgroep Data Security, 1977
AC 167.2 Rapport Werkgroep Inquiry Pakketten, 1980.

In het recente rapport worden de resultaten van een enquête onder de leden/gebruikers over de ter beschikking staande pakketten weergegeven.
De volgende pakketten passeren de revue:

gebruiker	pakketten
AKZO	GIS, EASYTRIEVE
AMRO-bank	Culprit, Lexicon
IBM	GIS
ICI	ASI/Inquiry
KKC	CA-EARL
Philips	IMS-inquiry.

2. Technical reports for management and DP professionals for 1980
James Martin / Savant Institute 1980

Gaarne willen wij U van deze serie van negen boeken, die is opgenomen in de OG-bibliotheek, deel V onder de aandacht brengen:

"Distributed processing - network mechanisms, standards and recovery".

Vooral het gedeelte dat de recovery behandelt kan van belang zijn voor automatisering en controle.

3. AC 293 Auditing computer-based systems (1979)
Additional GAO audit standards
Door het U.S. National Bureau of Standards en U.S. General Accounting Office zijn aanvullende standaarden gepubliceerd. Deze standaarden sluiten aan op de zienswijze zoals deze in het hierna genoemde rapport tot uitdrukking is gebracht.

"1978 Report, Conclusions, and Recommendations of the AICPA's Commission on Auditors Responsibilities."

De standaarden zijn ingedeeld in drie groepen:

1. Participatie bij ontwikkeling
2. Toetsen algemene controlemaatregelen
3. Toetsen controlemaatregelen in geautomatiseerde toepassingen.

Het boekje van bescheiden omvang (15 pagina's) vormt een goed toetsingsmiddel voor de inhoud van vragenlijsten die bij de beoordeling van automatisering en controle worden gebruikt. Niet gericht op details, maar op de hoofdlijnen. Verder komt onder meer tot uitdrukking dat de Amerikaanse overheid de taak van de internal auditor niet bepaald beperkt ziet.

Objective 1 uit groep 1 wordt als volgt omschreven:

"To assure that systems/applications faithfully carry out the policies management has prescribed for the system".

4. AC 301 Report of the Special Advisory Committee on Internal Accounting Control
American Institute of Certified Public Accountants

Inleiding

De betekenis van dit rapport is groot. Het doel is om de leiding van bedrijven een handreiking te doen hoe een adequaat stelsel van interne controlemaatregelen opgezet kan worden. Hiermede wordt voldaan aan de voorwaarden die de Amerikaanse wet stelt. Tevens zijn deze regels in overeenstemming met de codificatie van de beroepsregels van het Amerikaanse accountantsberoep. Door dit rapport - ook voor Europese verhoudingen - te beschouwen in het licht van automatisering en controle is een omgeving geschapen, waarin een duidelijk gestructureerd en eventueel versterkt stelsel van interne controlemaatregelen bereikt kan worden. De lessen van Equity Funding zijn dan niet voor niets betaald.

Table of Contents

Table of Contents (vervolg)

Foreword

The AICPA Special Advisory Committee on Internal Accounting Control was formed in August 1977. The AICPA recognized that the broad guidance in professional auditing literature had been developed for a limited purpose and that there was a need to provide guidance that would be helpful to management. Accordingly, the Institute appointed an advisory group consisting of financial executives, internal auditors, CPA's engaged in management advisory services and one CPA engaged in the practice of auditing to develop the desired guidance. The committee issued a tentative report for public comment in September 1978.

The Foreign Corrupt Practices Act of 1977 (AC 300) became law after the committee had begun its work. The act imposes, among other things, internal accounting control requirements on certain issuers of securities (public companies). Although the committee was not formed because of the act, this report should be useful to management and boards of directors in considering whether their companies comply with the internal accounting control provisions of the act. (Tot zover citaat uit het voorwoord.)

Toelichting

In de Verenigde Staten van Amerika wordt onderscheid gemaakt tussen administrative control (beheersingsregels van de leiding om een organisatie te leiden naar het gestelde doel - denk aan "minister" -) en accounting control (dit ruime begrip omvat het geheel van maatregelen dienend tot: a. interne controle op de behaalde resultaten [budgetcontrole] en de betrouwbaarheid van de verslaggeving daarover; b. interne controle op en beveiliging van de activa en de betrouwbaarheid van de vastlegging daarvan).
Over deze accounting controls handelt bovengenoemd rapport. Automatisering voegt geen nieuwe aspecten toe, maar geeft het geheel van maatregelen wel een extra dimensie.

In de Codification of Auditing Standards and Procedures SAS1 (AC 63) wordt accounting control als volgt gedefinieerd (zie 320.28):

"Accounting control comprises the plan of organization and the procedures and records that are concerned with the safeguarding of assets and the reliability of financial records and consequently are designed to provide reasonable assurance that

a. Transactions are executed in accordance with management's general or specific authorization.

b. Transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with general accepted accounting principles or any other criteria applicable to such statements and (2) to maintain accountability for assets.

c. Access to assets is permitted only in accordance with management's authorization.

d. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriated action is taken with respect to any differences."

Wanneer deze hoofdregels worden vergeleken met het eisenpakket - onderdeel interne controle - van een willekeurig informatiesysteem dan lijkt dit niets nieuws te bevatten. Echter:

a. De beoordeling van de betrouwbaarheid van de opzet en werking van de automatiseringsorganisatie en van de automatiseringssystemen leert dat de betrouwbaarheid van de informatiesystemen niet voldoende komt vast te staan als niet ook de informatieverwerkende afdeling in het onderzoek betrokken wordt.

b. Het is vereist dat een evenwichtige mix gevonden wordt tussen de algemeen geldende maatregelen van interne controle en de specifieke maatregelen in de informatiesystemen.

c. Het bijzondere van het Report wordt gevormd door de diepgang ofwel ruime strekking die aan "accounting control" kan worden gegeven.

Voor de verdere algemene overwegingen verwijzen we gaarne naar de tekst van het Report (23 pagina's).

In het hoofdstuk "EDP Considerations" (pag. 17) komt meer het terrein van Automatisering en Controle naar voren en wordt verwezen naar andere geschriften, zoals SAS3 - The Effects of EDP on the Auditor's Study and Evaluation of Internal Control en enige andere AICPA guides and guidelines.

Aan het Report is een appendix toegevoegd onder het opschrift: "An Illustration of Specific Objectives and Examples of Selected Control Procedures and Techniques by Cycle" (24 pagina's).
Deze appendix is eveneens niet speciaal gericht op automatisering en controle. Het is echter nuttig het onderdeel "Evaluation Internal Accounting Control" in samenhang met de appendix vanuit het gezichtspunt van automatisering en controle te bezien.

Onderscheiden worden vijf functies (cycles):

1.	Opbrengsten	:	verkopen en daarmede verband houdende zaken.
2.	Uitgaven	:	inkopen, kosten, enz..
3.	Produktie of conversie	:	produktie en kostprijsproduktie.
4.	Financiering	:	financieringsbronnen ter verkrijging van werkkapitaal en hun kosten en opbrengsten.
5.	Externe financiële rapportering	:	vervaardigen en de daarbij in aanmerking te nemen standaarden en regels.

In de appendix worden per functie (of regel) criteria en voorbeelden van gekozen interne controlemaatregelen en -technieken naar voren gebracht. Hierbij moet worden bedacht dat deze maatregelen geschreven zijn voor de Amerikaanse omstandigheden.

Bij iedere functie wordt een vaste indeling aangehouden en wel de doelstellingen/criteria met betrekking tot:

- autorisatie,
- accounting,
- bewaking activa.

In de vijf functies worden in totaal 47 doelstellingen genoemd met achter ieder van hen één of meer voorbeelden van gekozen procedures of technieken van accounting control. Bij het ontwikkelen van automatiseringstoepassingen zou het wenselijk/noodzakelijk zijn deze doelstellingen of mogelijk criteria zeer specifiek in aanmerking te nemen. Zodoende kan een duidelijk gestructureerd en eventueel versterkt stelsel van interne controlemaatregelen bereikt worden.
In een volgende bespreking willen we nader ingaan op de voorstellen die de Securities and Exchange Commission gedaan heeft met betrekking tot deze accounting controls en de voorstellen met betrekking tot de openbaarmaking ervan bij geconstateerde leemten. De volledige tekst van de voorstellen van de SEC is opgenomen in "Uit het buitenland", 30e jaargang no. 17, december 1979.

5. Verslag van de NOVI-conferentie "Decentralisatie in de praktijk" op 27 februari 1980, RAI Amsterdam
door H. Roos

Het doel van een dergelijke praktijkgerichte conferentie is uiteraard de deelnemers een beeld te geven van de huidige situatie.
Deelnemers die hier het eureka hadden verwacht zullen teleurgesteld huiswaarts zijn gekeerd. Zij die oog hadden voor het detail zullen een indruk hebben overgehouden van sterke nuanceverschillen.
De algemene conclusie moet zijn dat toepassingen van gedecentraliseerde informatieverwerking sterk gebonden zijn aan concrete organisatievormen. Zowel de technische, de economische als de menselijke mogelijkheden liggen in elke organisatie weer anders.
Juist vanwege die in de praktijk bestaande variaties was het een goede gedachte een vijftal inleiders te laten vertellen over hun praktijkervaringen op dit gebied.

De algemene inleiding werd verzorgd door Dr. Scheepmaker (Waarom is decentralisatie zo moeilijk?); de bankwereld werd vertegenwoordigd door de heer Geerdink (NMB) "Beleidsfilosofie ten aanzien van decentralisatie"; "Automatisering en geografische spreiding van bedrijfsactiviteiten" (van een produktie- en handelsonderneming) werden belicht door de heer Hermeler van Douwe Egberts; de heer Nuissl van Delta-Lloyd beschouwde "Mini's - Manco's - Macht" vanuit de verzekeringsbedrijfoptiek; Dr. Sonnemans schetste een beeld van "Centrale ontwikkeling van decentrale bedrijfsprocessen" bij het Gemeenschappelijk Administratie Kantoor en tot slot gaf de heer Roos van het Rijks Computercentrum zijn visie op een "Methode voor projectbesturing als beheersinstrument bij decentralisatie".
De dag werd besloten met een zeer geanimeerde paneldiscussie, waarbij de zaal stevig meedeed.

De bundel met inleidingen laat zich niet in enkele pagina's samenvatten. Hij is in de A.C.-documentatie opgenomen.

6. Informatie uit de werkgroep fysieke beveiliging
(Sectie Beveiliging van het Nederlands Genootschap voor Informatica)
door A.W. Neisingh

De werkgroep fysieke beveiliging behandelt op dit moment de volgende onderwerpen:

a. fysieke beveiliging,
b. verhuizing van computercentra,
c. praktische problemen bij bouw en inrichting van computercentra,
d. keuzecriteria vestigingsplaats van een computercentrum,
e. noodvoorzieningenplan.

Naar aanleiding van contacten, die ik in het kader van de werkgroepactiviteiten heb gehad, is een tweetal punten vermeldenswaard:

1. Bij de afdeling Bouw- en Woningtoezicht van gemeenten zijn tegen een geringe vergoeding de bouwtekeningen van panden en dus ook van computercentra voor een ieder verkrijgbaar.
Bedacht dient te worden dat op deze tekeningen nogal eens in detail de getroffen beveiligingsmaatregelen (bijvoorbeeld toegangsbeveiliging) zijn aangegeven, zodat op zeer eenvoudige wijze vertrouwelijke gegevens kunnen uitlekken.
Het verdient aanbeveling met gemeenten afspraken te maken met betrekking tot de mate van detaillering van de tekeningen en de verstrekking van bepaalde tekeningen.

2. Met een zekere regelmaat wordt brandsignaleringsapparatuur getest. De hiervoor gebruikelijke test blijkt slechts bedoeld te zijn om het elektrische circuit te testen en dus niet de goede werking van de snuffelapparaatjes.
Het zou veelvuldig voorkomen, aldus mijn zegslieden, dat brandsignaleringsapparatuur niet goed functioneert in geval van een brand.

Bij de bouw en inrichting van computercentra wordt men veelal geconfronteerd met praktische problemen.
Een aantal van deze problemen is hierna genoemd. Mocht U kennis hebben van andere problemen, dan verneemt de Sectie deze gaarne.

Bijlage bij punt 1: Praktische problemen (1 t/m 8) en attentiepunten (9 t/m 15) bij de bouw en inrichting van computercentra

1. Doorzakkende verhoogde vloer (ten gevolge van slechte kwaliteit).
2. Verkeerde aansluiting Halon-installatie; onvoldoende capaciteit voor de te behandelen ruimte.
3. Rook- en brandmelders niet correct afgesteld (signaleren dus niet in geval van nood).
4. Automatische koppeling spanning computer en Halon-installatie aan melders (problemen bij vals alarm).

5. Wegen niet gereed bij oplevering centrum, waardoor verhuiswagens het nieuwe centrum niet kunnen bereiken.
6. Deursloten defect.
7. Ondanks in contract opgenomen afspraken met aannemer/architect bestandenkluis niet brandvrij.
8. Telefoonlijnen niet tijdig beschikbaar.
9. Brandsignalering gehele gebouw ook in computercentrum (inclusief toiletten, operatorverblijfruimte en dergelijke) zichtbaar en/of "hoor"baar maken.
10. Bij uitgang van het computercentrum
    - brandmelder installeren,
    - korte instructies met betrekking tot brandmelding en -bestrijding ophangen.
11. Noodstroomvoorzieningen aanbrengen (of noodlamp).
12. Toegang tot centrum mogelijk maken voor brandweer (deblokkeren toegangscontrole-apparatuur, moedersleutel bij brandweer of iets dergelijks).
13. Geen voor wat betreft getroffen beveiligingsmaatregelen gedetailleerde tekeningen bij Bouw- en Woningtoezicht deponeren, omdat deze door derden ter inzage kunnen worden verkregen.
14. Testen van opgeleverde installaties door onafhankelijke bureaus.
15. Noodknop energievoorziening: uittrekken in plaats van indrukken in verband met risico van per ongeluk stroom uitschakelen.

7. Survey 1980

De EDP Auditors Association, Inc. heeft in een speciaal nummer van maart 1980 de EDP Auditor 2nd Salary Survey gepubliceerd. De resultaten zijn ontleend aan 257 antwoorden, zijnde 7% van het ledenbestand, 242 leden in het bedrijfsleven en 15 bij public accounting firms.

De volgende ratio's zijn gegeven:

1. De verhouding aantal "Application programmer", "Programmer analyst", "DP operation staff" alsmede "Internal auditors" ten opzichte van het aantal EDP auditors.
2. De inzet, uitgedrukt in percentages, bij de verschillende soorten opdrachten: "Data center audits", "Application systems review", "Operation systems", alsmede "System design/Development review".
3. De functionaris die de salarissen vaststelt.
4. Gemiddelde salaris per functie.
5. Doorsnee aantal jaren van ervaring in de verschillende posities.

De antwoorden zijn onderverdeeld in de volgende categorieën:
Totaal; Banking/Financial; Manufacturing; Insurance; Public Utility; Wholesale sales, Retail sales & Distribution; Government; Educational; Energy related; Miscellaneous; Public accountants.