compact

COMPUTER EN ACCOUNTANT

Klynveld Kraayenhof & co
ACCOUNTANTS

NUMMER 15 5E JAARGANG NAJAAR 1978

VAN DE REDACTIE

Wanneer in de controle het gebruik van de computer aan de orde komt, zullen in de meeste gevallen ook één of meerdere selecties van te controleren posten worden uitgevoerd op basis van een mathematische steekproef. Het ligt dan ook voor de hand, dat er veel contact bestaat tussen de AC-groep en diegenen, die zich binnen KKC meer in het bijzonder met steekproeven bezighouden. De vaktechnische verantwoordelijkheid voor de ontwikkeling en het gebruik van steekproefmethoden ligt bij de Steekproefcommissie, welke bestaat uit de heren J.H. Blokdijk, Mr. Drs. L.G.P. van Gasselt en C. Rietveld.

Het is deze laatste die reeds jaren geleden een voor de accountantscontrole doelmatige steekproefmethode ontwikkelde welke intern reeds bekend werd onder de naam "Zeefmethode".

In het regelmatig overleg tussen AC-leiding en de Steekproefcommissie kwam het gebrek aan mogelijkheden tot intern publiceren aan de orde. Gezien de relatie tussen accountantscontrole, automatisering en steekproeven heeft de redactie van Compact de heer Rietveld gaarne in de gelegenheid gesteld ons via het huisorgaan van de AC-groep met de Zeefmethode kennis te laten maken.

Ter gelegenheid hiervan wordt het herfstnummer van Compact, dat andermaal net op tijd gereed kwam, op wat ruimere schaal verspreid, zodat in principe iedereen vanaf de functie controleleider van de Zeefmethode kan kennis nemen.

Compact is een uitgave van de groep Automatisering en Controle 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:
A.W. Neisingh, J. Philippo, en D. Steeman.
Adres: Pr. Irenestraat 59 Amsterdam

DE ZEEFMETHODE ALS SELECTIEMETHODE VOOR STATISTISCHE STEEKPROEVEN IN DE CONTROLEPRAKTIJK (I)

door C. Rietveld

Algemene beschouwingen over de zeefmethode*

1. Inleiding

Statistische steekproeven zijn een belangrijk middel voor de verkrijging van een verantwoord oordeel over de betrouwbaarheid van te verifiëren gegevens. Een vereiste is echter de hantering van een selectie- en evaluatiemethode, die niet alleen statistisch correct, maar ook efficiënt en veelzijdig is in haar toepassingsmogelijkheden, gelet op de veelsoortigheid van de door ons te controleren verantwoordingen.

Uitgaande van de methode die door mij in 1959 werd gevonden, zijn in het licht van genoemde twee eisen meer recentelijk nieuwe technieken ontwikkeld, waarbij het flexibele karakter van de methode geheel kon worden benut. Dankzij dit karakter zijn thans toepassingen mogelijk, die voorheen niet of niet op efficiënte wijze te realiseren waren. Aan de methode en de daarop gebaseerde technieken heb ik de verzamelnaam zeefmethode gegeven.

In de controlepraktijk wordt naast de zeefmethode de guldenrangnummermethode gehanteerd. Deze methode werd door A. van Heerden in 1961 in het Maandblad voor Accountancy en Bedrijfseconomie geïntroduceerd. Kennisneming van eerder door hem geproduceerde stukken hebben mij tot de zeefmethode geïnspireerd. In zijn artikel refereert A. van Heerden aan deze methode, die hij omschrijft als een stratificatiemethode, samenhangend met de toenmalig toegepaste techniek.

De guldenrangnummermethode wordt om praktische redenen veelal niet toegepast zoals deze door A. van Heerden in zijn artikel werd beschreven. Daartoe zijn varianten ontwikkeld met toepassing van variabele intervallen. Tot die varianten is mede te rekenen de methode, die in de V.S. onder de naam cell-sampling werd geïntroduceerd en onder meer in Auditape wordt toegepast.

Hoewel de selectie bij de zeefmethode niet met die bij cell-sampling overeenkomt, is er statistisch verwantschap tussen beide methoden. De statistische juistheid van de cell-sampling-methode en van de zeefmethode werd bevestigd door het Mathematisch Centrum (met name drs. A.P.B.M. Vehmeyer, alsmede R.D. Gill voor de later ontwikkelde zeefmethodieken). In het hierna volgende worden conclusies voortvloeiende uit de bewijsvoering vermeld, zonder daar telkenmale naar te verwijzen.

* Degenen, die kennis willen nemen van beschouwingen over de toepassing van statistische steekproeven in het algemeen, verwijs ik naar het onderdeel III 11, geschreven door J.H. Blokdijk, in het handboek Accountancy.

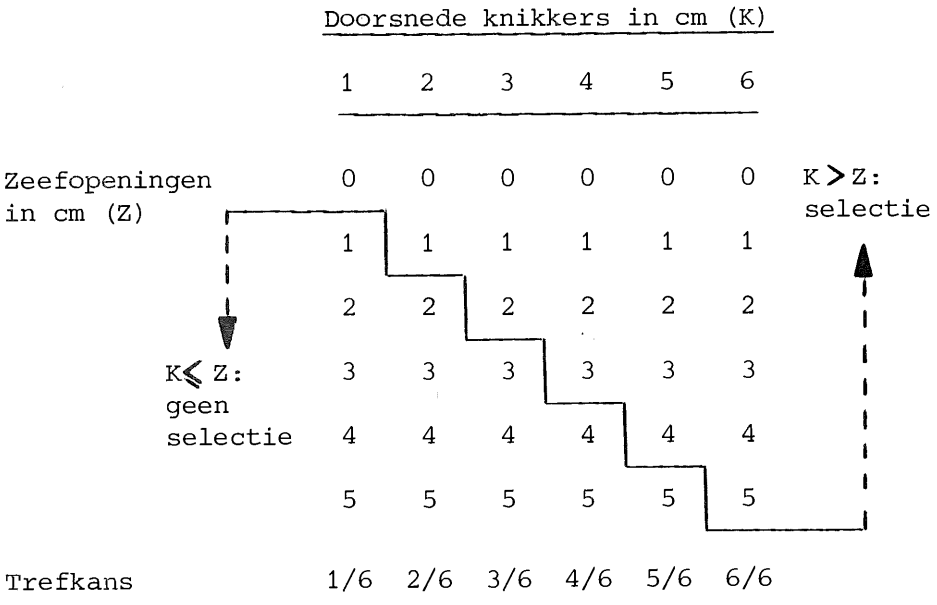
2. Knikkers gezeefd

De zeefmethode richt zich op een selectie van elementen (posten) uit een verzameling (verantwoording) met trefkansen evenredig aan hun grootten. Ik wil dit illustreren aan de hand van een voorbeeld met knikkers.

Gegeven zij een bak, gevuld met knikkers met doorsneden van respectievelijk 1, 2, 3, 4, 5 en 6 cm. Het aantal knikkers per doorsnede is onbekend. Men wil de knikkers ten dele aan een kwaliteitsonderzoek onderwerpen door toepassing van een zodanige selectie, dat een knikker met 1 cm doorsnede 1/6 kans heeft om getrokken te worden, één met 2cm doorsnede 2/6 kans, enz. en één met 6 cm doorsnede 6/6 (= 100%) kans.

Ten behoeve van de selectie worden de knikkers één voor één via een transportgoot langs een zeef geleid met een zeefopening, die een telkenmale wisselende doorsnede heeft. De variaties in de doorsneden van de zeefopening zijn 0, 1, 2, 3, 4 of 5 cm. Per knikker wordt door een random-generator een a-select getal (0, 1, 2, 3, 4 of 5) geproduceerd, welk getal bepalend is voor de doorsnede van de elektronisch bestuurde zeefopening.

Knikkers groter dan de zeefopening worden geselecteerd en via de goot naar de kwaliteitscontroleurs geleid. De knikkers die kleiner zijn dan c.q. gelijk zijn aan de doorsnede van de zeefopening en derhalve niet geselecteerd worden, worden via deze zeefopening afgevoerd. Uit de navolgende tabel blijken alle voorkomende gevallen, waarin selectie plaatsvindt en de daarmede samenhangende trefkansen.



Het selectiecriterium is hier: doorsnede knikker in cm > doorsnede zeefopening in cm? Het aantal gevallen, dat voldoet aan dit criterium neemt evenredig toe met de doorsnede in cm van de knikkers. Derhalve neemt ook de trefkans evenredig toe.

Het aantal cm doorsnede van een zeefopening noemen we zeefgetal (Z). De omvang van een zeefgetal wordt bepaald door het zeefmaximum (M), dat is de doorsnede (waarde) met 100% trefkans, te weten 6 cm. De zeefgetallen (Z) zijn dan 0, 1, ..., 5 of in het algemeen 0,1, ..., M-1. Het selectiecriterium luidt in het algemeen: waarde > zeefgetal?

Het is niet noodzakelijk, dat de mogelijke doorsneden van de knikkers een rekenkundige reeks vormen. Zouden er drie formaten zijn, bijvoorbeeld 1, 3 en 6 cm, dan vervallen alleen de kolommen ~~1~~ 2, ~~3~~ 4 en ~~6~~ 5 zonder aantasting van de overige bevindingen.

De zeefmethode is in de controlepraktijk op identieke wijze toe te passen, waarbij voor de aantallen cm doorsnede van de knikkers in de plaats treden de waarden van de posten in de verantwoording.

3. De toepassing van de zeefmethode in de controlepraktijk

De toepassing in de controlepraktijk wordt aan de hand van een voorbeeld besproken.

Een verantwoording sluit met een totaal van f 11,5 miljoen, waarbij we er voorlopig van uitgaan, dat de posten geheel goed of geheel fout zijn. Het steekproefplan richt zich op de uitspraak, dat de fouten in de verantwoording ten hoogste 2% (d.i. f 230.000) zullen bedragen met een betrouwbaarheid van tenminste 99% ten aanzien van de juistheid van die conclusie. In de verwachting dat in de steekproef geen fouten zullen voorkomen, wordt volgens de betrokken tabel op basis van de Poisson-verdeling de steekproefomvang op 230 (4,6 :0,02) bepaald.

Men stelle zich nu een grote zeef voor, waarin voor elke afzonderlijken post (P) van de verantwoording één zeefopening voorkomt. De grootten van de zeefopeningen worden a-select en onafhankelijk van elkaar bepaald. Elke post groter dan de voor die post aangewezen zeefopening blijft als steekproefpost ter controle achter. De overige posten vallen door de zeef en worden derhalve niet gecontroleerd.

De grootte van de zeefopening wordt door een a-select getal bepaald. Dit zeefgetal (Z) wordt als volgt berekend:

Bij een verantwoordingstotaal van f 11,5 miljoen en een steekproefomvang van 230 posten is er gemiddeld één steekproefpost per f 50.000 (11,5 miljoen : 230 ofwel T : m). Dit gemiddelde wordt gehanteerd als zeefmaximum (M). Posten met een waarde tenminste gelijk aan dat zeefmaximum krijgen een 100% trefkans.

De mogelijke zeefgetallen zijn dan 0,1, ..., M-1 ofwel 0,1, ..., 49999 (50.000 mogelijkheden). Deze zeefgetallen verkrijgt men bijvoorbeeld door uit de reeks 0,00000, 0,00001, ..., 0,99999 (100.000 mogelijkheden) voor elke post een a-select getal te trekken, deze met het zeefmaximum (50.000) te vermenigvuldigen en de uitkomst naar beneden op gehelen af te ronden.

De waarde van elke afzonderlijke post wordt getoetst aan het voor die post aangewezen zeefgetal: elke post groter dan zijn zeefgetal wordt als te controleren post aangewezen.

Bij een post van f 2.472 zal aanwijzing als te controleren post geschieden bij de zeefgetallen 0,1, ..., 2.471, dit is in 2.472 van de 50.000 gevallen (trefkans 4,944%). Bij een tweemaal zo grote post (f 4.944) zal de aanwijzing geschieden bij de zeefgetallen 0,1, ..., 4.943, dit is in 4.944 van de 50.000 gevallen (trefkans 9,888%). De trefkans neemt derhalve evenredig met de waarde toe.

Nader uitgewerkt voorbeeld:

Nrs.	A-select getal (a)	Posten (P)	Zeefmaximum (M)	Zeefgetal (Z = M * a)	Te controleren (P > Z?)
1	0,22683	3.780	50.000	11.341	neen
2	0,66041	14.720	50.000	33.020	neen
3	0,00846	1.150	50.000	423	ja
4	0,65429	7.715	50.000	32.714	neen
5	0,08035	2.570	50.000	4.017	neen
6	0,77440	56.230	50.000	38.720	ja

Post 6 bedraagt meer dan het zeefmaximum, en dus ook meer dan elk mogelijk zeefgetal. Dit impliceert een 100% trefkans.

Indien de steekproefomvang niet op 230 maar op 460 zou worden gesteld, wordt het zeefmaximum 11,5 miljoen, gedeeld door 460, dit is 25.000, zodat de zeefgetallen worden gehalveerd. Door de vermindering van het zeefgetal van post 5 van 4.017 tot 2.008, wordt deze post nu wel geselecteerd. Ten aanzien van de overige posten ondergaan de conclusies geen wijziging.

Bij een steekproefomvang van 115 posten wordt het zeefmaximum 11,5 miljoen, gedeeld door 115, dit is 100.000. Post 6 is nu kleiner dan het zeefmaximum en heeft geen 100% trefkans meer. Het zeefgetal wordt in het voorbeeld 77.440, zodat post 6 nu niet wordt geselecteerd.

De betekenis van de hier en elders gebruikte aanduidingen wordt voor naslag door de lezer hieronder gerecapituleerd en binnen een kader geplaatst.

T	=	totaalbedrag der verantwoording
m	=	tevoren bepaalde steekproefomvang
n	=	aantal in feite geselecteerde, te controleren posten
p	=	bovengrens van de fractie fouten in de verantwoording
P	=	bedrag van één bepaalde post
M	=	zeefmaximum, behorend bij een steekproefomvang van m-posten
a	=	a-select getal, behorend bij post P
Z	=	zeefgetal, behorend bij post P en een steekproefomvang van m posten

Het zal duidelijk zijn, dat n van het toeval afhankelijk is en daarom van m kan afwijken.

4. Evaluatie van de steekproefuitkomsten

Voor de evaluatie van de steekproefuitkomsten kunnen ook voor de zeefmethode de tabellen voor bovengrenzen, berekend op basis van de Poisson-verdeling, worden gebruikt.
Hieronder volgt een beknopte tabel voor mp:

Betrouwbaarheid in %	99,9%	99%	90%
Aantal fouten in de steekproef:			
0	6,91	4,60	2,30
1	9,23	6,64	3,89
2	11,23	8,41	5,33
3	13,06	10,05	6,69

We gaan er ook hier allereerst van uit, dat posten geheel goed of geheel fout zijn.

Bij 99% betrouwbaarheid en constatering van 0 fouten in de steekproef vinden we het getal 4,60. Dit is het produkt (mp) van

- de tevoren bepaalde steekproefomvang (m),
- de bovengrens van de fractie (= percentage/100) fouten in de verantwoording (p).

In ons voorbeeld op pag. 5 is de steekproefomvang 230. Wij kunnen dus met een betrouwbaarheid van tenminste 99% stellen bij constatering van 0 fouten, dat de verantwoording fout is voor ten hoogste:

$\frac{4,60}{230}$ = 2% van f 11,5 miljoen, dit is f 230.000.

Gaan we in ons voorbeeld uit van een steekproefomvang van 669, dan kunnen we bij 3 geconstateerde fouten met tenminste 90% betrouwbaarheid stellen, dat de verantwoording fout is voor ten hoogste:

$\frac{6,69}{669}$ = 1% van f 11,5 miljoen, dit is f 115.000.

Uit de bewijsvoering voor de zeefmethode vloeit voort, dat - evenals voor de guldenrangnummermethode - de Poisson-verdeling een maximaliserende benadering van de feitelijke kansverdeling geeft. Voor de zeefmethode geldt daarbij echter als vuistregel: de waarde van mp moet tenminste 2, dit is de betrouwbaarheidseis tenminste 87% zijn, welke grens in de accountantspraktijk geen enkel probleem vormt.

Indien gedeeltelijk foute posten in de verantwoording voorkomen, kan dezelfde selectieprocedure worden toegepast, zoals deze onder 3 is beschreven. Alleen zal in het steekproefplan moeten worden aangegeven, hoe gedeeltelijk foute posten bij de evaluatie zullen moeten worden behandeld. Een mogelijke behandelingswijze is de navolgende. Stel dat post 3 in het voorbeeld op blz. 5 ad f 1.150 voor f 350 fout is. De trefkans van de fout dient te zijn 350/50.000, dat is de fout in relatie tot het zeefmaximum. De kans de foute post te treffen wordt echter primair bepaald door de grootte van de post en is derhalve 1.150/50.000. De trefkans moet derhalve met 350/1.150 verkleind worden. Dit wordt gerealiseerd door toetsing van de fout aan het zeefgetal van de post. In ons voorbeeld is dat 423, zodat de fout van f 350 in post 3 voor de evaluatie niet als fout meetelt. De post zal wel meetellen bij de zeefgetallen 0,1, ..., 349, dit is in 350 van de 1.150 gevallen.

Wij krijgen dan:

- de kans dat post 3 ter controle wordt aangewezen is 1.150/50.000,
- de kans dat de fout in post 3 vervolgens in de evaluatie meetelt is 350/1.150,

zodat de resulterende kans, dat de fout in de steekproef valt volgens de produktregel is:

1.150/50.000 x 350/1.150 = 350/50.000.

Dit komt overeen met het belang van de fout, in relatie tot het zeefmaximum.

Een bijzonder aspect bij de evaluatie bieden de posten met 100% trefkans. Stel, dat in ons voorbeeld:

- een deel ad f 1,5 miljoen een 100% trefkans heeft en derhalve volledig wordt gecontroleerd (posten $\geq$ zeefmaximum, dit is 50.000);
- een deel ad f 10 miljoen derhalve steekproefsgewijs wordt gecontroleerd (posten $<$ zeefmaximum, dit is 50.000).

Stel voorts, dat in de steekproef de volgende fouten worden geconstateerd:

Nr.	Post	Fout	Zeefgetal
1	60.000	60.000	16.420
2	55.000	25.000	28.378
3	1.000	700	825
4	2.000	1.200	417

Ten aanzien van het deel dat volledig wordt gecontroleerd kan met 100% betrouwbaarheid gesteld worden, dat de fouten in totaal niet meer dan f 85.000 (posten 1 en 2) bedragen.

Uit het resterende deel worden evenredig minder posten getrokken, te weten 10/11,5 x 230 = 200.

De fout in post 3 telt statistisch niet mee, aangezien deze kleiner is dan het zeefgetal.

In de steekproef komt derhalve één fout voor. Met een betrouwbaarheid van tenminste 99% is nu te stellen, dat bij een steekproefomvang van 200 posten de fouten te zamen ten hoogste bedragen:

$\frac{6,64}{200}$ = 3,32% van f 10 miljoen, dit is f 332.000.

Deze uitkomst is gelijk aan die voor 1 fout in een steekproef van 230 posten en een verantwoordingstotaal van f 11,5 miljoen, te weten:

$\frac{6,64}{230}$ = 2,89% van f 11,5 miljoen, dit is f 332.000.

Het is derhalve niet nodig de posten met 100% trefkans te totaliseren, ten einde daaruit de omvang van het steekproefsgewijs gecontroleerde deel af te leiden. Men kan zonder meer uitgaan van de totale omvang van de verantwoording en van de steekproefomvang, die als basis voor het steekproefplan heeft gediend.

Samenvattend concluderen wij, dat de fouten in totaal bedragen:

- met 100% betrouwbaarheid	f 85.000
- met tenminste 99% betrouwbaarheid ten hoogste	" 332.000
- te zamen met tenminste 99% betrouwbaarheid ten hoogste	f 417.000

Er zijn andere benaderingen mogelijk, die echter mijns inziens minder exact zijn.

Volledigheidshalve vermeld ik ten behoeve van de kenners van de TARS-evaluatiemethode (onder meer gehanteerd bij Auditape), dat deze ook

bij de zeefmethode toe te passen is. Wel zij opgemerkt, dat de juistheid van deze evaluatiemethode - althans voor zover wij weten - nog niet bewezen is. Dit geldt derhalve ook voor de toepassing bij Auditape.

Nog afgezien van de invloed van volledig gecontroleerde posten ($\geqslant$ zeefmaximum) kan het getrokken aantal te controleren posten (n) afwijken van het aantal volgens het steekproefplan (m). Of uit een bepaalde trekking al dan niet de aanwijzing van een te controleren post resulteert is immers van het toeval afhankelijk. Het getrokken aantal zal echter wel het te voren bepaalde aantal benaderen. Het is bewezen dat een eventuele afwijking geen invloed heeft op de evaluatie. Men kan stellen, dat een aantal goede posten meer of minder er niet toe doet, als de trefkans van foute posten maar aan de te stellen eisen voldoet.
En deze trefkans wordt bepaald door de hoogte van het zeefmaximum, dat van de te voren bepaalde omvang afhankelijk is.

De trefkans van fouten neemt lineair toe met de grootte van die fouten, hoewel een iets minder dan evenredige toeneming voldoende zou zijn. Voor fouten tot 10 à 25% van het zeefmaximum is het effect te verwaarlozen. Bij aanwezigheid van grotere fouten neemt echter de feitelijke betrouwbaarheid van de uitspraken toe. Een incidenteel gevolg kan echter zijn, dat een grote fout in de evaluatie meetelt, doch bij een exactere benadering niet zou zijn getroffen. Dit is overigens alleen een probleem als er een onaanvaardbare uitkomst zou resulteren. Voor dat geval zijn reduktiefactoren te gebruiken (zoals bij Auditape voor het middle-stratum). In het licht van een nader onderzoek door het Mathematisch Centrum naar de mathematische aspecten van reduktiefactoren voor de zeefmethode en de cell-sampling methode ga ik op deze plaats niet nader op deze reduktiefactoren in.

5. Analyse van de verschillen van de zeefmethode ten opzichte van andere methoden

Deze analyse beperk ik tot een vergelijking met de guldenrangnummermethode, zoals deze door A. van Heerden in zijn artikel werd geïntroduceerd en met de cell-sampling methode als één van de varianten van de guldenrangnummermethode op basis van intervallen.

De oorspronkelijke guldenrangnummermethode nummert alle individuele guldens van de verantwoording doorlopend, in ons voorbeeld (blz. 3/4) derhalve: 1,2,...,11.500.000. Al deze rangnummers nemen deel aan één loterij.
Op deze rangnummers worden 230 maal trekkingen verricht, waarmede 230 rangnummers worden aangewezen van de 230 guldens (prijzen), die dienen te worden gecontroleerd. Met de aanwijzing van de te controleren guldens zijn tevens de te controleren posten bepaald.
De aldus a-select aangewezen rangnummers worden in nummervolgorde gesorteerd. Door middel van een doorlopende telling wordt de gulden (post) met het "prijs" bepalende rangnummer opgezocht.

Bij de cell-sampling methode worden de 11,5 miljoen guldens van de verantwoording in 230 cellen van f 50.000 gesplitst. In elke cel vindt één loterij met één trekking plaats, die steeds leidt tot aanwijzing van de gulden (prijs), die dient te worden gecontroleerd. Daartoe worden per cel de guldens doorlopend genummerd: 1,2,...,50.000. Uit de 50.000 rangnummers wordt één rangnummer getrokken die de te controleren gulden en daarmee de te controleren post aanwijst. Sortering behoeft hier uiteraard niet plaats te vinden. Met een doorlopende telling binnen de cel wordt de gulden (post) met het "prijs"-bepalende rangnummer opgezocht.

Bij de zeefmethode vindt per post één loterij plaats. Als de verantwoording in ons voorbeeld 60.000 posten zou omvatten, zijn er 60.000 loterijen. In elke loterij vindt één trekking plaats, in ons voorbeeld uit de getallen 0,1,...,49999. Deze trekking geeft alleen een kans op een "prijs"-bepaling, namelijk als de waarde van de post groter is dan het getrokken getal. Door deze directe confrontatie worden de te controleren posten gelijktijdig met de trekkingen aangewezen; voor de selectie zijn geen rangnummers, tellingen en sorteringen vereist. Er is bij de selectie geen enkele samenhang tussen de posten, zoals men die vindt bij de andere methoden door de vaststelling van rangnummers. Juist dit facet verleent aan de zeefmethode de grote mate van flexibiliteit.

De oorspronkelijke guldenrangnummermethode kent geen 100%-trefkans.

De cell-sampling methode kent een 100% trefkans voor posten die tenminste gelijk zijn aan twee cellen. Dit vloeit voort uit de mogelijkheid dat een grote post over twee cellen verdeeld kan zijn.

De zeefmethode heeft, zoals eerder bleek, een 100%-trefkans voor posten tenminste gelijk aan het zeefmaximum (= bij cell-sampling grootte van een cel bij gelijke steekproefomvang).

De oorspronkelijke guldenrangnummermethode geeft de meest exacte evaluatie-uitkomsten. Om aan enige praktische bezwaren tegemoet te komen (onder meer voorkoming van sorteerarbeid) is men overgegaan tot methoden met variabele intervallen. Zoals eerder gesteld zou men cell-sampling ook tot deze methoden kunnen rekenen. Men heeft bij deze methoden - overigens in het algemeen in aanvaardbare mate - de exactheid opgeofferd ter verkrijging van praktische selectie-methoden, wat een iets te hoge kans op het treffen van fouten tot gevolg heeft. Dit geldt in wezen ook voor de zeefmethode.

De mate van exactheid wordt bij de zeefmethode en de cell-sampling methode bepaald door de mate, waarin de fouten in de verantwoording over de posten (zeefmethode) respectievelijk de cel (cell-sampling) zijn verspreid. Dit impliceert een grotere exactheid van de zeefmethode omdat de spreiding over bijvoorbeeld 60.000 posten veelal groter zal zijn dan over bijvoorbeeld 230 cellen. De iets te hoge kans

op het vinden van fouten geldt voorts bij de zeefmethode alleen voor concentraties van fouten in grote posten, maar bij cell-sampling voor die binnen één cel, ook al zijn ze over verschillende kleinere posten verspreid.

Een ander verschil tussen de zeefmethode en de andere methoden is, dat voor alle posten a-selecte zeefgetallen moeten worden berekend en toetsing met deze getallen moet plaatsvinden. Bij vele, zo niet alle toepassingen met de computer is dit aspect niet of nauwelijks van enige betekenis. Voor de gevallen, waarin dit punt echter wel van belang is, zoals voor niet-geautomatiseerde verantwoordingen, zijn subselectiemethodieken beschikbaar. In het algemeen richt de selectie zich daarbij primair op de (sub)tellingen, die in de administratie voorkomen.

Een belangrijk praktisch verschil is echter vooral gelegen in de flexibiliteit en in de toepasbaarheid van de zeefmethode. Voor een analyse van deze praktische facetten van de zeefmethode is echter eerst kennisneming van de toepassing van zeefgrenzen en van de subselectietechniek vereist. Dit zal ik in een volgend artikel behandelen. In een derde artikel ga ik in op de mogelijkheden van selectiecombinaties, die met andere methoden niet of nauwelijks zijn te realiseren. De toe te passen methoden zijn daarbij niet alleen efficiënt ten aanzien van de selectieprocedure, maar leiden ook tot een minimalisering van de te controleren posten.

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

A. B. C. - N I E U W S

redactie A.W. Neisingh

Beveiliging

Gegevensbeveiligingssysteem van Boole & Babbage

Om te voorzien in een optimale beveiliging van computergegevens, introduceert de European Software Company het programmaprodukt "Secure" op de Europese markt. Secure is een produkt van het bekende Amerikaanse softwarebureau Boole & Babbage Inc. en is met groot succes in de markt aldaar ontvangen.

De heer J. Opschoor, Europees marketing directeur van The European Software Company, verklaarde dat de toegenomen druk van overheidswege en de publieke opinie het zonder meer noodzakelijk maken, dat de procedure, die de beveiliging van computergegevens beoogt, aanzienlijk hoort te worden uitgebreid. Dit omvat zowel de fysieke bescherming van de computerinstallatie en bestanden, als de beveiliging van de informatie binnen het systeem.

Secure voorziet in deze beveiliging zonder ingewikkelde ingrepen op en zonder extra belasting van de produktieprocedures van een dataprocessing organisatie. De fylosofie achter Secure is dat zinvolle gegevensbeveiliging alleen tot stand kan komen wanneer het wordt ondersteund door een gerichte beleidsvoering. Allereerst is fysieke controle en beveiliging noodzakelijk. Pas wanneer dat tot stand is gekomen heeft gegevensbeveiliging zin binnen een informatiesysteem.
Secure gaat uit van het concept dat een persoon verantwoordelijk is voor de beveiliging (security manager), zodat gecentraliseerde controle mogelijk is. Dit betekent dat het beschermingsmechanisme uitsluitend bekend is aan een of meerdere bevoegde personen. Om beschermde gegevens te benaderen machtigt Secure "jobs" in plaats van gebruikers, hetgeen om praktische redenen het ontwerpen van de beveiligingsprocedure vergemakkelijkt en waarbij tevens de kosten tot een minimum beperkt kunnen worden.
Secure maakt de tussenkomst van een operator overbodig, het beveiligt disk- en tapebestanden van zowel batch jobs als time sharing toepassingen en biedt een hoge mate van flexibiliteit in het vastleggen van toegangsbevoegdheden.
Bevoegdheid kan bijvoorbeeld worden gespecificeerd om het benaderen van bepaalde bestanden alleen tussen 20.00 uur en middernacht toe te staan en dan alleen nog door een specifiek programma als deel van een batch job.

Het bestand waarin de bevoegdheidssleutels zijn vastgelegd, de zogenaamde "Security Data Set", kan worden benaderd via meerdere aaneengeschakelde verwerkingseenheden. Daardoor kunnen beschermde bestanden worden verwerkt op elke centrale verwerkingseenheid zonder produktieplanning en controle te verstoren. Secure legt zowel iedere geslaagde als elke mislukte benadering van een beveiligd bestand vast (Audit). De computeroperator of time sharing gebruiker is niet betrokken bij de beveiligingsprocedure. De benadering van de beschermde gegevens wordt automatisch toegestaan of geweigerd door Secure.
Het aantal benaderingspogingen kan worden beperkt of alleen worden toegestaan als voldaan is aan zeer bijzondere voorwaarden.
Toegang kan ook beperkt worden tot specifieke jobnamen, speciale time sharing operating logon ID's, of aan specifieke programmanamen.
Secure werkt met de IBM operating systemen MFT, MVT, VSI, SVS en MVS.

De Automatiseringsgids, 22 juni 1978

Infrarood deurcontact

De Britse firma Euroswitch heeft een van de eerste miniatuur infrarood apparatuur op de markt gebracht in de vorm van een superveilig deurcontact voor stalen deuren, de Iroswitch.
Dit instrument moet het probleem van magnetische dispersie oplossen, dat zich voordoet wanneer de normale reed switches worden gebruikt in stalen deuren. De Iroswitch functioneert op iedere energiebron van 12 V en is compatibel met standaard-alarmsystemen. Het apparaat bestaat uit twee hoofdcomponenten, gebaseerd op de nieuwste CMOS (complementary metal oxide semiconductor) elektronische technologie. Het geïntegreerde circuit, de LED (light emitting diode) met gecodeerde infrarood-transmissie en een fotosensitieve diode bevinden zich in het ene gedeelte, dat een diameter van 15 mm heeft. Het andere gedeelte, een parabolische reflector met een diameter van 22 mm, geeft het apparaat zijn beveiligende capaciteiten. De twee componenten passen precies in elkaar. Het ene stuk komt in de deur zelf, het andere in de deurpost. Als het systeem in werking is gesteld, zendt de lichtgevende diode een gecodeerde infraroodstraal uit, die door de reflector wordt weerkaatst. De fotosensitieve diode leest de infraroodstraal af en zorgt ervoor, dat de schakelaar aan blijft staan als de fase, frequentie en intensiteit kloppen, en zet hem uit als deze gegevens onjuist zijn. Als iemand knoeit met de schakelaar wordt het alarm geactiveerd. De schakelaar kan ook worden gebruikt als branddetector.

De Automatiseringsgids, 3 augustus 1978

Slot op toetsenbord

Het Britse bedrijf Microbourne meent het eerste toetsenbord-grendelsysteem ter voorkoming van het onbevoegd gebruik van machines te hebben geïntroduceerd. Sentrymaster 2002 Machine Lock kan ieder instrumentarium beschermen, van typemachine tot draaibanken.
De sloten zijn autonoom en gemakkelijk te installeren. Wanneer ze eenmaal zijn gemonteerd, is geen verder onderhoud vereist. Met dit slot kan de machine pas worden gestart, wanneer de correcte, uit vier cijfers bestaande code is ingetoetst. Om de machine te blokkeren hoeft alleen maar een verkeerd cijfer te worden ingedrukt.
Het standaardslot kent twee versies en heeft een vermogen van maximaal 5 A bij 240 V. Het ene type slot is voorzien van mechanische drukknoppen en zit in een solide metalen huls. Het andere type heeft een volkomen afgesloten "touch-sensitive" toetsenbord zonder bewegende delen.
De te gebruiken code wordt bepaald door een verwisselbare afgesloten codeplug die met het blote oog niet kan worden afgelezen. De code kan worden veranderd door de plug gewoon te verplaatsen. Een alarmfaciliteit kan worden toegevoegd om op afstand een onjuiste code of geknoei met het toetsenbord te signaleren. Het alarm stopt automatisch wanneer de juiste code worde ingetoetst. Eén machine kan vanaf verschillende punten in de gaten worden gehouden, maar ook kan een heel stel machines tegelijk vanaf één punt worden beveiligd. Voor gevaarlijke of extreme omstandigheden kunnen waterproof omhulsels en hittewerende en geïsoleerde kabels worden geleverd.

De Automatiseringsgids, 3 augustus 1978

Computerfraude: Moeten we ermee leren leven?

Australia is hit by computer crime

Business in Australia is hit increasingly by computer related crime, but management is burying its head in the sand and hoping that the problem will go away. Making this comment, the Sydney chapter of the Electronic Data Processing Auditors' Association says that an increasing proportion of the $A 500 million a year that "white collar" crime is said to cost now involves computers.
A spokesman for the association said it was estimated that there were about 2,000 computers in the country and about 20,000 DP staff. Although that was small by US standards, it was worth remembering that the foreign assets and investments they control were not.

Australia is reputed to produce some of the world's most proficient white-collar criminals. A senior investigator of the Corporate Affairs Commission in New South Wales is on record as saying: "Per head of population, in all spheres of white-collar crime, Australians rank as one of the most distinguished groups of people in the world"
The fear among Australian computer people is, that as matters stand, there is little to deter this "distinguished group" from schemes of million dollar embezzlement through computer crime.
The 7,000-member Computer Society of Australia has issued computer security standards for Australian companies, which have been endorsed by the auditors' association, but within the Australian security business the feeling generally is that Australian management is more concerned to lock the computer than to employ expert DP auditors to check the programs for criminal activity.
There have been very few reported Australian computer crimes of any magnitude, and the Australian investing public is less accustomed to its reality than are Americans. For that reason management is more inclined to dismiss employees found guilty of fraud and embezzlement, than prefer criminal charges, since a scandal may well adversely affect the standing of the company.
Neither can foreign investors expect much protection from the Australian police. At a national crime seminar last year, delegates were told that more and more Australian criminals were turning to white-collar crime - in one State alone there had been an increase of 220% in fraud over the previous year - but the lack of technically trained staff rendered the state's police force powerless to deal with it.
The first seminar for police on computer crime was held last year at which 30 officers were given a five-hour lecture. The head of Sydney's fraud squad said: "In the end, we are going to have people specialising in computer crime".
But Australia already has people specialising in computer crime. Last year they stole an estimated $A 10 million, and Australian professional bodies know that those who hope to combat their larceny must match their skills with rather more than a few hours instruction.

The reality is that Australian police forces are inadequately staffed or trained for the task. But, even if Australian management did train their staff in computer security, would the Australian courts convict the criminals?
At a national seminar on white-collar crime a former director of the UN crime prevention programme said that Australian criminal courts were "grossly inadequate" in dealing with such crime, and he urged a change in the jury system to include technical experts. His argument is particularly valid in the cases of computer fraud.

Computer Weekly International, 13 juli 1978

VS werken aan wet, uitsluitend tegen computermisdrijven

Een groep Amerikaanse senatoren werkt op het ogenblik aan een wetsvoorstel, dat de bestraffing van misdrijven begaan met behulp van computers moet regelen. Het voorstel zal zich echter beperken tot het ge- of misbruik van systemen bij de overheid en van financiële instanties. Op het ogenblik wordt er naar schatting per jaar in de VS ruim tweehonderd miljoen gulden aan de computermisdaad verdiend, maar men verwacht, dat dit toch al fikse bedrag in de komende jaren aanzienlijk zal toenemen.
De maximale straf die men op een computermisdrijf wil stellen, bedraagt vijftigduizend dollar of vijftien jaar gevangenis.

Computable, 6 oktober 1978

Diefstal per computer, geavanceerde misdaad

Wie ooit in de clinch is gegaan met een computer en het niet heeft kunnen winnen zal zeker met plezier Thomas Whiteside's "Computer Capers" lezen. Zelfs de meest integere, ordelievende burgers zullen in hun hart bewondering hebben voor de "masterminds" achter deze waar-gebeurde verhalen over de elektronische diefstallen, ook al plegen ze luidruchtig hun diepgewortelde haat te ventileren tegen de technische wonderen die hun leven zijn binnengeslopen.

Volgens Whiteside zijn sommige foefjes om de computer te overtroeven verbluffend simpel, zoals in het geval van de jongeman die iets van het gedrag van computers wist, een persoonlijke lening aanvroeg en kreeg bij een bank in New York. Samen met het geld kreeg hij een boekje met computer-gecodeerde formulieren, waarvan hij er bij iedere maandelijks betaling één moest opsturen naar de bank. In plaats van het eerste formulier scheurde hij de laatste uit het boekje en stuurde hem samen met de maandelijkse aflossing naar de bank. Vervolgens ontving hij van de bank - dat wil zeggen van de computer - een brief waarin hij hartelijk werd bedankt voor het snelle aflossen van de lening en hem werd verzekerd dat zijn kredietwaardigheid voor de bank buiten kijf stond. De jongeman stal niet écht van de bank, hij wachtte daarna gewoon af wat de volgende stap van de computer zou zijn.

Je hoeft helemaal niets van computers te weten om deze verhalen van oplichterij en bedrog met plezier te kunnen volgen. In feite wisten veel van de computermisdadigers in het boek erg weinig van computers, maar des te meer van het menselijk gedrag.
Omdat de computer een zwijgende partner is, wordt slechts een fractie ontdekt van de misdaden die iets met computers te maken hebben. Computerbeveiligingsspecialisten schatten, dat diefstallen waarbij gebruik wordt gemaakt van een computer, per jaar gemiddeld het enorme bedrag van $ 300 miljoen oplevert.

Computermisdaden komen meestal niet aan het licht, vaak omdat mensen geintimideerd worden door computers. Zakenlieden, die werknemers nooit uit een belangrijke functie zouden ontslaan zonder het slot op de deur en de combinatie van het brandkastslot te veranderen, laten een computerterminal open en bloot achter en gebruiken één programmeur om het hele systeem te ontwerpen, terwijl ze een dergelijk persoon ontslaan zonder ook maar de meest rudimentaire veranderingen aan te brengen in het computerveiligheidssysteem. Het gevolg is, dat dezelfde zakenlieden soms niet in het openbaar durven toe te geven, dat ze het slachtoffer zijn geworden van computermisdaden.
Dit laatste, gecombineerd met het feit, dat geldig bewijsmateriaal moeilijk is te construeren aan de hand van digitaal opgeslagen informatie, heeft de vervolging van computermisdadigers erg moeilijk gemaakt.

Fabrikanten van computers, beveiligingsadviseurs (security consultants) en zakenlieden zoeken constant naar manieren om een computer onaantastbaar te maken. In het begin van de zeventiger jaren begon IBM met een programma dat $ 40 miljoen kostte, om veiligheidsproblemen met betrekking tot computers te bestuderen. Maar een functionaris van IBM vertelde Whiteside, dat totale veiligheid onbereikbaar is. Volgens hem kan een bedrijf alleen maar de kosten van het doorbreken van veiligheidsbarrières zo hoog maken, dat het niet de moeite waard is om het te proberen.

Toch blijf je na het lezen van dit boek sceptisch over de mogelijkheden van computerbeveiliging. Whiteside noemt twee gevallen waarin wachtwoorden (security passwords), ter beveiliging van het geheugen van de computer, door toedoen van ervaren programmeurs volkomen betekenisloos werden, nadat ze een leemte hadden ontdekt in het bedieningssysteem van de machine. En als je op deze manier een opening hebt gemaakt, is het makkelijk genoeg om aan de computer programma's te ontlokken, de stamlijst van geheime wachtwoorden, kortom bijna alle andere opgeslagen informatie.

Zoals te verwachten was, is dit een bijzonder groot probleem voor instellingen die gebruik maken van computers met gegevens die betrekking hebben op de nationale veiligheid. Bij een oefening die werd gehouden om te bepalen hoe goed een computer bij de Luchtmacht beveiligd was, bleken twee beveiligingsadviseurs in staat om het bedieningssysteem binnen twee uur te kunnen infiltreren. Ze hadden genoeg aan hun ruime ervaring en een keyboard-terminal, die gekoppeld was aan een gewone telefoon. Als de terminal bijvoorbeeld verbonden was geweest met een telefoontoestel in

Moskou, hadden de mannen de computer op precies dezelfde manier kunnen kraken. Het enige nadeel van dit bijzonder leesbare en informatieve boek is, dat een groot gedeelte al verschenen is in The New Yorker Magazine (waar Whiteside als staff writer aan verbonden is) en dat veel gevallen al eerder beschreven zijn door Donn B. Parker in zijn boek "Crime by Computer". Maar alles wijst erop, dat de computers "are here to stay". En gezien het feit, dat de opbrengsten groot en de risico's klein zijn in vergelijking met andere vormen van diefstal, wordt oplichterij per computer waarschijnlijk dé misdaadmode van de toekomst.

De Automatiseringsgids, 27 juli 1978 (gedeeltelijke weergave)

INTERMEZZO

Shoptalk

Ze zaten aan de bar in één van die betere gelegenheden, waar het licht gedempt, de achtergrondmuziek discreet en de slok prijzig is. Zakenlieden, zo te zien aan hun verzorgd uiterlijk, zelfverzekerd optreden en gemakkelijke gebaren. De één was nog jong, in een pijlsnel gesneden pak, de oudere gedistingeerd, iets grijzend aan de slapen.
"Kijk", hoorde ik de jongste zeggen, "Een modern manager kan niet zonder een eigen data processing system. Management information, vandaag de dag, is een must". Hij pakte zijn glas en nam een ferme teug. Zijn buurman luisterde belangstellend toe en knikte begrijpend.
"Een investment in computing facilities", zo vervolgde de eerste, "is een goede move. Neem nu bijvoorbeeld cost control: waar vloeien uw kosten naar toe". En in één teug ledigde hij zijn glas.
"Barman, mogen wij hier nog twee drinks?"
De conversatie zette zich voort en er waren nog één of twee rondjes doorgegaan, toen mijn aandacht getrokken werd door een schampere opmerking van de jongste van het stel. "Ach meneer, wat heet compatibel. Neem nu die hardware van Compufiel. Nothing sir, geen enkele upgrading facility, limited disk capacity ..., één storage module, no more." Met krachtige gebaren onderstreepte hij zijn woorden. "Modularity, meneer, da's essentieel. Modularity in hardware en software, met virtual memory en partitioning. Disk capacity voor data en programs, een source library en full object program library.
Een time sharing system met multi-programming facilities ... foreground en background processing ... dat is up to date zijn. Workstation met visual display units voor simultaneous data processing, direct memory access en multiplex channels voor pheripheral units. Optionals voor upgrading en expanding the system."
Het kwam er allemaal vlotjes uit en op het laatst werd hij zelf wat lyrisch ...
"Barman, de bill, want ik moet zien dat ik mijn plane nog haal."
Terwijl hij betaalde haalde hij uit zijn portefeuille ook nog een visitekaartje, dat hij zijn gesprekspartner met enige zwier overhandigde.
"Voor als u beslist ... je kunt immers nooit weten." Met een ferme handdruk nam hij afscheid en baande zich een weg naar de uitgang. De ander tuurde op het fraaie kaartje, waarbij zijn wenkbrauwen van verbazing omhoog gingen: Piet van Leus, Voorthuizen, Sales Representative. "Verrek, laat ik nu denken, dat het een Amerikaan was. Toch wel een goeie jongen."

Alternatief Automatiserings ABC, Nixdorf

Privacy

Sectie Postreclame

Onderzoek naar mening publiek over privacy

De Nederlandse Stichting voor Statistiek is begonnen met een onderzoek naar de rol van het begrip privacy in de relatie tussen het publiek en (postreclame)bedrijven die gebruik maken van adressenbestanden. Het onderzoek staat onder auspiciën van de sectie Postreclame & Sampling van het Genootschap voor Reclame.
Het NSS-werk is tweeledig. Aan de ene kant wordt het publiek ondervraagd en wordt bekeken hoe de opvattingen zijn over privacy en het gebruik van adressensystemen; wat denkt men dat met die adressen gebeurt. Tevens wordt de bekendheid gepeild van Antwoordnummer 666 Amsterdam - het adres voor verzoeken om schrapping uit adresbestanden.
De stichting pleegt daarnaast ook onderzoek in de (postreclame)branche zelf; hoe liggen de opvattingen rond privacy; wat is de aard van de bestanden; wat gebeurt ermee.
Met het onderzoek hoopt de sectie duidelijker zicht te krijgen op praktische knelpunten.
Een en ander gebeurt in het kader van de voorstellen die de zogenaamde Commissie Koopmans aan de regering heeft gedaan voor een wet op de persoonsregistratie. Ofschoon de regering Van Agt nog niet heeft laten weten wanneer een desbetreffend wetsvoorstel in de Tweede Kamer aan de orde komt, houdt men er in regeringskringen rekening mee, dat dit toch nog in 1979 zal gebeuren.

Informatiek, 24 oktober 1978

Informatie(f)

Washington, inventieve bureaucratie

De Amerikaanse regering was een van de eerste gebruikers van wordprocessing-apparatuur, wat geen verbazing hoeft te wekken, want de federale bureaucratie is een duidelijk voorbeeld van een "papierfabriek". Wel verbazend is het feit, dat Washington zich onderscheidt door enkele zeer inventieve toepassingen. Het tempo waarin Washington zijn burelen automatiseert ligt enorm hoog. Het Stanford Research Institute schat dat het aantal wordprocessors omstreeks 1980 gestegen zal zijn tot ongeveer 81.500 stuks, tegen 22.500 in 1973. Eén van de innovaties in Washington is het aan elkaar koppelen van systemen van wordprocessing-apparatuur. Het hoge niveau van de text editing typewriters die met elkaar kunnen "praten" weerspiegelt de behoefte van de bureaucratie aan snelle communicatiemogelijkheden. Dit soort systemen is nu in gebruik bij een heel scala van regeringsinstanties, variërend van de Library of Congress tot wervingsbureaus van de Marine. Het wordprocessing-systeem van de laatste instantie is een van de meest geavanceerde. Het bestaat uit een netwerk van 198 automatische schrijfmachines en 150 dicteerapparaten, verspreid

over 78 lokaties over het hele land, die allemaal in verbinding staan met het hoofdkwartier in Arlington. Het systeem kostte de Marine 1,5 miljoen dollar, maar het nieuwe netwerk betekent een jaarlijkse besparing van 4,6 miljoen dollar, voornamelijk op personeelskosten. Voorheen gebruikte de Marine Telecopiers voor het wederzijdse contact tussen hoofdkwartier en afzonderlijke lokaties. Deze facsimile-systemen deden zes minuten over het verzenden van een pagina via het telefoonnet. Het nieuwe systeem verzendt 12 pagina's in drie minuten, wat een drastische verlaging van telefoonkosten betekent.

Een ander voorbeeld van inventief gebruik van wordprocessors is het experimentele systeem van de Congressional Research Service, een tak van de Library of Congress. Hier komen dagelijks rond de 1.500 aanvragen om informatie binnen van congresleden en hun staf. Men gebruikte wel wordprocessors voor het conventionele "editen" van antwoorden op de verzoeken om informatie, maar de informatie zelf moet door ambtenaren worden opgegraven uit omvangrijke archieven. In het experimentele systeem is het archief nog wel de bron van informatie, maar wordt ieder rapport gepreparereerd door een wordprocessing-eenheid, en wordt de geprinte informatie niet alleen aan het congreslid verzonden, maar ook elektronisch doorgegeven aan een geautomatiseerde databank. Vervolgens kan de informatie weer opgeroepen worden en verwerkt in nieuwe rapporten, zonder dat men de conventionele archieven hoeft om te ploegen of steeds identiek typewerk te doen. Naarmate het elektronische archief groeit, zullen steeds meer rapporten afkomstig zijn van de databank. Er is een wet in de maak, die de General Services Administration het recht geeft regeringsinstanties te dwingen om wordprocessing-centra op te zetten, die alle correspondentie en het dicteerwerk zullen behandelen.

De Automatiseringsgids, 5 oktober 1978

DAP gaat robot besturen

De eerste "Distributed Array Processor" van ICL is verkocht aan het Queen Mary College van de Londense universiteit. Dit College verricht nogal wat technisch en wetenschappelijk onderzoek. Een van de meest in de publiciteit gekomen projecten is wel dat van de "denkende" robot, genaamd Junior. Bij dit project wordt de Distributed Array Processor, DAP, samen met een ICL 2980 ingezet.
Tot nu toe beschikt het Queen Mary College over een 1904-S computer van ICL.
De robot Junior moet zonder directe inmenging van de mens leren bewegen. Hij rijdt op drie wielen en bekijkt zijn omgeving via een televisiecamera. Z'n hersens zijn de ICL-computer, waar alle waarnemingen worden geanalyseerd en die Junior instrueert hoe hij obstakels uit de weg moet gaan en allerlei handelingen moet verrichten. Uiteraard heeft Junior geen enkel eigen initiatief. Zijn kennis, of liever die van de computer, moet worden gezocht in z'n geheugen, waarin alle eerdere ervaringen liggen opgeslagen.

Door vergelijking met en combinatie van die eerdere ervaringen kan Junior zijn beslissingen nemen over wat hij in een bepaalde situatie zal doen. De robot is radiotelegrafisch met de computerapparatuur verbonden. Robots zijn al langer bekend en zeker niet alleen in science fiction verhalen. Ze worden in bepaalde produktieprocessen toegepast. Die robots kunnen alleen bepaalde handelingen verrichten. Ze zijn niet in staat om onverwachte gebeurtenissen op te lossen. Robot Junior moet dit wel gaan doen, door van zijn eigen ervaringen te "leren". Junior leeft op elektriciteit, die in accu's is opgeslagen. Hij is al zo ver, dat hij zelfstandig een oplaadinstallatie opzoekt wanneer de spanning in de accu's beneden een bepaald niveau komt.

De Automatiseringsgids, 17 augustus 1978

Chequevervalsing

De reprotechniek staat voor niets. Dat vonden ook vele chequevervalsers in de Verenigde Staten. Zelfs de kleurenkopieermachine werd ingeschakeld om een eenvoudige cheque te vervalsen. Burroughs heeft nu voor deze reprografische vervalsingen een oplossing gevonden. Op de originele cheque is voor het oog onzichtbaar het woord "ongeldig" verborgen dat wel zichtbaar wordt zodra de cheque op welke manier dan ook reprografisch wordt gekopieerd. Niet dat hierdoor het vervalsen in een keer een halt wordt toegeroepen. Wel is zeker, dat vele "gelegenheidsvervalsers" een stop zullen merken in hun bijkomstig loon.

De Automatiseringsgids, 3 augustus 1978

Auditors Recommend EDP Documentation

During a review of the customer information system file maintenance area auditors noted that the only documentation for the control programs consisted of the programs themselves. And these were quite complicated. It was suggested to the Information Systems Department that a statement describing these control programs would not only be excellent documentation, but would provide a training tool for computer programmers. In addition, a copy of the test file, developed by our EDP audit staff, was turned over to Information Systems for its use in conducting independent tests of the system.

Los Angeles Chapter
The Internal Auditor, Oktober 1978

Geavanceerde 1100 Systems Monitor
Technische primeur voor Sperry Univac

Sperry Univac legde onlangs de laatste hand aan een nieuw monitorsysteem dat de prestaties van computers uit de 1100-serie op een groot aantal facetten nauwkeurig kan vaststellen. Het PDS-systeem, een afkorting van Performance Display System, meet niet alleen de verrichtingen van een 1100-systeem, maar geeft ook een beeld van de nog ongebruikte capaciteit en projecteert een en ander in kleur op een groot beeldscherm.
Op basis van de aldus verkregen gegevens, vooral bij het uitvoeren van een benchmark bewijst dit systeem zijn waarde, kan de ingezette 1100-configuratie worden beoordeeld en zonodig gewijzigd om een betere aanpassing aan de behoeften van de gebruiker te verkrijgen.
Er zijn momenteel twee van deze systemen die uniek zijn in de computerindustrie in gebruik. Eén bij Sperry Univac in Roseville, Minnesota USA, en één bij het Benchmark Centre van Sperry Univac's International Division in Londen.
Het meten en de daaruit voortvloeiende rapportering (in kleur via de beeldschermen en via printlijsten) strekt zich uit over de uit te voeren gebruikersprogramma's, het besturingsprogramma, de invoer/uitvoeractiviteiten en statistische gegevens omtrent volbrachte jobs. Hiertoe worden een aantal parameters ingevoerd, die zowel op apparatuur als op programmatuur betrekking hebben.
De parameters voor gebruikersprogramma's en het besturingsprogramma worden op het scherm zichtbaar gemaakt als een percentage van de beschikbare resources op een verticale as, terwijl op de horizontale as de tijd wordt aangegeven. De tijdbasis kan naar behoefte worden veranderd, zodat de gegevens op het scherm naar keuze betrekking hebben op enkele minuten dan dan wel meerdere uren.
De statistieken omtrent de jobs (aantal uitgevoerde jobs, aantal jobs in de wachtrij, enz.) worden in numerieke waarden uitgedrukt, terwijl de invoer/uitvoeractiviteiten per I/O-kanaal in een grafiek worden weergegeven. Naar wens kunnen daarnaast bijvoorbeeld het geheugengebruik of de prestaties van periferie-apparaten elk apart worden gevolgd.
PDS houdt voortdurend twee verschillende gegevensverzamelingen bij, de "Total History Mode", die de gehele verslagperiode bestrijkt en de "Instant Display Mode", die uitgaat van de variabele tijdschaal, in de praktijk doorgaans een periode van twee tot tien minuten. Hierdoor kunnen ook gegegevens uit een eerdere periode worden opgehaald en op het scherm worden gebracht, onder het gelijktijdig aanpassen van de tijdschaal naar behoefte.
Alle gemeten gegevens worden steeds volledig vastgelegd op band- en schijvengeheugens, zodat men later desgewenst offline het gehele verloop nog eens kan nagaan. De projectie kan ook op ieder moment worden "bevroren" en tevens kunnen afdrukken hiervan op papier worden verkregen.
Voorts is het computercentrum ook nog uitgerust met video-apparatuur voor opname en weergave, benevens een filmprojector, die vooral bij demonstraties en seminars uitstekende hulpmiddelen zijn.
Het hart van het PDS wordt gevormd door een Sperry Univac DCP (Distributed Communications Processor), die optreedt als besturingssubsysteem en een Data Monitoring Module met tape/disk-subsysteem, waarvandaan meer dan 300 sensoren per centrale verwerkingseenheid naar de "gastheer"-computer worden geleid.

De Automatiseringsgids, 27 juli 1978

Voorzetscherm neemt reflectie bij beelschermeenheden weg

Optical Coating Laboratoy Incorporated (OCLI) uit Santa Rosa in de Amerikaanse staat Californië heeft goed nieuws voor de Nederlandse FNV. Men ontwikkelde daar namelijk onder meer voor de ruimtevaart een voorzetscherm, dat reflectie van beeldschermen moet wegnemen. Deze voorzetschermen, die hier nu door Koning en Hartman op de markt worden gebracht, zijn voorzien van een anti-reflectielaag met polarisatiefilter en kunnen op bestaande beeldschermapparatuur worden aangebracht. Het scherm is verstelbaar, zodat elke gebruiker zelf de geschiktste beeldkwaliteit kan bewerkstelligen. Volgens de leverancier wordt bij gebruik van het voorzetscherm bovendien de hoek, waaronder de scherminformatie nog goed leesbaar is, vergroot. Verder zijn er een aantal kleurfilters verkrijgbaar, waarmee de tekens op het scherm in een andere kleur kunnen worden afgelezen. Het glazen voorzetscherm en de daarop aangebrachte laag zijn vrijwel even hard, hetgeen volgens Koning en Hartman de optische eigenschappen voor enkele jaren garandeert. De fabrikant van onder meer grafische beeldschermeenheden Tektronix gaat binnenkort deze apparatuur standaard met de OCLI-ruiten uitrusten. Misschien de Nederlandse vakbonden ook?

Computable, 8 september 1978

(Zie hiervoor ook het artikel in Compact voorjaar 1978: "Beeldscherm fel omstreden".)

"Flubble" biedt in toekomst kans voor hybride geheugens

Op de onlangs in Californië gehouden Western Electronic Show & Convention introduceerde een medewerker van Shugart, fabrikant van flexibele schijven en aanverwante apparatuur, een nieuw begrip: de "flublle". De man in kwestie, George Sollman, duidde hiermee op een gecombineerd flexibel schijf- en bellengeheugen.
Het bellen- of "bubble" geheugen moet hierbij dienen als buffer voor de flexibele schijf, waarin alvast die informatie wordt opgeslagen, die het computersysteem naar alle waarschijnlijkheid het eerst nodig zal hebben. Deze hybride geheugentechniek, waarbij hetzelfde principe als bij het "cache memory" wordt toegepast, zou de doorvoersnelheid aanzienlijk kunnen verhogen.

Computable, 6 oktober 1978

Coffee, $ 39,000 per cup

A person or persons unknown brought a cup of coffee into the computer room of the Los Angeles Times. Accidentally, the cup was overturned and its contents were spilled into an IBM 370/158. Costs to repair the damage amounted to $ 39,000. Item for internal control checklists: "Are all food and drink banned from the computer room?" A "no" answer should result in an audit comment!

Edpacs, juli 1978

DATA PROCESSING CRIMES

door A.W. Neisingh

Het navolgende artikel is een bewerking van een in EDPACS van januari 1978 verschenen artikel van de hand van Chris de Gouw. In het artikel tracht De Gouw antwoord te geven op de volgende vragen:

- Wat is een data processing crime.
- Welke soorten data processing crimes zijn er en wat is de doelstelling van die misdaad.
- Wie pleegt deze misdaden.
- Hoe worden data processing crimes gepleegd.
- Hoe kunnen deze misdaden worden voorkomen en opgespoord.

Begripsbepaling is gewenst, zodat schrijver dan ook start met een definitie van een data processing crime, te weten: "Any act which involves and is designed to cause loss or damage or in any way defraud the company or its customers through the use or manipulation of the data processing system". Naar mijn mening terecht concludeert De Gouw, dat deze definitie toch wel te beperkt is, omdat ook zaken als het ongeautoriseerd gebruik van gegevens verwerkt door de computer onder de data processing crime gerangschikt dienen te worden.

Men kan zich afvragen waarom nu ineens zoveel literatuur verschijnt waarin over deze misdrijven wordt gesproken. De geautomatiseerde gegevensverwerking is van grote betekenis voor het reilen en zeilen van een steeds grotere groep ondernemingen en is kwetsbaar omdat zeer veel informatie, zij het in niet direct voor de mens leesbare vorm, (veelal) op één plaats binnen die onderneming aanwezig is.
Daarnaast dienen wij ons te realiseren, dat het signaleren van de voorbereidingen van dergelijke misdaden weliswaar mogelijk is, doch het verkrijgen van bewijs tegen de daders geen sinecure is. Wel kunnen wij het de potentiële misdadiger moeilijk maken, waarover straks méér.

Uw commentator heeft geprobeerd het verhaal van De Gouw aangevuld met eigen op- en aanmerkingen in een matrix weer te geven.
De onderscheiding tussen personal gain crimes en destructive crimes, die in het oorspronkelijke artikel wordt aangehouden, loopt door de matrix heen. De problemen, die kunnen ontstaan door manipulatie met cheques (door computer ondertekend en dergelijke), zijn niet overgenomen, omdat deze problematiek in Nederland nauwelijks leeft.

In de navolgende matrix zijn antwoorden op een aantal door De Gouw geformuleerde vragen gegeven; echter bedacht dient te worden, dat de aangegeven preventieve maatregelen dienen te zijn verankerd in een stelsel van maatregelen van interne controle en beveiliging.

COMPUTER ABUSE	Schade voor het bedrijf
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")
b. Gebruik aanwezige programmatuur voor eigen doeleinden	. daaraan verbonden kosten . afdrukken van (eventueel geheime) bedrijfsgegevens
c. Verwerken eigen programma's om bedrijfsgegevens t.b.v. derden af te drukken (bedrijfsspionage)	. daaraan verbonden kosten . aantasting privacy . concurrentie-vervalsing . andere vormen van schade door bekend worden van niet voor derden bestemde gegevens
2. Manipulaties met resp. ongeautoriseerd gebruik van gegevens, besturingssysteem, programma's en formulieren	. fraude (omvang niet te bepalen) . niet meer juist functioneren van de programmatuur . verstrekken van onjuiste gegevens . werken met verminkte bestanden . verloren gaan van beveiligingskopieën . verlies van "voorsprong" . claims in kader van privacywetgeving
3. Moedwillige vernieling, diefstal	
a. Apparatuur	. materiële schade . stilstand informatieverwerking
b. Informatiedragers	. materiële schade . verlies bestanden . verlies programmatuur . stilstand informatieverwerking
4. Beïnvloeden van de goede werking van de apparatuur	. vertraging/verstoring van de gegevensverwerking
5. Datacommunicatie	. zie 1. en 2. . fraude . verlies bestanden resp. gegevens . verlies programmatuur

Preventieve maatregelen	Controlemiddelen
. motivatie van personeel . procedures m.b.t. planning en werkvoorbereiding, voortgangscontrole . catalogued jobstreams	. job accounting . console log . afdrukken programmabibliotheek . outputcontrole, ook op testwerk
. twee operators per shift . speciale beveiliging van geheime en vertrouwelijke gegevens	. beoordelen console en accounting
. procedures m.b.t. uitgifte van bestanden . afhaalsysteem voor output . datacommunicatiesystemen beveiligen met toegangscontrole . functiescheiding óók buiten normale werktijden . antecedentenonderzoek	. oogcontrole door leiding
. motivatie van personeel . antecedentenonderzoek . altijd twee operators in computercentrum . geen systeem- en programmadocumentatie onder bereik van operating . gebruik maken van beveiligingsmaatregelen die door bibliotheekpakketten worden geboden . bewaring gescheiden van operating . kopieën aanhouden . strikte procedure m.b.t. programmawijzigingen	. scheduling . bestandscontrolemethodieken . periodieke programmatests; eventueel cross reference
. motivatie van personeel . reconstructiemogelijkheden . bewaarder informatiedragers als aparte functie	. inventarisatie . review-activiteiten
. uitwijkmogelijkheid . opberging bestanden . administratie . tijdens ontslagperiode niet zonder meer op computercentrum toelaten . betrouwbaarheid operators . toegangsbeveiliging . closed shop . alarm . controle op inhoud van bestanden	
. motivatie van personeel	
. motivatie van personeel . toegangscontrole (identificatie, autorisatie, audit trail) . vercijferen van informatie	. oogcontrole bij terminals . beoordelen logging en accounting

Wie pleegt data processing crimes?
Een aantal groepen personen wordt achtereenvolgens onder de loep genomen, zoals ontevreden personeelsleden, personen, die de geautomatiseerde gegevensverwerking als een uitdaging zien en personeelsleden met persoonlijke moeilijkheden. Waarom hij de "gelegenheidsdief" niet noemt, is niet duidelijk.
Wij menen, dat door een samenloop van omstandigheden (leemten in de interne organisatie en de interne controle) nog al eens een fraude wordt gepleegd, waaraan overigens veelal om uiteenlopende redenen geen ruchtbaarheid wordt gegeven.
(Of De Gouw's suggestie op confidentiële basiservaringen inzake data processing crimes uit te wisselen veel navolging zal vinden, betwijfelen wij dan ook.)
Naast de catagorie personeel worden verder nog genoemd de ontevreden cliënten, de beroepsmisdaad en politiek gemotiveerde lieden.

N.B.: Het toeval (??) wil, dat in hetzelfde nummer van EDPACS een tweetal data processing crimes worden besproken, te weten:

1. fraude met behulp van de computer op een hondenrenbaan in Florida; buit $ 1 miljoen in circa vijf jaar;
2. aanslagen op tenminste tien computercentra in een periode van tien maanden door de Italiaanse "Communist Combat Unit". De omvang van de schade is niet bekend, echter gesproken wordt over gemiddeld $ 1 miljoen per centrum.

Hoe worden data processing crimes gepleegd, hoe kunnen ze worden voorkomen en opgespoord? Als we dat eens wisten! De onderscheiding tussen personal gaim crimes en destructive crimes volgend, kunnen wij trachten een analyse te maken van de gedragingen van de potentiële misdadiger. Degene, die een computerfraude zal willen plegen gericht op het behalen van persoonlijk voordeel, zal uiteraard onontdekt willen blijven.
Dit betekent, dat de manipulaties verborgen moeten worden (in programmatuur), dan wel dat zijn doen en laten met behulp van dezelfde computer moet worden uitgewist. De mogelijkheden zijn in ruime mate voorhanden.
Om de gedachten te bepalen:

- Na de manipulatie kan een programma worden verwerkt, dat alle sporen van de ongeoorloofde actie uitwist.
- Gebruik maken van foutafhandelingsprocedures, waarin controles ofwel ontbreken of zwakker zijn dan in de normale procedure.
- Het verschaffen van inside information inzake transporten e.d.

Het kan ook geld opleveren wanneer programmatuur en/of gegevens worden gestolen (dit is het onrechtmatig kopiëren van - delen van - de programmabibliotheek of van gegevensverzamelingen, het meenemen van een afdruk van programmatuur e.d.).

Voorkomen van deze data processing misdaden is in een aantal gevallen moeilijk, doch tot op zekere hoogte mogelijk door het invoeren en naleven van een samenstel van maatregelen van interne controle en beveiliging.

Het vernietigen van computercentra is in het algemeen eenvoudiger dan het plegen van fraude, omdat vele kritische plaatsen in het gehele traject van de geautomatiseerde gegevensverwerking onvoldoende beveiligd zijn tegen vernietiging.
Opgemerkt wordt, dat met relatief eenvoudige organisatorische (en technische) middelen, het strikt naleven van op beveiliging gerichte procedures en voorschriften een aanvaardbaar niveau van beveiliging kan worden verkregen.

In de matrix is onder het hoofd "controlemiddelen" aangegeven op welke wijze respectievelijk met behulp van welke middelen, opsporing van "onregelmatigheden" mogelijk zou moeten zijn. Er is echter geen sprake van een limitatieve oplossing.

Naast de vanuit accountantsoogpunt normaal te achten maatregelen van interne controle en beveiliging in de automatiseringsorganisatie, geeft De Gouw een aantal suggesties ter voorkoming van data processing crimes waarmee wij toch enige moeite hebben:

- Personeelsleden, die de computer als een uitdaging zien, zouden periodiek hun lusten mogen botvieren ("on a controlled basis" periodiek de beschikking kunnen krijgen over enige computertijd).
- Personeelsleden met financiële moeilijkheden zouden regelmatig aan kredietwaardigheidsonderzoekingen moeten worden onderworpen.

Tot slot een behartenswaardige opmerking:

"EDP has nog changed the company's basic concern about crime, but innovative measures must be employed to guard against these new data processing crimes."

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

LITERATUUROVERZICHT

door B.M. de Vries

In de A.C.-bibliotheek opgenomen boeken

AC 182 Operating System Structures to Support Security and Reliable Software 8 - 76 - Theodore A. Linden (Engels, 45 blz.)
Publikatie National Bureau of Standards B 31

Security has become an important and challenging goal in the design of computer systems. This survey focuses on two system structuring concepts that support security; namely, small protection domains and extended-type objects. These two concepts are especially promising because they also support reliable software by encouraging and enforcing highly modular software structures, in both systems software and in application programs. Small protection domains allow each subunit or module of a program to be executed in a restricted environment that can prevent unanticipated or undesirable actions by that module. Extended-type objects provide a vehicle for data abstraction by allowing objects of new types to be manipulated in terms of operations that are natural for these objects. This provides a way to extend system protection features so that protection can be enforced in terms of applications-oriented operations on objects. This survey also explains one approach toward implementing these concepts thoroughly and efficiently; an approach based on the concept of capabilities incorporated into the addressing structure of the computer. Capability-based addressing is seen as a practical way to support future requirements for security and reliable software without sacrificing requirements for performance, flexibility, and sharing.

AC 180 Audit and evaluation of computer security - Z.G. Ruthberg en R.G. McKenzie (Engels, 200 blz.)
Publikatie National Bureau of Standards, maart 1977 E 10
B 40

The National Bureau of Standards, with the support of the U.S. General Accounting Office, sponsored an invitational workshop on "Audit and Evaluation of Computer Security", held in Miami Beach, Florida on March 22 - 24, 1977. Its purpose was to explore the state-of-the-art in this area and define appropriate subjects for future research. Leading experts in the audit and computer communities were invited to discuss the subject in one of ten sessions, each of which considered a different aspect. A consensus report was produced by each of the ten sessions and these reports form the body of these Proceedings.
The ten topics reported on are: Internal Audit Standards, Qualifications and Training, Security Administration, Audit Considerations in Various System Environments, Administrative and Physical Controls, Program Integrity, Data Integrity, Communications, Post-Processing Audit Tools and Techniques, and Interactive Audit Tools and Techniques.

AC 181 Features of seven audit software packages: Principles and Capabilities - J. Neumann (Engels 51 blz.)
Publikatie National Bureau of Standards, juli 1977 D 10

Deze publikatie geeft een overzicht van de eigenschappen en kenmerken van 7 bestaande en belangrijke audit software packages. De audit software packages zijn:

1. Auditape, Haskins & Sells C.P.A.'s
2. Dyl 260, Dylakor Software Systems. Inc.
3. Easytrieve, Pansophic Systems, Inc.
4. EDP-Auditor, Cullinane Corporation
5. Hewcas, Health, Education and Welfare Computer Audit System, Department of Health, Education and Welfare Audit Agency
6. Mark IV/Auditor, Informatics, Inc. System Products
7. Score, Programming Methods Company of Informatics, Inc.

Vele aspecten van de audit software packages worden behandeld, waaronder:

- "input file" kenmerken,
- geschiedenis,
- beschikbaarheid en kostprijs,
- algemene systeemkarakteristieken,
- basisfuncties,
- specifieke controlefuncties,
- wijze waarop het package wordt gebruikt,
- vereiste computerconfiguratie.

De publikatie geeft een goed beeld van de mogelijkheden en van de beperkingen van de audit software packages. Voor de controle van geautomatiseerde informatiesystemen bevat het boek derhalve nuttige informatie.

AC 179 Computer Security and the Data Encryption Standard - D.K. Branstad (Engels, 125 blz.)
Publikatie National Bureau of Standards, februari 1978 B 40

These proceedings include papers or summaries of presentations of the fifteen speakers who participated in the Conference on Computer Security and Data Encryption Standard held at the National Bureau of Standards on February 15, 1977. Representatives from Federal agencies and private industry presented technical information and guidance with respect to computer security and the Data Encryption Standard. Subject of the papers and presentations include physical security, risk assessment software security, computer network security, applications and implementation of the Data Encryption Standard.
The questions raised at the conference and their answers are included in the proceedings.

Uit de tijdschriftenliteratuur

Automated logical data base design: concepts and applications -
N. Raver en G.U. Hubbard
Informatie (juni 1978) O 133

This paper describes the design effort for an integrated data base and then develops techniques for automating significant portions of labour. These techniques have been incorporated in a program to provide an effective data base design tool (Data Base Design Aid) in current use. The processes involved with this aid are discussed.

The SAC Study - H.E. Hardie
C.A. Magazine (maart 1978) - S 164

Hugh E. Hardie, auteur van de CICA computer control cursus, bespreekt het rapport "Systems Auditability and Control" (SAC) van het Institute of Internal Auditors. Het SAC-rapport bestaat uit de volgende onderdelen:

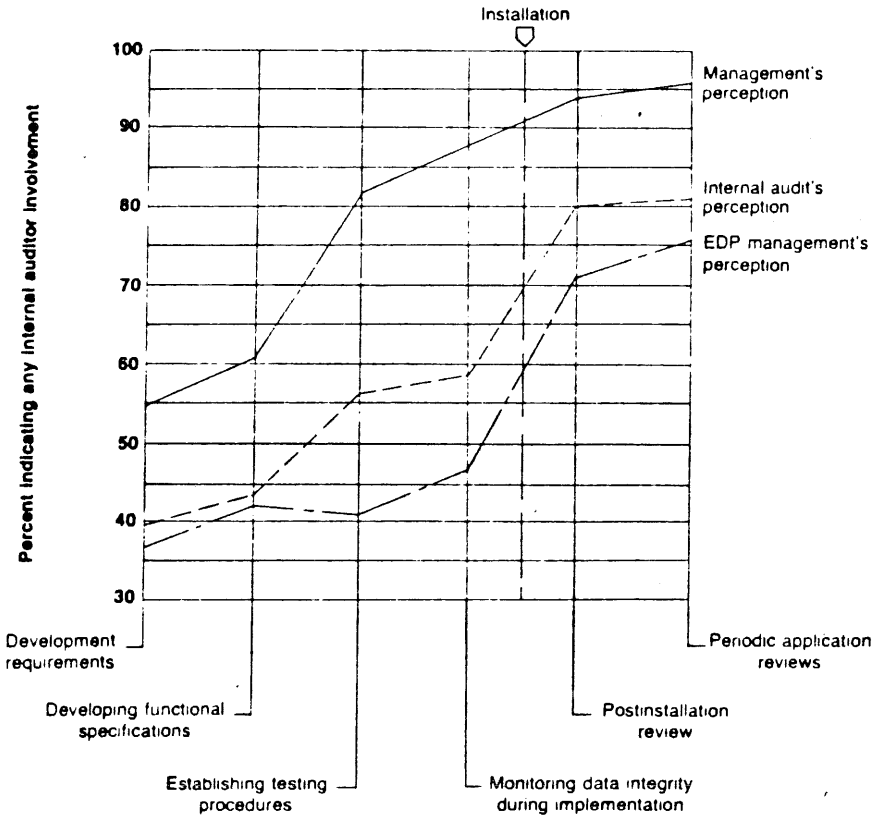
- Executive Report: "Exclusively prepared for executive management".
- Data Processing Control Practices Report: "This report presents information relating to control techniques applicable to computer-based information systems, computer service center operations, and the information systems development process".
- Data Processing Audit Practices Report: "This report presents information relating to auditing in the data processing environment".

Hardie maakt bij het SAC-rapport de volgende kanttekeningen:

- In het rapport wordt geen melding gemaakt van bestaande publikaties, die richtlijnen bevatten voor de interne en externe controle van geautomatiseerde systemen. Hardie wijst in dit verband op het bestaan van de publikaties van het CICA Computer Control and Audit Guidelines en van het boek Computer Control and Audit, geschreven door Mair, Wood en Davis.
- Figuur 3 van het Executive Report (blz. 13) geeft aan, dat de leiding de betrokkenheid van de interne accountant bij de systeemontwikkeling groter veronderstelt dan de interne accountant zelf. Hardie verbindt hieraan de conclusie, dat de interne accountant eerst dient vast te stellen, wat de leiding van hem verwacht.

Figuur 3 in Executive Report (blz. 13)

Internal Audit involvement

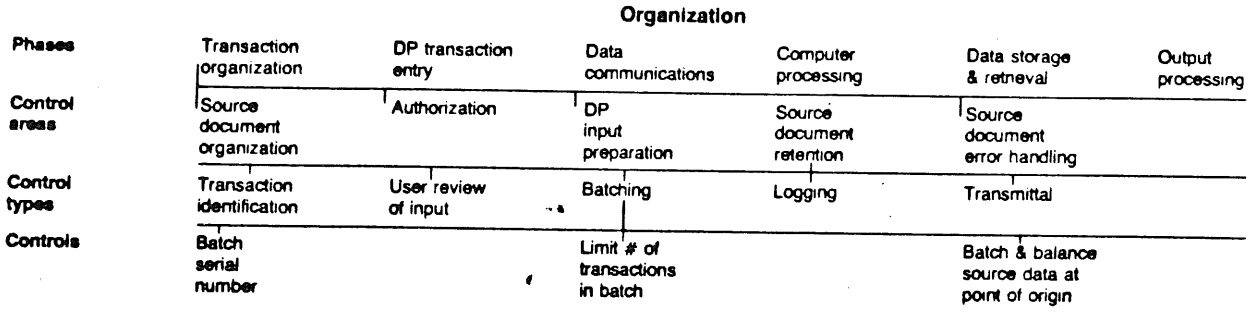


- In hoofdstuk 4 van het Control Practices Report (blz. 40 en 41) wordt het volgende vermeld:

  "Although an increasing number of internal auditors are using the computer to assist them, many are still only auditing around data processing. These auditors are ignoring the controls within application programs, believing that if processing results are verified, application controls must be effective".

  Volgens Hardie is deze interpretatie onjuist. De accountant, die de volledigheid en juistheid van de resultaten van het gegevensverwerkend proces verifieert, ignoreert de binnen het geautomatiseerde systeem opgenomen controlemaatregelen niet. Hij toetst ze op indirecte wijze. Of deze interpretatie op haar beurt de juiste is, lijkt mij aan twijfel onderhevig.

- Deel II van het Control Practices Report bevat een opsomming van de controles, die in de opeenvolgende fasen van de gegevensverwerking kunnen worden toegepast (zie onderstaand figuur).



In het rapport wordt echter de controledoelstelling voor iedere fase van de gegevensverwerking niet aangegeven.

- Hoofdstuk 11 Computer Service Center Controls en Hoofdstuk 12 Application System Development Controls van het Control Practices Report bieden weinig nieuws, behalve de behandeling van het onderwerp gestructureerd programmeren.

- Volgens Hardie zijn in sommige flowcharts bekende symbolen op ongebruikelijke wijze toegepast, hetgeen tot verwarring leidt.

- Het Audit Practices Report geeft op overzichtelijke wijze een overzicht van bestaande EDP-audittechnieken.

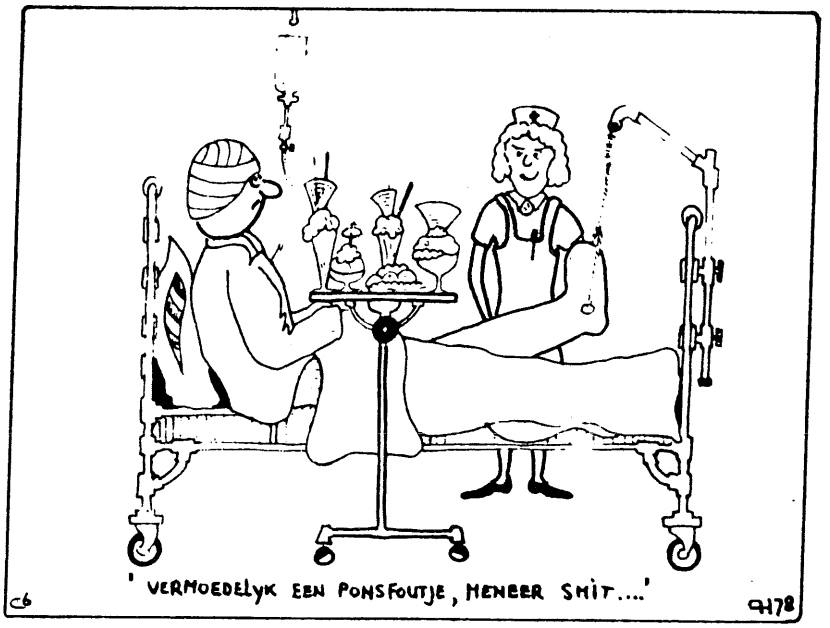
Hardie besluit zijn artikel met de volgende woorden:

"Of course, now that we have a study of what people are really doing, it would be useful to go back to the conceptual framework delineated in Computer Control Guidelines and see if what people are doing fits in that framework. If some items do not, perhaps the framework now needs expansion; if part of the framework is never used, perhaps it is redundant.

Recovery Techniques for Data Base Systems - J.S.M. Verhofstad
Computing Surveys (juni 1978) - S 202

A survey of techniques and tools used in filing systems, data base systems and operating systems for recovery, backing out, restart, the maintainance of consistency, and for the provision of crash resistance is given. A particular view on the use of recovery techniques in a data base system and a categorization of different kinds of recovery and recovery techniques and basic principles are presented. The purposes for which these

recovery techniques can be used are described. Each recovery technique is illustrated by examples of its application in existing systems described in the literature.
A main conclusion from this survey is that the recovery techniques described are all useful; they are applied for different purposes and in different environments. However, a certain trend in the increasing use of specific techniques during the past few years can be noted. Another main conclusion is that there are still enormous integrity and recovery problems to be solved for parallel processes and distributed processing.



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