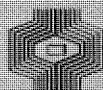


compact

COMPUTER EN ACCOUNTANT

- DE ZEEFMETHODE ALS SELECTIEMETHODE
VOOR STATISTISCHE STEEKPROEVEN IN
DE CONTROLEPRAKTIJK (II) 2
- PRIVACY-WETGEVING 14
- DE NABIJE TOEKOMST VAN COMPUTERGEBRUIK 18
- ABC-NIEUWS 23
- LITERATUUROVERZICHT 38



Klynveld Kraayenhof & co
ACCOUNTANTS

NUMMER 16

5E JAARGANG

WINTER 1979

VAN DE REDACTIE

Het winternummer 1979 dat U voor U heeft, bevat een keur aan artikelen:

- C. Rietveld vervolgt zijn artikel inzake de zeefmethode met een tweetal afleveringen;
- A.W. Neisingh en J.F.C. van Epen starten met een serie artikelen onder de kop "Privacy-wetgeving", terwijl
- de nabije toekomst van computergebruik wordt besproken door H. Roos naar aanleiding van publikaties in EDP-Analyzer.

Tot slot wijzen wij U op het ABC-Nieuws, waarin deze keer uitgebreid aandacht wordt besteed aan het onderwerp "gebruikersdocumentatie".

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. Philippon
en D. Steeman.

Adres: Pr. Irenestraat 59 Amsterdam

DE ZEEFMETHODE ALS SELECTIEMETHODE VOOR STATISTISCHE STEEKPROEVEN IN DE
CONTROLEPRAKTIJK (II en III)

door C. Rietveld

Inleiding

In mijn eerste artikel, verschenen in nummer 15 van Compact, heb ik de algemene principes van de zeefmethode uiteengezet¹⁾. Dit artikel besloot ik met de toetsing van de zeefmethode aan een tweetal andere methoden. Als praktisch verschil noemde ik de grotere flexibiliteit en het grotere toepasbaarheidsbereik van de zeefmethode, welke eigenschappen vooral tot hun recht komen bij de toepassing van zeefgrenzen.

Voorts kan de toepassing van subselectietechnieken een verdere bijdrage vormen voor efficiënte selectieprocedures op basis van de zeefmethode.

In hoofdstuk II bespreek ik de zeefgrenzen. Daarna komen in hoofdstuk III de subselectietechnieken aan de orde.

II SELECTIE EN EVALUATIE OP BASIS VAN ZEEFGRENZEN

1. Ten behoeve van de lezer worden hieronder de in dit hoofdstuk gehanteerde aanduidingen gerecapituleerd en binnen een kader geplaatst.

T	=	totaalbedrag der verantwoording
m	=	vooraf bepaalde steekproefomvang
n	=	aantal in feite geselecteerde, te controleren posten
p	=	bovengrens van de fractie fouten in de verantwoording
P	=	bepaalde post, alsmede bedrag van die post
F	=	grootte van fout in post P
M	=	zeefmaximum voor een steekproefomvang m (T/m)
a	=	a-select getal voor post P
Z	=	zeefgetal voor post P en een steekproefomvang m (M x a)
X	=	zeefgrensmaximum voor post P (T/P)
G	=	zeefgrens voor post P (X * a)

¹⁾ In het eerste artikel komt op pagina 4, regel 12, een storende fout voor. De tweede reeks cijfers 1, 3 en 6 dient gewijzigd te worden in 2, 4 en 5.

2. Wat zijn zeefgrenzen?

De toepassing van zeefgrenzen wil ik uiteenzetten aan de hand van het in mijn vorig artikel op pagina's 4 en 5 gegeven voorbeeld, dat ik hieronder in het kort memoreer.

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% (dit is 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 met toepassing van de tabel op basis van de Poisson-verdeling de steekproefomvang op 230 (4,6 : 0,02) bepaald.

Het zeefmaximum (M) wordt berekend door de deling:

$$\begin{aligned} & - \text{verantwoordingstotaal/steekproefomvang} \\ & \qquad \qquad \qquad T/m \\ & \qquad \qquad \qquad 11,5 \text{ mln.}/230 = 50.000 \end{aligned}$$

Uit een nader uitgewerkt voorbeeld met betrekking tot een aantal posten van deze verantwoording blijkt de wijze waarop de zeefprocedure plaatsvindt.

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

Het zeefgetal (Z) is voor post 5 als volgt berekend:

$$\begin{aligned} & - \text{zeefmaximum} * \text{a-select getal} \\ & \qquad \qquad \qquad T/m * a \\ & \text{d.i. } 50.000 * 0.08035 = 4.017 \text{ (afrondding naar beneden)} \end{aligned}$$

De waarde van post 5 (f 2.570) is kleiner dan het zeefgetal 4.017 (P < Z); de post wordt derhalve niet geselecteerd.

Bij een steekproefomvang van 460 is voor post 5:

$$\begin{aligned} & - \text{het zeefmaximum (M)} : T/m = 11,5 \text{ mln.}/460 = 25.000 \\ & - \text{het zeefgetal (Z)} : M * a = 25.000 * 0,08035 = 2.008. \end{aligned}$$

De waarde van de post (f 2.570) is groter dan het zeefgetal 2.008 (P > Z); de post wordt nu wel geselecteerd.

Uitgaande van de oorspronkelijke steekproefomvang van 230 zal bij toeneming van die omvang het zeefgetal dalen totdat het bij een bepaalde steekproefomvang een grenswaarde zal bereiken, die gelijk is aan de grootte van de post (f 2.570) dan wel deze grootte zal benaderen. De steekproefomvang noemen wij de zeefgrens (G), dit is de grens in de steekproefomvang, waarbij de post nog net niet geselecteerd wordt. Elke grotere steekproefomvang leidt tot een zeefgetal kleiner dan de waarde van de post en derhalve tot selectie van die post.

Ter illustratie wordt de selectieprocedure voor post 5 van ons voorbeeld ad f 2.570 in een tabel nader uitgewerkt.

Steekproefomvang (m)	Zeefmaximum (M = T/m)	Zeefgetallen (Z = M * a)	Post te controleren? (P = 2.570 > Z?)
230	50.000	4.017	neen
345	33.333	2.678	neen
358	32.122	2.581	neen
359 = G	32.033	2.573	neen
360	31.944	2.566	ja
460	25.000	2.008	ja

Post 5 wordt geselecteerd, als de waarde van de post (2.570) groter is dan het zeefgetal berekend met het a-select getal 0,08035 ($P > Z$). Aan deze voorwaarde wordt steeds voldaan als ook de steekproefomvang groter is dan de zeefgrens 359 ($m > 359$). Daarentegen wordt post 5 niet geselecteerd als de waarde van de post gelijk is aan c.q. kleiner is dan het zeefgetal ($P \leq Z$). Dit is het geval als ook de steekproefomvang gelijk is aan dan wel kleiner is dan de zeefgrens 359 ($M \leq 359$).

Hoe berekenen wij deze zeefgrens?

Zoals gesteld, is bij een steekproefomvang (m) gelijk aan de zeefgrens (G) het zeefgetal (Z) (nagenoeg) gelijk aan de grootte van de post.

Voor post 5 derhalve:

$$2.570 = 11,5 \text{ mln.} / G * 0,08035$$

$$P = T/G * a$$

Derhalve

$$G = 11,5 \text{ mln.} / 2.570 * 0,08035$$

$$G = T/P * a$$

$$= 4.474 * 0,08035$$

$$= X * a$$

$$= 359 \text{ (naar beneden afgerond).}$$

Het getal 4.474 is het zeefgrensmaximum (X), waarop ik hierna nog terugkom.

Uit het voorgaande vloeit voort, dat de toetsing

- post > zeefgetal? $P > T/m * a (= Z)?$
- vervangen kan worden door: $m/P * P > T/m * a * m/P?$
- steekproefomvang > zeefgrens? $m > T/P * a (= G)?$
- of
- zeefgrens < steekproefomvang? $G < m?$

Tevens blijkt dat de zeefgrens uit het zeefgetal kan worden afgeleid door de berekening:

- steekproefomvang/postgrootte * zeefgetal $G = m/P * Z$

Het nieuwe toetsingscriterium

- zeefgrens < steekproefomvang? $G < m?$

passen wij nu toe op het voorbeeld op pag. 3, waarbij de steekproefomvang (m) 230 is, en het zeefmaximum (M) derhalve 11,5 mln. : 230 of 50.000.

Nrs.	A-select getal (a)	Posten (P)	Zeefgrens- maximum ') (X = T/P)	Zeefgrens (G = X * a)	Post te controleren? (G < m = 230)?
1	0,22683	3.780	3.042	690	neen
2	0,66041	14.720	781	515	neen
3	0,00846	1.150	10.000	84	ja
4	0,65429	7.715	1.490	975	neen
5	0,08035	2.570	4.474	359	neen
6	0,77440	56.230	204	158	ja

') Het zeefgrensmaximum is in de berekening van de zeefgrens niet afgerond.

De conclusies zijn, zoals te verwachten viel, gelijk aan die bij de hantering van zeefgetallen (zie tabel op pag. 4).

Vragen wij ons af, hoe de conclusies zouden luiden bij een steekproefomvang van 460, dan moet bij selectie op basis van zeefgetallen een herrekening plaatsvinden van de zeefgetallen en derhalve een nieuwe tabel worden samengesteld. Uit deze tabel zal blijken dat post 5 nu ook wordt geselecteerd (zie pag. 3).

Bij de hantering van zeefgrenzen als toetsingscriterium kan de tabel voor een steekproefomvang van 230 zonder enige herrekening ook voor een omvang van 460 worden gebruikt. Toetsing van m (= nu 460) met de zeefgrenzen leidt uiteraard wel tot andere conclusies. Post 5 moet nu ook worden gecontroleerd, conform de conclusies bij toetsing met zeefgrenzen.

De toetsing op basis van zeefgrenzen is eenvoudiger, omdat per post slechts één variabele (zeefgrens) met één constante (omvang) wordt vergeleken. Toetsing met zeefgetallen vraagt telkenmale per post een vergelijking van twee variabelen, te weten postgrootte en zeefgetal. Het voordeel van deze vereenvoudiging, wordt in paragraaf 3 aan de hand van een voorbeeld geïllustreerd.

Blijkens een eerdere berekening van post 5 is de zeefgrens (G):

$$- 11,5 \text{ mln.} / 2.570 * 0,08035 = 359 \quad T/P * a = G$$

Aangezien het a-selecte getal $a < 1$ is, zijn alle zeefgrenzen voor deze post lager dan:

$$- \text{verantwoordingstotaal/postgrootte} \quad T/P = X$$

$$11,5 \text{ mln.} / 2.570 = 4.474 \text{ (naar beneden afgerond).}$$

Dit maximum wordt, zoals eerder vermeld, het zeefgrensmaximum (X) genoemd, uit welk maximum de zeefgrens (G) wordt afgeleid:

$$4.474 * 0,08035 = 359 \quad T/P * a = G$$

Een steekproefomvang die groter is dan dit zeefgrensmaximum, is ook groter dan alle mogelijke zeefgrenzen. Dan is er bij die steekproefomvang ook een 100% trefkans.

Hieruit vloeit voort, dat de vraag of een post bij een gegeven steekproefomvang (m) een 100% trefkans heeft niet alleen kan worden beantwoord door de toetsing:

$$- \text{postgrootte} > \text{zeefmaximum?} \quad P > T/m (= M)?$$

$$\text{maar ook door de toetsing} \quad m/P * P > T/m \times m/P?$$

$$\text{steekproefomvang} > \text{zeefgrensmaximum?} \quad m > T/P (= X)?$$

of

$$\text{zeefgrensmaximum} < \text{steekproefomvang?} \quad X < m?$$

Ter illustratie volgt hier een tabel met betrekking tot post 6 ad f 56.230 (P) in ons voorbeeld (T = 11,5 mln.).

Steekproefomvang (m)	Zeefmaxima (M = T/m)	Zeefgrens- maxima (X = T/P)	100% trefkans? (P = 56.230 > M?) (X = 204 < m?)
115	100.000	204	neen
204	56.372	204	neen
205	56.097	204	ja
230	50.000	204	ja

Ook hier blijkt, dat de toetsing

$$- \text{zeefgrensmaximum} < \text{steekproefomvang} (X < m)?$$

tot dezelfde uitkomsten leidt als de toetsing

$$- \text{postgrootte} > \text{zeefmaximum} (P > M)?$$

en ook - om dezelfde reden als voor de toetsing met zeefgrenzen - eenvoudiger is.

Uit het vorenstaande zal het de lezer naar ik vertrouw duidelijk zijn, dat de hantering van zeefgrenzen in plaats van zeefgetallen als selectie criterium in wezen geen verschil maakt. Er is sprake van hantering van een andere formulering van een volkomen gelijkwaardige toetsing.

3. De evaluatie bij hantering van zeefgrenzen

Uit het gestelde in de vorige alinea vloeit voort, dat mijn beschouwingen over de evaluatie in mijn vorig artikel onverkort gelden voor de selectie op basis van zeefgrenzen. Ik wil alleen op een tweetal punten wijzen.

Posten die gedeeltelijk fout zijn, worden bij de evaluatie als fout meegeteld als ook de fout gezeefd wordt, dit wil zeggen, als ook de fout groter is dan het zeefgetal (= maximaal aanvaardbare fout). Uit de zeefgrens kan het zeefgetal, zoals uit het vorengaande voortvloeit, als volgt worden afgeleid (zie pag.4):

$$\begin{array}{l} - \text{ foutgrootte} > \text{ zeefgetal} = & F > Z \\ & \text{zeefgrens} * \text{postgrootte}/ & = (G * P/m)? \\ & \text{steekproefomvang?} & \end{array}$$

Dus ook:

$$\begin{array}{l} - \text{ foutfractie} > \text{ zeeffractie} = \\ & \text{zeefgrens}/\text{steekproefomvang?} & F/P > G/m? \end{array}$$

ofwel

$$\begin{array}{l} - \text{ foutpercentage} > \text{ zeefpercentage} = \\ & 100 * \text{zeefgrens}/\text{steekproef-} & 100 F/P > 100 G/m? \\ & \text{omvang?} & \end{array}$$

Zoals reeds werd opgemerkt, worden posten met een zeefgrensmaximum lager dan de gekozen steekproefomvang met 100% trefkans geselecteerd. Deze posten worden derhalve ook met 100% trefkans geëvalueerd; dit geldt eveneens indien de posten gedeeltelijk fout zijn. Ik moge verder verwijzen naar mijn vorig artikel (pag. 7 en 8).

4. Flexibiliteit in de bepaling van de steekproefomvang

De flexibiliteit die de zeefgrens biedt bij de bepaling van de steekproefomvang, moge uit de volgende voorbeelden blijken.

Een verantwoording wordt steekproefsgewijs gecontroleerd op basis van de zeefmethode met hantering van zeefgrenzen. Gelet op de negatieve bevindingen in het vorige boekjaar (= kalenderjaar) wordt de steekproefomvang op 800 gesteld, uitgaande van een verwacht totaal van de verantwoording. De steekproefposten worden met een computer geselecteerd en afgedrukt. Bij elke post wordt de zeefgrens van die post afgedrukt, dit is een getal uit de reeks 0,1,...,799. Zeefgrensmaxima lager dan 800 worden eveneens afgedrukt.

In juni worden de steekproefposten van januari t/m maart gecontroleerd. Een nader onderzoek van de organisatie leidt tot de conclusie dat deze verbeterd is. Men besluit daarom de omvang van de steekproef tot 460 te beperken. Inmiddels zijn echter drie maanden op basis van een steekproefomvang van 800 gecontroleerd en heeft de computer ook de steekproefposten van april en mei op dezelfde basis geselecteerd.

Hoe nu te handelen?

Bij methoden gebaseerd op intervallen, zoals cell-sampling, is er naar mij bekend - althans praktisch - géén oplossing voor dit probleem. De zeefmethode met toetsing op basis van zeefgetallen biedt mogelijkheden, maar vraagt herrekening van de zeefgetallen, behorende bij de geselecteerde posten. De hantering van zeefgrenzen geeft echter een eenvoudige oplossing, aangezien deze grenzen door de herziening van de steekproefomvang geen wijziging ondergaan.

De procedure verloopt met zeefgrenzen als volgt:

- De evaluatie zal op een steekproefomvang van 460 gebaseerd dienen te worden. Indien in het eerste kwartaal fouten zijn gevonden, worden deze bij de evaluatie alleen meegeteld, voor zover de zeefgrenzen bij de betrokken posten lager zijn dan 460. Zou de selectie ook in de aanvang op een steekproefomvang van 460 zijn gebaseerd, dan zouden immers posten met een zeefgrens van 460 of hoger niet zijn geselecteerd en fouten daarin ook niet worden geconstateerd.
- De gedeeltelijk foute posten, die ook voor de evaluatie als fouten mee zouden tellen worden opnieuw getoetst:
 - . Fout > zeefgetal = $P/460 \times$ zeefgrens?in plaats van oorspronkelijk:
 - . Fout > zeefgetal = $P/800 \times$ zeefgrens?Hiermede wordt vastgesteld of er fouten zijn die nu lager zijn dan het nieuwe zeefgetal, waardoor zij voor de evaluatie niet meer als fout meetellen.
- Fouten in posten met een zeefgrens lager dan 460, en een zeefgrensmaximum > 460 doch < 800 , dienen - althans in principe - in de evaluatie niet meer als fouten met 100% trefkans behandeld te worden (de wijze van evaluatie werd besproken in mijn vorig artikel, pag. 7 en 8).
- Van de nog niet gecontroleerde lijsten van april en mei worden alleen de posten met zeefgrenzen < 460 gecontroleerd. Posten met hogere zeefgrenzen worden als niet-geselecteerd beschouwd.

Na voltooiing van de steekproef blijkt de uiteindelijke grootte van het verantwoordingstotaal. Is deze bijvoorbeeld 10% hoger dan het verwachte totaal, dan zal de vooraf bepaalde steekproefomvang (m),

te weten 460, ook met 10% tot 506 stijgen. De evaluatie geschiedt nu, zoals omschreven op pag. 6 van mijn vorig artikel op basis van het uiteindelijke verantwoordingstotaal, de steekproefomvang (506) en het aantal gevonden fouten.

De flexibiliteit kan ook in het steekproefplan worden ingebouwd, doordat men zich geheel de vrijheid voorbehoudt, de steekproefomvang op een later moment vast te stellen, uit te breiden respectievelijk in te krimpen, afhankelijk van de bevindingen met betrekking tot de administratieve organisatie.

Stel dat een steekproefplan voorziet in een steekproefomvang van maximaal 920. Op deze basis vindt de selectie plaats. Alle posten met zeefgrenzen < 920 worden afgedrukt.

Men besluit aanvankelijk te controleren op basis van een steekproefomvang van 460, waartoe alleen de posten met een zeefgrens < 460 in de controle worden betrokken.

Tussentijds wil men de omvang vergroten tot bijvoorbeeld 625 op grond van de bevindingen met betrekking tot de administratieve organisatie. Nu worden ook de posten met een zeefgrens ≥ 460 en < 625 gecontroleerd.

Op reeds geconstateerde fouten heeft de uitbreiding van 460 tot 625 de volgende effecten:

- Gedeeltelijk foute posten die op grond van de toetsing met het zeefgetal (herleid uit de zeefgrens) niet als fout zouden meetellen, worden opnieuw getoetst ter vaststelling of de vergroting van de steekproefomvang de conclusie doet wijzigen.
- Foute posten met een zeefgrensmaximum ≥ 460 en < 625 worden alsnog voor de evaluatie met "100% trefkans" gekenmerkt.

Men kan ook alleen de posten met een zeefgrens < 460 doen afdrukken en die met een hogere zeefgrens doch < 920 op een magneetband doen vastleggen. Bij de later gewenste uitbreiding tot 625 worden alsnog de posten met zeefgrenzen van 460 of meer, doch < 625 afgedrukt.

Gelet op situaties als in de twee voorbeelden vermeld, verdient het sterke aanbeveling bij de toepassing van computerprogramma's op basis van de zeefmethode afdruk van de zeefgrenzen en van de zeefgrensmaxima te verlangen. De afdruk van de zeefgrensmaxima is echter alleen nodig, voor zover zij lager zijn dan de steekproefomvang, waartoe de afdruk (maximaal) bestemd is.

De flexibiliteit in de bepaling van de steekproefomvang die door de introductie van zeefgrenzen mogelijk wordt gemaakt is mijns inziens een belangrijk middel om de efficiency bij de toepassing van steekproeven te bevorderen.

Voor degenen, die bekend zijn met sequential sampling en double sampling zal het duidelijk zijn, dat de zeefselectie op basis van zeefgrenzen ook daar bijzondere mogelijkheden kan bieden. Een en ander is nog in studie.

III SUBSELECTIETECHNIKEN

In zekere zin hebben we op pag. 9 reeds een vorm van subselectie besproken. In het voorbeeld worden posten op basis van een steekproefomvang van 920 geselecteerd en afgedrukt, doch dienen de posten op basis van een omvang van 625 te worden gecontroleerd. De zeefgrenzen geven daarbij een eenvoudige mogelijkheid van subselectie, door de posten met een zeefgrens < 625 voor de steekproef ter controle aan te wijzen. Deze wijze van subselectie zal in een volgend artikel nog verder worden uitgewerkt.

Ik wil op deze plaats vooral aandacht besteden aan een andere mogelijkheid van subselectie.

De zeefmethode is tot dusverre beschreven als een methode, waarbij voor elke post een zeefgetal of een zeefgrens wordt berekend en de grootte van de post of die van de steekproefomvang getoetst wordt aan het zeefgetal c.q. de zeefgrens.

De postgewijze selectie geeft geen problemen indien deze geschiedt met een computer en voor de invoer gebruik gemaakt kan worden van magneetbanden en dergelijke van de cliënt.

Voor toepassingen waarbij de computer niet kan worden ingeschakeld, is apparatuur beschikbaar, waarbij snel en doelmatig de zeefgetallen of -grenzen worden berekend en de relevante gegevens vergeleken. Dit lost echter het probleem van de tijdrovende invoer van de posten niet op. Hiertoe kan de navolgende subselectiemethode worden toegepast, die aan de hand van een voorbeeld wordt toegelicht.

Stel een inkoopverantwoording heeft een vijftal verantwoordingsniveaus:

1. Jaartotaal van f 20 miljoen, bestaande uit:
2. 12 maandtotalen, bijvoorbeeld januari 500.000, elk bestaande uit:
3. dagtotalen, bijvoorbeeld 15 januari f 35.000, elk bestaande uit:
4. bladtotaal, bijvoorbeeld één d.d. 15 januari van f 20.000, elk bestaande uit:
5. posten, bijvoorbeeld in het bedoelde bladtotaal één van f 570.

De steekproefomvang is 500, derhalve het zeefmaximum f 40.000.

We zullen nu de procedure vanaf niveau 2 op de voet volgen.

Niveau 2:

De maandtotalen zijn alle groter dan het zeefmaximum, zodat steekproefsgewijze controle op dit niveau geen zin heeft. Wel wordt de aansluiting van de 12 maandtotalen (niveau 2) met het jaartotaal ad f 20 miljoen (niveau 1) vastgesteld.

Niveau 3:

De feitelijke selectieprocedure vangt bij dit niveau aan.

Primair wordt vastgesteld dat de dagtotalen van januari (niveau 3) te zamen gelijk zijn aan het maandtotaal in januari ad f 500.000 (niveau 2).

Per dagtotaal wordt op grond van de selectieprocedure vastgesteld of het al dan niet voor verder onderzoek wordt aangewezen.

Stel dat het dagtotaal van 15 januari ad f 35.000 een zeefgetal heeft van 14323. Aangezien de telling groter is dan het zeefgetal, wordt dit dagtotaal voor verder onderzoek aangewezen, dit wil zeggen, wordt er naar niveau 4 "afgedaald".

Zou het zeefgetal 35.000 of meer zijn, dan wordt het dagtotaal aanvaard, zonder nadere controle van de samenstellende bladtotaal en posten (in niveaus 4 en 5).

Aangezien selectie van het dagtotaal ad f 35.000 plaatsvindt bij de zeefgetallen 0,1,...,34999 (35.000 van de 40.000 mogelijkheden), is de trefkans van het dagtotaal ad f 35.000 bij een zeefmaximum van 40.000

$$35.000/40.000.$$

Vindt selectie plaats

- omdat het zeefgetal kleiner is dan het dagtotaal,
- en is voorts het dagtotaal lager dan het zeefmaximum,
- met andere woorden, vindt selectie bij wijze van steekproef (< 100% trefkans) plaats,

dan wordt voor de selectieprocedure op niveau 4 het zeefmaximum gereduceerd tot de grootte van het dagtotaal (35.000).

Dit is het alternatieve zeefmaximum. Zoals hierna zal blijken, vindt de reductie plaats om bij de subselectieprocedure voortdurend een juiste trefkans te handhaven.

Niveau 4:

Primair wordt per geselecteerd dagtotaal (niveau 3) nagegaan dat het overeenstemt met de samenstellende bladtotaal (niveau 4).

Per bladtotaal wordt op grond van de selectieprocedure vastgesteld of het al dan niet voor verder onderzoek wordt aangewezen.

Stel, dat het bladtotaal d.d. 15 januari ad f 20.000 een zeefgetal heeft van:

- alternatief zeefmaximum * a-select getal
bijvoorbeeld $35.000 * 0,00927$, dit is 324.

Het bladtotaal is groter, zodat voor nader onderzoek naar niveau 5 moet worden "afgedaald".

Bij zeefgetallen van 20.000 of meer, wordt het bladtotaal zonder nadere controle van de samenstellende posten aanvaard.

Selectie vindt plaats bij de zeefgetallen 0,1,...,19999 bij een alternatief zeefmaximum van 35.000. De trefkans van het bladtotaal (niveau 4) ad f 20.000 is derhalve:

$$20.000/35.000,$$

gegeven de kans op selectie van het dagtotaal ad f 35.000 van

$$35.000/40.000 \text{ (zie niveau 3).}$$

De resulterende trefkans van het bladtotaal is het produkt van deze kansen:

$$20.000/35.000 * 35.000/40.000, \\ \text{dit is } 20.000/40.000.$$

Voor niveau 5 geldt als alternatief zeefmaximum 20.000, dit is de grootte van het geselecteerde bladtotaal (niveau 4) conform de uiteenzetting voor niveau 3.

Niveau 5:

Primair wordt de telling van de posten van het geselecteerde bladtotaal geverifieerd. Van elk geselecteerd bladtotaal wordt per post nagegaan of deze voor controle wordt aangewezen.

Stel, dat het zeefgetal van de post ad f 570 is $20.000 * 0,02076$, dit is 415: de post wordt geselecteerd en gecontroleerd.

Selectie van de post vindt plaats bij de zeefgetallen 0,1,...,569 bij een alternatief zeefmaximum van 20.000. De trefkans van de post is derhalve:

$$570/20.000$$

bij een trefkans van het bladtotaal ad f 20.000:

$$20.000/40.000 \text{ (zie niveau 4).}$$

Met inachtneming hiervan wordt de trefkans:

$$570/20.000 * 20.000/40.000, \\ \text{dit is } 570/40.000,$$

ofwel 570 ten opzichte van het oorspronkelijk zeefmaximum van 40.000.

Deze trefkans komt overeen met die bij een geheel postgewijze selectieprocedure.

De vereiste trefkans wordt bij deze subselectiemethode gehandhaafd door bij de selectie op een bepaald niveau de telling van het voorafgaande niveau als alternatief zeefmaximum te hanteren, indien:

- dit voorafgaande niveau in de selectieprocedure werd betrokken (hier vanaf het 3e niveau),
- de telling lager is dan het oorspronkelijke zeefmaximum.

Een voordeel van de subselectiemethode is dat de tellingen, zoals zij in de administratie voorkomen, op de voet worden gevolgd. Er is geen afzonderlijke selectietelling vereist, zoals dit bij de guldenrangnummermethode en bij cell-sampling het geval is.

De subselectiemethode is voor de praktijk nog verder verfijnd, waardoor een uiterst efficiënte procedure kon worden bereikt. Aan degenen die zich daarvoor interesseren, zal ik gaarne praktische toepassingen demonstreren.

Voorts ben ik gaarne bereid eventuele vragen te beantwoorden, die bij lezing van mijn artikelen mochten zijn gerezen.

In een volgend artikel hoop ik de eerder toegezegde selectiecombinaties aan de orde te stellen.



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

PRIVACY-WETGEVING

door A.W. Neisingh en J.F.C. van Epen

Inleiding

Bewustwordingsproces

Het zal nauwelijks meer verbazing wekken als reclamemateriaal van een tot nu toe onbekende onderneming correct geadresseerd in onze brievenbus glijdt. Evenmin maken we ons er zorgen over als de bankemployé eerst een beeldscherm raadpleegt alvorens onze vraag om geld te honoreren. Vervelend, maar nog steeds niet onrustbarend, ervaren wij het als de politie vaststelt dat we nog geen maand geleden in een andere hoek van het land ook al te hard hebben gereden en zijn betrapt.

Al deze zaken zijn onder één noemer te brengen: Er worden gegevens over ons bewaard, doorgaans in snel toegankelijke (computer)bestanden.

En zolang gegevens van ons banksaldo bij de bankier, de gegevens over de overtreding bij de politie en die over onze gezondheidstoestand onder berusting van onze huisarts blijven, kunnen we er wel vrede mee hebben.

Maar zijn we het er ook mee eens dat bedrijf X onze adressen kopieert uit de bestanden van de organisaties Y en Z? Toch gebeurt dit thans op ruime schaal. Immers, wanneer de kosten voor het inbrengen van de gegevens eenmaal zijn gemaakt, kunnen deze gegevens naar behoefte worden verwerkt, gekopieerd dan wel verkocht. Indien het sleutelgegeven identiek is, kunnen gegevens, die voor verschillende doeleinden zijn vergaard, worden gecombineerd. Hieruit zijn andere, vaak ongewenste conclusies te trekken. Vandaar dat in sommige kringen ernstig bezwaar bestaat tegen de invoer van het Algemeen Administratienummer voor Personen. Het sleutelgegeven is dan voorhanden!

Toepassing van geavanceerde vastleggings- en opvragingstechnieken impliceert een gevaar waar het om persoonsgebonden gegevens gaat. Namelijk het gevaar van de inbreuk op de persoonlijke levenssfeer. Vooral bestaat dit gevaar wanneer niet de nodige zorgvuldigheid wordt betracht.

Uit de praktijk zijn tal van voorbeelden te geven van onzorgvuldige vastlegging van gegevens dan wel van weliswaar zorgvuldig vastgelegde, maar wellicht ongewenste afgifte van persoonlijke informatie.

We noemen ter illustratie hiervan een aantal voorbeelden:

- Abusievelijk tot stand gekomen informatie omtrent iemands kredietwaardigheid kan leiden tot een weigering van een aangevraagd krediet.

Als een reusachtig spinneweb

„Gedurende zijn hele leven vult de mens reeksen formulieren in, op talloze vragen geeft hij antwoord en alles wordt opgeslagen. In zijn woorden zitten honderden draden verborgen.

Als die plotseling zichtbaar werden, zou de lucht er uitzien als een reusachtig spinneweb en als het banden waren – bussen, treinen, zelfs mensen zouden het vermogen verliezen zich te bewegen. De wind zou niet in staat zijn opgewaaide kranten en herfstbladeren door de straten van de stad te dragen.

Ze zijn niet zichtbaar, die draden, ze hebben geen vorm, maar ieder is zich voortdurend van hun bestaan bewust. Elk mens heeft zijn eigen lijnen, ieder ontwikkelt een natuurlijk ontzag voor de mensen die aan de touwtjes trekken...”

**ALEXANDER
SOLZJENITSYN**

Uit: Elseviers Weekblad

- Het tegen politieke tegenstanders gebruiken van niet terecht verkregen persoonlijke gegevens (koopsompolissen-affaire).
- Het blokkeren van een promotie op grond van negatieve beoordeling in het verleden.
- Het door de fiscus doorgeven van het belastbaar inkomen aan bijvoorbeeld kerkgenootschappen.

Hoewel in het verleden deze inbreuken op de privacy ook voorkwamen, heeft de automatisering de mogelijkheden ervoor aanzienlijk verruimd bij een daling van de relatieve kosten. Hiervan is de publieke opinie zich langzaam aan bewust gaan worden: men vraagt zich thans af WIE heeft WELKE GEGEVENS over mij en WAAR worden zij bewaard? En ook: gaat men vertrouwelijk met mijn gegevens om (illustratief is in dit verband nevenstaande cartoon uit Computable).

In vele landen heeft dit bewustwordingsproces geleid tot studies waaruit ontwerpen of voorstellen voor wetgeving op dit gebied zijn ontstaan. Om echter een voorstel daadwerkelijk in een wet om te zetten is politieke wil nodig. De overheid is immers zelf "slachtoffer" van een dergelijke wetgeving.

In een beperkt aantal landen is inmiddels een privacywet van kracht geworden. Wij noemen Zweden (1973), de Verenigde Staten (1974) en West-Duitsland (1978).

Nederland behoort tot de landen waar een rapport met voorstel tot wet aan de regering is aangeboden: het Eindrapport van de Commissie Koopmans. Het moment waarop het wetsontwerp zal worden ingediend lijkt echter nog veraf.



"KLOPT DAT ?....."

Privacy versus security

Zonder te willen komen tot een definitie van het begrip mogen we stellen dat we onder privacy datgene verstaan, wat het individu in staat stelt zichzelf te zijn. We kunnen het vertalen met "persoonlijke levenssfeer". Het begrip reikt echter verder dan het individu alleen; het strekt zich ook uit tot groepen van personen (bijvoorbeeld Etnische minderheden) en rechtspersonen (bijvoorbeeld bedrijven).

Het privacy-begrip kan vanuit een aantal gezichtspunten worden gezien. Wij zullen dit doen vanuit de verwerking en bewaring van gegevens. Daarom wordt in dit verband wel gesproken van informatieprivacy.

In de vorige paragraaf is naar voren gekomen dat de inbreuk op de (informatie) privacy op verschillende wijzen kan plaatsvinden:

1. Inzage in persoonlijke gegevens door onbevoegden.
2. Verzamelen van gegevens die niet per se ter zake doen (informatievervuiling).
3. Gebruik van gegevens voor een ander doel dan waarvoor deze zijn verzameld.
4. Combineren van gegevens waardoor nieuwe conclusies - al dan niet terecht - kunnen worden getrokken.
5. Het niet tijdig laten vervallen (verwijderen) van niet meer geldige gegevens.

Volgens onze cultuuropvatting dient de persoonlijke levenssfeer beschermd te worden. Hiervoor dienen regels te worden opgesteld. Deze regels zullen zich derhalve richten op de bescherming van personen c.q. rechtspersonen.

Het begrip security richt zich op de bescherming van gegevens. We bedoelen hier met name gegevens die in een machinaal leesbare vorm zijn vastgelegd. Het begrip wordt vertaald met "gegevensbeveiliging".

Heeft privacy te maken met "wettelijke" aspecten, data security impliceert vooral technische en organisatorische aspecten.

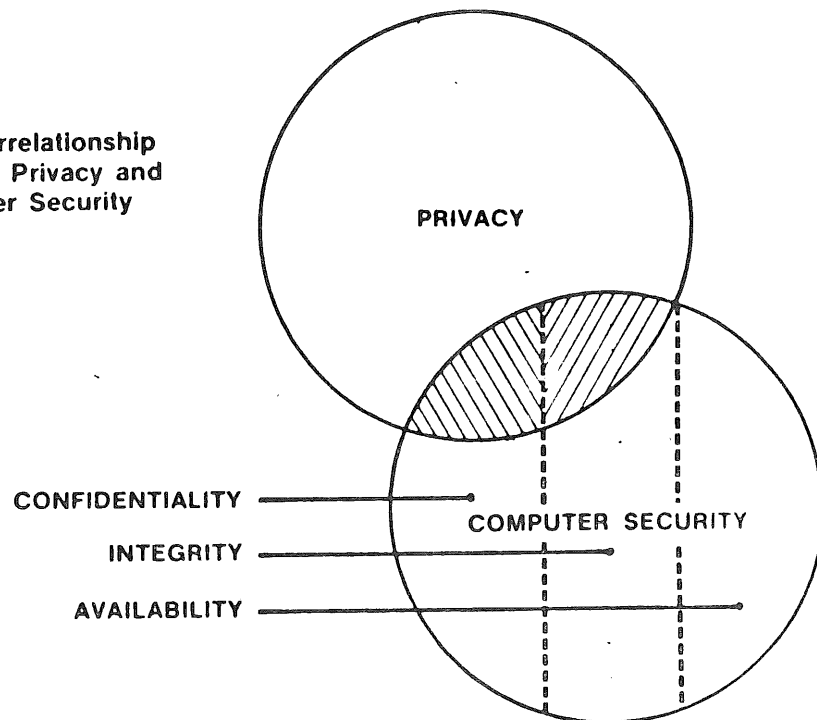
Aangezien voor het voldoen aan de gestelde regels en wetten, dus voor de uitvoering, gebruik wordt gemaakt van eveneens technische en organisatorische maatregelen, zien we dat er een zekere mate van overlapping bestaat tussen beide gebieden.

De figuur op de volgende pagina (ontleend aan The Internal Auditor) moge een en ander illustreren.

Binnen dit overlappingsgebied zullen we de toegangsbeveiliging tot computerprogramma's en -bestanden aantreffen. Zo behoort de bewaking van de juistheid van bestanden ook tot beide interessegebieden.

Er zijn echter ook tegenstrijdigheden waar te nemen. Zo wordt de verwerking van vertrouwelijke gegevens (directiesalarissen) soms steeds door dezelfde operator verricht; dit is strijdig met de beveiligingseis van voldoende functiescheiding. Een ander aspect is het beveiligen van bestanden door duplicering: de mogelijkheid tot diefstal is dan eveneens verdubbeld.

The Interrelationship Between Privacy and Computer Security



Resumerend kan worden gezegd, dat privacy-maatregelen de **PERSOON** beschermen en beveiligingsmaatregelen de **GEGEVENS**. Deels zal de bescherming van personen en persoonsgebonden gegevens met dezelfde maatregelen kunnen worden verkregen, deels zullen zij strijdig met elkaar zijn.

In elk geval zal de invoering van privacy-wetgeving consequenties hebben voor de organisatie van de onderneming, de ontwikkeling van geautomatiseerde systemen, de gegevensverwerking en de gegevensbeveiliging.

Er zullen speciale eisen gesteld dienen te worden aan operating systems. Gegevens zullen niet zonder meer over de landsgrenzen gebracht kunnen worden.

Er zullen verzekeringen komen om de financiële gevolgen van inbreuk op de privacy-wetten te beperken.

Op een aantal van deze consequenties zullen wij in komende artikelen terugkomen. Daarbij zullen wij de belangrijkste aspecten van reeds ingevoerde wetten en ingediende wetsontwerpen in andere landen bespreken. Ook zal hierbij aandacht worden besteed aan de activiteiten van de Raad van Europa met betrekking tot de wetgeving op de bescherming van persoonsgebonden gegevens.



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

DE NABIJE TOEKOMST VAN COMPUTERGEBRUIK

door H. Roos

Inleiding

Richard Canning brengt in zijn maandelijks "EDP-Analyzer"'s het spectrum van de automatisering op verkennende en evaluerende wijze onder de aandacht van zijn lezers.

Hij slaagt er daarbij telkens weer in een nauwe band te handhaven met de praktijk van de voorhoede van de automatisering. Kritische bespreking en evaluatie van nieuwe produkten, systemen en methoden worden geïllustreerd met praktische ervaringen van gebruikers.

De wijze waarop is bovendien duidelijk gericht op het automatiseringsmanagement.

"Get ready for major changes"

Voor het management en zeker niet alleen voor het automatiseringsmanagement, is een verkenning van de in de naaste toekomst te verwachten ontwikkelingen een belangrijk zaak.

In het november-1978-nummer van de EDP-Analyzer geeft Canning zo'n verkenning onder de veelzeggende titel "Get ready for major changes".

De invloed van de chip

Het allesbeheersende thema is de micro. Hij legt er de nadruk op dat niet het vage onderscheid tussen maxi, mini en micro de aandacht vraagt, doch de mogelijkheden van de micro.

Hij stelt vast dat het technisch mogelijk is om een enkele chip processor te vervaardigen die plug-compatible is met bijvoorbeeld de IBM 370 en werkt met een snelheid van een model 148 of 158. En dat tegen zeer lage produktiekosten.

Het kernpunt van de ontwikkeling is zo bezien de micro als bouwsteen.

Mainframes versus plug-compatible

Van groot belang voor het management is wat de invloed van deze ontwikkeling zal zijn op het aanbod van de grote mainframers (IBM, UNIVAC, enz.), hoe deze zullen reageren op de scherpe concurrentie van de plug-compatible fabrikanten en hoe de kostenverhoudingen van communicatie, van computersystemen (hardware en software) en van personeelskosten zich zullen ontwikkelen.

Plug-compatible fabrikanten maken in beginsel geen eigen software. Zij maken computers die kunnen werken met (bijvoorbeeld) IBM-software. Het succes van plug-compatible computers moet derhalve geheel zijn gebaseerd op een prijsverschil met vergelijkbare IBM-apparatuur, dat zodanig groot is, dat de koper het prijsverschil neemt in ruil voor het opgeven van de zekerheid die hij denkt te kopen wanneer hij IBM-apparatuur aanschaft.

Communicatie-, computer- en personeelskosten

De beweging die Canning ziet in de markt wordt veroorzaakt door de potentiële mogelijkheden tot zeer sterke prijsdalingen voor hardware.

Hij noemt een tweetal verhoudingen die illustratief zijn voor wat ons te wachten staat.

De eerste gaat uit van het extrapoleren tot 1983 van in 1975 vastgestelde trends.

Met als uitgangspunt de verhouding in 1975 van communicatiekosten 19%, computerkosten 46% en personeelskosten 35% zou dat in 1983 als verhouding opleveren: communicatiekosten 10%, computerkosten 17% en personeelskosten 73%.

Alleen al de onmogelijkheid om voldoende personeel op te leiden om aan deze geweldige vraag te voldoen (\$ 35 miljard in 1983 aan personeelskosten!) vormt een geweldige prikkel tot trendwijziging.

Als tweede verhouding citeert hij een verwachting van een IBM'er die neerkomt op: communicatiekosten 39%, computerkosten 37% en personeelskosten 24%.

Deze verhouding is gebaseerd op de verwachting dat de ontwikkeling van gedistribueerde systemen grote opgang zal maken.

Een tweede belangrijke veronderstelling is dat in deze systemen de gegevensverwerking en de kantoorautomatisering zullen worden geïntegreerd.

Weer een grote conversie?

Op basis van deze eenvoudige gegevens ontwikkelt Canning een aantal mogelijke scenario's van de IBM-policy.

Kernpunt daarin is steeds dat die policy gericht zal zijn op het scheppen van afstand tussen IBM en de plug-compatible fabrikanten. En wel zodanig dat die laatste na elke "zet" van IBM enkele jaren nodig zullen hebben voor een antwoord.

Alleen op die manier kan IBM volgens Canning voorkomen dat de prijzen van de hardware te veel zullen dalen. Vervolgens, refererend aan het door de overgang naar de 370-serie indertijd veroorzaakte conversiesyndroom, gaat hij na op welke manieren IBM de overgang naar een geheel nieuw systeem aantrekkelijk kan maken.

Hij draagt een groot aantal mogelijkheden aan waarvan er een aantal is dat speciale vermelding verdient.

Virtual storage en multi-programming

Het gebruik van virtual storage technieken zou kunnen worden beperkt ten behoeve van het data management. Een goedkoop alternatief voor virtual storage technieken als element van multi-programming zou kunnen zijn het gebruik van meerdere processoren. Complexe software zou dan alleen nodig zijn voor het beheer van de andere systeemcomponenten die wel gemeenschappelijk gebruikt zullen worden.

Het principe van meerdere processoren kan tevens worden toegepast op de conversieproblematiek. Een of meerdere kunnen zo worden gebouwd (of micro-programmed!) dat ze een 370 emuleren.

Openbare data-netwerken

Wat betreft de ontwikkeling op het gebied van openbare data-netwerken merkt Canning op, dat deze werken in het voordeel van plug-compatible fabrikanten door de standaardisatie van de koppeling.

De conclusie moet zijn dat de mainframers deze ontwikkeling niet zullen stimuleren en hun eigen netwerksystemen aan de man zullen trachten te brengen (zoals IBM's SNA en Univac's DCA).

Overigens past hierbij zeker voor Europese verhoudingen een vraagteken. In elk geval hebben de Europese PTT-organisaties hierop een belangrijke invloed, onder meer door een tariefpolitiek. Die invloed kan zwaarder zijn naarmate het relatieve aandeel van de communicatiekosten groter is.

Microcode en data-encryption

Een tweetal andere mogelijkheden zijn volgens Canning het gebruik van microcode die bij elk nieuw operating system release wordt gewijzigd en het consequent toepassen van data-encryption voor het datatransport tussen de CPU en de randapparatuur.

Ondersteuningssoftware

Kijkend naar de gebruiker wordt verwacht dat er in grotere mate dan tot nu toe ondersteuningssoftware zal worden aangeboden met als voorname functie het vergroten van de aantrekkingskracht van nieuwe systemen. Een element hieruit zijn de systeemontwikkelingshulpmiddelen.

Improved programming technologies

In de EDP-Analyzer van november 1977 wordt een overzicht gegeven van wat IBM toentertijd aanbood onder de naam Improved programming technologies. Een drietal produkten uit deze serie zijn HIPO (Hierarchy plus Input-Process-Output) als software design hulpmiddel, de Structured Programming Facility onder TSO (Time Sharing Option) en de COBOL Interactive debug facility.

Voor het gebruik in combinatie met andere pakketten bestaan ook dergelijke produkten.

Rond het data base - data communication systeem IMS zijn zogenaamde productivity aids beschikbaar die de hele ontwikkelingscyclus dekken.

Hetzelfde geldt voor de combinatie CICS (Customer Information Control System, een TP-monitor) met DL/1 (Data Language one, het data base deel uit IMS).

Deze trend zet zich duidelijk door in de nieuwere systemen. Ten behoeve van System 34 is een hulpmiddel voor het genereren van interactieve programma's beschikbaar, genaamd Work Station Utility (WSU).

The analyses of user needs

In de EDP-Analyzer van januari 1979 behandelt Canning een aantal van deze hulpmiddelen op het terrein van de informatie-analyse tot aan het systeemontwerp. De titel is "The analyses of user needs".

Het belangwekkende van die beschouwing is dat een tweetal betrekkelijk nieuwe methoden, een Amerikaanse getiteld SADT (Structured Analysis and Design Technique) en daarvan alleen het SA-deel, en een Europese, IA (Information Analysis) van Langefors en Lundeberg worden vergeleken met IBM's HIPO.

Analyse van de beide eerste methoden geeft een indicatie voor de reden van geringe acceptatie van HIPO.

Alle drie bevatten als kenmerken het principe van "bounded context" dat wellicht vertaalbaar is met "systeembegrenzing", een grafische notatie die zowel voor ontwikkelaars als voor gebruikers goed is te begrijpen, terwijl het goed mogelijk is om door HIPO te combineren met "structured walk-through" een inspectiemethode te creëren. Dit aspect is ingeweven in de beide andere methoden.

Wat HIPO echter mist en de beide andere wel bezitten is een aantal eigenschappen die van invloed zijn op zowel de effectiviteit in het gebruik als de bereikbare discipline in dat gebruik:

- Het onderscheid tussen verschillende niveaus van abstractie blijkt fundamenteel voor het verwerven van inzicht in complexe situaties.
- Gelijkelijke aandacht voor activiteitenanalyse en voor data-analyse (eigenlijk informatie-analyse).
- De diagrammen moeten eenvoudig te wijzigen zijn.
- De diagrammen moeten door middel van een nummersysteem aan elkaar zijn gerelateerd en verschillende versies moeten eveneens op grond van een nummer identificeerbaar zijn.
- Een beproefde gebruiksmethode moet beschikbaar zijn die samen met:
- Adequaat materiaal voor training
borg moet staan voor het bereiken van een goede communicatie tussen alle betrokkenen.
- De diagrammen moeten een audit trail vormen van het ontwikkelingsproces. Dit is alleen mogelijk wanneer de besprekingsnotities op de diagrammen zelf gesteld worden.
- De analysemethode moet op natuurlijke wijze overvloeien in de ontwerp-methode.

Beide methoden, SA zowel als IA, lenen zich voor ondersteuning door speciale software.

Diagrammen kunnen worden "getekend" op een grafische terminal, ze kunnen worden opgeslagen op bijvoorbeeld schijfbestanden en afgedrukt met behulp van een speciale printer.

In elk geval het verrichten van het aan de methoden verbonden routine-werk is zo te automatiseren.

Daarnaast denkt Canning aan mogelijkheden tot ondersteuning tijdens het analyseproces in twee richtingen:

- van het systeem deel uitmakende checklists;
- signalering van inconsistente, onvolledige en/of ontbrekende "requirement statements".

Besluit

Tot slot een tweetal relativerende citaten uit respectievelijk november 1978 en januari 1979:

- "It should be recognized that the impact of distributed systems and distributed data bases upon the organization is not yet well understood."

- "Three main problems with these methodologies still exist:
 - . there are no formal criteria for guiding decomposition,
 - . there is no way to enforce semantic rigor,
 - . there is no way to judge if a diagram is good, or even to know what 'good' means."

Naschrift

Een aantal op het gebied van de hardware geschetste mogelijkheden begint zich in de praktijk reeds af te tekenen.

De recent door IBM aangekondigde nieuwe machines System 38 en de 4300-serie gaan in die richting.

Op beide machines zal in een volgend nummer van Compact worden ingegaan.

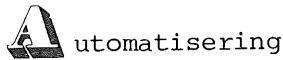


COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & co

N I E U W S

Automatisering
Beveiliging
Controle

door H.C. Kocks



Onderzoek Datapro inzake softwarepakketten

Datapro heeft in 1978 wederom een onderzoek ingesteld naar de bevindingen van de gebruikers van softwarepakketten inzake:

- Data Base Management Systems,
- Telecommunications Monitors,
- Data Management Systems.

De gebruikers werd verzocht de bij hen in gebruik zijnde pakketten een waardering te geven op de volgende punten:

- Overall satisfaction,
- Throughput/efficiency,
- Ease of installation,
- Ease of use,
- Documentation,
- Vendor technical support,
- Training.

De waardering kon zijn: poor (1), fair (2), good (3) en excellent (4).

In de resultaten van het onderzoek zijn de beoordelingen van die pakketten (totaal 260) verwerkt, waarvan 5 of meer gebruikers het hun toegezonden vragenformulier ingevuld hadden geretourneerd.

Aan 36.000 gebruikers is een vragenlijst toegezonden. De respons bedroeg $\pm 17\%$ (± 6.000).

De volgende drie tabellen geven de waarderingen van de meest gangbare pakketten inzake:

- Data Base Management Systems (tabel 1),
- Telecommunications Monitors (tabel 2),
- Data Management Systems (tabel 3).

Tabel 1

HOW USERS RATED THE POPULAR DATA BASE MANAGEMENT SYSTEMS								
Weighted Average User Ratings								
Package & Vendor	Number of users reporting	Overall Satisfaction	Throughput/Efficiency	Ease of Installation	Ease of Use	Documentation	Vendor Technical Support	Training
		ADABAS , Software ag of N.A.	28	3.5	3.1	3.5	3.3	2.8
Datacom/DB , Applied Data Research	15	2.9	3.1	3.0	3.2	2.5	2.9	2.8
DBMS-10/20 , Digital Equipment Corp.	6	2.8	2.5	3.0	2.8	2.5	2.2	2.7
DBOMP , IBM Corp., DPD	25	2.8	2.5	2.1	2.5	2.3	2.3	2.3
DL/1 DOS/VS , IBM Corp., DPD	36	2.8	2.5	2.5	2.5	2.5	2.7	2.8
DL/1 Entry , IBM Corp., DPD	8	3.0	2.6	2.6	3.1	2.5	3.0	2.8
DMS-II , Burroughs Corp.	30	3.4	3.3	3.4	3.4	2.5	2.6	2.5
DPL , National Information Systems	6	3.5	2.3	3.8	3.5	3.0	3.0	3.2
IDMS , Cullinane Corp.	42	3.5	3.3	3.5	3.4	3.1	3.5	3.3
IMAGE/1000 , Hewlett-Packard Co.	9	3.0	2.9	3.4	3.0	2.5	2.7	3.3
IMAGE/3000 , Hewlett-Packard Co.	30	3.5	3.3	3.7	3.6	3.2	3.0	2.7
IMS , IBM Corp., DPD	34	2.9	2.4	2.2	2.5	2.8	2.8	2.6
INQUIRE , Infodata Systems, Inc.	8	3.8	2.8	3.6	3.3	2.9	3.3	2.9
SYSTEM 2000 , MRI Systems	24	3.3	2.9	3.1	3.2	2.8	2.8	3.0
TOTAL , Cincom Systems, Inc.	108	3.2	3.1	3.2	3.2	2.7	2.7	2.7

Tabel 2

HOW USERS RATED THE POPULAR TELECOMMUNICATIONS MONITORS								
Weighted Average User Ratings								
Package & Vendor	Number of users reporting	Overall Satisfaction	Throughput/Efficiency	Ease of Installation	Ease of Use	Documentation	Vendor Technical Support	Training
		CICS , IBM Corp., DPD	174	2.9	2.7	2.3	2.4	2.8
Com-plete , Software ag of N.A.	5	3.2	4.0	3.2	3.8	2.2	3.2	2.8
Datacom/DC , Applied Data Research	13	3.3	3.5	2.9	3.2	2.6	3.2	3.2
ENVIRON/1 , Cincom Systems	16	3.0	3.3	3.2	3.1	2.5	2.8	2.7
ETSS , IBM Corp., DPD	19	3.3	3.2	2.4	3.2	2.4	2.2	2.4
GBASWIFT , GBA International	10	3.2	3.0	3.5	3.5	3.3	3.4	2.6
INTERCOMM , Informatics	11	2.8	3.0	2.3	2.7	2.3	2.6	2.4
MINICOMM , Informatics	9	3.6	3.8	3.6	3.7	2.6	2.9	2.9
MTCS , IBM Corp., DPD	13	2.7	2.6	2.5	2.2	1.4	2.4	1.7
NDL , Burroughs Corp.	35	3.4	3.2	3.3	3.4	2.5	2.5	2.6
ROSCOE , Applied Data Research	20	3.5	3.5	3.3	3.5	3.1	3.0	2.8
Shadow II , Altergo Software, Inc.	18	3.7	3.7	3.5	3.4	3.1	3.4	3.2
TASK/MASTER , Turnkey Systems	27	2.9	3.0	2.6	2.9	2.5	2.5	2.7
WESTI , Westinghouse Electric	46	3.7	3.6	3.5	3.4	3.2	3.2	3.1

Tabel 3

HOW USERS RATED THE POPULAR DATA MANAGEMENT SYSTEMS								
Package & Vendor	Weighted Average User Ratings							
	Number of users reporting	Overall Satisfaction	Throughput/Efficiency	Ease of Installation	Ease of Use	Documentation	Vendor Technical Support	Training
Batch Query (S/3) , IBM Corp., GSD	12	2.5	2.1	2.3	2.6	2.5	2.3	2.0
CULPRIT , Cullinane Corp.	12	3.3	3.1	3.4	3.0	2.9	3.3	3.1
Data Analyzer , Program Products	10	3.2	3.0	2.9	3.2	2.8	3.0	2.9
DATATRIEVE , Digital Equipment Corp.	5	2.4	2.6	3.0	3.0	2.0	1.6	—
DYL-260 , Dylakor Software Systems	46	3.6	3.4	3.7	3.4	2.9	3.2	3.0
EASYTRIEVE , Pansophic Systems	68	3.5	3.4	3.6	3.4	3.0	3.0	2.9
EXTRACTO , Optipro, Inc.	15	3.3	2.9	3.2	3.6	2.9	2.3	2.6
FORTE , Burroughs Corp.	14	3.3	2.9	3.3	3.4	2.6	2.6	2.7
GIS (GIS/VS) , IBM Corp., DPD	6	2.5	2.3	3.0	3.0	2.3	2.3	2.3
MARK IV , Informatics	61	3.2	2.8	3.2	2.9	2.8	2.8	2.9
POISE , The Poise Company, Inc.	7	3.4	2.6	3.7	3.6	2.7	3.1	3.0
QDMS , Quodata Corp.	5	2.8	2.8	3.0	2.8	2.2	2.6	2.3
QUIKJOB , System Support Software	37	3.6	3.5	3.8	3.6	3.0	3.0	2.7
RAMIS II , Mathematica Products Group	5	3.0	2.4	2.5	3.0	2.4	2.4	3.0
SAS , SAS Institute, Inc.	22	3.5	3.1	3.3	3.3	3.0	3.3	2.9
SCORE , Informatics	5	2.6	3.0	2.8	3.0	2.6	2.8	2.7

Wie kennis wil nemen van de waarderingen van de overige in het onderzoek betrokken pakketten, wordt verwezen naar het artikel: User Ratings of Software Packages, Datamation december 1978.

Volgens Datapro geven de resultaten van het onderzoek het volgende algemene beeld te zien:

- Data processing community and data processing applications are changing.
- Major changes are in the increasing emphasis on minicomputer usage, especially in distributed environments and in the continuing conversion to data base management.
- Software is becoming more important to the typical installation.
- Users are becoming more critical of software packages and their support. (De gemiddelde waardering was in 1978 lager dan in 1977.)

Datamation, december 1978

Allerlei

IBM ontwikkelt 1 megabyte "Whitney"-schijf

Het is nu al bekend, dat IBM waarschijnlijk binnenkort met een 1 megabyte schijf op de markt zal komen, die nu nog met de codenaam Whitney wordt aangeduid. Volgens insiders wordt voor deze schijf gebruik gemaakt van een dunne laag materiaal voor het vastleggen van de gegevens. Een en ander is nog het onderwerp van een onderzoek, dat door IBM-technici wordt uitgevoerd in het researchcentrum van de fabriek in San José in Californië. De schijf zal worden voorzien van een zeer zachte keramische laag, die op de traditionele aluminiumplaat wordt aangebracht. Bij de fabricage echter zal, naar men aanneemt, een aantal nieuwe materialen en technieken worden toegepast, waaronder een fijnkorrelige vastleggingslaag, welke via een nieuwe coating-techniek op de plaat wordt aangebracht. Door deze laag zo dun mogelijk te houden hoopt men een zeer hoge schrijfdichtheid te kunnen realiseren in combinatie met een hoge omloopsnelheid van de schijf zelf.

Wanneer de schijf precies op de markt zal komen is tot op heden niet bekend.

Computable, december 1978

Data dictionary

Users of IDS/1 (integrated Data Store/1) on this vendor's large mainframes now can get a Data Dictionary. The package handles data element reporting, where-used reports, record creations, maintenance reporting, and other functions. Routines are included for analyzing COBOL, Index Sequential Processing, and transaction-driven systems source programs, identifying the data elements accessed and how the program uses each element. The package can be used to determine the fundamental structure of the data, as well as the way events and functions use data.

The IDS/1 Data Dictionary needs 48K words of memory.

Datamation, december 1978

Al lang verwachte IBM 4300 uitgebracht

IBM verder met prijsontkoppeling

IBM heeft wereldwijd de 4300-serie geannonceerd, die, zo luidt het officiële communiqué, "de gunstige prijs/prestatieverhoudingen, de flexibiliteit en de verwerkingssnelheden van de hogere modellen van het systeem 370 en de 3030 processors ook binnen het bereik brengt van kleinere gebruikers".

Bij de annoncering van de 4300-computerserie, die onder de codenaam E-serie is ontwikkeld en (voorlopig?) uit twee modellen bestaat, zet IBM

de voor het eerst bij de 8100-serie gewijzigde prijspolitiek ten opzichte van de mee te leveren systeemprogrammatuur door. Alhoewel een basispakket, vergelijkbaar met DOS, gratis is, moet alle verdere systeemprogrammatuur afzonderlijk worden betaald. De prijsontkoppeling van apparatuur en programmatuur geldt dus vrijwel volledig voor de nieuwe 4300-serie.

Levering start medio en eind 1979

Als belangrijkste kenmerken van de 4300-serie ziet IBM zelf een nieuw virtueel geheugenconcept, een verdergaande miniaturisering door onder meer toepassing van de zelf ontwikkelde 64 K chip in geheugen en verwerkingseenheid en uitwisselbaarheid van programmatuur en verwerkings- en geheugencircuits van de 370-serie. Er zijn nu twee modellen gelanceerd, waarvan de kleine - het model 4331 - in juni van dit jaar en de grotere - het model 4341 - rond de komende jaarwisseling leverbaar zullen zijn.

Wanneer IBM zelf spreekt over de mogelijkheden van de grotere computers voor de kleinere gebruiker bereikbaar te maken, dan bedoelt zij wat exacter uitgedrukt, dat de 4331 is bedoeld voor de huidige gebruikers van 370/115 en 370/125-systemen en de 4341 kan worden gezien als uitbreidingsmogelijkheid voor de 370/138.

De annoncering van de nieuwe serie wordt begeleid door de introductie van diverse programmatuurfaciliteiten en randapparaten. Daarbij maakt IBM het de fabrikanten van compatibele apparatuur weer moeilijker door gebruik te maken van microcode, maar de gebruiker (die in wezen toch het belangrijkste is) krijgt vele configuratiemogelijkheden. Hierbij herconfigureert IBM in principe het systeem, zodat daarvoor geen systeemprogrammeur bij de gebruiker meer aanwezig hoeft te zijn.

Apparatuur- en programmatuurbeschrijving

IBM noemt de nieuwe 4331 zelf "bij uitstek geschikt voor data base / datacommunicatietoepassingen".

Het systeem kan worden uitgerust met een werkgeheugen van een half of één megabyte, terwijl er afhankelijk van de aard en hoeveelheid van de werkzaamheden tien tot twintig beeldschermeenheden op kunnen worden aangesloten. Dit gebeurt door middel van geïntegreerde adaptoren, waaraan tevens een kaartlezer en de opslagmedia worden gekoppeld. Verder beschikt het systeem over een ingebouwde flexibele schijveneenheid en een speciale communicatie-adaptor, die ook het werken onder SNA mogelijk maakt.

De 4341, die kan worden uitgerust met twee of vier megabytes aan werkgeheugen, kan volgens IBM binnen een enkel toepassingsgebied op diverse manieren worden geconfigureerd. Zo kan men er direct lokaal op werken of via op afstand opgestelde terminals, gedistribueerd over groepen van gebruikers of, net zoals bij het kleine model, binnen een SNA-netwerk. Wederom afhankelijk van de toepassingen kunnen er op dit systeem twintig tot zestig à zeventig terminals worden aangesloten.

Herconfigureren en programmatuur

De besturingsfuncties van de 4300-serie worden in principe door IBM vastgelegd op flexibele schijf, waar vanaf ze kunnen worden ingelezen in een microcodegeheugen, dat los van het werkgeheugen staat. Op deze manier kan tevens op een andere configuratie worden overgegaan, zonder dat er een systeemprogrammeur aan te pas hoeft te komen. Een aantal besturingsfuncties heeft IBM echter in de apparatuur ingebouwd, hetgeen met de naam "extended control program support" wordt aangeduid.

Alhoewel men de "oude" besturingsprogrammatuur van de 360- en 370-series op de 4300 kan overnemen, zijn er speciaal aangepaste en verbeterde DOS/VS, VM/370 en OS/VS-1 versies voor de nieuwe systemen ontwikkeld. Zo wordt het selecteren en in het geheugen brengen van toepassingsprogramma's vereenvoudigd door gebruik te maken van de zogeheten "system installation productivity option/extended" (System IPO/E's; over vakjargon gesproken!).

Hierover zegt IBM zelf:

"Elke System IPO/E bestaat uit een besturingssysteem (VM/370 en/of DOS/VSE) en verscheidene speciale besturingsprogramma's die van belang zijn voor het realiseren van bijzondere toepassingen. Dank zij System IPO/E's wordt de taak van onder andere systeem- en applicatieprogrammeurs aanzienlijk verlicht, wat kan resulteren in het brengen van de beschikbare verwerkingscapaciteiten naar meer eindgebruikers."

De 4300-serie kent diverse nieuwe randapparaten, waaronder een magneetbandeenheid, schijfeneenheden en een -besturingseenheid.

De nieuwe 8809-bandeenheid, waarvan er maximaal zes aan de 4331 kunnen worden aangesloten, kan met de lees/schrijfsnelheid van 12,5 of 100 inches per seconde werken. Van de eveneens gelanceerde 3310-schijfeneenheid, die op vaste schijf 64,5 megabytes kan bevatten, kunnen tot zestien stuks aan de 4331 worden gekoppeld.

De nieuwe 3370 schijfeneenheid is ook met een vaste schijf uitgerust, die echter door een grotere schrijfdichtheid een opslagcapaciteit heeft van 570 megabytes. Van deze eenheid is een model met ingebouwde besturingseenheid verkrijgbaar. Op de 4331 kunnen maximaal zestien en op de 4341 maximaal 32 3370's worden aangesloten. De laatste noviteit bij de 4300-serie is de 3880 schijfbesturingseenheid.

Bij de verder aan te sluiten randapparaten behoren onder andere de 3278-beeldschermeneenheden, de kassa- en bankterminals en diverse regeldrukkers, terwijl uitsluitend met de 4341 de 3800-laserdrukker en de magneetbandeenheden van het type 3420 kunnen werken.

De 4331-machine is in het researchlaboratorium van IBM in het Westduitse Böblingen ontwikkeld, de grotere 4341 in Endicott in de Amerikaanse staat New York.

Computable, 9 februari 1979

Beveiliging

Wanneer in de accountancy-wereld over beveiliging in de automatisering wordt gesproken, wordt veelal gedacht aan fysieke beveiligingsmaatregelen met betrekking tot een rekencentrum, bestanden en dergelijke, dan wel aan toegangsbeveiliging tot gegevens met behulp van een sleutel of password. Daarnaast is er echter het "operating system" dat uit beveiligingsoogpunt (i.c. de betrouwbaarheid van de gegevensverwerking) minstens zoveel, zo niet meer aandacht verdient.

De accountant dient ervan te worden doordrongen - hetgeen jammer genoeg niet in de vakliteratuur tot uitdrukking komt - dat de betrouwbaarheid van de gegevensverwerking in belangrijke mate afhankelijk is van het correct functioneren van het operating system (dit is het besturingssysteem van de computer). Hiermee wil niet gezegd worden dat de accountants zich massaal op de beveiligingsaspecten ten aanzien van het operating system moeten werpen.

In onderstaand artikel dat wij gezien het belang ervan geheel in de taal van de schrijver hebben overgenomen in Compact, wordt ingegaan op softwarepakketten waarmee data security kan worden gepleegd. Van de invloed van het besturingssysteem van de computer en de job control taal op de beveiligingsmaatregelen wordt een tipje van de sluier opgelicht. De lering uit het artikel is weergegeven in de laatste zin: "the fact that you cannot protect something completely is no reason not to make it difficult to penetrate".

Security is a warm package

At only 200 or so IBM computer sites, a new breed of software package is being put to use. These packages, designed to provide data security, bear such names as: Secure, RACF, Secure/IMS, and ACF2. They are all attempts to compensate for holes in operating systems that were never designed with the need for security in mind.

At virtually every corporate data center, measures to provide physical security against trespasses and physical attacks are employed. They make entry into the computer center impossible except by those authorized to be in the room or rooms. And systems designed to be remotely accessible employ passwords and user ID's to control access to a system. But these newer packages build upon that, restricting an authorized user's access only to specific and predetermined data sets.

For example, there's Secure, a package from Boole & Babbage of Sunnyvale, California. It allows access to certain data sets at only certain times

First they controlled access to systems. Now you can restrict authorized users only to selected data sets.

of the day. It can restrict access to TSO only or to batch only, or it can allow a person to write a data set but not scratch it. And it has such options as execute only or update only.

Similar capabilities are provided by another package, Secure/IMS, which was placed on the market recently by Software Module Marketing of Sacramento, California. It allows a security manager to determine the parameters of who can do what from which terminal, such that data entry operators, for example, would be allowed to update only certain portions of the data base and not be able to access any other part. And again, access can be restricted to only certain times of the day.

In addition, however, these packages also produce an access history of activity against protected information. They provide an audit trail of access activity, admittedly an after-the-fact sort of protection, right? "Yes, but normally no one is going to hit you the first time", says Software Module president Harris A. Herman. He explains that attempts to penetrate a system are usually made by a terminal operator at the urging of a friend. They will attempt to see what kinds of data they can gain access to, probing the system over a period of time. These probings, these attempts to browse, can be spotted and action taken in real-time. The security manager is alerted to the use of a bad password or to someone trying to access data without proper authorization - in which case the IMS master terminal operator is immediately notified.

Secure/IMS, which operates with IMS in the teleprocessing environment, logs every access to the data base from any terminal. "We even monitor the security manager", explains Herman. He says a security manager can, from his terminal, change the parameters under which someone can access the data base - perhaps staying online beyond the terminal operator's normal 5 p.m. quitting time. "But the auditor will get a report, so he will know each time the security manager is changing parameters", says Herman.

INTERRUPT

This is a tale of times long ago when the venerable Atlas 1 at Chilton possessed sixteen 1 in tape drives as its main backing store together with a high speed drum.

Being heavily used, the tape drives frequently developed errors, which involved switching the tapes from one deck to another.

One day the operators realised that a certain drive was performing particularly well as it read without errors tapes that had failed on other decks. Then a system tape failed and it was duly transferred to the "good" drive. This led to a number of very heavy operating system crashes.

It was then realised that the good deck had really been extremely naughty. For it had a fault of its own - it failed to register that it had detected bad data.

THE MORAL: All that flatters is not good. Or don't rely on hardware checks alone.

"It's not at all difficult for someone to really hurt a company very badly with some fairly simple computer-type thefts", says Shawn McLaren, director of the Cambridge Systems Group, Cupertino, California. "So a lot of people are being pressured by their managements or their auditors to make a decision on a security product."

A security manager can, from his terminal, change the parameters under which someone can access the data base.

A major New York City bank recently went through such an exercise. It was not prompted by any federal requirements, according to a spokesman in dp. Rather, the applications running, indicated that the level of security was not as high as they wanted, and so dp started a search for products available to them.

They looked closely at three of the four packages mentioned above (they don't run IMS) and settled on ACF2. Why that one? Because, according to the spokesman who asks not to be named, they thought it would require the least amount of time to achieve some acceptable level of security, and it would take the least amount of resources to get there.

When asked whether any of these packages really provide security, users and vendors alike admit that security is a function of the care exercised by individual users. Write your password down where others can see it and the system is compromised. For this reason, some packages use no external password, but instead generate them internally.

"There are two questions here", says McLaren. "One is whether you can really provide security. The other is whether you can provide a semblance of security. For some companies, a semblance of security is good enough." It is enough, he explains, to satisfy an auditor who says you must have a security product in place. "Most auditors aren't capable of distinguishing between a really good security product and one that just says it's a security product."

Banks, of course, are not the only users. Manufacturing companies, oil companies, insurance firms, and service bureaus are also mentioned by the package vendors.

McLaren's company has been selling ACF2 for six months or so, and during that time has installed 20. He figures it will have 25 out by year-end and an additional 75 next year. "The only limitation in the market, I guess, is the fact that there are only so many MVS sites out there." His package runs only with MVS.

The best seller to date is Boole & Babbage's Secure, of which some 130 are said to be installed. IBM has installed an estimated 20 of its RACF, which has been on the market the longest. Secure/IMS, on the market for only a few months, is only now being installed.

"I can see every computer system in the world having some sort of security package within the next five years", optimistically says David Tootill, senior software engineer at Boole & Babbage. The firm's product manager David L. Mosby notes that IBM doesn't enter a software market that doesn't ensure a good return on its investment. And IBM, he says, has made available in Europe an enhanced version of RACF.

Harris Herman foresees an active interest in data security by users in the late 1979 - early 1980 timeframe, when he foresees legislation requiring some level of security in systems. It's a new technology and a young market that is only now getting set to take off. "People all know they have a security problem", says Herman. "But they're approaching it first, I guess, with physical security."

For now, it seems, these retrofits are the best that users can hope for. But Robert P. Abbott, president of EDP Audit Controls in Oakland, California, says vendors are working on new systems in which security has been designed in from the beginning. And they're going to be tough, he says.

"The biggest holes today are through the JCL", Abbott notes. Many changes to the operating system today are motivated by the wish to improve the facilities of the job control language, he explains. "That's where the weak link is right now, and it'll be that way when these new systems come out." Five years after these new systems come out, Abbott says, he'd like to have the intimate knowledge of how they work that he does of today's systems. "I'd be very interested in seeing whether the constant changes to operating systems, the improvements, the new releases erode the security that was in the first versions. That's where the problem is going to be." The reason, he adds, is that people who do the maintenance on those systems will not be the same people who designed them, and thus they won't know why all those functions are in the operating system.

Abbott, who earlier had studied security flaws that exist in numerous operating systems for the Defense Department (February 1974, p. 90), says of access control software: "Some of them have as many holes in them as the holes they're trying to correct."

And a dp executive with a manufacturing firm admits that "a good systems programmer can get to anything. I don't think you can protect against that".

But this is perhaps best placed into perspective by Boole & Babbage's David Tootill: "the fact that you can't protect something completely is no reason not to make it difficult to penetrate".

Edward K. Yasaki

Datamation, december 1978

Techniek

Steeds worden nieuwe technische snuffjes bedacht om iemand bijvoorbeeld de toegang tot iets te ontzeggen. De twee volgende artikeltjes geven elk een nieuwe uitvinding weer. De ene verkeert nog in een experimenteel stadium.

De eerste uitvinding - minizendertje - heeft de prettige bijkomstigheid dat minder gewenste personen op afstand worden gehouden. De tweede - veiligheidssysteem met weggooisleutels - zal elke accountant met argwaan bekijken. Alles wat de mogelijkheid biedt om weggegooid te worden zonder een spoor (trail) achter te laten is per definitie verdacht.

Minizendertje opent deuren

Mastiff Security Systems Ltd. in Engeland heeft onlangs met de K9 een nieuw elektronisch produkt op de markt gebracht, dat een goedkopere en vereenvoudigde versie is van het Mastiff-systeem, een automatische toegangscontrole. Het zeer geavanceerde Mastiff-systeem vindt succesvol toepassing in veel Europese landen en in Canada. Varel in Roermond, de Nederlandse alleenvertegenwoordiger van Mastiff, brengt K9 in ons land uit. Met dit produkt worden deuren naar vertrouwelijke ruimten automatisch geopend, uitsluitend voor bevoegde medewerkers. Deze mensen hebben een miniatuurzendertje bij zich; zodra zij een beveiligde deur naderen, gaat deze automatisch open. De medewerker heeft zijn handen vrij en kan met boeken, tekeningen of ontwerpen in de hand ongestoord naar binnen gaan. Achter hem sluit de deur zich weer automatisch. Onbevoegden kunnen zich geen toegang verschaffen tot de aldus beveiligde ruimten.

Het produkt is ook geschikt voor het afschermen van drukbezette medewerkers tegen te veel inloop van ongenode bezoekers op zijn kamer. Door slechts een select groepje naaste medewerkers te voorzien van een K9-zendertje wordt bereikt, dat hij zich beter kan concentreren op zijn werk.

K9 is overall interessant waar slechts een deel van het personeel toegang heeft tot bepaalde ruimten. Dat kunnen laboratoria en computerruimten zijn, maar ook directiekamers, archieven en ontwerpafdelingen en tevens vertrekken waar geld of waardevolle goederen liggen.

K9 kan voor vrijwel elk type deur worden toegepast. Het zendertje van zeer geringe afmetingen wordt in de zak gedragen of met een klem aan de kleding gestoken. Bij het verlaten van het bedrijf steekt de medewerker het in een daarvoor bestemd kastje. Hij heeft een sleutel om zijn zendertje er weer uit te kunnen pakken. Tijdens zijn afwezigheid wordt het weer geladen. Een gestolen zendertje werkt na korte tijd niet meer, terwijl een ontbrekend zendertje in het opbergkastje meteen opvalt.

Er zijn een groot aantal variaties mogelijk op het codesignaal dat het zendertje geeft, zodat veel veiligheid kan worden ingebouwd.

De grote kracht van het systeem zit echter in het feit, dat men de handen vrij heeft. Het hanteren van sleutel of een gecodeerd "toegangskaartje" wordt vaak als hinderlijk ervaren met als resultaat, dat veel deuren naar beveiligde ruimten worden opengelaten.

De Automatisering-gids, 25 jan. 1979

Veiligheidssysteem met weggooisleutels

Het Amerikaanse onderzoeksbureau Arthur D. Little ontwikkelt een nieuw elektronisch veiligheidssysteem, waarbij door microprocessors bewaakte sloten met van goedkoop materiaal vervaardigde weggooisleutels geopend kunnen worden. Elke sleutel heeft een uniek combinatiepatroon, dat door veranderingen in de code steeds door de sleutelbeheerder gewijzigd kan worden. In elk slot is een goedkope microprocessor met geheugen gemonteerd, die - bij wisseling van sleutels - telkens opnieuw geprogrammeerd wordt en afgestemd op de nieuwe sleutel.

Het systeem dat met name de veiligheid in hotels en industriële ondernemingen aanzienlijk kan verhogen, verkeert in de laatste experimentele fase. Voor het systeem is in de Verenigde Staten en in Engeland patent verleend, in Japan is het aangevraagd.

De Automatisering-gids, 25 jan. 1979

Controlle

Gebruikersdocumentatie

Een hoopgevende ontwikkeling in het automatiseringsgebeuren is dat steeds meer automatiseringsafdelingen overgaan tot de ontwikkeling van een handboek automatisering, waarin naast organisatieschema en functie- en taakbeschrijvingen van automatiseringspersoneel de procedures en voorschriften, die dienen te gelden in de organisatie van de gegevensverwerking (= het computercentrum) en in die van de ontwikkeling van informatiesystemen worden opgenomen. Hierin dienen dan ook de algemene richtlijnen te worden opgenomen waaraan de documentatie dient te voldoen. Een onderdeel van de documentatie wordt gevormd door de gebruikersdocumentatie.

Gebruikersdocumentatie is het geheel van vastleggingen dat voor praktische aanwending ter beschikking staat van de gebruikers van een geautomatiseerd informatieverzorgend systeem.

De gebruikersdocumentatie moet degene die deze hanteert inzicht geven in het systeem en hem zodanig instrueren met betrekking tot de door hem te verrichten handelingen dat het systeem optimaal en doeltreffend kan functioneren.

Dit betekent dat de gebruikersdocumentatie

- praktisch aanwendbaar moet zijn;
- de gebruiker inzicht moet geven in het systeem voor zover noodzakelijk is voor een goede taakuitoefening;
- de gebruiker moet instrueren met betrekking tot de door hem te verrichten handelingen welke deel uitmaken van het systeem.

In het algemeen wordt eerst de documentatie van het systeem als geheel gegeven en - indien nodig - van de afzonderlijke, duidelijk te onderkennen delen: de subsystemen.

Voor de indeling naar subsystemen wordt meestal gekeken naar de computerverwerking binnen het systeem.

Een andere indeling in subsystemen is die naar de administratieve procedures waarbinnen de computerverwerkingen op organische wijze zijn ingepast. Het voordeel hiervan is dat de gebruikersdocumentatie aansluit op de dagelijkse taakuitoefening van de gebruiker en in feite onderdeel is van de functie-/taakbeschrijvingen en instructies binnen de organisatie.

De hierna opgenomen "Beschrijving gebruikersdocumentatie" berust op de "eerste indeling" en is geschikt zowel voor systemen als "subsystemen". Daarnaast is de beschrijving gericht op het documenteren van gebruikersdocumentatie bij batchgewijze verwerking.

Beschrijving gebruikersdocumentatie

Geautomatiseerd informatieverzorgend (sub)systeem

- a. TITELBLAD (naam van het systeem, geleideblad laatste wijziging, datering van de documentatie, distributie)
- b. DOEL van het systeem
- c. SAMENHANG MET ANDERE (SUB)SYSTEMEN / VERDELING IN SUBSYSTEMEN
- d. WERKING
 - stroomschema
 - beschrijving
 - condities
 - acties
 - rekenregels
 - controles
- e. BESTANDEN (GEGEVENSVERZAMELINGEN)
- f. INPUT (GEGEVENS)
Per input:
 - naam, formuliernummer, doel
 - voorbeeld, ingevuld, toelichting
 - controles
 - signaleringen
- g. PROCEDURES TEN BEHOEVE VAN INVOER, CORRECTIE, AFHANDELING
 - beschrijving
 - behandelingsschema
 - toelichting
 - instructie per handeling
 - verantwoordelijkheid
- h. OUTPUT (INFORMATIE)
per output:
 - naam, doel, voorbeeld, toelichting
 - distributie
 - frequentie
 - signaleringen
 - afhandeling
 - verwijzing naar correctieprocedures

i. TIJDSHEMA

- aanlevering gegevens
- planning verwerking
- oplevering output

j. BETROUWBAARHEID

- maatregelen van interne controle en beveiliging
- netwerk van controletotalen

In de gebruikersdocumentatie bij online-systemen dienen nog tenminste de volgende zaken te worden gedocumenteerd:

- (uitgebreide) beschrijving van de apparatuur,
- uitgebreide instructies om de apparatuur te gebruiken,
- correctieprocedures,
- onderkenning en behandeling van storingen,
- herstart procedures,
- dagelijks en technisch onderhoud,
- beveiliging (gebruik van codes en dergelijke) en controle.

LITERATUUROVERZICHT

door B.M. de Vries

In de A.C.-bibliotheek opgenomen boeken

Dit keer geven wij een nadere toelichting op een tweetal boeken, te weten:

- AC 187 Policy issues in data protection and privacy - Rapport 10
Publikatie OECD, 1978 (Engels, 322 blz.)

This publication constitutes the proceedings of the Seminar on Data Protection and Privacy held at OECD from 24 - 26 June, 1974. The initiative to hold the Seminar came from the Data Bank Panel created by the OECD Computer Utilisation Group in order to study policy issues arising from the widespread use of computerised data banks.

The subjects proposed for discussion during the Seminar met with great interest from many well-known experts in the field, who agreed to make major contributions to the discussions.

The objective of the Seminar was to highlight a range of policy options relating to data protection and privacy at a time when intensive efforts were being made in many OECD Member countries with a view to preparing appropriate legislation.

The options expressed in the various papers are those of the participants and authors and do not necessarily reflect the views of the Data Bank Panel or the Computer Utilisation Group members, their governments or the OECD Secretariat.

The Synthesis Report has been reviewed by the Data Bank Panel, but responsibility for reflecting correctly the discussions at the various sessions lies with its authors. It has not been submitted formally to Member governments for approval and should not therefore be construed as constituting their official policies or opinions.

The success of the Seminar must be attributed to the dedicated, active and keen participation of its Chairmen, experts and members. To them the organisers of the Seminar wish to express their gratitude.

- AC 197 Audit considerations in electronic funds transfer systems -
Auditing Electronic Funds Transfer Systems Task Force - AICPA,
1978 (Engels, 24 blz.)

Almost 37 billion checks will be written per year by 1980 to pay personal, commercial and governmental obligations. During recent years, financial institutions have been experimenting with and, in many cases, implementing new systems designed to reduce the need for "paper based" payments. Through the application of computer and communications technologies, these institutions are developing systems that transfer funds electronically rather than physically - electronic funds transfer systems (ETFS).

Initially, these new systems were limited in terms of the services provided and restricted in geographical area and so did not figure clearly in the future of electronic banking.

Today, however, these systems are growing rapidly and are impacting far larger numbers of consumers and businesses, as the following examples illustrate. A large New York bank recently installed approximately five hundred remote-banking terminals throughout its branch network, and an additional 3,500 terminals in retail stores. In California, a new centralized switching network is being installed on a cooperative basis by a group of ninety-two savings and loan associations to allow the transfer of funds between participating merchants' and customers' savings accounts.

Similar networks have been formed in several other states. And, as a final example, thirty-two separate automated clearing houses currently are clearing funds transactions electronically rather than through the physical movement of paper payment instruments.

EFT systems do not employ totally new technology, but rather, adapt existing technology to provide a new method for exchanges of value. This adaptation does not represent revolutionary, but rather an evolutionary, change in auditing requirements or procedures.

These and other current developments as well as the potential for changes in the near future have led to the development of this paper. The computer services executive committee of the AICPA requested it to ascertain the state of the art in electronic funds transfer systems and to determine the impact these systems will have on the audits of business entities involved in EFTS.

This guide is divided into four chapters. The first chapter addresses the nature of EFT systems and provides background information on EFTS; chapters 2 and 3 cover the current status of EFTS in government and the legal community, respectively; and the final chapter discusses the task force's initial assessment of the audit impacts of EFT systems and is designed to present comments and suggestions for further research and professional deliberation.

Uit de tijdschriftenliteratuur

Designing the data base - D.C. Tsichritzis en F.H. Lochovsky

Datamation (augustus 1978)

Trefwoord : A 62

Data base generation should not be regarded as a conversion problem, but as an opportunity to plan the organization, use, and management of the data.

Most DBMS vendors recognize the critical role of data base generation, and provide utilities to help the data base administrator generate the data base appropriately. However, these utilities are not universal. The successful generation and implementation of a data base calls for a carefully organized plan. The basic steps in such a plan are:

1. Identify the data organization requirements of the enterprise

Data organization requirements are best identified by conducting a series of interviews within the various user departments. These may be conducted informally, or through questionnaires. Either way, several interviews may be required in each department to clarify needs and resolve apparant conflicts. The result of the process is a list of all the entities of interest to each department, and the relationships between entities. Merging the lists for the different departments generates the first iteration toward establishing a data dictionary of all data base names and their meaning. While merging the lists we need to resolve name conflicts, isolate candidate keys (unique identifiers) and check for functional dependency properties. After merging the lists, the aggregate list is shown to the various departments for their approval. A relationship is a known correspondence between two entities. It is a fact or condition which links one entity to another entity. From the list of entities and the relationships between them, we now produce an enterprise description. The enterprise description is a synthesis of the data requirements of each department with redundancy eliminated. The enterprise description can now be documented. It is important to identify the data organization requirements of an enterprise as the users perceive them or would like them to be.

2. Identify the data processing requirements of the enterprise

All current and projected transactions on the data base are included. For each transaction it is necessary to identify its nature (retrieval, update), its frequency, its origin (department), and its purpose together with the part(s) of the data base it affects. The result of this step is a list of all transactions and their characteristics.

3. Generate the schema(s)

The enterprise description is next expressed as a data model schema, a graphical description of the proposed schema according to the data model of the DBMS under consideration.

Existing commercial DBMS's can be grouped into three main categories: hierarchical, network, or relational.

For a hierarchical system the enterprise description is transformed into a set of spanning trees of the network. Each data base transaction should be reflected as a navigation through these trees.

For a network system the enterprise description must be transformed into a data structure diagram. Each data base transaction is mapped into a navigation through the data structure diagram.

For a relational system the enterprise is transformed into a relational schema. Data base transactions are mapped into relational operations on the base relations.

The result of transforming the enterprise description into a data model schema according to a particular DBMS approach represents a documentation of the data base structure. The schema(s) and navigational sketch(es) should again be discussed with the different departments in order to obtain their approval.

The final choice of a particular approach, DBMS, and schema may hinge on several factors. There are three possibilities:

- 1) a DBMS may have already been selected on the basis of hardware, economic, political, or other considerations;
- 2) after completion of the data model generation for each approach, the results may point to an obvious choice; and
- 3) there may be no obvious best choice for data model schema.

After a choice has been made, the data model schema and outline of transactions are used for the actual conversion process.

4. Convert the data organization and processing operations to the DBMS environment

The physical generation of the data base consists of a phased plan which involves:

- 1) relating existing data to the data model schema;
- 2) writing the data definition language (DDL) programs which will implement the DBMS schema;
- 3) loading the data according to the schema as described by the DDL programs, either from existing files or from newly generated data;
- 4) implementing each application using the data manipulation language (DML) of the DBMS according to the outline of the data base transactions; and
- 5) testing and running each application.

A phased plan for conversion is necessary. The plan should provide for parallel operations of the current and proposed systems, and for checkpoints. It should also list the conversion utilities needed, indicating whether they will be provided by the vendor or produced in-house.