M ten Wolde

# compact

## COMPUTER EN ACCOUNTANT




Klynveld Kraayenhof & co
ACCOUNTANTS

HERFST 1976 3E JAARGANG NR. 2


9

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,
D. Steeman en J.H. Urbanus.

Adres: Pr. Irenestraat 59 Amsterdam

## VAN DE REDACTIE

Bij het verschijnen van het najaarsnummer van de derde jaargang verwelkomen wij een groep nieuwe lezers, namelijk de cursisten van de automatiseringscursus 1976. Wellicht is dit het goede moment de doelstelling van Compact, zoals deze is weergegeven op het schutblad van dit nummer, nogmaals te belichten.
"Het verstrekken van informatie" veronderstelt ook een behoefte aan informatie; deze behoefte kan de redactie alleen onderkennen uit reacties, problemen en ervaringen van de lezers.
Zou het niet goed zijn in Compact bijvoorbeeld tot een discussie te komen over de automatiseringscursus, waarbij zowel de inhoud van de cursus als het nut ervan voor de controlepraktijk naar voren komt?
Of in het ongunstigste geval, U met problemen blijft zitten?
U kent het adres van de redactie.

In dit nummer worden twee onderwerpen belicht, namelijk "Verzamelingen in data bases" door A.H.C. Koedijk en "Gegevensbeveiliging", een bespreking door J.F.C. van Epen van een drietal artikelen in Informatie (september 1975).
Indien U zich in de besproken materie wilt verdiepen dan kunt U de aangehaalde literatuur verkrijgen bij de A.C.-documentatie.

# VERZAMELINGEN IN DATA BASES

door A.H.C. Koedijk

Dit artikel is geschreven naar aanleiding van de voordracht van prof. ir. G.M. Nijssen tijdens de NOVI-workshop Data Base Technologie en is mede gebaseerd op de daar verstrekte documentatie.


## Korte inhoud

Uitgaande van een uiterst omvangrijke werkelijkheid kan men via waarneming, selectie en classificatie komen tot een referentiekaderschema. Hierbij wordt opgemerkt dat computertechniek op de totstandkoming van een referentiekaderschema geen invloed heeft. De gegevens in een data base en de relaties tussen deze gegevens, het referentiekaderschema, kunnen worden weergegeven door de gegevens te classificeren in verzamelingen en door de relaties tussen die verzamelingen, gebaseerd op de behoeften van de gebruiker aan te geven.
Tevens moet in de relaties het unieke gegeven (of de unieke combinatie van gegevens) dat (die) wezenlijk relatiebepalend is, aangegeven worden.
Een van de problematische verschijnselen waar de accountant in de automatisering op stuit is de data base. Het problematische effect wordt onder meer veroorzaakt door een gebrekkige communicatie tussen hem en de automatisering-specialist. De specialist heeft te maken met computertechniek, de gebruiker en ook de accountant, en is slechts geïnteresseerd in gegevens. De laatsten willen met de computertechniek van de data base liever geen kennis maken.


## Gemeenschappelijke taal

Er bestaat behoefte aan een gemeenschappelijke probleem(structuur)beschrijvende taal voor de gebruiker (en daarmee ook de accountant) en de specialist te zamen. Een taal die, om manipuleren met gegevens te kunnen begrijpen, kennis van computertechniek overbodig maakt.
Een taal die zowel de accountant als de specialist begrijpt, zodat "vertaalwerk" tussen de twee categorieën mensen, alsmede onbegripvergrotende onjuistheid en onvolledigheid van dit vertaalwerk tot een minimum worden teruggebracht. Wil dit doel bereikt worden, dan dient aan een voorwaarde, namelijk die van eenvoud, te worden voldaan. Er zal gebruik gemaakt moeten worden van eenvoudige vaardigheden die elk mens zich - veelal onbewust - heeft eigen gemaakt.

## Geen computertechniek?

Is het nu inderdaad zo dat een accountant, als hij een middel ter beschikking heeft om de manipulaties met gegevens op eenvoudige wijze te doorgronden en vast te leggen, geheel ontlast is van de technische problemen?

Wanneer de accountant zich een oordeel wil vormen over de mate van interne controle in een bepaald geautomatiseerd systeem, dan kan hij zich niet beperken tot een a-technisch model van dat systeem alleen.

De feitelijke werking wordt in belangrijke mate wel degelijk bepaald door de techniek.
Het grote voordeel van een a-technisch model is evenwel, dat het kan dienen als intermediair, als gemeenschappelijk referentiekader, voor de controlerend accountant en de op automatisering gespecialiseerde A.C.-accountant, die hem met betrekking tot de technische problemen bijstaat.

## Vaardigheden

Een voor het onderhavige onderwerp relevante menselijke vaardigheid is classificeren. De meeste mensen passen deze "techniek" waarschijnlijk minder bewust toe. Het toekennen van bepaalde eigenschappen aan mensen en die vervolgens "een etiket opplakken" is in feite classificeren.

## Verzamelingen

Een gemeenschappelijke taal, die aan de eis van eenvoud voldoet, is in dit artikel beschreven. Deze taal maakt gebruik van de grondbeginselen van de verzamelingenleer, een wetenschap die in het huidige onderwijs de basis vormt van de wiskunde; een wetenschap derhalve die in lagere klassen van basisscholen reeds wordt gedoceerd en waarvan de begrippen eenvoudig duidelijk te maken zijn.

## Schema's en tabellen

Het zal verhelderend werken indien wij onze gegevens en de relaties ertussen in beeld kunnen brengen. Er is dus behoefte aan een methode om dit te bereiken, bijvoorbeeld om verbale teksten te schematiseren. Ook in het basisonderwijs wordt de verzamelingenleer in belangrijke mate met behulp van plaatjes verduidelijkt.
In de hierna beschreven gemeenschappelijke taal wordt tevens gebruik gemaakt van het gemak waarmee een mens "in tabellen" kan denken.

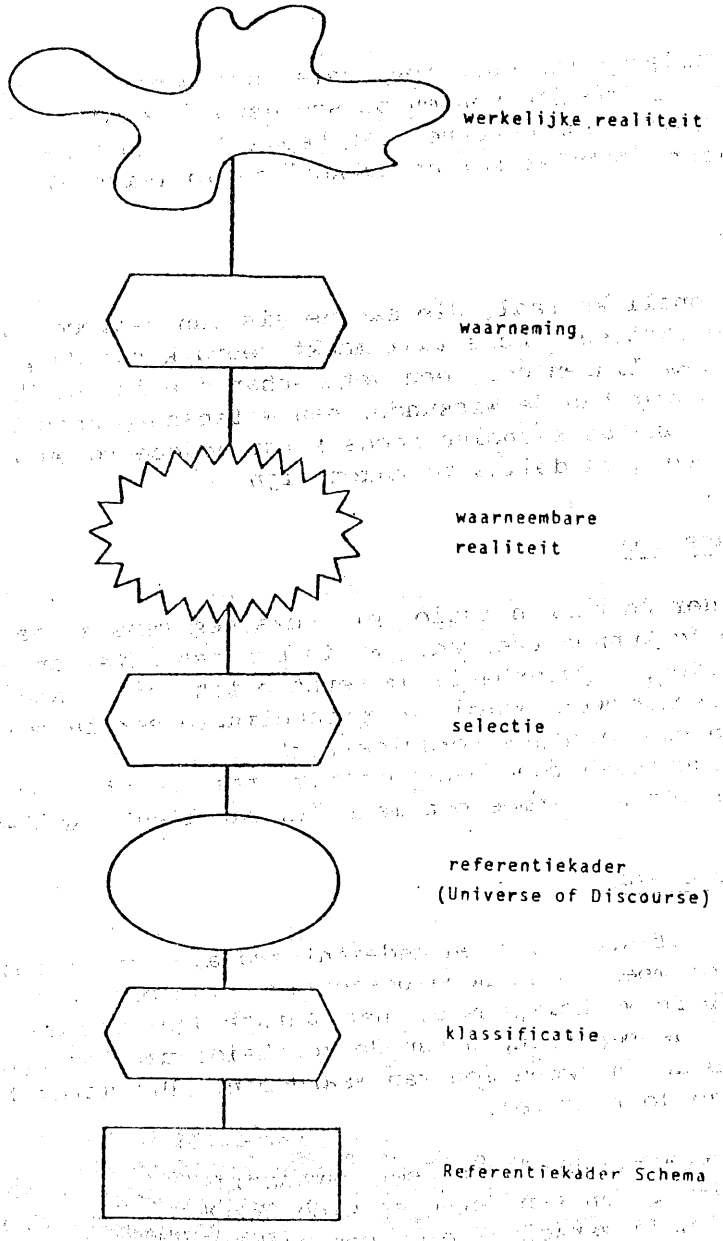
## Referentiekaderschema

Een data base wordt door Nijssen gedefinieerd als een verzameling gegevens die een of meer toestanden beschrijven van een gekozen gedeelte van de waarneembare werkelijkheid. Het laatste deel van deze definitie vloeit voort uit de beperkingen van de mensheid: men kan zich met niet meer bezighouden dan hetgeen men kan waarnemen. Dit wordt bepaald door de stand van de techniek.

De waarneembare werkelijkheid is zeer omvangrijk. In de praktijk houdt een persoon of een groep van personen zich bezig met een klein gedeelte van deze waarneembare werkelijkheid: men selecteert, kiest een deel. Men houdt zich dan verder bezig met gegevens behorende tot dit gekozen gedeelte van de waarneembare werkelijkheid, door Nijssen genoemd het "referentiekader" (vertaling uit het Engels van "Universe of discourse").

Zo'n referentiekader kan een groot aantal elementen omvatten. Om het geheel te kunnen overzien moet de mens gebruik maken van zijn vermogen tot classificeren. Via een classificatieproces komt hij tot een overzichtelijk beeld van hetgeen hij moet overzien, het referentiekaderschema.

Het bovenstaande is in de volgende figuur weergegeven.



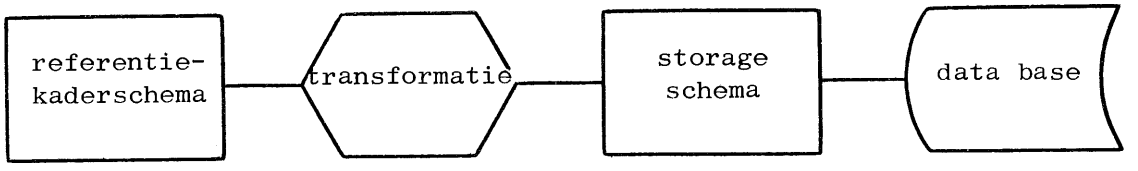

figuur 1

Een voorbeeld: Van 1.950.000 elementen, te weten 1 miljoen personen, 500.000 auto's en 450.000 wegenbelastingbetalingen kan men komen tot 3 klassen: personen, auto's, betalingen.

## Referentiekaderschema vs computertechniek

Het referentiekaderschema bevat slechts zaken die betrekking hebben op gegevens uit de data base. Het beschrijft de klassen van elementen in de data base (verzamelingen) en de relaties tussen die klassen.

Dit staat los van de wijze waarop de elementen werkelijk in de geheugens van computers zijn opgeslagen. Naast het referentiekaderschema moet er derhalve nog een opslagschema zijn, dat de werkelijke organisatie van de gegevens (elementen) aangeeft. Dit schema wordt in de literatuur veelal Storage Schema of Internal Schema genoemd. Tussen dit schema en het referentiekaderschema zal een transformatieproces moeten staan (figuur 2). Het referentiekaderschema is van belang voor controlerend accountant zowel als A.C.-accountant. Het transformatieproces en het storage schema liggen op het terrein van de A.C.-accountant, die op automatiseringstechniek gespecialiseerd is.




figuur 2

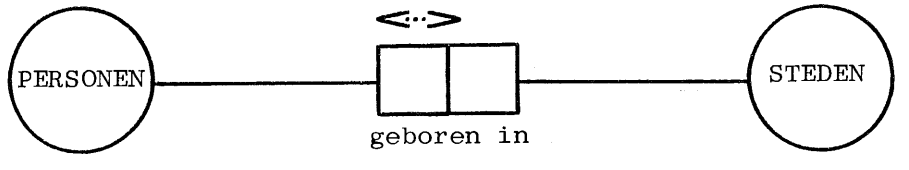
De verwachting is, dat Data Base Management Systemen in de toekomst op dit concept gebaseerd zullen zijn: gegevensmanipulatie staat los van gegevensopslag.

## De "taal"

Thans komen wij toe aan een methode om een referentiekaderschema weer te geven, gebruik makend van

- classificatie
- verzamelingen
- "plaatjes"
- tabellen.

Indien een (kleine) data base bestaat uit een aantal personen met hun geboorteplaatsen, dan kan het referentiekaderschema als volgt worden weergegeven:




figuur 3

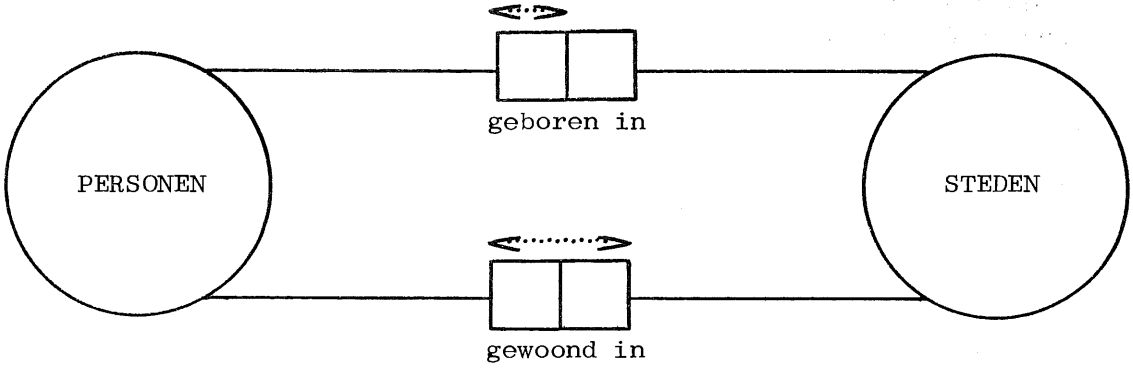
De elementen (dat kunnen er vele zijn) van deze data base zijn onderverdeeld in twee klassen (verzamelingen): Personen en Steden. Een verzameling wordt aangegeven door een bol. Een vierkantje geeft een element aan uit de verzameling waarmee dit verbonden is. Door middel van het gestippelde pijltje wordt het unieke element in de relatie "PERSONEN geboren in STEDEN" aangegeven, in dit geval de Persoon. Immers, een persoon kan in slechts één stad geboren zijn. De persoon is derhalve het unieke element van de relatie.

Het bovenstaande kan met een tabel verduidelijkt worden:

| Personen | Steden |
|---|---|
| 1 | A |
| 2 | B |
| 3 | A |
| 4 | C |

Het zal duidelijk zijn, dat een stad meerdere keren kan voorkomen: in een stad kunnen meerdere personen geboren zijn. Stad is dan ook niet een uniek element in deze relatie.

Indien een gebruiker behoefte heeft aan kennis omtrent de steden waar de personen gewoond hebben, dan kan het referentiekaderschema eenvoudig uitgebreid worden met een nieuwe relatie tussen de verzamelingen Personen en Steden:

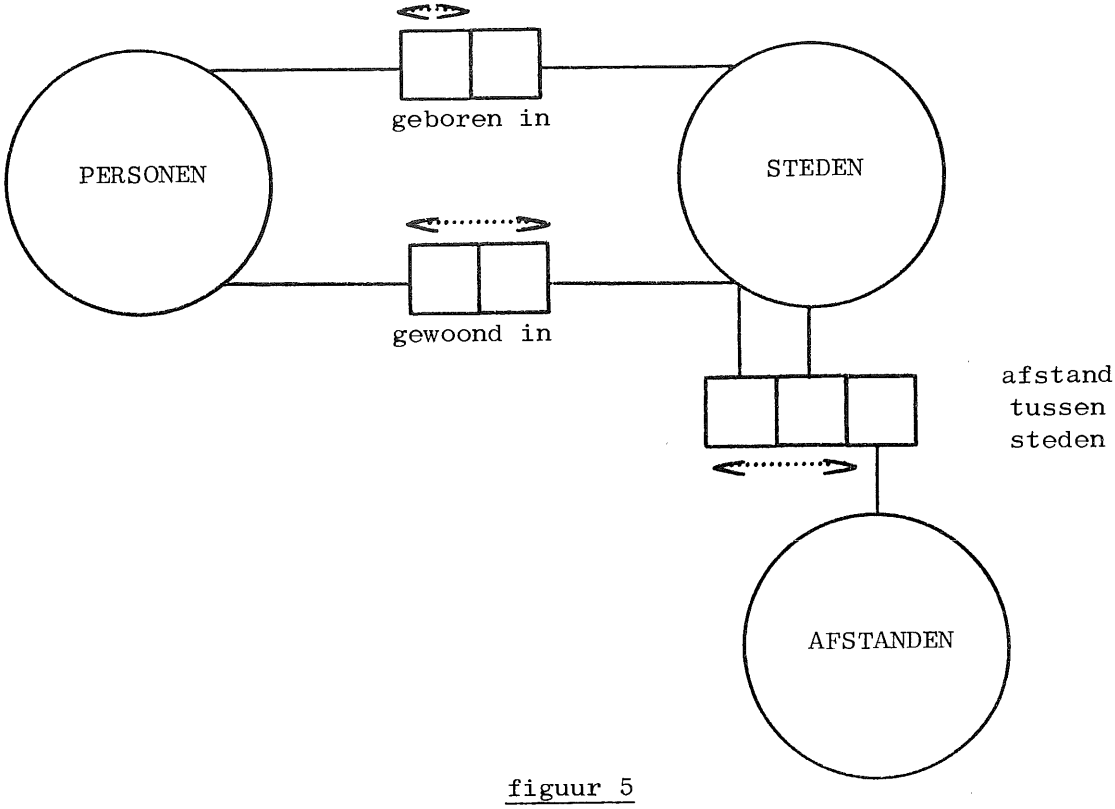



figuur 4

Uit het pijltje in de relatie "PERSONEN gewoond in STEDEN" blijkt, dat de combinatie van elementen Persoon en Stad uniek is. Immers, een persoon kan in meerdere steden gewoond hebben. Een persoon kan thans derhalve eveneens meerdere keren voorkomen in de tabel, echter een combinatie Persoon - Stad slechts één keer:

| Personen | Steden |
|---|---|
| 1 | A |
| 1 | B |
| 2 | B |
| 3 | A |
| 3 | C |
| 4 | D |

Ook de afstand tussen steden kan eenvoudig in ons schema worden opgenomen:




figuur 5

Er is een nieuwe verzameling toegevoegd: Afstanden. Vervolgens is de relatie tussen Steden en Afstanden aangebracht. In deze relatie "Afstand tussen Steden" is de combinatie van elementen Stad - Stad uniek (een afstand wordt bepaald tussen twee steden), hetgeen verduidelijkt wordt in de volgende tabel:

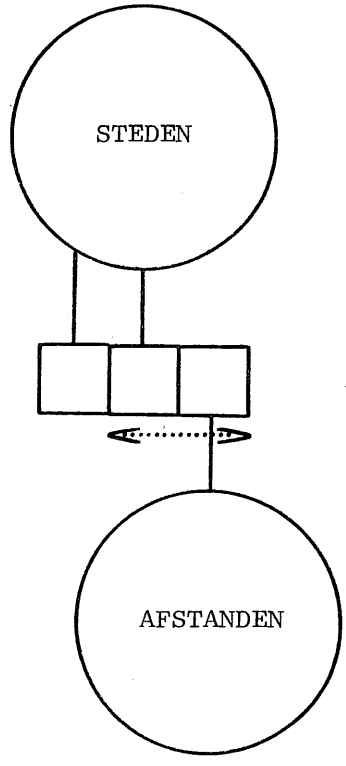
| Stad 1 | Stad 2 | Afstand |
|---|---|---|
| A | B | 100 |
| A | C | 200 |
| B | C | 150 |
| B | D | 150 |

De vragen die met behulp van deze relatie beantwoord kunnen worden, zijn:

a. Wat is de afstand tussen Stad 1 en Stad 2?

b. Welke combinaties van twee steden liggen op afstand x van elkaar?

Men kan zich de tweede vraag, vraag b, ook geconditioneerd voorstellen: Welke steden liggen op afstand x van elkaar, waarbij Stad 1 is A. Met andere woorden: Welke steden liggen op afstand x van stad A? Deze vraag is echter met behulp van de aangegeven relatie niet op te lossen. Wij hebben in onze relatie immers aangegeven, dat de combinatie van elementen Stad - Stad uniek is. In dit verband houdt uniek tevens in: relatiebepalend. We kijken naar figuur 6.



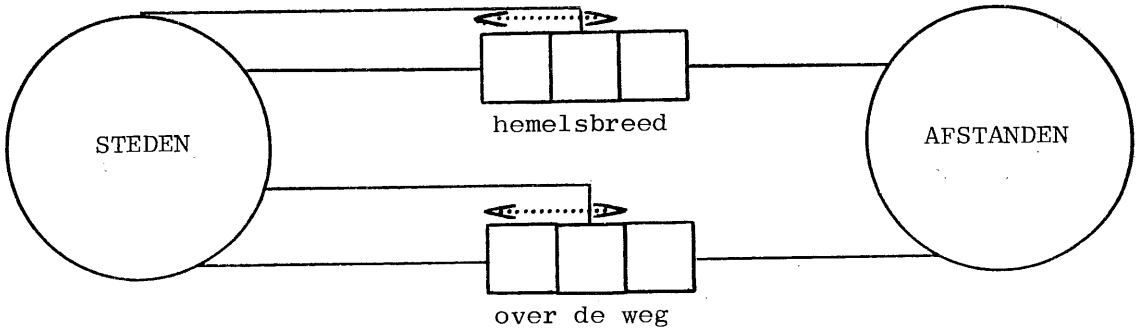

figuur 6

In figuur 6 is tussen de verzamelingen Steden en Afstanden de volgende relatie aangebracht: steden die op een bepaalde afstand van een bepaalde stad liggen. Thans kan onze laatste vraag eveneens beantwoord worden! We zien, dat het unieke element of de unieke combinatie van elementen in een relatie tevens relatiebepalend is!

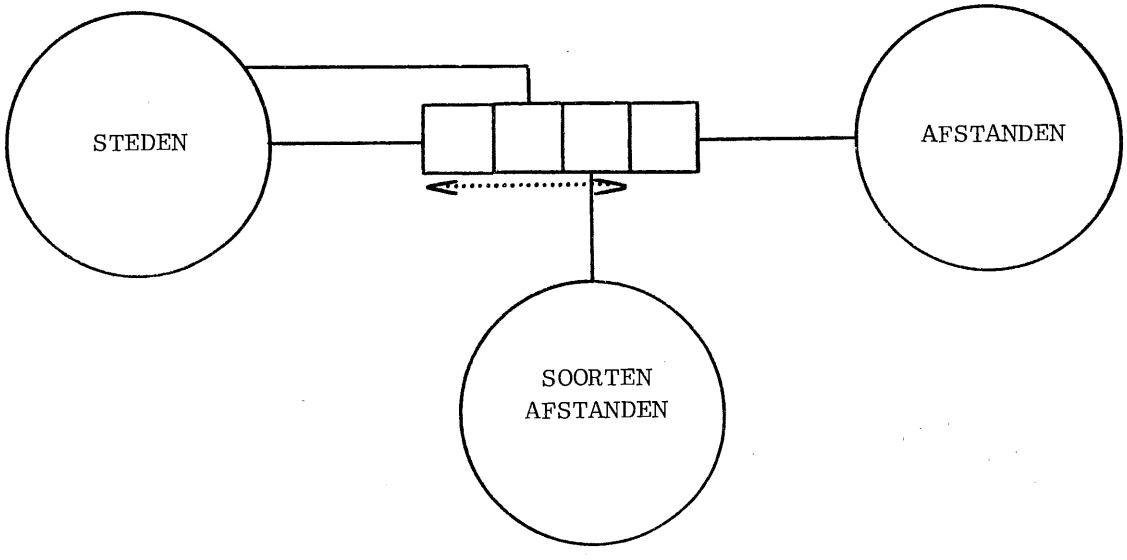
In tabelvorm kan dit verduidelijkt worden:

| Stad 1 | Afstand | Stad 2 |
|---|---|---|
| A | 100 | B |
| A | 200 | C |
| B | 100 | A |
| B | 150 | C |
| B | 150 | D |
| C | 200 | A |
| C | 150 | B |
| D | 150 | B |

Ter afsluiting van ons voorbeeld: Indien de gebruiker de afstanden tussen steden wil onderscheiden in "hemelsbreed" en "over de weg", moeten wij ons schema weer iets uitbreiden; dit is in principe op twee manieren mogelijk:




figuur 7a




figuur 7b

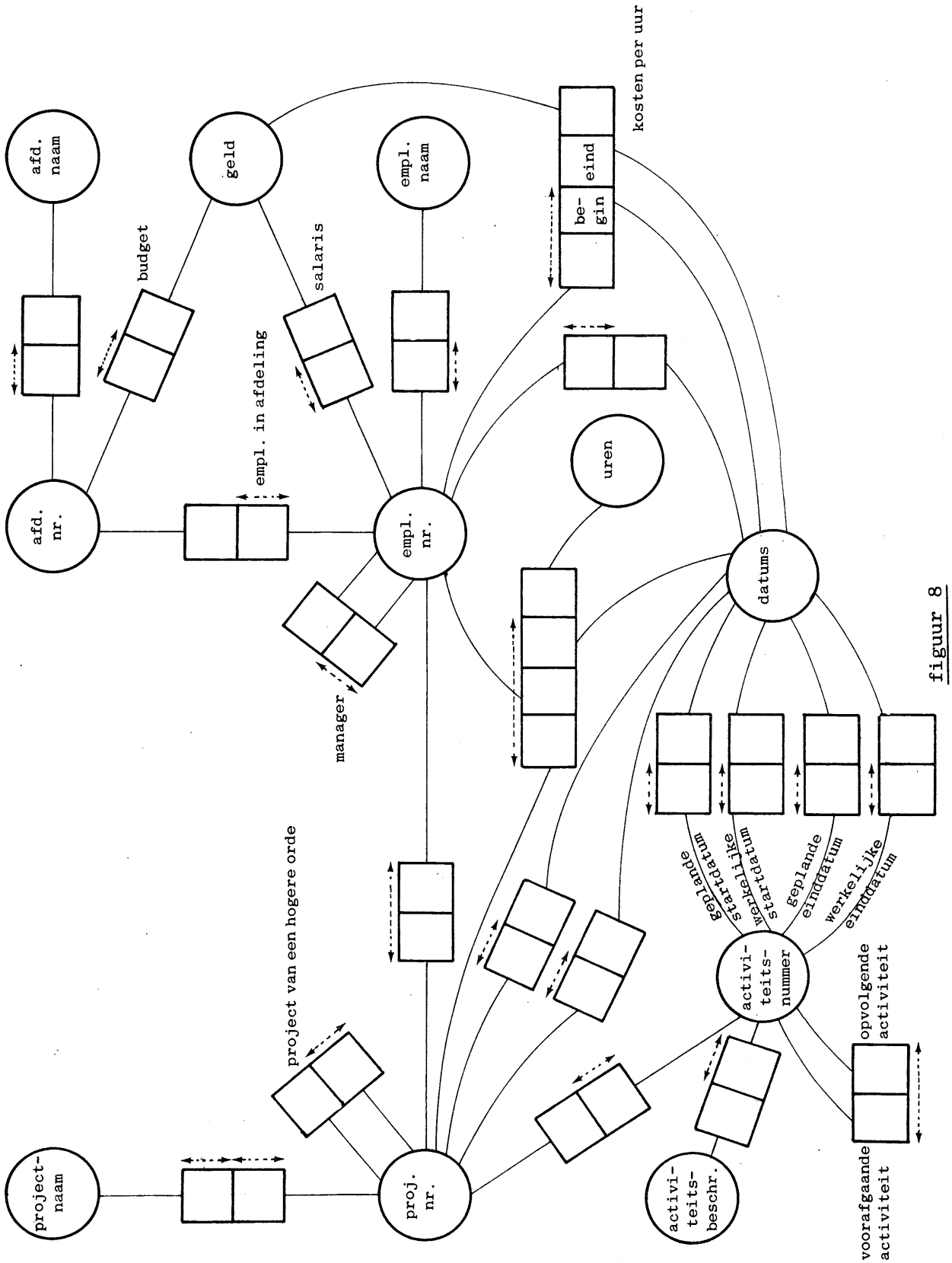
Hierbij kan worden opgemerkt, dat bij de tweede oplossing (figuur 7b) eenvoudiger meer soorten afstanden kunnen worden toegevoegd.

## Toch computertechniek?

Het is duidelijk, dat bij een grote data base het referentiekaderschema eveneens groot wordt en daardoor te ingewikkeld om te hanteren. Hiervoor zal dan ook de computer moeten worden ingeschakeld. De computer fungeert dan echter als een hulpmiddel om het a-technische model van de data base te hanteren en te administreren.

## Voor de liefhebber

Voor U is, tot slot, in figuur 8 nog een voorbeeld gegeven van een iets uitgebreider referentiekaderschema.


afd. naam
geld
empl. naam
kosten per uur
budget
salaris
be- gin
eind
empl. in afdeling
afd. nr.
empl. nr.
uren
manager
datums
project van een hogere orde
gepland startdatum
werkelijke startdatum
geplande einddatum
werkelijke einddatum
activi- teits- nummer
opvolgende activiteit
project- naam
proj. nr.
activi- teits- beschr.
voorafgaande activiteit

figuur 8

# GEGEVENSBEVEILIGING

door J.F.C. van Epen

In september 1975 is van het tijdschrift Informatie een speciale uitgave verschenen gewijd aan Gegevensbeveiliging.
Op verzoek van de redactie van Compact zijn excerpten gemaakt van die artikelen die van belang zijn voor de accountantspraktijk.

Het eerste uittreksel van het artikel "Begrip en praktijk van EDP-auditing" door D. Steeman en J.H. Urbanus is reeds geplaatst in het zomernummer 1976 van Compact.

Thans vragen wij Uw aandacht voor de excerpten van de volgende artikelen:

- A systematic approach to data security (R.H. Courtney)
- Gegevensbeveiliging in Data Base Management Systemen (ir. C.H.C. van de Sandt)
- Beveiligingsaspecten rondom een data base: Een voorbeeld uit de praktijk (drs. R.J. Romein en ing. W. Visser).

## A systematic approach to data security (R.H. Courtney)

In dit artikel tracht Courtney de lezers bewust te maken van een mogelijke benadering van het beveiligingsprobleem. Hij rangschikt daartoe zowel de problemen als mogelijke oplossingen systematisch.
De conclusie luidt na ampele overweging, dat voor het vraagstuk van de gegevensbeveiliging helaas geen standaardoplossing kan worden gegeven. Voor elk informatiesysteem moeten de beveiligingsmaatregelen afzonderlijk worden bepaald.
Courtney definieert gegevensbeveiliging als volgt: "Data security refers to the safety of data from all of the unfortunate things which can happen to it". Deze kunnen onder meer zijn het per ongeluk dan wel opzettelijk ongeautoriseerd verwerken, vernielen of onthullen van gegevens. Het relatieve belang van elk van deze calamiteiten varieert niet alleen per informatieverwerkend systeem, maar zelfs per bestand binnen één systeem.

Bij de keuze van de toe te passen maatregelen dient men zichzelf twee kritische vragen te stellen: "Zijn de maatregelen effectief?" en: "Zijn zij economisch verantwoord?".
De geschiktheid van specifieke veiligheidsmaatregelen kan worden uitgedrukt in een functie van de effectiviteit en de kosten ervan. Uit een

en ander valt af te leiden dat, voordat tot een selectie van beveiligingsmaatregelen overgegaan kan worden, eerst het probleem in zijn geheel gedefinieerd dient te worden. Let wel:

> Gedeeltelijke probleemdefinitie met een daaruit voortvloeiende gedeeltelijke probleemoplossing kan leiden tot een overlapping of zelfs tot een onderling tegenstrijdig zijn van veiligheidsmaatregelen voor een systeem als geheel. Dit is economische verspilling!

Redenen voor beveiliging

Courtney noemt zes redenen voor beveiliging, die vrijwel altijd aanwezig zullen zijn.

1. De afhankelijkheid van de onderneming van het EDP-systeem: het moet continu beschikbaar zijn.
2. Er zijn - soms - grote offers gebracht om gegevens te verkrijgen, zij zijn veelal slechts tegen hoge kosten te reconstrueren en zij kunnen noodzakelijk zijn om het bedrijf te besturen: Gegevens vormen een belangrijk "actief".
3. Het beschermen tegen kennisneming van bepaalde gegevens door onbevoegden is noodzakelijk.
4. De mogelijkheid tot misbruik van het systeem bestaat.
5. Personeel heeft er recht op niet onder verdenking te staan, dat zij oneerlijke activiteiten uit zou voeren.
   Malafide gebruikers moeten daarom geïdentificeerd kunnen worden.
6. Het systeem-management moet in staat zijn aan te tonen dat zij het haar toevertrouwde systeem verantwoord heeft beheerd, dat zinvolle maatregelen zijn genomen tegen redelijkerwijs voorzienbare calamiteiten.

Vervolgens geeft Courtney een opsomming van de aspecten die maatregelen van beveiliging noodzakelijk maken. Deze opsomming is systematisch en wel in volgorde van afdalende waarschijnlijkheid van voorkomen.

1. Het zeer bekende probleem van fouten en weglatingen (errors and omissions).
2. Oneerlijk personeel. Hierbij plaatst Courtney een belangrijke kanttekening: Het is opvallend dat zelden wordt gefraudeerd met gegevens die geen verband houden met de dagelijkse werkzaamheden van betrokkenen. Vertrouwdheid met de gegevens is min of meer een voorwaarde voor het malafide gebruik ervan!
3. Brand. Brand buiten de computerruimte komt vaker voor dan erin en richt ook vaak grotere schade aan. Aangrenzende ruimten moeten evengoed beveiligd worden tegen brand als de computerzaal zelf.

4. Ontevreden personeel. De door hen aangerichte schade is vaak hoog, al komt het weinig voor. Het management moet echter waken voor het langdurig ophopen van ontevredenheidsgevoelens.

5. Waterschade. Let op goede daken, veilige waterleidingen en dergelijke. Overigens behoeft een goed bestrijdingsmiddel niet duur te zijn. In dit geval: een rol plastic en een schaar.

6. Schade door derden. Verbied de toegang tot de computerruimte aan allen die er niet moeten zijn.

Wanneer wij nu gaan onderzoeken welke veiligheidsmaatregelen er genomen moeten worden, moeten wij ervoor zorgen díe risico's af te dekken die een relatief grote kans van optreden hebben. Anders gezegd: het is weinig zinvol geld en ongerief te offeren voor de bescherming tegen calamiteiten die voor zover bekend nog nimmer zijn opgetreden of voor maatregelen die misschien in de toekomst nodig zijn maar waaraan thans nog niemand behoefte heeft.

Courtney deelt de veiligheidsmaatregelen in in vier categorieën: identificatie, autorisatie, audit en integriteit van het systeem (zie ook het hierna besproken artikel van Van de Sandt).

1. Identificatie

Identificatie is noodzakelijk omdat slechts een beperkt aantal handelingen, afhankelijk van de gebruiker, met het systeem verricht mogen worden. De gebruiker moet dus individualiseerbaar zijn. De drie identificatiemethoden zijn:

a. herkenning door middel van iets dat men moet weten: bijvoorbeeld een pass word;
b. herkenning door middel van iets dat tot het wezen van de individu behoort: vingerafdruk, stempatroon;
c. herkenning door middel van iets dat men bij zich heeft: badge of credit card.

Methode a. wordt het meest gebruikt, methode b. het minst. Een combinatie van a. en c. geeft een vrij hoge graad van zekerheid.

2. Autorisatie

De schrijver doelt vooral op geautoriseerd terminalgebruik. Hiertoe kan het nodig zijn de terminal te individualiseren; noodzakelijk is het de bediener van de terminal te identificeren, ten einde malafide gebruik tijdig te ontdekken en de terminal zonodig te blokkeren.
(N.B.: De schrijver gaat in dit artikel voorbij aan procedures die moeten waarborgen dat uitsluitend met geautoriseerde programma's wordt gewerkt.)

3. Audit

Ook de toegang tot applicaties waartoe een gebruiker normaal geen toegang heeft dient bemoeilijkt te worden, mits dit tegen acceptabele kosten ten opzichte van de waarde ervan kan geschieden.
Onder "Audit" verstaat Courtney dan het uitgebreid vastleggen van wat iedere gebruiker heeft gedaan, welke bestanden hij gebruikt heeft en dergelijke. Ongeoorloofd gebruik zal hierdoor, hoewel achteraf, toch bekend worden.

4. Integriteit van het systeem

Dit betreft het juist functioneren van hardware en programma's, aangevuld met de fysieke beveiliging en organisatie van het rekencentrum. Hieronder mede te verstaan de beveiligingen tegen diverse vormen van spionage.
Ieder systeemontwerp dient apart gereviewed te worden met betrekking tot specifieke beveiligingsproblemen. Hoewel er enkele richtlijnen te geven zijn die vrij algemeen gelden, blijken er toch altijd weer foutenmogelijkheden te bestaan die voordien over het hoofd zijn gezien.

Een middel om het afluisteren c.q. aftappen van lijnen bij telecommunicatie te bemoeilijken is het toepassen van cryptografie. Bij datatransmissie van uiterst geheime gegevens kan men deze door middel van een algoritme omzetten in een codeschrift (geheimtaal). De potentiële dief van gegevens zal de afgetapte informatie moeten decoderen, wat bij een tamelijk gecompliceerde algoritme nauwelijks zal lukken.
Vooraf moet men zich wel realiseren hoe groot de waarde van de informatie voor de onderneming is. (Dit is bijvoorbeeld het geval bij "cash-issuing terminals".)

## Gegevensbeveiliging in Data Base Management Systemen (ir. C.H.C. van de Sandt)

Ir. Van de Sandt beschouwt de vier beveiligingscategorieën van Courtney (identificatie, autorisatie, audit en integriteit van het systeem) in relatie met Data Base / Datacommunicatiesystemen. Hierbij gaat hij uitsluitend in op voorzieningen die in het algemeen bij data base / datacommunicatiesystemen in de genoemde beveiligingscategorieën worden aangetroffen. Daarbij dient te worden bedacht dat in de meeste toepassingen de Data Base (DB) en de Datacommunicatie (DC) gedeeltelijk afzonderlijke software-pakketten zijn, zodat er overlappingen kunnen voorkomen in de beveiligingsvoorzieningen.

### Identificatie

De meest gebruikelijke voorziening is de SIGN ON / SIGN OFF procedure. De gebruiker moet zich identificeren door middel van een pass word of code. Hiertoe is in het systeem een SIGN ON TABEL aanwezig waarmede de code gechecked wordt.

Autorisatie

In deze categorie vallen al die faciliteiten die, voor iedere gebruiker afzonderlijk geregelde, beperkingen opleggen ten aanzien van het gebruik van de verschillende systeemcomponenten:

1. In de SIGN ON TABEL wordt vastgelegd welke transacties een bepaalde gebruiker mag uitvoeren.
2. Autorisatie op toegang tot de verschillende niveaus van de logische gegevensstructuur en de fysieke opslag, door blokkades te specificeren in de externe data base beschrijvingen. De autorisatie geschiedt meestal door de verplichte overeenstemming tussen de gespecificeerde blokkades en een door het applicatieprogramma op te geven sleutel vast te stellen.
3. Gekoppeld aan de toegangsbeveiliging is meestal de controle op de wijze van gegevensmanipulatie (lezen, schrijven, bijwerken), die het betreffende programma mag uitvoeren.
   Bij geconstateerde (pogingen tot) overtreding zal signalering aan de systeemsupervisor en vastlegging ten behoeve van de audit moeten plaatsvinden.

Audit

Dit aspect krijgt nog meer betekenis in een DB/DC-omgeving.
Van de Sandt wijst erop dat vastlegging van gegevens over de transactieverwerking behalve voor de administratie en de accountant ook van belang is voor een eventueel herstel van de data base. (Dit laatste aspect wordt in het volgende artikel verder uitgewerkt.)
De controle kan op een aantal aspecten betrekking hebben, te weten:

- overtredingen tegen identificatie en autorisatie;
- gegevens over transactieverwerking;
- gegevens over systeemactiviteit (statistische gegevens en accounting).

Systeemintegriteit

Systeemintegriteit omvat het complex van maatregelen, die een juist functioneren van apparatuur, programma's, gegevensverzamelingen en personeel moeten waarborgen. Het is van groot belang voor toepassingen waarbij gebruikers online bestanden kunnen bijwerken, veel meer nog dan wanneer alleen informatie opgevraagd kan worden en het bijwerken van de data base batchgewijze geschiedt.
Het artikel gaat uitvoerig in op de softwarefaciliteiten die ten behoeve van de systeemintegriteit in een DBMS geïmplementeerd kunnen zijn, waaronder ook begrepen de softwarepakketten om het aftappen van informatie tegen te gaan.
De schrijver geeft dan in een tweetal schema's een overzicht van een aantal softwarefaciliteiten en de problemen waarvoor die een oplossing bieden. Het eerste schema, "Voorzieningen in DBMS voor het handhaven van de systeemintegriteit", toont aan dat de meeste problemen ontstaan wanneer meerdere gebruikers of programma's gelijktijdig de gegevens van een data base kunnen wijzigen. Het tweede schema is een "overzicht van voorkomende Back-up en Restart faciliteiten in DBMS".

Tenslotte geeft de schrijver in een overzicht aan hoe in een viertal data base managementpakketten de autorisatie-, audit- en integriteitsvoorzieningen zijn geregeld. Hierbij maakt hij gebruik van gegevens die zijn verzameld ten behoeve van een uitgave van Consultdata (1975) inzake selectiecriteria voor DBMS-en: "Some features of four data base management systems". Er vindt vergelijking plaats van de pakketten:

- DMS 1100 van Univac
- IMS van IBM
- SYSTEM 2000 van MRI Systems Corporation
- TOTAL van Cincom Systems.

Uit deze publikatie heeft Van de Sandt de volgende items gelicht.

1. Autorisatie van de toegang tot gegevens en wijze gegevensmanipulatie.
2. Audit.
3. Systeemintegriteit ten aanzien van:
   a. gelijktijdige benadering van een record;
   b. dead lock situatie;
   c. gegevensmanipulatie (validatie van invoergegevens, verandering gegevensstructuur en herstart-faciliteiten).

Uit deze schema's blijkt dat niet alle pakketten aan elk der veiligheidsaspecten een even grote waarde toekennen. Daarenboven dient men erop bedacht te zijn dat de implementatie van deze faciliteiten extra programmatuur en soms ook extra hardware vereist, waardoor tevens de snelheid van verwerking nadelig kan worden beïnvloed.
Voor iedere toepassing moet dan ook nagegaan worden welke faciliteiten in dat geval noodzakelijk zijn.

Beveiligingsaspecten rondom een data base: Een voorbeeld uit de praktijk (drs. R.J. Romein en ing. W. Visser)

Ook deze schrijvers stellen dat zij geen "standaard"-oplossing kunnen verschaffen, eenvoudig omdat die niet bestaat. Uitvoerig wordt uiteengezet hoe de beveiliging van gegevens in de data base toepassing bij het Sociaal Fonds Bouwnijverheid (SFB) is georganiseerd.
Het betreft een nog in opbouw zijnde toepassing, een data base met circa 1,1 miljoen records. Thans is het zo dat door middel van beeldbuisterminals gegevens kunnen worden opgevraagd (information retrieval) maar dat de via deze terminals opgegeven mutaties worden verzameld en tweemaal per dag batchgewijze worden verwerkt. In de toekomst wordt echter gedacht aan het online muteren van de data base. Mede uit voorgaande artikelen zal het duidelijk zijn dat de thans gekozen situatie goede beveiligingsmogelijkheden biedt.

Het SFB Data Base Systeem berust op drie pijlers:

1. Het gegevensbeheersysteem: hierin worden alle gegevens geregistreerd en beschreven.
2. FMS8 (File Management System onder het Exec 8 Operating System): regelt de fysieke opslag van de gegevens in de data base. Het artikel geeft een beschrijving van de werking van FMS8.
3. Data management routines (interfaces): regelen de toegang tot de data base voor de toepassingsprogramma's en verzorgen het transport van de gegevens tussen de data base en het toepassingsprogramma.

Het SFB acht het noodzakelijk ten aanzien van de volgende aspecten beveiligingsmaatregelen te nemen:

a. Verlies van gegevens in de data base door fysieke beschadiging van de apparatuur en aantasting door niet geautoriseerde programmatuur.

b. Ongeautoriseerde toegang door batch- en datacommunicatieprogramma's.

c. Onbereikbaarheid van gegevens bij uitval van kanalen en schijveneenheden in de computerconfiguratie.

Men is gekomen tot de volgende oplossingen:

Beveiliging tegen verlies van gegevens in de data base

a. Loggen

Van ieder gemuteerd record worden de voor- en na-status (before and after images) vastgelegd, van tijd tot tijd aangevuld met een checkpoint: een datum-tijd-record, welk record ook op de console printer afgedrukt wordt.
De logbestanden kunnen worden gebruikt om, uitgaande van een bepaalde stand van de data base, deze te herstellen in een toestand die deze had op een gespecificeerde datumtijd.

b. Back-up

Per einde van een dag wordt de data base op magneetband gekopieerd. Deze tapes worden een week bewaard. Bij elke tape wordt ook de bijbehorende logtape bewaard, zodat volledige reconstructie mogelijk is.

c. Recovery

Uitgaande van de jongst bruikbare kopie van de data base en de logtape wordt de DB gereconstrueerd tot een checkpoint waarvan men weet dat op dat moment de DB nog correct was. Recovery is noodzakelijk:

- wanneer een programma dat de data base muteert in een foutsituatie eindigt;
- bij storingen tijdens het bijwerken van de data base;

- bij hardware-storingen op de magneetschijven;
- als blijkt dat de data base onbetrouwbaar is geworden.

d. Integriteit

De integriteit van de data base wordt gecontroleerd met behulp van een eigen ontwikkeld data base relatie-controleprogramma.

Beveiliging tegen ongeautoriseerde toegang door programma's

a. Batch-programma's

Een belangrijke beveiliging is reeds dat alleen met behulp van batch-programma's de data base gewijzigd kan worden, omdat de betreffende datamanagement-routines alleen door deze programma's aangeroepen kunnen worden. De opslagstructuur van de data base is dermate ingewikkeld dat het zonder hulp van deze datamanagement-routines uitgesloten geacht moet worden de data base te kunnen wijzigen. Ook zijn er - onder andere organisatorische - maatregelen genomen om te zorgen dat programma's in de testfase uitsluitend met een test data base werken. In FMS8 zijn voorzieningen opgenomen die een programma alleen toegang tot de data base verschaffen indien programma- en run-identificatie akkoord zijn. Ook tijdens de run wordt voor iedere handeling gecontroleerd of het betreffende programma bevoegd is deze handeling te verrichten.

b. Datacommunicatieprogramma's gebruikt door beeldbuisterminals

Allereerst dient de terminalist zich te melden met een pass word (dat van tijd tot tijd gewijzigd wordt). De lettercodes geven aan tot welke actie(s) de betreffende terminalist bevoegd is.
Het intoetsen van gegevens kan slechts plaatsvinden na het opvragen van een zogenaamd "masker". Iedere programmamodule heeft een eigen masker. Delen van het masker waar geen gegevens ingetoetst mogen worden zijn "protected" en daarmede onbereikbaar voor de terminalist. Wijzigen in de data base is door datacommunicatieprogramma's voorlopig nog niet mogelijk.

Beveiliging tegen onbereikbaar worden van gegevens bij gedeeltelijke uitval van de schijven subsystemen

De data base is verdeeld over beide schijven subsystemen. Deze beide systemen zijn door middel van twee kanalen en dual access features met de centrale verwerkingseenheid verbonden. Uitval van één kanaal leidt daardoor niet tot uitval van een subsysteem. Bovendien is het mogelijk bij uitval van één subsysteem de betreffende data base schijven-pack op de andere unit te monteren.

Door de verkorte weergave van een aantal artikelen hebben wij getracht U een inzicht te geven hoe in Informatie van september 1975 het probleem van de gegevensbeveiliging is belicht. Mocht een bepaald artikel Uw nadere interesse hebben, dan kan bij de A.C.-documentatie om een kopie worden verzocht.

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

door A.W. Neisingh

## Computer abuse

- Bestandsvergelijking op computer brengt fraudes aan 't licht

Begin deze maand ontdekten de gerechtelijke autoriteiten van het Bronx district te New York, dat meer dan veertig ambtenaren in dienst van de staat en de gemeente het computersysteem van de sociale dienst ten eigen nutte hadden aangewend. In drie jaar tijds verdween een bedrag van 250.000 dollar aan sociale gelden via deze uiterst asociale weg in hun zakken. Alhoewel er nog dertien van de 42 fraudeurs voortvluchtig zijn, brengt dit het aantal ambtenaren dat dit jaar in Amerika voor dit vergrijp is gearresteerd, op tachtig.

Het Welfare Fraud Bureau, de Amerikaanse instantie die misbruik van de sociale voorzieningen moet opsporen, heeft een zogeheten "file match-up"-methode ontwikkeld, waarmee kan worden onderzocht of ambtenaren in dienst, of zij die voor een ambtelijke post solliciteren, niet in de computerbestanden van de sociale dienst voorkomen. Door het opsporen van onterecht gedane uitkeringen heeft men dit jaar naar schatting alleen al zo'n elf miljoen dollar bespaard.

Computerfraude toch met sociaal tintje

De 42 gevallen van computerfraude, die begin deze maand werden ontdekt, brachten aan het licht, dat men zich onrechtmatig bedragen variërend van 1.500 tot 25.000 dollar aan sociale uitkeringen had laten uitbetalen. Gewoon door wel in overheidsdienst te zijn, maar ook sociale bijstand te genieten. De fraudes werden ontdekt, toen men eenvoudigweg de computerbestanden van de sociale dienst ging vergelijken met die van de salarisadministratie van de overheid. Simpeler kan het eigenlijk niet.
Deze methode werd enkele weken terug toegepast met behulp van het IBM 370/158 computersysteem van de Human Resources Administration en hierbij rolden de 42 fraudeurs eruit. De "ironie" van het geval wil, dat deze 42 ambtenaren misschien toch wel enige sociale steun nodig hadden, want zij behoorden allen tot de groep der laagst betaalden. Het hoogste salaris uit de groep bedroeg 9.500 dollar per jaar.
In wezen is het onbegrijpelijk, dat men nu pas deze bestandsvergelijkingsmethode toepast. In nog geen acht maanden zijn er al tachtig man gearresteerd, waarvan volgens de Amerikaanse justitie - gezien de veroordelingen - ongeveer negentig procent terecht. Vorig jaar voerde de Human Resources Administration zelf een "file match-up" uit, hetgeen tot gevolg had, dat er ruim 1.500 uitkeringen werden stopgezet en 726 werden beknot. De Amerikaanse justitie heeft dit jaar de taak maar overgenomen.

(Computable, 27 augustus 1976)

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

Op 3 september 1976 publiceerde The New York Times een artikel over een grote computerfraude bij TRW Data Systems, een onderafdeling van TRW Inc. of Cleveland. Deze onderneming beheert een data bank die op het gebied van kredietwaardigheid van meer dan 50 miljoen Amerikaanse burgers informatie bevat.
Computable meldt deze fraude in het nummer van 5 november 1976, welk artikel wij hierna onverkort overnemen.

## Weer kredietwaardig worden kon bij TRW al voor 600 dollar

Zes mensen zijn tot op heden gearresteerd wegens het manipuleren met gegevens over de kredietwaardigheid opgeslagen in Amerika's grootste databank op dit gebied. Zij maakten het namelijk mogelijk om voor zeshonderd dollar weer voor elk krediet in aanmerking te komen, gewoon door de gegevens die TRW Credit Data op magneetband had staan, te laten uitwissen. Een TRW-medewerkster zorgde hier à raison van vijftig dollar voor.

TRW Credit Data beschikt over de grootste databank met gegevens over de kredietwaardigheid van personen in de Verenigde Staten. Het gehele informatiesysteem omvat alleen al aan computerapparatuur twee IBM 370/158 en een 370/155 systeem. Hierop zijn een kleine vierhonderd Datapoint terminals, tweeduizend regeldrukkers en honderd Raytheon beeldschermeenheden op afstand aangesloten.

Sinds enige tijd was het echter voor personen, die als niet-kredietwaardig bij TRW te boek stonden, mogelijk om daar iets aan te doen. Zij konden zich tot een door de Amerikaanse pers tot "wasman" gedoopte figuur wenden, die tegen betaling van ettelijke honderden dollars (degene die hiervan aangifte bij de FBI deed werd zeshonderd dollar gevraagd) bereid bleek om hen weer een schone lei te bezorgen.

De zogeheten wasman kocht op zijn beurt een TRW-medewerkster om, die voor vijftig dollar de kredietgegevens van de betreffende persoon uitwiste. De persoon in kwestie kon dan rustig weer krediet trachten te verkrijgen, want als TRW werd geraadpleegd, bleek hij niet in het bestand van niet-kredietwaardige personen voor te komen. De zaak liep enkele weken terug fout, toen een door de wasman benaderde inwoner van Los Angeles hiervan aangifte bij de politie deed.

In de Amerikaanse pers wordt erop gezinspeeld, dat er door deze fraude verliezen van tegen het miljoen dollar zijn geleden. De procureur-generaal, die de TRW-zaak in behandeling heeft en inmiddels zes mensen heeft laten arresteren, noemde de affaire echter "te knullig opgezet om ooit veel succes te hebben". TRW Credit Data heeft daarnaast verklaard, dat men ervoor heeft gezorgd, dat in het vervolg dergelijke frauduleuze handelingen binnen haar systeem niet meer mogelijk zijn.

. Onder meer naar aanleiding van deze fraude is Computable in hetzelfde nummer gestart met een artikelserie over Amerikaanse onderzoekingen naar frauduleus gebruik van de computer.
In het eerste artikel wordt aandacht besteed aan de TRW-zaak.
Computable schrijft hierover:

De TRW-fraude komt natuurlijk niet als een verrassing. Helaas niet, zou men moeten zeggen. In de laatste tien jaren is de "gecomputeriseerde misdaad" enorm toegenomen. Maar tot nog toe waren bij vrijwel alle misdaden slachtoffers betrokken, die in rechtstreeks verband stonden met het computersysteem, waarop de misdaad werd gepleegd. Bijvoorbeeld de eigenaar ervan was het slachtoffer. En de crimineel was een individu, die meestal geautoriseerd toegang had tot die computer.
Maar in de TRW-zaak werd rigoureus gebroken met deze "regel". De fraudeurs kenden de uiteindelijke slachtoffers van hun handelingen niet. Zij konden met geen mogelijkheid weten, wie gegevens uit de door hen gewijzigde kredietbestanden zouden opvragen of wat voor effect het veranderen van een bestand zou hebben. Maar de zakenman begreep wel degelijk, wat de draagwijdte van deze malversaties kon zijn. De informatie, waar hij zolang blindelings op had vertrouwd, kon best eens vals zijn.

## Beveiliging door middel van kryptografie

. Kodeerapparaat van AEG zorgt voor beveiliging tijdens gegevensoverdracht

AEG heeft het kodeerapparaat "Telekrypt 8" geïntroduceerd. Dit apparaat kan tussen een terminal en een modem worden geschakeld en draagt er dan zorg voor, dat de doorgevoerde informatie in gekodeerde vorm wordt overgeseind. Het kodeersysteem wordt bepaald aan de hand van een door de gebruiker ingestelde sleutel, die $10^{30}$ variatiemogelijkheden bezit. Door een ingebouwde beveiliging wordt te allen tijde voorkomen, dat het apparaat als gevolg van enigerlei defect ongecodeerde informatie vrijgeeft. De Telekrypt 8 kan werken met overdrachtssnelheden van nul tot tienduizend bits per seconde, terwijl er afzonderlijke versies verkrijgbaar zijn voor half duplex en volledig duplex verbindingen.
Het apparaat biedt volgens de fabrikant een volledige bescherming van gegevens tegen diefstal of vervalsing tijdens de overdracht, omdat voor wie niet over de sleutel beschikt, "decodering van de gegevens met elk huidig denkbaar middel onmogelijk is".

(Computable, 10 september 1976)

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

## Nederlands Datanet

### PTT gaat speciaal net voor datatransmissie aanleggen

Het Staatsbedrijf der PTT zal een openbaar geschakeld datanet aanleggen dat voor 1980 in werking zal kunnen treden. Het oprichten van dit net zal vermoedelijk f 30 miljoen gaan kosten.
De beslissing is genomen omdat er sterke indicaties waren, dat bij uitblijven van een dergelijk openbaar geschakeld datanet er een aantal nieuwe particuliere datanetten ontstaan.
Het nieuwe datanet zal qua eigenschappen en omvang zo goed mogelijk aansluiten bij de wensen en verlangens van de beperkte groep van potentiële gebruikers. Maar ook andere gebruikers kunnen tot het net toetreden, voor uitwisselen van computergegevens.

Om de ontwikkeling van het net zo goed mogelijk te doen aansluiten bij de wensen van de mogelijke gebruikers zal een "gebruikersclub" in het leven worden geroepen ter begeleiding van de noodzakelijke ontwikkelingsactiviteiten.

In principe is voorts al besloten, dat het net zal worden aangesloten op het "Euronet", dat op EEG-niveau bestaat voor uitwisseling van wetenschappelijke en technische gegevens.
Via het nieuwe PTT-datanet zullen naar verwachting tegen 1980 ongeveer 4.000 terminals hun verkeer afwikkelen. Er bestaat al een dergelijk net in Engeland, terwijl er in Frankrijk aan wordt gewerkt.
Wat het dataverkeer betreft neemt Nederland in Europa de vierde plaats in achter Frankrijk, Duitsland en Engeland. Het aantal terminals in ons land is gegroeid van 3.200 in 1972 tot 16.000 in 1976 en zal volgens prognoses in 1985 ongeveer 45.000 bedragen.

Het datanet zal dienen voor het met hoge snelheid transporteren van computergegevens: tot 48.000 bits per seconde. Het gaat om verkeer tussen computers onderling, computers en terminal en terminals onderling. PTT denkt vooral aan het verkeer tussen bankkantoren en computercentra, reisreserveringen en aan de eigen postloketten ten behoeve van de Postgiro en voor het opvragen van abonneegegevens voor de telefoondienst uit de computer te Leidschendam.
De onderlinge verschillen tussen de terminals zullen door PTT worden geharmoniseerd door tussenkoppeling van speciale processoren alvorens toegang wordt verkregen tot het datanet.
Voor de aanleg van het datanet gaat PTT uit van het bestaande kabel- en straalverbindingsnet. Hiervan zal 1% van de capaciteit worden vrijgemaakt voor het datanet.

Welke leveranciers de opdrachten zullen krijgen is nog niet bekend. De Nederlandse industrie komt volgens PTT zeker ook in aanmerking, al zijn er momenteel geen complete datasystemen leverbaar volgens het door PTT gewenste concept.

(Het Financieele Dagblad, 10 september 1976)

## Bespreking van het Infotech-rapport "Real time software" gericht op praktijk

In de serie "State of the Art"-rapporten van het Engelse opleidingsinstituut Infotech is het deel "Real time programmatuur" verschenen. In de loop van de ruim 800 pagina's van het rapport wordt een groot aantal onderwerpen aan de orde gesteld, zoals bijvoorbeeld: ontwerp van operating systemen, data base gebruik, talen voor real time toepassingen, ontwikkeling van toepassingsprogramma's en dergelijke. Daarnaast zijn 19 artikelen opgenomen van deskundigen op het gebied van real time programmatuur, waaruit onder meer valt te lezen dat de discussie over de speciale eisen, die real time toepassingen aan de apparatuur stellen, nog lang niet is uitgewoed. Hoewel er ook aandacht aan de theorie wordt geschonken, vormen de praktijkervaringen van gebruikers en ontwerpers van verschillende systemen het voornaamste uitgangspunt van het rapport.

"De ontwikkeling van real time programmatuur is op een kritiek punt aangekomen. We hebben de onvermijdelijke beginnersfouten en -desillusies achter de rug, maar we zijn nog niet zo ver dat sommige van die fouten door een te vroege standaardisatie gemeengoed zijn geworden." Aan het woord is John P. Spencer, redacteur van het nieuwe Infotech "State of the Art"-rapport "Real time software". Hij acht dit dan ook het juiste ogenblik voor een dergelijk rapport, omdat enerzijds veel tot stand is gebracht dat inventarisatie behoeft en anderzijds de tijd rijp is voor een discussie over de verdere ontwikkeling van het vakgebied.

### Apparatuureisen onderwerp van discussie

Het rapport is bedoeld als naslawerk voor ontwerpers en gebruikers van real time systemen. Op theoretische gronden worden eisen geformuleerd waaraan real time programmatuur moet voldoen. De hoofdmoot van het rapport wordt echter gevormd door een praktische evaluatie van apparatuur en systeemprogrammatuur voor real time toepassingen. Aan de apparatuurkant komen onder meer de ICL 2900 en IBM 360- en 370-series aan de orde. Voor wat betreft de programmatuur worden operating systemen, zoals Rtos van Univac en TDS van Honeywell, besproken. Ook besturingsprogramma's (monitors) voor teleprocessing passeren de revue: CICS van IBM, Environ/1 van Cincom en Task/Master van Turnkey onder andere.

Het eerste deel van het rapport telt negen hoofdstukken, waarvan de operating systemen en de teleprocessing monitors er drie in beslag nemen. Verdere onderwerpen zijn: apparatuur, talen voor real time gebruik, ontwikkeling van toepassingsprogrammatuur en bestandsbeheer, dit laatste toegespitst op het gebruik van data bases. Het inventariserende gedeelte van het rapport besluit met twee hoofdstukken over de optimalisering en de betrouwbaarheid van real time programmatuur.

Het tweede deel van het rapport bestaat uit negentien artikelen van real time deskundigen en krijgt voor wat betreft de apparatuuraspecten duidelijk het karakter van een discussie. Waar enerzijds wordt staande gehouden, dat de huidige apparatuur in staat is voor de komende

twintig jaar in de behoefte van de ontwerpers van real time systemen te voorzien, horen we anderzijds dat de systeemontwerpers en -gebruikers eigenlijk pas sinds zeer kort in staat zijn duidelijk geformuleerde eisen bij de apparatuurfabrikant naar voren te brengen. Ook de filosofie achter operating systemen is in dit gedeelte onderwerp van bespreking. De teneur hierbij is dat doelgerichte systemen beter voldoen dan systemen, die zo algemeen mogelijk zijn opgezet.

Aan het rapport is een uitgebreide bibliografie toegevoegd, waarin ook uittreksels van belangrijke artikelen zijn opgenomen. De toegankelijkheid van het lijvige geheel, het rapport telt 880 pagina's, wordt gewaarborgd door een serie indexen.

(Computable, 27 augustus 1976)

## Internal auditors en EDP

Het Amerikaanse Institute of Internal Auditors heeft op haar begrotingen twee EDP-activiteiten opgenomen, te weten voor:

- het ontwikkelen van EDP-software applications voor interne accountants;
- het ontwikkelen van een jaarlijkse publikatie over EDP-auditing samengesteld uit de beste gepubliceerde artikelen van het jaar en ander nieuw materiaal.

Daarnaast organiseert het IIA jaarlijks de Conference on Auditing, Control and Security.
Director of EDP and Research van IIA is Bill Perry.

Een recente uitgave is "Computer Control and Audit", een boekwerk van ca. 500 pagina's, dat is voorbereid door Touche Ross & Co. Het bevat naast een algemeen gedeelte met de principes een complete set van "Control and Evaluation Tables".

## Databanken ("1984")

### Automatisering bij Westduitse politie

De Westduitse politie gaat haar straatagenten binnenkort uitrusten met een apparaatje waarmee zij direct uit een databank allerlei noodzakelijke informatie kunnen putten; van bijzonderheden over voortvluchtige misdadigers via de nummers van gestolen auto's tot aan de jongste rechterlijke uitspraken toe. Via deze computerterminal wordt de straatagent, "frontsoldaat" in de misdaadbestrijding, omgetoverd in een soort criminologische allesweter.

De aanstaande geboorte van deze "computeragent" werd onlangs bekend gemaakt door Horst Herold, directeur van de Westduitse federale recherche in een rede bij het 25-jarig bestaan van dit instituut.

De terminal is licht, handig, en ongeveer zo groot als een zakrekenmachientje. Het apparaat geeft niet alleen allerlei inlichtingen, maar houdt tevens de centrale meldkamer van het bureau doorlopend op de hoogte van de plaats waar een agent of surveillancewagen zich bevindt.

Tegelijk met de terminal komt een geheel op computergeheugen vastgelegde criminologische bibliotheek beschikbaar, die het urenlang napluizen van dossiers en leggers verleden tijd gaat maken.
Een groot voordeel acht de politie dat het nieuwe computerverbindingssysteem absoluut ontoegankelijk is voor buitenstaanders. Iedereen die er een paar honderd gulden voor over heeft kan de politieradio afluisteren, en als die op "scramble" (geluidsdeformatie) overschakelt zijn ook daarvoor decoders te koop. Het nieuwe systeem is volgens deskundigen echter niet te "infiltreren".
Zou een agent zijn terminal kwijtraken, dan is die voor de dief of de vinder van geen enkel praktisch nut omdat de computer pas antwoordt wanneer een bepaalde code wordt ingetikt. Daarbij worden eventuele vermiste "terminals" automatisch voor verder contact geblokkeerd.
Oom agent zelf kan ook maar niet klakkeloos alles opvragen. De computer registreert alle verzoeken van elke agent en deze zal in twijfelgevallen achteraf moeten uitleggen waarvoor hij bepaalde gegevens dacht nodig te hebben.
Door middel van het nieuw te introduceren systeem zal de politie dezelfde taken als thans kunnen vervullen, waarbij echter 20% minder personeel nodig is.
Ondanks alle voor de hand liggende voordelen van het nieuwe systeem, zijn er veel oosterburen die met enig onbehagen denken aan het door George Orwell in diens "1984" geschilderde beeld van een alomtegenwoordige, alleswetende autoriteit.
Met datzelfde onbehagen herinnert men zich dat ook West-Duitsland plannen heeft voor een centrale databank met alle persoonsgegevens van zijn 60 miljoen burgers. Sommigen zien hierin een reëel gevaar, niet alleen voor de persoonlijke privacy, maar ook voor de overheid zelf.
De eventuele revolutionairen van de toekomst, redeneren die mensen, zullen bij een staatsgreep de kanselarij links laten liggen, maar de centrale computer bezetten en daarmee het hele land in hun greep hebben.

(Het Financieele Dagblad)

# LITERATUUROVERZICHT

door J. Philippo

## In de A.C.-bibliotheek opgenomen boeken

AC 91 Basiskennis bestandsorganisatie - M.A.M. Demmer / K. v/d Heide (191 blz.)

Dit boek is een zeer bruikbare inleiding voor allen die zich willen oriënteren op het gebied van de bestandsorganisatie. Het behandelt en verklaart alle begrippen en technieken die bij bestandsorganisatie en de verwerking van bestanden een rol kunnen spelen.

AC 93 Centrale personenadministratie

Bevat de door de Ministeries van Binnenlandse Zaken, van Justitie en van Economische Zaken ontworpen tekst van een voorontwerp van de wet op de centrale personenadministratie en het advies dat hierover is uitgebracht door de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties. (De Staatscommissie - Koopmans)

AC 94 IBM Data Security Symposium, April 1973 (220 blz.)

The symposium was intended to provide a forum in which the participants could communicate their requirements for data security to IBM and to other principals in the studies. The papers are reprinted without changes and without comment.

AC 95 IBM Data Security Forum, September 1974 (500 blz.)

Deze publikatie omvat gebruikers - van IBM-systemen - en IBM-werkstukken betreffende "security actions planned or on the way in their installations" en is opgesplitst in de volgende delen:

- Architecture
- Management and Policy
- Data Base and Operations
- Government
- Operating System
- Program Integrity and Hardware.

De bijlage A bevat "Results of the Data Security Survey".

AC 97 Proceedings of the NSF Software Auditing Workshop (134 blz.)

These proceedings are a report of a workshop held as part of the tasks performed under a grant to the Lawrence Livermore Laboratory from the National Science Foundation. The grant deals with the auditing of software application programs. This work is an application of certain technologies which were developed by the RISOS (Research In Secured Operating Systems) Project.

A major goal of the grant has been to identify problems dealing with the auditing of computer software and to draw up a set of research topics that would effect solutions. These topics could then be used by government agencies and other funding groups to direct future research efforts.

The workshop presented an opportunity for people to influence national policy in regards to future research in the area of software auditing.

AC 98 Guidelines for General System Specifications for a Computer System - American Institute of Certified Public Accountants (34 blz.)

The computer applications subcommittee of the AICPA was appointed to determine the desirable features of the data processing applications for a CPA firm and an approach to selecting the equipment, software and services for processing these applications.
The first step in the work has been to determine the features of the data processing applications most likely to be the components of a beginning automated data processing system for a CPA firm, including client general ledger accounting, income tax return preparation and practice management accounting.

N.B.: Een werkgroepje bestaande uit de heren Kamstra, Pruijm en Roos heeft een commentaar op dit rapport naar het subcommittee gezonden d.d. 28 oktober 1976.

Modern concept of internal auditing - The Institute of Internal Auditors Inc.

Onder deze titel is een serie boekjes - ca. 20 pagina's - verschenen welke de titels dragen:

AC 99 Auditing Computer Centers

AC 100 Auditing Fast Response Systems

AC 101 Hatching the EDP Audit Function

AC 102 Establishing the internal audit function in EDP

Auditing Computer Centers is essentially designed to be an "auditing-aids package" and could be considered as a guide which the auditor might follow in approaching the computer complex in today's environment. To this paper is added an Audit Program Outline.

The first part of "Auditing Fast Response Systems" includes:

- Systems development
- Systems component
- Hardware controls
- Pre-installation audit of control requirements
- Audit trails
- Diagnostic programs
- System malfunction.

These topics are intended to provide the auditor with a brief description of the history, hardware and systems design requirements of a "fast response" system.
The second part of this paper outlines techniques or areas of consideration for auditing these systems. Techniques to be reviewed include:

- Auditing the CPU functions
- Test decks
- Balancing controls
- Error resolution
- Test of transactions
- Auditing remote terminal locations
- Terminal security
- Data security
- Control against unauthorized entry.

Hatching the EDP Audit Function
One of the recurrent questions asked is "How do I organize and undertake the auditing of electronic data processing?".
The answer is split up in the following sessions:

- Planning the EDP audit function
- Organizing the EDP audit function
- Areas objectives and approach
- Priorities of areas to be audited
- Scheduling audits.

Establishing the Internal Audit Function in EDP
The purpose of this paper on internal auditing in EDP is to provide guidance for organizations in the establishment of an audit function in EDP. This paper contents:

- Organizing internal auditing for auditing EDP
- Explanation of job descriptions
- Responsibilities of internal audit EDP unit
- Job descriptions.

AC 107 The design of real time applications - Maurice Blackman (265 blz.)

This book is a guide for analysts, project leaders and managers who are designing an application which uses the real time mode of processing.
Content description:

part I Nature of real time
part II Application system design
part III Application systems installation
part IV Conversion and conclusion.

AC 110 Methoden voor systeemonderzoek - W. Hartman / J. Roos (376 blz.)

In navolging van het "Information Systems Handbook", beter bekend onder het acroniem ARDI, geeft dit boek per onderzoekfase gegroepeerd een zo compleet mogelijke beschrijving van de onderzoekactiviteiten.
Het accent ligt voornamelijk op de daarbij te hanteren methoden.

AC 111 Computer Management - R. Yearsley en R. Graham (Nederlandse bewerking F. Cochius en W. Sipman)

Dit boek is gericht op twee belangrijke groepen in het bedrijfsleven, namelijk:

- de specialist of stafmanager, die een inzicht wil krijgen in de grote lijnen van het computergebeuren die zijn werk raken;
- toekomstig kader, studenten in bedrijfskunde en management, die de beschreven technieken willen beheersen.

Het boek bevat de volgende delen:

I Overzicht van computersystemen
II Het kopen van computerdiensten
III Het leiden van de automatiseringsfunctie
IV Toepassing van computers in de bedrijfsvoering.

Vooral deel III omvat onderwerpen waarover in het algemeen weinig gepubliceerd wordt, met als onderwerpen:

- Beheer, budgettering en planning van computeractiviteiten (leiding en organisatie, [project]planning)
- Management van het rekencentrum (beheer en controle van tijd, ruimten, gegevens en budgetten)
- Normen voor bestuur en management (standaards en handboek)
- Personeelsbezetting en batch-omschrijvingen
- Opleiding voor automatiseringspersoneel
- Doorlichting van systemen, programmatuur, operations
- Veiligheid van computerinstallaties.

LITERATUUROVERZICHT

## Uit de tijdschriften

### Accountant en Automatisering - Prof. L.C. van Zutphen

(Intermediair, 27 augustus 1976; T 721)

In de serie over het accountantsberoep verscheen dit interessante - hoewel algemeen gestelde - artikel, waarin aandacht wordt besteed aan de volgende onderwerpen:

- het dienstenpakket van de Nederlandse accountant;
- filosofie en aanpak van de accountantscontrole bij geautomatiseerde systemen;
- interne controle als basis voor de accountantscontrole van het geautomatiseerde systeem;
- de rol van de accountant tijdens de systeemontwikkeling;
- het gebruik van de computer in de accountantscontrole;
- de accountant als automatiseringsadviseur;
- EDP-auditing, een bijdrage tot beheerst computergebruik;
- EDP-auditing; door "wie" en "wat".

Ten aanzien van het dienstenpakket stelt de schrijver:
"De primaire functie van de accountant is het onderzoeken van de getrouwheid van verantwoordingen. In het algemeen zullen deze getrouwheidsonderzoeken als bijprodukten een hoeveelheid controle- en adviesuitkomsten kunnen opleveren, die voor het gecontroleerde bedrijf evenzeer van waarde zijn, met name ook in die gevallen waar de gegevensverwerking is geautomatiseerd. Men denke aan het signaleren van defecten in het stelsel van interne controle en beveiliging, geconstateerde inefficiencies in de administratieve organisatorische structuur, procedures, werkmethoden, aanbevelingen tot verbetering van het systeem van informatievoorziening, de te gebruiken hulpmiddelen en dergelijke.
Daarnaast kunnen ook kwalitatieve mededelingen een verantwoordingskarakter dragen. Frielink noemt als voorbeeld de mededeling van de leiding van een computerservicebureau inhoudende dat de organisatie en werkwijze van het servicebureau voldoen aan daaraan te stellen eisen van beveiliging en controle. Een onderzoek naar de juistheid van een dergelijke mededeling moet naar zijn mening zeker geacht worden te vallen onder het begrip 'onderzoek naar de getrouwheid van een verantwoording'. Het ligt in de verwachting, dat de behoefte aan dergelijke onderzoekingen, juist als gevolg van automatisering, in de toekomst sterk zal toenemen."

Bij de filosofie en aanpak bespreekt de schrijver publikaties welke in de afgelopen jaren zijn uitgegeven door de verschillende accountantsorganisaties. NIvRA 13 (de modelsituatie) en Computer Audit Guidelines (de systems oriented approach) worden hierbij naar voren gebracht; de schrijver geeft hierna de volgende conclusie:

"Indien het controle-object een dergelijk hoge organisatiegraad vertoont naar opzet en werking, worden de belangrijkste ingredienten van het controleprogramma:

1. het evalueren van de opzet en werking van het interne controlesysteem;
2. het verrichten van onderzoek naar het cijfermateriaal, nader te specificeren als:
   - cijferbeoordeling
   - toetsen van de verantwoording aan ex-ante gegevens (prognoses, begrotingen, budgetten, normen)
   - verbandscontroles
   - afstemming adminstratie/werkelijkheid
   - evaluatie detailcontroles.

De controlemiddelen met een zuiver verificatiekarakter zullen bij een dergelijke controle-aanpak duidelijk in het minimum zijn."

Bij de aanpak, waarbij de interne controle als basis voor de accountantscontrole wordt genomen (ook wel analytische aanpak genoemd), zal de accountant in de eerste plaats een onderzoek doen naar de kwaliteit van de interne controles en beveiligingen, zoals die zijn opgenomen in de interne en administratieve organisatie van het bedrijf. In S.A.S. no. 3 (AICPA) zijn als essentiële punten gegeven:

- de functiescheidingen;
- de interne controle op de transactieverwerking;
- een adequate administratieve vastlegging en verwerking van alle transacties;
- regelingen met betrekking tot de beschikkingsmacht over materiële en immateriële waarden van het bedrijf;
- het systeem gericht op de afstemming van administratie en werkelijkheid.

Een rol van de accountant tijdens de systeemontwikkeling ziet de schrijver ten aanzien van:

- de betrouwbaarheid van verwerking en gegevens;
- de continuïteit van informatieverschaffing.

Daarnaast zal de accountant als toekomstig medegebruiker moeten waken voor de controleerbaarheid van het systeem. In een overzicht worden de momenten tijdens de systeembouw, waarop de accountant om bijdragen moet (of kan) worden gevraagd, aangegeven.

Als factoren voor het gebruik van de computer door de accountant worden genoemd:

- stijgende arbeidskosten (van controlewerk);
- snellere controlebewerkingen van anders praktisch niet uitvoerbare werkzaamheden;
- integratie van bewerkingen, bestanden en beslissingsregels doen voor de mens leesbare gegevens wegvallen;
- door gebruik van de computer kan de accountant de organisatie en werkwijze van het computercentrum - zij het partieel - testen.

Bij de EDP-audit onderscheidt de schrijver:

- een doorlopende partiële EDP-audit als 'bijprodukt' van periodieke accountantscontrole;
- een gerichte EDP-audit volgens speciale opdracht.

Bij de gerichte EDP-audit wordt veelal onderscheid gemaakt tussen onderzoeken die alle systemen raken (de zogenaamde operational audits) of die zich concentreren op een concrete toepassing (system audit); als voorbeelden worden gegeven:

- Operational audit
  - Organisatiestructuur, kwaliteit personeel, procedures en werkmethoden in computercentrum.
  - Gang van zaken bij keuze van computers, software en andere faciliteiten.
  - Organisatie en procedures bij de systeemontwikkeling.
  - Opzet en naleving documentatiesysteem.
  - Systeem van programmeren (inclusief onderhoud van programma's).
  - Prestatiemeting computer- en communicatie-apparatuur.
  - Kosten/batenanalyses van automatiseringsplannen, systeemontwerpen, rekencentrum, computersystemen en dergelijke.
  - Fysieke beveiliging, reconstructie, assurantie.
  - Opzet en beoefening noodvoorzieningenplan.
  - Idem systeem van tariefstelling en kostentoerekening van automatiseringsactiviteiten.
  - Idem systeem ter bescherming van privacy en bedrijfsgeheimen.
- System audit
  - Doelmatigheid informatieproduktie (vooral periodieke overzichten).
  - Review van specifieke computertoepassingen tijdens de verschillende fasen van ontwikkeling (voor, tijdens, achteraf).
  - Opzet en werking systeem voor preventie, detectie van fouten en fraude (ook operational audit).
  - Periodieke evaluatie van operationele systemen.

Auditing and Job Accounting Data - Carol A. Schaller

(Journal of Accountancy, mei 1976, T 691)

Job accounting, een waardevolle audit-bron, kan van belang zijn voor het vaststellen van:

- de doorberekening van computerkosten aan gebruikers;
- het gebruik door geautoriseerd personeel van de geëigende programmatuur en bestanden;
- het gebruik van de computerinstallatie overeenkomstig de werkindeling;
- het ongeautoriseerd gebruik (of poging tot) vanaf terminals;
- inefficiënties of bottle-necks.

Job accounting betekent het verzamelen en onderhouden van historische gegevens over de activiteiten van het computersysteem en het gebruik van "bronnen" (programma's, bestanden, etc.) tijdens de uitvoering van een job (programma of serie van programma's).
In de loop der jaren zijn de eenvoudige job accounting systemen (meestal dienend voor het doorberekenen van de computertijd) vervangen door serviceprogrammatuur met meer mogelijkheden; te noemen vallen onder andere IBM OS/SMF en Burroughs EDP/TABS.
In beginsel zijn deze faciliteiten gericht op efficiënt computergebruik; echter ook voor audit (welke dan ook) geven zij bruikbare gegevens.

IBM/SMF, dat in het artikel meer uitvoerig besproken wordt, is een programmapakket dat:

- overeenkomstig op te geven parameters gegevens over de programma's in verwerking verzamelt en in een bestand opslaat;
- de gebruiker in staat stelt door middel van opgenomen routines deze opgeslagen informatie naar verschillende gezichtspunten te analyseren.

SMF wordt geactiveerd door het operating system op grond van de uitvoering van de jobs (vastgelegd in job control) welke in het computersysteem actief zijn.
Het bestand dat door SMF wordt opgebouwd kan bestaan uit 31 verschillende soorten records; de gebruiker kan met behulp van de routines uit het bestand een selectie maken (bijvoorbeeld naar soort), tellen, sorteren, etc..
Dit laatste betekent dat de accountant ook in staat is met de geselecteerde file (en de daarin opgenomen records) met behulp van eigen programmatuur verdere verwerkingen te doen.
De gegevens in het SMF-bestand betreffen de volgende categorieën:

- accounting (per job van een gebruiker);
- data set activity (gebruik van bestanden);
- volume utilisation (gebruik informatiedragers);
- system use (computersysteemgebruik);
- sub-system (bijvoorbeeld terminalgebruik);
- user specified (records ontstaan uit SMF door aanvullende programmering door de gebruiker).

Voor het gebruik van deze categorieën wordt verwezen naar het artikel of naar uitgebreidere artikelen in Edpacs (sept. 1974 en jan. 1975).

System and Audit Aspects of the Data Dictionary - D.L. Adams

(Edpacs, mei 1976)

De Data Dictionary (DD) is een documentatiehulpmiddel om te komen tot gestandaardiseerde definities van alle data-elementen (velden), -segmenten (records) en data bases (bestanden). De DD bevat zowel een technische beschrijving van alle data, als informatie over beveiliging, editing (opmaak), structuur en gebruik door applicaties.
De DD is als een steeds toegankelijk bestand in het computersysteem opgenomen.
De invoering van een DD vereist:

- het opstellen van conventies voor naamgeving en nummering;
- het opstellen van een table driven edit monitor, een programma, dat alle ingevoerde data bij applicaties op juistheid (overeenkomstig de informatie in de DD) controleert;
- het bepalen van de inhoud van de DD;
- het bepalen van de verslaglegging en rapporten uit de DD.

Voor de implementatie van een DD-systeem wordt in het artikel een standaardbenadering gegeven met de onderscheiden stappen.

Een DD-systeem zal in het algemeen omvatten:

- Hiërarchie-diagrammen welke de verhoudingen tussen de data-elementen aangeven.
- Segment libraries, bibliotheken, welke de informatie over ieder te gebruiken segment (en de daarin behorende elementen) geeft.
- Gedetailleerde documentatie over de datasegmenten (het artikel somt 21 punten ter aandacht op).
- Indexering van de data-elementen.

Een DD-systeem biedt als voordelen:

1. Eenvoudige en effectieve beheersing van alle data-definities.
2. Het volgen van het data-pad door het systeem wordt vereenvoudigd.

3. Standaard-edits (check op juistheid van gegevens overeenkomstig data definitions) voor alle applicaties mogelijk.
4. Bij onderhoud van programmatuur is bij wijziging van de inhoud van segmenten snel de mogelijke invloed op andere toepassingen vast te stellen.
5. Daar data-definitie voor het hele systeem centraal wordt bijgehouden, verhoogt dit de ontwerp-efficiëntie.
6. Voor overgang naar een data base systeem is reeds het materiaal verzameld.

Daar in een DD grote hoeveelheden informatie opgeslagen zijn welke snel naar verschillende ingangen teruggevonden moeten worden, is het gewenst hiervoor programmatuur te gebruiken. Een reeks van standaardpakketten zijn hiervoor op de markt (het artikel geeft een overzicht).

Voor de accountantscontrole kan de DD informatie verschaffen welke van belang kan zijn bij:

- het oordelen over en de werking van het systeem;
- review van de opgenomen beveiligingen van en de controles over gegevenselementen;
- review van screening van ingevoerde gegevens;
- het ontwerpen van steekproeven;
- gebruik van data voor toepassing audit packages.

Daarnaast zal de voor het onderhoud van de DD in te stellen functie bijdragen tot betere functiescheidingen en verantwoordingen tijdens systeemontwerp en -beheer.