compact

COMPUTER EN ACCOUNTANT

Klynveld Kraayenhof & co
ACCOUNTANTS

KMG
Klynveld Main Goerdeler
Accountants-international

NUMMER 22 7E JAARGANG HERFST/WINTER 1980/1981

VAN DE REDACTIE

In dit herfst-/winternummer 1980/1981 zijn de volgende hoofdartikelen opgenomen:

- Computersabotage
  door H. de Jong en drs. P.T.M. Laagland
- Het supportcentre Amsterdam
  door drs. J.E. Huizenga
- Computer-controletoepassing bij ziektekostenverzekering
  door H. Bruis
- De main driver, kern van het besturingssysteem
  door J.M. Verheul
- Systeembeheer in al zijn aspecten
  door J.M. Verheul en H.J.M. van der Wielen.

De vaste rubrieken bestaan uit:

- Literatuuroverzicht, samengesteld door J.C.P.M. Vermeeren en drs. B.M. de Vries
- ABC-Nieuws, verzameld door drs. H.C. Kocks.

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

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

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

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

Redactie:
Drs. J.E. Huizenga,
A.W. Neisingh en
Prof. D. Steeman.

Kopij kunt U inleveren bij de secretaris van de redactie:
H.J.M. van der Wielen.
Adres:
Pr. Irenestraat 59,
1077 WV Amsterdam.
Postadres:
Postbus 7137
1007 JC Amsterdam.

COMPUTERSABOTAGE

door H. de Jong en drs. P.T.M. Laagland

(Overdruk uit Nieuws in brief met toestemming van schrijvers en redactie)

1. Uitgangssituatie

Een geautomatiseerde administratie vertegenwoordigt voor een bedrijf een belangrijke investering. Sabotage kan leiden tot het verlies van een deel van deze investering, maar kan tevens verstrekkende gevolgen hebben voor de gehele bedrijfsvoering. In onze adviespraktijk werden wij geconfronteerd met een situatie, waarin twee essentiële programma's van de geautomatiseerde administratie met opzet waren vernietigd. De schade kon beperkt worden, omdat reconstructie van beide programma's mogelijk was.
Wij vermoeden echter dat de omstandigheden waarin deze sabotage kon plaatsvinden, niet uniek zijn voor het betreffende bedrijf.
Het ging om een bedrijf, dat voor een deel van de administratie een minicomputer met schijvengeheugen gebruikte. De beveiliging van de programmatuur en de bestanden was als volgt geregeld. Van alle programma's was zowel een source- als een objectversie aanwezig op één van de produktieschijven. De produktieschijven werden wekelijks gekopieerd. Hiervoor waren twee series schijven beschikbaar, die afwisselend de vader- en de grootvaderkopie van de programma's en de bestanden bevatten. Van alle programma's was een extra kopie van de sourceversie op een schijf, die in de kluis bewaard werd. Tevens was van ieder programma een listing aanwezig in het archief. De operator had duidelijke instructies voor het uitvoeren van de beveiligingsprocedures, alhoewel deze niet op schrift gesteld waren. Hij had voldoende routine-ervaring om de normaal te verwachten situaties te kunnen afhandelen.

2. Sabotage

Op een bepaald moment bleek, dat de operator het loonprogramma niet kon starten, ook niet door gebruik te maken van de vaderkopie van dit programma. De operator nam aan, dat dit veroorzaakt werd door een technische storing en belde de technische dienst van de leverancier op. Voordat de technicus tot de machine werd toegelaten maakte de operator, volgens instructie, een kopie van de produktieschijven. Hiervoor gebruikte hij de serie schijven die op dat moment de grootvaderkopieën bevatten.
Uit het onderzoek van de technicus bleek, dat van een technische storing geen sprake was, maar dat zowel de source- als de objectversie van het loonprogramma verdwenen waren van de produktieschijven. Ook de vaderkopie van beide programmaversies was verdwenen, terwijl de grootvaderkopie, zo al aanwezig, door het kopiëren van de produktieschijven overschreven was. Bovendien bleek, dat de sourceversie van het programma eveneens ontbrak op de schijf in de kluis, en dat de betreffende programmalisting verdwenen was uit het archief. Verwacht werd, dat reconstructie van het programma niet meer mogelijk was.

Eén dag later trad dezelfde storing op bij het inkoopprogramma. De operator had inmiddels opdracht gekregen de gehele computerverwerking direct te staken indien deze situatie zich voor zou doen. Hierdoor was het mogelijk de grootvaderkopie van het inkoopprogramma te redden. De inmiddels ingeschakelde softwarespecialist van de leverancier wist in de objectversie van dit programma enkele instructies te traceren, die, zoals in het verdere verloop van dit artikel zal blijken, het effect hadden van een programmatische tijdbom. De desbetreffende instructies kwamen echter niet voor in de sourceversie van het programma, zodat zij bij een normale visuele inspectie niet aan het licht zouden zijn gekomen.

3. Analyse

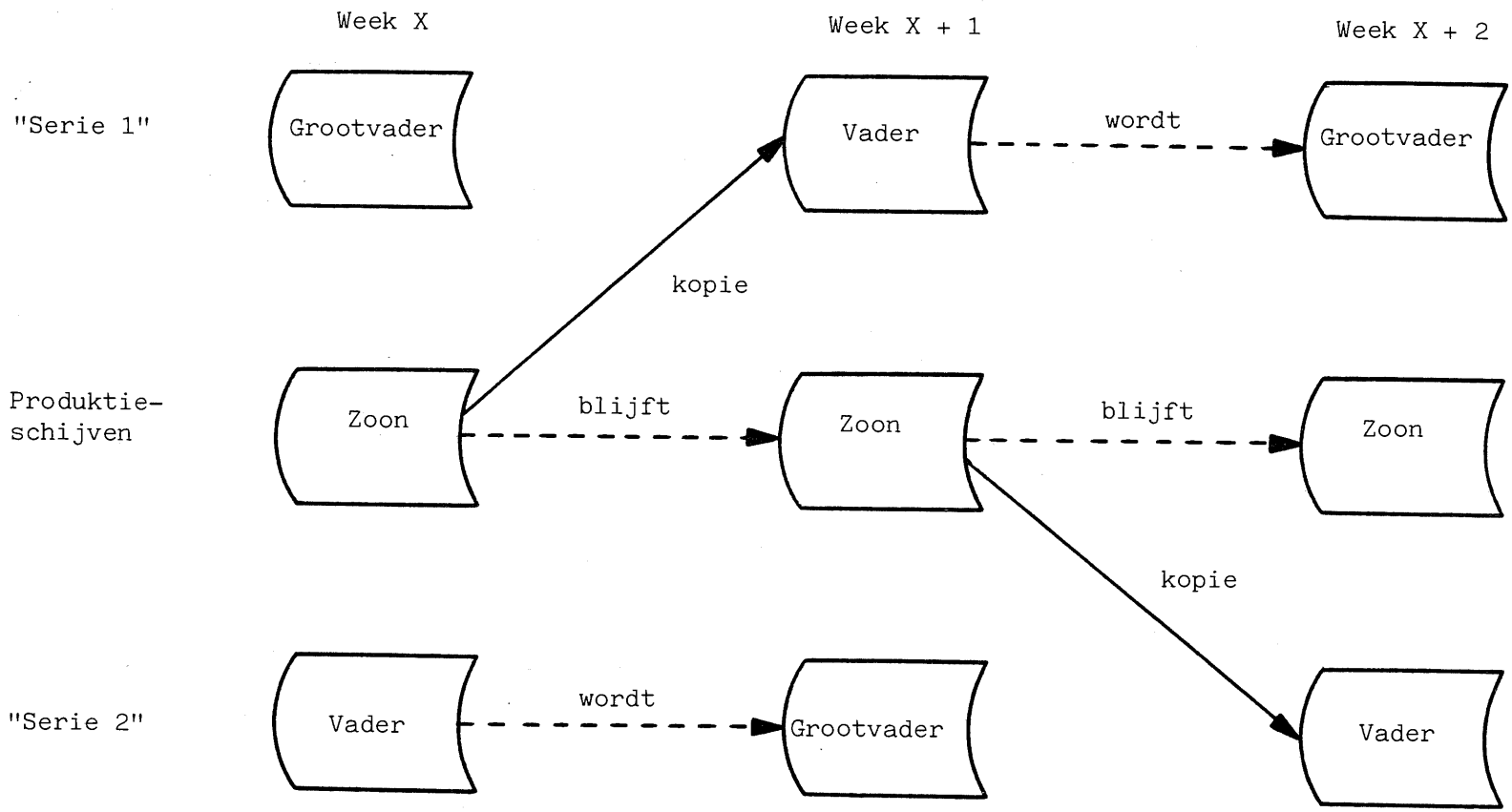
De sabotage is uitgevoerd op een eenvoudige wijze. Met enkele instructies in de objectversie van het loonprogramma werden zowel de source- als de objectversie van het programma vernietigd. Twee beveiligingsprocedures, waarvan bij de sabotage waarschijnlijk is aangenomen, dat ze blindelings zouden worden uitgevoerd door de operator, zorgden ervoor, dat de sabotage doorwerkte in de vader- en de grootvaderkopie van beide programmaversies.
De sourceversie in de kluis en de programmalisting in het archief moeten vooraf vernietigd zijn tijdens het uitvoeren van programma-onderhoud. De sabotage van het inkoopprogramma verliep op overeenkomstige wijze.

3.1 Standaard-kopieerprocedure

Voor het beveiligen van de programmatuur en de bestanden hanteerde men een grootvader-vader-zoon-systeem. Wekelijks werd de inhoud van alle produktieschijven gekopieerd. Hiervoor waren twee series schijven beschikbaar, genaamd "serie 1" en "serie 2". De kopieën werden alleen gebruikt in geval van storing in de computerverwerking. De produktieschijven behielden daarom altijd de rol van "zoon" in de beveiligingsprocedure, de beide series kopieschijven waren afwisselend "vader" en "grootvader" (zie figuur 1). De zwakke schakel in deze procedure is het feit, dat er direct ná het kopiëren maar twee verschillende versies zijn van de programmatuur en de bestanden, "vader" en "zoon" zijn op dat moment identiek.

3.2 Procedure bij technische storing

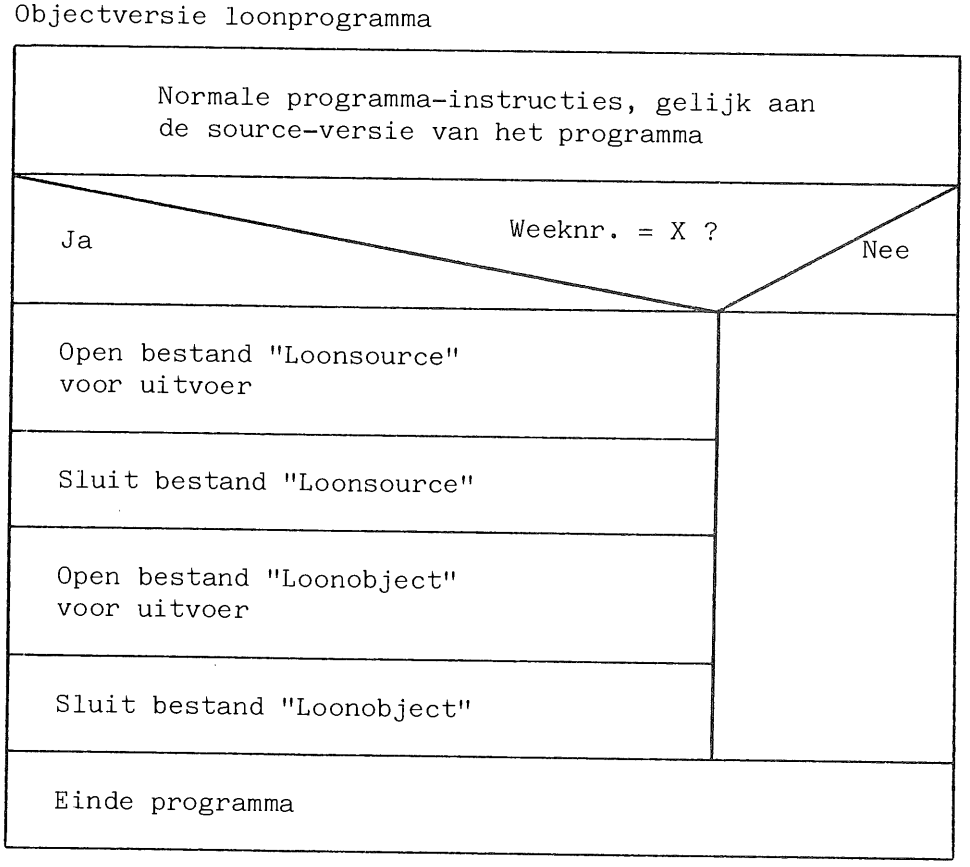
In geval van machine-onderhoud of een technische storing werd altijd eerst een kopie gemaakt van de produktieschijven vóórdat de technicus werd toegelaten tot de computer. Door gebrek aan schijven gebruikte men hiervoor echter de serie schijven, die op dat moment de grootvaderkopieën bevatte. Dit is een onjuiste procedure, omdat hiermee een goede kopie van programmatuur en bestanden wordt overschreven door de inhoud van de produktieschijven, waarvan men niet zeker kan zijn. Immers, de storing zou veroorzaakt kunnen zijn door het slecht functioneren van de produktieschijven en de daarop aanwezige programma's en bestanden zouden verminkt kunnen zijn.



Figuur 1: Standaard-kopieerprocedure

3.3 Sabotage-instructies

Het is bij batchverwerking gebruikelijk, dat sequentiële bestanden bij iedere cyclus opnieuw worden gebruikt (bijvoorbeeld mutatiebestanden). Het programma bevat daartoe instructies, waarmee het bestand wordt geopend voor het ontvangen van uitvoer. Het eerste record, dat het programma aanbiedt wordt vóór in het bestand geplaatst, zodat de oude inhoud van het bestand overschreven wordt. Bij het sluiten van het bestand wordt een end-of-file-indicatie weggeschreven ná het laatste nieuw geschreven record. De eventueel overblijvende ruimte wordt vrijgegeven aan het operating-systeem voor ander gebruik. Het is mogelijk op te geven, dat wanneer het programma geen enkel record wegschrijft maar het bestand meteen weer sluit, het operating-systeem het bestand moet verwijderen uit de directory. Het bestand is dan niet fysiek verwijderd, maar het operating-systeem kent het niet meer en zal de ruimte in de toekomst opnieuw gaan gebruiken.
Bij veel minicomputers is de bestandsorganisatie van programma's gelijk aan die van sequentiële bestanden. Bij de sabotage is hiervan gebruik gemaakt door in het loonprogramma (evenzo in het inkoopprogramma) instructies op te nemen, waarmee de beide bestanden, die de source- en de objectversie van dat programma bevatten, uit de directory werden verwijderd (zie figuur 2).



Figuur 2: Sabotage-instructies

3.4 Effectuering sabotage

Het verloop van de sabotage kan nu worden gereconstrueerd. Eén week voordat de sabotage aan het licht kwam werd het loonprogramma uitgevoerd en (schijnbaar) normaal beëindigd. Door het uitvoeren van de laatste serie instructies was de ruimte op schijf, waarop de source- en de objectversie van het loonprogramma stonden, vrijgegeven. Deze ruimte werd vrijwel onmiddellijk gebruikt voor een tijdelijk bestand van een ander programma, zodat beide programmaversies ook fysiek overschreven werden. Door het uitvoeren van de standaard-kopieerprocedure aan het eind van de week werd een vaderkopie van de produktieschijven gemaakt, zonder het loonprogramma. De volgende week kon de operator het loonprogramma niet starten omdat het zowel van de produktieschijven als van de vaderkopie verdwenen was. Omdat hij een technische storing vermoedde liet hij de technicus van de leverancier komen, maar voerde eerst de kopieerprocedure bij technische storing uit. Hiermee werd de laatste kopie van het loonprogramma overschreven en was de sabotage voltooid (zie figuur 3).

3.5 Alternatief scenario

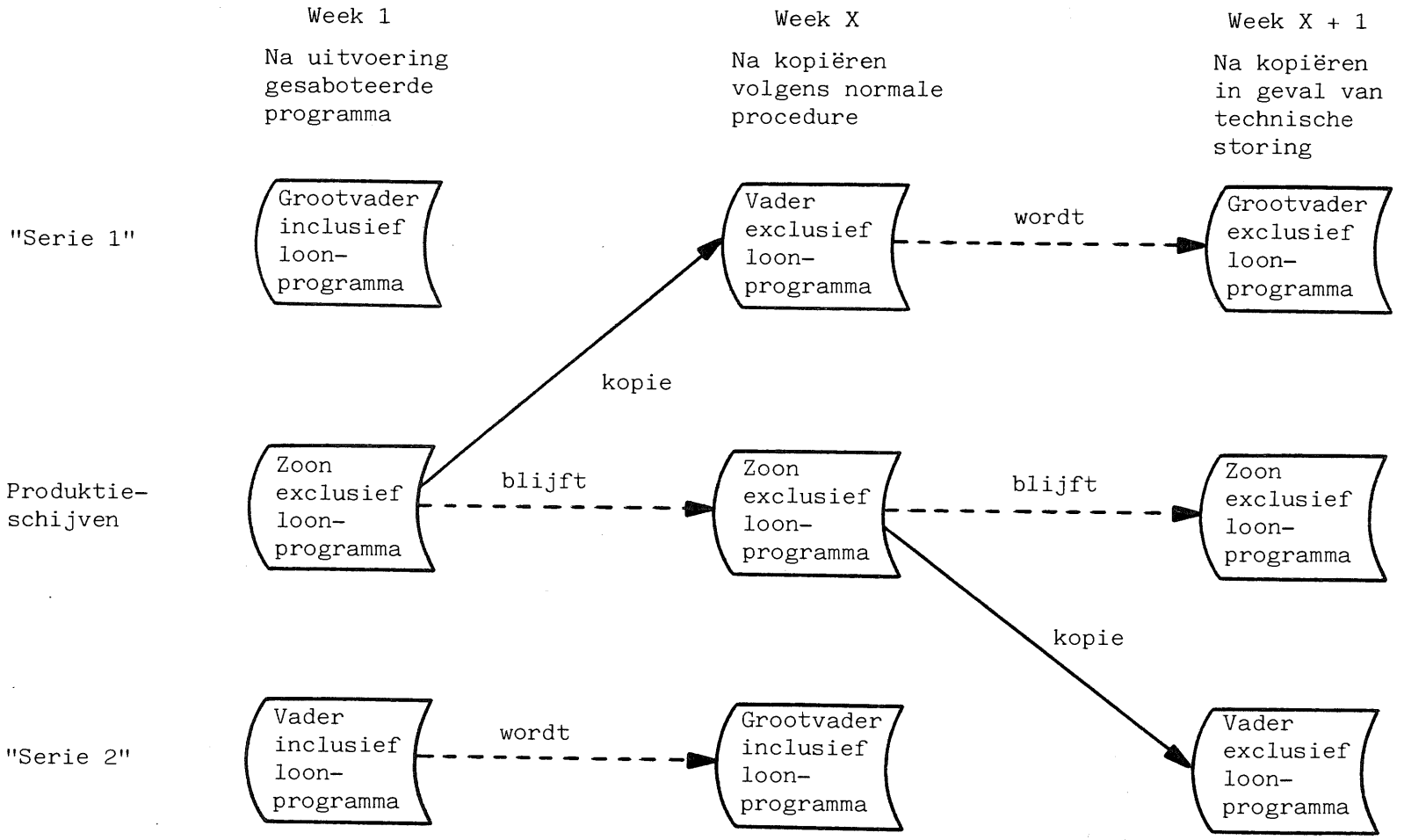
Bij de reconstructie van de sabotage zijn wij ervan uitgegaan, dat beide programma's wekelijks zouden worden uitgevoerd. Wanneer echter na het vernietigen van een programma meer dan een week zou verlopen, voordat het opnieuw zou worden uitgevoerd, zou het tweemaal uitvoeren van de standaard-kopieerprocedure eveneens hebben geleid tot het vernietigen van de vader- en de grootvaderkopie van dat programma.
Hieruit kan een belangrijke conclusie getrokken worden, namelijk, dat deze wijze van saboteren bij iedere cyclische beveiligingsprocedure zal slagen, wanneer alle kopieschijven, ongeacht hun aantal, gebruikt worden, tussen het tweemaal uitvoeren van een programma.

4. Afwikkeling

De sabotage van de twee programma's had diep ingrijpende gevolgen kunnen hebben voor de bedrijfsvoering. Door het ingewikkelde loonstelsel was het handmatig berekenen van de lonen praktisch onmogelijk, terwijl het gebruik van standaard-loonprogrammatuur veel problemen zou geven. Het opnieuw ontwikkelen van het loonprogramma zou tenminste twee maanden doorlooptijd gevergd hebben.
Hierna zal kort worden beschreven in hoeverre de sabotage strafrechtelijk vervolgd kon worden en in hoeverre de geleden schade door de bedrijfsschadeverzekering kon worden gedekt. Maar allereerst wordt beschreven, hoe de schade uiteindelijk toch beperkt kon worden.

4.1 Herstel programmatuur

Met enig puzzelwerk en een flinke dosis geluk kon het loonprogramma worden teruggevonden. De source-versie van dit programma moet van de schijf in de kluis verwijderd zijn tijdens het uitvoeren van programma-onderhoud. De vrijgekomen ruimte was echter niet opnieuw



Figuur 3: Effectuering sabotage

gebruikt, zodat het loonprogramma nog volledig intact aanwezig was op deze schrijf. Met behulp van systeem-utilities kon het weer toegankelijk gemaakt worden. Van het inkoopprogramma was de grootvaderkopie niet overschreven, zodat alleen de source-versie opnieuw gecompileerd moest worden. Om na te gaan of er nog met andere programma's was geknoeid werden alle programma's opnieuw gecompileerd. De lengte van de nieuwe objectversie was steeds gelijk aan die van de oude objectversie, zodat het onwaarschijnlijk werd geacht, dat deze programma's op dezelfde wijze gesaboteerd waren. Binnen één (zij het lange) week kon de computerverwerking hervat worden.

4.2 Strafrechtelijke aspecten

De Officier van Justitie heeft een onderzoek ingesteld naar mogelijke strafbare feiten. Hij heeft de zaak echter geseponeerd, omdat het plegen van de sabotage niet op heterdaad betrapt werd en er geen bekentenis verkregen kon worden van eventuele strafbare feiten. Het ziet er naar uit dat er in de Nederlandse strafwetgeving (nog) geen rechtsgrond aanwezig is, op basis waarvan computersabotage kan worden vervolgd. Slechts het verduisteren of vernietigen van tastbare bedrijfseigendommen, zoals programmalistings en informatiedragers, is strafbaar, niet het vernietigen van de daarop vastgelegde informatie. Wij menen, dat het voor het vakgebied automatisering een belangrijke bijdrage zou zijn, indien de juridische aspecten van computersabotage nader bestudeerd zouden worden.

4.3 Verzekering

Een gesprek met de verzekeringsadviseur bracht in dit geval aan het licht, dat schade aan de computer of veroorzaakt door de computerverwerking weliswaar onder de afgesloten bedrijfsschadeverzekering viel, maar dat sabotage daarbij uitgesloten was (vergelijk molest). Bedrijfsschade als gevolg van sabotage is niet voorzienbaar, niet bewijsbaar als schade-oorzaak en niet vooraf berekenbaar en valt daardoor buiten vrijwel elke verzekering.

5. Lering

In veel bedrijven zullen zich situaties voordoen, die ten aanzien van bepaalde aspecten vergelijkbaar zijn met de in dit artikel beschreven situtatie. Vooral in kleinere organisaties worden beveiligingsprocedures, documentatie, functiescheiding en dergelijke als overdreven lastig en kostbaar beschouwd. In zekere zin is dat juist, maar een bewuste afweging van de kosten tegen de risico's moet wel worden gemaakt. Bedacht moet worden, dat ook in grotere organisaties, waarin gedistribueerde gegevensverwerking wordt toegepast, de afzonderlijke automatiseringseenheden in een vergelijkbare situatie verkeren.
Het is een illusie te veronderstellen, dat sabotage volledig uitgesloten kan worden. Wel kan het risico worden verkleind en de gevolgen beperkt door een aantal goed op elkaar afgestemde procedures van zowel organisatorische als technische aard.
Externe deskundigen kunnen hierbij nuttig worden ingeschakeld.

In "International Management" van juli 1979 op pagina 46 las de redactie:

How to avoid computer crime

- *Set up a task force* to establish and monitor computer security procedures. The task force must include representatives from the data processing department, security, auditors and user departments.

- *Perform a systematic risk analysis* covering potential loss through accident as well as intentional crimes.

- *List computer applications* and identify possible opportunities for computer crimes; develop a system of defences.

- *Establish site inspections and interviews covering:*

  Physical state of computer room and user departments,
  Access control,
  Documentation,
  Segregation of duties,
  Unnecessary or excessive over-working by staff,
  General personnel environment.

- *Give special attention to accounting information.* Most computer fraud concerns the following areas:
  Purchase orders and invoices,
  Inventories,
  Sales,
  Pay-roll,
  Pensions.

- *Avoid:*
  Reliance on one person for vital functions,
  Chances for collusion,
  Periodic repetition of security checks, rely on *ad hoc* spot checks instead,
  Unsupervised work, particularly late at night; slack staff recruitment, appraisal and termination procedures,
  Reduction of security in moving from manual to computer system.

Zou het probleem hiermee opgelost zijn? (Red.)

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

HET SUPPORT CENTRE AMSTERDAM

door drs. J.E. Huizenga

Inleiding

Op het gebied van audit software fungeerde in MML (McLintock Main Lafrentz & Co.), één van de rechtsvoorgangers van KMG (Klynveld Main Goerdeler), het instituut "Control Centre". Ook binnen KMG zullen voor de audit software Control Centres gaan functioneren, zij het onder de naam "SUPPORT CENTRE".
Aangezien één van de Support Centres in Amsterdam gevestigd is, lijkt het goed een uiteenzetting te geven over functie en functioneren van de Support Centres.

Achtergrond

Het Computer Audit Committee (CAC) van MML had tot taak richting te geven aan "Computer Audit".
Naast initiëren en coördineren van diverse cursussen op het gebied van controle en automatisering was deze commissie ook belast met het harmoniseren van de standaard-computerprogrammatuur voor accountantscontrole.
Uit een door de CAC in 1977 ingesteld onderzoek bleek, dat de diverse in MML deelnemende nationale maatschappen de beschikking hadden over verschillende, veelal verouderde, programmapakketten.
Na een inventarisatie van de wensen van de edp-auditors en een vergelijking tussen de op de markt verkrijgbare pakketten werd besloten tot aanschaf van drie pakketten van Cullinane Corporation (zie ook bijlage 1):

- CARS-3: een COBOL-generator, welke op bijna alle grote main frame computers gebruikt kan worden;
- EDP-AUDITOR (Culprit plus de EDP-AUDITOR library of routines): een krachtig en snel pakket dat alleen gebruikt kan worden op IBM 360/370/303X en thans ook op de 4300-serie of hiermede geheel compatibele machines;
- EDP-AUDITOR/3: alleen geschikt voor IBM System/3.

De verwachting was, en tot op heden is het tegendeel niet gebleken, dat met deze set pakketten in de praktijk elk bestandsonderzoekprobleem kon worden opgelost.
Omdat MML een wijd verbreide organisatie was (voor KMG geldt dit in nog sterkere mate), moesten hoge eisen gesteld worden aan de coördinatie van:

- opleiding en training in het gebruik van de software;
- testen en distribueren van nieuwe versies;
- documentatie;
- support in geval van (technische) problemen.

Het was aantrekkelijk voor MML om een groot deel van deze taken zelf te verzorgen, omdat daardoor enerzijds veel know-how kon worden opgebouwd en anderzijds de kosten voor onderhoud van de pakketten laag konden blijven.
Voor de uitvoering van deze ondersteunende taken voorzag het contract met Cullinane in de oprichting van vijf "Control Centres" in New York, Toronto, Londen en Amsterdam (het vijfde werd in reserve gehouden).

Verwacht mag worden dat het nieuwe contract met Cullinane ook gebaseerd zal zijn op het functioneren van Support Centres binnen de KMG-organisatie voor de ondersteuning van het gebruik van audit software.

Werkwijze

De Support Centres kregen elk een regio toegewezen (Amsterdam: continentaal Europa) en zijn verantwoordelijk voor de ondersteuning van de software in dat gebied.
Dit betekent onder andere dat alleen het Support Centre direct in contact treedt met Cullinane voor het aanvragen van documentatie, nieuwe versies en dergelijke en het oplossen van technische problemen.
De Support Centres communiceren met hun achterban via "Support Centre bulletins", waarin nieuwe ontwikkelingen, waarschuwingen voor mogelijke problemen, aankondigingen van cursussen en "slimmigheden" hun plaats vinden.
De Support Centres wisselen onderling zoveel mogelijk relevante informatie uit door toezending van elkaars Support Centre bulletins, telexen in spoedgevallen en een jaarlijkse bijeenkomst.
Voor het goed functioneren van het systeem is het van groot belang, dat het Support Centre voldoende informatie krijgt over het feitelijk functioneren van de software. Daartoe bestaat een formulier waarop in het kort elke toepassing wordt beschreven en dat periodiek naar het Support Centre gezonden wordt. Op deze wijze wordt een soort bibliotheek van toepassingen opgebouwd, die geraadpleegd kan worden om te voorkomen dat binnen KMG het wiel meerdere keren wordt uitgevonden.

Alvorens met de software te kunnen werken, zal er eerst een opleiding gevolgd moeten zijn. Daartoe hebben Thomson McLintock (UK) en Thorne Ridell (Canada) voor respectievelijk CARS en EDP-AUDITOR een cursus ontwikkeld, waarin ruimschoots gelegenheid is daadwerkelijk toepassingen te programmeren.
Deze cursussen zijn ook door oud-PHT gevolgd en gegeven.

Toekomst

Nu MML is opgegaan in het grotere KMG mag verwacht worden, dat er meer behoefte zal bestaan aan het gebruik van standaardprogrammatuur in de accountantscontrole. Deze ontwikkeling zal ook aan het Support Centre Amsterdam niet voorbijgaan.
Op korte termijn zal vooral in een opleidingsbehoefte voorzien moeten worden, waarbij dankbaar gebruik kan worden gemaakt van het KKC-rekencentrum.
In MML was een ontwikkeling aan de gang om de Support Centre structuur te gebruiken voor meer dan alleen de software en het uit te bouwen tot een algemeen communicatiemiddel op het gebied van de edp-audit.
Wanneer die ontwikkeling zich ook in KMG voortzet, kan het Support Centre Amsterdam uitgroeien tot een belangrijk instrument voor een internationale benadering van de edp-audit.

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

CURRENT STATUS OF KMG-SOFTWARE

Retrieval programs currently available from Cullinane, indicated yes if present in Amsterdam, as of May 1st 1980.

COMPUTER HARDWARE	OPERATING SYSTEM	AVAILABILITY	AVAILABLE DATA BASE INTERFACE	COBOL COMPILER	CORE REQUIREMENTS FOR GENERATOR
CARS-3					
IBM 360/370	OS and OS/VS	Yes	IMS and TOTAL	ANSI '68	76 KB (NON-VS) 113 KB (VS) 96 KB (VM)
IBM 360/370	DOS and DOS/VS	Yes	DBOMP	ANSI '68	76 KB (NON-VS) 113 KB (VS) 96 KB (VM)
Honeywell 6000/level 66 Series	GCOS	Yes	AREA/IDS and IDSI	ANSI '68	33 KW
Honeywell Bull Series 60/level 62	GCOS	Yes			
Honeywell Bull Series 60/level 64	GCOS	No			
Honeywell Bull 2000	Under OS 2000	No[1]		OS/2000 ANS 1	
Burroughs 1700-1800	Standard MCP	Yes		ANSI '68	25 KB
Burroughs Large Systems (6700-7800)	Standard MCP	Yes	DMS II	ANSI '68	13 KW
Burroughs Medium Systems (1500-4800)	Standard MCP	Yes	XRAM	ANSI '68	52 KB
		Yes	DISK FORTE 2, RUFF FINE		
		Yes	THRIFT W/TIF		
		No	THRIFT W/MIF		
		Yes	DISK FORTE 1, RUFF FINE		
NCR-Century/criterion	B1-B5	Yes	CIF and Stage II	Stage 2 or Stage 3	65 KB
NCR 8200	IMOS III	Yes		ANSI '74	55 KB
Univac 1100	EXEC 8-12	Yes	DMS 1100	ANSI '68 (ASC II)	110 KB
Univac 90 Series	VS9/VMOS/TDOS, DOS	Yes		ANSI '68	100 KB
Univac 90 Series	OS3	Yes		ANSI '68	64 KB
Univac 90 Series	OS4	Yes		ANSI '68	64 KB
CDC 6000/Cyber 70		Yes		ANSI '68	10 KW
ICL 1900 - Small 2900	GEORGE or EXEC	Yes		ANSI '68	26 KW
Prime		Yes		COBOL (Revision 15) ANSI '74	110 KB
PDP-11	RSTS/E V06B RSX/11M V03, IAS V02	No		COBOL V03 (ANSI '74)	
EDP-AUDITOR			PROGRAM DESCRIPTION		
IBM 360/370	DOS and DOS/VS	Yes	Culprit release 4.3B		52 KB
IBM 360/370	OS	Yes	Culprit release 4.3B		80 KB
IBM 360/370	DOS, DOS/VS and OS	Yes	EDP-AUDITOR release 4.0		
IBM 360/370	DOS, DOS/VS and OS	Yes	Culprit release 4.5A (IDMS-version)		
IBM 360/370	DOS, DOS/VS and OS	Yes	Culprit release 5.0		
EDP-AUDITOR/3					
IBM SYS/3 Model 8, 10, 12		Yes	Release 1.0B		16 KB
IBM SYS/3 Model 15A, B, C, D		Yes	Release 1.0B		16 KB

1) Also not available from Cullinane before 01.01.'80

EEN COMPUTER-CONTROLETOEPASSING BIJ EEN ZIEKTENKOSTENVERZEKERING-MAATSCHAPPIJ

door H. Bruis

1. Inleiding

Sinds 1978 wordt bij een cliënt gebruik gemaakt van de computer als hulpmiddel bij de accountantscontrole. Het betreft hier een grote ziektekostenverzekeraar op onderlinge basis.

De computertoepassingen zijn ontwikkeld ten behoeve van de controle op de premie (ontvangsten) en de schade-uitkeringen. Alvorens de toepassingen toe te lichten, volgen eerst korte beschrijvingen van de werkwijze van de polis- en uitkeringsafdelingen van de cliënt, alsmede van de aanpak van de controle.

2. Korte beschrijving werkwijze cliënt

In het externe geheugen van de computer zijn de gegevens van alle polissen opgeslagen. Dit polisbestand is voor informatiedoeleinden online beschikbaar voor diverse afdelingen. Mutaties op het polisbestand worden door de polisafdeling via terminals aangebracht.
De premieberekening is grotendeels geautomatiseerd, terwijl de berekening van nieuwe premiestanden per maand, kwartaal, enz., van de verschillende soorten verzekering volledig zijn geautomatiseerd.
Op vervaldata worden de (prolongatie)premienota's opgeleverd, alsmede nota's voor eventuele meer-, dan wel minderpremie (als gevolg van mutaties op polissen tussen twee vervaldata). Een koppeling met de debiteurenadministratie is aanwezig. Naast de nota's worden door de computer incassotapes en stortingsacceptgirokaarten aangemaakt. Maandelijks wordt de totaal op te brengen premie van die maand opgeleverd ter boeking in het grootboek.

Van elke polis bevindt zich in het geheugen van de computer (online toegankelijk) een overzicht van alle ingediende nota's van het laatste anderhalf jaar (schade-overzichten).
Na ontvangst van nota's van verzekerden levert het systeem schade-overzichten aan de afdeling "uitkeringen".
Er vindt een beoordeling plaats van de ingediende nota's en controle of aan de verzekeringsvoorwaarden (inclusief uitgezonderde verrichtingen) wordt voldaan.

De bruto-schadebedragen worden door de afdeling "uitkeringen" via terminals ingebracht. In de programmatuur is een groot aantal geprogrammeerde controles ingebouwd, zoals controle op maxima voor bepaalde verstrekkingen, juiste inhouding van eigen risico, enz..
Door de computer wordt van de bruto ingebrachte schade de netto uit te betalen schade berekend en een afrekening voor de verzekerde opgesteld. Daarnaast levert de computer een groot aantal signaleringslijsten voor bijzondere gevallen (onder andere uitkeringen aan verzekerden met achterstand in de premiebetaling, uitkeringen via cheques, enz.), statistische gegevens, betaaltapes, alsmede informatie ten behoeve van de zogenaamde outputcontrole.

Deze controle, die plaatsvindt op de afdeling Interne Controle, richt zich op bepaalde soorten uitkeringen en houdt tevens de betalingsfiattering van de uitkeringen in. Door deze afdeling wordt na controle de betaaltape vrijgegeven voor verdere verwerking. De afrekeningen worden te zamen met de ingediende nota's op microfilm vastgelegd, waarna verzending van ingediende nota's naar de verzekerde plaatsvindt. De uitbetaalde schades worden maandelijks in het grootboek geboekt.

3. Aanpak van de controle

Het ontbreken van de controleverbanden, zoals die bij een bedrijf met een goederenbeweging aanwezig zijn, leidt ertoe dat veel aandacht aan de administratieve organisatie en het functioneren van de hierin begrepen interne controle besteed dient te worden.
Gezien de massaliteit van de mutaties, de omvang van de populaties en omdat de administratieve organisatie voldoet aan de daaraan uit controle-overwegingen te stellen eisen, is gekozen voor een wiskundige steekproef om de premie-opbrengsten en de schade-uitkeringen te controleren. Een hierbij optredend probleem is, dat de "massa" schade geen normale spreiding te zien geeft. Dit is opgelost door de totale "massa" in drie min of meer homogene massa's te verdelen, waarbij in twee massa's een steekproef wordt genomen en de derde massa (naar boven niet begrensd) integraal wordt gecontroleerd.
De geselecteerde posten worden gecontroleerd met de opgestelde afrekeningen voor de verzekerden en de ingediende nota's. Tevens vindt controle plaats op de juistheid van de premieberekening van de desbetreffende polissen. Om vast te kunnen stellen of de gecontroleerde premies verantwoord zijn in de totale premiebate worden alle premies getotaliseerd. Voor de controle op de premie zijn aparte programma's ontwikkeld.
Het aantal afrekeningen met verzekerden bedraagt jaarlijks circa 275.000. Het op een verantwoorde wijze selecteren van te controleren posten, alsmede het doortellen van schade- en premiebestanden bleek zonder het inschakelen van de computer ondoenlijk.

4. De computer en de controle

Maandelijks worden door de cliënt kopieën van het schadebestand van die maand alsmede van het cumulatieve polisbestand verstrekt. Verwerking van de programma's vindt plaats op het computercentrum van kantoor Amsterdam.

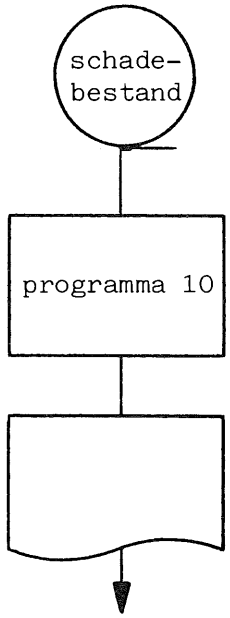
Het aantal ten behoeve van de controle ontwikkelde programma's bedraagt 5, die achtereenvolgens worden behandeld.

Per programma is weergegeven:

- summiere flow,
- voor welke controle de geproduceerde tellingen en verslagen dienen.

Programma 10

Doortellen van het schadebestand om totaaltellingen te verkrijgen naar verschillende gezichtspunten.

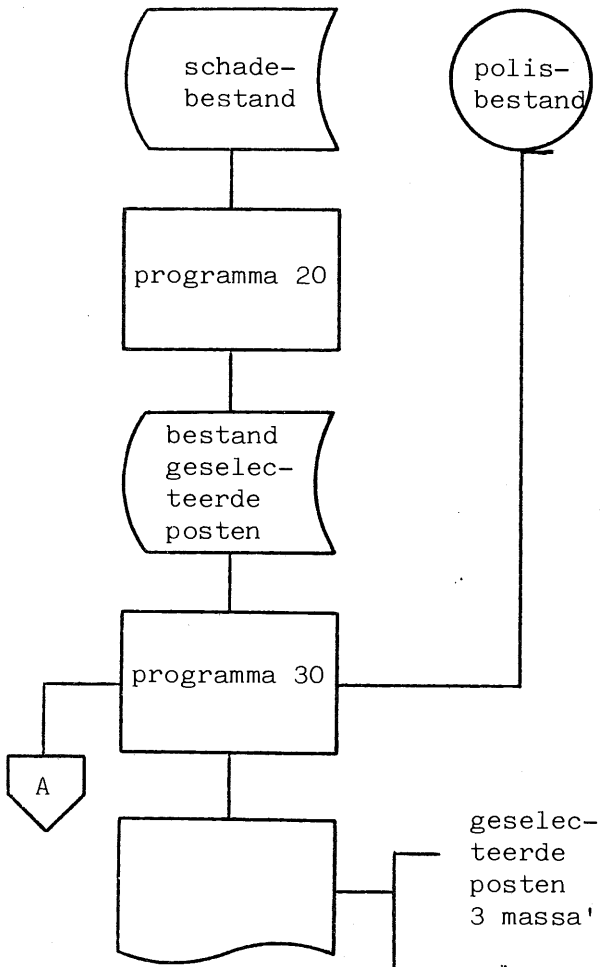


- Totalen schadebestand	:	Aansluiting grootboek
- Totalen per schadejaar	:	Beoordeling schadeverloop in totaal Volledigheidscontrole schadereserves
- Totalen per schadesoort	:	Controle op herverzekerde schade en verhaalschade
- Totalen per schadejaar en -soort	:	Beoordeling schadeverloop per soort
- Diverse controletellingen:		Controle werking eigen audit-toepassing

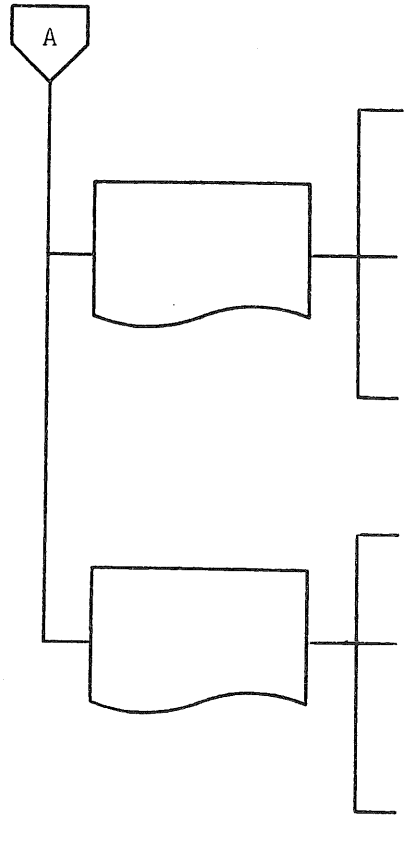
Programma 20/30

In programma 20 wordt vervolgens het schadebestand verdeeld in de in punt 3 genoemde massa's en vindt de steekproefselectie plaats. Tevens worden in dit programma nog een aantal posten geselecteerd uit een specifiek gedeelte van het schadebestand, waarvoor een aparte accountantsverklaring moet worden afgegeven.
Bovendien worden in dit programma de negatieve uitkeringen integraal afgedrukt (na eerst uit de "massa" voor de steekproef gelicht te zijn) voor afzonderlijke controle.
Na het aanmaken van de verschillende bestanden van geselecteerde posten, worden in programma 30 van elke geselecteerde post uit het

schadebestand de polisgegevens van de bij de geselecteerde uitkering behorende polis alsmede de gefactureerde premie opgezocht uit het polisbestand.



geselec-teerde posten 3 massa's	:	Positieve controle van schade met bescheiden en polisgege-vens.
polis- en premie-gegevens	:	Controle premie.
bijzondere signale-ringen	:	Polis niet in polisbestand, bijvoorbeeld nagekomen scha-de bij beëindiging verzeke-ring.



: Positieve controle van de schade ten behoeve van aparte accountantsverklaring.

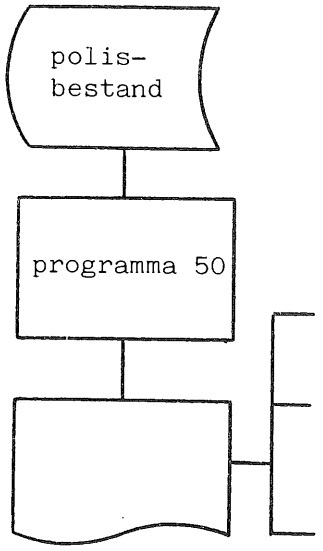
: Premiecontrole ten behoeve van aparte accountantsverklaring.

: Polis niet in polisbestand ten behoeve van aparte accountantsverklaring.

Voornamelijk bedoeld voor afwerking van gevonden fouten in de geselecteerde uitkeringen die intern al hersteld zijn.

Programma 50

In dit programma worden tenslotte de premies uit het polisbestand getotaliseerd naar verschillende gezichtspunten.



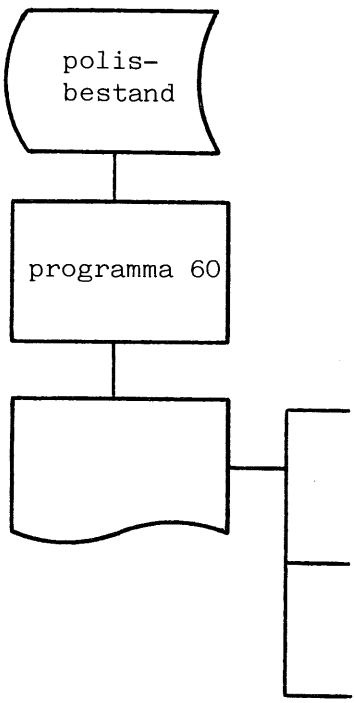
totaal-
premie : Aansluiting grootboek.

totalen per
premiesoort : Beoordeling premieverloop.

totalen per
continuïteit
(premie-
termijn) : Beoordeling premieverloop. Verbandscontroles bij controleberekening onverdiende premie op meerjarencontracten.

Programma 60

Naast de hiervoor genoemde produktie wordt jaarlijks het laatste cumulatieve polisbestand nog gebruikt voor een aantal specifieke controles. In programma 60 worden uit het polisbestand bepaalde soorten polissen geselecteerd en ten behoeve van de aparte accountantsverklaring premies geteld.

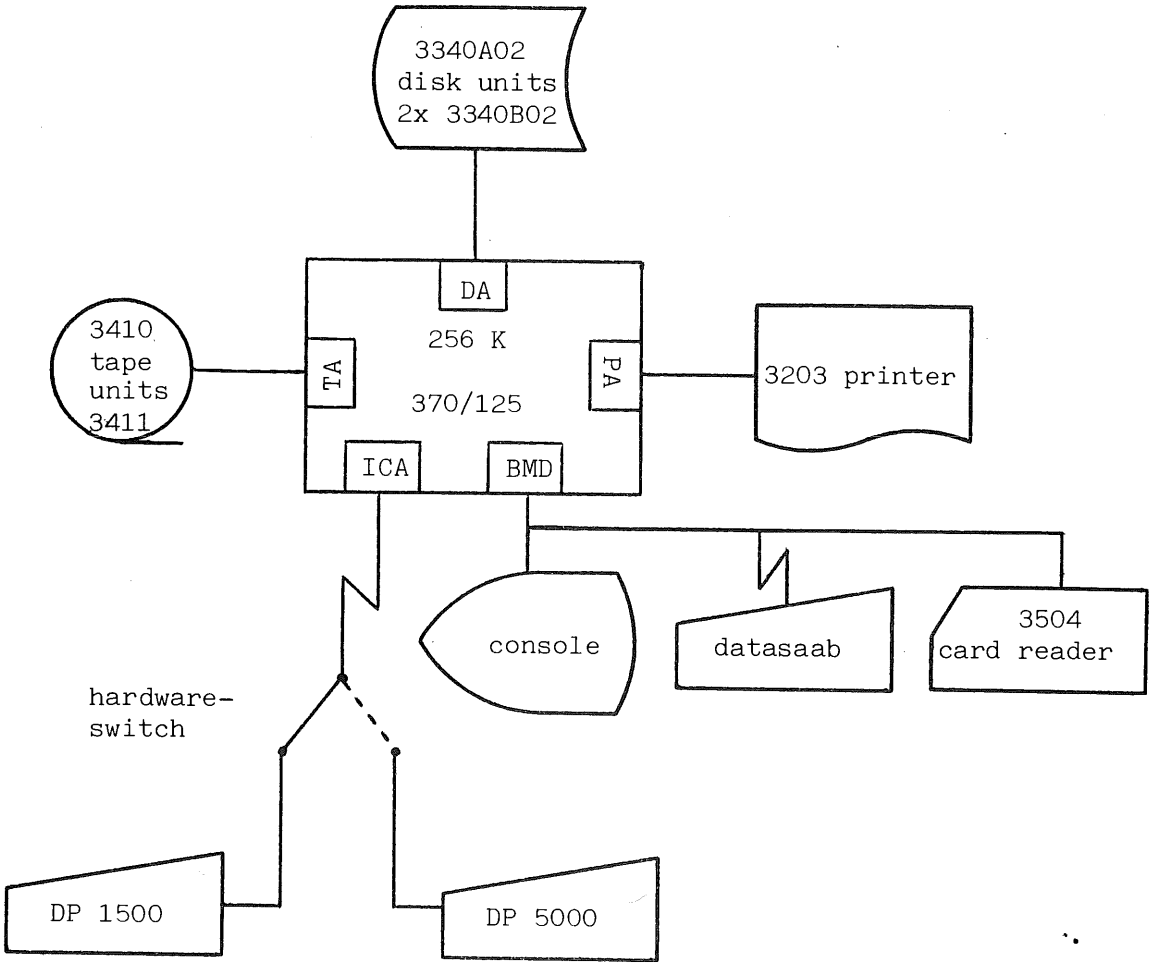


overzicht meerjaren-contracten	:	Volledigheidscontrole op de (handmatige) berekening van de onverdiende premie op meerjarencontracten.
totale premie t.b.v. verklaring	:	Aansluiting grootboek.
overzicht polissen t.b.v. verklaring	:	Volledigheidscontrole op de (handmatige) berekening van de herverzekeringspremie van een aantal specifieke polissen.

5. Computerconfiguratie, audit software en steekproefmethode

Computerconfiguratie

De computerconfiguratie op het computercentrum van KKC te Amsterdam is als volgt schematisch weer te geven.



Audit software

Bij de ontwikkeling van de controletoepassingen is in eerste instantie gebruik gemaakt van het informatie-retrieval-pakket CA-EARL. Na enige tijd bleek dat de efficiency van de verwerking te wensen overliet in verband met de grootte van de door cliënt toegezonden bestanden. Daarnaast bleken de mogelijkheden die CA-EARL bood te beperkt om aan de wensen van de controlerend accountant te kunnen voldoen. Daarom is een aantal CA-EARL-programma's vervangen door een in COBOL geschreven toepassing.

Steekproefmethode

Als steekproefmethode is in eerste instantie gekozen voor de guldenrangnummermethode met een variabel interval. Met ingang van 1981 zal de guldenrangnummermethode worden vervangen door de zeefmethode.

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

DE MAIN DRIVER, KERN VAN HET BESTURINGSSYSTEEM')

door J.M. Verheul

1. Functie en doelstelling van een besturingssysteem (operating system / OS)

In dit artikel wordt het fenomeen Besturingssysteem benaderd vanuit het gezichtspunt van de voor het computergebruik verantwoordelijke leiding.
Een OS vormt de interface tussen toepassingsprogramma's en hardware. Vanuit het gezichtspunt OS zijn dienst- en hulpprogramma's, en programma's voor het management van datacommunicatie en data bases, gelijk aan toepassingsprogramma's.

Onder hardware wordt verstaan de centrale processor, het hoofdgeheugen en de plaatselijke perifere eenheden. In moderne computers hebben de laatste eigen verbindingen met het hoofdgeheugen en verdere "intelligentie" waardoor zij onafhankelijk van de centrale processor functioneren. (Mass Storage wordt door OS niet "gezien", tenzij als 3350 schijf. Daardoor zijn verkeerde reacties van operators op bepaalde foutboodschappen onvermijdelijk.)
Een OS heeft ten doel een hoog nuttig en tegelijk betrouwbaar gebruik van de hardware en tevens het ontlasten van applicatieprogrammeur en operator van routinewerk.

Optimalisatie vormt een afzonderlijk onderwerp en is niet altijd een OS-functie. Optimalisatie richt zich op een hoge, evenwichtige belasting voor een gehele shift of ander tijdvak. Het bereiken van een optimaal computergebruik hangt af van vele factoren waaronder de eigenschappen van het besturingssysteem en de samenstelling van het werkaanbod. Niet ieder OS slaagt in optimalisering van de job mix, althans niet even goed.

De kern van OS, aangeduid als main driver, supervisor, executive of monitor, richt zich op een gelijktijdig gebruik van hardware-componenten en poogt met name, afhankelijk van het werkaanbod, de perifere eenheden zoveel mogelijk tegelijk te laten werken. Daartoe is veelal nodig dat het werkaanbod bestaat uit onderling onafhankelijke karweien (multiprogramming) of semi-onafhankelijkheid vertoont zoals bij toepassing van multithreading") op datacommunicatie-boodschappen.

') Verkorte weergave van de uitvoerige syllabus Hardware-software for computer operations, uitgereikt op het CDI seminar: EDP operations - today, in Stratford-upon-Avon (1980).

") Multithreading: eigenschap van een real time besturingsprogramma welke het gebruik van de processor toestaat tijdens een invoer-/uitvoeractiviteit. Dit ten dienste van vragen of opdrachten van andere terminals. Deze eigenschap betekent het gebruik van queues van invoer- en uitvoerboodschappen. Hiermede wordt de verwerking van de opdrachten losgekoppeld van de ontvangst en de verzending van de opdrachten en boodschappen. Een en ander berust voorts op de scheduling-functie in OS (het aanwijzen welke boodschap aan de beurt is om te worden verwerkt). Het is meestal - alhoewel niet noodzakelijk - gekoppeld aan een programmeertechniek die waarborgt dat een programma-onderdeel op zich ongewijzigd blijft, met andere woorden niet door het systeem gemoduleerd zal worden (re-entrancy).

2. Samenstelling van OS

De main driver reageert op service calls waarvandaan die in de vorm van interrupts kenbaar worden gemaakt. Als antwoord op en analyse van de betreffende interrupts selecteert de main driver de juiste routine. Voorbeelden van deze laatste zijn Scheduler, Disk Allocater, Memory Allocator I/O Executive, Log, Accounting, Wait. Ten tijde van de samenstelling van OS (de generatie van het systeem) wordt, al naar gelang de door de leverancier geboden mogelijkheden, gekozen uit een beperkt tot zeer omvangrijk aanbod van opties.

Omdat toepassingsprogramma's geen standaard-OS tegenover zich vinden is er een overbrugging nodig in de vorm van job control statements. De daarin medegedeelde aanvullende en stuurinformatie wordt door OS op aanvaardbaarheid gecontroleerd. (Zeer vele abends') zijn terug te voeren op fouten in JCL.)
De grens tussen hardware en besturingsprogrammatuur is niet scherp te trekken. De hardware-instructieset kent bijvoorbeeld geprivilegieerde instructies met geen ander doel dan het vervangen van omvangrijke OS-routines door hardware.

3. Hardware-aspecten; interrupts

Meerdere perifere eenheden gebruiken gezamenlijk een kanaal en een of meer control units (processoren). Verschillende vormen van interleaving en multiplexing worden gebruikt om de perifere eenheden van verschillend tempo asynchroon en non stop te laten werken, en telkens op tijd een of meer woorden in of uit het hoofdgeheugen te brengen. Een OS is op zich blind, waardoor een groter aanbod aan een kanaal of het hoofdgeheugen kan worden gecreëerd dan de capaciteit van de verbindingen toelaat. Daaruit resulterende missers die uitmonden in herhaling (dat wil zeggen vertraging) of definitief gegevensverlies moeten uitzonderingen zijn. Zij zijn door waarschijnlijkheidsrekening te voorspellen. De configuratie kan erop worden gekozen of aangepast. Het installeren van Data Rate Weighting in OS kan channel en memory overrun alsmede aanpassing van de configuratie voorkomen.

De genoemde en andere abnormale toestanden (bijvoorbeeld tape-fout) en de normale status (bijvoorbeeld I/O complete) van de omringende hardware wordt de processor kenbaar gemaakt door hardware-interrupts. De op de kernfunctie gerichte actieve interrupts onderbreken vrijwel terstond of na korte tijd de lopende werkzaamheden van de processor en dwingen tot analyse en antwoord. Andere, passieve interrupts wachten erop te worden opgemerkt tot OS vrij is om rond te zien naar onbeantwoorde interrupts en nieuw werk.
OS kan na analyse de behandeling van interrupts uitstellen. Het is uiteraard niet de bedoeling dat zulks leidt tot het verlies van gegevens.

') Abends: abnormal end of a task. Een onvoorziene (dus niet geprogrammeerde) beëindiging van een programmaverwerking, veroorzaakt door een fout, die niet kan worden hersteld tijdens de uitvoering van het programma.

4. Prioriteiten, scheduling

In de hardware liggen een aantal prioriteiten in het verkrijgen van service vast. Ten einde onherstelbaar gegevensverlies te voorkomen wordt aan gegevenstransport voor real time en datacommunicatie de hoogste prioriteit gegeven. Daarna volgt de langzame periferie, terwijl de snelste lokale eenheden de laagste prioriteit hebben. De centrale processor sluit de rij. De prioriteitstelling van hardware-interrupts volgt uit het voorgaande, alsmede uit de aard en ernst van de in de periferie opgetreden status die door OS gekend moet zijn. Bij meervoudige verzoeken van gelijk prioriteitsniveau past OS scheduling-algoritmen toe.

De werkvoorbereider heeft door het inbrengen van jobs (en de JCL) in de job queue uiteraard invloed op de daaruit door OS verkregen job mix en prioriteiten. Tal van omstandigheden, waaronder partitionering, beïnvloeden de uiteindelijke behandeling van prioriteiten; in de job mix vindt de prioriteitentoekenning dynamisch plaats. Wijzigingen in prioriteiten, tijdens de verwerking uitgevoerd door operators met het doel doorlooptijden te beïnvloeden, hebben niet zelden een averechtse uitwerking.

De door de werkvoorbereider of operator aan een job toegekende prioriteit kan "onderweg" in feite wijziging ondergaan door meegegeven restricties in tijd, in de frequentie waarin een job aan de beurt mag zijn, in swapping-activiteit, en dergelijke, alsmede door het FIFO-concept. Met prioriteitstelling dient voorzichtig te worden omgegaan.

Scheduling: met het noemen van ingang in de job queue en dynamische prioriteitenstelling is nog geen beeld gegeven van de scheduling-functie van OS. Men dient zich in elke installatie een beeld te vormen van de opbouw van queues en de passage van jobs door de reeks queues.

Manueel voorbereide scheduling is moeilijk, hetgeen resulteert in een onbevredigende mate van multiprogramming.
Hoewel er pakketten voor automatische scheduling in de handel zijn (zie Datapro) slaagt de implementatie ervan in slechts een enkel geval.

5. Besturingssysteem en overhead

Na het voorgaande kan de kernfunctie nader worden omschreven als: het toewijzen van capaciteiten op basis van kennis van de actuele status van hardwarecomponenten en vergelijking van beschikbaarheden met vragen, rekening houdend met prioriteiten.

De toewijzing (allocatie) is dynamisch of statisch van karakter. Voorbeelden van het eerste zijn het vrijmaken van de processor, het aanwijzen van een toegangspad in real time toepassingen. Statische

toewijzingen betreffen bijvoorbeeld het aanwijzen van geheugengebieden, de toewijzing van een magneetbandeenheid.

Het verkrijgen van simultaneïteit in de werking van computercomponenten heeft uiteraard zijn prijs, lopend van 10 tot 30 procent gebruik van de centrale processor voor de uitvoering van eigen OS-instructies. (Het daarvan aan I/O bestede deel is eigenlijk geen overhead.) De cijfers zijn van toepassing bij een optimale job mix. Als men stelt dat het efficiënt gebruik van een computer wordt bereikt als de centrale processor voor niet meer dan 65 à 80% is belast, blijft er (meetbaar) voor toepassingen niet meer dan de halve capaciteit over.
Bij data base toepassingen kan opnieuw van een halvering sprake zijn, zodat slechts 1/4 voor direct produktief gebruik zou kunnen resteren. (Vandaar het belang van batch update van de data base, en beperking tot online-bevraging.)

Hogere percentages dan de genoemde 30% kunnen optreden als het handhaven van antwoordtijden primair staat en daardoor optimalisering in de weg loopt.
Bekend is ook dat virtuele systemen op aanmerkelijk hogere percentages improduktief gebruik uitkomen. Daarbij kan ook "thrashing" optreden (OS is te vaak bezig met page-wisseling; de mix is dan te veel uitgedijd ten opzichte van het beschikbare geheugen).

6. Performance; uitwijk

Naarmate een OS méér naar maat wordt gegenereerd en de voorbereiding van job control mede daardoor het werk van specialisten wordt (ten einde met weinig problemen de verwerking door te komen), komt het voor het computergebruik verantwoordelijk management verder van OS af te staan. In feite beslissen staffunctionarissen over het computergebruik, het disk space management, enz., dus over zaken die tot de competentie van het management behoren.
Het is van belang dat management zorgt voor een tegenkracht door het doorlopend kennis nemen van rapportages over computergebruik en fouten, alsmede het toepassen van software-monitors.
In de V.S. stelt IBM aan DOS/VS-gebruikers gratis het SMS-programma van Boole en Babbage ter beschikking voor het meten en analyseren van het gebruik van de verschillende computercomponenten.

Tenslotte, de eigenschappen van OS en JCL hebben invloed op de uitwijk en de keuze van de uitwijkcomputer.

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

SYSTEEMBEHEER IN AL ZIJN ASPECTEN')

door J.M. Verheul en H.J.M. van der Wielen

Er zijn rond geautomatiseerde informatiesystemen en automatiseringsorganisaties een groot aantal beheerstaken op uiteenlopende beheersgebieden. De uitvoering van die taken is niet het werk van één persoon. "De" systeembeheerder bestaat niet.

In dit verslag wordt de terminologie toegelicht. De op het symposium genoemde beheerstaken worden in de systematiek van de bovengenoemde hoorders weergegeven.

Hoe krijgt het systeembeheer gestalte in de organisatie?

Veelal zijn het bijbanen of deeltaken die op verschillende plaatsen in de hiërarchie kunnen verschijnen. We kunnen drie hoofdtypen onderscheiden:

1. Technisch systeembeheer bij het computercentrum.
2. Inhoudelijk beheer zowel voor de ontwikkelings- als voor de onderhoudsafdeling van de projecten/systemen. Dit beheer betreft:
   - de functies van de programmatuur: wat moet het systeem doen, en veelal
   - de metagegevens = gegevens over de gegevens (waaronder definities).
3. Beheer van de actuele exploitatie aan de gebruikerszijde. Als regel onderdeel van de gebruikersorganisatie.

In de praktijk komen vaak combinaties van de hoofdtypen voor of combinaties met andere functies, zoals:

- Technisch systeembeheer (1) + Inhoudelijk beheer (2).
- Technisch systeembeheer (1) + outputcontrole namens het centrum. Soms namens gebruiker; in dit laatste geval kan het een inbreuk betekenen op een goede functiescheiding.
- Beheer van de actuele exploitatie (3), vaak gecombineerd met controle namens de gebruiker, zoals met standen. Een gevaar voor machtsconcentratie dreigt in een dergelijk geval.

Een voorbeeld van de combinatie Technisch systeembeheer (1) + Inhoudelijk beheer (2) is weerspiegeld in de voordracht over het CVI. Op het technisch systeembeheer wordt in dit verslag niet nader ingegaan.
De combinatie van Beheer van de actuele exploitatie (3) + controle namens de gebruiker wordt gevonden in het schema van AKZO (zie het schema op blz.30).

Duidelijk blijkt dat het zaak is om steeds bewust een goed onderscheid te maken:

a. Wat omvat de functie systeembeheer in het concrete geval.
b. Wat is de functie- en taakomschrijving van de "belendende" functies.

') Verslag van het gelijknamige NOVI-symposium d.d. 10 september 1980.

Samenvattend het symposium overziende kan men stellen dat nog eens duidelijk werd dat een organisatie met één op zich goed fungerende gebruikersafdeling met daarnaast een afdeling voor elektronische verwerking en, ad hoc, een afdeling voor systeem- en programma-onderhoud, niet toereikend is. Er zijn afspraken die steeds opnieuw moeten worden gemaakt (waaronder de dienstregeling, die vaak meerdere afdelingen aangaat), onverwachte gebeurtenissen en knelpunten die alleen snel kunnen worden opgelost als men zowel het systeem als de gebruikersomgeving goed kent. Dat laatste is ook vereist voor het helpen beoordelen en doorvoeren van wijzigingen in systeem, programma's en procedures.

Beheer (als te onderscheiden van leiding geven) is het bewaren van orde en samenhang. Het gaat hier om de behartiging van gebruikersbelangen.

Völlmar spreekt van de applicatiebeheerder die in delegatie van de verantwoordelijke lijnchef een aantal beheerstaken behartigt. Bij Völlmar gaat het niet over dagelijkse uitvoerende werkzaamheden, zoals het in ontvangst nemen en controleren van invoer en uitvoer. Anderen zien ook daar een taak voor een systeembeheerder.
"De" systeembeheerder bestaat dus niet. Er zijn rond systemen een groot aantal beheerstaken op uiteenlopende beheersgebieden, taken die men op verschillende wijzen kan onderbrengen. Daaronder zijn er die zich goed lenen voor bundeling in een afzonderlijke beheersfunctie, met name omdat zij een hoeveelheid kennis van systeem, gebruikersorganisatie en automatisering veronderstellen die slechts bij enkelen kan worden opgebouwd en onderhouden.

Hieronder is een overzicht van te vervullen en eventueel te bundelen beheerstaken opgenomen zoals die her en der in de lezingen naar voren werden gebracht. Ten aanzien van de taken sub B. (te weten behartiging van gebruikersbelangen in automatiseringsafdelingen) werd wel de vraag naar het uit te oefenen toezicht opgeworpen, maar praktische oplossingen kwamen niet naar voren. Uw verslaggevers verwijzen gaarne naar de belangrijke suggestie van drs. Lagerwerf in het verslag van zijn voordracht "De weg naar een goed systeembeheer". Hij noemt de rol van de accountant als edp-auditor, zijnde degene die mede ten behoeve van gebruikers kan oordelen over opzet en werking van maatregelen op trajecten buiten zicht van de gebruiker.

Overzicht van systeembeheerstaken

A. Beheerstaken binnen de gebruikersorganisatie

- Het medewerken aan de totstandkoming van een dienstregeling met betrekking tot aanlevering van in- en uitvoer en terminalgebruik.
- Kanalisering en controle van in- en uitvoer (gescheiden, anders functievermenging (red.)).
- Het beheren van de metagegevens. In overleg met betrokkenen de gegevens vaststellen die van gemeenschappelijk belang zijn, alsmede de definities en coderingen van deze gegevens. Toezien op de naleving van de regels van het beheer van metagegevens.

- Het toezien op een juiste uitvoering van de procedures voor het verzamelen, vastleggen, controleren en verzenden van de te verwerken gegevens.
- Het onderhouden van contact met het computercentrum inzake alle aspecten van de verwerking en de bewaring van de gegevens, met inbegrip van beveiliging en continuïteit; het behandelen van knelpunten, storingsberichten, klachten, systeem- en programmafouten; het bevorderen van efficiëntie bij ad hoc verwerkingen; het prognostiseren van kwantiteiten en daaruit voortvloeiende papierbehoefte, en dergelijke.
- Het beheren van de gebruikersdocumentatie.
- Het verstrekken van inlichtingen over het systeem en de verwerking van de gegevens in de meest ruime zin.
- Het instrueren van medewerkers, vooral nieuw aangestelde, inzake hun taken bij de gegevensinvoer en het gebruik van de resultaten van de verwerking.
- Het verzamelen en beschrijven van wensen voor verandering en uitbreiding van het systeem, het beoordelen van deze wensen op nut en kosten, het consolideren van deze wensen en het op gang brengen van een eventueel noodzakelijke goedkeuringsprocedure bij groot onderhoud.
- Het nemen van initiatief tot het plegen van overleg met andere afdelingen over consequenties van voorgenomen systeemwijzigingen.
- Het doen realiseren van klein onderhoud als daarvoor een eigen onderhoudsbudget beschikbaar is.
- Het meewerken aan het opstellen van specificaties bij omvangrijke wijzigingen of uitbreidingen en het verkrijgen van de benodigde goedkeuring daarvoor.
- Mede goedkeuring van nieuwe projecten, waarbij als maatstaf zal gelden het behoud en de bevordering van uniformiteit van de systemen; stellen van prioriteiten daarbij.
- Het optreden als opdrachtgever bij de realisering van systeemonderhoud ten aanzien van de invoercontrole en mutatieprogramma's en voor de overige programma's, die van algemeen belang zijn.
- Het aanbrengen of doen aanbrengen van wijzigingen en uitbreidingen in de gebruikersdocumentatie na systeemonderhoud of uitbreiding van het systeem.
- Het leveren van bijdragen aan het centrale gegevensbeheer (data-administratie, data dictionary).
- Het opstellen van het door de directie goed te keuren budget ten aanzien van de algemene onderhoudskosten. Rapportage over totale kosten.
- Het controleren van de doorberekening door het computercentrum.
- Het zorgen voor periodieke evaluatie met inbegrip van de beoordeling van de verwerkingsefficiëntie (manueel, niet-manueel).
- Het meewerken aan risico-analyses en noodvoorzieningenplanning.
- Namens de gebruikers optreden als contactpersoon met externe instanties in geval van zaken van algemeen belang.
- Het tijdig onderkennen van nieuwe componenten, die voor beheer in aanmerking komen. Kortom het inspelen op veranderingen.
- Toezien op de tijdige invoering van nieuwe procedures op gebruikersafdelingen in geval van nieuwe of gewijzigde systemen.

- Participeren in de procedures rond het testen, eventueel opnieuw testen en overdragen van het systeem.
- Het onderhouden van contacten met de externe/interne accountant ten aanzien van de controle-aspecten en periodiek evalueren van het systeem.

Noot

Bij het hebben van meerdere gebruikers voor dezelfde applicatieprogrammatuur of wanneer meerdere gebruikers van dezelfde gegevensverzameling gebruik maken zal van systeembeheer een strakke coördinatie gevraagd worden.

B. Behartiging van gebruikersbelangen in automatiseringsafdelingen

- Vertaling van gebruikerswensen ten aanzien van beveiliging en continuïteit; toezicht op daadwerkelijke effectuering daarvan binnen de verwerkingsorganisatie.
- Programmabeheer.
- Bestandsbeheer en bestandsreorganisatie.
- Beheer van systeem-, programma- en verwerkingsdocumentatie.
- Kwaliteitszorg.
- Optimalisering van "performance".
- Trouble-shooting.
- Uitvoering van recovery en restart.
- Organisatorische beveiliging van het systeem in overeenstemming met de door de leiding aanvaarde voorschriften.
- Het tijdig inspelen op technische veranderingen.
- Het participeren in de procedures rond het testen, eventueel opnieuw testen en overdragen van het systeem.
- Het door de beheerder doen bewaken van de werking van het geautomatiseerde gegevensverwerkende systeem (g.g.-systeem) waarbij de exploitatiekosten van het systeem ook als één van de beheerscriteria kan worden gezien.
- De operationele gebruikswaarde van het g.g.-systeem periodiek doorlichten en evalueren. Te denken valt hier ook aan de rol van de accountant als edp-auditor.
- Het handhaven van de operationele status van het g.g.-systeem door toe te zien op de organisatie van de vastlegging en invoer van de gegevens en door goede afspraken met het computercentrum en de zorg voor naleving van die afspraken.

Overzicht van gegevensbeheerstaken

Ten einde het eerdergenoemde onderscheid tussen systeembeheer en daarmee verwante, belendende functies te illustreren wordt tot slot enigszins ingegaan op de functie gegevensbeheer.
Hieronder wordt verstaan - aldus Lexicon Informatica 1978 - het creëren, bijhouden en vernietigen (uitdunnen) van gegevensverzamelingen, alsook het verschaffen van toegang tot en het beveiligen van de betrokken gegevens. Bij geautomatiseerde gegevensverwerking met behulp van

een computer worden de gegevens in daartoe geschikte geheugens vastgelegd. De besturingsprogrammatuur van de computer omvat dan uitgebreide voorzieningen ten behoeve van het gegevensbeheer (data management), waaronder mede begrepen de mogelijkheid tot toepassing van speciale adresseringsmethoden voor het gebruik van rechtstreeks toegankelijke geheugens.
Voor het gegevensbeheer bij toepassing van een gegevensbank (data base) zijn de door de gebruikelijke besturingsprogrammatuur geboden voorzieningen echter onvoldoende, zodat dan extra programmatuur nodig is.
Deze wordt gewoonlijk als data base management system (DBMS) aangeduid.
(Tot zover het citaat.)

De taakstelling van de gegevensbeheerder ziet er als volgt uit:

- het beheren van de verzameling metagegevens - de gegevens over gegevens - van de in zijn gebied in gebruik zijnde gegevens. Opeenvolgende standencontrole hieronder begrepen;
- het verstrekken van inlichtingen daarover aan ieder die daar uit hoofde van zijn functie behoefte aan heeft;
- het waar nodig streven naar verbetering van de metagegevens, met name de definitie van het begrip en de beschrijving van de samenhang in de verschillende gegevens;
- het meewerken aan de verbetering en de uitbreiding van de logische gegevensstructuur voor de betrokken gegevensbank.

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

LITERATUUROVERZICHT

door J.C.P.M. Vermeeren en drs. B.M. de Vries

In de A.C.-bibliotheek opgenomen boeken

AC 234 Computer Fraud and Countermeasures - Krauss en Mac Gahan
Prentice Hall 1979 (500 blz., Engels)

Computer fraud is an extremely sensitive topic today, with our society's enormous dependence on data processing in all phases of commercial, industrial, and governmental activity. Computer Fraud and Countermeasures is a lucid overview of many of the concerns which occupy data security professionals, but it suffers from a lack of focus. It sheds light over a broad area but does not pinpoint the exposures and preventive tactics that the reader would expect from the title.

(naar Steven J. Ross, The EDP Auditor)

AC 238 Security: checklist for computer center self-audits
AFIPS 1979 (189 blz., Engels)

Dit is de tweede druk van checklists ten behoeve van een onderzoek naar de interne controle- en beveiligingsmaatregelen binnen het rekencentrum. In deze checklists wordt onder andere aandacht besteed aan risico-analyse, distributed processing, systems hardware en software, terwijl een afzonderlijk hoofdstuk is gewijd aan "administrative controls".

AC 245 Computer networks and their protocols - Davies, Barber, Price, Solomonides

Wiley & Sons 1979 (487 blz., Engels)

Computer networks are part of a general trend towards distributed computing which can be seen in multicomputer systems, in distributed data bases and in the use of intelligent terminals. The rapidly decreasing cost of processors removed the need to concentrate computing power and gave the economic incentive for distributed computing. This new flexibility in system design enables the functions of a complex system to be divided physically as well as logically. A computer network connects terminals, computers, data bases etc. at a distance one from another. The communication function has inherent limitations, such as delay, throughput restriction, errors and breakdowns. We are therefore concerned, in this book, with multicomputer systems which can operate satisfactorily in this harsh environment.

AC 250 International data flow - Jan Freese
Student literature 1979 (71 blz., Engels)

In het kort wordt ingegaan op de verschillende soorten van internationaal gegevensverkeer en de daarbij naar voren komende beveiligingsaspecten.
Over de oplossing van het beveiligingsprobleem betreffende het grensoverschrijdend gegevensverkeer bestaat tussen de verschillende landen geen concensus. Het gevolg van dit gemis aan overeenstemming is, dat internationaal ondersteunde beveiligingsmaatregelen (via wetgeving) ontbreken.

AC 267 The Codasyl approach to data base management - T.W. Olle
John Wiley & Sons 1979 (287 blz., Engels)

In dit boek vindt U een uitvoerige beschrijving van de Codasyl-benadering. Eén hoofdstuk (hfdst. 18) is geheel gewijd aan de privacy-aspecten, de gedachten hierover binnen de Data Base Task Group en de uitwerking ervan in het Codasyl-concept. In het afsluitende hoofdstuk 25 worden een aantal kritische opmerkingen geplaatst ten aanzien van de Codasyl-benadering en wordt ingegaan op mogelijke toekomstige ontwikkelingen van Codasyl.

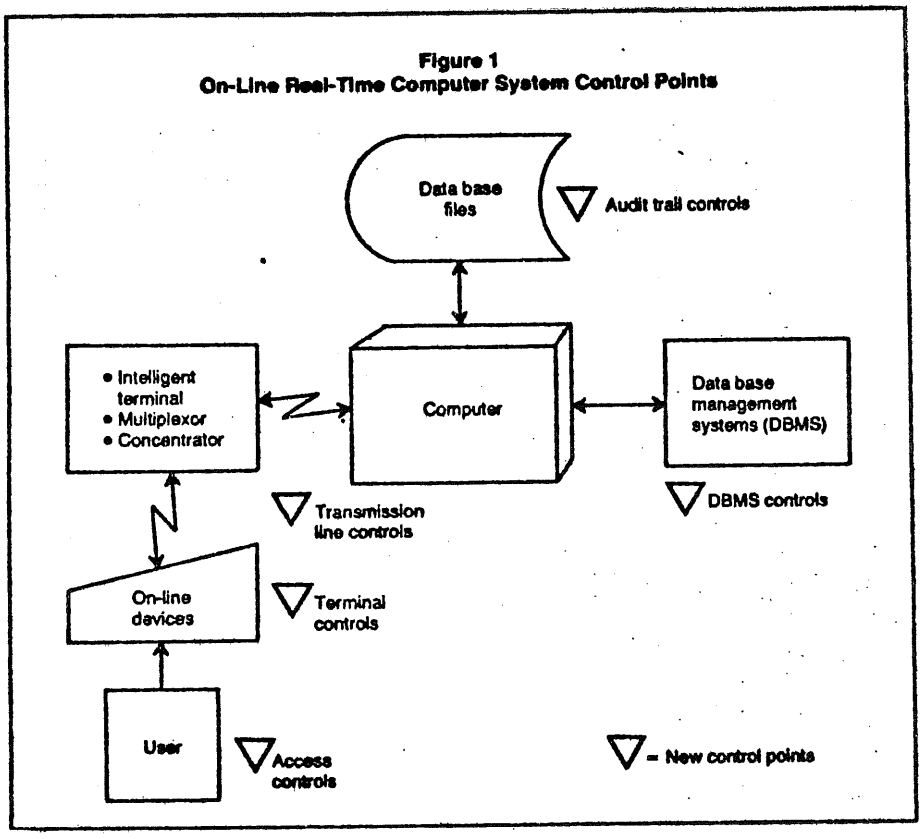
Uit de tijdschriftliteratuur

Controls for online real time computer systems - J. Cerullo
CA Magazine (maart/mei 1980) - S 468

Trefwoord: E 12

In het artikel wordt ingegaan op de maatregelen van interne controle die van belang zijn voor geautomatiseerde systemen met online/real time (OL/RT) verwerking. Zij zijn echter aanvullend op de controlemaatregelen, die voor ieder geautomatiseerd systeem gelden, zoals general controls (niet applicatiegebonden), application controls, en security controls (fysieke beveiliging).

De maatregelen van interne controle, die van belang zijn voor OL/RT-systemen zijn: access controls, terminal controls, transmission line controls, audit trail controls en data base management controls (zie Figuur 1).



Access controls

De access controls laten zich indelen in vier categorieën; de toegang tot de computerzaal, toegang tot de terminal, toegang tot de computer en toegang tot programmatuur en bestanden. De schrijver geeft per categorie aan, welke maatregelen van toegangsbeveiliging toegepast kunnen worden.

Niet duidelijk wordt gemaakt, waarom de toegang tot computerzaal, computer, programmatuur en bestanden in het bijzonder van belang zijn voor OLRT-systemen. Zij zijn uiteraard van belang voor ieder systeem van geautomatiseerde gegevensverwerking!
De access controls worden in het artikel als volgt weergegeven:

Figure 2

Possible Access Control Points in an OLRT Computer System

User must gain access to terminal room
- User has proper key/magnetic card strip
- Guard or receptionist requests user's identification
- Guard or receptionist then may request an oral password

User must gain access to terminal
- User unlocks terminal
- User inserts magnetic strip card or uses other identifier (fingerprints, hand geometry, voice recognition)

User must gain access to computer
- User calls central computer
- User indicates account or identification number
- User indicates password; computer checks and accepts or rejects it
- Computer requests other identifier(s)

User must gain access to given files or programs
- User requests a file or record; computer checks authorization table
- User requests that file or record be read; computer checks authorization table
- User instructs processing; computer checks authorization table; computer executes requested operations and transmits results

Note: • = Possible control points

Terminal controls

Gesteld wordt, dat de terminal controls de access controls ondersteunen. Onder terminal controls verstaat Cerullo maatregelen van fysieke beveiliging rondom de terminals en de terminalprocedure. Daarmee wordt onduidelijk onder welke categorie interne controlemaatregelen, de fysieke beveiliging rondom de terminal thuishoort, onder access control of onder terminal control. Wellicht is bedoeld onder terminal controls een nadere uitwerking te geven van een onderdeel van de access controls.
Onder terminal controls valt:

- gebruik van terminal identification, locks, identification cards;
- toezicht op de terminalruimte en op het gebruik, dat van deze ruimte gemaakt wordt;
- foutdetectie- en correctieprocedures voor de terminalverwerking;
- noodvoorzieningenplan;
- afstemming van totalen;
- autorisatie- en goedkeuringsprocedures voor wijzigen van bestanden.

Transmission controls

Het ongeautoriseerd opvangen van berichten, die via verbindingslijnen of via draadloze verzending worden overgeseind, behoort tot de mogelijkheden. Controlemaatregelen om het onderscheppen van berichten te voorkomen of te ontdekken dienen daarom te worden toegepast. In het artikel wordt vrij uitvoerig ingegaan op deze transmission line controls. Hier volgen enige citaten:

"Wiretapping and radiation penetration can be prevented or detected by using data encryption methods and detectors. Highly confidential or sensitive data is enciphered at the terminal and transmitted in code or cipher. The encoded data is deciphered at the computer centre and enters the system in a non-coded format. Since any code can be broken, highly strategic information should not be sent over regular communication lines, even in code."

"Assurance that all data transmitted is being accurately received can be derived from error-detecting codes, dual transmission, and retransmission. Error-detecting codes are designed to detect transmission line errors as they occur so that corrective action can be readily taken."

"Dual transmission means that all messages are transmitted from the input device twice and compared for accuracy at the computer centre. This control is similar to dual keypunching, and it is used when operator errors are high; for instance, in an airline reservation system. Retransmission is the process of transmitting a message and a character, or bit, check (derived from using an appropriate error-detection technique) to a receiving station. If an error is detected, the message is ignored and a request to retransmit is sent to the transmitting station. Depending on the input device, this message may be automatically or manually re-entered into the device and retransmitted. Finally, alternative routing ensures the availability of back-up transmission when the primary lines cannot be used."

Audit trail controls

Bij de toepassing van online/real time (OL/RT) systemen zal de audit trail in vergelijking met minder geavanceerde toepassingen in geringere mate aanwezig zijn. Het is zelfs mogelijk dat de audit trail ontbreekt! Volgens de schrijver liggen hieraan de volgende redenen ten grondslag:

- gebruikers kunnen de gegevens rechtstreeks invoeren in de computer, waardoor de vastlegging op invoerdocumenten niet meer wordt verricht;
- brondocumenten en back-up records worden een uit controlegezichtspunt korte periode bewaard;
- hard copy wordt bij OL/RT-systemen veelal slechts in uitzonderingsgevallen opgeleverd;
- door het ontbreken van hard copy en door het automatisch initiëren van transacties kan functiescheiding met de daarmee gepaard gaande formele en schriftelijke overdracht van informatie (schriftelijke verantwoording) worden aangetast.

De controles op juistheid en volledigheid van de verwerking zijn niet meer gericht op batches, maar op de individuele transacties of op een transactiesoort. Voor wat betreft de individuele transactie wordt als controlemiddel genoemd: read back, volledigheidstest per transactie, redundancy tests en opeenvolging van nummering. Per transactiesoort kan gecontroleerd worden met behulp van controletotalen, het periodiek dumpen van bestanden, hard copy en transaction logs.
N.B.: Over natellingen wordt niet gerept.

Data base management system (DBMS) controls

Onder dit hoofd worden de beheersaspecten ten aanzien van DBMS besproken. Ingegaan wordt op de functie van de data base administrator en de vanuit interne controlegezichtspunt voor deze functie belangrijke taken.

Cerullo heeft in zijn artikel op bondige en heldere wijze de interne controle-aspecten van online real time systemen belicht. De door hem gehanteerde indeling van de maatregelen van interne controle van belang voor online real time systemen is echter niet in alle gevallen duidelijk.

Minicomputers, a big risk - H.W. Honinckman
CA Magazine (augustus 1980) - S 365
door J.C.P.M. Vermeeren

Trefwoord: E 13, B29

Dit artikel kreeg als ondertitel mee "Mini-mizing audit and control problems".

De eerste twee paragrafen van het artikel zijn gewijd aan de afbakening van het probleem. De problematiek die de schrijver behandelt richt zich primair op computers van circa 32 K bytes geheugen, 10 Megabytes extern geheugen met één à twee beeldbuis-werkstations en één regeldrukker met een afdruksnelheid van 150 regels/minuut. De software is buiten de deur gemaakt of als standaardpakket gekocht.

Verder wordt ervan uitgegaan dat er meerdere gebruikers zijn terwijl "echte" data base management systemen als access-methode uitgesloten worden.

Vele van de problemen, die zich in de bovengeschetste situatie voordoen worden eveneens van toepassing geacht op satelliet-mini's toegepast in netwerken.

De problematiek wordt behandeld vanuit de conceptie van "control objectives" volgens Computer Control Guidelines, waarbij aandacht wordt gegeven aan development controls en processing controls.

Indien de software is verkregen als standaardpakket zal deze vaak niet voldoen aan de te stellen eisen ten aanzien van

- voldoende niveaus van audit trail,
- beveiligings- en beheersingsprocedures,
- recovery-routines.

Toch kan ieder standaardpakket uit gezichtspunt van controleerbaarheid "safe" worden gemaakt als de verkoper dat wenst. (Men bedenke dat ook de koper in dezen geen willoze partij is.)

In geval van op bestelling vervaardigde software liggen de zaken anders. De koper kan dan, eventueel geholpen door zijn accountants, bereiken dat de ontwikkelingscontrolestandaards worden gehaald en dat de benodigde hulpmiddelen voor de verwerkingscontroles, zoals bijvoorbeeld audit trails en transactie-logs, aanwezig zijn. Ook in de testfase kan de accountant zijn cliënt zinvol assisteren.

Aan de hand van de control objectives voor processing controls (hfdst. V Computer Control Guidelines) wordt het onderwerp verwerkingscontroles afgehandeld.

Volledigheidshalve worden deze hier weergegeven:

L - to ensure the completeness of data processed
M - to ensure the accuracy of data processed
N - to ensure that all data processed is authorized
O - to ensure the adequacy of management trails.

Door de wijze van verwerking gaat vaak het onderscheid tussen master- en transactiebestanden verloren. Dit kan de doorlooptijd van recovery-procedures verlengen. Aan batch-verwerking inherente controlemaatregelen, kunnen niet toegepast worden terwijl voorts de primaire vastlegging in een niet onbelangrijk aantal gevallen rechtstreeks op de computer plaatsvindt zonder hard copy.

De voornaamste techniek, om control objective N te halen, is aldus de schrijver "anything and everything of even the remotest significance that is processed by, or done to, the system by any user(s) must appear in some audit/management trail, with appropriate information recorded". Er dient dus een volledige logging van alle handelingen te zijn. Voorbeelden van activiteiten en mutatie-logs worden hieronder weergegeven.

Exhibit 5

ABC Limited
Activity Report for 18/MAY/79

TIME	USER CODE	ACTIVITY	FUNCTION
09:01 01	HWH	SIGN-ON	
09.02.10	HWH	MAIN MENU	
09 02 24	HWH	ORDER ENTRY/INVOICING MENU	
09 03 02	HWH	ORDER MAINTENANCE	ADD
09 05 15	HWH	ORDER MAINTENANCE	ATTEMPTED DELETE
09 06 12	HWH	ORDER ENTRY/INVOICING MENU	
09.06.22	HWH	ATTEMPTED ACCESS TO ACCOUNTS PAYABLE SYSTEM	
09:07.42	HWH	SIGN-OFF	

Exhibit 4

ABC Limited
Accounts Payable Supplier Change Register

SEQUENCE NUMBER	DATE	USER CODE	— SUPPLIER — NO.	NAME	FIELD CHANGED	OLD CONTENTS	NEW CONTENTS
38	09/AUG/78	GWS	101	L.B KIROUAC	ADDRESS #1	18 MAIN ST.	3478 EASTWAY
39	18/AUG/78	HWH	201	A.C. LETAL LTD.	TERMS	2/10 N/30	N/30
40	20/AUG/78	HWH	310	B.J. LOADER	NAME	ADDED	B J LOADER
					ADDRESS #1	ADDED	101 FRONT STREET
					ADDRESS #2	ADDED	TORONTO, ONTARIO
					POSTAL /	ADDED	M4X 3L2
					TERMS	ADDED	N/15
					PHONE	ADDED	978-2274
41	28/AUG/78	GWS	121	MAIN LUMBER	NAME	MAIN LUMBER	DELETED
					ADDRESS #1	34 THE DONWAY	DELETED
					ADDRESS #2	DON MILLS, ONTARIO	DELETED
					POSTAL	M4K 3K7	DELETED
					TERMS	2/30 N/60	DELETED
					PHONE	449-8619	DELETED

Voorts dient er een "security"-systeem te zijn dat op basis van operatorcodes, en voor kritische acties ook op basis van passwords, menu's en delen daarvan beschikbaar stelt. De achilleshiel is natuurlijk de beveiliging van het "security"-systeem zelf.

Tenslotte dienen alle transacties door het systeem voorzien te worden van een doorlopend volgnummer en een identiteitsaanduiding (bijvoorbeeld initialen) van de inbrenger (zie voorbeelden). De identificatie kan ontleend worden aan de operatorcode. (Omgevingscontrole op gebruik en beveiliging operatorcode en passwords is dan wel vereist.)

De hiervoor reeds genoemde volgnummers zijn uiteraard ook van belang voor de volledigheid (controle objective N). Ten aanzien van de volledigheid van de correcties wordt geen wezenlijk probleem aanwezig geacht. Zorg voor een zodanige validatie dat geen foutieve posten worden geaccepteerd. Vraag blijft of alle transacties wel ter verwerking worden aangeboden. Hoewel geen volledig afdoende oplossing, is de suggestie om de systemen zoveel mogelijk op transacties te laten anticiperen een waardevolle vingerwijzing.

De juistheid van de verwerking wordt door de handmatige besturing (handholding) positief beïnvloed. Voorts worden goede, op de gebruiker afgestemde foutboodschappen als een belangrijk hulpmiddel aangewezen. Standaardpakketten zijn op dit punt vaak zwak. Hetgeen voor de foutboodschappen wordt gesteld, is evenzeer van toepassing op de gebruikersdocumentatie.

In multi-gebruiker-systemen dient het gelijktijdige bewerken van een gegeven of record door meerdere programma's onmogelijk te worden gemaakt (concurrent updating).

Ten aanzien van de recovery-procedures wordt aanbevolen stam- en mutatiebestanden in fysieke zin strikt gescheiden te houden (bijvoorbeeld afzonderlijke schijfeenheden). Zodoende kan een storing in de hardware niet leiden tot verlies van beide soorten bestanden. Indien leveranciers niet in deze mogelijkheden voorzien, vermijde men hun systeem. Ook wordt het wenselijk geacht de onderlinge consistentie van de gegevensverzamelingen dagelijks te toetsen.

Beveiliging tegen het ongeautoriseerd wijzigen of toevoegen van programma's kan worden bereikt door het verwijderen van de compileerprogramma's uit het systeem (er is toch geen automatiseringsstaf).
Voor "interpreter driven" programmeertalen is deze oplossing niet toepasbaar. Dit type systemen moet worden gemeden, aldus de schrijver, tenzij de leveranciers in een veilig operating system kunnen voorzien.

Wellicht ten overvloede wordt geconstateerd dat accountantspakketten doorgaans niet kunnen worden toegepast en dat speciaal geschreven accountantssoftware doorgaans te duur zal zijn.

Rekening houdend met zijn overwegingen, die hierboven verkort zijn weergegeven, acht de schrijver mini's in menig opzicht veiliger dan grotere computersystemen. Voor het doorzien van de bewakings- en controleproblematiek in de specifieke toepassing zal specialistische hulp echter veelal niet gemist kunnen worden.

IBM System Journal / 1979 nr. 2 - 0 260
P.E. Green - trefwoord: A 54, B 38

An introduction to network architectures and protocols

This tutorial paper is intended for the reader who is unfamiliar with computer networks, to prepare him for reading the more detailed technical literature on the subject. The approach here is to start with an ordered list of the functions that any network must provide in tying two end users together, and then to indicate how this leads naturally to layered peer protocols out of which the architecture of a computer network is constructed. After a discussion of a few block diagrams of private (commercially provided) and public (common carrier) networks, the layer and header structures of SNA en DNA architectures and the X.25 interface are briefly described.

Beveiliging van gegevens op magneetband (naar aanleiding van een artikel in Datenschutz-Berater nr. 8 + 9 van 1978)

door B.M. de Vries

Het extern geheugenmedium magneetband heeft nog steeds bestaansrecht binnen de geautomatiseerde gegevensverwerking, ondanks het toenemend gebruik van magneetschijven en massageheugens. Een reden voor de redactie van Datenschutz-Berater om aandacht te schenken aan de beveiligingsaspecten van de magneetband. Resultaat is een artikel, waarin de beveiliging van magneetbanden vanuit IBM-optiek wordt benaderd.

Fysieke beveiliging van de magneetband

Beperken wij ons tot de magneetband als fysiek fenomeen, dan roepen de beveiligingsproblemen geen nieuwe vragen op. Klassieke maatregelen zoals

- brandbeveiliging,
- fysieke toegangscontrole,
- achter slot opbergen,
- back-up-bestanden,
- bijhouden van een logboek van de magneetbanden,

zijn voldoende.

De beveiliging van de magneetband krijgt pas reliëf, indien we ons richten op het gebruik van de op magneetband opgeslagen gegevens. Beveiligingsmaatregelen mogen niet beperkt blijven tot de magneetband zelf, maar zullen zich moeten uitstrekken tot de software, die gebruik maakt van de magneetbanden. De enige bestaande hardwarebeveiliging op dit gebied is de schrijfring. Zonder deze ring kan de magneetband niet beschreven worden.

Standaardbeveiligingsmaatregelen

Het operating-systeem biedt de volgende standaardbeveiligingsmaatregelen ter beveiliging van de gegevens op magneetband.

1. Labels

   Labeling van de magneetbanden beperkt het gevaar, dat met verkeerde banden wordt gewerkt. Labeling houdt in, dat een identificatierecord (een stukje geheugenruimte) op de magneetband van controlegegevens wordt voorzien, zoals het nummer van de magneetband (volume serial number), naam en volgnummer van de gegevensverzameling(en), password voor de operator. Met behulp van laatstgenoemde label-gegevens kan het gebruik van de magneetband door operators afgeschermd worden.
   Overschrijven van een magneetband kan buiten het gebruik van de schrijfring nog voorkomen worden door het in het label opnemen van een vervaldatum. De waarde van labeling uit hoofde van beveiliging is echter beperkt. Er zijn mogelijkheden om deze beveiliging te omzeilen. Naast labeling zullen aanvullende maatregelen moeten worden genomen.

2. Magneetbanden zonder een label

Bij het gebruik van deze magneetbanden wordt geen van bovengenoemde controles uitgevoerd. Zelfs het verwisselen van de originele magneetband met een vervalste kopie is zeer eenvoudig en de enige manier om dit te voorkomen is een zich op de haspel bevindende onverwijder- en onvervalsbaar kenteken.

Manipulaties met van labels voorziene magneetbanden

Het omwisselen van banden, die voorzien zijn van labels, blijft mogelijk. Dit zal echter in elk goed georganiseerd rekencentrum opvallen, aangezien het nummer (VSR) in de label niet hetzelfde is als dat op de spoel. Verwerking met omgewisselde banden is dan slechts mogelijk met medewerking van de operator(s). Het gebruik van labels biedt dus betere beveiligingsmogelijkheden.
Echter in het operating system bevindt zich een parameter, waarmee het mogelijk is om de van labels voorziene magneetbanden te benaderen als ware het niet van labels voorziene magneetbanden. Deze parameter wordt de Bypass Label Processing (BLP) parameter genoemd. De met het label samenhangende controles worden door middel van deze parameter omzeild. Het gebruik van BLP zou derhalve verboden moeten worden, of nog beter, de BLP zou bij de systeemgeneratie niet in het operating system opgenomen moeten worden. Dit is echter eenvoudiger gezegd dan gedaan. Diverse utilities maken gebruik van deze parameter.
Organisatorisch zou het gebruik van BLP beperkt kunnen worden. De mogelijkheden om het label te omzeilen zijn daarmee echter niet verdwenen.

Het direct uitvoeren van kanaalprogramma's

De gegevensuitwisseling tussen de magneetband-unit en het systeem gebeurt door kanalen welke worden bestuurd door kanaalprogramma's. Een kanaalprogramma bestaat als het ware uit twee gedeelten. Het eerste gedeelte wordt alleen aan het begin van het programma (bij een Open instructie) gecreëerd en gecontroleerd. Het tweede gedeelte kan zowel door het operating system worden gegenereerd als door een eigen programma worden gecreëerd en gecontroleerd. Met behulp van de Assembler-instructie EXCP (execute channel program) is het mogelijk dit tweede gedeelte te creëren en zodoende zonder enige controle van het systeem de magneetband te positioneren, te lezen en zelfs te beschrijven. Met andere woorden, na één legale Open kan de hele magneetband verwerkt worden zonder enige controle (dus hetzelfde effect als bij gebruik van BLP). Het grote gevaar van EXCP werd en wordt nog steeds in veel rekencentra onderschat. De toegangsmogelijkheden met behulp van EXCP worden ontoelaatbaar vergroot en zelfs gebruik van passwords kan dit niet verhinderen.

Voorbeeld 1

Een magneetband met multifile organisation (meerdere bestanden op een magneetband). Iemand heeft toestemming om slechts één bestand van die magneetband te mogen lezen en bezit hiervoor de nodige gegevens inclusief password. Hij opent dit ene bestand legaal en is daarna met behulp

van EXCP in staat de hele magneetband (dus alle andere bestanden) fysiek door te lezen.

Voorbeeld 2

Iemand weet het aantal bestanden op een magneetband (met schrijfring). Hij positioneert de magneetband met behulp van job-besturingsinformatie voor de laatste tape mark en overschrijft deze.
De aard van de bescherming van alle andere gegevens is daarbij niet van belang. Na het schrijven is men in staat, met behulp van EXCP, de hele magneetband te lezen en te beschrijven. Na afloop hiervan kan, weer met behulp van EXCP, de tape mark teruggeschreven worden en eventueel ontstane sporen worden verwijderd en/of vervalst.

Voorbeeld 3

Indien de gegevens op een magneetband verouderd zijn worden deze overschreven. Eventuele restinformatie is met behulp van EXCP weer te benaderen.

Resumerend kan gezegd worden dat indien één bestand legaal geopend is de hele tape "legaal" verwerkt kan worden.

Organisatorisch te nemen maatregelen

- Per magneetband dient slechts één programmeur met het onderhoud van op de magneetband opgeslagen bestanden belast te zijn.
- Gegevens, die privacy-gevoelig zijn, op een aparte magneetband.
- Laatste bestand op een magneetband aanvullen met "fake records" tot het eind van de magneetband, opdat geen lege ruimte op de band ontstaat.
- Magneetbanden met verouderde gegevens schoonmaken alvorens opnieuw te beschrijven.
- Dump-, back-up-, beveiligingsbanden achter slot.
- Herstel van uitgewiste of verminkte gegevens met behulp van deze magneetbanden alleen door daartoe bevoegde personen doen uitvoeren.
- Het gebruik van een uit beheersingsgezichtspunt goed catalogue-systeem.
- Een strikte functiescheiding tussen werkvoorbereider (verstrekking van besturingsinformatie) en de operator.

Tenslotte kan nog opgemerkt worden, dat de bestaande magneetbandkoffers bijna allemaal hetzelfde slot hebben. Bij verzending van "gevoelige" gegevens is het aan te bevelen de koffer te voorzien van een niet-uniform en moeilijk te forceren slot.

In het artikel zijn een aantal mogelijkheden, om ongeautoriseerd bestanden op magneetbanden te benaderen, behandeld. De mate, waarin met name

de Assembler-instructie EXCP (execute channel program) toegepast kan worden, is afhankelijk van de Assembler-kennis van de applicatieprogrammeur.
De in het artikel genoemde organisatorische maatregelen bemoeilijken het onbevoegd benaderen van bestanden op magneetbanden; zij zijn echter niet in staat om dit geheel te voorkomen. De te nemen organisatorische maatregelen dienen op elkaar aan te sluiten om de beveiliging rondom de magneetband te versterken.
Naast de in het artikel genoemde mogelijkheden om magneetbanden te benaderen, moet worden gewezen op de mogelijkheid om via utilities (zoals de IBM-utility DITTO) dit te realiseren. Aan deze mogelijkheid wordt in het artikel geen aandacht besteed.

Automatisering
Beveiliging
Controle
NIEUWS

door drs. H.C. Kocks

Automatisering

Klacht tijdens tiende ACPA-conferentie

De eisen des tijds veranderen met de regelmaat van de klok. Het op de hoogte blijven van vaktechnische ontwikkelingen is thans meer dan ooit noodzaak om zich te kunnen handhaven. Alom komt men het begrip "permanente educatie" tegen. Het volgende artikel gaat over de vak(on)bekwaamheid van de huidige programmeur. De vraag is echter of het feilen van de programmeurs alleen aan hen is toe te schrijven.

Programmeurs vaak niet vakbekwaam

"De meeste programmeurs doen zó weinig moeite om technisch bij te blijven, dat zij voor hun werkgevers eerder een last dan een aanwinst betekenen", aldus dr. Richard Hamming, één van de bekendste programmatuurexperts in de Verenigde Staten. "In veel gevallen zouden de werkgevers zich misschien veel beter kunnen ontdoen van hun meeste programmeurs of ze gewoon doorbetalen en zeggen dat ze maar beter thuis kunnen blijven." Hamming sprak deze woorden tijdens de tiende jaarlijkse conferentie van de Association of Computer Programmers and Analysts (ACPA), die onlangs in San Francisco werd gehouden.

Zoals hun collega's in de meeste andere technisch geavanceerde vakgebieden, beginnen de meeste programmeurs vaak op een technisch hoog niveau aan hun carrière. Maar dat duurt zelden lang. Nog vóórdat zij het zelf in de gaten hebben, beginnen zij in technisch opzicht achter te raken en naarmate de jaren verstrijken, veroudert hun technische kennis nog meer. Tenslotte heeft de techniek hen volkomen ingehaald. Dit was de kern van het betoog van Hamming, die tijdens deze conferentie herinneringen ophaalde aan zijn lange en voortreffelijke carrière bij de Bell laboratoria en andere bedrijven.

Waar ligt de schuld?

"De schuld voor het over het algemeen lage niveau van de vakbekwaamheid van de programmeurs ligt duidelijk bij de programmeurs zelf", zo voegde Hamming eraan toe. "De meeste medewerkers van programmeerafdelingen steken nauwelijks een vinger uit om het technisch niveau te handhaven, dat zij behoren te hebben. Er zijn hier momenteel honderdduizenden programmeurs aan het werk, maar het is misschien wel op z'n minst vijf jaar

geleden sinds de meesten van hen iets buiten hun bedrijf hebben gedaan om hun vakkennis op een hoger peil te brengen", aldus Hamming tijdens een interview na afloop van deze conferentie.
Hamming, die vroeger de leiding had over de Association for Computing Machinery en die nu optreedt als buitengewoon hoogleraar aan de Post-Graduate School van de Amerikaanse marine, wees verouderde vakkennis als één van de voornaamste redenen aan van de over het algemeen lage produktiviteit van de programmeurs.

Alleen de besten

Om de vaak armzalige resultaten van hun programmeurs te kunnen compenseren, nemen vele managers van computerafdelingen eenvoudigweg extra programmeurs aan, maar hierdoor wordt het produktiviteitsprobleem gewoonlijk alleen maar groter. "Als je een project hebt, waarbij je achterop bent geraakt, dan werkt het inschakelen van nog meer mensen alleen maar vertragend", zo stelt Hamming. "Je kunt beter over een paar erg goede programmeurs beschikken en ze een hoog salaris uitbetalen dan over een grote groep tweederangs mensen. Het kost je veel meer wanneer je over tweederangs programmeurs beschikt dan wanneer je er een paar hebt, die werkelijk goed zijn. Het enige doeltreffende middel tegen het probleem van de lage produktiviteit van de programmeurs is het volgen van een strikt beleid, gericht op de professionele ontwikkeling. Dit beleid omvat het lezen van boeken, het bijwonen van bijeenkomsten en het bestuderen van vakbladen", zo stelde Hamming.
Hamming's beleid voor zijn eigen professionele ontwikkeling omvat het 's avonds geven van colleges aan de universiteit, waardoor hij wordt gedwongen de snelle technologische ontwikkelingen van dit vakgebied bij te houden. Af en toe recenseert hij ook boeken en technische artikelen.

In de vuurlinie

"Ik ga regelmatig in de vuurlinie staan, daar waar de actie plaatsvindt. Ik verstop me niet op een veilige plaats. Behalve dat ze moeten voorkomen dat ze professioneel achterop raken, moeten programmeurs ernaar streven dat hun systemen gemakkelijk zijn te gebruiken, te corrigeren en te modificeren, zodat de niet-technische gebruikers hun werk kunnen doen zonder dat ze zich voor ondersteuning hoeven te wenden tot de computerafdeling van hun bedrijf. Programmeurs moeten hun programma's zodanig schrijven, dat een systeem zonder hun hulp kan worden gebruikt. Jammer genoeg zijn de meeste programmeurs bang dat de gebruikers onafhankelijk van hen worden. Als een gevolg daarvan zijn ze voortdurend druk in de weer waardoor ze nauwelijks tijd hebben om na te denken."
Hamming drong er ook op aan dat de programmeurs continu moeten streven naar eenvoud in hun werk. "De meeste programma's", zo stelde hij, "zijn veel te ingewikkeld." Hij drong er ook op aan dat de programmeurs de onder handen zijnde projecten regelmatig opnieuw in ogenschouw nemen gedurende de ontwikkelingscyclus.
Hamming voegt de daad bij het woord. Toen hij nog werkzaam was in Bell laboratoria, reserveerde hij elke vrijdagmiddag om "diep na te denken", waarbij hij ervoor zorgde dat hij niet door alledaagse problemen werd afgeleid.

De Automatisering Gids, 21 januari 1981

Evenals in voorgaande jaren heeft Datapro Research Corporation in 1979 aan gebruikers van standaardsoftwarepakketten de mening gevraagd. In het volgende artikel is een overzicht opgenomen van de 44 pakketten met de hoogste score. In het artikel zelf is aangegeven op welke punten de mening van de gebruikers is gevraagd en hoe het eindcijfer is bepaald. De conclusies dienen met de nodige voorzichtigheid te worden geïnterpreteerd, omdat - zoals Datapro dat zelf heeft weergegeven - er vele factoren meespelen bij het selecteren van het juiste programmapakket.

Vierenveertig pakketten op Datapro erelijst

Vierenveertig programmapakketten zijn door Datapro Research Corporation op de "1979 Software Honor Roll" geplaatst als een gevolg van de kwalificaties, die werden ontvangen in antwoord op een vragenlijst. Deze was verstuurd naar ongeveer 37.000 deskundigen op het gebied van de gegevensverwerking bij bedrijven, die gebruik maken van deze produkten. Slechts dertig pakketten waren vermeld op de erelijst van 1978, aldus een woordvoerder van Datapro.

Hoewel Datapro een aantal van haar interne procedures voor het rapporteren van de onderzoeksresultaten heeft gewijzigd, vermeldt de erelijst nog steeds de pakketten, die de hoogste waardering ontvingen en die werden genoemd en gekwalificeerd door tien of meer gebruikers. De pakketten werden genoemd door de gebruikers zelf en niet gesuggereerd door Datapro.
Hoewel meer dan twaalf pakketten dit jaar voor het eerst op de erelijst staan, worden er vijf al voor de zevende keer genoemd. Dit zijn Alltax van Management Science America Inc., het Disk Utility System van Westinghouse Electric Corporation, Epat van SDI, The Librarian van Applied Data Research Inc. (ADR) en Panvalet van Pansophic Systems Inc.. Vier pakketten werden voor de zesde keer in de lijst opgenomen: Easytrieve van Pansophic, Fast/Dump/Restore (FDR) van Innovation Data Processing Inc., Quikjob van Systems Software Support Inc. en Syncsort van Whitlow Computer Systems Inc..

5.683 reacties

Datapro ontving reacties van 5.683 gebruikers, die kwalificaties gaven van 2.142 pakketten. De complete resultaten zijn opgesomd in het rapport "User ratings of proprietary software", dat 15 dollar kost en dat werd herdrukt van het december-supplement van Datapro 70, het voornaamste naslagboek van deze resesarch-organisatie.
Het rapport verschaft onderzoeksresultaten van de 335 pakketten, die door vijf of meer gebruikers van een kwalificatie werden voorzien, alsmede de financiële gegevens, die door vele van de reagerende organisaties werden verstrekt. Het rapport verschaft ook suggesties over hoe

men programmatuur moet selecteren.
De gebruikers kwalificeerden elk pakket in zeven categorieën, waarbij een waarderingsschaal van vier punten werd gebruikt, die van slecht (1) naar uitstekend (4) liep. Behalve de rubriek "gemiddelde tevredenheid", waren er nog rubrieken voor doorvoercapaciteit, eenvoud van het installeren, gebruiksgemak, documentatie, technische ondersteuning door de leverancier en opleiding. De gebruikers kwalificeerden elk pakket ook nog aan de hand van de voordelen en nadelen, op de tijd, die nodig was voordat de resultaten zodanig waren als was toegezegd en op het feit of er modificaties noodzakelijk waren.
Pakketten, die een gewogen gemiddelde scoorden van 3,5 voor de rubriek "gemiddelde tevredenheid" en 2,8 voor de rubrieken doorvoercapaciteit, eenvoud van het installeren, documentatie en technische ondersteuning door de leverancier, werden vermeld op de erelijst. Datapro gaf een eervolle vermelding aan nog eens 21 pakketten, die ook hoog scoorden in deze rubrieken, maar die slechts door vijf tot negen gebruikers waren gekwalificeerd.

Systeemprogrammatuur

Zoals elk jaar het geval is sinds deze erelijst in 1973 werd opgezet, overheerste de systeemprogrammatuur. Alleen Alltax, het pakket voor het berekenen van de belasting, vertegenwoordigde op deze lijst de toepassingsprogramma's. In de Datapro-overzichten, die de resultaten per categorie voor elk pakket geven, heeft men afgezien van de vroegere gewoonte van het vermelden van het exact berekende gewogen gemiddelde. In plaats daarvan hebben de onderzoekers dicht bij elkaar liggende uitkomsten in groepen ingedeeld.
Als een gevolg van deze verandering zal een leverancier niet meer kunnen wijzen op het feit dat zijn produkt "beter" was - misschien maar één-tiende punt - dan dat van de anderen. In elk geval was men bij Datapro wel zo verstandig om erop te wijzen dat de gegevens in het rapport "met de nodige voorzichtigheid en het juiste begrip" moeten worden gehanteerd aangezien er "vele factoren meespelen bij het selecteren van het juiste programmapakket.

1979 Datapro Software Honor Roll

Seven-Time Member

Alltax — Management Science America, Inc.
Disk Utility System — Westinghouse Electric Corp.
Epat — SDI
The Librarian — Applied Data Research, Inc.
Panvalet — Pansophic Systems, Inc.

Six-Time Member

Easytrieve — Pansophic Systems, Inc.
Fast/Dump/Restore — Innovation Data Processing, Inc.
Quikjob — Systems Software Support, Inc.
Syncsort — Whitlow Computer Systems, Inc.

Five-Time Member

DYL-260 — Dylakor Software Systems, Inc.
1130/Fortran — DNA Systems, Inc.
RPG-II (360/370) — IBM Data Processing Division
Westi — Westinghouse Electric Corp.

Four-Time Member

CA-Sort — Computer Associates, Inc.
IDMS — Cullinane Corp.
SAS — SAS Institute, Inc.
Slick — NCI, Inc.
1130/Sort — DNA Systems, Inc.

Three-Time Member

Adabas — Software AG of North America, Inc.
Extended DOS — The Computer Software Co.
Flee/Flim — Goal Systems
Image/3000 — Hewlett-Packard Co.
Roscoe — Applied Data Research, Inc.
RPG-II (S/3) — IBM General Systems Division
Software 1040 — SAB, Inc.

Two-Time Member

BEM — Univac
Docs — CFS, Inc.
Faqs — Goal Systems
Shadow II — Altergo Software, Inc.
Sort (S/3) — IBM General Systems Division
TLMS — Capex Corp.

First-Time Member

Boost — Macro-4, Inc.
CP/M — Digital Research
Disk Space Manager — Westinghouse Electric Corp.
Dynam/T — Computer Associates, Inc.
FTL — Goal Systems
Logout — Macro-4, Inc.
On-Line Source Maintenance Facility — IBM General Systems Division
OWL — NCI, Inc.
RPG-II (S/34) — IBM General Systems Division
Scepter — Westinghouse Electric Corp.
Space/Manager — Altergo Software, Inc.
SRI/Edit — Systems Research, Inc.
Vollie — Applied Data Research, Inc.

Annonceringen van nieuwe produkten is aan de orde van de dag. Om concurrentieredenen kan een annoncering nadelige invloed hebben, vooral als de datum van beschikbaarheid is aangegeven.

IBM krijgt proces in Frankrijk

De pannenfabriek Tefal heeft bij het hooggerechtshof in Annecy een proces aangespannen tegen de computerfabrikant IBM. Tefal is vooral gegriefd door het feit, dat IBM zeer veel reclame heeft gemaakt voor een computer die nog niet bestond. Tevens was de computergigant nogal rap met het accepteren van bestellingen voor de serie 38, want daar gaat het over. Tefal had dit apparaat besteld aan het eind van 1978, met de garantie van IBM, dat het systeem vanaf oktober 1979 beschikbaar zou zijn. Tefal wil nu van de bestelling af, niet alleen omdat het systeem niet leverbaar is, maar omdat het zelfs nog niet eens bestaat!

Dit proces is tekenend voor de toestand waarin we ons, wat computers betreft, nu bevinden. De gang van zaken brengt twee dingen aan het licht, te weten:

- In hoeverre kan en mag een fabrikant reclame maken voor een apparaat, dat nog in staat van ontwikkeling verkeert?
- In hoeverre kan de fabrikant zich beroepen op de clausules van beperkte aansprakelijkheid, die in het contract zijn opgenomen, als er in feite geen produkt is?

Het is nu aan de rechter, om uit te maken in hoeverre de fabrikant juist heeft gehandeld bij het opstellen van advertenties. Boze tongen spreken reeds van volksverlakkerij.

De Automatisering Gids, juni 1980

Het volgende artikel behoeft geen toelichting. De inhoud spreekt voor zich. Hoewel de meningen over de oorzaak van de mislukking van het project uiteenlopen, is wel duidelijk dat zulke voorvallen leiden tot lering en vermaak.

Rechtbank ziet af van computer

Na een voorbereidingsfase van meer dan zeven jaar heeft het districtsgerechtshof van de stad Grand Rapids (Michigan) afgezien van een geautomatiseerd rechtbankinformatiesysteem. In die periode is meer dan 400.000 dollar besteed aan proefnemingen, onderzoeken en mankracht. Het hele project werd geteisterd door een opeenvolging van vertragingen, defecte apparatuur en "bureaucratische onverschilligheid". Het automatiseringsproject, dat eigenlijk nooit uit de testfase is gekomen, is nu voorgoed in de ijstkast gezet. Men houdt alle informatie gewoon weer handmatig bij.

Eén van de administrateurs van de rechtbank verklaarde het falen van het project als volgt: "Er waren zoveel mensen bij betrokken en nog veel meer personen moesten erover beslissen, dat het project wel gedoemd was te mislukken". Het informatiesysteem was ontwikkeld voor gebruik op de computer van de gemeente, een Burroughs 3500 mainframe.

De bedoeling was, dat het systeem gegevens bij zou houden van parkeer- en verkeersovertredingen, aankondigingen van de rechtbank zou produceren en in het algemeen de communicatie binnen de rechtbank zou bevorderen. Hoewel de programmatuur volkomen was getest en een getrainde staf aanwezig was, kwam het systeem niet van de grond. De meningen over de oorzaak van de mislukking lopen uiteen, maar de meesten zijn het er wel over eens, dat het mis ging toen het project in volle gang was. Rond die tijd werd aangekondigd, dat de stad Detroit haar databank ging uitbreiden, en daardoor verloor het gemeentebestuur van Grand Rapids haar

belangstelling voor het systeem. Hierdoor werd de toekomst van het rechtbanksysteem onzeker en ontstond een vertraging van ongeveer zes maanden. Als gevolg van de wrijving tussen de rechtbank en de stadsbestuurders werd laatstgenoemden zelfs een proces aangedaan. Tijdens de rechtszaak werd de stadsbestuurderen ook verweten, dat zij de belangrijkste programmeur wilden ontslaan, omdat "hij niet aan bepaalde criteria voldeed". De rechtbank won het proces, maar toch werd de programmeur ontslagen.

Vanaf die tijd ging het volkomen bergafwaarts met het rechtbanksysteem. Door het vele werk, wat de gemeentecomputer moest verzetten, was er bijna geen tijd vrij om het rechtbanksysteem te testen. Dit alles kostte veel tijd en geld, zoveel zelfs dat men nu maar heeft besloten om er totaal van af te zien.

De Automatisering Gids, 10 september 1980

Bankgirocentrale ontvangt nu ook betalingsgegevens per telefoonlijn

Aldus de kop van een artikeltje in Computable van 28 november 1980. Thans wordt bij vervoer van gegevens gebruik gemaakt van zogenaamde transportable media als cassettes, magneetbanden, ponskaarten, enz., welke vorm van vervoer niet in alle gevallen even accuraat en veilig blijkt te zijn. Wel dient men zich af te vragen welke controlemaatregelen binnen en buiten het computercentrum (extra) moeten worden genomen om de nieuwe transportfaciliteit in alle gevallen accuraat en veilig te doen zijn.

De aanlevering van betalingsgegevens bij de Bankgirocentrale is een proces waarbij voor het vervoer van de gegevens nog veelvuldig gebruik werd en wordt gemaakt van transportable media zoals cassettes, flexibele schijven en magnetische banden.
Deze vorm van vervoer blijkt niet in alle gevallen even accuraat en veilig te geschieden. De bankgirocentrale heeft echter voor de verbinding met klanten die van hun telefoon en eigen computer gebruik willen maken voor het verwerken van betalingsgegevens, een 2780 protocol-emulator op de eigen Burroughs-machine gerealiseerd.
Gekozen is voor deze emulator omdat na onderzoek bleek dat bijna alle cliënten van de Bankgirocentrale die zich geautomatiseerd weten, gebruik (kunnen) maken van dit protocol. In de toekomst wordt eveneens gedacht aan het implementeren van het IBM 3780 protocol en wellicht X-25. De meeste bedrijven die nu hun gegevens overzenden zijn kleine en middelgrote banken.
Daarnaast zijn enkele bedrijven ertoe overgegaan hun gegevens via deze datacommunicatiemogelijkheid te laten verwerken. Met name Beko, een bakkersinkoopcombinatie op een Datapoint computer en Unox in Oss met

een Data 100 machine sturen de betalingsgegevens per telefoon op. De problemen die zich voordeden bij de conventionele wijze van verzenden, zoals het niet op tijd kunnen verwerken van de gegevens door verlate postbestelling, de gebrekkige beveiliging en het niet tijdig kunnen uitbetalen van salarissen, lijken hiermee tot het verleden te behoren.

Computable, 28 november 1980

Beveiliging

A computer anecdote uit Operating Systems Review, april 1980.

Hoewel bijna niet te geloven, toch "absolutely true".

This story is absolutely true. Names have been omitted for obvious reasons.

Several years ago I worked as a systems programmer at an eastern university. We had a single IBM 360/65 to serve all elements of the campus not only teaching and research, but also the administrative chores of grades and payroll.

The university had a large number of very bright and energetic students. Some of these students regarded the computer system security as a personal challenge. Since we were running OS/360, there were plenty of opportunities for these students to crack the system and run their programs for free. The most talented group gave us fits for months. The system had been behaving strangely for some time. One day it crashed in a manner that was totally beyond any reasonable explanation. Suspicious, we checked the user jobs in the system. On one printer, we found a listing of a very professional looking program. The comments at the beginning of the program said "The purpose of this subroutine is to turn off the system accounting routines, allowing the user job to run for free. This is proprietary software, and may not be used without the permission of" and went on to list three names and phone numbers and the address of one of the campus fraternities!

The technique they were using was basically correct; however, one small error had caused the mysterious crash. We took the three students named in the program before the university judiciary. One of them, who seemed to be both the smartest and most aggressive, brashly told the judiciary that the computer center should simply make the system impregnable, so that students couldn't steal computer time!
This student, who had already given a very convincing demonstration of his ability, was accordingly sentenced by the judiciary to carry out his own recommendation. As a first step, he was told to go through OS/360 and make a list of the important security loopholes. He began to methodically study the code and write notes about how to penetrate the system security. After he had counted about a hundred major loopholes, his note taking became less thorough, and he was seen walking up and down the halls of the computer center, head down, hands in pockets, mumbling "Boy, what a mess" in a discouraged voice. Finally the boss

took pity and set him to work on the next phase of his sentence, which was to plug the loopholes he had found, and mousetrap the holes that couldn't be plugged. This improved his morale, since he enjoyed thinking up clever little mechanisms, and in fact was quite good at it. Soon his efforts began to show results, as other students attacked the system security. About once a month he would go around to the other programmers with a particularly damning piece of evidence, chortling "Boy, is this guy an amateur, he doesn't know the first thing about OS!". Then he would be off for a visit with his old friend the judiciary, to instruct some hapless student in the error of his ways.

Eventually our creative student was deemed to have paid his debt to society, and so he was put on the computer center payroll as a security expert. One of his tasks was to pester IBM to design better security into OS. The lobbying from its customers finally caused IBM to produce a package called RSS, which was advertised as a set of changes to OS which could make it quite secure. Our security expert was amazed that IBM would make such a claim without some fundamental redesign of OS, since he had become convinced that the worst security problems were embedded in the basic design of the system. He obtained a copy of RSS and eagerly studied it.
Sure enough, there were still a number of loopholes! The experience with the judiciary had not changed his basic outlook on life, so he sought to expose IBM's pretentions in the most decisive manner possible. He carefully wrote a user's manual describing how to use half a dozen of the larger loopholes in RSS, made several hundred copies, and passed them out at the next SHARE.

Our "reformed" student never really lost his independent attitude. He had particular difficulty with the operations manager, whose firm conviction it was that operators should always do exactly as they were told. The student was convinced that this was an absurd policy, and set out to prove it. One day one of the disk packs for the 2314 drives became damaged beyond repair, so field service threw it in the waste-basket. Our student fished the pack out, took it home and disassembled it. He threw away the platters and reassembled the hub with eleven old phonograph records where the platters had been. Then he took this concotion back to the computer center, put it into a standard disk pack cover, put the covered pack on the shelf with a normal-looking label, and ran a program which asked the operator to mount the pack on a disk drive. Of course the spurious pack with the phonograph records was much lighter and looked quite different from a normal pack.
Unfortunately, the operations manager had carried out his policy with great thoroughness. The operator did exactly what the computer told him to do; he mounted the imitation pack on a disk drive and started it spinning! Needless to say, the results were spectacular. The spindle disintegrated, hurling ball bearings all over the machine room.
Our student felt that he had proved his point. However, neither field service nor the computer center management was much entertained, and the price of the spindle was deducted from his paycheck.

Op Oeso-studiekonferentie blijkt:

Achttien landen gaan akkoord met privacy-richtlijnen

Enige tijd geleden zijn achttien van de vierentwintig landen, die zich in de Organisatie voor Economische Samenwerking en Ontwikkeling (Oeso) hebben verenigd, akkoord gegaan met richtlijnen ter bescherming van de privacy bij internationaal gegevensverkeer. Dit is gebeurd op een studieconferentie, die het afgelopen najaar door de Oeso in Parijs was georganiseerd. Ook Nederland bevond zich bij de achttien voorstemmers; de overige zes, te weten Australië, Canada, Ierland, Turkije, het Verenigd Koninkrijk en IJsland onthielden zich van stemming. Voor het merendeel van hen bleek dat echter slechts een tijdelijke zaak te zijn; eerst zouden daar nog een aantal problemen, zoals grondwettelijke bezwaren, uit de weg moeten worden geruimd.

Computable, 23 januari 1981

Hoewel Nederland nog geen privacy-wetgeving heeft, heeft ze zich wel akkoord verklaard met de Oeso-richtlijnen inzake bescherming van privacy. De stand van zaken in de vierentwintig Oeso-landen wordt in het volgende overzicht weergegeven en enigermate toegelicht.

Stand van zaken op het gebied van wetgeving voor de bescherming van de privacy in de vierentwintig Oeso-landen

	Nationale privacy-wet aanwezig	Aan wetsontwerp op privacy-gebied wordt gewerkt	Voorbereidende maatregelen (rapporten e.d.)	Nauwelijks noemenswaardige activiteiten	Houding t.a.v. Oeso-richtlijnen ')
Australië			●		o
België		●			a
Canada	●				o
Denemarken	●				a
Finland			●		a
Frankrijk	●				a
Griekenland				●	a
Ierland				●	o
Italië			●		a
Japan			●		a
Luxemburg	●				a
Nederland		●			a
Nieuw-Zeeland	●				a
Noorwegen	●				a
Oostenrijk	●				a
Portugal			●		a
Spanje		●			a
Turkije				●	o
Ver. Staten	●				a
Ver. Koninkrijk			●		o
West-Duitsland	●				a
IJsland		●			o
Zweden	●				a
Zwitserland		●			a

') Toelichting: Een "a" wil zeggen, dat het desbetreffende land akkoord is gegaan met de Oeso-richtlijnen, een "o" betekent dat men zich van stemming heeft onthouden.

Controle

In het volgende een korte samenvatting van Steve Hinde inzake een onderzoek van het generalised audit software package PANAUDIT, dat gebaseerd is op EASYTRIEVE.

Audit tools

Tools that the auditor can use to check the inner workings of a computer are coming into fashion. In this article Steve Hinde of Brook Bond-Oxo examines PANAUDIT and EASYTRIEVE, the interrogation language on which it is based.

Pansophic's PANAUDIT is a generalised audit software package based on EASYTRIEVE, and can only be run on IBM and UNIVAC computers.
The cost of PANAUDIT is £3000 for OS and £2500 for DOS, whilst EASY-TRIEVE, which is a prerequisite, costs between £4000 and £10250 (depending upon the operating system and whether it is to be used exclusively by auditors or also by DP).

PANAUDIT's main advantage seems to be for the audit department that has limited manpower or expertise in computer auditing. With its use of audit routines and straightforward use of English commands and keywords, it enables the auditor to access information independently from computer based data quickly and easily with techniques that the non-EDP auditor can use as readily as the EDP auditor. PANAUDIT can also be used as a base to build up sophisticated interrogations using its Command System and user-written EASYTRIEVE modules.

PANAUDIT is not just for auditors. In fact, the test data generation enhancement currently being developed will be of interest to systems and programming departments, as will PANAUDIT's other facilities.
The summary of Release 1.0 PANAUDIT which follows has been extracted from the User's Manual. Additional features will be included in Release 2.0. These are summarized later in the article.

PANAUDIT features

General

English language format
Automatically formatted reports
Automatically centred reports
Automatic column headings
Self-documenting audit trails
Simple use of Boolean logic (IF, AND, OR)
Simple use of all relational operators (equal to, less than, etc.)
Simple file statements
Mathematical calculations following normal sequence
No compile or testing time
Execution at I/O speeds

File input

Accepts an unlimited number of input files in a single job
Extracts information from any storage facility
Operates with sequential, indexed-sequential, VSAM, or data base files such as IMS, DL1, TOTAL, IDMS
Allows data to be in alphanumeric, packed, packed-unsigned, or binary form

Record selection

Matches and merges any number of files in a single job
Permits any number of condition sets per job
Searches files and performs logical data selection based on input or calculations

Operations

Performs special tests such as end of file, blanks, sort status, test under mask, numeric and alpha tests, matched files, and control break tests
Calls user programmes and sub-routines and integrates them into the job
Sorts on up to ten keys
Has nine control break levels for sub-totals plus final totals

Output

Writes any number of output files
Prints any number of reports
Formats and centres reports automatically with many options for user modifications
Provides automatic or alternate column headings

PANAUDIT routines

PANAUDIT routines may be sub-divided into:

1. System Ranking Routines
2. Generalised Audit Routines
3. SMA and DOS/VS Routines

These routines are held in the Command System, and are included in a job by use of the word "INCLUDE". The user may write additional routines and add them into the Command System. Routines may have other routines included (nested) in them up to a level of five nests. A Data Dictionary facility provides for the storage of file definitions. The dictionary is also held in the Command System.

System Ranking Routines

The System Ranking Routine provides a rational, consistent and flexible approach to establishing a priority for systems to be audited. A three level hierarchical data base structure is established for all systems. In addition to ranking the various systems, the reports produced can serve a number of functions, such as:

A list of all systems and their characteristics;
A history of audits;
Evidence for third parties demonstrating the assessment process;
Sensitivity analysis by changing selected parameters and evaluating the effect of the change.

Generalised Audit Routines

The audit routines built into PANAUDIT may be divided into five areas, viz:

Integrity Tests;
Data and Time Routines;
Statistical Auditing;
Number Function Routines;
Generalised Utility Routines.

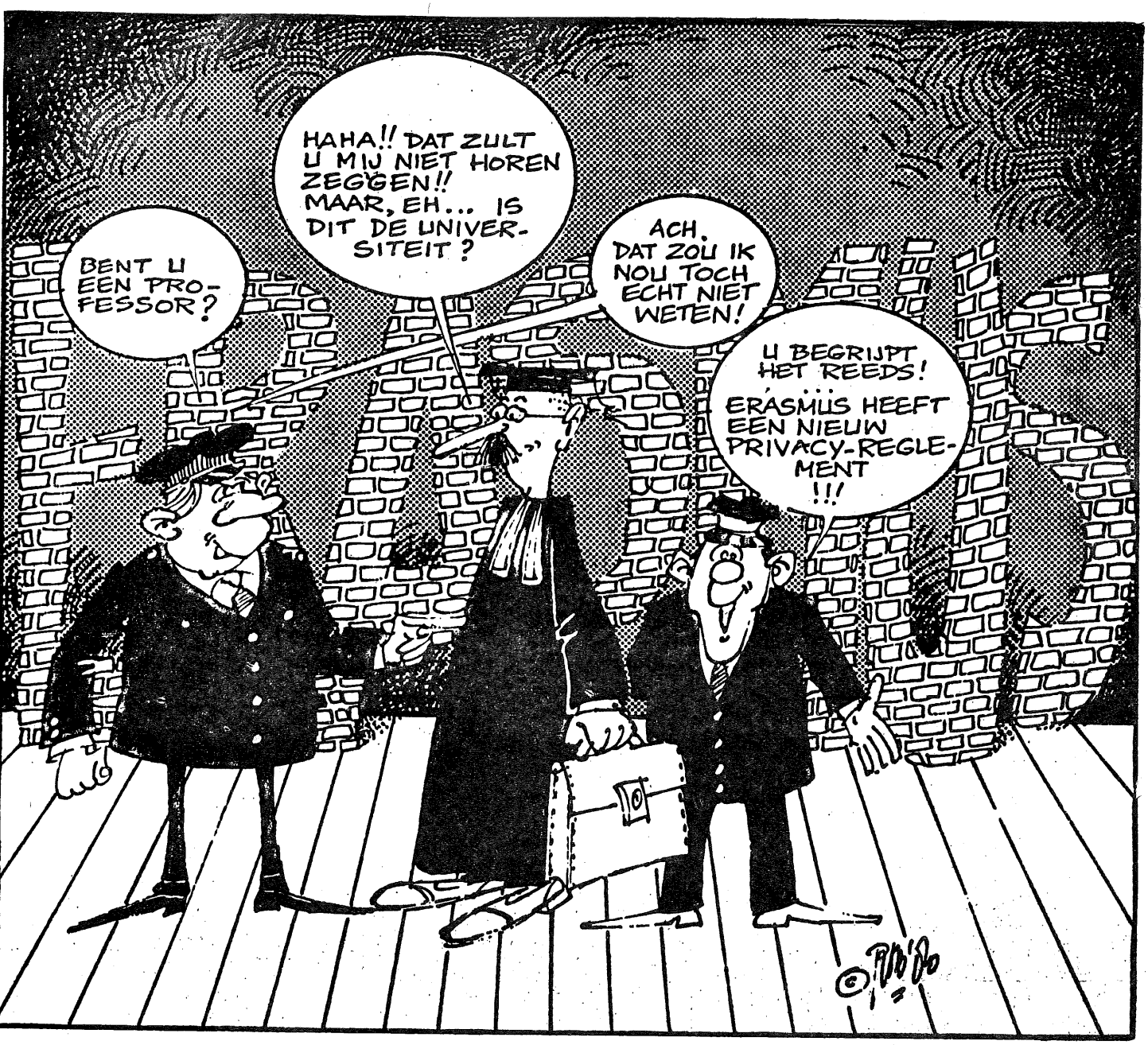
SMF and DOS/VS Routines

There are a variety of SMF routines, including IPLs, abnormal step terminations, abnormal job terminations, control output forms, SMF lost data, data set activity, scratched data sets, renamed data sets, all frequency distribution of record types showing record collection activities.

The DOS/VS job accounting facility is accessed to provide information in the following areas: job log analysis; DITO usage analysis; cancel code analysis; program usage; and program problem trends.

Release 2.0 will appear in Juni 1980. It includes the following additional facilities: test data generator; duplicate records routine (SUPERDUP) which will test on up to four user selected keys for duplicates; ageing report in which the user defines up to 10 time intervals; more SMF routines; SYSLOG (console log) analysis; comparison of two source programmes with identifications of all changes, deletions, additions.

Computer Fraud & Security Bulletin, Vol. 2, No. 8



Uit Quod Novum
Weekblad van de Erasmus Universiteit
d.d. 10 september 1980.