KMG Klynveld Kraayenhof & Co.
Automatisering & Controle-groep

COMPACT 8511

Computer en Accountant

Hoe betrouwbaar zijn onze computers?
door A.W. Neisingh

Beveiliging in lokale netwerken
door Ing. H.A.J.M. Spape

Basic groeit
door J.E. de Bue

Computerverzekering
door J.F.C. van Epen

Nummer 37 11e jaargang winter 1984/1985

COMPACT

COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE

nummer 37 11e jaargang winter 1984/1985

Winter 1984/1985

VAN DE REDACTIE

Dit is het laatste nummer van jaargang 11 en wel het winternummer. Hoewel laat dit keer - de griep velde ook een deel van de redactiestaf - willen wij u deze aflevering niet onthouden.

COMPACT speelt graag tijdig in op nieuwe ontwikkelingen op AC-gebied. Wij hebben deze keer zes primeurs voor u.

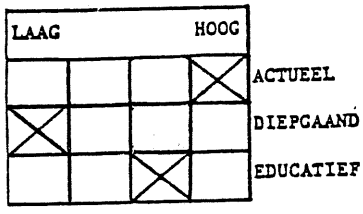
In onze rubriek actualiteiten kunt u lezen over:
- K-Memory, blz. 5;
- Cursussen 85-86, blz. 5;
- Opleidingsbeurs, blz. 6;
- Data base en accountant, blz. 6;
- Nieuw AC-fact sheet, blz. 7.

Over Computerverzekering, blz. 32.

Ook uit de hoofdartikelen springt het begrip actualiteitswaarde naar voren. De betekenis is niet synoniem met snelheid of spoed zonder meer maar vereist ook een weloverwogen oordeel over deze recente informatie die op zichzelf juist, volledig, tijdig alsmede goedgekeurd moet zijn.

Hoe betrouwbaar zijn onze computers?

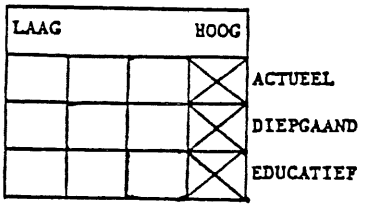
door A.W. Neisingh



Het artikel is met de losse hand geschreven voor het blad "Het Bestuursjournaal". De lezerskring wordt gevormd door het commissarissen en bestuurders van bedrijven die als regel beperkte mogelijkheden hebben om kennis te nemen van alle facetten van automatisering. Echter wel een categorie leidinggevenden met grote verantwoordelijkheden voor automatisering en controle. De schrijver tracht een aantal dringende attentiepunten onder hun aandacht te brengen.

Beveiliging in lokale netwerken

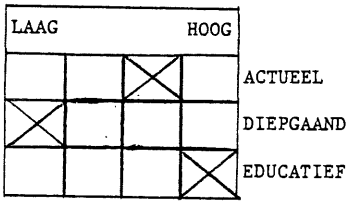
door ing. H.A.J.M. Spape



Door specifieke eigenschappen van lokale netwerken onderscheiden deze zich voor wat betreft beveiligingsaspecten gedeeltelijk van "grote" netwerken. Dit artikel beoogt een aanvulling te zijn op reeds veelvuldig verschenen literatuur inzake beveiliging van netwerken in het algemeen. De specifieke beveiligingsproblematiek van lokale netwerken alsmede de daaruit voortvloeiende mogelijkheden en beperkingen ten aanzien van de beveiliging worden belicht. Het artikel vooronderstelt voorkennis van datacommunicatie in het algemeen en enige begrippen inzake lokale netwerken in het bijzonder.

Basic groeit

door J.E. de Bue



Dit artikel, informatief van aard, beoogt een beeld te geven van de geschiedenis van BASIC vanaf het ontstaan aan het Dartmouth College in 1963 tot nu. Daarnaast zal de mogelijkheid van het gebruik van rechtstreeks toegankelijke bestanden (random access files) als een voorbeeld van de mogelijkheden van Microsoft, BASIC, besproken worden. Het doel van dit artikel is de lezers erop attent te maken dat Basic niet voor niets zoveel gebruikers kent (vanwege de eenvoud en het ongestructureerd programmeren met deze taal). Gebruikers echter, die in vele gevallen de mogelijkheden van BASIC onderschatten.

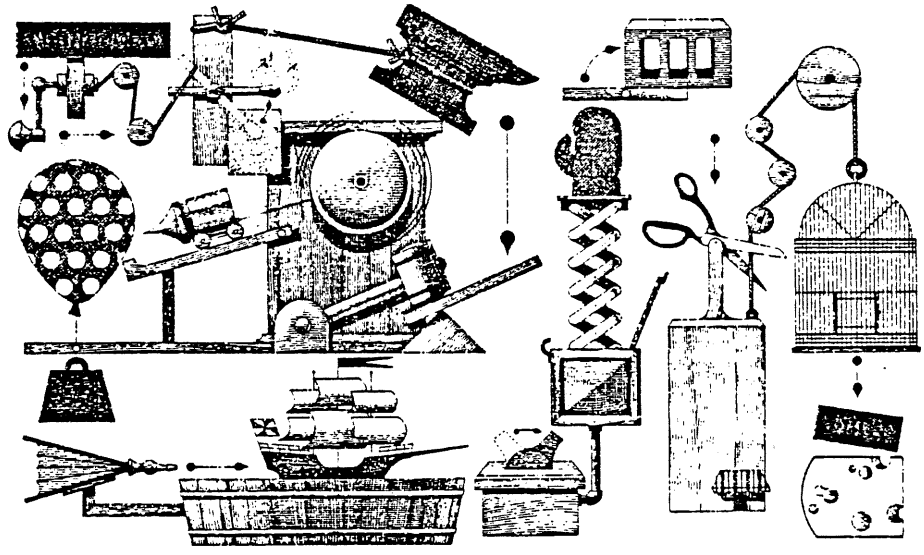
Rubrieken

De inhoud van de rubrieken wordt zorgvuldig geselecteerd uit de grote hoeveelheid "info" die wordt aangeboden.
Wat is nieuw, Wat is goed doordacht, Wat is goed geformuleerd, Wat hebben we er aan zijn de informele kriteria, die de min of meer blijvende waarde bepalen.

Korte inhoud.

Voor uw bijdrage - geachte lezer - is steeds plaats beschikbaar in ons blad, al dan niet voorzien van commentaar van redactiezijde.
Wij zijn zeer attent op uw signalen.
Bij voorbaat dank.

In het blad VAX/RSTS provisional van februari 1985 vonden we onderstaand plaatje, aangevend hoe ingewikkeld de samenhang van een computersysteem soms lijkt of blijkt.
TIME IS ON YOUR SIDE is de titel van het artikel dat begint met de volgende troostrijke gedachte.
"When God made time he made plenty of it. But when you're running a programming project, you might not always believe it."



Winter 1984/1985

COMPACT (R) is een uitgave van de
Automatisering & Controle-groep van
KMG Klynveld Kraayenhof & Co.

Deze informatie is in de eerste plaats bestemd voor diegenen, die in de algemene controlepraktijk werkzaam zijn. De in dit tijdschrift weergegeven meningen mogen niet altijd gezien worden als officiële zienswijzen van KMG Klynveld Kraayenhof & Co. De in de rubrieken besproken artikelen worden soms geheel opgenomen of verkort aangehaald, tevens als regel voorzien van commentaar.

Redactie:
Drs. J.E. Huizenga,
A.W. Neisingh,
Prof. D. Steeman en
H.J.M. van der Wielen (secr.).

Kopij kunt u inleveren bij de
secretaris van de redactie.
Adres:
Prinses Irenestraat 59,
1077 WV Amsterdam.
Postadres:
Postbus 7137
1007 JC Amsterdam.

Indien u belangstelling heeft voor meerdere exemplaren kunt u deze aanvragen bij de secretaris van de redactie, evenwel zolang de voorraad strekt (telefoon 020 - 5461394).

ACTUALITEITEN

1. K-Memory

Onze overkoepelende organisatie KMG - u weet Klynveld Kraayenhof & Co. is een van de oprichters van Klynveld Main Goerdeler - heeft de eerste KMG Computer Newsletter, genaamd K-Memory het licht doen zien.

Het blad is in eerste aanleg voor intern gebruik.
De volgende onderwerpen worden daarin behandeld:
- introductie van K-Memory;
- KMG projects: the state of the art.
  Hierin wordt de audit software voor KMG besproken, zoals:
  . WISPR (het produceren van "Workpapers");
  . PASS (steekproef);
  . Concept Consolidation;
  . CARS.
- Verder nieuws over KMG-seminars voor KMG en/of derden.

Voor belangstellenden - ook voor onze cliënten - is een exemplaar beschikbaar. U kunt een exemplaar bij de redactie van Compact aanvragen.

2. Cursussen 85-86

Ons Bureau Opleidingen is verheugd te melden dat onze nieuwe brochure gereed is.
Nadere gegevens of inlichtingen ontvangt u van
Klynveld Kraayenhof & Co.
Bureau Opleidingen
Antwoordnummer 17414
1000 SN AMSTERDAM
U kunt ook een exemplaar bij ons redactiesecretariaat aanvragen.

Onder de rubriek Onderwijs hebben wij het overzicht van het programma van de open cursussen opgenomen (pag. 7 tot en met 10 van de brochure).

3. Opleidingsbeurs

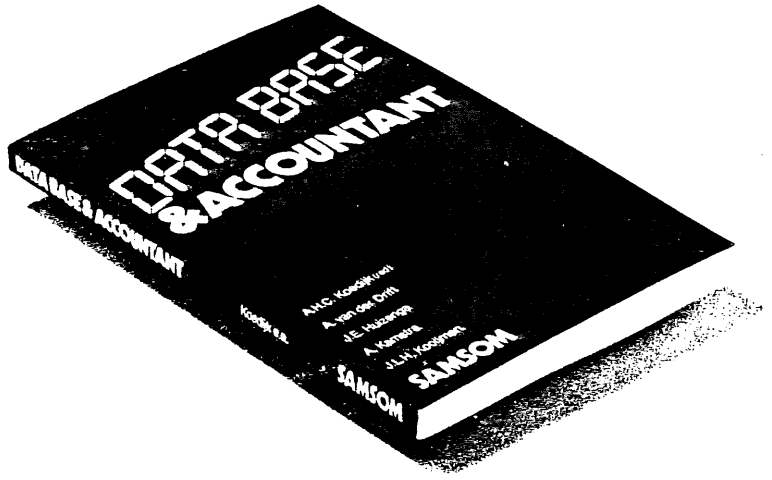
KKC heeft een stand op de Opleidingsbeurs
die van 16 tot en met 18 april 1985
gehouden zal worden in de Jaarbeurs Utrecht.
Tijdens de openingsuren 10-17 uur
zullen in de Bernhardhal I
ook leden van de AC-kern aanwezig zijn.
Wij zullen gaarne uw vragen over
opleidingsmogelijkheden beantwoorden.

Opleiding & Training

4. Data base & accountant

Nu verkrijgbaar:
Data base & accountant.

Sinds 7 februari 1985 jongstleden ligt de volledig vernieuwde uitgave van DATA BASE & ACCOUNTANT nu in de erkende vakboekhandel. De winkelprijs bedraagt f 39,50.
Zoals bekend is dit boek thans een 100% KKC-produkt. Aan het boek werkten mee A.H.C. Koedijk (redacteur), A. van der Drift, J.E. Huizenga, A. Kamstra en J.L.H. Kooijman.
Bij BDI bevinden zich exemplaren van het boek om uit te lenen. Voor een korte beschrijving van de inhoud wordt u verwezen naar Compact nummer 36, herfst 1984.



5. Nieuw AC-fact sheet

KMG Klynveld Kraayenhof & Co. introduceerde de AC-groep als gespecialiseerde groep in 1973.
Dit om het hoofd te bieden aan gerezen controle/beveiligingsproblemen veroorzaakt door de automatisering van de informatieverzorging alsmede om een passend antwoord te kunnen geven op de nieuwe ontwikkelingen, die zich regelmatig aandienen.

Opdrachten tot onderzoek en/of assistentie terzake van automatisering en controle alsmede verzoeken tot opleiding op dit gebied bereiken ons van verschillende categorieën opdrachtgevers, te weten van:
- collega's binnen de KKC/KMG-controlepraktijk zowel in Nederland als daarbuiten;
- het management van bedrijven, instellingen of vanwege de overheid;
- partijen die gezamenlijk gebruik maken van computercentra en/of netwerken;
- verbijzonderde instanties op AC-gebied.

Hoofdactiviteiten:

Terzake van regelmatige opdrachten tot controle van de jaarrekening
- ondersteuning van de collega's, die belast zijn met opdrachten voor de algemene jaarrekeningcontrole, speciaal bij onderzoeken van:
  . automatiseringsorganisaties, computer operations;
  . informatiesystemen (in exploitatie, in het stadium van voorbereiding);
- ondersteuning inzake het gebruik van de computer (mainframes zowel als micro's) voor het toetsen van de automatiseringsorganisatie en voor bestandsonderzoeken.

Bij de opleiding/voorlichting
- samenstellen gevolgd door het geven van AC-cursussen dan wel het geven van adequate training (zie onze brochures op dit gebied);
- het verzorgen van voordrachten op eigen of door derden georganiseerde AC-dagen;
- het publiceren van een intern vaktijdschrift Compact met relevante AC-informatie;
- het uitgeven van KKC-brochures:
  . Kleinschalige automatisering;
  . Computerbeveiliging;
  . SWIFT;
- het publiceren van boeken op AC-vakgebied.

Het plegen van research op het gebied van beveiligings- en controleproblematiek onder meer gericht op:
- Data base management systems;
- Operating systems;
- Data-communication;
- On-line operations;
- Risk management/Risk analysis;
- Audit micro.

Bijzondere opdrachten
Door de verkregen technische deskundigheid als gevolg van ervaring en research worden regelmatig ook opdrachten uitgevoerd welke buiten de jaarrekeningcontrole liggen, zoals op het gebied van:
- beveiliging van gegevens en rekencentra;
- privacy;
- grensoverschrijdend gegevensverkeer;
- beoordeling van de doelmatigheid en doeltreffendheid van organisaties en processen;
- zelfstandig onderzoek naar betrouwbaarheid van opzet en werking van automatiseringsorganisaties en informatiesystemen, gevolgd door een mededeling ten behoeve van derden;
- optreden als deskundige in arbitrages;
- technische en operationele reviews (audits) terzake van automatisering;
- enquetes met uitwerking daarvan met behulp van eigen programmatuur;
- risico-analyse, onderkenning van continuïteitsbedreigende factoren door automatisering.

Bemanning
De AC-groep wordt centraal geleid door 6 vennoten en bestaat verder uit:
- 11 EDP-auditors;
- 15 aankomend EDP-auditors;
- 17 programmeurs.

Derhalve 49 personen die zich in volledige dagtaak met het vakgebied automatisering en controle bezighouden. Daarnaast ca. 35 AC-accountants, verspreid over de vestigingen van KKC in Nederland, België etc. op part-time-basis met AC-werk belast.

Allen hebben een gerichte opleiding ontvangen op het gebied van:
- systeemontwerp, programmering, alsmede operating;
- beoordeling van automatiseringsorganisaties en informatiesystemen;
- controle met behulp van de computer.

Bovendien krijgen jaarlijks 8 à 9 stagiairs de gelegenheid om onder deskundige leiding hun stage-opdracht uit te voeren. Deze opdrachten houden nauw verband met de werkterreinen van de AC-groep.

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

COMPACT

Winter 1984/1985

HOE BETROUWBAAR ZIJN ONZE COMPUTERS?

door A.W. Neisingh

De betrouwbaarheid van computers is afhankelijk van de mate waarin de organisatie voldoet aan bepaalde eisen, met andere woorden of "een adequaat stelsel van maatregelen in die organisatie is opgenomen". Zo'n stelsel moet waarborgen dat niet toegestane handelingen worden voorkomen of tijdig kunnen worden ontdekt.
Een groeiend aantal huishoudingen is steeds meer afhankelijk van een ongestoorde geautomatiseerde informatieverwerking. Uitval van de computer kan men zich niet veroorloven. Indien wel afgewogen maatregelen ontbreken kan op het moment van langdurige uitval niet met de beschuldigende vinger naar de computer worden gewezen. Op de aspecten die hierbij een rol spelen zal hier nader worden ingegaan.

Beleid

Automatiseringsbeleid

Het definiëren van beleid, het concretiseren en uitvoeren ervan en vervolgens het beheersen ervan (control) zijn nauw verbonden. In de praktijk blijkt dat vaak onvoldoende wordt nagedacht over de doelstellingen van een onderneming in verband met het daaruit af te leiden automatiseringsbeleid. Zo komt het nogal eens voor dat ambitieuze automatiseringsplannen worden ontwikkeld, waarvan het fundament niet in de onderneming kan worden teruggevonden. Het automatiseringsmanagement gaat dan op de filosofische toer en bedenkt de meest geavanceerde geautomatiseerde informatiesystemen (relationele data base management systemen, gedistribueerde gegevensverwerking, integratie van persoonlijk computergebruik met tekstverwerking en tekstverwerking met verwerking op grote computers enz.), terwijl de basis in casu de gebruikersorganisatie zich in deze plannen niet kan herkennen en ook niet de inspanning kan leveren om deze ambitieuze plannen te realiseren. Kapitaalvernietiging en een verspilling van kostbare inspanning is het gevolg.

Beveiligingsbeleid

Met de introduktie van automatisering en daardoor toenemende concentratie van risico's krijgt beveiliging meer nadruk.
De verdergaande ontwikkeling in de automatisering - verandering van seriegewijze gegevensverwerking naar onvertraagde postgewijze gegevensverwerking en persoonlijk computergebruik - brengt de noodzaak met zich mee fundamenteel over de eisen die aan beveiliging van die geautomatiseerde gegevensverwerking dienen te worden gesteld, na te denken. Het zal duidelijk zijn dat met name op het gebied van de toegangscontrole steeds zwaardere eisen moeten worden gesteld. Gaat men om de concretisering van die eisen heen dan zal dit veelal betekenen dat de automatisering in casu de programmatuur en de gegevensverzamelingen voor iedere gebruiker "open" is.
De continuïteitsaspecten van de geautomatiseerde verwerking verdienen ook bijzondere aandacht. Immers, de overgang naar onvertraagde postgewijze verwerking betekent dat vaak honderden gebruikers via terminals aan het computersysteem zijn gekoppeld en dat - ingeval zich een storing van enige omvang voordoet - het systeem zichzelf in de laatste goede stand moet kunnen terugvinden.
Indien de beleidslijnen inzake de beveiliging van de automatisering niet zijn gedefinieerd kunnen onevenwichtige situaties ontstaan die leiden tot ongecoördineerde ad hoc-oplossingen. Systeemontwerpers en informatie-analisten gaan afzonderlijk bedenken op welke wijze in hun werk aan betrouwbaarheids- en continuïteitseisen kan worden voldaan, zonder het geheel te kunnen overzien. Het totale kader - de beleidsvisie - ontbreekt.

Evenals bij het ontbreken van een automatiseringsbeleid zal bij het ontbreken van een beveiligingsbeleid kapitaalvernietiging optreden, alsmede kostbare (menselijke) inspanning verspild worden. Bovendien bestaat het risico dat wanneer hier en daar wel wat wordt gedaan het gevoel en de indruk kan ontstaan dat de zaak "wel goed zit".
Naast een goed beleid op het gebied van beveiliging is de uitvoering en de aanpassing aan gewijzigde omstandigheden essentieel. Dan blijven de risico's die gelopen worden bekend en kunnen er maatregelen worden genomen om onacceptabele risico's te beperken.

Risico-analyse

Vaak is het moeilijk te beginnen met het definiëren van een beveiligingsbeleid. Daarom behelst de beleidsvoorbereiding het uitvoeren van een risico-analyse.
Een risico-analyse beoogt op objectieve wijze vast te stellen welke risico's in welke omvang aanwezig zijn en daarmee een richtsnoer te zijn voor het treffen van maatregelen. De uitkomst van een risico-analyse geeft onder andere aan of er onevenwichtigheid bestaat in het

stelsel van maatregelen en of ten onrechte op deelgebieden de klemtoon is gelegd bij het treffen van maatregelen. Er dient evenwicht (een stelsel van maatregelen) te zijn tussen organisatorische, technische en in programmatuur opgenomen controle- en beveiligingsmaatregelen. Het niet uitvoeren van een risico-analyse leidt er nogal eens toe dat gekozen wordt voor slechts enkele maatregelen uit het palet van beschikbare controle- en beveiligingsmaatregelen, zodat er belangrijke leemtes blijven bestaan.

Noodvoorzieningenplan

In het voorgaande werd reeds vermeld dat bedrijven steeds meer afhankelijk worden van het voortdurend beschikbaar zijn van geautomatiseerde gegevens. Deze afhankelijkheid geldt niet alleen voor grote ondernemingen, zoals banken en verzekeringsmaatschappijen, maar evenzeer voor grossierderijen waarbij bestellingen van cliënten telefonisch worden ontvangen en direct in de computer worden ingetoetst.
Indien zich een calamiteit van enige omvang voordoet is de kans groot dat (delen van) het geautomatiseerde gegevensverwerkende systeem buiten bedrijf raken. Tot voor kort waren de consequenties van een calamiteit te overzien als kopieën van programmatuur en gegevens elders werden bewaard en afspraken met andere computergebruikers waren gemaakt om de verwerking te kunnen continueren: het "noodvoorzieningenplan in de dop". Bij de meer geavanceerde technologieën waarvan op dit moment gebruik wordt gemaakt, waarbij ingevoerde posten onvertraagd en onmiddellijk in verschillende gegevensverzamelingen worden opgeslagen en verschillende acties worden geïnitieerd (zoals het vervaardigen van produktie-orders en het uitleveren van goederen) moet het noodvoorzieningenplan hieraan worden aangepast.
Het vervaardigen van zo'n noodvoorzieningenplan is geen sinecure. Van elke verandering - op welk terrein ook - binnen "de automatisering" dient te worden nagegaan of het consequenties heeft voor het noodvoorzieningenplan. De gebruiker speelt hierbij een niet weg te denken rol.

Zo'n noodvoorzieningenplan kan weliswaar technisch door de Automatiseringsafdeling worden opgezet, maar de gebruikersorganisatie zal moeten aangeven in hoeverre zij voor de uitoefening van de primaire bedrijfsfunctie kwetsbaar is, indien de geautomatiseerde gegevensverwerking voor kortere of langere tijd niet beschikbaar is. Pas dan kan een evenwichtige keuze worden gemaakt uit maatregelen van preventieve en repressieve aard. Als een noodvoorzieningenplan eenmaal gedefinieerd en aangepast is en de voorzieningen daarvoor getroffen zijn wil dat niet zeggen dat de zaken voor elkaar zijn. De praktijk heeft geleerd

dat met enige regelmaat de voorzieningen daadwerkelijk moeten worden uitgetest opdat men niet wordt geconfronteerd met eventualiteiten indien de nood echt aan de man komt. In verschillende landen en ook in Nederland bestaan organisaties die bedrijven behulpzaam zijn bij het opzetten en voortdurend testen van de noodvoorzieningenplannen.
Omdat het bijna niet meer mogelijk is in geval van een calamiteit uit te wijken naar collega-bedrijven, zijn zogenaamde uitwijkcentra ontstaan die een scala van mogelijkheden bieden.
Uitgaande van de risico's die "in-house" niet zijn af te dekken (ook niet door verzekeringen) zal een beroep op die uitwijkcentra kunnen worden gedaan. Te veel komt het nog voor dat bedrijven uit het produktenscala van die centra een "aangepaste keuze" doen, die bij hun intuïtief bepaald budget past. Dit is een onderschatting van het probleem. Het is noodzakelijk dat het management erop toeziet dat alle "noodfaciliteiten" worden ingehuurd die volgens de risico-analyse nodig zouden kunnen zijn.

Meestal hebben noodfaciliteiten betrekking op gebouwen en apparatuur. Ingeval van die faciliteiten gebruik moet worden gemaakt dienen de "bedrijfseigen gegevens" beschikbaar te zijn. Dat zijn dan de programmatuur en de diverse gegevens. Zonder deze gegevens is uitwijken zinloos. In de praktijk komt het voor dat voor de uitwijk nog wel voorzieningen zijn getroffen, doch dat de maatregelen met betrekking tot de beschikbaarheid van de bedrijfseigen gegevens ten ene male onvoldoende zijn. Meestal blijkt er geen controle te zijn of de getroffen maatregelen wel worden nageleefd, zoals op het juiste moment de kopie maken en de kopie op het juiste moment naar de kluis elders brengen. In een dergelijke situatie blijkt pas in geval van calamiteiten dat de zaak niet in orde is. Ter illustratie het volgende voorbeeld:

Bij een bedrijf gold de volgende regeling: iedere vrijdagmiddag moesten kopieën worden aangemaakt van de bestanden en programmatuur. De magneetbanden waarop die kopieën werden opgeslagen, moesten aan het eind van de vrijdagmiddag naar de bank gebracht worden om daar in een kluis te worden opgeborgen. Bij controle bleek dat het personeelslid dat was belast met het ophalen en wegbrengen van de magneetbanden vrijdagsmorgens op weg naar zijn werk de banden haalde bij de bank en 's avonds de nieuwe kopieën wegbracht. Gedurende de gehele vrijdag waren dus geen kopieën van bestanden en programmatuur buiten de deur aanwezig. Het bedrijf kreeg gelukkig geen brand; een ander bedrijf waar de procedure identiek was, kreeg wel brand op vrijdag en kon vervolgens met de hand allerlei bestanden en programma's gaan reconstrueren. In beide gevallen ontbrak derhalve interne controle op de naleving van procedures en voorschriften.

Betrouwbaarheid van geautomatiseerde informatiesysteem

In het voorgaande is voornamelijk gesproken over het automatiserings- en beveiligingsbeleid en de mogelijke consequenties indien zo'n beleid ontbreekt.
Een ander belangrijk element is de betrouwbaarheid van geautomatiseerde informatiesystemen.
Het traject van een informatiesysteem loopt vanaf ontvangst c.q. vervaardigen van een basisdocument tot en met de verwerking en controle van de uitkomsten van de verwerking (output). Bij een vergaande integratie van processen zullen er weinig handmatige bewerkingen meer worden uitgevoerd. Het basisdocument verdwijnt steeds vaker, de gegevens worden direct ingevoerd waarna de computer de controle kan uitvoeren op die invoer, om vervolgens een en ander te verwerken. Met opzet is gesteld dat controles kunnen worden uitgevoerd door de computer. Deze moeten dan wel worden gedefinieerd en in programmatuur worden opgenomen.
Het definiëren van controle- en beveiligingsmaatregelen is derhalve een bezigheid die op maat gesneden moet worden voor ieder individueel systeem. Daarbij moet niet uit het oog worden verloren dat een samenstel van maatregelen moet worden gecreëerd, dat wil zeggen dat zodanige controles worden gedefinieerd dat de gebruiker zijn verantwoordelijkheid kan dragen. Van die controles kunnen een aantal in de programmatuur worden opgenomen. Ook hier is de term "een evenwichtig stelsel van maatregelen" op zijn plaats. Het mag niet zo zijn dat alles verschoven wordt naar de automatisering (dus ook de verantwoordelijkheid van de gebruiker). Onbeheersbare systemen komen in de praktijk maar al te vaak voor. Kunstgrepen in de gebruikersorganisatie moeten de feilen van de automatisering compenseren. Daarvoor is automatisering niet bedoeld.
Betrouwbare informatiesystemen kunnen slechts worden gebouwd indien in de gebruikersorganisatie en in de automatiseringsorganisatie voldoende deskundigheid op het gebied van administratieve organisatie en interne controle aanwezig is. Daarbij komt dat ook feeling met betrekking tot deze materie noodzakelijk is om tot goede systemen te kunnen komen.
Het zal ook hierbij duidelijk zijn dat gebruikers en automatisering slechts bereid en in staat zijn voldoende controlemaatregelen in systemen op te nemen indien ondersteuning vanuit het management met betrekking tot beheersbaarheid van systemen wordt gevoeld. En hier sluit dan de cirkel automatiseringsbeleid, beveiligingsbeleid en feitelijke ontwikkeling op elkaar aan.
Voorbeelden dat het ten gevolge van het ontbreken van toereikende controlemaatregelen mis zou kunnen gaan zijn er te over. Voorbeelden dat het echt mis is gegaan, zijn slechts mondjesmaat beschikbaar. Bij misgaan wordt meestal het eerst gedacht aan fraude. Enige tijd geleden kwam een fraude in de pers die weer eens aantoonde dat de computer kan worden misbruikt omdat de organisatie niet goed in elkaar zit of steken laat vallen.

Een operator/programmeur had kans gezien in het geautomatiseerde betalingensysteem gelden ongeautoriseerd weg te sluizen. Uit de gegevens van de media bleek dat hij kans had gezien ongeautoriseerd wijzigingen in de programmatuur aan te brengen en zodoende geld over te boeken naar zijn eigen bankrekening. De fout ligt in deze niet bij de computer maar bij de automatiseringsorganisatie én bij de gebruiker. Bij de eerste bleek geen controle op programmawijzigingen te zijn. Bij de gebruiker bleek controle op de betaling zelf te ontbreken.
Was het vroeger zo dat ieder bedrijf zeer kritisch toezag op het verrichten van betalingen, nu de betalingen geautomatiseerd plaatsvinden door inlevering van een magneetband of diskette bij de bank respectievelijk bankgirocentrale worden een reeks maatregelen plotseling niet meer nodig geacht. Van deze omstandigheid heeft de betrokkene in het voorbeeld dan ook gebruik gemaakt. Naar mijn mening dient in de situatie van geautomatiseerde betalingen juist kritisch te worden gekeken naar de organisatie waarin de tape of diskette wordt aangemaakt en de controlemaatregelen. (De belangstellende lezer die dieper op deze problematiek wil ingaan verwijs ik gaarne naar het artikel dat collega J. ten Wolde in het Maandblad voor Accountancy en Bedrijfshuishoudkunde van november 1980 (nr. 10) publiceerde.)
Een aspect waaraan nog al eens te weinig aandacht wordt geschonken is het effectueren van bevoegdheidsregelingen in de geautomatiseerde systemen.
Voorheen bleek uit parafen en controletekens op documenten wie wat had gedaan hetgeen dan werd ondersteund door schriftelijk vastgelegde procedures; de voortgaande integratie van de automatisering (de uitwisseling van factureringsgegevens tussen producent en afnemer geschiedt reeds op magneetband) noopt ertoe de bevoegdheden en beslissingsregels met betrekking tot bepaalde transacties of transactiesoorten, in het geautomatiseerde systeem zelf vast te leggen.
Van de organisatie vereist dit discipline met betrekking tot het gebruik van zogenaamde identificatiecodes en wachtwoorden. Wordt met wachtwoorden nonchalant omgesprongen dan loopt men risico's vergelijkbaar met het beschikbaar stellen van blanco getekende betalingsopdrachten.
De introductie van zogenaamde point of sales-systemen controleert gebruikers en automatisering met een nieuwe dimensie van problemen. Zoals wellicht bekend is het de bedoeling dat op korte termijn in Zuid-Nederland bij benzinestations en op langere termijn in het gehele land kan worden afgerekend door het invoeren van de eurocheque-kaart of bankpas voorzien van magnetische strip. Invoeren van de kaart in een lezer en vervolgens intoetsen van een personal identification number (pin) en de accordering van het bedrag betekent dat het bedrag van de eigen bankrekening wordt afgeschreven en bijgeschreven op die van de leverancier. Uiteraard zal te zijner tijd in allerlei winkels en warenhuizen op deze wijze kunnen worden afgerekend.

Bekend is dat leveranciers van computers zeer uitgebreid onderzoek verrichten naar de beveiligingsmogelijkheden van deze nieuwe vorm van betalingsverkeer, terwijl een aantal accountants betrokken is bij het beoordelen van de controle- en beveiligingsmaatregelen.
De achteloze bezitter van zo'n kaart die het pin op de kaart schrijft kan bij verlies rekenen op het spoedig leeghalen van zijn gehele bankrekening.

Resumerend: het opnemen van controle- en beveiligingsmaatregelen in geautomatiseerde informatiesystemen is zeer wel mogelijk. Van de gebruiker en van automatisering wordt verwacht dat zij met inventiviteit controlemaatregelen in de informatiesystemen opnemen, dat de gebruiker respectievelijk gebruikersorganisatie controlebewust is en daarnaar handelt.
Een ieder dient zich te realiseren dat er nog geen eind is gekomen aan de gebruiksmogelijkheden die de automatisering biedt. Het is uit voorgaande hopelijk duidelijk geworden dat de betrouwbaarheid van de computer van de betrouwbaarheid van de organisatie afhankelijk is. Daarbij speelt de mens een overheersende rol. Van uw accountant mag u verwachten dat hij een belangrijke bijdrage levert in het denken over beheersbaarheid van geautomatiseerde gegevensverwerking nu en in de toekomst.

Fysieke beveiliging

De geautomatiseerde gegevensverwerking dient uiteraard omgeven te worden met een reeks maatregelen ter fysieke beveiliging. Ook hier zal het management uiteindelijk moeten beslissen in hoeverre maatregelen worden getroffen. Een risico-analyse zal, het is reeds eerder gesteld, moeten uitwijzen waar het evenwicht ligt tussen preventieve en repressieve maatregelen. Het zal de lezers bekend zijn dat veel computercentra voorzien zijn van allerlei toegangscontrolebarrières variërend van slotgrachten en ophaalbruggen tot een portier bij de deur van het computercentrum of door het herbergen van een computercentrum in zo'n oud gebouw dat men niet verwacht daarin een belangrijk computercentrum aan te treffen (zo'n voorbeeld vond ik eens in San Francisco).

Beveiliging van microcomputers

Wat de beveiliging van microcomputers en het gebruik ervan betreft zullen op deze plaats slechts enkele aspecten de revue passeren.
Een probleem dat niet eenvoudig kan worden opgelost is het onrechtmatig kopiëren van programma's en gegevensverzamelingen bijvoorbeeld op diskette voor gebruik op een microcomputer en het meenemen ervan buiten het bedrijf ten behoeve van verkoop of illegaal gebruik. Tegen deze vorm van diefstal lijkt op dit moment weinig te doen.

De vraag is of het zelfs kan worden voorkomen nu er een tendens waarneembaar is naar steeds meer thuiswerken omdat de personal computer via de telefoon kan worden verbonden met andere personal computers in het bedrijf of het mainframe en het dus niet nodig is iedere dag naar de onderneming te gaan.
Verzekeren van apparatuur tegen diefstal is in ieder geval één oplossing.

Het is van belang te onderstrepen dat degenen die bij een organisatie behoren als een goed huisvader/moeder met de apparatuur dienen om te gaan omdat het waardevolle machines betreft en als regel nog veel waardevoller informatie.

Een fenomeen dat inmiddels al niet meer is weg te denken uit het zakenleven is de zogenaamde elektronische brievenbus (electronic mailbox systems). Berichten van allerlei aard en formaat worden door de bezitters van microcomputers/personal computers, die voorzien zijn van een modem, in een elektronische brievenbus gezet en - indien bestemd voor henzelf - eruit gehaald. Een ongecontroleerde flow van berichten is hiermede ontstaan.
Slechts ondersteund met discipline ten aanzien van de wachtwoorden kan waarborgen dat onbevoegden verkeerde berichten in handen krijgen of dat ondergeschikten te vroeg kennis krijgen van mededelingen, boodschappen en dergelijke die in eerste aanleg voor het management zijn bedoeld.

Tot slot

In het artikel is gepoogd in een notedop de problematiek ten aanzien van de beheersbaarheid en continuïteit van de automatisering de revue te laten passeren. Vanzelfsprekend kan dit in een artikel van deze omvang niet uitputtend zijn; door het toevoegen van enige praktijksituaties is gepoogd het betoog te accentueren en aan te geven dat het niet louter theoretisch moet worden opgevat.

Laat het overigens wel duidelijk zijn, dat automatiseren geen éénmanszaak is! Wil het totale systeem beheersbaar worden gemaakt en gehouden, dan vereist dat een grote betrokkenheid van het management door bijvoorbeeld actief deel te nemen in een stuurgroep automatisering (voorbereiden en vaststellen van het beleid ten aanzien van automatisering en beveiliging, controle op voortgang van automatiseringsprojecten en dergelijke).

Niet minder belangrijk is de inzet van de afzonderlijke gebruikers, die zijn te onderscheiden (administratie, inkoop, verkoop en dergelijke). Zij dienen immers hun kennis van het (dagelijkse) gebeuren over te dragen op basis waarvan informatie-analisten de functionele specificaties van de informatiesystemen kunnen vervaardigen.
Specialisten (automatiseerders) zullen deze specificaties ná een aantal tussenstappen uiteindelijk omzetten in programma's.
In de fase van het vervaardigen van de functionele specificaties wordt nogal eens weinig aandacht geschonken aan interne controle en beveiliging.
Het management van de gebruikersorganisaties is daarvoor te blameren.

Interne en/of externe accountants schieten daarop in door reeds in een vroegtijdig stadium de documentatie, die na afloop van de onderscheiden fasen van ontwikkeling beschikbaar komt, aan een kritische beoordeling te onderwerpen.

Van het management mag worden verwacht dat de aanbevelingen van accountants serieus worden genomen.
Om te voorkomen dat accountants voortdurend als "zendelingen" ten aanzien van de beheersbaarheid van de automatisering moeten opereren, dient het management zich over een aantal zaken te informeren.
Genoemd kunnen worden:
- de besturing en beheersing van de automatiseringsinspanning (betrokkenheid in stuurgroep en projectgroepen);
- de toenemende afhankelijkheid van de onderneming van de geautomatiseerde gegevensverwerking (continuïteitsbedreigende factoren);
- de invloed van de automatisering op de (administratieve) organisatie en interne controle van de onderneming.

Automatisering kan niet slagen indien het management zich aan haar verantwoordelijkheid (in casu directe betrokkenheid) onttrekt. Automatisering is per slot van rekening geen geïsoleerd gebeuren meer; een multidisciplinaire aanpak is noodzakelijk, omdat van de kennis van een reeks deskundigen gebruik moet worden gemaakt.

De ontwikkelingen op het terrein van de automatisering staan niet stil. Accountants spelen in op de problematiek van beheersbaarheid en continuïteit van die automatisering door specialistisch personeel (EDP-auditors) in hun organisaties op te nemen. Accountants met deze bijzondere signatuur zijn niet slechts betrokken bij de beoordeling op de aspecten betrouwbaarheid en continuïteit van automatiseringsorganisaties en geautomatiseerde systemen vanuit hun accountantswerk, maar zijn op die wijze tevens geequipeerd om het management op voornoemde terreinen adequaat te kunnen adviseren. Zij zijn per slot van rekening deskundig op het gebied van administratieve organisatie en (interne) controle.

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

BEVEILIGING IN LOKALE NETWERKEN

door ing. H.A.J.M. Spape

Door specifieke eigenschappen van lokale netwerken onderscheiden deze zich voor wat betreft beveiligingsfacetten gedeeltelijk van "grote" netwerken. Dit artikel beoogt een aanvulling te zijn op reeds veelvuldig verschenen literatuur inzake beveiliging van netwerken in het algemeen. De specifieke beveiligingsproblematiek van lokale netwerken alsmede de daaruit voortvloeiende mogelijkheden en beperkingen ten aanzien van de beveiliging zullen worden belicht. Het artikel vooronderstelt voorkennis van datacommunicatie in het algemeen en enige begrippen inzake lokale netwerken in het bijzonder.

1. Begripsvorming

Er is tot op heden nog geen formeel geaccepteerde definitie van een lokaal netwerk (Local Area Network, LAN). Het in dit artikel gehanteerde begrip LAN voldoet aan de beschrijving:

> Een lokaal netwerk is een communicatienetwerk dat voorziet in de verbinding van een variëteit aan datacommunicatie-apparatuur binnen een beperkt geografisch gebied.

Hierin omvat de term "een variëteit aan datacommunicatie-apparatuur", in principe alle apparatuur die gegevens verstuurt over c.q. ontvangt van een transmissie-medium, zoals:

- computers;
- terminals;
- randapparatuur (printers, disk-units);
- sensors;
- telefoons;
- televisiezenders en -ontvangers;
- facsimile.

Bij een "beperkt geografisch gebied" moet gedacht worden aan een gebouw of een groep van gebouwen, zoals een fabrieks- of kantorencomplex.

Doordat niet alle OSI-lagen gestandaardiseerd zijn, kunnen we in het geval van LAN's niet van "echte" open systemen spreken. Een van de belangrijkste eisen aan een LAN te stellen blijft echter "high connectivity" met een inherent risico ten aanzien van de beveiliging.

De variëteit aan datacommunicatie-apparatuur welke via het LAN communiceert, impliceert dat een LAN een open systeem moet zijn in de zin van de ISO-OSI-terminologie. Dit houdt in dat wanneer overeenkomstige protocollen gehanteerd worden, apparatuur van een willekeurige producent zinvol op het netwerk moet kunnen aansluiten. Hiermee wordt het gebied van protocolstandaardisatie betreden. Begin 1985 zal ISO draft proposals uitbrengen van de van IEEE-802 overgenomen Local Area Network standaardprotocollen. Deze omvatten echter slechts de onderste twee lagen (datalink en physical) van het OSI-model.
In dit artikel wordt er verder van uitgegaan dat de organisatie welke het LAN gebruikt, er tevens volledig beheer over heeft, met andere woorden dat het niet afhankelijk is van door andere organisaties getroffen maatregelen met betrekking tot beheer en beveiliging van het LAN.

Onder een beveiligd LAN zullen we verstaan, een LAN dat de gebruiker kan garanderen dat:
- "zijn" gegevens niet door onbevoegden kunnen worden ingezien als ze via het LAN worden verstuurd (autorisatie);
- "zijn" gegevens niet door onbevoegden kunnen worden gemuteerd als ze via het LAN worden verstuurd (integriteit);
- de gegevens niet onopgemerkt verloren gaan of verminkt worden als gevolg van netwerkfouten (integriteit);
- berichten die hij ontvangt of verstuurt afkomstig zijn van respectievelijk arriveren bij degene(n) met wie hij communiceert en niet van respectievelijk bij anderen (authenticiteit).

2. Beveiliging in relatie tot het transmissiemedium

De bekabeling van een LAN (het fysieke netwerk) zal veelal zodanig zijn aangelegd dat aansluiten op het netwerk of het creëren van nieuwe aansluitpunten eenvoudig is. Het is daarom wellicht zinvol de bij LAN's gebruikte transmissiemedia te beschouwen in relatie tot ongeautoriseerd aftappen/modificeren van berichten op het LAN.

Media welke bij LAN's gehanteerd worden zijn:*
- twisted pair wire;
- fiber optic cable;
- coaxial cable;
  - . baseband;
  - . broadband.

* Ook andere media (zoals straalverbindingen) worden gebruikt. Hier wordt in dit artikel niet op ingegaan.

Twisted pair heeft als belangrijkste beveiligingsnadelen dat het elektromagnetische straling emitteert en dat het gevoelig is voor externe elektromagnetische beïnvloeding. Het is bovendien eenvoudig er fysiek op in te breken. Twisted pair wordt veelal toegepast omdat het goedkoop is. Het is dan in principe niet zinvol relatief dure fysieke maatregelen te treffen om de mogelijkheden tot aftappen/modificeren te reduceren.

Fiber optic cable heeft de nadelen van twisted pair niet. In tegenstelling tot koperdraad, dat direct of via een inductieve koppeling afgetapt kan worden, moet fiber optic onderbroken worden en moet een verbindingsstuk worden geplaatst om de lijn te kunnen aftappen. Dit vereist momenteel nog speciale kennis. De risico's ten aanzien van aftappen en modificeren zijn dus nog steeds aanwezig, doch zijn kleiner dan die bij andere media. Dit is evenwel slechts zo zolang de technologie niet voorziet in eenvoudige koppelingen in fiber optic.

Coaxiaal cable is momenteel het meest populaire LAN-medium. Doordat het is afgeschermd, is het minder gevoelig voor externe beïnvloeding dan twisted pair. Er is echter eenvoudig fysiek toegang toe te verkrijgen. De mate waarin afluisteren/modificeren mogelijk is, wordt onder meer bepaald door het gebruik van baseband- of broadband-technieken.

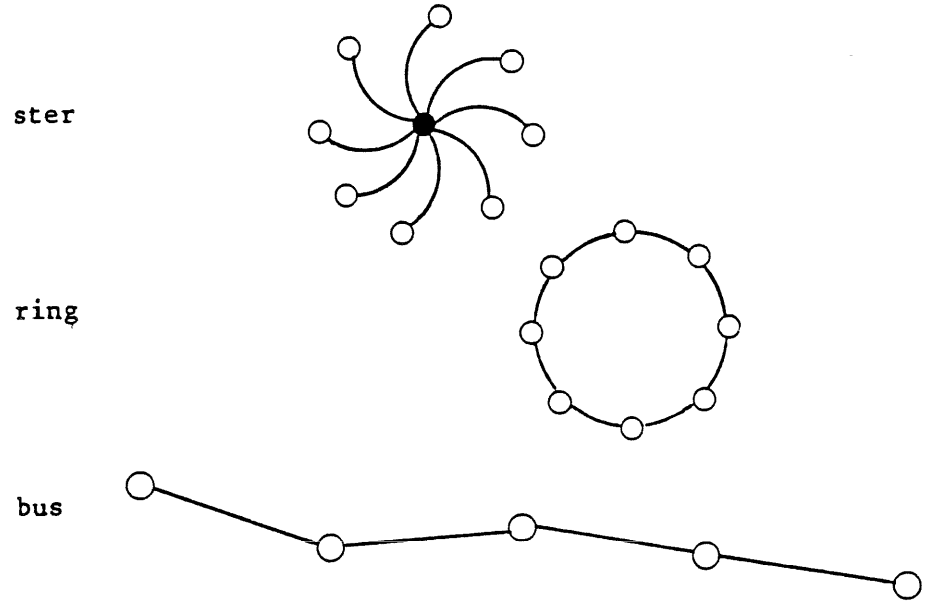
Bij gebruik van baseband is het signaal op de kabel de digitale weergave van de gebruikersgegevens en protocolinformatie van één bericht. Bij broadband zijn verscheidene berichten gemoduleerd over diverse frequentiegebieden (analoge signalen). Ten behoeve van aftappen en/of modificeren van berichten welke volgens de broadband-methode verzonden worden, is dus meer kennis van het netwerk of meer onderzoek nodig dan bij baseband, doch dit voorkomt het aftappen/modificeren niet.

Conclusie: De keuze van een transmissiemedium bepaalt mede het risico dat de gebruikers ten aanzien van afluisteren c.q. modificeren lopen. Om aftappen/modificeren tegen te gaan (eigenlijk: zinloos maken) zijn speciale voorzieningen nodig zoals bijvoorbeeld encryptie. Deze moeten door de gebruikersorganisatie zelf worden getroffen in de protocollen voor de hogere lagen.

De mogelijkheden tot afluisteren/modificeren zijn vanzelfsprekend ook gedeeltelijk bepaald door de wijze waarop het netwerk is aangelegd, c.q. welke topologie is toegepast. Enige attentiepunten dienaangaande worden gegeven in het volgende hoofdstuk.

3. Beveiliging in relatie tot de topologie van het LAN

Het begrip topologie definieert de omvang en vorm van een netwerk en wel in het bijzonder op de wijze waarop de aansluitpunten met elkaar zijn verbonden. In het kader van LAN's worden ruwweg drie topologieën aangetroffen.

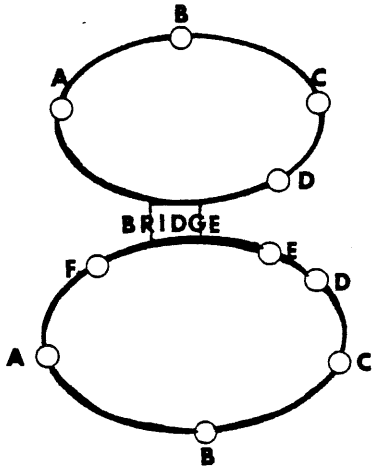


Typisch voorbeeld van een ster-topologie is de PBX (Private Branche Exchange). In het kader van beveiliging biedt de ster het voordeel dat er een centraal punt is, van waaruit de gehele communicatie beheerst kan worden. Bovendien geschiedt communicatie tussen twee punten niet via andere punten (uitgezonderd het centrale punt), zoals dat bij ring en bus het geval is.

Mogelijk is dat het centrale punt tabellen bevat welke aangeven wie naar wie wat mag zenden en wie wat van wie mag ontvangen. Iets dergelijks is zelfs fysiek te bewerkstelligen door het onmogelijk te maken bepaalde lijnen met andere lijnen door te verbinden. De kans dat deze of een soortgelijke benadering in de commercieel beschikbare LAN's (en PBX) wordt toegepast wordt echter klein geacht, voornamelijk omdat het afbreuk doet aan één van de grondgedachten achter LAN's, namelijk een zodanige flexibiliteit dat in principe iedereen met iedereen moet kunnen communiceren.

Bovendien zouden we ons altijd tot topologieën met een of enkele centrale punten moeten beperken, hetgeen om andere dan strikte beveiligingsredenen (zoals "failure tolerance") meestal niet wenselijk is.

Het "wie mag communiceren met wie" kan in het netwerk zelve worden vastgelegd, waardoor een mate van waarborg ten aanzien van handhaving van functiescheidingen door het netwerk wordt gegeven. Dit kan worden bereikt door middel van "bridges". Een bridge is een functie die voorziet in de koppeling van identieke (dat wil zeggen dezelfde protocollen gebruikende) netwerken. Als we ons bij wijze van voorbeeld beperken tot twee LAN's, welke door middel van een bridge met elkaar verbonden zijn, dan zal de bridge onder meer tot taak hebben een adresconversie uit te voeren. Immers, elke LAN zal zijn eigen adressen (voor zender en ontvanger) gebruiken. Als gebruiker A in LAN-1 een bericht wil sturen naar gebruiker B in LAN-2, terwijl er ook een gebruiker B in LAN-1 bestaat, dan zal hij gebruiker B van LAN-2 niet aanduiden door middel van adres B, maar door een ander adres, bijvoorbeeld S. De bridge zal op het betreffende bericht reageren alsof het voor hem bestemd is en het doorsturen naar gebruiker B in LAN-2, welke niet bekend hoeft te zijn met het feit dat het bericht uit een ander LAN afkomstig is. (Evenals A niet hoeft te weten dat S niet in zijn netwerk opgenomen is.)



Tabel in bridge

LAN-1 address	LAN-2 address
R	C
S	B
T	D

Op deze wijze hebben gebruikers van LAN-1 geen toegang tot de gegevens van LAN-2, als deze niet expliciet door een gebruiker van LAN-2 naar gebruikers van LAN-1 gestuurd worden. Risico's worden dus op deze wijze verkleind. Het kan derhalve zinvol zijn deze constructie toe te passen, dan wel met de beveiligingsaspecten/mogelijkheden rekening te houden als om andere redenen bridges worden gebruikt.

(N.B. In plaats van de bridge-functie kan ook een gateway-functie worden toegepast. Dit is in deze context een bridge waarin ook protocolconversie geschiedt.)

4. Beveiliging in relatie tot IEEE-Logical Link Control (LLC)

De OSI-datalink-laag is in de IEEE-standaardisatie (zie 2, 3 van de literatuurlijst pag. 25) opgesplitst in twee sublagen, LLC en een sublaag welke de diverse medium toegangsprotocollen omvat (CSMA/CD, token ring, token bus).
Logical Link Control (LLC) is het OSI-Data Link Control-protocol gedefinieerd voor gebruik in IEEE-LAN's.
Het protocol ondersteunt logische verbindingen tussen twee of meer stations welke een gezamenlijk fysiek kanaal delen. Een belangrijke functie van LLC is het verzekeren van de integriteit (in deze paragraaf gebruikt in de zin van de 2de in paragraaf 1 gegeven betekenis) van de gebruikersgegevens als deze verzonden worden over de datalink. Dit wordt bereikt door middel van een combinatie van foutdetectie en hersteltechnieken.

Het IEEE-LLC-protocol lijkt veel op, maar is niet gelijk aan, HLDC (High Level Datalink Control).

Er zijn drie LLC-serviceniveaus te gebruiken bij transmissie:
- unacknowledged connectionless service;
- connection oriented service;
- acknowledged connectionless service.

Unacknowledged connectionless service (type 1 service) betekent dat verzonden berichten niet op LLC-niveau bevestigd worden voor ontvangst. Indien dit vereist is moet dit door de hogere lagen verzorgd worden. Deze maken zoals reeds opgemerkt geen deel uit van de IEEE-802-standaard. Als deze connectionless service wordt gebruikt dan kan dit verloren gaan van gegevens tot gevolg hebben zonder dat dit op dit niveau gedetecteerd wordt. Er is ook geen foutherstel op LLC-niveau. De integriteit van berichten moet derhalve op hogere niveaus gewaarborgd zijn.

Connection oriented service (type 2 service) houdt in dat een verbinding tussen twee stations wordt opgezet, dat gegevens betrouwbaar (error recovery, sequence control, flow control) verzonden/ontvangen worden en dat de verbinding in onderlinge overeenstemming weer verbroken wordt. Integriteit is dus voor een belangrijk deel gewaarborgd. Dit betekent dat op de hogere niveaus minder maatregelen dienaangaande genomen behoeven te worden.

Acknowledged connectionless service (type 3 service) (nog geen definitieve standaard) voegt aan de unacknowledged service een graad van bescherming toe door middel van een bevestiging voor elk deelbericht dat verstuurd is.

Alle stations die aan de standaard voldoen moeten in type 1 service voorzien als een minimum vereiste om toegang tot het medium te kunnen verkrijgen. Een station dat alleen type 1 service biedt is een class 1 station.
Een station dat in type 2 service voorziet moet ook type 1 als onafhankelijke functie bieden. Dergelijke stations zijn class 2 stations.

Momenteel voldoen de meeste stations slechts aan de class 1 specificaties.
Dit impliceert dat de maatregelen die vereist zijn om de gebruiker integriteit van zijn gegevens te kunnen waarborgen, genomen moeten worden in het protocol van de transportlaag, waarvoor helaas nog geen standaard is geaccepteerd. Het komt uiteindelijk dan op de organisatie of diens leveranciers zelf neer om alle relevante stations te voorzien van programmatuur en/of apparatuur welke voorziet in integriteitsbehoeften.

5. Conclusies

De IEEE-802-lokale netwerken voorzien nauwelijks in beveiligingsmaatregelen. Als een leverancier stelt dat zijn netwerk hierin wel voorziet, dan is het geen lokaal netwerk meer in de zuivere betekenis, omdat op de hogere lagen, waar de leverancier zijn beveiligingsmaatregelen zal hebben ondergebracht, geen standaardisatie bestaat en het LAN dus alleen met een variëteit aan communicatie-apparatuur zal kunnen werken als deze met extra programmatuur en/of apparatuur is uitgerust. Wanneer een gebruikersorganisatie een lokaal netwerk als communicatiemedium gaat toepassen, moet zij zich de daaraan verbonden veiligheidsrisico's realiseren en beseffen dat zij voorzieningen moet treffen indien deze risico's niet aanvaardbaar zijn. Deze voorzieningen zullen betrekking moeten hebben op de integriteit en authenticiteit van berichten en zijn te waarborgen door gebruik van een geschikt transportlaagprotocol. Dit zal moeten voorkomen dat data verloren gaat, foutief geraakt of ongeautoriseerd wordt ingezien, al dan niet door inmenging van een niet geautoriseerde gebruiker. Voydock en Kent (1) komen tot de conclusie dat deze maatregelen (die zich concentreren rond encryptie) genomen moeten worden in het transportlaagprotocol.

Gebruik van bridges bij de opbouw van het LAN kan voorkomen dat essentieel geachte functiescheidingen door het gebruik van het LAN doorbroken worden.

Literatuur

1. Voydock V.L. and Kent S.T.; Security Mechanisms in High Level Network Protocols; Computing Surveys, Vol. 15 no. 2, June 1983.

2. Draft IEEE-standard-802.1 part A, revision B, June 1983 (Unapproved Draft Published for Comment Only).

3. Graube M; Local Area Nets: A pair of standards. IEEE-Spectrum, June 1982.

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

BASIC GROEIT

door J.E. de Bue

Inleiding

Dit artikel, informatief van aard, beoogt een beeld te geven van de geschiedenis van BASIC vanaf het ontstaan aan het Dartmouth College in 1963 tot nu. Daarnaast zal de mogelijkheid van het gebruik van rechtstreeks toegankelijke bestanden (random access files) als een voorbeeld van de mogelijkheden van Microsoft, BASIC, besproken worden. Het doel van dit artikel is de lezers erop attent te maken dat Basic niet voor niets zoveel gebruikers kent (vanwege de eenvoud en het ongestructureerd programmeren met deze taal). Gebruikers echter, die in vele gevallen de mogelijkheden van BASIC onderschatten.

De geboorte ...

Het ontstaan van BASIC was een antwoord op de problemen die er heersten aan het Dartmouth College, waar de heren Thomas E. Kurtz en John G. Kemeny onderwezen. De problemen die deze heren ondervonden waren enerzijds dat slechts 25% van de aanwezige studenten geen moeilijkheden had met het vak "computer science" en anderzijds dat de op dat moment in roulatie zijnde programmeertalen (Fortran, Algol, Assembler) naar hun mening niet geschikt waren om die studenten, welke geen wetenschappelijke studierichting gekozen hadden, te leren programmeren. Om deze studenten toch de mogelijkheid te bieden het programmeren uit te voeren, zochten Kurtz en Kemeny naar een oplossing. De oplossing moest zodanig zijn dat de zogenaamde "niet-wetenschapsstudenten" zich niet hoefden te bekommeren over details wat betreft declaratie van variabelen of het gebruik van integers of gebroken getallen.

Beïnvloed door Fortran en Algol, ontstond in 1964 de eerste versie van de Beginners All-purpose Symbolic Instruction Code, BASIC. Deze versie bevatte een veertiental instructies en werkte, evenals andere BASIC-versies, op een time-sharing 1 systeem met behulp van een interpreter 2. Variabelen bestonden uit een letter of een letter gevolgd door een cijfer.
De tweede versie, welke vijf maanden later gereed was, verschilde niet veel van de eerste versie. De punt-komma werd toegevoegd als een scheidingsteken in het PRINT-commando en de nul-index voor een of twee dimensionale array's werd ingevoerd.

De derde versie, gereed in 1966, werd een uitgebreide tweede versie; de uitbreiding betrof onder andere de toevoeging van het RESTORE-commando, welke de pointer van het DATA-commando terug kan zetten naar het eerste DATA-element, en het INPUT-commando, welke gegevens kan accepteren tijdens de uitvoering van een programma. Dit laatste hield in dat BASIC een interactieve taal werd.
De vierde versie, 1967, een nieuwe experimentele versie van BASIC, voerde onder andere RANDOMIZE en ON-GOTO in. Daarbij werden alle variaties van ON-GOTO en IF-THEN geaccepteerd. De TAB-functie ontstond, en voor het eerst initialiseerde BASIC alle gebruikte numerieke variabelen met nul.
De vijfde versie, 1970, had ten opzichte van de vierde een belangrijke verandering ondergaan.
Deze versie werd ontworpen om met random access files te werken. Dit vereiste een aantal extra commando's om het werken met files aan te kunnen; READ en WRITE voor het lezen van en schrijven naar een bestand. Daarnaast werden de volgende functies toegevoegd:
- LOC de locatie pointer voor het in behandeling zijnde bestand en
- LOF welke de lengte van het betreffende bestand voorstelde.

Een zogenaamde end-of-file conditie kon als volgt worden gedetecteerd:

```
IF LOC (#1) >= LOF (#1) THEN  <eof proces>
```

Daarnaast introduceerde deze versie het CHAIN-commando, waarmee een programma een ander programma kan opstarten, en een aantal string-behandelingsfuncties (zie figuur 1, blz. 31).
De zesde versie, 1971, verving het FILES-commando door een commando, dat de opgegeven bestandsnaam kon vergelijken met de actuele bestandsnaam en al dan niet een foutmelding kon produceren.
Het doel dat door Kurtz en Kemeny was bepaald als een gemakkelijk te leren en te gebruiken taal voor de zogenaamde niet-programmeurs leek hiermee te zijn bereikt.

BASIC nu

In 1974 werd de eerste microcomputer BASIC interpreter geschreven door Paul Allen en Bill Gates. Deze interpreter, geschreven voor de Altair 8800 microcomputer welke door de firma MITS geleverd werd, werd gelicenceerd onder Microsoft in 1975.
De interpreter bleek een dusdanige populariteit te hebben, dat firma's als Commodore Ltd. en Tandy Radio Shack gebruik gingen maken van deze programmatuur. Zowel Commodore als TRS zouden echter gauw nieuwe versies van de interpreter - naar eigen idee - uitbrengen. Vanaf dat moment ontstaan de zogenaamde BASIC-dialecten.

True BASIC

Tien jaar na het ontwerp van BASIC komen Kurtz en Kemeny terug met een BASIC-versie gebaseerd op de voorgestelde ANSI BASIC standaard. True BASIC heeft alle mogelijkheden van de oudere BASIC, zoals die door henzelf werd ontworpen, maar heeft daarnaast een aantal mogelijkheden waarmee een gebruiker grote, gecompliceerde programma's kan schrijven; machine onafhankelijke grafische mogelijkheden, aanroepen van apart gecompileerde procedures, ondersteuning van moderne programmeringstechnieken, gebruik van verschillende typen bestanden, en dergelijke. Belangrijk is echter dat deze BASIC grote hoeveelheden direct adresseerbaar geheugen aankan; ondanks het feit dat de meeste interpreters geschreven zijn voor 32K of 64K computers, is True Basic geschreven voor computers met minstens 128K direct adresseerbaar geheugen.

BASIC 09

BASIC 09, ontwikkeld door Microware Corp., is geschreven voor computers met een 6809 Motorola processor en wordt gebruikt met het disk operating system OS-9, dat vergelijkbaar is met UNIX. BASIC 09 heeft, wat betreft de syntax, meer overeenkomsten met programmeertalen als PASCAL of C wat betreft programmastructuur, maar behoudt zijn overeenkomsten met andere versies van BASIC wat betreft de instructieset. Georganiseerd als een compiler/interpreter heeft deze versie van BASIC de voordelen van compileren, snelle programma's en interpreteren, foutmeldingen en dergelijke. Daarnaast beschikt BASIC 09 over de mogelijkheid met name genoemde procedures aan te roepen, moderne controlstructures als WHILE-DO, REPEAT-UNTIL en FOR-NEXT uit te voeren en diverse typen bestanden te kunnen verwerken.

Better BASIC

Deze BASIC-versie, ontwikkeld door Summit Software Technology Inc., is bedoeld voor de IBM-PC, de PC-junior en hiermee compatibel zijnde microcomputers.
Better BASIC heeft een modulaire structuur, dat houdt in dat er binnen Better BASIC-programma's modules aanwezig zijn voor de uitvoering van speciale taken als werken met "windows", het gebruik van de grafische mogelijkheden en dergelijke.
Modules kunnen echter ook door de gebruiker geprogrammeerd worden.
Syntactisch is Better BASIC compatibel met Microsoft GW BASIC en IBM-PC BASIC, waarbij ongeveer 80% van de commando's gebaseerd zijn op de voorgestelde ANSI BASIC standaard.

Grote verschillen met ANSI BASIC zijn echter:
- de mogelijkheid van locale (alleen in een bepaald deel van het programma te gebruiken) en globale (door het hele programma te gebruiken) variabelen is aanwezig;
- men kan procedures definiëren (een soort van subroutine welke bijvoorbeeld los van de applicatie gecodeerd is);
- de taal is modulair uitbreidbaar.

Ook Better Basic werkt in de vorm van een compiler/interpreter met de reeds eerder genoemde voordelen van dit systeem: incremental compilation. Daarnaast kan worden vermeld dat Better BASIC twee vormen van variabelen declaratie kent, te weten explicite declaratie, waarbij alle te gebruiken variabelen in het programma gedeclareerd worden, en automatische declaratie, waarbij Better BASIC de te gebruiken variabelen initialiseert op nul.

Het gebruik van random access files in MSBASIC versie 1.1

Random access files zijn bestanden waaruit men gegevens kan halen zonder het bestand sequentieel te benaderen. Dit betekent dat als men het 200ste record uit een bestand wil verwerken, niet eerst de daarvoor liggende 199 records verwerkt behoeven te worden, maar men direct toegang heeft tot dit record. Om deze wijze van bestandsverwerking te verwezenlijken zijn in MSBASIC een aantal commando's aanwezig waarmee men random access files kan creëren en benaderen.

Creatie van een random access file

Om een random access file op te bouwen, waarbij de recordlengte maximaal 32767 byte mag zijn, zijn een aantal stappen nodig. Ten eerste moet men het bestand openen. Dit gebeurt met het OPEN-commando waarbij men een bestandsnaam toekent, een buffer toekent en de recordlengte definieert. Als tweede definieert men de opbouw van het record binnen de gedefinieerde buffer waarbij tevens per veld binnen een record de veldlengte wordt gespecificeerd. Om gegevens in het bestand te plaatsen wordt een record veld voor veld opgebouwd, waarbij met behulp van het LSET- of RSET-commando de betreffende gegevens in de buffer worden geplaatst, waarna het PUT-commando zorgt voor de overdracht van de gegevens in de buffer naar de diskette waarop het bestand wordt opgebouwd en geeft bij deze overdracht het record een nummer tussen 1 en 32767.

Toegang tot een random access file

Om gegevens van een random access file te gebruiken voor verwerking in een programma zal men als eerste het bestand moeten openen, waarbij wederom de bestandsnaam, de buffer en de recordlengte worden gedefinieerd. Het openen van een te lezen bestand gebeurt met OPEN. Daarna wordt met FIELD de velddefinitie binnen het record bepaald, waarna met behulp van het GET-commando een record, met het in GET gespecificeerde recordnummer van de diskette naar de buffer wordt overgebracht. Men moet echter voor ogen houden dat numerieke gegevens geconverteerd moeten worden voordat een rekenkundige verwerking mogelijk is, dit omdat BASIC de ingelezen numerieke gegevens binnenhaalt als een alfanumeriek gegeven; een string waarmee BASIC niet kan rekenen.
Dit gebeurt met de convertcommando's; CVI voor integere waarden, CVS voor single-precision en CVD voor double precision-waarden.

Na gebruik van het open commando moet er logischerwijs een close-commando volgen. Dit geldt zowel voor creatie als het lezen van het gebruikte bestand. End-of-file-situaties kunnen met behulp van de LOC- en de LOF-functies gedetecteerd worden, waarbij LOC het recordnummer van het laatst door GET of PUT behandelde record bevat.

Epiloog

Uit de ontstaansgeschiedenis van BASIC blijkt dat de bedoeling van Kurtz en Kemeny om een makkelijk te leren taal te ontwerpen volgens hen in de vijfde versie verwezenlijkt was. Wat zij echter niet hadden kunnen voorzien was het feit dat BASIC, via Microsoft, zeer grote populariteit verkreeg bij een publiek welke men kan typeren als niet-programmeurs. Deze ontwikkeling hield in dat concurrentie op de microcomputermarkt ervoor zou zorgen dat er verschillende versies van BASIC zouden ontstaan. Dit samen met de technologische ontwikkelingen in de micro-elektronica geeft een van de oorzaken aan van zeer geavanceerde uitvoeringen van BASIC, waarbij nauwelijks meer gesproken kan worden over een beginnerstaal.
Het grootste nadeel van deze forse groei van BASIC is het feit dat compatibiliteit nauwelijks aanwezig is. Dit probleem hoopt men op te lossen door invoering van een standaard-BASIC welke de basisfuncties zal omvatten waaraan elke BASIC-uitvoering geacht wordt te voldoen.

Noot:
1. Het time-sharing-systeem werd ontworpen en geïntroduceerd aan het Dartmouth College.
2. Ondanks het feit dat in eerste instantie een compiler gebruikt zou worden, is er gekozen voor een interpreter.

Literatuur

- History of programming languages, edited by Richard L. Wexelblat, Academic Press, 1981.
- Better Basic, G. Michael Vose, Byte april 1984.
- True Basic, Brig Elliot, Byte april 1984.
- Basic 09, Brian Capouch, Byte april 1984.
- Basic 09 programming manual, author onbekend.
- Programming the 6809, Rodnay Zaks en William Labiac, Sybex, 1982.
- Basic by Microsoft, IBM, 1981.

Ontwikkeling van BASIC: versie 1 tot en met 5

1st	2nd	3rd	4th	5th
LET →				
PRINT →				
END →				
FOR-NEXT →				
GOTO →				
IF-THEN →				
DEF →				
READ →				
DATA →				
DIM →				
GOSUB →				
RETURN →				
REM →				
	; →			
	0 index →			
		INPUT →		
		RESTORE →		
			RANDOMIZE →	
			ON-GOTO →	
			0 initiali-	
			satie →	
				READ/WRITE
				LOC/LOF
				CLK$
				DAT$
				LEN
				USR$
				STR$
				VAL
				ASC
				TIM

Figuur 1

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

COMPUTERVERZEKERING

door J.F.C. van Epen

Voorwoord van de redactie

Gezien het aantal kritische vragen dat door de aanwezigen op de vergadering werd gesteld, is er nog veel onduidelijkheid omtrent reikwijdte, strekking en interpretatie terzake van computerverzekering.
Ook het formele punt van het voldoen aan alle gestelde regels in de kleine letters van de polis is op zich reeds een gevaarlijk punt.

Daarbij komt nog dat het assuradeur zijn een vak op zich is, dat niet zonder meer door de accountant wordt bestreken zonder raadpleging/gebruik maken van de deskundige inbreng van assurantiemakelaars.

Door de heer J.F.C. van Epen secretaris van de N.G.I.-Sectie Beveiliging werd het volgende verslag gemaakt.

COMPUTERVERZEKERING

Op 14 maart jl. werd voor de N.G.I.-Sectie Beveiliging een lezing gehouden over de Verzekering van risico's in de automatisering.
In een volgend nummer van Compact nemen wij een volledig verslag op van deze lezing. Een aantal belangrijke aspecten echter willen we thans reeds vermelden omdat in de praktijk is gebleken dat er met betrekking tot dit type verzekeringen niet steeds een duidelijk beeld bestaat.

Onderscheiden worden "Maatschappij"-polissen en "Makelaars"-polissen, waarvan de eerste categorie - op een enkele uitzondering na - veelal beperkt is ten aanzien van het verzekeren van specifieke risico's.
Attentie is hier geboden!

De volgende aspecten kunnen worden verzekerd:
- materiële schade;
- extra kosten (bijvoorbeeld bij uitwijken);
- reconstructiekosten;
- bedrijfsschade;
- fraude/misbruik;
- beroepsaansprakelijkheid (indien voor derden wordt verwerkt).

Een zogenaamde computerverzekering dekt in één polis de eerste drie genoemde risico's. Soms is hierbij ook het brandrisico meeverzekerd, meestal echter niet!

Verzekering van materiële schade houdt in:
- plotselinge en onvoorziene materiële beschadiging en
- verlies van de verzekerde zaak ten gevolge van diefstal.

Ten aanzien van een groot aantal zaken kunnen uitsluitingen voorkomen, die meestal wel tegen een extra premie zijn mee te verzekeren. Sommige zaken zoals verduistering of slijtage zijn uiteraard niet verzekerbaar.

Bij de verzekering van "extra kosten" dient goed te worden gelet op de omschrijving daarvan. Bijvoorbeeld: Extra kosten zijn kosten, welke zijn verschuldigd in verband met het op een andere wijze uitvoeren van de werkzaamheden. Daaronder kunnen vallen (in een uitwijksituatie):
- meerkosten gebruik van bij derden aanwezige apparatuur;
- transportkosten;
- meerkosten voor het elders te werk stellen van het eigen personeel, dan wel het inhuren van personeel van derden.

Verzekering van reconstructiekosten voor verloren gegane bestanden en/of programmatuur is alleen aan te bevelen indien dit tegen een acceptabele premie kan geschieden. In veel gevallen is het beter goede back-up-procedures te hanteren, kopiebestanden buitenshuis te bewaren etc.

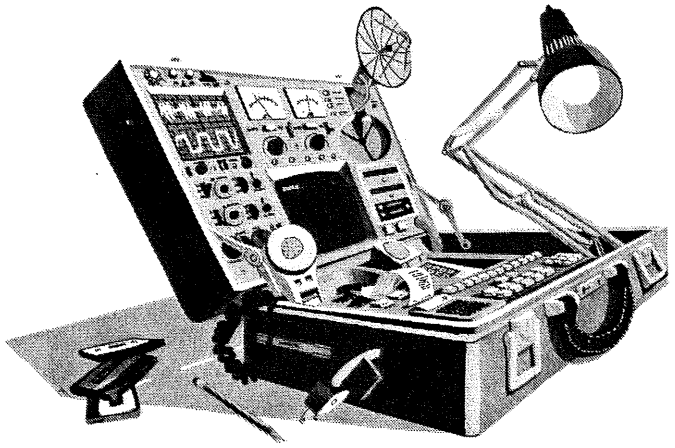
De overige genoemde verzekeringssoorten komen minder voor.
Het verzekeren tegen bedrijfsschade ten gevolge van schade aan de apparatuur is alleen noodzakelijk indien er met de computerverwerking niet kan worden uitgeweken.

Bij fraudeverzekering dient te worden bedacht dat deze alleen dekt het geldelijk verlies dat men kan lijden ten gevolge van frauduleuze handelingen via de computer.

Wordt voor derden verwerkt, dan is een beroepsaansprakelijkheidsverzekering aan te bevelen. Grove nalatigheid kan namelijk door bijvoorbeeld leveringsvoorwaarden moeilijk worden uitgesloten!

Zoals gezegd zullen wij in de volgende Compact nader op deze materie ingaan, onder meer door de nu weergegeven kernpunten te voorzien van kanttekeningen, commentaar en voorbeelden. Uiteraard zoals deze in de gehouden lezing naar voren zijn gekomen.

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



DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

Deze keer twee bijdragen van verschillende schrijvers. Het artikel van Marieke van Lith behandelt weliswaar niet diepgaand een belangrijk facet van het gebruik van Multiplan; in onze cursus Personal Computer wordt hierop dieper ingegaan.

Het tweede artikel is van de hand van Henri Spape, die een verhelderend artikel schreef over de "Conversie van programmatuur op microcomputers".

CONTROLE-ASPECTEN BIJ MULTIPLAN

door mevrouw drs. M.C. van Lith

Multiplan is een voorbeeld van een spread-sheet calculator, een toepassingsprogramma voor microcomputers, dat werkt op basis van "14-kolommenpapier". De "cellen" van zo'n spread-sheet worden aangeduid met een rij en een kolomnummer. Elke cel kan een tekst, een getal of een formule bevatten en gegevens kunnen van de ene sheet naar de andere worden gekopieerd met behulp van external copy's. Het pakket wordt veel gebruikt voor toepassingen zoals consolidatiemodellen, afschrijvingsstaten, budgetten, resultatenprognoses etc.

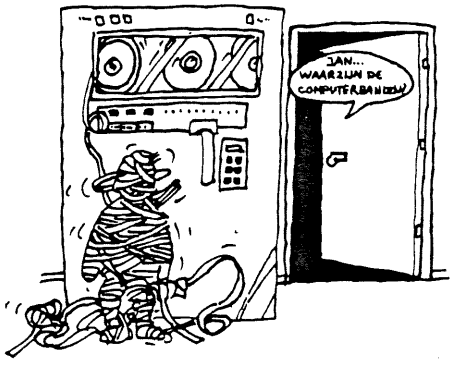
In het pakket zijn een aantal geprogrammeerde controles aangebracht, bovendien zijn er een aantal mogelijkheden voor de gebruiker om zijn gegevens zelf te beschermen.

Enkele controles verzorgd door het pakket zijn onder andere:
- de controle op fouten in formules;
- in principe kunnen alleen Multiplan-bestanden worden geladen;
- beveiliging tegen overschrijven van de bestanden op de diskette. (Er wordt om een bevestiging gevraagd.)

Door de gebruiker uit te voeren controles:
- een mogelijke beveiligingsmethode is het gebruik van de IF-opdracht. Deze opdracht kan gebruikt worden om een foutboodschap af te drukken "if" een bepaalde fout optreedt;
- met behulp van het lock-commando is het mogelijk bepaalde cellen vast te zetten, zodat ze niet per ongeluk kunnen worden overschreven;
- Multiplan biedt de mogelijkheid de spread-sheet in formulevorm te printen. Met dit overzicht is het mogelijk snel fouten op te sporen.

Een goede documentatie is onontbeerlijk en hoort te bestaan uit:
- een relatiediagram, dit is een schema waarin de verschillende external copy's zijn vastgelegd;
- sheet-registratie, dat wil zeggen een overzicht van de inhoud van de verschillende sheets;
- disketteregistratie, bevattende de inhoud van de verschillende diskettes.

Zoals de praktijk helaas al te vaak heeft aangetoond, is het regelmatig maken van een back-up (een volledige copy op een andere diskette) heel erg belangrijk.



Met behulp van een plakkertje over de inkeping van de diskettes, de write protect notch, kan worden voorkomen dat op de diskette bestanden worden overschreven. Uiteraard verdient het aanbeveling belangrijke gegevens achter slot en grendel te bewaren.

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

CONVERSIE VAN PROGRAMMATUUR OP MICROCOMPUTERS

door ing. H.A.J.M. Spape

1. Inleiding

In wezen is de conversie van programmatuur voor microcomputers niet anders dan die voor andere computers.
Enkele specifieke eigenschappen van microcomputers kunnen echter extra moeilijkheden of voordelen met zich mee brengen. Deze eigenschappen zijn:

a. Een microcomputer wordt veelal aangeboden als een samenstel van bij elkaar behorende apparatuur. Dikwijls is een groot deel van de randapparatuur geïntegreerd in één behuizing. Derhalve is het, in tegenstelling tot de situatie bij grotere computers, slechts beperkt mogelijk om zelf randapparatuur te kiezen, dan wel de reeds in gebruik zijnde apparatuur bij een andere CVE te gebruiken.
b. De markt voor microcomputers is voortdurend aan veranderingen onderhevig. De ontwikkelingen op het gebied van hardware (16 bit micro's, grotere interne geheugens, winchester disks in plaats van of naast floppies) leiden tot een aanbod van meer en betere software en de intrede van nieuwe besturingssystemen.
Deze frequente veranderingen kunnen betekenen dat meer geconverteerd moet worden, hetzij naar andere hardware, hetzij naar een ander besturingssysteem, dan wel beide.
c. Gangbare besturingssystemen voor microcomputers (CP/M, MS-DOS) worden door nagenoeg elke microcomputerproducent in combinatie met de apparatuur aangeboden. Dit betekent dat de conversie-inspanning gering kàn zijn wanneer wordt overgegaan naar andere hardware.

In dit artikel zullen nader belicht worden:

a. Conversieproblematiek bij overgang naar een andere microcomputer met hetzelfde besturingssysteem (operating system, OS) en dezelfde processor.
b. Moeilijkheden welke zich voor kunnen doen bij overgang naar een ander besturingssysteem en/of een andere processor.

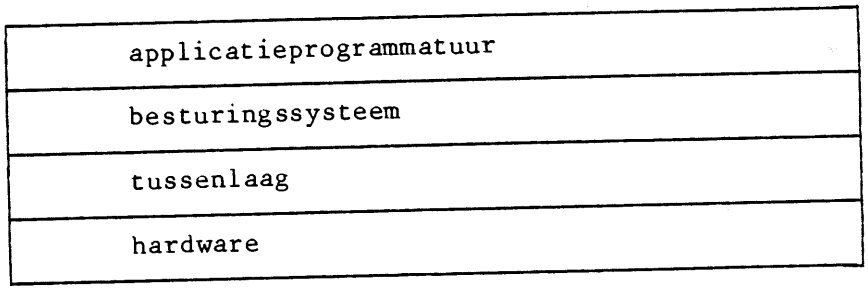
In beide gevallen zal worden ingegaan op de gevolgen voor zowel zelfgeschreven programmatuur als softwarepakketten.

Overgang naar een andere microcomputer met zelfde OS en processor

2.1 Algemeen

De overgang naar een andere microcomputer met hetzelfde besturingssysteem en dezelfde processor als de oorspronkelijke micro kan zich bijvoorbeeld voordoen bij annoncering van goedkopere doch qua capaciteit en kwaliteit vergelijkbare microcomputers, bij standaardisering van in een organisatie te gebruiken microcomputers of in geval van ontevredenheid over de prestaties van de te vervangen microcomputer en/of de leverancier ervan.
Het feit dat de processor ten opzichte van de vervangen microcomputer niet veranderd is, betekent dat vertaalde (dit is slechts in machinecode aanwezige) programma's in principe uitvoerbaar zijn.
Bij de overgang naar een andere microcomputer ligt de basis van de conversiemoeilijkheden in de andere samenstelling van de hardware (in casu randapparatuur). Het besturingssysteem schermt een belangrijk deel van de hardware af van de toepassingsprogramma's. Dat wil zeggen, het besturingssysteem schept een omgeving voor de programmatuur die nagenoeg onafhankelijk is van de gehanteerde apparatuur. Dit gebeurt veelal door de mogelijkheid randapparatuur aan te duiden met een naam. Deze naam identificeert voor het OS een bepaald randapparaat (bijvoorbeeld "A:" voor een diskette-eenheid). Wanneer op een andere microcomputer met hetzelfde besturingssysteem aan een randapparaat met een bepaalde naam wordt gerefereerd zal dit randapparaat zich op dezelfde wijze aan de toepassingsprogrammatuur voordoen als op de vervangen micro het geval was. Zelfs voor een groot deel van het besturingssysteem zelf, zijn specifieke hardware-eigenschappen transparant. Deze eigenschappen worden afgeschermd door een tussenlaag (vergelijk: Interface programma [DRIF82]) die op een universele wijze met de om input of output vragende programma's communiceert (zie afbeelding 1). Zie hier het gebruik van een tussenlaag door de producent van het besturingssysteem teneinde de conversie-inspanning bij het implementeren van het OS op andere hardware te minimaliseren.

Afbeelding 1.
Afschermen specifieke hardware-eigenschappen voor het OS.



Dit betekent bijvoorbeeld dat diskettes (floppy disks), aangemaakt op de te vervangen microcomputer, in vele gevallen zonder meer door de nieuwe micro gelezen kunnen worden. Voorwaarde hiervoor is slechts dat de fysieke eigenschappen van de diskettes overeenkomen (bijv. de omvang 5.25 vs. 8 inch). Evenzo geldt voor de uitvoer naar de printer, het beeldscherm of een datacommunicatiepoort dan wel invoer van het toetsenbord of een datacommunicatiepoort dat dit tot op zekere hoogte onafhankelijk van de gebruikte microcomputer gebeuren kan. Problemen doen zich voor wanneer van speciale mogelijkheden van randapparatuur gebruik wordt gemaakt. Met speciale mogelijkheden worden bijvoorbeeld bedoeld:

- eigenschappen van het beeldscherm zoals knipperen, onderstrepen of het op een andere wijze accentueren van een bepaald gedeelte van het scherm;
- functietoetsen op het toetsenbord;
- de mogelijkheid om een (matrix)printer een afwijkend lettertype te laten afdrukken.

Omdat een microcomputer veelal interactief wordt gebruikt zijn de eerste twee bijzonder belangrijk.

De besturingscodes welke naar de randapparatuur moeten worden gestuurd om een speciale eigenschap in te schakelen zijn over het algemeen afhankelijk van het gebruikte merk en type randapparaat. Hoewel veel verschillende randapparatuur overeenkomstige speciale mogelijkheden heeft is er nagenoeg geen standaardisatie in de besturingscodes. Deze worden ook niet door het besturingssysteem afgeschermd. Er is derhalve geen universele manier om, zonder zelf voorzieningen daartoe te treffen, een speciale mogelijkheid van een beeldscherm, toetsenbord of printer te benutten.
Het spreekt overigens voor zich dat, wil een voor de gebruiker onmerkbare conversie mogelijk zijn, de vervangende microcomputer over tenminste de speciale mogelijkheden van de vervangen micro moet beschikken (als zelfgeschreven programma's of standaardpakketten gebruik maken van tien functietoetsen zullen deze op beide micro's aanwezig moeten zijn).

2.2 Standaardpakketten

Voor de gangbare besturingssystemen voor microcomputers bestaat een uitgebreid scala aan standaardprogrammatuur. Een aantal pakketten zal zonder meer naar een andere microcomputer overdraagbaar zijn, namelijk die, welke geen gebruik maken van speciale mogelijkheden van randapparatuur.

Producenten van de software-pakketten ondervonden vanzelfsprekend de problemen die zich voordoen met betrekking tot de speciale mogelijkheden van randapparatuur. Er is op twee manieren getracht dit te ondervangen:

1. Het aanpassen van het pakket aan de hardware van een specifieke micro, waardoor het uitsluitend voor die micro of compatibele micro's geschikt is.
2. Het gebruik maken van een tussenlaag. Hierbij is de mogelijkheid geschapen om aan te geven van welke microcomputer gebruik wordt gemaakt, veelal door een keuze te maken uit een aantal, bij het pakket bekende, types. Het is zelden mogelijk om de bij een bepaalde functie van een randapparaat behorende besturingscode op te geven.
   Door deze methode is het standaardpakket alleen geschikt voor de microcomputers die qua eigenschappen aan het pakket bekend zijn.

Wanneer een bepaalde microcomputer bijzonder gewild is, doet zich het verschijnsel voor dat software-leveranciers hun produkten specifiek voor deze micro geschikt maken. Er wordt dan in bepaalde gevallen, dikwijls om redenen van verwerkingssnelheid, om het besturingssysteem heen, direct de hardware (bijvoorbeeld beeldscherm) aangestuurd.
Het spreekt voor zich dat de overdraagbaarheid van deze pakketten bijzonder gering is.
Voor de koper van zo een pakket is veelal niet merkbaar dat het programma speciaal voor zijn merk of type computer werd gemaakt. Hoogstens blijkt het uit een vermelding bij het starten van het programma, zoals bijvoorbeeld "standaardprogramma A, merk X versie". Vóór aanschaf van een standaardpakket moet daarom vastgesteld worden of het mogelijk slechts voor één bepaalde computer geschikt is.

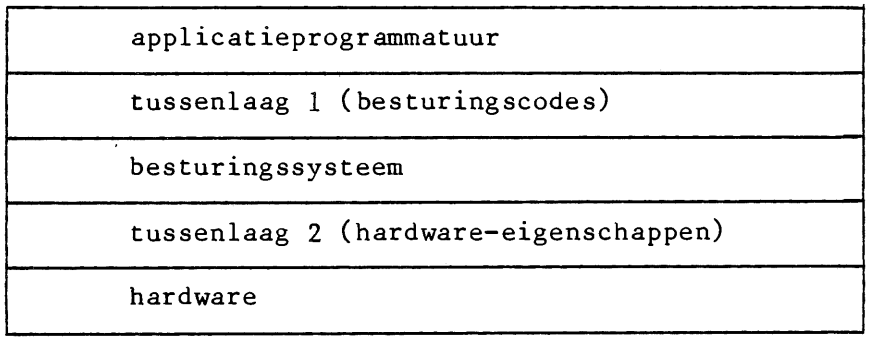
2.3 Zelf ontwikkelde programmatuur

De meeste programmatuur voor microcomputers zal (voor zover dit niet door professionals gebeurt) geschreven worden in BASIC (Beginners All Purpose Symbolic Instruction Code). Hiermee doet het eerste probleem zich reeds voor. Er zijn ettelijke verschillende Basic-versies in gebruik. Gepretendeerd wordt wel dat er enkele (...) de facto standaard Basic-versies zijn, zoals Microsoft's MBASIC en Digital Research's CBASIC. Bij gebruik van dezelfde Basic interpreter op verschillende computers zou de programmatuur dan zonder meer werken. Hieraan zijn echter twee beperkingen.

1. Omdat Basic bij nagenoeg elke microcomputer standaard geleverd wordt, wordt het (door, of in opdracht van de leverancier van de computer) dikwijls voorzien van mogelijkheden die juist op die bepaalde microcomputer aanwezig zijn. De Basic statements die dit verzorgen zullen door dezelfde Basic interpreter op een andere microcomputer niet of niet goed worden uitgevoerd.

2. Basic kent geen geschikte faciliteiten om op een zinvolle manier gebruik te maken van tussenlagen ten einde onafhankelijk te zijn van bepaalde besturingscodes van de hardware. Hier wordt een laag tussen applicatieprogramma en besturingssysteem bedoeld (zie afbeelding 2.). Bij overgang naar andere hardware behoeft dan slechts de tussenlaag en niet alle applicatieprogrammatuur te worden veranderd (zie [DRIF82]).

Afbeelding 2.
Applicatieprogrammatuur onafhankelijk maken van specifieke besturingscodes voor randapparatuur.



Zo een tussenlaag wordt wel "virtueel randapparaat" genoemd.
Een ieder die (micro)computers gaat gebruiken zal vaststellen aan welke basiseisen die computer zal moeten voldoen. Verlangd wordt bijvoorbeeld dat de printer in twee lettergroottes moet kunnen werken en dat het beeldscherm de mogelijkheid moet hebben bepaalde delen van het scherm te accentueren door middel van oplichten, knipperen en onderstrepen.
Op grond van deze eisen kunnen (nog vóórdat een computer wordt aangeschaft) virtuele randapparaten worden gedefinieerd waarna gestart kan worden met het ontwikkelen van de programmatuur.
Het definiëren van de virtuele randapparaten houdt niets anders in dan het vastleggen welke besturingstekens de virtuele terminal heeft om een bepaalde functie uit te voeren.
Als de besturingscodes van de uiteindelijke apparatuur bekend zijn kan een tussenlaag worden gebouwd die, wanneer een virtuele besturingscode ontvangen wordt, deze omzet in een die voor het specifieke randapparaat geldt.

Wanneer van een geschikte programmeertaal gebruik wordt gemaakt kan de aanwezigheid van een tussenlaag voor de applicatieprogrammeur volledig transparant zijn.

Het gebruik van tussenlagen brengt onvermijdelijk een performance-verlies met zich. Er wordt immers een extra stap uitgevoerd. Wanneer dit performance-verlies niet acceptabel is, en de wijze waarop de tussenstap wordt uitgevoerd niet verder te optimaliseren is, zal het concept van de tussenlaag verlaten moeten worden. Het enige alternatief is de programmatuur te verdelen in onderdelen die wel en die niet apparatuurafhankelijk zijn (waarvoor dus geen respectievelijk wel een tussenlaag kan worden gebruikt), en dan de apparatuurafhankelijke delen op een zodanige wijze te documenteren dat precies vastligt waar welke wijzigingen moeten worden aangebracht als naar andere apparatuur wordt overgegaan.

3. Overgang naar een ander OS en/of een andere processor

Deze verandering zal zich bijvoorbeeld voordoen bij verschuiving van het software-aanbod in de richting van andere besturingssystemen (zoals recent gebeurde van CP/M naar MS-DOS) of in het geval een dringend gewenst programmapakket alleen onder het andere besturingssysteem verkrijgbaar is en het werken met verschillende operating systems niet gewenst is.
Er zijn twee gevallen te onderscheiden, namelijk overgang naar een ander besturingssysteem én andere hardware en het in gebruik nemen van een ander besturingssysteem op de reeds aanwezige micro. De problematiek van een geheel andere microcomputer is reeds onder 2. aan de orde gekomen. Beperking tot het tweede geval is derhalve voldoende, waarbij bovendien niet uitgebreid zal worden ingegaan op bestandsconversie, aangezien dit buiten het bestek van dit artikel valt.
De problematiek bij overgang naar een ander besturingssysteem is ernstiger dan die welke onder 2. behandeld is. De eerste moeilijkheid is dat bestanden die onder het ene OS zijn aangemaakt niet zonder meer door het andere te lezen zijn. Elk besturingssysteem beschrijft en beheert een diskette op een eigen wijze. Dit betekent dat allerlei gegevensbestanden, door zowel standaardprogrammatuur als eigen programmatuur aangemaakt niet meer beschikbaar zijn. Dit geldt evenzo voor tekstbestanden en dus ook voor programma-source (mits als tekst opgeslagen). Door gebruik te maken van een eenvoudige datacommunicatieverbinding kunnen bestanden van de te vervangen naar de vervangende microcomputer worden overgestuurd. Met name tekstbestanden kunnen op deze wijze zonder veel moeite van de ene op de andere microcomputer worden overgezet. Bij bestanden die verwerkt worden door standaardsoftware kan een extra complicatie optreden. Deze wordt beschreven in de volgende paragraaf.

3.1 Standaard-software

Wanneer zich op de software-markt een duidelijke verschuiving naar een ander besturingssysteem voordoet betekent dit dat vele standaard-software-producenten zich genoodzaakt zullen zien tot het aanpassen van hun pakket aan het nieuwe operating system. In het meest gunstige geval heeft dit voor de gebruiker geen gevolgen. Dan moet de nieuwe versie van het pakket dezelfde functies op dezelfde wijze uitvoeren als de oude versie en moeten door het oude pakket gehanteerde record-indelingen ook door het nieuwe worden geaccepteerd. Met name dit laatste zal in de meeste gevallen niet van toepassing zijn doordat van faciliteiten die het nieuwe OS inzake bestanden en dergelijke biedt gebruik is gemaakt. Dit betekent dat alle gegevens die met het nieuwe pakket worden gebruikt opnieuw moeten worden ingevoerd, of dat een conversie-programma moet worden gemaakt als de verschillen tussen oude en nieuwe record lay-out bekend zijn.
Bovendien zal de producent van het software-pakket de noodzakelijke conversie-inspanning benutten om eventuele zwakke punten in het pakket te elimineren, waardoor het functioneel ook anders kan zijn.
Wanneer van veel standaard-software gebruik wordt gemaakt zal terdege overwogen moeten worden of het niet beter is van twee besturingssystemen gebruik te maken.

3.2 Zelf ontwikkelde programma's

Als een ander besturingssysteem in gebruik wordt genomen zullen programma's die oorspronkelijk onder een ander OS werden gebruikt, opnieuw vertaald moeten worden en wel door een compiler die gemaakt is voor gebruik met het nieuwe besturingssysteem. Beginadressen van I/O afhandelingsroutines e.d. zullen immers anders zijn. Dit impliceert dat een compiler voor de betreffende programmeertaal beschikbaar moet zijn voor het nieuwe OS. Dit zal, wanneer zowel taal als besturingssysteem veel gebruikt worden, geen probleem zijn. Belangrijker is dat de compiler voor het nieuwe besturingssysteem dezelfde taaldefinitie hanteert als die van de oorspronkelijke compiler. Bedenk hier dat de producent van de compiler mogelijk kleine wijzigingen in de nieuwe versie heeft aangebracht. Het is daarom belangrijk te kiezen voor een programmeertaal waarvoor een (de facto) standaard bestaat. Is reeds een programmeertaal in gebruik waarvoor geen standaard bestaat dan zullen verschillen van de nieuwe met de vervangen compiler moeten worden astgesteld en zal de programmatuur op de betreffende plaatsen moeten worden aangepast. Hierna zal het geheel opnieuw op juiste werking onderzocht worden (testen). Als de taal op essentiële punten afwijkt moet wellicht tot volledig herprogrammeren worden besloten. Over het algemeen worden geen conversie-tools aangeboden.

Anticiperend op conversie moet in de programma's rekening gehouden worden met een eventuele verandering van operating system. Dit houdt onder andere in dat onderdelen die OS afhankelijk zijn, zoals bestandsnamen en namen van randapparaten slechts één keer in een programma mogen voorkomen, namelijk op een vaststaand punt (bijvoorbeeld bovenin het programma) alwaar ze worden toegekend aan een door het gehele programma gebruikte andere naam.

4. Samenvatting en afsluiting

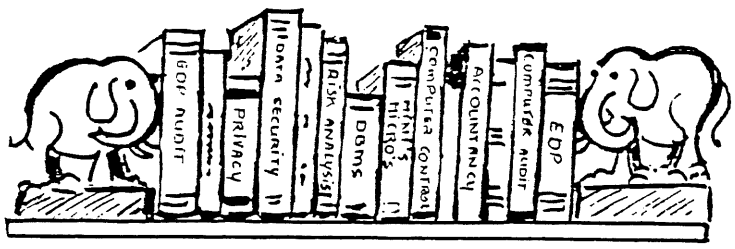
Conversie van programmatuur op micro's onderscheidt zich vooral van die op andere computers door het feit dat het dikwijls mogelijk is om op een andere computer hetzelfde besturingssysteem te blijven gebruiken. Dit kan, wanneer bij het ontwikkelen van programmatuur op een eventuele conversie is geanticipeerd, de conversie-inspanning aanzienlijk beperken. Bij dit anticiperen is het gebruiken van tussenlagen een krachtig hulpmiddel. Wanneer wordt overgegaan naar een ander besturingssysteem is het van belang of destijds voor een in voldoende mate overdraagbare programmeertaal is gekozen. Is dit niet het geval dan belandt men in de chaos van verschillende programmeertaalversies die op de micro-software-markt worden aangeboden.
Als gebruik wordt gemaakt van standaard-software dan zal overgang naar een andere computer met hetzelfde besturingssysteem weinig problemen opleveren, zeker als men bereid is het software-pakket voor de andere microcomputer opnieuw aan te schaffen waardoor een aan eventuele speciale apparatuureigenschappen aangepaste versie wordt verkregen. Als naar een ander besturingssysteem wordt overgegaan kunnen er moeilijkheden optreden met betrekking tot het lezen van door de andere versie van het pakket aangemaakte bestanden, ook al zijn deze naar de lay-out van het nieuwe OS geconverteerd.

Literatuurverwijzing.

[DRIF82] Anticiperen op conversie.
A. van der Drift
Compact jaargang 9, nummer 29 herfst 1982.

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

Winter 1984/1985



Boeken

AUDITING ADVANCED EDP SYSTEMS, A RESEARCH STUDY BY DR. GORDON B. DAVIS AND DR. RON WEBER FOR THE LIMPERG INSTITUTE, THE NETHERLANDS, 1-7-1981

Boekbespreking door H. Roos*)

1. Inleiding

De bespreking is gebaseerd op het officiële "Final Technical Report" (1). De handelseditie wijkt daar niet essentieel van af (2). Citaten zijn tussen aanhalingstekens geplaatst en zo veel mogelijk vertaald. Het is niet zonder reden dat deze bespreking eerst geruime tijd na de publicatie van het "final technical report" zijn weg vindt naar deze rubriek.
De reden is dat er enige bedenkingen van nogal fundamentele aard zijn te maken bij deze studie. Dat heeft referent doen aarzelen omdat beide auteurs bepaald hun sporen wel verdiend hebben en bijgevolg het risico van verkeerde beoordeling nadrukkelijk aanwezig is. Het uitstel heeft als voordeel dat inmiddels wel alle geïnteresseerden van het rapport kennis zullen hebben genomen en hun eigen mening gevormd en voorts dat latere publicaties van de auteurs (3,4) en van anderen (5,6) over het onderhavige onderwerp geraadpleegd konden worden, wat de kans op misverstand hopelijk heeft verkleind.

2. Algemene opmerkingen

In de eerste plaats moet mij van het hart dat het niet geheel begrijpelijk is waarom een bij uitstek Nederlands onderzoeksinstituut een dergelijke opdracht niet aan Nederlandse onderzoekers heeft verstrekt. Dit getuigt mijns inziens van een onderschatting van het potentieel dat binnen het Nederlandse beroep aanwezig is.
Voorts enige opmerkingen over de afbakening van het onderwerp. Het begrip "auditing" wordt niet gedefinieerd. Mogelijk verschillende controledoelstellingen komen dan ook niet aan de orde.
Het accent ligt op "geavanceerde EDP-systemen".

*) Deze boekbespreking is aanvankelijk in een eerdere versie gepubliceerd in de Accountant nr. 5 van januari 1985 onder de rubriek "Accountant en automatisering". pag. 304.

De auteurs onderkennen de afbakening van dit begrip als probleem en stellen dat het geven van voorbeelden alleen niet bevredigend is. De definitie die ze geven "Een geavanceerd computersysteem is beter in staat tot aanpassing aan en opvangen van zich wijzigende gebruikers- en omgevingseisen dan bestaande wijdverbreide computer-systemen" (p.10) wordt gemotiveerd met de veronderstelde overeenkomst met levende systemen.
Dit lijkt wat ver te gaan. Een geavanceerd systeem zou op die manier op één lijn komen met spreeuwen, kraaien en straatgras (Poa annua L.) als bij uitstek adaptieve levende systemen. Realiseren we ons wat dat ten aanzien van levende systemen betekent.
Kenmerk van een levend systeem met groot aanpassingsvermogen is de geringe mate van specialisatie, waardoor handhaving onder zeer uiteenlopende omstandigheden mogelijk is. Het past zich dus niet echt aan, maar is op zich reeds door zijn genetisch bepaalde eigenschappen aangepast.
Aldus geïnterpreteerd zou een geavanceerd systeem nauwelijks enige aanpassing behoeven bij het optreden van drukfactoren. De systeemstatus zal niet wijzigen en de accountant zal bijgevolg geen aanleiding hebben tot het onderzoeken van gewijzigde systeemfuncties en interne controles.
De auteurs gaan echter verder en beschouwen een systeem als soort en niet als individu. Een gewijzigde systeemversie wordt vergeleken met een mutant. Voldoet die aan de gewijzigde omstandigheden dan zouden de daarvoor verantwoordelijke eigenschappen in andere systemen worden overgenomen en zou de aldus ontstane soort niet langer als geavanceerd worden beschouwd (p.11). Dit impliceert dat een systeem pas kan worden beschouwd als geavanceerd indien en nadat is gebleken dat het met succes kon worden aangepast aan andere systeemeisen die zowel technisch als functioneel van aard kunnen zijn. Zowel aanpassing als eisen mogen mijns inziens niet triviaal zijn.
Een voorbeeld ter verduidelijking. Het is in het algemeen wenselijk dat een toepassing betrekkelijk ongevoelig is voor wijzigingen in het hardware/software deelsysteem.
Een bekend antwoord daarop is de standaardisatie van programmeertalen. Volgens de definitie konden toepassingen die in de begintijd van COBOL in die taal werden geschreven als geavanceerd worden aangemerkt. Hetzelfde geldt thans bijvoorbeeld voor microcomputertoepassingen die in "C" zijn geschreven. De definitie blijkt derhalve te kunnen worden toegepast op andere dan de door de auteurs min of meer intuïtief als geavanceerd aangemerkte systemen en zelfs op historische situaties.
Het is duidelijk dat de gegeven definitie verre van operationeel is voor de dagelijkse controlepraktijk en derhalve als niet bruikbaar dient te worden verworpen.

In feite komen de auteurs dan ook niet verder dan het geven van globale voorbeelden van geavanceerde systemen: online realtime update systems, database management systems en distributed systems. Een nadeel hiervan is dat het niet goed mogelijk is om vast te stellen of een systeem geavanceerd is of niet. Dit heeft als gevolg dat bij de toetsing van hypothesen geen rekening kon worden gehouden met eventuele verschillen in geavanceerdheid tussen ogenschijnlijk gelijksoortige systemen.

3. Beknopte weergave van de door de auteurs gekozen werkwijze en geponeerde theorie

De auteurs hebben binnen de blijkbaar ruim geformuleerde opdracht gekozen voor: "het ontwikkelen van een theorie om te verklaren waarom en hoe EDP systems veranderen van eenvoudig naar meer complex en het testen van die theorie en zijn gevolgen voor de controlepraktijk". De studie beoogt een uitgangspunt te bieden voor "discussie en onderzoek ter beoordeling van de bruikbaarheid van een systeemveranderingstheorie ten behoeve van EDP auditors" (p.VI).
Accountants onderzoeken geautomatiseerde systemen en de daarmee verband houdende interne controles als onderdeel van het controleproces. Het resultaat is een vastlegging van het systeem op een bepaald moment in de vorm van vragenlijsten, stroomdiagrammen en verbale beschrijvingen. Indien het systeem is gewijzigd wordt dit proces herhaald per een volgend moment.
De auteurs stellen nadrukkelijk dat daarbij het veranderingsproces zelf niet in het onderzoek wordt betrokken.
Hier past een vraagteken. Ze beogen nu een systeemveranderingstheorie met behulp waarvan de onderzoekende accountant zich geheel kan concentreren op de veranderingen, op het waarderen van wijzigingen in de interne controle en het ontwerpen van andere controleprocedures en wel zodanig dat hij zich bij wijzigingen kan beperken tot een zo klein mogelijk deel van het systeem.
De voorgestelde theorie gaat uit van de beschouwing van organisaties als open systemen, waarin veranderingsprocessen op gang worden gebracht door druk uit de omgeving. Als de belangrijkste drukfactoren die de invoering van geavanceerde systemen kunnen veroorzaken worden onderkend:

- "tijdigheid van verwerking en toegang tot gegevens", leidend tot online realtime update systemen;
- "gemeenschappelijk gebruik, beschikbaarheid en aanpasbaarheid", leidend tot data base management systemen;
- "gemeenschappelijk gebruik en beschikbaarheid van de hulpmiddelen voor gegevensverwerking", leidend tot gedistribueerde systemen.

De theorie stelt dat druk en de reactie daarop achtereenvolgens optreden in:
- de omgeving;
- de organisatie;
- gegevensverwerkende deelsystemen;
- interne controles en
- accountantscontroleprocedures.

Het toepassen van de theorie is geformuleerd in de vorm van door de accountant te volgen procedures.
1. "Verdeel het geautomatiseerde systeem in deelsystemen".
2. "Onderken de huidige mate van bezorgdheid ten aanzien van mogelijke verliezen per deelsysteem".
3. "Onderken de drukfactor die aanleiding is tot verandering in de geautomatiseerde gegevensverwerking en het deelsysteem dat moet worden gewijzigd om de druk het hoofd te bieden".
4. "Onderken de veranderingen in de interne controle die nodig zijn als gevolg van de wijzigingen in het deelsysteem".
5. "Waardeer de invloed van de wijzigingen in de deelsystemen en in de interne controles op de mate van bezorgdheid ten aanzien van mogelijke verliezen".
6. "Onderken de noodzakelijke wijzigingen in accountantscontroleprocedures ten behoeve van het testen van de gewijzigde processen en van nieuwe of veranderde interne controles".

Door middel van een enquête onder 30 accountants is onderzocht of er overeenstemming bestaat tussen hun aanpak van systeemveranderingen en de systeemveranderingstheorie. Met andere woorden ligt die theorie mogelijk impliciet ten grondslag aan hun feitelijk opereren. Op basis van de enquêteresultaten is nauwelijks een uitspraak mogelijk.
Het heeft de onderzoekers verrast dat slechts weinig veranderingen in interne controle bleken te zijn gemotiveerd door de invoering van de drie types geavanceerde systemen. Hiermee in overeenstemming bleek dat tevens slechts weinig wijzigingen in audit-procedures door de geavanceerdheid van systemen werden gemotiveerd. De auteurs schrijven dit toe aan het ontbreken van een veranderingstheorie en aan een gebrek aan duidelijkheid van de in EDP-auditing gebruikte termen.
Onder de kopjes "de verdeling in subsystemen", "het gebruik van deskundigen bij het beoordelen van de invloed van geavanceerde systemen" en "het opheffen van dubbelzinnigheid in audit terminologie" worden enkele vermoedelijk hierop van invloed zijnde factoren besproken. Een mogelijke andere - gefaseerde - aanpak van onderzoek wordt kort geschetst die, wegens de daarbij beoogde maximale bundeling van kennis, een beter uitzicht biedt op het verklaren van thans niet op te helderen verschillen in beoordeling in ogenschijnlijk vergelijkbare situaties.

De studie besluit met een korte beschrijving van een stapsgewijze benadering van een wijzigingssituatie. De verschillende stappen sluiten formeel aan bij de gepostuleerde theorie. Bij nadere beschouwing beschrijven ze evenwel een normale audit procedure. Dat wil zeggen signaleer wijzigingen in het systeem, ga de invloed na op de interne controle en pas op grond daarvan het audit-plan aan. Het gebruik van termen als "expected loss concerns", "stress motivating the change", "closeness to the stress" en "accomodate the stress" werken eerder vertroebelend dan verhelderend.

4. Commentaar

Men kan zich afvragen of aan een dergelijke theorie behoefte bestaat en, indien bevestigend beantwoord, of die beperking tot EDP-auditors wel doelmatig is. De basis voor elke audit is immers een toereikend inzicht in het controle-object. Voorts zijn audit-doelstellingen in het normale geval van een financiële verantwoording als object onafhankelijk van welke techniek van administreren dan ook. Ergo, de beoogde basis voor het kunnen anticiperen op de invloeden van (technische) veranderingen bestaat in beginsel uit het op de voet volgen van die ontwikkelingen.
Aangezien nieuwe technieken praktisch altijd geruime tijd voor hun praktische commerciële toepassing in de vakpers worden besproken, ligt het voor de hand dat het regelmatig en systematisch kennis nemen van in die vakpers gepubliceerde ontwikkelingen een doeltreffende voorbereiding vormt op de confrontatie met nieuwe soorten systemen.
Aan het eind van het rapport komen de auteurs ook met zo'n suggestie, zij het dat de motivering totaal anders is. Onder de kop "gevolgen van de bevindingen voor verder onderzoek" (p.142), wordt gesteld dat het ontwikkelde begrippenstelsel (dit is een vertaling van het door de auteurs gebruikte begrip "conceptual framework") weliswaar een beknopte, krachtige theorie is die echter verdere verfijning behoeft. Voorts dat de geringe mate van overeenstemming tussen de geënquêteerden nadere verklaring behoeft en (nu komt het) zonodig corrigerende maatregelen dienen te worden getroffen zoals terzake het beroepsonderwijs. De auteurs vermoeden blijkbaar dat het verschil in reactie op vergelijkbare audit-situaties (het is overigens zeer de vraag of de vergeleken situaties wel voldoende homogeniteit vertonen) best kan komen door verschil in kennis en ervaring. Dat behoeft overigens mijns inziens beslist niet te leiden tot verschillen in doeltreffendheid van de uitgevoerde audits, hoogstens tot doelmatigheidsverschillen. Deze problematiek komt jammer genoeg niet aan de orde. Het gaat er in de praktijk niet alleen om of de accountant in een bepaalde situatie nog wel in staat is tot een oordeel te komen. Maar vooral ook, in het licht van de onvermijdelijk verder toenemende concurrentie, of hij dat op doelmatige wijze kan.

Een onduidelijk punt is de categorische stelling dat "De aanpak van het maken van nieuwe systeembeschrijvingen bij het onderzoek van het nieuwe systeem het systeemveranderingsproces niet behandelt" (p.2). De organisatie van de automatisering is immers te beschouwen als het overkoepelende deelsysteem - de infrastructuur - waardoor de wijzigingen in alle deelsystemen, ook de automatiseringsorganisatie zelf, tot stand komen. Blijkens de vakliteratuur en de vakvoorschriften is dat wel degelijk een object van accountantscontrole. Dit is de auteurs natuurlijk ook bekend. Verder zal geen accountant een systeem beoordelen los van zijn context. Het is jammer dat een tweetal in dit verband cruciale deelsystemen, te weten "systems management" en "computer operations" niet als deelsystemen in de enquête waren opgenomen. De auteurs erkennen dit ook als een gemis (p.32).
Een bezwaar is dat de toegepaste verdeling in deelsystemen niet voldoet aan de door de auteurs gestelde eis van losse koppeling. De auteurs stellen dat "de deelsystemen zijn bepaald in overeenstemming met de normatieve theorie die ten grondslag ligt aan gestructureerd ontwerpen; namelijk dat deelsystemen een interne samenhang vertonen en slechts zwak zijn gekoppeld met andere deelsystemen" (p.30). Het is jammer dat de auteurs op dit fundamentele punt niet nader zijn ingegaan. Verwijzingen naar de zeer goede literatuur hierover ontbreken geheel. Voor een overzicht kan worden verwezen naar Myers (7), waarin verwijzingen naar het merendeel der relevante publicaties zijn opgenomen. Kennisname van die literatuur en toepassing van de kernstukken daaruit op de door de auteurs gemaakte verdeling in deelsystemen (p.32) toont aan dat niet aan de op zich juiste eis van losse koppeling is voldaan. Een vermoedelijke oorzaak hiervan is dat de door de auteurs onderscheiden deelsystemen van zeer verschillende aard en orde zijn.
De auteurs onderkennen dat de geïntroduceerde hiërarchie van computersystemen arbitrair is (ref.3 p.35). Dit is een belangrijke oorzaak van de door de auteurs gesignaleerde onzekerheid met betrekking tot de precieze betekenis van de door EDP-auditors gebruikte terminologie.
Voorts vermelden ze een drietal problemen bij het toepassen van het "principe van nabijheid van de druk-factor", te weten:
het ontbreken van een "taxonomie van druk-factoren", het ontbreken van een methode om "nabijheid" te meten, en het ontbreken van een theorie ter verklaring van de plaats van wijzigingen in interne controles (p.145). Speciaal het laatste punt is van cruciaal belang.
De manier van onderscheiden van deelsystemen is van fundamenteel belang (p.143). De voorgestelde praktische benadering in een aantal stappen (6 volgens p.3, 8 volgens p.147 e.v.) heeft slechts zin indien

daarmee inderdaad de mogelijkheid wordt geboden tot een logische beperking tot "een of meer deelsystemen dicht bij de druk-factor" (ref.3 p.35). De auteurs doen geen poging aannemelijk te maken dat een onderscheid in deelsystemen mogelijk is, zodanig dat ten eerste de daarin voorkomende interne controle logisch onafhankelijk van de overige interne controles staat en ten tweede die deelsystemen een zodanig gering deel van het totale systeem vormen, dat deze benadering inderdaad tot een reële besparing leidt. Een logisch probleem is dat toetsing van de eerste voorwaarde praktisch nodig blijft. De vraag is hoeveel additionele inspanning daarmee gemoeid zal blijken.
Het is de vraag of het probleem niet reeds ligt in het geïntroduceerde hiërarchische verband. De systeemhiërarchie heeft betrekking op de doorwerking van de drukfactoren. Dit sluit echter niet uit dat er vanuit het interne controledeelsysteem relaties bestaan met meerdere computersystemen. Bezien vanuit controle-oogpunt is de relatie juist omgekeerd. Dit geldt ook voor de organisatie als laag in de hiërarchie. Die wordt gekenmerkt door een delegatiepatroon als gevolg van functie- en taakverdeling gebaseerd op specialisatie. Elke delegatie roept de noodzaak op tot controle en verantwoording (8). De interne controles kunnen met andere woorden niet worden los gezien van de verschillende niveaus van delegatie in de organisatie. Dit levert een aanmerkelijk ingewikkelder patroon van deelsystemen op. Er is nog wel sprake van een hiërarchie, doch de trits organisatie - computersysteem - interne controlesysteem komt op verschillende niveaus voor. Aangezien de totale organisatie geacht mag worden een gemeenschappelijk doel na te streven, zullen er tussen die "clusters" allerhande verbanden zijn te onderkennen. In elk geval de onder Nederlandse accountants zo vertrouwde geld- en goederenbeweging en de haaks daarop staande veranderingsorganisatie die moet zorgen voor een doorlopend evenwicht tussen vraag en aanbod van computerdiensten.

Referenties:

1. Auditing advanced EDP systems, Final technical report, July 1, 1981, A research study by Dr. Gordon B. Davis and Dr. Ron Weber for the Limperg Institute, The Netherlands.
2. Auditing advanced EDP systems, A survey of practice and development of a theory, Gordon B. Davis and Ron Weber, The management informations systems research center, The University of Minnesota, The Institute of Internal Auditors 1983.
3. The audit and changing information systems, Gordon B. Davis and Ron Weber, The Internal Auditor August 1983, p. 34-38.
4. Auditing advanced EDP systems: a system change model, Gordon B. Davis and Ron Weber, in Earl M. Wysong and Ivo de Lotto, Information Systems Auditing, Proceedings of the Information Systems Auditing Conference, Milan, Italy, September 26-28, 1983, Amsterdam, North Holland Publishing Company, 1983.

5. Book review by William F. Messier Jr., The Accounting Review, January, 1984, p.145.
6. Book review by Steven J. Ross, EDP Journal 1984, Vol. 1, p.41-44.
7. Composite/Structured design, Glenford J. Myers, Van Nostrand Reinhold, NY, 1978.
8. Organizations, James G. March and Herbert A. Simon, John Wiley & Sons, Inc., 1958.

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

Winter 1984/1985

TIJDSCHRIFTEN

door mw. D. Jansen Heijtmajer, J.L.H. Kooijman en L.N.M. Straathof met medewerking van J.C. Boer en drs. J. Kuipers

"Decentralizing Data Security"
Gordon L. Reid
Datamation, december 1984

De schrijver begint zijn artikel met de discussie omtrent de aard van de problematiek van gegevensbeveiliging (data security): is gegevensbeveiliging een organisatorisch of een technisch probleem?
Volgens hem kan een effectief beveiligingsprogramma alleen tot stand komen op basis van een beveiligingsbeleid, beveiligingssoftware en ondersteuning door het management en de gebruikers.
Indien sprake is van een geografische spreiding van bedrijfsactiviteiten alsmede gegevensbeveiliging zowel centraal als decentraal van belang is, heeft decentralisatie van (de verantwoordelijkheid voor) gegevensbeveiligingsactiviteiten een positieve invloed op de doeltreffendheid ervan.
De schrijver motiveert dit als volgt:

- Op de decentrale plaatsen kent men de gegevensbeveiligingsfunctionaris en zal men meer geneigd zijn om gegevensbeveiligingsmaatregelen na te leven en minder geneigd zijn om ongeautoriseerd de gegevens te gebruiken dan wel te wijzigen.
- De decentraal werkende gegevensbeveiligingsfunctionaris is sneller (en wellicht tijdiger) op de hoogte van functionarissen die ongeautoriseerde handelingen zouden kunnen uitvoeren dan een centraal werkende functionaris op gebied van gegevensbeveiliging.
- Gedecentraliseerde gegevensbeveiliging komt sneller tot stand en kost minder dan een gecentraliseerde gegevensbeveiliging. Dit is vooral van belang als de wijze van het computergebruik relatief veel wijzigt.

In het artikel wordt de nadruk gelegd op decentralisatie van gegevensbeveiligingsactiviteiten. Centraal zal echter zorg moeten worden gedragen voor coördinatie van deze activiteiten door middel van een "overall-gegevensbeveiligingsprogramma" en bepaalde standaardregels.

"Information Security: Reality and Fiction"
Richard I Polis
Computers & Security 3, 1984
Elsevier Science Publishers B.V.

door J.C. Boer

Het artikel geeft de ervaring weer die de auteur opgedaan heeft als partner van de Geneva Management Group. Dit Zwitserse bureau adviseert zo'n 5 jaar Europese bedrijven met betrekking tot de beveiliging van informatie bij geautomatiseerde gegevensverwerking en datacommunicatie.

De bewustwording van de noodzaak tot informatiebeveiliging is het sterkst bij de financiële instellingen. Binnen de overige takken zoals de industrie bestaan grote verschillen in het zich bewust zijn van de noodzaak tot informatiebeveiliging. Er is echter altijd een verschil tussen hetgeen noodzakelijk geacht wordt en de werkelijk getroffen maatregelen.

Door de opkomst van de Personal Computer is bij het grote publiek over het algemeen een bewustwording ontstaan voor het beveiligingsprobleem in samenhang met geautomatiseerde gegevensverwerking. Wat tot nu voor de meesten een risico was waar men ver van afstond, is nu een tastbaar probleem geworden.

De wijze waarop de financiële instellingen de organisatie, gericht op informatiebeveiliging hebben ingericht, varieert. De functie van informatiebeveiliging is ondergebracht bij een Interne controle-afdeling, een Organisatie-afdeling of is gespreid over de organisatie. Over het algemeen is slechts sprake van stafbevoegdheden (adviserend, verstrekken van functionele richtlijnen).
De reactie van de fabrikanten op eisen die de afnemers ten aanzien van beveiliging stellen, lopen uiteen van het zeer betrokken zijn bij het zoeken van een oplossing tot het afwimpelen van de noodzaak tot beveiliging.
De PTT (ook in internationaal samenwerkingsverband) is nauw betrokken bij ontwikkelingen op het gebied van beveiliging van datacommunicatie. Dit niet alleen omdat zij de leverancier van de datacommunicatieverbindingen is maar ook vanuit haar positie als financiële instelling.

Het artikel wordt afgesloten met de aanduiding welke stappen genomen moeten worden om tot een veilig systeem te komen. Genoemd worden: risico-analyse, system security audit, ontwerp en ontwikkeling van adequate maatregelen.

"Tutorial on telecommunications and security"
C.H. Nestman, J.C. Windsor en M.C. Hinson in Computers & Security 3, 1984

Wij kozen dit artikel om, evenals de schrijvers aangeven, "to jog the minds of the reader to remember key elements and components of Telecommunication systems".
In het artikel wordt een overzicht gegeven van de belangrijkste beveiligingsaspecten in een telecommunicatienetwerk.

Enkele stellingen: de aard van het beveiligingsprobleem is veranderd als gevolg van de toepassing van telecommmunicatie, omdat men niet meer zeker kan zijn van de veiligheid van alle hardware in het systeem. Het Operating System kan wel goed zijn beschermd, maar de netwerkgebruiker heeft nauwelijks enige grip op de lijnverbindingen die de computers koppelen. Voorts zijn de terminals in de verschillende locaties moeilijker te bewaken en ook de software in de verbindingsknooppunten (switches) is vaak zo complex dat het moeilijk is, zekerheid te verkrijgen dat de boodschappen uitsluitend aan de bedoelde geadresseerde zijn verzonden.

Beveiliging moet naast toegangscontrole worden gericht op het beveiligen van de data als zij in het netwerk onderweg is.

A. "Security Danger Points"

1. Terminals.
   - Fysieke beveiliging, automatische log-off, identificatiecodes voor zowel gebruiker als terminal zijn nodig.
2. Andere randapparatuur.
   - Kaartlezers, printers, tape- en schijfeenheden krijgen vaak onvoldoende aandacht.
3. Lijnverbindingen.
   - Zijn veelal geen eigendom zodat de beveiligingsmaatregelen alleen betrekking kunnen hebben op het onbruikbaar maken van berichten voor onbevoegden.
     Als enig mogelijke effectieve beveiliging wordt encryptie aanbevolen.
4. Verbindingsknooppunten.
   - Hier geldt hetzelfde als voor de lijnverbindingen: encryptie derhalve.

5. Gegevens.
   - Als bescherming van de gegevens zelf, worden genoemd end-to-end-encryptie en de verzending van de encrypte gegevens in een vorm die moeilijk te ontwarren is, bijvoorbeeld via packet switching, of via compressietechnieken.
6. Computer; CPU en Operating System.
   - Wordt uitermate belangrijk als de computer deel uitmaakt van het netwerk. Onbevoegde toegang kan bijvoorbeeld gericht zijn op remote-bestanden of programma's in bepaalde netwerklocaties. Het centrale systeem is er verantwoordelijk voor dat de locale installaties hiervan gevrijwaard blijven.

B. Beveiligingsaspecten met betrekking tot het telecommunicatienetwerk

De belangrijkste beveiligingsproblemen liggen bij de toegang tot het systeem en de integriteit van de informatie in het systeem.
(Omdat in dit deel van het artikel wellicht nuttige tips zijn opgenomen volgt een wat uitgebreider behandeling dan gewoonlijk.)

1. Toegangscontrole.
   Identificatie ("the identification of one member of a communication system to the other in a reliable, unforgetable way"); passwords, sleutels, etc.
   Passwords zijn overigens verre van ideaal, maar er zijn momenteel geen betere methoden beschikbaar.

   Autorisatie, dat wil zeggen het toekennen van bevoegdheden aan de gebruiker/terminalcombinatie.

   De definitie van identification geeft aan dat het gaat om de identificatie van de deelnemers van een communicatiesysteem, de schrijvers dringen er dan ook op aan dat niet alleen de gebruiker, maar ook de terminal zijn identiteit moet aantonen en dat voorts ook in bepaalde systemen de computer waarmee verbinding wordt gezocht, zich zal moeten identificeren aan de terminal.
   Dit om te voorkomen, dat terminalgebruikers passwords en identificatiecodes gaan doorgeven aan een onbevoegde die zich voordoet als het mainframe.
   Om het probleem "wie doet het eerst zijn masker af" op te lossen, wordt de volgende procedure geadviseerd:
   - gebruiker A (de terminal) stuurt een willekeurig, doch uniek gegeven, bijvoorbeeld een tijdsaanduiding (uur, minuut, seconde) naar het centrale systeem;
   - het centrale systeem encrypt het ontvangen gegeven met gebruikmaking van zijn authenticator-sleutels en stuurt het aldus vercijferde gegeven terug naar de terminal;

- de terminal ontcijfert het gegeven en vergelijkt het met het origineel verzonden bericht.
  Beide deelnemers zijn nu achtereenvolgens geïdentificeerd, zonder dat geheime gegevens zijn blootgesteld aan mogelijke indringers in het netwerk. De tijd als gegeven is uniek in zoverre dat het moeilijk is de encryptiesleutels te ontcijferen ook al vermoedt de indringer de inhoud van het bericht.

Autorisatie, systeem van dubbele identificatie:
Hierbij gaat het om de toegangsrechten tot de verschillende systeemcomponenten.
Geadviseerd wordt, toegangsrechten toe te kennen aan zowel gebruikers als terminals.
Als een gebruiker zich via een bepaalde terminal meldt, zal de combinatie de laagste van de twee toegangsrechten krijgen.
Hierdoor is het mogelijk, bepaalde bevoegdheden alleen toe te kennen aan die terminals die fysiek goed zijn beveiligd. Anderzijds kan voorkomen worden dat - overigens bevoegde gebruikers - vanuit onveilige locaties of over onveilige lijnen gevoelige berichten verzenden.

2. Integriteit

Encryptie wordt aanbevolen als beste middel voor de handhaving van de integriteit van gegevens die via het netwerk worden verzonden.

Conclusie

Zolang men apparatuur en software in eigen beheer heeft, kunnen beveiligingsregels worden gesteld waaraan het eigen personeel zich heeft te houden en waarop effectieve controle mogelijk is.
Zodra echter gebruik gemaakt (moet) worden van diensten van derden, hetgeen in een telecommunicatienetwerk al snel het geval is, zullen de berichten die over de lijnen worden verzonden zodanig moeten worden "verpakt" dat verkeerde bezorging of ongeautoriseerd kennis nemen geen risico's oplevert.
De situatie kan het beste vergeleken worden met een onderneming waarbinnen strikte procedures bestaan voor controle, autorisatie, verpakking en adressering van berichten, waarna vervolgens aan een toevallige voorbijganger wordt gevraagd de bezorging op zich te nemen.

Een en ander houdt in dat een bericht zodanig gecodeerd zou moeten zijn, dat het slechts informatiewaarde bevat voor degene voor wie het bericht bedoeld is.
Een effectieve regeling hiervoor kan alleen worden bereikt door gebruik te maken van geheime codes: encryptie.

"Cryptography for Computer Security: Making the Decision"
Warren W. Fisher
Computers & Security 3, 1984

door J.C. Boer

Het uitgangspunt van dit artikel van Warren Fisher is, dat cryptografie niet in alle gevallen de aangewezen weg is om tot informatiebeveiliging te komen. Hij sluit het artikel ook af met de opmerking dat cryptografie geen maatregel opzich is, doch een plaats heeft in de kosten/batenafweging waarbij alle beveiligingsmaatregelen betrokken zijn.

Na een korte historische inleiding wordt ingegaan op het DES (Data Encryption Standard). Hierbij wordt de vergelijking getroffen met een combinatieslot. Het mechanisme (bij DES het algoritme) is algemeen bekend, doch de cijfercombinatie (bij DES de uit 56 binaire posities bestaande sleutel) is geheim.

Voordat cryptografie overwogen wordt, moet eerst vastgesteld worden of beveiligingsmaatregelen noodzakelijk zijn. Indicaties voor de noodzaak tot beveiliging zijn:
- de informatie heeft betrekking op geld (of andere waarden);
- de informatie betreft bedrijfs- of overheidsgeheimen;
- er is sprake van vertrouwelijke gegevens van cliënten of werknemers;
- de informatie is nodig voor de uitvoering van routinematige activiteiten die specifiek zijn voor de huishouding.

De te treffen maatregelen kunnen bestaan uit:
- fysieke beveiliging;
- het gebruik van passwords;
- afschermen van gegevens voor bepaalde gebruikers of terminals (bijvoorbeeld het gebruik van unieke terminal-identificatiegegevens).

Deze maatregelen kunnen versterkt worden met cryptografie. De getroffen maatregelen dienen met elkaar in evenwicht te zijn. Indien tot cryptografie besloten wordt zal bijzondere zorg aan de sleutel (zowel tijdens het transport als tijdens het gebruik) moeten worden besteed.

Geconcludeerd wordt dat cryptografie alleen toegepast moet worden indien:
- er gegevens zijn die beveiligd moeten worden;
- de toepassing van cryptografie de bedreigingen vermindert;

- voldoende physieke beveiligingsmaatregelen getroffen zijn;
- het een economische oplossing is; dat wil zeggen hiermee niet getracht wordt andere beveiligingsdoelstellingen te bereiken dan waarvoor cryptografie opgezet is.

Opmerking

In het artikel wordt geen bijzondere aandacht besteed aan het onderscheid tussen het gebruik van cryptografie bij datacommunicatie en de opslag van gegevens. Dit onderscheid maakt ons inziens een nadere nuancering van de criteria mogelijk.

Laser optical disk: the coming revolution in on-line storage
Larry Fujitani in Communications of the ACM, June 1984 Volume 27 Number 6

door drs. J. Kuipers

Behoefte aan capaciteit

De toegenomen behoefte aan on-line gegevensopslag leidde tot de ontwikkeling van opslag media met een steeds grotere capaciteit. Een van de factoren die aanleiding geeft tot grote behoefte aan opslagcapaciteit is het gebruik van graphics. Ter vergelijking, een pagina tekst beslaat ongeveer 2,5 kilobytes terwijl een kleurenbeeld met hoge helderheid 5 megabytes nodig heeft. De ontwikkeling van de magnetische technologie zal leiden tot grotere opslagcapaciteit. Om echter aan de hele hoge capaciteitsbehoefte te kunnen voldoen zal gebruik worden gemaakt van op lasertechniek gebaseerde optische schijven. Een optische schijf met een doorsnede van 12 inch heeft een capaciteit van 1000 megabytes, te vergelijken met de opslag van 400.000 getypte bladzijden of 10 magneetbanden van 6250 bits per inch.

Voordelen
Voordelen van optische schijfeenheden ten opzichte van magnetische schijfeenheden zijn:
- hoge opslagcapaciteit;
- lage kosten per opgeslagen bit;
- de mogelijkheid om de schijf uit de schijfeenheid te halen;
- massadupliceerbaarheid van de schijf, als bij een grammofoonplaat;
- de onuitwisbaarheid.

Door deze eigenschappen zijn optische schijven erg geschikt voor elektronische dossiervorming, data bases in netwerken en beeldverwerkende toepassingen, zoals de opslag van grote hoeveelheden röntgenfoto's.

Verschil en overeenkomst
Er zijn een aantal verschillen en overeenkomsten tussen de magnetische en optische schijven, die tot de conclusie leiden dat beide vormen elkaar zullen aanvullen. Besturing en techniek van de schijfeenheden komen voor beide vormen sterk overeen. Een nadeel is dat de optische schijven (voorlopig) eenmalig beschrijfbaar zijn.

Verder is de toegangstijd van optische schijven veel lager hoewel daar het voordeel van de hoge opslagcapaciteit (minder schijfwisselingen e.d.) tegenover staat. Voordelig verschil is de massadupliceerbaarheid van optische schijven en de mogelijkheid om de schijf uit de eenheid te nemen waardoor archieffunctie en externe opslag mogelijk is. De omgevingseisen, aan die externe opslag te stellen, zullen bovendien minder zwaar zijn. Beide technieken vullen elkaar aan wanneer gegevens tijdelijk worden verzameld op vaste schijf ten behoeve van een snelle verwerking, waarna archivering van het eindprodukt in de vorm van een optische schijf plaatsvindt. Volgens het artikel zal de magneetband worden vervangen door de optische schijf.

Toepassing
Optische schijven zijn ongevoelig voor magnetische velden en niet uitwisbaar. Er zijn toepassingen waar het niet uitwisbaar zijn van gegevens een voordeel is. In financiële toepassingen kan een permanent audit trail zodoende veel beter gewaarborgd blijven. De mogelijkheid om zonder veel kosten een snapshot te maken van data bases biedt belangrijke herstelfaciliteiten voor grote data bases. Een praktische toepassing voor de massa-opslag van read-only-bestanden is bijvoorbeeld "megadoc" van Philips; een installatie die vergelijkbaar is met de bekende juke-box.

Conclusie
De schrijver concludeert dat op korte termijn optische schijven beschikbaar zijn in een write-one, read-many-times vorm. De write-many-times vorm zal tot 1987 op zich laten wachten (de techniek waarmee de optische schijf herschreven kan worden, is overigens inmiddels beschikbaar, zij het nog niet op grote schaal commercieel ingewijd). De eenmalig beschrijfbare optische schijven kunnen mijns inziens als aanvulling op magneetschijven goede diensten bewijzen bij het opslaan van kritische vaste gegevens. Daarnaast lijkt deze techniek een goed alternatief voor het Mass Storage Device.

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

COMPACT

Automatisering
Beveiliging
Controle
NIEUWS

Winter 1984/1985

door J.F.C. van Epen en M.C. Duym

Automatisering

Mutualisme, nieuwe processortechnologie

Dit is een nieuwe automatiseringsterm die door Amdahl wordt gehanteerd om een nieuwe vorm van opsplitsing van de hardware aan te duiden.

Bij de introductie van de 3081- en 3084-computers enkele jaren geleden, gebruikte IBM de term dyadisch om de processoren in deze modellen te typeren. Een dergelijke processor bestaat uit twee geïntegreerde centrale verwerkingseenheden, die onder een enkel besturingssysteem werken. Elke CVE heeft toegang tot een gemeenschappelijk gebruikt deel van het hoofdgeheugen en heeft eigen kanalen.

Bij het door Amdahl toegepaste mutualisme wordt door installatie van de "Multiple Domain Feature" (MDF) op een fysieke processor meerdere logische processoren verkregen. De MDF is een combinatie van hardware, microcode en macrocode.

Op elke logische processor kan een van de volgende besturingssystemen (System Control Programs) worden geïnstalleerd:
- MVS/SP Version 1, Release 3 (MVS/370);
- MVS/SP Version 2, Release 1 (MVS/XA);
- VM/SP HPO Release 3.2 en 3.4.

Door de operator kan aan elk domain, en dus per besturingssysteem, een deel van de capaciteit van het interne geheugen, de arithmetische en logische eenheid en de kanaalbezetting worden toegekend. De prestaties zijn volgens Amdahl op zijn minst 95% van gebruik met één SCP.

Amdahl ziet onder meer de volgende toepassingsgebieden voor dit produkt:
1. Testen. Nieuwe SCP's, hun subsystems (JES, VTAM, etc.) en applicaties kunnen overdag worden getest. SCP- en subsysteem-fouten (en dan natuurlijk ook applicatiefouten) hebben geen invloed op de andere logische processoren.

2. Bedrijfsvoering. Combinatie van verschillende verwerkingsbehoeften in een grote machine, waardoor de overhead-kosten worden gedrukt.
3. Conversie. Vergemakkelijking als gevolg van het parallel kunnen uitvoeren op een installatie.
4. Back-up/stand by voor kritieke toepassingen.

De scheiding tussen de domains wordt gewaarborgd door:
1. hardware-faciliteiten voor het valideren van alle toegangen tot het hoofdgeheugen (fetch en store);
2. het feit, dat een kanaal op een bepaald moment maar aan één domain kan zijn toegewezen.

De MDF zal pas in het tweede kwartaal 1985 voor een bepaald type processor beschikbaar zijn (580 model). Er zullen dan alleen nog 2 domains gecreëerd kunnen worden. Gewerkt wordt aan toepassing voor meerdere types en versies met meer domains.

(Naar aanleiding van een artikel uit Computable van 14 december 1984 en informatie van Amdahl.)

Oppassen met uitvoer van computerartikelen uit Amerika

Het decembernummer van INAD-informatiebulletin maakt melding van het feit, dat voor de uitvoer van computerapparatuur en -programmatuur uit Amerika met een waarde van meer dan $ 1,000 een exportvergunning noodzakelijk is. Dit in verband met mogelijke export naar communistische landen. Bij ontbreken van de vergunning krijgt men een boete van $ 10,000.

Unix, opkomst van een besturingssysteem

Het besturingssysteem Unix, dat al een tweetal decennia in de universitaire wereld veelvuldig wordt gebruikt, dringt langzamerhand ook door in het bedrijfsleven. Dit zowel voor de microcomputers (bijvoorbeeld Xenix voor de IBM PC) als voor de mainframes. Voorboden hiervan zijn:
1. de samenwerkingsovereenkomst die zes grote Europese computerbedrijven hebben gesloten om het ontwikkelen te bevorderen van programmatuur voor computers die onder dit besturingssysteem werken;
2. de aankondiging van IBM, dat het in november 1985 Unix zal gaan voeren voor onder VM werkende apparatuur. Als naam is gekozen IX/370.

De genoemde samenwerkingsovereenkomst is aangegaan door: Philips, Olivetti, Bull, ICL, Nixdorf en Siemens. Uit de gepubliceerde gegevens blijkt niet, of de programmatuur zich richt op de mainframe-, de mini-, de microgebruiker of alle drie.

Gezien de genoemde ontwikkelingen zal Unix op zeer korte termijn de aandacht van de EDP auditors opeisen. Daar er van dit besturingssysteem echter meerdere versies zijn (versie III en V zijn het meest voorkomend) en elke leverancier zijn eigen aanpassingen hierop zal aanbrengen, zal men uiterst voorzichtig moeten zijn met het generaliseren van de uitkomsten van verrichte onderzoeken. Van een volledige standaardisatie zal waarschijnlijk nog geen sprake zijn.

(Naar aanleiding van artikelen in Het Financieele Dagblad d.d. 19 februari 1985 en Computable d.d. 22 februari 1985.)

Remote Support

In de Automatisering Gids van 10 oktober 1984 vonden wij een artikel gewijd aan "onderhoud op afstand", meestal aangeduid met Remote Support of Remote Maintenance.
De titel respectievelijk ondertitel van dit artikel luidt "Wat moet de gebruiker met remote support?", "Reparatie op afstand geeft aanzienlijke besparing".
De bedoelde besparing betreft niet alleen het bedrag dat op reisuren en -kosten van de monteur bespaard kan worden, maar ook de besparing die wordt bereikt door de kortere stilstand van de computer. Enkele opmerkelijke feiten worden in het betreffende artikel genoemd; reden voor ons om dit onderwerp eens bij de kop te nemen.
"Bij twintig bedrijven in de Verenigde Staten van Amerika is gedurende een aantal maanden nauwkeurig bijgehouden waarop storingsmeldingen betrekking hadden, waar de oorzaken van de storingen lagen en in hoeverre deze storingen via remote support opgeheven hadden kunnen worden.
De hieruit resulterende statistiek luidt:

5% was zelf-corrigerend;
25% was terug te voeren op operators-handelingen;
45% vond zijn oorzaak in de systeem-software;
25% kon door de operator worden gerepareerd of afgesteld.

Hoewel het een relatief gering aantal bedrijven betreft toch opmerkelijke cijfers. Vooral het relatief grote aantal storingen dat door de systeem-software werd veroorzaakt."

Alle genoemde oorzaken zouden door middel van een remote support facility vastgesteld en deels verholpen kunnen zijn. Voor het andere deel hadden aan de operator instructies gegeven kunnen worden, waarmee hij de storing kon opheffen.

Een pleidooi derhalve voor remote support.
Ook wordt gesteld dat leveranciers veelal voorstanders zijn van deze faciliteit: "technici zijn schaars, elke storing vraagt om directe oplossing en een goede remote support geeft commerciële en financiële voordelen".
Enkele alinea's verder worden in het artikel nog een aantal voordelen opgesomd. Wij citeren:
"De huidige mogelijkheden geven de support specialist de gelegenheid de gebruiker te assisteren bij het opstarten van zijn systeem. Een analyse kan worden gemaakt van de maintenance-log, waarbij kan worden bepaald of de apparatuur nog aan de gestelde normen voldoet."
"Een analyse kan worden gemaakt van het systeemgeheugen om vermeende systeem-software- of -hardware-fouten te kunnen localiseren. Ook de applicatieprogramma's kunnen aan een kritische analyse worden onderworpen door memory dumps te maken. Deze dumps kunnen naar het Support Centrum worden overgezonden, zodat aldaar de specialisten zich kunnen buigen over de problematiek."
Deze beide citaten geven ons aanleiding om een kritische vraag te stellen, namelijk:

Welke risico's zijn verbonden aan remote support?

Het Support Centrum heeft via de lijn op het hoogste niveau toegang tot de computer van de gebruiker, inclusief de programmatuur en de bestanden. Dit wil zeggen dat derden (niet tot de eigen organisatie behorende) technici in principe kennis kunnen nemen van de knowhow van hun cliënten.
Tenzij er bij de gebruikers maatregelen en procedures zijn die voorkomen dat de computerleverancier ongevraagd het systeem "binnenkomt" en regelen dat hij alleen kennis kan nemen van die gegevens, die de gebruiker hem toestaat.
Remote support lijkt ons dan een goede methode die ongetwijfeld positieve invloed heeft op het reduceren van de down-tijd van de computerinstallatie. De voordelen spreken vooral in een on-líne-omgeving!
Tenslotte geven wij nog enige attentiepunten voor het realiseren van een "veilige" remote support facility.

1. Het initiatief tot het tot stand brengen van de verbinding met het Support Centrum dient bij het gebruikerscentrum te liggen.
2. Het management dient toestemming te geven voor het tot stand brengen van de verbinding.
3. Voorkomen dient te worden dat onbevoegden toegang tot het computersysteem krijgen, bijvoorbeeld door middel van password-controle.
4. Ontkoppel zoveel mogelijk programmabibliotheken en bestanden.

5. Leg alle maintenance-activiteiten vast in een logboek, met vermelding van bijvoorbeeld:
   - datum en tijdstip van het verzoek;
   - reden;
   - initiatiefnemer;
   - begin en einde van de maintenance;
   - goedkeuring van het management.
6. Controleer machinelog.
7. Voer een machineherstart uit met de eigen parameters en - zo mogelijk - met de langs reguliere weg ontvangen programma's.

Het papierloze kantoor

Als de gegevens in een door Océ Office Automation opgesteld rapport juist blijken te zijn, kan de accountant zeker nog tot 1995 volop zijn vinken op originelen of duplicaten en kopieën daarvan zetten. Pas dan verwacht men dat beeldscherminformatie, rechtstreeks of indirect via afdrukken, gaat doorbreken.

Beveiliging

Onderzoek naar computermisbruik in Australië

In EDPACS van augustus 1984 is een artikel opgenomen van K.J. Fitzgerald getiteld "Computer-Related Crime in Australia". Het betreft een analyse van een 123 gevallen van computermisbruik in Australië. De informatie over de misdaden was voor het grootste deel afkomstig van het Computer Abuse Research Bureau van het Chishol Institute of Technology (CIT-CARB), waarvan de auteur directeur is.

De gevallen waarover wordt gerapporteerd vallen onder de volgende definitie:
Diefstal, fraude, of schade in relatie met computer inclusief:
- ongeautoriseerd gebruiken van computer-in- en/of -uitvoer;
- ongeautoriseerd verkrijgen van toegang tot de computer via beeldschermeenheden;
- ongeautoriseerd wijzigen of gebruiken van computerprogramma's;
- inbraak in een computercentrum en/of diefstal van apparatuur, bestanden of uitvoer;
- sabotage van computerapparatuur;
- ongeautoriseerd onderscheppen van gegevens.

In 65 van de 123 gevallen was de schade vast te stellen en bedroeg gemiddeld $ 86,800 (gevallen vanaf 1975). Het meeste kwamen fraude, ongeautoriseerd gebruik en diefstal van uitvoer voor (respectievelijk 50, 25, en 9 procent van alle gevallen).
De gemiddelde schade per geval was veruit het hoogst voor de fraudecategorie ($ 114,000 ten opzichte van respectievelijk $ 500 en $ 3,000). Van de 7 sabotagegevallen was er maar van één de schade vast te stellen ($ 900,000). Het is aan te nemen, dat in deze categorie de gemiddelde schade hoger ligt dan bij fraude.
Naast een rangschikking naar type misbruik worden in het artikel ook nog tabellen gegeven waarbij een rangschikking heeft plaatsgevonden naar:
1. gebruikte technieken (invoer, installatie, verwerking, uitvoer georiënteerd);
2. misbruikers (automatiseringspersoneel, gebruiker, buitenstaander);
3. functieniveau misbruikers;
4. branche.

Van de bovengenoemde tabellen is die met betrekking tot het functieniveau overbodig, omdat dit van de helft van de gevallen onbekend was. Ook tabel vier lijkt moeilijk te interpreteren, daar geen nadere informatie wordt gegeven over de omvang van de computeractiviteiten per branche en de mogelijke wettelijke en verzekeringtechnische consequenties van wel of niet rapporteren. (Zo lijken state en federal government sterk oververtegenwoordigd.)

"Voorzichtige conclusies" die getrokken kunnen worden uit de gegevens van de andere tabellen zijn:

1. In de gerapporteerde gevallen werd vooral gebruik gemaakt van technieken gericht op het invoertraject en installatie. Hierbij wordt aangetekend dat in de overige twee categorieën de kans op ontdekking en/of rapportering waarschijnlijk geringer is;
2. Automatiseringspersoneel en gebruiker de grootste misbruikerscategorie zijn, waarbij de gemiddelde schade voor de laatstgenoemde categorie meer dan vijf keer zo hoog ligt als voor de eerstgenoemde.

Enkele vermeldenswaardige opmerkingen die in het artikel worden gemaakt, zijn:

- de gelegenheid tot computermisbruik zal snel toenemen als gevolg van het snel verspreidende computergebruik. (Opmerking: hierbij moet naar onze mening vooral gedacht worden aan de nieuwe generaties schoolverlaters, die allen in meer of mindere mate kunnen programmeren. Hierdoor zal deze generatie beter in staat zijn de structuur van de verwerking te begrijpen.);
- "business crime becomes computer crime";
- verdere betrokkenheid van georganiseerde misdaad evenals terrorisme is een logisch gevolg van de inherente zwakte van veel geautomatiseerde gegevensverwerking (snelle toegang en/of manipulatie van grote volumes op centrale plaats);
- de tendens is dat een stijging plaatsvindt in misbruik door management en hogere employees voor hoge bedragen;
- het management moet niet alleen maar aandacht hebben voor informatieproduktie, maar ook voor de daarbij behorende controle.

Beeldscherm op afstand afleesbaar

Het Dr. Neher-laboratorium van de PTT heeft via de pers bekend gemaakt dat de straling die uitgaat van beeldschermen kan reiken tot in het UHF-gebied en daarmede in principe met "gewone" TV-toestellen is op te vangen.
In de Telegraaf (9 februari 1985) lazen wij de kop:

Beeldscherm door muur afleesbaar

Dit artikel citeert een woordvoerder van de Centrale Directie van de PTT: "... een van de simpelste en daardoor juist meest onderschatte manieren om informatie uit een computer te stelen".
Het Financieele Dagblad presenteerde het nieuws (op 12 februari 1985) aldus:

TV-toestel kan tot op kilometers afstand computerterminal "afkijken"

Een citaat uit dit artikel: "Computergebruikers die met hoogst geheime informatie werken (zoals in militaire kringen), zijn zich al geruime tijd bewust van de "afkijk"-mogelijkheid. Hun computerterminals schijnen hier al tegen beschermd te worden. Maar daarbuiten lijkt lang niet iedereen zich van dit risico voor openbaarmaking van geheime, vertrouwelijke of gevoelige gegevens bewust. Volgens een woordvoerder van Digital Equipment in Utrecht gaat het hier wel om een in "automatiseringskringen" algemeen bekend verschijnsel."
Het betreffende artikel vermeldt voorts dat er wel degelijk methoden zijn om straling te voorkomen en dat deze ook worden toegepast. Deze variëren van voorzieningen in de terminal tot het plaatsen van de terminal in een zogenaamde "kooi van Faraday", een metalen kast of kooi waar de elektromagnetische straling niet doorheen dringt.

Reeds op 15 februari 1985 komt Het Financieele Dagblad in zijn rubriek COMPUTER AUTOMATISERING met het artikel:

PTT ontwikkelt beeldlijnenklusters tegen het ongewenst afkijken van computerterminals

Dit artikel gaat verder in op de "afkijk"-problematiek. Het stelt dat het risico bij deskundigen zeer wel bekend was en dat er ook maatregelen tegen bestaan, maar dat de argeloze gebruiker van beeldscherminformatie, die in bepaalde gevallen een vertrouwelijk karakter kan hebben, het niet wist.
Thans is, mede door de ruime ruchtbaarheid die er via de pers aan is gegeven, bekend geworden dat de PTT voor verontruste computergebruikers een relatief goedkope oplossing heeft ontwikkeld: een soort "beeldlijnenkluster". Hierdoor wordt niet de straling op zich tegengehouden, maar wel de leesbaarheid van de informatie voorkomen.
Het artikel geeft voorts nog een technische uitleg over "hoe het kan" en "hoe het kan worden voorkomen". Geïnteresseerden verwijzen wij derhalve naar het betreffende artikel.

Beveiliging van gegevens in een personal computer

In het tweede nummer van het tijdschrift PC+ vernemen wij een mededeling over het op de markt komen van een cryptografisch programma voor de personal computer. Bij de opmars van het gebruik van PC's op velerlei plaatsen en door functionarissen van diverse niveaus is het goed te weten dat een dergelijk produkt bestaat. Het programma heet P/C Privacy. Het bestaat uit een tweetal programma's - aldus PC+ - ENCRYPT en DECRYPT geheten. De programma's kunnen op een schijf met een tekstverwerkings- of ander toepassingsprogramma worden gekopieerd. Om een bestand te versleutelen moet na de "systeemprompt" ENCRYPT worden ingetikt. Het programma vraagt dan de bestandsnaam enz. Tevens wordt gevraagd naar de sleutelcode.
Volgens een (Amerikaanse) test duurt het versleutelen van een bestand van 28K 90 seconden. Het bestand "groeit" hierdoor tot 43K. Het ontcijferen van de 43K duurt 114 seconden.

Voor de argeloze gebruiker: Vergeet de sleutelcode niet!

Password security systems

Dit is de titel van een hoofdartikel in het Amerikaanse tijdschrift EDPACS (The EDP Audit Control and Security Newsletter). Het stelt dat password-beveiliging de meest gebruikte niet-fysieke beveiligingsmethode is. Populair omdat het zo'n goedkope methode is.
Helaas geven dergelijke systemen niet steeds de bescherming die er door wordt gesuggereerd. Wij citeren:
"Unfortunately, many password systems provide inadequate barriers to unauthorized computer access. Common deficiencies include:

- Departmental passwords. All members of a department share the same password.
- Lack of scheduled password changes. Password may be used for years.
- Divulged passwords. Although each person has an individual password, some passwords are known by other staff members.
- Meaningful passwords. When individuals are permitted to choose their own passwords, they often select their spouse's or children's names, residential street names, telephone numbers, social security numbers, initials or birth dates. While easy to remember, such passwords are easily compromised.
- Failure to report invalid password attempts. Unless otherwise programmed, a computer will ignore invalid passwords and wait for the entry of a valid password. In this situation, someone can break the password protection scheme by entering character strings until one of them works.

Hiermede zijn de voornaamste gebreken van password-systemen aangegeven. Het genoemde artikel beschrijft verder wat een organisatie te doen staat als zij een correct werkend systeem wenst of een bestaand systeem wenst te verbeteren. Gezien de uitgebreidheid van de behandeling verwijzen wij de geïnteresseerde lezer naar dat artikel. Om een indruk te geven, krijgt u van ons de titels van de paragrafen van het artikel:

- PRE-IMPLEMENTATION DECISIONS
- PASSWORD FORMAT (Numeric, alphabetical, alphanumeric or full keyboard characters)
- RANDOM PASSWORDS SELECTION
- RANDOM CHARACTERS SELECTION
- BOOK KEYED CODES
- IMPLEMENTING A PASSWORD SYSTEM
- PASSWORD SYSTEM MAINTENANCE
- CONCLUSION

De laatste zinnen van de samenvatting van het artikel willen wij u niet onthouden:
"The capabilities of (potential) computer criminals increase. A static security system, no matter how adequate it is today, will be obsolete in the future. A well-designed and maintained password system will provide an effective and relatively low-cost crime deterrent now and in years to come."

Controle

"Beoordeling van de Administratieve Organisatie (in een geautomatiseerde kleinschalige omgeving)" is de titel van een artikel in de rubriek Accountant en automatisering in De Accountant van november 1984 van de hand van drs. A. Eijkenaar.
Schrijver signaleert dat de accountant, indien hij de beoordeling van de automatiseringsomgeving noodzakelijk acht als onderdeel van de beoordeling van de administratieve organisatie, hij in een grootschalige omgeving vaak gebruik maakt van een specialist (EDP auditor), doch dat dit in een kleinschalige omgeving om redenen van efficiency niet steeds mogelijk is.
Met de opkomst van de - relatief goedkope en aan zijn omgeving weinig eisen stellende - zakelijke microcomputer is een zo hoge graad van automatisering bereikt dat in vrijwel elke organisatie sprake is van administratieve automatisering. Dergelijke "kleine" computers zijn vaak in staat om via beeldscherm-terminals door meerdere gebruikers tegelijk te worden benut.
Meestal is slechts één persoon belast met de bediening, terwijl een tweede beschikbaar is om redenen van continuïteit.
Met behulp van een kleine configuratie worden administratieve toepassingen gerealiseerd die variëren van een groepsgewijze verwerking van handmatig ingevoerde journaalposten tot het direct in het voorraadbestand verwerken van mutaties in de goederenvoorraad. Met andere woorden: een veelheid van administratieve toepassingen die elk in hun eigen situatie uniek zijn.
Tot zover enkele (samengevatte) inleidende alinea's van het aangehaalde artikel.

Aan de hand van een voorbeeld (geautomatiseerd goederensysteem) behandelt de schrijver een aanpak ter zake van de beoordeling van de administratieve organisatie in een omgeving zoals geschetst. Althans voor zover deze afwijkt van die in een middelgrote of grote omgeving.
Onderscheiden wordt een drietal fasen:
1. het formuleren van de controledoeleinden;
2. het verkrijgen van inzicht in de administratieve en interne organisatie;
3. de beoordeling van de AO (evaluatie).

Op fase 1 wordt niet verder ingegaan. Deze hangt af van de typologie van de huishouding en is niet zozeer afhankelijk van de aard van de automatisering.
Op fase 2, het verkrijgen van inzicht, wordt in het artikel meer uitvoerig aandacht besteed. Een probleem voor de externe beoordelaar is het veelal ontbreken van kant en klare beschrijvingen op basis waarvan het vereiste inzicht kan worden verkregen.

De schrijver noemt een aantal mogelijke bronnen, waaraan informatie ontleend zou kunnen worden:

a. systeemontwerp;
b. gebruikersinstructies;
c. bestandsspecificaties;
d. computeruitvoer;
e. beheersinstructies;
f. libraries (bibliotheken van programma's en eventuele bestanden);
g. "cradle to grave"-test (een steekproef waarbij bepaalde verwerkingen van hun initiëring tot en met de definitieve uitvoer worden gevolgd door gebruikersorganisatie en automatisering heen; geeft inzicht in de "transactiestroom";
h. interview.

Met betrekking tot deze laatstgenoemde techniek wijst de schrijver erop het interview met terughoudendheid toe te passen, omdat hij deze als tijdsintensief beschouwt, waarbij naast de tijd van de accountant ook beslag gelegd wordt op de tijd van functionarissen binnen de huishouding.

Commentaar

Op grond van eigen ervaringen hebben wij kritiek op deze zo stellig geschreven bewering. Een interview gaat doorgaans veel sneller dan het bestuderen van - vaak moeilijk toegankelijke en onvolledige - documentatie. Met behulp van enkele andere hulpmiddelen, zoals een hoofdstroomschema, afdrukken van de keuzemenu's, de invoerverslagen en de computeruitvoer kan vrij efficiënt een beeld van de structuur van het programmapakket worden verkregen. Daaruit kunnen dan de maatregelen van interne controle afgeleid worden die het pakket minimaal zou moeten bieden, waarna vastgesteld kan worden of in het pakket aan de geformuleerde minimale eisen is voldaan.

(Deze laatstgenoemde aanpak is gebaseerd op de methode zoals die door KKC in de CASA-cursus wordt onderwezen. Zie rubriek Onderwijs in dit Compactnummer.)

Het aangehaalde artikel behandelt vervolgens de noodzaak tot vastlegging van het waargenomene, enerzijds ten behoeve van de beoordeling, anderzijds voor de reguliere dossiervorming.

Vervolgens wordt fase 3, de beoordeling van de interne controle, onder de loupe genomen. Hier wordt gewezen op een aantal specifieke omstandigheden zoals die zich kunnen voordoen in een kleinschalige omgeving met automatisering:

1. De systeembeheerder heeft mogelijkheden tot het wijzigen in bestanden buiten de gebruikers om.
2. Het systeem van toegangsbeveiliging functioneert slecht (of ontbreekt geheel; toevoeging redactie).

3. Risico's ten aanzien van de continuïteit van de geautomatiseerde administratieve verwerking zijn aanwezig.
4. De accountant zal problemen kunnen ondervinden bij het vaststellen van de voortdurend juiste werking van diverse interne controles.

Genoemde omstandigheden worden door de schrijver nader becommentarieerd. Wij verwijzen hiervoor naar het betreffende artikel. Aan het daar opgenomen commentaar en adviezen zouden wij nog het volgende willen toevoegen:

Ad 1. Gebruikers die toegang hebben tot de systeem-software (besturingssysteem, utilities en dergelijke) zijn even "gevaarlijk" als de systeembeheerder. Organisatorisch is het vrij moeilijk af te schermen, aangezien functionarissen ook privé over de betreffende software kunnen beschikken.

Ad 2. Het toepassen van zogenaamde "menu-security" is - indien de mogelijkheid daartoe aanwezig is - een goed middel om gebruikers te beperken tot die functies waartoe zij functioneel gerechtigd zijn. Menu-security wil zeggen dat de gebruiker alleen die functies kan uitvoeren die in "zijn" menu voorkomen. Hij krijgt toegang tot zijn menu via een geldig password (zie ook in deze rubriek onder Beveiliging).

In zijn slotwoord wijst de heer Eijkenaar op de VERA-cursus Kleinschalige Automatisering, die van nut kan zijn voor de met betrekking tot geautomatiseerde administraties onervaren accountant. Wij voegen hieraan toe dat deze, binnen KKC ontwikkelde cursus ook in ons cursuspakket voorkomt.

Een op maat gesneden geautomatiseerd controleprogramma

Bovenstaande is een vertaling van de titel boven een stukje uit de rubriek "Practitioners forum" in het "Journal of Accountancy" van november 1984.

Beschreven wordt hoe uit een in de computer opgeslagen standaard controleprogramma een voor een bepaalde cliënt op maat gesneden controleprogramma kan worden verkregen.

De accountant geeft op welke onderdelen hij van het standaard controleprogramma in het controleprogramma van een bepaalde cliënt wil hebben. Enkele onderdelen zal hij hierbij nooit kunnen overslaan.
De geselecteerde paragrafen worden her ummerd en als een nieuw controleprogramma afgedrukt. De ingetypte selectiecriteria kunnen voor een volgende keer worden bewaard, zodat hernieuwd opgeven overbodig wordt en wijzigingen makkelijk aangebracht kunnen worden.

Alhoewel automatiseringstechnisch deze toepassing alleen als "veredelde tekstverwerking" is te classificeren, zal het duidelijk zijn dat de moeilijkheid bij het opstellen van het standaard controleprogramma ligt. Is dit niet veelzijdig genoeg, dan zal voor veel controles toch weer een eigen programma worden geschreven waardoor de voordelen, te weten:
- meer uniformiteit;
- minder tijd nodig voor opstellen;
- minder kans op vergeten van punten

teniet worden gedaan.

Toename in uitbesteding/overname automatiseringsactiviteiten

Voor wat betreft het overnemen van de automatiseringsactiviteiten van grotere bedrijven door software-houses, doet zich een zelfde tendens voor als die ten aanzien van de overname van (delen van) interne accountantsdiensten door externe accountantskantoren.

Voorbeelden zijn:
- IMDATA (automatiseringsdochter Internatio-Muller) door RAET;
- UDEMA (dochter SHV) door RAET;
- RSV Data door EDS;
- SVZ (Scheepvaart Vereniging Zuid) door CMG;
- Goudse Verzekeringen door ORDA-B.

Tot de redenen om tot deze stap te besluiten, behoren:
- de te verwachten tendens naar geautomatiseerde gegevensverwerking door de eindgebruiker met behulp van een microcomputer, die eventueel aan de centrale computer is aangesloten;
- de moeilijkheid om voldoende gekwalificeerd personeel te krijgen gecombineerd met de schaarste daaraan. Zelfs bij een middelgroot computercentrum (IBM 43XX omvang) is de omvang van de automatiseringsafdeling veelal te klein om voldoende carrièrekansen te bieden voor hoger geschoold automatiseringspersoneel. Gevolg: er wordt zelf personeel opgeleid, dat vervolgens vertrekt;
- de relatief hoge overhead-kosten welke gepaard gaan met het bijblijven op hard- en software-gebied.

Echter, in hoeverre deze overgang een blijvend karakter heeft, blijft de vraag. Bij veel van de genoemde bedrijven is er al weer een tendens merkbaar tot het, op beperkte schaal, in eigen beheer nemen van de automatiseringsactiviteiten.

Voor de accountant betekent deze ontwikkeling, die in principe een versterking van de interne controle inhoudt, dat hij onder meer zijn werkzaamheden dient te richten op:
- beoordeling van de inhoud van de contracten, speciale aandacht voor het aspect continuïteit;
- beoordeling van de sterkte van de in- en uitvoercontroles om daaruit conclusies te kunnen trekken met betrekking tot de volledige en juiste verwerking van de gegevens.

Verder wordt verwezen naar NIVRA-geschrift 16, "Accountant en computerservicebureaus" dat uitvoerig op de genoemde gevolgen voor de accountantscontrole ingaat.
De noodzaak van een third party review kan in deze gevallen oppportuun worden. In NIVRA-geschrift 26 "Mededelingen door de accountant met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking" wordt ingegaan op de problematiek van onderzoek en rapportering over de betrouwbaarheid en continuïteit van automatiseringsorganisaties en geautomatiseerde delen van informatiesystemen.

International Symposium on Auditing in an advanced complex computerized environment

Onder deze titel is van 10 tot en met 12 september 1984 in Amsterdam door het NIVRA een symposium georganiseerd. In De Accountant van december 1984 is hiervan een verslag gepubliceerd.
Aangezien het hier reeds een samenvatting betreft willen wij een en ander niet nogmaals samenvatten. Wij zullen volstaan met het noemen van de lezingen met namen van sprekers die aan het betreffende verslag zijn ontleend (blz. 248 e.v.):
1. Het aandeel van de EDP-auditor in de ontwikkeling van gedistribueerde systemen.
   Spreker: James H. David, USA.
2. Risico-analyse in een geautomatiseerde omgeving.
   Spreker: Eric Guldentops, België.
3. Beveiliging en beoordeling van besturingssystemen.
   Spreker: Herman Roos, Nederland.
4. Gedistribueerde data-bases: de gevolgen voor de interne controle en de benadering door de accountant.
   Spreker: Hans Leenaars, Nederland.
5. Elektronisch betalingsverkeer: interne controle en accountantsaspecten.
   Spreker: Michel Leger, Frankrijk.
6. Gebruik van microcomputers in de accountantscontrole.
   Spreker: William C. Mair, USA.

7. IFAC.
   Spreker: Luc van Zutphen, Nederland.
8. De gevolgen van het gebruik van vierde generatietalen voor de controle.
   Spreker: Nick Pasricha, UK.
9. De controlebenadering: systeem- of transactie-georiënteerd.
   Spreker: Rod C.L. Perry, UK.

Conclusie van de schrijvers van het verslag:
"De organisatoren zijn erin geslaagd om de diverse aspecten van controle in geavanceerde, complexe geautomatiseerde omgevingen goed en volledig aan de orde te laten komen. Duidelijk is gebleken dat het niveau van EDP-auditing in Nederland vergelijkbaar is met dat in de UK en de Verenigde Staten." ...
"De ontwikkelingen staan niet stil. De micro is in opmars en zal ook het "leven" van de accountant gaan beïnvloeden. De EDP auditors kunnen hierin een belangrijke rol vervullen. Het symposium is voor herhaling vatbaar, bijvoorbeeld eenmaal in de twee jaar. Accountancy en ook EDP audit tenslotte wordt meer en meer een internationale zaak, waarbij blijkt dat Nederlandse accountants een inbreng hebben te leveren die ook voor collega's in het buitenland van belang is."

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

ONDERWIJS

Seminar Managing and Controlling the IBM System/38 (2½ dag)

Door de AC-kern is in samenwerking met KKC/Organisatie-adviseurs een seminar ontwikkeld met als titel "Managing and Controlling the IBM System/38". Het seminar kan in de Nederlandse of in de Engelse taal gegeven worden. Seminar-documentatie is in het Engels.
"Keywords" van het seminar zijn: control, audit en productivity.
Het seminar is bedoeld voor EDP managers en EDP auditors.

Een eerste seminar zal onder auspiciën van IBM worden gegeven in Helsinki in april a.s. Voorts staat een KMG-intern seminar gepland voor eind mei a.s. (USA).
Verdere seminars zullen eerst na de zomer van 1985 kunnen worden gegeven. Vanzelfsprekend staat ook Nederland hierbij op de lijst.

Voor nadere inlichtingen kunt u zich wenden tot de secretaris van de redactie.

Aan de seminar-brochure worden de volgende (Engelse) beschrijvingen ontleend.

OBJECTIVE: This seminar enables delegates to tailor the System/38 environment to their specific needs to give the highest possible control, security and productivity. Models of supporting tools will be provided.

DESIGNED FOR: DP-management and systems, design- and programming-staff responsible for developing applications in an IBM System/38 environment, as well as EDP auditors.

CONTENTS

1. Organizational Framework

This session covers the conceptual business organization, based upon controllability concepts. The model includes functions as data (base), development, systems, end-user, facilities and security management. The model will be used in later sessions, where the confrontation of System/38 features with the model will be discussed.

2. Technical Environment

In this session the control and security concepts (such as: object philosophy, control and security structure, unified Control Language) of the System/38 will be discussed.

3. Control and Security Policy and Standards

This session covers the process of mapping the technical environment onto the conceptual EDP and business functions. This results in: a global library and object organization; allocation of objects to libraries, and organizational functions; an identification of efficiency and security constraints.

4. Compliance Testing

This session introduces ideas and suggestions of management's task and possible EDP auditor activities to establish compliance with the developed procedures. Software options will be identified and evaluated on effectiveness and efficiency.
Models of supporting aids will be discussed.

5. Productivity Defined

Productivity is often discussed in terms of workload balancing and tuning. Although performance may be a substantial part of productivity problems, there are several other factors which may affect the productivity of a System/38 site, dramatically. In this session those factors will be put in perspective of the total computer environments' organization.

6. Understanding System/38

In designing "performance friendly" applications, as well as in creating an optimal production environment, it is essential to have a more elaborate knowledge of the internal structure and ways of operating of the System/38. This session will cover the subjects CPF-structure, Storage management, Process management, Data and Data base management.

7. Organizing the Operational Environment

The arrangement of the System/38 environment in terms of libraries, subsystems, authorizations, etc., should be adapted to the specific needs of the workload structure (existing as well as future), the EDP departments' organization and the end-users. As needs will change in time, so should the environment change accordingly. In spite of the potentialities of System/38, necessary procedures have not always been implemented and/or adhered to, mainly caused by their static nature. This session covers the possibilities of using System/38 options in organizing the operational environment, application development, data base administration and security management.

8. Optimal Design

As many sites have been migrating from a System/3 or System/34 to a System/38, EDP staff often is insufficiently familiar with the specific possiblilities and constraints of the System/38, in terms of data base and application design, and user friendliness. This session hands some of the do's and don'ts in designing applications and data bases.

9. Performance Control

Staying within the limits of an optimal performance, demands a regular control of the workload on your System/38.
Control requires information and one of the problems is to achieve the right level:

- too little information, and actions and future plans will of necessity be based upon intuition rather than on fact;
- too much information, and the essential will be hidden by the irrelevant.

This session covers the organization for adequate performance control, interactive performance measurement, simple and sophisticated tools as an aid in controlling, as well as various ways to adjust to dynamically changing workloads.

(10. Delegates' Problems) (Optional; last half day)

(This part of the seminar will be dedicated to problems as posed by the delegates, and the ways they could be dealt with. As a matter of course, the problems must be within the scope of this seminar.)

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

Cursussen 85-86
Nieuwe brochure.

INLEIDING

Programma

Als accountantskantoor met een breed geschakeerde cliëntenkring komen wij in aanraking met allerlei bedrijven en instellingen. Cliënt zijn zowel ondernemingen in de industrie, de handel en het transportwezen alsook dienstverlenende bedrijven, non-profit organisaties en overheidslichamen.
Hieronder zijn starters, groeiers en sinds jaren gevestigde ondernemingen. Onze werkzaamheden omvatten zowel controle van jaarrekeningen als het adviseren op bedrijfseconomisch, organisatorisch, administratief en fiscaal terrein.
In onze dagelijkse praktijk onderkennen wij vaak een behoefte aan cursussen die inzicht geven in de bedrijfsproblematiek en hoe daar mee om te gaan. Met ons cursusprogramma spelen wij op deze behoefte in.

De cursussen worden gegeven door in de praktijk werkende accountants en adviseurs, waardoor een gerichte overdracht van kennis, maar vooral ook van praktische ervaring wordt bereikt.
Na afloop ontvangen de cursisten een certificaat van deelneming.
De in deze brochure vermelde cursussen zijn als volgt in te delen:

Open cursussen

De open cursussen worden in de loop van 1985 en de eerste helft van 1986 gegeven. Een volledig overzicht van deze cursussen vindt u op blz. 7, 8, 9 en 10.

Voor de open cursussen kan door een of meer individuele deelnemers uit één organisatie worden ingeschreven. Hiervoor kan gebruik worden gemaakt van de aanmeldingsformulieren die u achter in deze brochure vindt.

Maatcursussen

Dit zijn cursussen die naar behoefte van de instelling of onderneming kunnen worden ontwikkeld, afgestemd op de specifieke situatie. Deze bedrijfsgerichte trainingen kunnen zowel in een conferentie-oord als in het bedrijf zelf worden gegeven op in onderling overleg overeen te komen data.

Nadere gegevens of inlichtingen ontvangt u van
Klynveld Kraayenhof & Co.
Bureau Opleidingen
Antwoordnummer 17414
1000 SN Amsterdam
Tel. 020 - 5461243
waar u kunt vragen naar Pien Schepel.

Programma open cursussen

Inleiding Administratieve Organisatie
De cursus is gericht op het leren beheersen van verschillende structuren en processen binnen een organisatie d.m.v. een systeem van informatieverzorging en controle.

Cursusduur 5 dagen
Data 18 t/m 22 maart 1985
30 september t/m 4 oktober 1985
Prijs f. 2.775,-

Inleiding Controleleer
De cursus geeft de hoofdlijnen van de controleleer, aangevuld met groepsgewijze behandeling van vraagstukken en problemen.

Cursusduur 5 dagen
Data 3 t/m 7 juni 1985
28 oktober t/m 1 november 1985
Prijs f. 2.775,-

Personal Computers
De cursus is erop gericht de cursist met een Personal Computer te leren werken met behulp van de pakketten Multiplan en DBase.

Cursusduur 2 dagen (inleiding en Multiplan)
3 dagen (inleiding, Multiplan en DBase)
Data in overleg
Prijs f. 800,- c.q. f 1.200,-

Kleinschalige automatisering
Verschaft inzicht in de aanpak van automatisering in het midden- en kleinbedrijf, bedoeld voor leidinggevende functionarissen, belast met het nemen van beslissingen inzake automatisering.

Cursusduur 3 dagen
Data 3 t/m 5 juni 1985
28 t/m 30 oktober 1985
Prijs f. 1.605,-

Workshop Samenwerken in Automatiseringsprojecten
Samenwerking tussen deskundigen en managers maakt het nodig dat er één taal gesproken wordt. Deze cursus wordt gegeven in samenwerking met RAET-opleidingen en vormt de basis voor deze communicatie.

Cursusduur 3 dagen
Data 8 t/m 10 mei 1985
en najaar 1985
Prijs f. 1.975.-

PRISMA
De PRISMA-methode kan worden gebruikt voor het opstellen van een informatieplan en het ontwikkelen van een functionele specificatie.

Cursusduur Deel 1: 2 dagen
Deel 2: 2 dagen
Data Deel 1: 22 en 23 april 1985 en
21 en 22 oktober 1985
Deel 2: 6 en 7 mei 1985 en
4 en 5 november 1985
Prijs Deel 1 f. 1.070,-
Deel 2 f. 1.070,-

Het managen van datacenters
Deze cursus wordt gegeven in samenwerking met RAET-opleidingen en is met name bestemd voor managers van rekencentra en aanverwante afdelingen.

Cursusduur 3 dagen
Data 8 t/m 10 mei 1985
en najaar 1985
Prijs f. 495,- per dag

Computer Controls
In werkgroepen en plenaire besprekingen worden de cursisten vertrouwd gemaakt met controle op het gebied van de automatiseringsorganisatie en geautomatiseerde informatiesystemen.

Cursusduur 4 dagen
Data 16 t/m 19 september 1985
Prijs f. 2.140,-

Aanpak Systeembeoordeling en Accountantscontrole (CASA)
Beoordelen van de interne controlemaatregelen in een geautomatiseerd informatiesysteem (5 dagen), gevolgd door de aanpak van de accountantscontrole (2 dagen).

Cursusduur 5 dagen (blok A en B) of
7 dagen (blok A, B en C)
Data 15 t/m 19 april1985 (Blok A en B) en
22 en 23 april 1985 (Blok C)
30 september t/m 4 oktober 1985 (Blok A en B)
7 en 8 oktober 1985 (Blok C)
Prijs f. 2.775,- (Blok A en B)
f. 3.745,- (Blok A, B en C)

Controle bij Geïntegreerde Gegevensverwerking (GGV)
Vertrouwd raken met de interne controleproblematiek in een on-line geïntegreerd gegevensmodel.

Cursusduur 5 dagen
Data 21 t/m 25 oktober 1985
9 t/m 13 december 1985
Prijs f. 2.775,-

Kleinschalige automatisering
Verschaft inzicht in de aanpak van automatisering in het midden- en kleinbedrijf alsmede in de opzet van het controleplan van de accountant.

Cursusduur 3 dagen
Data 11 t/m 13 november 1985
Prijs f. 1.605,-

Management
Het ontwikkelen van een eigen management-conceptie. Dat wil zeggen een op zichzelf consistent denkbeeld over doel, rol en techniek van management.

Cursusduur 5 dagen
Data 6 t/m 10 mei 1985
4 t/m 8 november 1985
Prijs f. 4.400,- (incl. kosten van het verblijf in het conferentie-oord, excl. BTW)

Organisatie-analyse en vastleggingstechnieken
De cursus is gericht op het overbrengen van een methodische aanpak voor het tot stand brengen van organisatiebeschrijvingen en op het kennis maken met toepassingsmogelijkheden van vastleggingstechnieken. Uitgangspunt van de methodiek is om door middel van organisatiebeschrijvingen bij te dragen tot een betere beheersing van de organisatie.

Cursusduur 2 dagen
Data 23 en 24 april 1985
en najaar 1985
Prijs f. 1.070,-

Pensioenen
Het overdragen van zoveel kennis, dat men in staat is zelf de weg te vinden bij de raadpleging van externe deskundigen en de gegeven adviezen op hun toepasbaarheid kritisch te kunnen beoordelen.

Cursusduur 3 of 4 dagen
Data 18 t/m 21 november 1985
Prijs f. 1.605,- resp. f. 2.140,-

Alle vermelde prijzen zijn excl. BTW. De kosten van maaltijden en verblijf zijn niet in de prijzen begrepen (zie reserveringsvoorwaarden op blz. 65 van de cursusbrochure), tenzij anders vermeld.

U kunt de brochure "Cursussen 85-86" aanvragen bij de secretaris van de redactie van Compact.