KMG Klynveld Kraayenhof & Co.
Automatisering & Controle-groep

COMPACT 853

Computer en Accountant

De overdrachtsprocedure is meer dan een gebruikerstest
door J.C. Boer

New technology and new risks in security and control
beveiligingsproblematiek in POS en ATM systemen bij banken
door A.W. Neisingh en H. Weerd

Documentatie van geautomatiseerde informatiesystemen en systeemonderzoeken; vragenlijsten
door J.M. Verheul

Nummer 39 12e jaargang zomer / herfst 1985

COMPACT

C O M P U T E R E N A C C O U N T A N T

INHOUDSOPGAVE

nummer 39 **12e jaargang** **Zomer/Herfst 1985**

COMPACT

Zomer/Herfst 1985

VAN DE REDACTIE

"Heroriëntering" ofwel "opnieuw bezinnen" vormt de les die ons in dit COMPACT-nummer wordt voorgehouden.

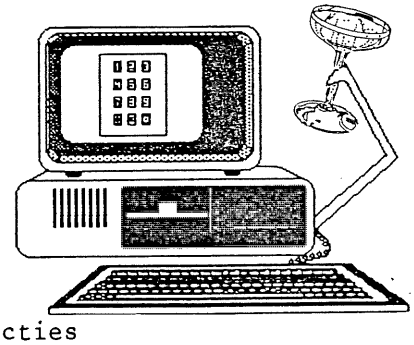
Aanleiding daartoe kunnen vormen: technische ontwikkelingen, maatschappelijke veranderingen dan wel nieuwe vragen van opdrachtgevers. Of - in het geval van de redactie - ook eventueel de huisvesting in nieuwe burelen; overigens - schrikt u niet - op hetzelfde vertrouwde kantooradres.

Onze keus van hoofdartikelen is gevallen op een drietal onderwerpen, zoals op de voorpagina staat aangegeven. Voor de samenvatting verwijzen we naar het volgende blad. Het geheel voorafgegaan door een tweetal actualiteiten:
- KMG K memory nummer 3;
- de Installatie van de Commissie Computercriminaliteit door minister Korthals Altes (rede onverkort afgedrukt).

en gevolgd door de rubrieken Micro, Boeken, Tijdschriften en ABC-nieuws. Onderwijs komt de volgende keer aan de orde.

Met het oog op de naderende feestdagen wagen we ons aan een enkele beschouwing.
Zal de bovengenoemde les ons beter van onze verantwoordelijkheid bewust maken en kunnen we die aan?

Prachtig! Op een goed 1986 met veel moed.

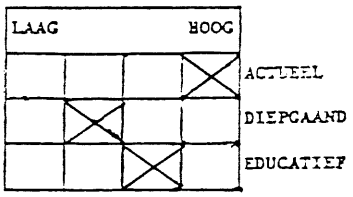


Wisseling rubrieksredacties

- L.N.M. Straathof heeft zijn redacteursschap voor Tijdschriften beeindigd. De Compactredactie dankt Leo voor zijn korte edoch levendige bijdragen.
- Nieuwe benoemingen tot mederubrieksredacteur:
  - J.C. Boer voor Tijdschriften;
  - D. de Kruif, J.C. van Winkel en J.A.W. Winterink voor Boeken;
  - J. Kuipers voor ABC-nieuws.

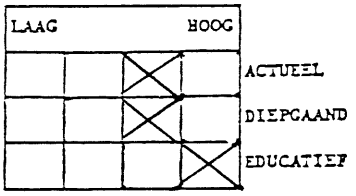
Succes met veel inspiratie.

"New technology and new risks in security and control"
Beveiligingsproblematiek in POS- en ATM-systemen bij banken
door A.W. Neisingh en H. Weerd



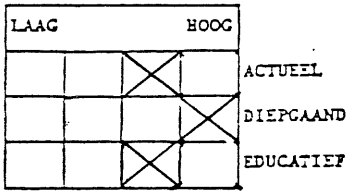
Menige organisatie staat bloot aan nieuwe bedreigingen ten gevolge van wijzigingen in de techniek. Dit moet aanleiding zijn tot herbezinning op de risico's. Hoewel nieuwe technieken drempelverhogend kunnen werken ten aanzien van kwaadwillenden vormt communicatie, in het bijzonder datacommunicatie een kwetsbaar gebied. In het artikel wordt ingegaan op POS- (Point of Sale) en ATM- (Automated Teller Machine) systemen.

De overdrachtsprocedure is meer dan een gebruikerstest
door J.C. Boer



Op grond van de acceptatie door het "Technisch beheer", de "Produktie", de "Beveiliging" en de "Opdrachtgever", zal de "Beheerder van programmabibliotheken" de systeemcomponenten kunnen overzetten naar de produktie-omgeving. Op deze overdrachtsprocedure dient namens de leiding controle uitgeoefend te worden.
In het artikel wordt door de schrijver op ieder van bovengenoemde facetten ingegaan.

Documentatie van geautomatiseerde informatiesystemen en systeemonderzoeken; vragenlijsten
door J.M. Verheul



Doel van dit artikel is het ontvouwen van een systematiek voor de documentatie van onderzoeken van geautomatiseerde informatiesystemen, als onderdeel van een dossierstelstel. In dat verband wordt afzonderlijk aandacht besteed aan de toepassing van vragenlijsten.
Bij de lezer wordt algemene kennis verondersteld van het ontwikkelen, onderhouden en exploiteren van informatiesystemen.

COMPACT

Zomer/Herfst 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:
A.H.C. Koedijk
A.W. Neisingh,
Prof. D. Steeman
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

KMG Computer Newsletter Memory

K-memory wordt uitgegeven door het Bureau Praktijkontwikkeling van KMG Executive Office onder supervisie van J.H. Urbanus als lid van de Computer Audit Sub Comittee (CASC).
Het blad is in eerste aanleg voor intern gebruik binnen KMG. Voor belangstellenden - ook voor onze cliënten - is een exemplaar van de jongste editie van september 1985 beschikbaar.

De inhoud kan als volgt kort worden samengevat:

- **Green light for CASC**
  - ontwikkeling goedgekeurd voor een gebruikersvriendelijk interface met EDP-AUDITOR;
  - geschikt maken van File Analysis Tool (FAT) en File Conversion Tool (FCT) voor kleine gegevensverzamelingen op diskettes;
  - aankondiging van een nieuwe rubriek op het gebied voor cursussen en educatie.

- **KMG-projects: the state of the art**
  Hierin wordt de software van KMG besproken zoals:
  - The KMG File Analysis Tool (FAT);
  - KMG Information Registry.

- **KMG training and education**
  - Registry of auditing and consultancy related microcomputer training courses;
  - KMG computer audit conference, waarop ondermeer het IBM system 38 aan de orde is gesteld. (Voor deze nieuwe cursus zie Compact no. 37 pag. 76).

- **KMG computer services-office by office**
  - The Planning Machine. KMG Denmark;
  - The Invisible Chain: modern methods of information retrieval. KMG heeft toegang tot tal van databases en databanken. Hierdoor is on-line literatuuronderzoek mogelijk. (zie Compact no. 38 pag. 77);
  - Positive Reaction to Prisma. Prisma is een methode voor het beschrijven van organisaties en hun informatiesystemen. Een recente brochure is op aanvraag leverbaar. De PRISMA-methode wordt ondersteund door een geautomatiseerd documentatiesysteem. Dit systeem biedt de mogelijkheid de verschillende PRISMA-schema's grafisch in te voeren en af te drukken op papier.

- Who's who in EDP-audit
  - Frederic D. Winslow, recently appointed chairman of CASC (pag. 7)
  - Raymond H. Healey, during six years chairman of CASC (pag. 1). Van zijn hand is een toekomstgericht artikel in 3 afleveringen opgenomen in Compact nrs. 30 t/m 32 in de rubriek "De microcomputer in de accountantscontrole".

- Bytes & Pieces
  - Wanted! New name for CARS;
  - Evaluation of Swiss Interbank Clearing System;
  - KMG PSI-symposium (zie deze Compact).

U kunt een exemplaar van K-memory bij de Redactie van Compact aanvragen.

Installatie Commissie-Franken

De Staatscourant van donderdag 21 november 1985 no. 227 vermeldt op de voorpagina de installatie van de Commissie Computercriminaliteit door Minister Korthals Altes.

Gezien het belang van het onderwerp heeft de redactie van Compact besloten de samenvatting alsmede de tekst van de voordracht van Minister Korthals Altes en het antwoord van staatsraad mr. H. Franken, voorzitter, integraal uit de Staatscourant over te nemen. Zie laatste pagina's van deze Compact.

Samenvatting onder de titel "Bestaand en nieuw recht".

In zijn installatietoespraak vermeldde de minister dat Justitie met de bestaande strafbepalingen niet geheel machteloos is tegen crimineel gebruik van computers. Technische ontwikkelingen kunnen oorzaak vormen dat de wetgeving nu leemten vertoont.
Hij noemt:
- afluisteren telefoongesprekken, opvangen etherberichten;
- manipulatie van gegevens die vermogensverschuiving ten gevolge hebben;
- kraken van computers;
- zonder toestemming gebruik maken van andermans computer.

De minister hoopt dat de commissie met voorstellen komt, die voor tientallen jaren kunnen gelden.

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

DE OVERDRACHTSPROCEDURE IS MEER DAN EEN GEBRUIKERSTEST

door J.C. Boer

1. Inleiding

Over de inhoudelijke verantwoordelijkheid van de gebruiker voor de geautomatiseerde verwerking van zijn gegevens bestaat nog maar weinig discussie. De verwerking is immers slechts een delegatie*) aan een gecentraliseerde afdeling.

De gebruiker van een informatiesysteem kan, bij een goed opgezet informatiesysteem, zijn verantwoordelijkheid voor een juiste en volledige informatieverwerking dragen door de gebruikerscontroles geïntegreerd in het informatiesysteem. Deze controles zijn repressief van karakter; tevens dragen zij bij tot het bereiken van een organisatie die verantwoordelijkheden kan dragen ten aanzien van de eigendomsrechten van programma's en gegevens, de continuïteit, de privacy en de geheimhouding.

De functiescheidingen in de automatiseringsorganisatie hebben tot doel zekerheid te geven over het ongewijzigd bewaren van de programma's en gegevens. De computerproduktie en de benadering van gegevens (een uitvoerende functie) vindt in opdracht van de gebruiker/eigenaar plaats.

De belangrijkste functiescheiding in de automatiseringsorganisatie is de scheiding tussen de ontwikkeling en produktie. In de ontwikkelomgeving kan de programmatuur vrijelijk aangepast worden, in de produktie-omgeving moet de programmatuur ongewijzigd blijven. De scheiding tussen ontwikkeling en produktie impliceert een overdracht, waarbij aan de systeembouwers décharge wordt verleend en de automatiseringsorganisatie het systeem voor verwerking accepteert. De décharge wordt verleend door de gebruiker die vanaf dat moment de verantwoordelijkheid voor de inhoudelijke gegevensverwerking op zich neemt. Over de acceptatie door het onderdeel van de automatiseringsorganisatie belast met de bewaring en de uitvoering van het informatiesysteem wordt weinig gesproken.

*) Bij decentrale "stand alone"-verwerking is van deze delegatie geen sprake. Dit artikel is geënt op een (deels) gecentraliseerde opslag en/of verwerking van gegevens van functioneel gescheiden afdelingen of bedrijven.

Voorafgaande aan het fiat van de gebruiker wordt een acceptatie- of gebruikerstest uitgevoerd. In de praktijk wordt veelal waargenomen, dat de acceptatietest zich beperkt tot het vaststellen van de functionele werking van de programmatuur. Voor een betrouwbaar informatiesysteem is echter niet alleen de functionele werking belangrijk, ook zullen allerlei eisen ten aanzien van de automatiseringsorganisatie ingevuld moeten zijn.
Gedacht moet hierbij worden aan continuïteit, privacy, etc. Veelal wordt er impliciet van uitgegaan, dat aan deze eisen wordt voldaan. Een definiëring van deze eisen in het functioneel ontwerp, gevolgd door een test van de invulling van deze eisen door de automatiseringsorganisatie vindt slechts bij uitzondering plaats.

In het functioneel ontwerp zal vastgelegd behoren te worden, welke eisen het informatiesysteem aan de automatiseringsorganisatie stelt. Op het moment van overdracht van het systeem zal vastgesteld moeten worden of in voldoende mate invulling aan deze eisen is gegeven.

De nieuwe (c.q. aangepaste) programmatuur heeft zijn invloed op de totale automatiseringsorganisatie. Een acceptatie (waarbij het hiervoor bedoelde functioneel ontwerp "in ruime zin" de norm vormt) zal niet alleen door de opdrachtgever/gebruiker plaats moeten vinden, doch ook door alle betrokken onderdelen van de automatiseringsorganisatie.

2. Functioneel ontwerp

Het functioneel ontwerp vormt de basis voor de verdere uitwerking van het geautomatiseerde informatieverwerkende systeem. Het is de opdrachtspecificatie aan de automatiseringsorganisatie. Het gerealiseerde informatieverwerkende systeem zal aan de specificaties van het functioneel ontwerp moeten voldoen. Bij de acceptatie van een systeem is het functioneel ontwerp de norm.
Om als algehele norm te kunnen fungeren zullen naast de functionele eisen, betrouwbaarheids-, effectiviteits- en efficiëntie-eisen ook de eisen ten aanzien van de automatiseringsorganisatie opgenomen dienen te zijn. Over het algemeen zijn dit geen onbekende organisatorische maatregelen binnen de automatiseringsorganisatie. Het is echter noodzakelijk in het functioneel ontwerp aan te geven in welke mate deze maatregelen voor een specifiek systeem van belang zijn. In de acceptatietest vormt deze vastlegging de norm bij de toetsing van de wijze waarop binnen de automatiseringsorganisatie invulling aan de gestelde eisen is gegeven.

Eisen te stellen aan de automatiseringsorganisatie

Voor het bereiken van een beheersing van de informatieverwerking is het noodzakelijk, dat in het functioneel ontwerp onder meer de volgende aspecten belicht worden:

- eisen ten aanzien van de betrouwbaarheid;
- eisen ten aanzien van de continuïteit;
- eisen ten aanzien van de geheimhouding (o.a. van financiële informatie, research- en produktgegevens);
- eisen ten aanzien van de privacy;
- eisen voortkomend uit wettelijke bepalingen.

Naast deze aan de automatiseringsorganisatie gestelde eisen zal tevens in het functioneel ontwerp aangegeven moeten worden hoe de raakvlakken met de administratieve organisatie bij de opdrachtgever/gebruiker liggen. Bekend moet zijn wie over (delen) van het informatiesysteem mag beschikken en wie geautoriseerd zijn om (delen) van het informatiesysteem te gebruiken. Gedefinieerd moet zijn:

- het eigendom van het systeem (beschikkend),
- het eigendom van (categorieën van) gegevens (beschikkend),
- de delegatie van het gebruik van het systeem (uitvoerend),
- de delegatie van het gebruik van de gegevens (uitvoerend),
- de delegatie van elementen uit de beschikkende functie,
- de wijze waarop wijzigingen in de delegaties geautoriseerd worden.
- de wijze waarop een controle op de delegaties plaatsvindt.

Het functioneel ontwerp kan slechts als norm fungeren nadat het gefiatteerd is door de opdrachtgever (de persoon, afdeling, instelling die budgettair verantwoordelijk is).
De automatiseringsorganisatie kan tot uitwerking van het systeem overgaan nadat zij vastgesteld heeft, dat de hiervoor genoemde aspecten in het functioneel ontwerp opgenomen zijn en een fiattering door de opdrachtgever plaatsgevonden heeft. Indien een verbijzonderde interne controle-afdeling aanwezig is, zal zij op dit punt een formele controle op de volledigheid van de inhoud van het functioneel ontwerp kunnen uitvoeren.

3. De acceptatie van het informatieverwerkende systeem

Vanuit beheersbaarheidsoogpunt zijn twee belangrijke momenten te onderscheiden:

- de definitieve vaststelling van het functioneel ontwerp;
- de acceptatie van het gebouwde informatiesysteem.

In de vorige paragraaf is ingegaan op de aspecten verbonden aan het functioneel ontwerp, zodat het als een norm kan fungeren voor het te bouwen informatiesysteem.
Direct voorafgaande aan de produktiefase zijn de volgende functionarissen betrokken:

- de toekomstige technisch beheerder van het systeem,
- de uitvoerder van de computerverwerking (produktie),
- de beveiligingsfunctionaris (toegang tot programma's en data).
- de opdrachtgever/gebruiker; de beschikkende functie met betrekking tot het informatiesysteem (functioneel beheer).

Bij de nadere uitwerking van de inhoud van deze functies op het moment van acceptatie zal het accent liggen op de in de vorige paragraaf naar voren gebrachte eisen ten aanzien van de automatiseringsorganisatie.

Alvorens tot operationele verwerking van het informatieverwerkende systeem overgegaan kan worden zullen alle betrokkenen hun fiat hieraan moeten geven. De binnen de automatiseringsorganisatie verantwoordelijke functionarissen verplichten zich hiermee tijdens de operationele fase van het systeem voor de invulling van de eisen zorg te dragen. Alhoewel formeel gesteld moet worden, dat het fiat van de betrokkenen binnen de automatiseringsorganisatie op het moment van invoering van het informatiesysteem aanwezig moet zijn, kan uit doelmatigheidsoogpunt een eerder tijdstip zinvol zijn. Hiermee wordt voorkomen, dat een functioneel ontwerp met onrealistische eisen aan de automatiseringsorganisatie zonder afstemming tot aan de produktiefase wordt uitgewerkt. Een beoordeling op grond van de acceptatiecriteria kan voor een deel reeds op grond van het door de opdrachtgever vastgestelde functioneel ontwerp plaats vinden.
Een voorwaarde voor een beheersbaar verloop van de acceptatieprocedure is, dat de opzet van de organisatie van de automatisering zodanig is, dat sprake is van een gescheiden ontwikkel-, test- en produktie-omgeving. De overdracht van de systeemcomponenten van ontwikkel- naar testomgeving en van test- naar produktie-omgeving moet plaatsvinden door de programmabibliotheekbeheerder. Deze bewarende functionaris, werkzaam binnen de automatiseringsorganisatie, moet een ander zijn dan de hiervoor genoemde functionarissen.

Acceptatie technisch beheer

De technisch beheerder wordt verantwoordelijk voor het onderhoud van het systeem. Kent een organisatie geen afzonderlijke technisch beheerfunctie dan zal de leiding van de systeemontwikkelafdeling moeten vaststellen, dat het produkt van zijn medewerkers van voldoende kwaliteit is om een onderhoudscontinuïteit te kunnen garanderen.
De volgende aspecten zijn voor een technische acceptatie van belang:
- de volledigheid van de systeemdokumentatie uit oogpunt van systeemonderhoud;
- de invulling van de persoon of instelling die over het systeem mag beschikken (verstrekken van opdrachten);
- de vastlegging van eventueel gedelegeerde bevoegdheden (b.v. het technische onderhoud zonder aantasting van de functionaliteit) en de controle die hierop uitgeoefend gaat worden;
- de kwaliteit van het systeem zodat het onderhoudbaar is; de programma's en het systeem moeten logisch gestructureerd zijn.

Kortom de voor het onderhoud verantwoordelijke functie moet vaststellen, dat zij haar onderhoudsverantwoordelijkheid kan dragen.

Acceptatie door de uitvoerder van de computerverwerking

Alvorens een systeem in produktie genomen gaat worden zal vastgesteld moeten worden, dat de afdeling die voor de computerverwerking verantwoordelijk is, in staat is voor het betreffende systeem deze verantwoordelijkheid te dragen.

De uitvoering van het systeem in de operationele fase moet zodanig plaatsvinden dat aan de eisen gesteld in het functioneel ontwerp wordt voldaan.
De produktiefunctie zal na acceptatie moeten zorg dragen voor de nakoming van de gestelde eisen ten aanzien van de continuïteit, en enkele aspecten ten aanzien van de geheimhouding en de privacy.
Aan de continuïteitseisen in het functioneel ontwerp zal zij invulling moeten geven door (voorzover noodzakelijk) zorg te dragen voor:
- reserve hardware;
- externe uitwijkfaciliteiten;
- het bewaren van de back-up copieën van programma's en de bestanden; van belang hierbij is:
  - een benoeming van de bestanden;
  - de frequentie van de aanmaak;
  - de bewaartermijn;
  - de bewaarplaats;
- het treffen van bijzondere voorzieningen in verband met datacommunicatie en data-entry;
- de procedure met betrekking tot afhandeling van transacties die nog niet geheel afgehandeld zijn op het moment van de storing (tussenbestanden, de zogenaamde pijplijn).

Ten aanzien van de geheimhouding en de privacy zal zij maatregelen moeten treffen, opdat aan de vereisten uit het functioneel ontwerp voldaan wordt. Aandachtspunten hierbij zijn:
- de procedure van overdracht van gegevens aan de geautoriseerde gebruiker van het informatiesysteem;
- de procedures en de organisatie van de nabewerkingsafdeling;
- het hergebruik en de vernietiging van gegevensdragers die gebruikt zijn bij de verwerking van systemen met privacy-gevoelige of geheime informatie.

Bij haar acceptatie zal de afdeling vaststellen, dat zij de produktieverantwoordelijkheid voor het systeem kan dragen. In het algemeen gesteld is hiervoor van belang dat zij haar fiat geeft aan:
- de in het funkioneel ontwerp gestelde eisen ten aanzien van de benodigde verwerkingscapaciteit, continuïteit en geheimhouding (technische realisatiemogelijkheden versus de kosten);
- de produktiedokumentatie,
- de produktieprocedures (J.C.L.),
- de doelmatigheid van het systeem in termen van machinebeslag (verwerkingstijd en ruimte) en nabewerkingsprocedures.

Acceptatie in samenhang met de beveiliging

Voorafgaande aan de produktie zal vastgesteld moeten worden of de invoering van het systeem geen aantasting van het algehele beveiligingsniveau van de organisatie van de automatisering betekent.

Tevens zullen de voor het betreffende systeem noodzakelijke toegangsregels gedefinieerd moeten worden.

Afhankelijk van de organisatie zal de acceptatie vanuit het beveiligingsoogpunt plaatsvinden door het hoogst hiërarchische niveau verantwoordelijk voor de geautomatiseerde informatieverwerking, een security officer, de data-administrator en/of een data-security officer. De invulling van de bedoelde security-functie wil in de praktijk nog wel eens verschillen. De toewijzing van de verantwoordelijkheden moet gezien worden tegen de achtergrond van een specifieke organisatie en de daarin gebruikte systeemprogrammatuur. Indien blijkt, dat in een organisatie voor deze aspecten geen verantwoordelijke functionaris aan te wijzen is, dan zal tot een organisatiewijziging besloten moeten worden om een veilige informatieverwerking te bereiken.

Voordat de beveiligingsfunctie zijn fiat aan een systeem zal geven dient door haar vastgesteld te worden dat:
- de grenzen van het systeem (programmatuur en data) vastliggen, zodat de toegangsregels zodanig gedefinieerd kunnen worden, dat gebruikers van het informatiesysteem de algehele beveiliging niet kunnen aantasten;
- de gebruikers van het systeem aangegeven zijn, zodat de toegang tot het systeem in de toegangsbeveiligings-software aangebracht kan worden;
- vastgelegd is welke persoon of instelling bevoegd is wijzigingen in de toegang tot de systeemfuncties en de data aan te geven (de beschikker over het systeem);
- het gebruik van gegevens en/of delen uit systemen onder de verantwoordelijkheid van anderen door de beschikkende functie over deze gegevens en/of systemen is geautoriseerd; in een geïntegreerde data base omgeving zal toegezien moeten worden op de juistheid van de subschema's; de subschema's vormen een onderdeel van de software waarop een scherp toezicht noodzakelijk is om te ruime toegang tot gegevens te voorkomen;
- directierichtlijnen, wettelijke en internationale regels (transborder data flow) met betrekking tot integraties tussen informatiesystemen opgevolgd zijn;
- de bijzondere maatregelen uit hoofde van de geheimhouding en de privacy geïmplementeerd kunnen worden.

Na acceptatie van het systeem door de afdeling verantwoordelijk voor beveiliging wordt zij verantwoordelijk voor een juiste en volledige implementatie van de in het functioneel ontwerp vastgelegde toegangsregels. De afscherming van het betreffende systeem en haar gegevens ten opzichte van alle andere computergebruikers en de automatiseringsorganisatie behoort tot haar verantwoordelijkheid.

Acceptatie door de opdrachtgever

De acceptatie door de opdrachtgever betekent een décharge voor de medewerkers binnen de automatiseringsorganisatie die betrokken zijn geweest bij de tot stand koming van het gegevensverwerkende systeem. De verantwoordelijkheid voor de betrouwbaarheid van het systeem en de toereikendheid van de gemaakte afspraken ten aanzien van het eigendom, de delegaties, de continuïteit, de privacy en de geheimhouding gaat op het moment van acceptatie over naar de eigenaar van het systeem.
Voordat de opdrachtgever het systeem zal accepteren dient hij vast te stellen, dat de getroffen maatregelen ter beheersing van de informatieverwerking zodanig zijn gerealiseerd, dat de eisen, zoals vastgelegd in het functioneel ontwerp, volledig zijn ingevuld.
De opdrachtgever zal met het uitvoeren van de acceptatietest starten, nadat hij vernomen heeft dat het systeem binnen de automatiseringsorganisatie geaccepteerd is. Dit betekent, dat de verantwoordelijkheden voor de technische aspecten, uitvoeringsaspecten en beveiligingsaspecten aanvaard zijn.
In de acceptatietest zullen elementen opgenomen moeten zijn ter vaststelling van een juiste en volledige invulling van deze verantwoordelijkheden.
De norm voor de uitvoering van de acceptatietest in de ruime betekenis is het functioneel ontwerp. De opdrachtgever zal vaststellen of aan de norm voldaan is. De test die hij daarvoor zal uitvoeren is ruimer dan een test op de functionele aspecten.
De elementen van de acceptatietest zijn:
- de functionele aspecten;
- de betrouwbaarheid (volledige, juiste en tijdige verwerking);
- de toegang tot de functies van het informatiesysteem;
- de effectiviteit vooral gericht op de aspecten van de gebruikersvriendelijkheid en de geschatte exploitatiekosten;
- de toereikendheid van de dokumentatie en opleidingen;
- de continuïteit;
- de geheimhouding;
- de privacy;
- de wettelijke regelingen.

Testen op de continuïteit houdt in, dat vastgesteld moet worden, dat de continuïteit binnen de gestelde grenzen van het functioneel ontwerp is geëffectueerd. Diverse storingen zullen moeten worden gesimuleerd. Indien externe uitwijkfaciliteiten geëist zijn in het functioneel ontwerp zal een uitwijktest tijdens de acceptatiefase moeten plaatsvinden.
Door de opdrachtgever zal vastgesteld moeten worden of de getroffen back-up- en recovery-voorzieningen overeen komen met de voor het systeem gestelde eisen. Aan de hand van de in de uitwerking gedefinieerde bewaartermijnen voor de bestanden met gegevens, parameters en programma's zal de opdrachtgever moeten vaststellen dat aan zijn reconstructie-eisen voldaan wordt.

Ten aanzien van de geheimhouding, de privacy en de opvolging van de wettelijke vereisten zal hij zich op de hoogte moeten stellen van de getroffen maatregelen gevolgd door een beoordeling van deze maatregelen ten opzichte van de vastlegging in het functioneel ontwerp. Zover als mogelijk is zal hij door middel van enkele "inbraakpogingen" de effektiviteit van de getroffen maatregelen vast moeten stellen.
Na een acceptatietest op alle aspecten van het functioneel ontwerp zal de opdrachtgever zijn fiat geven voor het in produktie nemen van het systeem.

4. Uitvoering van de overdracht naar produktie

Op grond van de acceptatie door het technisch beheer, produktie, beveiliging en de opdrachtgever zal de beheerder van de programmabibliotheken de systeemcomponenten overzetten naar de produktie-omgeving.

Indien in de organisatie een verbijzonderde interne controle-functie aanwezig is zal deze namens de leiding moeten vaststellen in hoeverre deze acceptatieprocedure op een verantwoorde wijze uitgevoerd wordt. Onder tijdsdruk is het risico aanwezig dat onderdelen van de automatiseringsorganisatie verantwoordelijkheden accepteren die zij gezien de getroffen maatregelen niet kunnen dragen. Na constatering van ernstige tekortkomingen moet de interne controle-functie in staat zijn de invoering van het systeem tegen te houden totdat de tekortkomingen zijn verholpen respectievelijk vanuit het organisatorische niveau, waarvan de controle-opdracht afkomstig is, een expliciet fiat voor de invoering wordt gegeven.

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

NEW TECHNOLOGY AND NEW RISKS IN SECURITY AND CONTROL
BEVEILIGINGSPROBLEMATIEK IN POS- EN ATM-SYSTEMEN BIJ BANKEN *)

door A.W. Neisingh en H. Weerd

[Dit artikel**) is gebaseerd op de lezing van A.W. Neisingh tijdens het mede door KMG gesponsorde Payment Systems International (PSI) symposium in Kopenhagen, november dit jaar. Het eerste, algemene deel van de lezing is door de redactie kort in het Nederlands samengevat; daarna volgt de letterlijke Engelse tekst van de gepresenteerde "paper".]

Inleiding

Menige organisatie staat bloot aan bedrijfsbedreigingen; deze bedreigingen kunnen als volgt worden gecategoriseerd:
- Discontinuïteit;
- Onjuiste beslissingen ten gevolge van fouten;
- Fraude;
- Nadeel ten opzichte van de concurrentie;
- Wetsovertredingen (bijvoorbeeld ten aanzien van privacy).

De invloed van electronische gegevensverwerking op deze risico's wordt reeds lang onderkend. Wijzigingen in de toegepaste (computer-) technologie leiden echter ook steeds weer tot wijzigingen in de risico's. Het op de juiste wijze inspelen op deze wijzigingen vereist:
- een goede beveiligingsorganisatie;
- een door de hoogste leiding vastgesteld beveiligingsbeleid;
- controle of op de juiste wijze uitvoering aan dit beleid wordt gegeven (controle op de implementatie).

(Over het belang van dit soort zaken is reeds geschreven in Compact 84/3 door H.C. Kocks.)

Steeds weer als beslist moet worden over wijzigingen in de toegepaste technologie, zal moeten worden vastgesteld of het beveiligingsbeleid moet worden bijgesteld en wat de invloed is op het geïmplementeerde beveiligingssysteem.

Overduidelijk manifesteren de bedreigingen en de invloed van toegepaste computer technologie op de bedreigingen zich bij banken.

*) POS staat voor Point of Sale, ATM voor Automated Teller Machine.
**) De volledige tekst van de voordracht kan op aanvraag toegezonden worden. U kunt uw verzoek richten aan de secretaris van de redactie van Compact.

Een van de meest risico-rijke onderdelen wordt gevormd door communicatieprocessen. Hoewel nieuwe technieken (zoals het gebruik van fibers en satellieten) drempelverhogend kunnen werken ten aanzien van kwaadwillenden vormt communicatie, in het bijzonder datacommunicatie, een kwetsbaar gebied.

Hieronder wordt ingegaan op onder meer Point of Sale- en Automated Teller Machine-systemen.

EFT at the POS is a good example of the interrelation of risk areas

The most demanding requirements for secure transactions in large commercial networks are likely to be found in Electronic Funds Transfer in the Point of Sale system or EFTPOS as it is known. EFTPOS is a good example of the interrelation of risk areas.
This can be illustrated by looking at a model of the EFTPOS environment in terms of its transaction structure and network functions.

An EFTPOS transaction has three basic phases, authorization of the request, creation of the transaction, and data capture. Each phase consists of a group of activities which are to be performed by network functions.

1. Authorization can be further subdivided into four distinct subfunctions as follows:
   - an access request: the card issuer verifies the validity of the terminal, the uniqueness of the transaction, and the identity of the card user;
   - granting access: the card issuer sets terms and conditions of access, limitations on the transaction and prerequisites to be met;
   - a negotiation phase: during this phase the parties (card holder and retailer) agree to details on the transaction;
   - an agreement phase with the authority of the parties to proceed on the basis of that agreement.

   The Personal Identification Number (PIN) is the card holders authority and should be used for message authentication only after agreement has been reached.

2. When authorization has been granted, the actual physical transaction takes place. This concludes with the production of a journal entry of the transaction and a receipt. At this point there is no possibility of cancelling the transaction since the consumer has left the store. The EFTPOS system's responsibility now is to capture the transaction data.

3. Data Capture consists of two operations: the real time storage of the data on recoverable media, and the subsequent forwarding of transaction details to the parties involved.

   For the integrity of the data all transactions must be authenticated:
   by a network function using the card holders PIN-code.
   The authenticated transactions must be confirmed:
   by a network function using a retailer's bank confirmation code.
   The confirmations must be acknowledged:
   by a network function using a retailer-terminal acknowledgement code.
   After succesfull acknowledgement the responsibility for the transaction data including its recovery and integrity is transferred from the retailer to the retailer's bank. The originator (retailer) can now erase his copy of that transaction data.

The processing of the transaction data by the banking system to reconcile and settle is not of importance to the network; however, the transaction structure and message contents must support:
- automated and efficient reconciliation;
- a sound basis for an audit trail;
- the view of a transaction should be consistent to all parties involved.

The general network structure contains each of the three basic phases of the major network functions as separate components.

The general network structure provides for:
1. end user interface and control in the retailer's terminal;
2. data recovery, transaction control and routing in the data capture node;
3. a message switching service;
4. gateway functions between EFTPOS-terminal and the host systems;
5. an authorization system acting on behalf of the consumer;
6. a sponsor acting on behalf of the retailer;
7. network administration functions.

By merging the functions of one or more components, many different network implementations can be created. Each of these is, in effect, a derivative of the general network structure.
The data capture node, the message switching service and the network administration functions are shared by the retailer, the card issuer and the retailer's bank.
The shared functions have an effect on system security, but are not under the direct control of the participants since they are shared. Hence an approach to security must be adopted that allows the shared use of the EFTPOS-system without representing an exposure to the participants.
This approach should be a requirement for the EFTPOS-system. Design decisions should be made in accordance with this approach.

Other new technologies also carry associated risks.

The Automated Teller Machine (ATM) provides a retail service. ATM's can be used for own banking services or for shared use. The ATM can be connected with a computer or can be used as a stand-alone machine to carry out simple banking transactions, balance inquiry, and deposits and withdrawals.

Checking the PIN against the card identity can be done in the terminal if the PIN is related to the account number and checking other card data is accomplished by an algorithm, for example, the use of a digit with a secret key. Having the relationship dependent on a secret key which is the same for all ATM's is a risk, because the key is held at so many places. Compromise of the key makes the whole system unsafe because an enemy is able to discover the PIN of any stolen cards or make his own cards and determine the PIN which will match them. The physical security surrounding an ATM makes it very unlikely that the secret key will be discovered by intrusion. The weakness, if any, is in the way the key is loaded into the ATM. The key can be the result of a calculation employing data from several sources or the algorithm can be a complex one requiring several keys. It can then be arranged so that no one person has access to all the data necessary to forge cards.

The keys are used in two places in the system, at the ATM's for checking the relationship of the PIN with the account number and other card data and at, for example, the bank headquarters where PIN's are calculated for distribution to customers. It is probably in the central area that the security of the keys is most at risk and this type of risk appears in some form in any on-line system, whatever method is used centrally for managing or checking PIN's.

Therefore, the additional risk in an off-line ATM system due to the multiplicity of places at which PIN checking is carried out can be small if the system is designed well.
The physical security of the ATM's is an essential factor in this evaluation.

Personal Identification Number (PIN) management is the subject of a U.S. National Standard. Three types of PIN are distinguished: assigned derived PIN's, assigned random PIN's and customer-selected PIN's. To the customer the only detectable difference is between a PIN he is assigned or a PIN he can choose himself.

The dialogue for an on-line ATM should at least contain ATM-id, security number (hologram) read from the card, and the PIN (enciphered).

In the case of shared ATM-systems, we have a problem. The methods the various banks use for verifying PIN's against card identity will not be the same; therefore, no single algorithm operation in an ATM can verify the PIN's of all the customers it serves. Therefore, PIN verification must be done centrally by each card issuer; all ATM's must be on-line when they serve the customer of other banks, and all ATM processors of all banks must be connected by a communications network.

In the ATM area, there are three basic types of fraud:
- unauthorized use of access devices. Bank card and Personal Identification Numbers can be obtained by an unauthorized user. A daily withdrawal limit of $ 200 to $ 300 can help limit losses;
- fraud by an authorized cardholder. Cardholders can deny knowledge of transactions they entered into their own accounts;
- insider manipulation. Employees within the bank or its suppliers can steal bank cards, remove cash from ATM replenishment funds or deposits, manipulate account records, or carry-out some form of electronic attack.

Retail services and home banking share many characteristics with ATM's. Account holders may retrieve information about their accounts, make payments or transfer funds between accounts. In fact identification and authorization procedures have to take place. However the terminal is entirely under control of the client.

Finally, some remarks with regard to legislative aspects of ATM's.

When Automated Teller Machines are used there are two situations where an international transfer of data occurs:

1. when activating an ATM outside of one's own country, resulting in an international transfer of data such as names of the parties to the transactions, the amount and nature of the transaction and the date;
2. when activating a local ATM for a purely domestic transaction which can imply that the data concerned pass one or several borders due to centralisation of data flow from the bank's branches at the head office.

These financial data are personal data as defined in various European data protection laws since the data concerns information relating to an identified or identifiable subject.

These data protection laws contain provisions restricting the international flow of such data to countries not offering equivalent protection to those data. Data flows to the U.S. especially are subject to those restrictions.

One should, therefore, be aware of the existence of these regulations, and of the national laws of all countries in transit and of destination when using an international EFT-system or when using any international network for the transfer of personal data, for any other purpose. It might be useful to consult legal advisors or the local data protection authorities to ensure oneself of the existence of and content of such regulations.

Front Office Automation is an aspect of the new technology which illustrates some new risks with respect to unauthorized access to information

On the one hand, Front Office Automation creates the opportunity to extend more privacy to customers inside the bank branch. Clients can discuss their finances with bank employees across a bureau top instead of through bulletproof glass. Yet on the other hand, Front Office Automation means that employees will have increased access to clients personal information.

Let's first define what front office automation means.

To begin with, front office automation is a tool for improving the quality of retail activities by banks. It means, for example, that bank employees will be able to provide clients with advice tailored to the clients financial situation. The resulting improvement in service can mean increased market share and more profit.

This could be done by automating the cash and computer traffic extensively.

To enable the bank employee to verify a clients identity, the client must present a card and enter a Personal Identification Number known as a PIN-code. On screen, the employee will have access to the clients personal information and his financial information such as account balances, credit limits, stocks, options, insurance and so forth.

It is clear that a number of internal controls and security measures need to be taken in such an environment. The infrastructure of application software and the computer installation must be adequate.

The network which links the branch office to the central computer must be secure.

The organization of the branch must be adequate. This means that environmental provisions which govern access to terminals, access to the network processor and so forth must be instituted. This means segregation of functions support by procedures and so on.

As well, Front Office Automation requires control over the employee's identification cards which reflect the segregation of duties within the branch at a certain moment. Even more important is the segregation of duties within transaction cycles within the branch.

Provisions need to be made to serve clients who do not want to use PIN-codes. This is a security exposure to the system because these provisions give more opportunities for the branch-office staff to misuse the system.

Periodic audits are required to confirm that the introduction of new technology is under effective control

Although a thorough audit should cover all of the relevant risk areas, We would like to pay special attention to the risk area of organization and, the use of audit reports as a management tool.

The introduction of large new applications and technologies can roughly be divided into the following stages:
1. requirement definition;
2. design;
3. coding;
4. implementation.

An Internal System Audit is recommended for the requirement definition and design stages to confirm that design decisions have been made in accordance with the banks security policy.

Once the system is up and running, an Installation Audit carried out by an independent (external) auditor is recommended to answer questions such as:

- was the architectural design fully and correctly implemented?
- if not, why? What was wrong with the architectural design and/or resolutions?
- if they were implemented, were there any problems with them?
- what problems were encountered that the design should have resolved, but did not?

An audit report covering these points should be issued, and corrective action taken where necessary.

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

COMPACT

Zomer/Herfst 1985

DOCUMENTATIE VAN GEAUTOMATISEERDE INFORMATIESYSTEMEN EN SYSTEEMONDERZOEKEN; VRAGENLIJSTEN

door J.M. Verheul

INHOUD

Dit artikel zal eveneens verschijnen in het Handboek Accountancy '84.

1. Inleiding

In de jaarrekeningcontrole wordt de aandacht steeds meer verlegd naar de organisatie en de geautomatiseerde informatiesystemen, producenten van de registraties en verantwoordingen waarop de jaarcijfers zijn gebaseerd.
Zulks stelt hoge eisen aan de accountantsprofessie, mede omdat moderne systemen tevens een stuurfunctie hebben in de bedrijfsuitoefening (1)(2). De inrichting van de op de administratieve organisatie en de verdere interne organisatie betrekking hebbende onderdelen van accountantsdossiers dient met die eisen in overeenstemming te zijn en het effectief leiden van een opdracht, kwaliteitscontrole en waar nodig het afleggen van verantwoording over verrichte werkzaamheden tegenover de Raad van Tucht e.d. mogelijk te maken. In een doorlopend fungeren verdient het middels dossiers overdragen van kennis van de administratieve automatisering bijzondere aandacht (3).

Doel van dit artikel is het ontvouwen van een systematiek voor de documentatie van onderzoeken van geautomatiseerde informatiesystemen, als onderdeel van een dossierstelsel. In dat verband wordt afzonderlijk aandacht besteed aan de toepassing van vragenlijsten (onderdeel 5).

Bij de lezer wordt algemene kennis verondersteld van het ontwikkelen, onderhouden en exploiteren van geautomatiseerde informatiesystemen. Aan het documenteren van dat geheel wordt in het volgende onderdeel een korte bespreking gewijd.

2. Documentatie als basis voor onderzoek en controle

Door accountants (4)(5) en andere deskundigen is er vanouds op aangedrongen dat het ontwikkelen van geautomatiseerde informatiesystemen gepaard gaat met de totstandkoming van documentatie en rapportages welke onder meer de mogelijkheid bieden tot:

- een effectief project-management;
- het vermijden van misverstanden tussen gebruikers en specialisten;
- het voorkomen van fouten;
- kwaliteitszorg en -bewaking;
- fasegewijze evaluatie en autorisatie;
- goede voorbereiding van eindtests, conversies en invoering;
- tijdige aanpassingen aan veranderde omstandigheden (onderhoud).

Eveneens van belang zijn de verzamelingen algemene voorschriften, standaards, richtlijnen, functie-, taak- en procedurebeschrijvingen in de automatiseringsorganisatie, eventueel in de vorm van handboeken.

De documentatiegraad van afzonderlijke informatiesystemen en programmatuur is tevens van belang voor interne en externe onderzoekers. Mede dáárom zal vaak een oriëntatie voorafgaan aan een eventueel onderzoekopdracht. Daarbij blijkt veelvuldig dat documentaties en handboeken hiaten vertonen en/of sterk onvoldoende aan veranderingen zijn aangepast. Als oorzaken worden genoemd tijd- en geldgebrek. De werkelijke redenen zijn veelal een gebrek aan methodische systeemontwikkeling en toezicht. Vele ontwerp- en ontwikkelingsmethoden leiden niet of onvoldoende tot gerichte aandacht voor en beschrijving van eisen betreffende interne controle, beveiliging en continuïteit.

Een gelukkige omstandigheid is dat de algemene programmatuur voor besturing en management van computersystemen en files, welke onder meer het gebruik van hogere programmeertalen en een goed beheer van gegevensverzamelingen (waaronder databases) en programmabibliotheken mogelijk maakt, voorziet in de automatische vervaardiging van documentatie. Dat draagt er toe bij dat gebreken in documentatie niet spoedig leiden tot een voor de onderzoeker onwerkbare situatie. Zelfs standaardtoepassingen voor kleinere ondernemingen, waarbij over niet veel meer dan commercieel getinte handleidingen wordt beschikt, blijken in de praktijk vatbaar voor onderzoek, zij het dat de kosten te hoog kunnen zijn voor één cliënt.

3. Betrouwbaarheidsonderzoeken

Informatiesystemen kan men met verschillende doelstellingen en vanuit verschillende gezichtspunten onderzoeken. Binnen het kader van dit handboek gaat de belangstelling uit naar betrouwbaarheidsonderzoeken. Het aspect betrouwbaarheid is van overwegende invloed op de inhoud en de systematiek van accountantsdossiers betreffende EIV-onderzoeken*). Dat geldt niet alleen bij onderzoeken in het kader van jaarrekeningcontroles. In advieswerkzaamheden op het terrein van administratieve organisatie en bij operationeel onderzoek van de informatievoorziening zal eveneens veel aandacht aan betrouwbaarheid worden gegeven.
De hierna te presenteren systematiek van de onderzoekdocumentatie sluit dan ook aan bij de verschillende rollen waarin de interne of externe accountant zich met geautomatiseerde informatieverzorging bezig houdt.
De onderstaande invulling van de term betrouwbaarheid zal dit verduidelijken en belangrijke elementen voor de documentatiesystematiek aandragen.

In het kader van de jaarrekeningcontrole valt de hoofdaandacht op het stelsel van interne controlemaatregelen en de werking van dat stelsel. De onderzoeken van (delen van) informatiesystemen leiden tot toetsing en aanvulling van de uit andere controle-onderdelen verkregen kennis van interne controles.

*) EIV = Elektronische Informatie Verwerking

Voor zover nodig strekt de aandacht van de accountant zich uit tot maatregelen welke zijn gericht op het voorkomen, althans tijdig signaleren en ontdekken van ongeoorloofde handelingen ten aanzien van gegevens, gegevensverzamelingen en computerprogramma's. De aandacht kan daarbij tevens uitgaan naar het tijdig ontdekken van ingrepen, van storingen en menselijke fouten, alsmede naar de mogelijkheden voor een snel herstel van de juiste toestand en snelle hervatting van de gegevensverwerking.
De aandacht kan nog verder gaan en zich uitstrekken tot het voorkomen van calamiteiten, het beperken van de schade na een calamiteit, het tijdig hervatten van de meest essentiële verwerkingen en de geleidelijke volledige hervatting daarvan binnen aanvaardbare tijd.
In de cliëntorganisatie is een samenhangend geheel van interne controles, beveiligingsmaatregelen en continuïteitsvoorzieningen, aangevuld met beheer en toezicht, bepalend voor de betrouwbaarheid van de informatievoorziening.
Voor de controlerend accountant gaat het om de getrouwheid van de financiële registratie en de daarop gebaseerde presentatie van jaarcijfers. Dat vergt geen volkomen beoordeling van hetgeen in de cliëntorganisatie aan voorzieningen en procedures tot stand is gebracht. In de adviesfunctie, operationeel onderzoek en andere bijzondere EIV-onderzoeken zullen accountants en andere automatiseringsdeskundigen zich veelal breder en dieper met het stelsel van maatregelen dienen bezig te houden dan in jaarrekeningcontroles het geval is. De optiek is echter dezelfde. Voor zover nodig dient men zich rekenschap te geven van de nauwe samenhangen binnen een uitgebreid en complex geheel van maatregelen, alsmede het meervoudig effect van tal van maatregelen en het algemene karakter ervan. Met het laatste wordt bedoeld dat een belangrijk deel van de maatregelen van toepassing is op de meeste, zo niet alle in gebruik zijnde informatiesystemen. Het systeem dat de zwaarste eisen stelt bepaalt goeddeels het niveau van het gehele algemene stelsel. Men spreekt hier wel van paraplu-maatregelen. Deze treft men vooral aan in de automatiseringsorganisatie, waarvan hier in het bijzonder zijn te noemen de onderdelen waarin:

- informatiesystemen worden ontworpen, ontwikkeld en onderhouden;
- de omzetting van en naar voor mens respectievelijk machine leesbaar schrift wordt verzorgd;
- de elektronische verwerking plaatsvindt;
- de gegevensverzamelingen, op machinaal leesbare informatiedragers, worden gehouden.

Het is van belang op te merken dat tal van belangrijke functiescheidingen, alsmede beheers- en controleprocedures in algemene, zogenaamde systeemprogrammatuur zijn ondergebracht.

Het onderzoek van een informatiesysteem beperkt zich om bovenvermelde redenen niet tot de desbetreffende zogenaamde gebruikersomgeving, maar strekt zich uit tot in de automatiseringsorganisatie. De aandacht daarvoor wordt, in een doorlopend fungeren van de accountant, bepaald door het informatiesysteem waarvoor - uit een oogpunt van jaarrekeningcontrole - de paraplu-maatregelen het belangrijkst zijn.

Systeemonderzoeken worden vaak als een meerjarige cyclus opgezet. Daarin worden de resultaten van onderzoek naar algemene maatregelen, na update, steeds opnieuw gebruikt.
Het meerjarig gebruik van dossiers - ook door niet gespecialiseerde accountants - onderstreept het belang van een systematiek die de toegankelijkheid van onderzoekdocumentatie bevordert en van voorschriften betreffende:
- de wijze van beschrijven en vastleggen;
- het gebruik daarbij van vragenlijsten en andere formulieren;
- nummering en rangschikking van documenten;
- vermelding van datum, auteur, bron en dergelijke op documenten;
- datering, etc. van latere wijzigingen van en toevoegingen aan documenten.

In het volgende onderdeel wordt de automatisering van informatiesystemen nader beschouwd, opnieuw met de ogen van gebruikers en accountant, ten einde daaraan verdere elementen voor een systematiek van onderzoekdocumentatie te ontlenen.

4. Invloed van de automatiseringspraktijk op onderzoek en onderzoekdocumentatie

4.1 Het zicht van gebruikers en accountant op informatiesystemen

Toen er nog slechts sprake was van handwerk en mechanisatie in de gegevensverwerking maakten accountants voor het vastleggen van hun waarnemingen algemeen gebruik van route-, behandelings- en andere procedureschema's, als aanvulling op verbale beschrijvingen. Doel was het snel verkrijgen van duidelijke antwoorden op de "wat, wie, hoe en wanneer"-vragen, en vragen betreffende de interne controle in de meer enge en formele zin, zoals functiescheidingen, controles op volledigheid, juistheid, bevoegdheid en tijdigheid van primaire en financiële registraties. Beschrijvingen door de cliënt, zo al aanwezig, waren veelal ontoereikend.

Automatisering schakelt de menselijke tussenkomst uit en omvat de niet-vrije keuzehandelingen. Naast registratie vindt ook sturing van transacties en andere handelingen plaats. De stuurgegevens (normen) zijn voor programma's bereikbaar of daarin opgenomen. Andere normen, zoals prijzen en kortingpercentages, kunnen automatisch aan primaire vastleggingen van transactiegegevens worden toegevoegd.
Vele controles op de invoer, het verloop van het elektronisch verwerkingsproces, de raadpleging en mutering van gegevensverzamelingen, de uitvoer en het gebruik van bevoegdheden, zijn eveneens geautomatiseerd. Op basis van kennis van in programma's neergelegde functies, normen en controles is exact voorspelbaar wat bij een bepaalde invoer de inhoud van de uitvoer zal zijn.
Geautomatiseerde systemen zijn ten dele zelfdocumenterend.

Het denken van de (toekomstige) gebruikers van systemen richt zich op het specificeren van de in systemen te vervullen informatieverwerkingsfuncties ten behoeve van bedrijfs- en controlefuncties. De daaruit voortvloeiende beschrijvingen vormen het uitgangspunt voor ontwerp, bouw en documentatie. Na realisatie van een informatiesysteem, door specialisten, kan door zorgvuldig testen worden vastgesteld dat het systeem de uit de beoogde functies voortvloeiende taken werkelijk verricht. De betreffende procedures, herleid tot machinecode, worden aldus op indirecte wijze en als totaliteit waargenomen. Zolang in het dagelijks gebruik geen systeem- of programmafouten worden geconstateerd bepaalt de gebruiker zich veelal tot invoercontroles en daaraan gerelateerde, veelal overkoepelende, uitvoercontroles. Men kan dit typeren als een bewaking aan de grenzen van het systeem zoals zich dat aan de gebruiker voordoet. Dit onderstreept het belang van een goede test- en controledocumentatie.

De gebruikers van systemen, evenals de eigenaren en hun systeembeheerders, zijn genoodzaakt meer aan de automatiseringsorganisatie en het technisch beheer over te laten dan zij beseffen. In essentie komt dat neer op onbekendheid met functiescheidingen - en de handhaving daarvan tot in de computer - die voor het systeem van belang zijn.
Het management zal gebruikers de nodige waarborgen dienen te geven wat betreft interne controles, beveiligingen en continuïteitsvoorzieningen in de automatiseringsorganisatie. Zoals gezegd zal de gebruiker met de hoogste (door het management aanvaarde) eisen niveau-bepalend zijn.

De controle-accountant kan niet volstaan met het kennen van systeemfuncties en het beoordelen van visuele en geautomatiseerde controles. Verdergaande passende aandacht is - minstens - nodig voor functiescheidingen, zowel binnen het informatiesysteem als in de gebruikersorganisatie en de automatiseringsorganisatie.

De in de aanhef genoemde traditionele benadering blijft van belang bij het onderzoek van manuele trajecten, voornamelijk het zogenaamde voor- en natraject van een informatiesysteem. De aandacht voor functiescheidingen, volledigheid, juistheid, bevoegdheid en tijdigheid betreft evenwel het gehele systeem.

Wat continuïteit betreft zal de controlerend accountant veelal volstaan met de constatering dat aan de meest voor de hand liggende maatregelen is gedacht en dat de cliënt zich ook overigens bewust is van hetgeen nodig is om een calamiteit werkelijk te boven te komen.

4.2 Manco's en extra's in tests van informatiesystemen

De indirecte waarneming als hiervoor bedoeld, dat wil zeggen het door middel van gebruikerstests met een operationeel (verklaard) programma constateren, voor zover mogelijk, dat beoogde functies, controles en beveiligingen in een informatiesysteem zijn geïmplementeerd, vereist een vakkundig en uitputtend samengesteld geheel van proefgevallen. Door argeloosheid aan gebruikerszijde en tijddruk zijn tests vaak onvoldoende. Nog vaker worden latere verbeteringen en veranderingen in het systeem niet opgenomen in proefgevallen.
De omstandigheden van het onderzoek, bijvoorbeeld de reeds door gebruikers en accountant opgedane ervaring met het systeem, bepalen of laatstgenoemde zal overgaan tot een beoordeling en uitbreiding van de proefgevallen. Deze maken daarom niet steeds deel uit van de onderzoekdocumentatie.

Een onderzoek van uitgelijste programmastappen zal in het algemeen niet nodig zijn. Omdat in het algemeen na afsluiting van het onderzoek het dossier alleen documentatie zal bevatten met informatie die de accountant heeft gebruikt of later nog nodig kan hebben, zullen de desbetreffende lijsten (die overigens steeds op afroep naar de laatste toestand kunnen worden verkregen) veelal afwezig zijn.

Indien nodig kan een test, na toevoeging van speciale standaardprogrammatuur, uitwijzen of programmatakken niet zijn doorlopen. Zulks wijst dan op manco's in de test, op overtollige programmastappen en eventueel op onereuze bedoelingen.

4.3 De uitvoeringspraktijk van interne controle

Gebruikers voldoen doorgaans, ondersteund door geprogrammeerde invoercontroles, aan het principe van "schone" invoer. Op grond van de gedachte dat de elektronica zelden fouten maakt is daarentegen de visuele uitvoercontrole - helaas - vaak onderhevig aan slijtage.

Afgezien daarvan is de uitvoercontrole in vele gevallen niet zodanig dat bedieningsfouten en opzettelijke ingrepen, waarbij de volledigheid van de uitvoer niet lijkt te zijn aangetast, terstond aan het licht zullen komen.
Ook de gebruikerscontroles op de integriteit van gegevensverzamelingen zijn vaak ontoereikend te noemen, mede door een te geringe frequentie. Het betreft veelal totaalcontroles, waarbij opzettelijke verschuivingen binnen gegevensverzamelingen niet aan het licht zullen komen.
Het is mogelijk totaalcontroles toe te passen op de operationele programma's dat wil zeggen de machinecode zelve. Deze vinden evenwel weinig toepassing.

Uit het voorgaande blijkt opnieuw het belang van toereikende vormen van beheer, beveiliging en controle in de automatiseringsorganisatie voor het handhaven van de integriteit van de daarin behandelde en bewaarde gegevens, gegevensverzamelingen en programma's. De bevindingen ter zake, voor zover benodigd in jaarrekeningcontrole of operationeel onderzoek, dienen gezien de in onderdeel 3 genoemde complicerende factoren volgens een duidelijke systematiek te worden vastgelegd en gedocumenteerd.

4.4 De behandeling van uitzonderingsgevallen en correcties

Automatisering reduceert het aantal personen dat bij bedrijfshandelingen is betrokken. Daardoor komt in de manuele trajecten, waarin uitzonderingsgevallen, door programma's gesignaleerde posten (twijfelgevallen) en geweigerde posten (fouten) worden behandeld, vaak onvoldoende functiescheiding voor.
Invoer of herinvoer van reeds complete, nieuwe of gecorrigeerde gegevens zijn niet zelden van geprogrammeerde controle uitgezonderd en/of worden in invoer- en uitvoerverslagen niet van een speciaal kenmerk voorzien.
Het in programma's opnemen van uitzonderingsgevallen leidt ondanks hogere kosten van ontwikkeling en onderhoud niet steeds tot een correcte verwerking.
Als veel soorten twijfelgevallen worden gesignaleerd verslapt de aandacht voor signalen in de uitvoer.
Vastleggingen van de desbetreffende (manuele) trajecten vormen een belangrijk onderdeel van de onderzoekdocumentatie.

4.5 Compensaties van gebreken in interne controles

De in de bovengenoemde paragrafen vermelde voorbeelden van zwakke punten kunnen ertoe leiden dat in een (vervolg-) onderzoek de zogenaamde gebruikersomgeving in ogenschouw wordt genomen.

Daarbij gaat het niet alleen om de behandeling en controle in formele zin maar ook om het feitelijk gebruik van computeruitvoer in de bedrijfsvoering, bijsturing en managementcontrole. De achterliggende gedachte is dat bij een frequente uitvoer stelselmatige gebreken en ernstige fouten of ingrepen spoedig aan het licht zullen komen als die uitvoer wordt gebruikt door meerdere over grote bedrijfskennis beschikkende personen.
Een hoge frequentie vergt van de onderzoeker eventueel grotere aandacht voor het aspect tijdigheid en de daarop betrekking hebbende maatregelen. De accountant heeft er overigens belang bij dat overkoepelende controles, waarin verwerkingen over meerdere korte perioden tegelijk worden begrepen, niet zullen verdwijnen.
Een onderzoek als boven bedoeld kan zich uitstrekken tot meerdere afdelingen als elders in het bedrijf medegebruikers zijn van uitvoer en gegevensverzamelingen, eventueel in de vorm van een database. Daarbij kan worden nagegaan of in het zogenaamde gegevensbeheer alsmede het logisch en technisch beheer van databases, voldoende aandacht aan betrouwbaarheid wordt besteed (6). De genoemde onderzoekgebieden hebben hun plaats in de documentatiesystematiek.

Uit een en ander blijkt de noodzaak van een "vertaling" van bevindingen, met name als een gespecialiseerde onderzoeker niet tot het controle-team behoort, ten behoeve van gebruik in de jaarrekeningcontrole en aanpassing van het controleprogramma. In de desbetreffende bespreking wordt gebruik gemaakt van een beknopte samenvatting van zwakke punten en aangetroffen of mogelijk aanwezige compensaties en contrarollen. De samenvatting dient bruikbaar te zijn bij het schatten van controlerisico's. Het besprokene wordt in een gespreksnotitie samengevat.

Uiteraard zijn aan het begin gesprekken nodig. Als er onzekerheid is over de ratio van een onderzoek kan een korte oriëntatie plaatsvinden ten einde zicht te krijgen op de nut-kosten-verhouding van een onderzoek en op de wenselijke opdrachtformulering.

4.6 De functionele benadering van geautomatiseerde informatiesystemen

De onderstaande schets rondt de serie opmerkingen af.
Accountants zijn gewoon het bedrijfsgebeuren bij controle cliënten te benaderen in termen van de "grote" functies inkoop, produktie, verkoop, enzovoort. Zulks sluit goed aan bij het in 4.1 genoemde systeemdenken en kan leiden tot een eveneens functionele benadering van geautomatiseerde informatiesystemen. Daarin wordt na het beschrijven van functies en eigenschappen, in vrij abstracte termen, de aandacht gericht op de in bestuur en beheer toegepaste normen, de verantwoording over bestuur en beheer in relatie tot de normen, alsmede de op de verantwoordingsregistratie toegepaste controles, een en ander met een zoveel mogelijk voorbijgaan aan de uitvoering op het niveau van taken en procedures.

Uit de functiebeschrijvingen worden, in overeenstemming met belang en reikwijdte van het onderzoek, Soll-posities afgeleid van aan te treffen essentiële gegevens, beslissingen, beveiligingen en controles. De Ist-positie wordt geïnventariseerd aan de hand van invoer, uitvoer, gegevensverzamelingen (waarin ook normen), beslissingsschema's ten aanzien van normgebruik, overzichten van geprogrammeerde controles en voorschriften voor visuele controles. Van elk essentieel gegeven in de Soll-Ist vergelijking wordt de aanvaardbaarheid overwogen in termen van:

- eigenaar, beheerder en gebruikers van het gegeven of de groep gegevens;
- herkomst, bestemming en gebruiksdoel ervan;
- controle en beveiliging ervan. Bij afwijkingen wordt gelet op mogelijke schadelijke effecten. De beveiligingen en continuïteitsvoorzieningen vergen aanvullend onderzoek in de automatiseringsorganisatie c.q. een review welke onder meer de eventuele na een eerder onderzoek opgetreden veranderingen aan het licht zal brengen.

5. Vragenlijsten

De bespreking tot dusverre van elementen die de voornaamste inhoud en de daarop geënte systematiek van onderzoekdocumentaties bepalen, wordt thans afgerond met een korte beschouwing over de rol van vragenlijsten in onderzoek en dossiervorming.

Vragenlijsten zijn ontwikkeld uit checklists en lijsten met attentiepunten. Veel vragenlijsten laten dat duidelijk zien. Het zijn bevindingen.
Vragenlijsten kunnen ook evaluatievragen bevatten, bij voorkeur in een afzonderlijke rubriek.
In vragenlijsten zoals deze in de accountantspraktijk worden gebruikt vormen, veelal, korte antwoorden de basis voor een snelle oordeelsvorming.
De ruimte voor antwoorden kan bijvoorbeeld gaan van 3 kolommen voor "ja", "nee" en "niet van toepassing", tot veel wit voor het maken van notities: bevindingen, bronvermelding, verwijzing naar vindplaatsen in het dossier of de cliëntdocumentatie.
Vragenlijsten ondersteunen ook de review-arbeid, welke is gericht op het onderkennen van mogelijke na een eerder onderzoek opgetreden veranderingen.
Daartoe kan men antwoordkolommen toevoegen voor gebruik in volgende controlejaren.

Hoewel ja/nee antwoorden minder passen op evaluatievragen treft men deze laatste toch wel aan tussen inventarisatievragen door. Ook komt vermenging voor van inventarisatievragen betreffende veel voorkomende toepassingen met vragen inzake algemene maatregelen die voor alle toepassingen van betekenis zijn (paraplu-maatregelen).

De literatuur bevat veel voorbeelden van vragenlijsten. Sommige hebben een specifiek karakter (7)(8). De onderlinge verschillen kunnen aanzienlijk zijn. Tal van voorbeelden zijn van het gemengde type. De belangstelling voor dat type neemt toe wegens de invloed van het gebruik van werkstations en andere gespreide apparatuur in de financiële hoofd- en sub-administratie. De gemengde vragenlijst leent zich in ieder geval voor gebruik bij kleinere cliënten. De ingevulde vragenlijst vormt daar de kern van de onderzoekdocumentatie.

Losbladige vragenlijsten maken het mogelijk, de documentatie van het antwoord direct achter het blad dat de vraag bevat op te bergen. Het verdient echter de voorkeur belangrijke documenten op te bergen achter de indexbladen waarop zij staan ingeschreven.

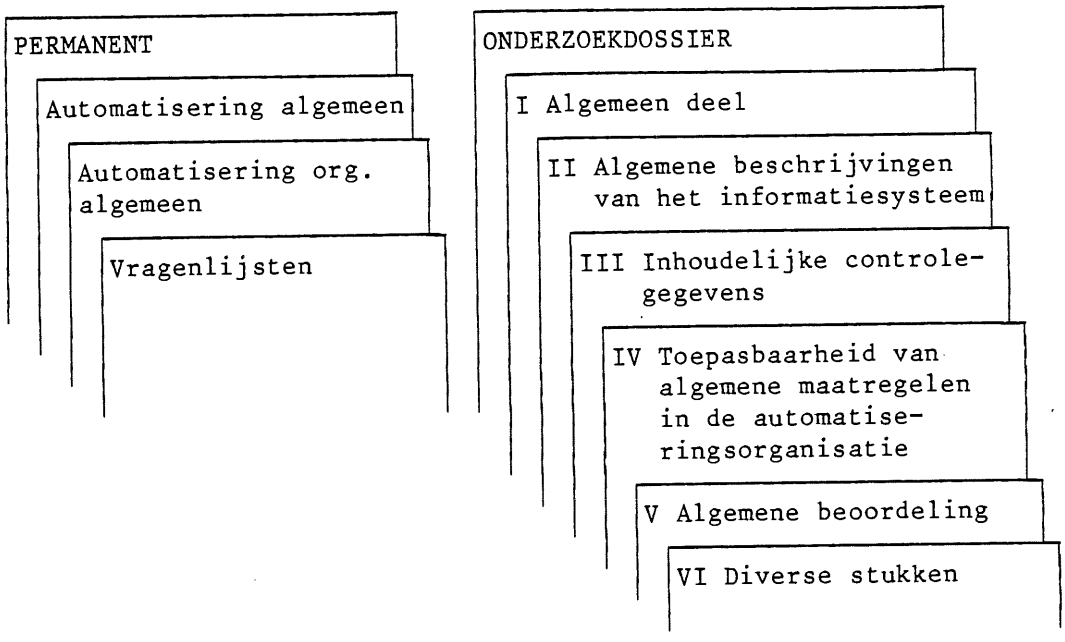
6. Systematiek van de onderzoekdocumentatie

De hierna tot slot gepresenteerde systematiek ligt in het verlengde van de voorgaande beschouwingen. Het betreft een voorbeeld in de vorm van een reeks namen van indexbladen, rubrieken en documenten c.q. zeer korte aanduidingen van de inhoud of strekking van documenten.
Een deel van de reeks behoort typisch bij een doorlopend fungeren in interne of externe EDP-audits en/of financiële controles.
Het stramien verwijst naar onderzoeken van in exploitatie zijnde geautomatiseerde informatiesystemen waarin men zich richt op het aspect betrouwbaarheid. In andere gevallen, bijvoorbeeld in onderzoeken naar doeltreffendheid en doelmatigheid, zullen aanvullingen op het hier aangeboden stramien nodig zijn.

In een doorlopend fungeren worden gegevens met lange werking opgenomen in permanente dossiers. Het voorbeeld noemt cliëntgerichte gegevens, algemene maatregelen in de automatiseringsorganisatie, en de verzameling van geautomatiseerde informatiesystemen.

Het onderzoekdossier in het voorbeeld houdt het midden tussen een permanent en een jaardossier (lopend dossier). De werking strekt zich uit over de (resterende) levensduur van het betreffende informatiesysteem. De in het systeemonderzoek nodige gegevens over algemene maatregelen in de automatisering, geldend voor meerdere of alle informatiesystemen, worden ontleend aan het permanente dossier.
Omgekeerd leidt vrijwel elk (systeem)onderzoek tot aanvulling of wijziging van gegevens in het permanente dossier.
Onder verwijzing naar onderdeel 3 wordt er wat betreft het opnieuw gebruiken van evaluaties van algemene maatregelen aan herinnerd, dat voorzichtigheid is geboden zolang geen onderzoek is ingesteld dat beantwoordt aan het informatiesysteem dat zowel uit het oogpunt van de cliënt als de accountant de zwaarste betrouwbaarheidseisen aan de automatiseringsorganisatie stelt.

Onderdeel van de systematiek is dat de namen van indices (in het achterstaande vetgedrukt) zullen staan in de kop van indexbladen, te zamen met naam en code van de cliënt. Achter voorgedrukte regels op indexbladen kan men door middel van een teken aangeven dat het betreffende onderdeel in het achterliggende is gedocumenteerd. Indexbladen dienen ruimte te laten voor met de hand geschreven aanvullingen. In de praktijk zal men op de plaats van de streepjes op indexbladen voorgedrukte nummers aantreffen. De nummers worden overgenomen op de achterliggende dossierstukken.



PERMANENT DOSSIER

Automatisering algemeen

- Deel van de considerans van het programma jaarrekeningcontrole dat betrekking heeft op administratieve organisatie en automatisering.
- Kerngegevens betreffende de cliënt.
- Organisatieschema van de cliënt. De voornaamste functionarissen.
- Korte historie van de automatisering bij de cliënt.
- Informatie- en automatiseringsbeleid. Informatie- en automatiseringsplan.
- Besturing: stuurgroep, projectorganisatie en -management.
- Overzicht van geautomatiseerde informatiesystemen (jaartal, type, programmeertaal e.d.).
  . korte omschrijving met vermelding van belang voor jaarrekeningcontrole en cliënt;
  . verrichte en geplande onderzoeken; verwijzingen naar dossiers;
  . rapportexemplaren.
- Notities en correspondentie met lange werking.
- Chronologische overzichten.
  . interne en externe rapportages en mededelingen; organisatiebrieven;
  . lijst van in het permanent dossier aangebrachte wijzigingen en toevoegingen.

Automatiseringsorganisatie algemeen

- Inhoudsopgave van automatiseringshandboek of vergelijkbare verzameling.
- Organisatie- en sterkteschema.
  . vervulling van vacatures.
- Overzicht van functionarissen en bevoegdheden.
  . tijdelijke en nevenfuncties.
- Overzicht van centraal beheerde apparatuur, per lokatie.
- Overzicht van decentraal beheerde apparatuur, per lokatie.
- Overzicht van data-lijnen, netwerken.
- Overzicht van systeemprogramma's en verdere algemene programmatuur;
  . opties in gebruik/niet in gebruik.
- Overzicht van beveiligingen tegen verkeerd gebruik en misbruik in toepassingen, met behulp van eigenschappen van hardware en programmatuur (harde software):
  . centrale apparatuur;
  . algemene programmatuur;
  . bibliotheken van toepassingsprogramma's en gegevensverzamelingen;
  . niet programmeerbare stations;
  . programmeerbare stations;
  . overige apparatuur op of bij de werkplek;
  . data-lijnen, netwerken.

Vragenlijsten
betreffende algemene maatregelen voor betrouwbaarheid van de informatieverzorging als geheel.
(Typering van de voornaamste onderwerpen en aandachtspunten die in vragenlijsten, ten gebruike in grotere automatiseringsorganisaties, plegen te worden genoemd.)

- Functiescheiding tussen en binnen delen van de automatiseringsorganisatie; neutraliteit ten opzichte van overige bedrijfsfuncties (beschikking, bewaring, registratie).
- Ontwikkeling en onderhoud van toepassingen:
  . voorschriften en richtlijnen, mede betreffende documentatie;
  . beveiliging van documentatie, per lokatie, tegen verlies en inzage door onbevoegden;
  . test-, acceptatie- en autorisatieprocedures.
- Logisch beheer van gegevens en databases.
- Intermediair beheer van aan functionarissen toegekende rechten ten aanzien van toegang tot apparatuur, programma's en gegevensverzamelingen.
- Voorbereiding van computerverwerkingen (machine-planning; ontvangst van invoermateriaal; bereikbaar maken programma's en gegevensverzamelingen).
- Computer-operating:
  . voorbehouden aan operators; ondersteund door toegangsverbod;
  . vernietiging van niet bruikbare papieren uitvoer.
- Controle op het verwerkingsproces; uitvoercontrole volgens voorschrift van de gebruikers:
  . gebruik controleregisters.
- Nabewerking (decarboniseren, snijden); distribueren uitvoer.
- Beheer van files (afzonderlijk voor programma's, gegevensverzamelingen, wachtwoorden en dergelijke, overige tabellen, onder meer voor karweibesturing en gebruiksrechten):
  . afzonderlijk voor toepassingsprogramma's en overige programmatuur (systeemprogrammering);
  . afzonderlijk voor test en produktie.
- Bewaring van files en, afzonderlijk, van bronprogramma's.
- Technisch beheer van databases.
- Beheer van datacommunicatielijnen, netwerken, on-line-apparatuur, gespreide apparatuur:
  . beperkingen in beschikbaarheid, openstelling en gebruiksmogelijkheden.
- Automatiseringsmanagement:

  "dagelijks", naast leiding en toezicht:
  . beoordeling van aanbod van nieuwe systemen, wijzigingen en incidenteel werk;

. inzien van logs en andere produktie- en beheersregistraties, annex controle op volledigheid van de registratie;
. vergelijking met machine-planning; natrekken van trouble shooting, ongeautoriseerde handelingen en bijzondere voorvallen.

"periodiek"
. reviews, steekproefsgewijze volgen van audit trails in automatiseringsregistraties;
. doorberekening aan gebruikers (tevens controlemiddel);
. fysieke en andere inventarisaties ter vastlegging van aanwezigheid van files, signalering van overtolligheid, controle op bewaartermijnen.

- Fysieke beveiliging; continuïteitsvoorzieningen:
  . risico-management;
  . risico-analyses door de cliënt;
  . back-up en uitwijk; tests van de voorzieningen.

Evaluatie van bevindingen volgens de vragenlijst.

Evaluatie van de invloed van nadien opgetreden wijzigingen.

ONDERZOEKDOSSIER
Betreffend: (naam informatiesysteem).

I. Algemeen deel

- Opdracht (intern of extern): voorbespreking, oriëntatie, review, formulering.
- Tijd- en werkplan; namen van uitvoerders; urenverantwoording; chronologische aantekeningen van interviews en belangrijke momenten.
- Belangrijke correspondentie en gespreksnotities.
- Gebruikte rapporten van cliënt of derden.
- Verslagen van besprekingen met opdrachtleider, leider controleteam jaarrekeningcontrole.
- Exemplaar van rapport of mededeling inzake het onderzoek; uittreksels van organisatiebrieven.
- Beknopt overzicht van belangrijke zwakke punten en onzekerheden; contra-rollen en andere compensaties.
- Chronologische lijst van na het onderzoek opgetreden belangrijke wijzigingen.

II. Algemene beschrijving van het informatiesysteem

- Beknopte typering en beschrijving; structuurschema; relatie of koppeling met andere informatiesystemen; belang voor de cliënt en de jaarrekeningcontrole; herkomst; jaar van ingebruikneming.
- Functionele beschrijving.
- Runcharts met aanduiding frequentie, programmanummers en -versies, bestandsnamen; korte programmabeschrijving of typering; gebruikte programmeertalen; gebruikte apparatuur en stations; lokaties.
- Systeembeheer aan gebruikerszijde; contactpersonen.
- Beheer en aanpassing van proefgevallen ten behoeve van nieuwe tests.
- Evaluatie van de documentatie bij de cliënt.
- Evaluatie van de eindtest en acceptatie; aandeel daarin van de gebruiker.
- Modellen:
  - intoetsconcepten; invoer- en foutlijsten;
  - overige gedrukte uitvoer en uitzonderingsrapportage (exception reporting);
  - beeldscherm-sequenties en -indelingen;
  - logische records in gegevensverzamelingen.

III. Inhoudelijke en controlegegevens

- Transactiesoorten, codestelsels, normen, parameters.
- Functionarissen in de gebruikersomgeving.
- Bevoegdheden in autorisatie, controles, aan stations, in vaststelling en invoer van normen en dergelijke.
- Uitvoerdistributieschema (namen, gebruiksdoelen).
- Belangrijke gegevensverzamelingen; bestandsorganisatie.
- Geprogrammeerde controles; signaleringen en foutmeldingen op gedrukte uitvoer, op beeldscherm:
  . toegepast op postgewijze of stapelsgewijze invoer;
  . herhaling van controle bij (uitgestelde) mutatie van gegevensverzamelingen.
- Overige belangrijke beslissingen (beslissingsschema's).
- Belangrijke in programma's gegenereerde gegevens.
- Belangrijke regels.
- Handelingen en controles in data-collectie en invoervoorbereiding.
- Controle op omzetting in machinaal leesbaar schrift.
- Visuele invoer- en uitvoercontroles:
  . in de automatiseringsorganisatie;
  . in de gebruikersomgeving.
- Geprogrammeerde en visuele controle op integriteit van gegevensverzamelingen.
- Behandeling van uitzonderingsgevallen en correcties:
  . manueel, aan werkstation (opheffing van blokkering en/of signalering); gebruik suspense account/verschillenrekening;
  . signalering van onvoltooide transacties en sessies aan werkstations;
  . wijziging achteraf van reeds geaccepteerde of verwerkte invoer (in wachtbestand, in historiebestand).

IV. Toepasbaarheid van algemene maatregelen in de automatiserings-organisatie

- Gebruik en effect van standaard- en optionele beveiligingen in hardware en programmatuur, vermeld in het permanent dossier; eventuele toevoegingen (ten behoeve van de onderzochte applicatie) aan hardware en/of programmatuur:
  . bevoegdheidscontrole (wachtwoorden en dergelijke);
  . blokkering van werkstation of console na ongeldig wachtwoord of dergelijke.

- Toereikendheid van verdere algemene maatregelen; eventuele toevoegingen ten behoeve van de applicatie en in applicatieprogramma's:
  . functiescheidingen;
  . menu-beveiliging;
  . bescherming van normen, wachtwoorden en dergelijke tegen onbevoegd muteren;
  . periode-overzicht van bestandsraadplegingen en andere activiteiten aan werkstations, ten dienste van de beheerder van stations;
  . bewaartermijnen;
  . controle na recovery en reconstructie van gegevensverzamelingen.

- Fysieke beveiligingen; continuïteitsvoorzieningen.

V. Algemene beoordeling

- Overzichten van kritische gegevens in de invoer, uitvoer, blijvende gegevensverzamelingen, programmatabellen en dergelijke (constanten, semi-constanten, variabelen); schema's en sub-schema's van databases:
  . naam van het gegeven of groep van gegevens;
  . definitie;
  . herkomst en bestemming; relatie met transactiesoorten en gegevensverzamelingen;
  . verantwoordelijke eigenaar of gedelegeerde (invoer, muteren, annuleren);
  . bevoegde gebruikers (raadpleging), gebruiksdoelen;
  . betrouwbaarheidsindicaties.

- Audit trail.

- Schema van controles op kritische momenten en omspannende controles.

- Evaluatie.

- Overzicht van zwakke punten en compensaties.

VI Diverse stukken

- Correspondentie.
- Gespreknotities.
- Aantekenbladen met vermelding van beslissingen van de opdrachtleider.
- Overige werkpapieren.

LITERATUURLIJST

1. Accountant en elektronische informatieverwerking, door prof. D. Steeman (onderdeel III.300 van het Handboek Accountancy '84).

2. EDP Audit door J.H. Urbanus en J.M. Verheul (onderdeel ... van het Handboek Accountancy '84).

3. Vastlegging van verrichte accountantswerkzaamheden Meningsuiting 4, september 1982, NIvRA-bundel RADAR.

4. Documentatie van automatiseringsprojecten. NIvRA-geschrift nr. 33, 1984.

5. Documentatie van automatiseringsprojecten, door drs. H.A. Kampert RA, in de Accountant, februari 1985.

6. Data Base & Accountant, red. A.H.C. Koedijk Uitgave Samsom, tweede druk 1985.

7. Checklist ter beoordeling van (standaard) toepassingsprogrammatuur voor de financiële administratie op small-business computers (rapport van de werkgroep Small Systems van de Userclub, 1980).

8. Accountant en computer servicebureaus. NIvRA-geschrift nr. 16, 1976.

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

LEZERS REAGEREN

H. de Jong reageert op het artikel "Vierde generatietalen" (zie COMPACT 85/2 nummer 38 pagina 67 en volgende).

Voorzover in het artikel van drs. J.E. Huizenga de indruk zou zijn ontstaan dat 4GL's eigenlijk nog nauwelijks zijn toegepast, geeft H. de Jong als zijn ervaring dat de toepassingen van SQL-QIT voor microcomputers reeds werkelijkheid is geworden. Deze 4GL voor micro's voldoet aan de karakteristiek van 4GL's (zie Compact 85/2 pagina 69).

Laten we nu H. de Jong aan het woord.

COMPACT

Zomer/Herfst 1985

VIERDE GENERATIETALEN, een gebruikerservaring met micro's

door Hans de Jong, Queensland Computer Quality Consultancy, Brisbane
vh Consultant bij Klynveld Kraayenhof & Co.,
Management Advisery Services Amsterdam.

IBM in USA, aansluitend op het baanbrekend werk van dr. Ted Codd, ontwikkelde in 1982 SQL (Structured Query Language) een 4GL gebaseerd op een real relational database-model en een zeer gebruikersvriendelijke opvraagtaal. Deze SQL was bedoeld en wordt sinds 1983 gebruikt door grote mainframe centra waar de terminals ten dienste van eindgebruikers van SQL worden voorzien. Ook binnen grote rekencentra worden SQL-modules te zamen met COBOL gebruikt om meer efficiënte retrievalprogramma's te kunnen schrijven.
Met dit doel voor ogen is IBM SQL slechts mogelijk via een samenwerking met de in de mainframe voorhanden hostlanguage bijvoorbeeld COBOL.

In 1983 slaagde een internationale research-groep in de Universiteit van Queensland er onder leiding van de alom bekende prof. S. Nijssen in, IBM SQL in een vrijwel 100% compatibele vorm te realiseren voor gebruik op een grotere microcomputer. Zelfs de manuals van IBM SQL konden zonder afwijkingen voor deze micro-SQL worden gehanteerd.
SQL-QIT werd daarna uitvoerig beproefd en in 1984 werd door schrijver de eerste commerciële toepassing ontworpen, geïmplementeerd, geïnstalleerd op een IBM-PC en na uitvoerig testen en instructies door de gebruikers operationeel gestart na circa 6 maanden.
Het betrof hier een inkoopcombinatie van 400 fruit-farmers, die voor gezamenlijke rekening een eigen warenhuis met ongeveer 4000 artikelen exploiteren. Het doel was de volledig handmatige administratie met de computer af te handelen met als hoofddoel een directe on-line transactiegewijze verkoopregistratie met factureren en een geïntegreerde inkoop-, voorraad- en orderadministratie.
De IBM-PC werd uitgerust met twee printers waardoor op elk gewenst moment de "klant" direct een factuur kon krijgen aan de verkoopbalie.
Het bedrijf had ongeveer 200 leveranciers en enige honderden orderregels per dag. Uiteraard moest ook de periodieke voorraadopname worden verwerkt. Daarnaast was de wens het kasboek, de debiteuren en een "shareholders"-administratie met de winstverdeling in het systeem op te nemen. Ten einde de kleine staf van personeel niet te zwaar te belasten met nieuwe zaken, was de eis dat alle procedures zo veel mogelijk gelijk zouden blijven; de hoofdreden om te kiezen voor een "tailormade"-oplossing en geen standaardpakketten.
Samenvattend een heel scala van toepassingen en nogal ambitieus voor een "first time user", waar een gelukkige omstandigheid was, dat de manager bijzonder ervaren was.

Dit laatste resulteerde in een systeembeschrijving binnen 2 weken. Aangezien een relationele database veel kenmerken heeft van de klassieke kaartenbak was het ontwerp van de database twee weken daarna gereed, zodat na een maand met de programmering kon worden gestart. Met een tempo van ongeveer een programma per dag werden de ruim 80 applicaties in ongeveer 3 maanden geïmplementeerd en daarna getest. Voor de omvangrijke operatie van de conversie van alle gegevens van kaarten en boeken naar de database werd van de tussenweg via dBASE II gebruik gemaakt op een kleine micro in eenvoudige tabellen.
Hierdoor kon de IBM-PC voor het vullen met de informatie vrij blijven voor test en wijzigingen en kon de definitieve database in zeer korte tijd worden geladen.
Al ras bleek bij de programmering dat enkele complexe rapporten en de validatie bij de verkoopinvoer (voorraad voldoende) niet in standaard SQL te realiseren was, zodat het research-team ijlings extra hulpmiddelen aandroeg voor de acties.
Daardoor werd SQL-QIT tot een volwassen product en minder afhankelijk van een host-taal dan big brother's-versie.
Het resultaat was dat na ongeveer 6 maanden het systeem operationeel werd overgedragen en sindsdien is er nauwelijks enige professionele assistentie bij de gebruikers nodig geweest, hoewel de toepassing door henzelf wel is aangepast.
Na deze eerste praktijkervaring is SQL-QIT verder uitgebouwd en vervolmaakt en nu in gebruik op honderden microcomputers in Australië, USA en Europa.
Na de eerste toepassing werd schrijver verzocht in maart jl. een SQL-applicatie voor een NEC APC III-microcomputer te ontwikkelen voor een geïntegreerde orderregistratie en verkoopstatistiek met facturering voor een advertentiebureau.
Het aantal orders was ongeveer 1000 per maand en de statistiek moest worden gebouwd rond 300 cliënten, 120 agenten, 200 media en 5 mediagroepen. De cijfers moesten kwantiteiten, totale omzet, provisie en budgetten bevatten ook voor het vergelijken met vorig jaar.
Uit de offertes bleek dat een oplossing in dBASE III nauwelijks te realiseren was en meer dan tweemaal zoveel tijd zou kosten.
De implementatie in SQL-QIT geschiedde en in de recordtijd van twee maanden werd èn de database (36 tables, 424 kolommen) èn de programmatuur (56 routines) getest opgeleverd. Na twee maanden schaduwdraaien is het systeem nu volledig zelfstandig.
Ook hier was er sprake van een "first time user" en werd de operationele werkwijze vrijwel geheel in dezelfde staat gehandhaafd, hetgeen groot voordeel had in de schaduwperiode tijdens het vergelijken oud/nieuw.
Wezenlijk is bij dit systeem dat de directeur en de verkopers nogal ongebruikelijke opvragingen uit het systeem willen en kunnen realiseren na een zeer korte instructie.
Geënt op de succesvolle KKC-video in 1983 zijn door mij dan ook 2 video tapes geproduceerd met een inleiding en een complete cursus SQL.

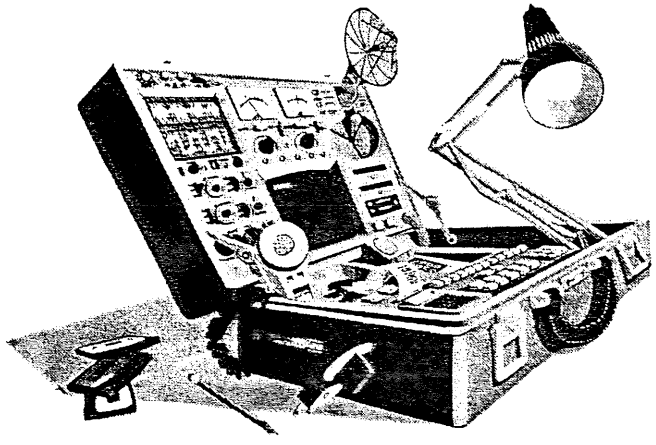
Vooral in dit land waar de afstanden tussen steden zijn te vergelijken met die tussen Amsterdam en Stockholm of Amsterdam en Gibraltar blijkt dit een goed instructiemiddel.

Het leek schrijver nuttig als een aanvulling op het artikel van Jur Huizenga dat nogal in de toekomst werd geschreven alsof 4 GL's pas voor de deur stonden, uit het verre Australië aan de oud collegae te laten weten dat hier al veel met 4 GL is gerealiseerd vooral met micro's.
Van het genoemde SQL-QIT zijn op Sperry micro's in Highschools in Queensland al 35 systemen operationeel en honderden besteld. Er is erg veel belangstelling ook vanuit Australische en Amerikaanse accountants en een van deze multinationals is schrijvers volgende afnemer, vooral geïnspireerd door machine-onafhankelijkheid en de nu beschikbare multi-user-versies. Ook het in het vooruitzicht gestelde drastisch vereenvoudigen van programmering en het onderhoud daarvan maakt in de praktijk de toepassing veel minder star dan voorheen.
Schrijver is erin geslaagd zijn applicaties bovendien volledig zelfdocumenterend te maken inclusief cross-references waardoor de beschrijvingen na wijziging in programma's direct in de documentatie kunnen worden opgenomen.
Voor de technisch geïnteresseerde lezer nog het volgende:
Minimum hardware 16bits micro, 640k memory, 10M harddisk, PCDOS, MSDOS, UNIX.
Educational version: 512k + 2 x 360k floppy.
Apparatuur thans (?): IBM-PC, Sperry micro's, NEC APC III, NCR TOWER, Burroughs B25, SIRIUS, Olivetti M24, Tandy 1000, IBM-compatibles, Altos, etc.
Security: dezelfde faciliteiten als IBM SQL voor back-up, rollback, commit, logging and automatic recovery, evenals passwordbeveiligingen op gewenst niveau.

Helaas is er hier vrijwel geen informatie over SQL-gebruik in Nederland; willen Nederlandse SQL-users reageren of meer weten?
Vragen, opmerkingen aan redactie of schrijver:
PO Box 232
CAPALABA 4157
Australia

Tenslotte nog een "variant" op het grapje van Jur: Laat op al het computerpapier voordrukken: "PAS OP, COMPUTERAFDRUK, KAN DUS ONBETROUWBAAR ZIJN".
Uiteindelijk is computercrime bedacht door professionele programmeurs en niet door de eindgebruikers.

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



DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

Dit maal wil ik in deze rubriek Uw aandacht vragen voor een fenomeen, dat de laatste jaren enorm aan "populariteit" heeft gewonnen en mijns inziens van de moderne EDP-auditor enige aandacht verdient. Ik doel hier op het "hacken": het inbreken in computersystemen via het openbare telefoonnet door mensen met huis- of microcomputers.
In deze editie een eerste aanzet tot kennismaking met het hacken in de vorm van een uitgebreide boekbespreking.
In volgende uitgaven zal ik wat dieper ingaan op de gevaren, verbonden aan de mogelijkheid van toegang tot een computersysteem via het openbare telefoonnet.

"The Hackers Handbook" by Hugo Cornwall (149 bladzijden).

Inleiding

Het steeds verder afnemen van de kosten van microcomputers en communicatiemiddelen heeft tot gevolg dat het "hacken" steeds eenvoudiger en goedkoper werd.
Geïnspireerd door de film "Wargames", waarin kinderen met hun huiscomputer toegang weten te krijgen tot het meest beveiligde deel van de Pentagon Computers, hebben duizenden mensen over de hele wereld hun computer op het openbare telefoonnet aangesloten om vervolgens aansluiting te zoeken met andere computersystemen; niet met het doel om een derde wereldoorlog te ontketenen, zoals dat in de film bijna gebeurde, maar simpel om het plezier en het bevredigen van de nieuwsgierigheid.
Dit boek brengt de leerling-hacker de beginselen van het vak bij, zoals: welke apparatuur hij nodig heeft, hoe een modem werkt en verschillende lijsten met telefoonnummers van allerlei computersystemen.

Andere onderwerpen, die in dit boek behandeld worden, zijn:
- wachtwoorden, en hoe ze kunnen worden achterhaald;
- wat moet je doen als je niet weet met welk type computer je verbinding hebt;
- toegang tot afgeschermde delen van computersystemen;
- hacken met behulp van een korte golf ontvanger.

Samenvatting

In de introductie wijst de schrijver er met nadruk op dat hackers, zoals de personen genoemd worden die met behulp van hun microcomputer en een modem inbreken*) in andere computersystemen, geenszins misdadigers zijn.

Het oogmerk van de hacker is slechts te proberen zoveel mogelijk uit te vinden over het lijdend voorwerp, en om er zover mogelijk in door te dringen. Geenszins, benadrukt de schrijver, is het de bedoeling van de hacker om zodanige wijzigingen in het computersysteem aan te brengen, dat hij er zelf beter van wordt, of de eigenaar slechter.

In het eerste hoofdstuk wordt geadviseerd welke apparatuur nodig is om te kunnen hacken en welke hardware en software handig is om beschikbaar te hebben.
Vervolgens wordt de leerling-hacker de beginselen bijgebracht van datacommunicatie. De historie van de datacommunicatie en de meest gebruikte protocollen passeren de revu.
In hoofdstuk 3 wordt dieper ingegaan op de technieken. Besproken worden de criteria waaraan de computer van de hacker dient te voldoen. De vereiste communicatiepoort wordt gedefinieerd, en ook worden de eisen vermeld waaraan het terminal-emulatieprogramma moet voldoen alvorens het gebruikt kan worden om in te breken.
Tot slot wordt in dit hoofdstuk de benodigde modem besproken, het apparaat dat de microcomputer aan het telefoonnet moet verbinden.

On-line hostcomputers, waarin voornamelijk bibliografische informatie was opgeslagen, vormden de categorie computers, die als eerste door het hackfenomeen werd getroffen.
Vervolgens werden ook nieuwsdiensten, financiele diensten als Wall Street en Reuters door de hackers ontdekt, gevolgd door universiteitscomputers, banken en verzekeringsmaatschappijen, electronische postbusdiensten en regeringscomputers.
De aktieve hacker dient te beschikken over enige apparatuur en programmatuur maar daarnaast en vooral over zeeën van tijd. Aan het hacken ligt namelijk diepgaand onderzoek ten grondslag. Informatie over potentiele slachtoffer-computers dient zorgvuldig te worden gezocht en beoordeeld.

*) Onder de nieuwe wetgeving zullen deze handelingen volgens de wet strafbaar kunnen worden gesteld. (Zie onder Actualiteiten in deze Compact over de Installatie van de Commissie Franken.)

Het overgrote deel van deze informatie is te vinden in telefoonboeken, kranten en tijdschriften en andere publikaties, maar ook op buro's, verlaten tijdens de lunchpauzes, of op afgelegde computeroutput.
De verkregen informatie gecombineerd met een dosis gezond verstand kan vaak voldoende zijn om tot de aanval over te gaan.
Maar de grootste bron van informatie vormen wel de Bulletin Boards. Dit zijn informatiediensten in de vorm van geautomatiseerde prikborden, waarmee hackers verbinding kunnen krijgen via het openbare telefoonnet en waarop zij gegevens over hackpogingen kunnen achterlaten voor collega-hackers, en waarvan zij zelf hun informatie kunnen betrekken.
Enkele voorbeelden van conversaties tussen hackers via zo'n Bulletin Board zijn in het boek opgenomen en geven een overduidelijke indruk hoe waardevol de informatie op dergelijke boards kan zijn. Informatie varieert van een user-id en password, die bleken toegang te bieden tot een bepaald computersysteem, tot een electronische schakeling met behulp waarvan het mogelijk is om kosteloos te bellen naar welke computer dan ook over de gehele wereld!

Speciale aandacht wordt geschonken aan het bedenken van passwords; de meest gebruikte wachtwoorden zijn opgesomd, maar daarnaast wordt een aantal hints gegeven, zoals het leren kennen van de gebruiker, wiens user-id als ingang voor de hack gebruikt gaat worden. Zo zijn de door militairen meest gebruikte wachtwoorden FEARLESS, VALIANT en TOPDOG, terwijl tuinders het woord CLEMATIS zeer regelmatig gebruiken.

Een inleiding in de verschillende typen netwerken wordt afgesloten met een lijst van de meest bekende netwerken in Groot Brittannie, inclusief telefoonnummers en protocolspecificaties, en een extractie uit de ellenlange conversaties met het besloten packetswitching netwerk SERCNET, dat aansluiting geeft met alle universiteiten in de UK, maar tevens sluizen (gateways) heeft naar onder meer het CERN in Zwitserland.
Uitgebreide aandacht krijgt het Engelse Viewdata systeem, dat allerlei diensten biedt. Zowel technische als de gebruikersaspecten worden belicht, doorspekt met verslagen van succesvolle hacks.
In het kort wordt de lezer ingelicht over de toe te passen technieken wanneer de hackerij gegevens betreft die via de radiofrekwenties worden gezonden. Een zeer eenvoudig hulpmiddel hierbij is de radiocassette-recorder, waarmee de afgeluisterde signalen direct op cassette kunnen worden vastgelegd. In dit geval is het hacken in feite niet meer dan afluisteren en ontcijferen van de verzonden gegevens.

Tot op heden speelt hacking nog slechts een ondergeschikte rol, wanneer we kijken naar de verschillende soorten van computermisdaad. Schattingen melden dat niet meer dan 3 procent van de computermisdaden via hackerstechnieken zijn uitgevoerd.

De computer security consultant vormt een gevaar voor de hacker, terwijl het hacken sterk wordt bemoeilijkt doordat in de modernere besturingssystemen meer en meer beveiligingsmaatregelen zijn opgenomen.
We staan echter aan het begin van het communicatietijdperk; meer en meer computersystemen worden aangesloten op openbare netwerken of direct op het telefoonnet, en meer en meer managers willen op afstand een verbinding hebben met hun computersysteem.
En hoewel de beveiligingsmaatregelen meegroeien en het de hacker moeilijker en moeilijker zullen maken om in te breken, zal de uitdaging voor deze toegewijde hobbyisten alleen maar groter worden.

Appendices

In een zevental appendices is kort en bondig een serie richtlijnen en informatie opgenomen met betrekking tot de volgende zaken:

I Trouble shooting; handige tips wanneer de koppeling met de host-computer niet zondermeer wil lukken.

II Een uitgebreide termenlijst, waarin de meeste termen uit de hackerswereld staan uitgelegd.

III Een overzicht van de standaards op het gebied van datacommunicatie van het CCITT.

IV Een uitgebreide beschrijving van de vier meest voorkomende computeralfabetten, te weten ASCII, Baudot (telex), Viewdata en EBCDIC (IBM).

V Een overzicht van de meest voorkomende communicatieprotokollen, die de hacker op zijn tocht zal tegen komen.

VI Een volgend overzicht geeft inzicht in de verschillende banden in het radiospectrum, die gebruikt (kunnen) worden voor gegevensverkeer.

VII Tot slot krijgt de hacker een uitgewerkt schema, waaruit hij kan lezen, op welke wijze het mogelijk wordt om een lange reeks van telefoonnummers automatisch af te werken, op zoek naar een computerverbinding.

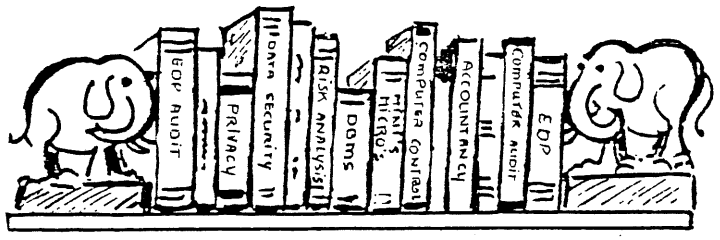
Commentaar

Opgemerkt dient te worden dat de schrijver meldt dat de in dit boek vermelde informatie over specifieke hacks momenteel niet meer waardevol is, omdat in alle gevallen de beveiligingen zouden zijn verbeterd. Aangenomen dat dat inderdaad het geval is, betekent dit niettemin dat de methoden en technieken dermate algemeen en grondig worden besproken dat ze op vele computersystemen van toepassing zullen blijken te zijn.
De schrijver vertelt door het hele boek over zijn eigen ervaringen als hacker en over de ervaringen van anderen. Vele "hacks" hebben betrekking op apparatuur van British Telecom, de Britse PTT.
Hij heeft veel contacten met de Britse hackerwereld, waardoor hij kans heeft gezien een grote hoeveelheid "inside" informatie te bemachtigen.

Naar mijn persoonlijke mening is de schrijver tamelijk naief door te veronderstellen dat momenteel slechts eerlijke hackers het hackerspad bewandelen.
Er zijn wellicht evenveel hackers met minder eerlijke bedoelingen, maar evenmin moet worden vergeten dat de "goede" hacker de "kwade" helpt door hackersinformatie op bulletinboards te vermelden!

Tot slot wil ik opmerken dat het boekje voor iedereen, die een beetje handig begint te worden met zijn microcomputer, het lezen ruimschoots waard is.

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



Boeken

Titel: Inleiding Relationele Databases
Auteurs: A. Mayne/M. Wood
Uitgever: Samsom 1985
Omvang: 198 pagina's
Boekbespreking door J.A.W. Winterink

Relationele databases zijn in enkele jaren zeer populair geworden. Het gigantische aanbod van database-pakketten voor de personal computer spreekt wat dat betreft voor zich. De meeste van deze pakketten worden bestempeld als "relationeel" maar slechts weinigen weten wat deze mysterieuze term precies inhoudt.

Het boek INLEIDING RELATIONELE DATABASES onthult het mysterie. Op een heldere wijze wordt een beschrijving gegeven van de onderliggende concepten en van de diverse benaderingen van het relationele ideaal. Bij de behandeling van de relationele talen worden, naast duidelijke voorbeelden, beschrijvingen van structurerings- en modelleringsfaciliteiten gegeven. Aandacht krijgen: sleutels en normalisatie, gegevensonafhankelijkheid, toegangscontrole, integriteit en herstelfuncties.

Tenslotte komen de meest populaire pakketsoorten met hun specifieke kenmerken aan bod:
- SQL;
- QBE;
- Ingres;
- Oracle;
- dBase III.

Hierna zal kort op de inhoud van het boek worden ingegaan.

Deel 1

1. Relationele database-concepten

In dit hoofdstuk wordt ingegaan op het basisconcept in relationele systemen. Het basisconcept is de tabel.

Wil een database-systeem relationeel zijn dan moet er aan een aantal simpele regels voldaan zijn, welke zijn afgeleid uit een wiskundige theorie, die voor een solide theoretische fundering zorg draagt. Deze basisregels worden oppervlakkig behandeld.

Na aandacht te hebben besteed aan de gegevens, wordt er naar de verwerkingsfaciliteiten van relationele systemen gekeken. Ingegaan wordt op de basis relationele operatoren (selecteren/projecteren/verbinden). Het resultaat van deze operatoren is altijd een nieuwe tabel.

Tot slot wordt in het hoofdstuk nog kort ingegaan op de ongebruikelijke terminologie over relationele systemen.

2. Relationele talen

Relationele talen zijn, met behulp van verschillende programmeertalen, op veel verschillende manieren geïmplementeerd.
De rijke variëteit die deze talen bieden, is in het boek in een drietal belangrijke groepen ingedeeld:
- relationele algebra;
- relationele berekeningstalen;
- vraag- en schermtalen.

In een aantal paragrafen worden vervolgens in abstracto een aantal verschillende relationele talen onderzocht om te zien hoe ze conceptueel werken. Wat er wordt beschreven is meer bedoeld als illustratie dan als een specificatie van een of ander bestaand systeem. Dit draagt bij aan de eenvoud.

3. Sleutels en normalisatie

Bij de gegevensverwerking dienen sleutels om records te identificeren, zodat er aan gerefereerd kan worden of zodat ze benaderd kunnen worden. Sleutel en sleutelwaarde zijn fundamentele begrippen uit de gegevensverwerking. Het zal daarom duidelijk zijn dat binnen de relationele benadering, faciliteiten moeten bestaan om met sleutels te kunnen werken. In feite hebben relationele systemen speciale regels ten aanzien van sleutels.
Deze worden in dit hoofdstuk behandeld.

Ook wordt aandacht besteed aan normalisatie. Normalisatie is een techniek die ontwikkeld is om ervoor te zorgen dat een gegevensstructuur efficiënt is. Die gegevensstructuur kan op verschillende manieren gemodelleerd worden. Het relationele model is zo'n manier. Achtereenvolgens wordt ingegaan op:
- de voordelen van normalisatie;
- de basisprincipes van normalisatie;
- de praktijk van het normaliseren.

4. Logische structurering en data-onafhankelijkheid

Een database is een verzameling van gegevens, die op een zodanige wijze is georganiseerd, dat aan elke behoefte aan gegevens van de gebruiker voldaan kan worden. Een relationele database is een van de vormen van database-organisatie (andere zijn de netwerkbenadering en de hiërarchische benadering).
Een database management-systeem (DBMS) is een verzameling van algemeen toepasbare programma's die voor alle gebruikers de toegang verzorgt en voor het toevoegen, het wijzigen en het opzoeken van gegevens, gecontroleerd gebruik realiseert.
Bovendien zijn faciliteiten beschikbaar voor data-onafhankelijkheid, integriteit en beveiliging.

Een DBMS moet de juiste faciliteiten verschaffen om deze doelstellingen te ondersteunen. In dit hoofdstuk worden twee aspecten van die ondersteuning behandeld: data-onafhankelijkheid en structureringsfaciliteiten.

5. Toegangscontrole

Een database-benadering betekent dat een organisatie haar gegevens als een primaire geïncorporeerde bron beschouwt. Van elk gegevenselement mag er slechts één logische kopie bestaan. Een gevolg hiervan is dat verschillende gebruikers toegang moeten hebben tot de database als ondersteuning bij hun werkzaamheden. Daardoor zal er behoefte bestaan aan een gecontroleerde toegang tot de gegevens, zodat alleen bepaalde mensen gegevens kunnen lezen en/of muteren.

In een relationele database betekent dit dat het systeem in staat moet zijn om bepaalde toegangscontroleregels uit te voeren. Op één der technieken om zulke toegangscontroles te definiëren wordt in dit hoofdstuk ingegaan.

6. Beveiliging en integriteit

De gegevens die door een organisatie in haar database worden bewaard, zijn van grote waarde; veel zakelijke gegevens zullen er in voorkomen. Adequate ondersteuning vanuit de database is voor de organisatie dus essentieel.

Beveiliging betekent bescherming tegen aanvallen en/of fouten.
De database wordt door beide, opzettelijk of per ongeluk, bedreigd.

Hierdoor kunnen verliezen ontstaan in de vorm van beschikbaarheid, integriteit en betrouwbaarheid van de database.

Achtereenvolgens worden behandeld:
- back-up, herstart en herstel (drie belangrijke technieken om de integriteit van een database te onderhouden);
- integriteitsregels;
- referentie-integriteit.

7. Relationele database-technologie

De relationele benadering maakt het mogelijk om op een bijzonder eenvoudige manier verzoeken voor informatie te formuleren. Er wordt echter nogal bezwaar gemaakt tegen deze benadering, omdat deze niet efficiënt door de huidige technologie ondersteund zou kunnen worden.
Er zijn evenwel grote vorderingen gemaakt in de technieken om relationele operatoren te implementeren. Bij de implementatie van verzoeken om gegevens, wordt gebruik gemaakt van optimaliseringsstrategieën om de verwerking te versnellen. In dit hoofdstuk wordt hier nader op ingegaan.

Deel 2

Representatieve systemen

In dit deel komen de meest populaire pakketsoorten met hun specifieke kenmerken aan bod:
- SQL;
- QBE;
- Ingres;
- Oracle;
- dBase III.

In deze boekbespreking wordt hier niet verder op ingegaan.

Epiloog

In dit boek wordt een heldere uiteenzetting gegeven van de onderliggende concepten en van de diverse benaderingen van relationele databases.

Men geeft aan dat een goed ontworpen relationeel systeem een uitstekend hulpmiddel kan zijn voor het oplossen van bepaalde problemen. Het steunt op een stevige theoretische basis; echter, alleen wanneer het juist wordt gebruikt zullen de potentiële mogelijkheden tot ontplooiing kunnen komen.

Het boek is met name geschikt voor een ieder die zich wil oriënteren op het terrein van de relationele databases.

Voor accountants die bij hun klanten geconfronteerd worden met het fenomeen van de relationele databases, is het dan ook zeker aan te bevelen over te gaan tot de aanschaf van dit boek. Van het mysterie van relationele databases zal dan geen sprake meer zijn.

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

TIJDSCHRIFTEN

door mw. D. Jansen Heijtmajer, J.L.H. Kooijman en J.C. Boer
met medewerking van W.C. Bakker en P.A.J. van der Knaap

"Security strategy for small computers"
Adolph F. Cecula Jr.
Information age, volume 7, no 1, January 1985

door W.C. Bakker

De schrijver behandelt in zijn artikel de ontwikkeling en implementatie van het US Geological Survey's computer security programma ten aanzien van decentraal opgestelde kleine computersystemen (mini's en micro's).

Het ontwikkelen van dit programma werd noodzakelijk omdat veel managers en gebruikers, zeer waarschijnlijk ten onrechte, stellen dat zij geen gegevens hebben, die beveiligd dienen te worden (hetgeen risico's opwerpt ten aanzien van de gegevensbescherming).
Deze stellingname is doorgaans ontsproten uit de idee, dat computer security slechts beperkingen oplevert ten aanzien van de gegevensverwerking.
De voordelen van computer security worden (wegens onvolledige opleiding of dergelijke) in te geringe mate begrepen, hetgeen noodzaakt om over te brengen dat computer security moet worden beschouwd als onderdeel van goed bestuur en goede gegevensverwerking.

Het opzetten van een **eigen** security-programma ten behoeve van de beveiliging rond kleine computersystemen werd noodzakelijk omdat:
- de hoeveelheid en verscheidenheid van aanwezige kleine computersystemen exponentieel toenam;
- de eindgebruikers steeds meer kennis van computertechniek verkregen (door het lezen van literatuur over computers en het dagelijks gebruiken van de apparatuur);
- de meeste aanwezige security-literatuur alleen betrekking heeft op grote centrale computercentra;
- de ervaring had geleerd dat een informatie security-programma toegesneden moet zijn op de behoeften van een organisatie en dus een security-programma van een andere organisatie niet kan worden gebruikt.

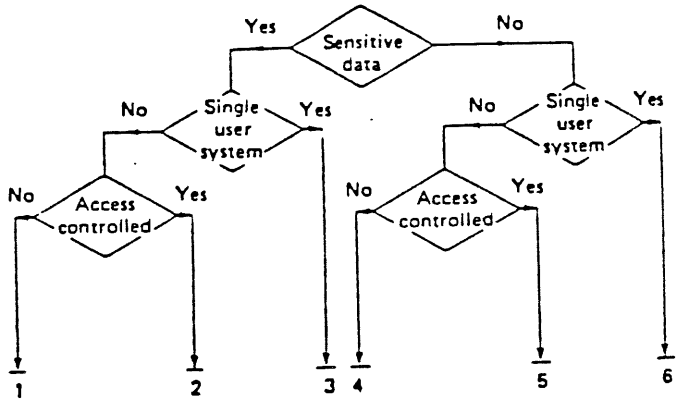
Het computer security-probleem werd in 2 fasen aangepakt, te weten:
1. ontwikkeling van een management-strategie, waarin de diverse verantwoordelijkheden voor de opbouw en beheersing van het computer security-programma werden toegewezen aan, hoog in de organisatie staande, individuen;
2. bepaling van beleid ten aanzien van het te bouwen security-programma, waarin werd gesteld dat:
   - de nadruk moet liggen op de informatie en niet op de computersystemen;
   - het beheer van de geautomatiseerde systemen uitgevoerd moet worden door managers binnen de gebruikersorganisatie (dus niet door een Security Officer).

   Vanwege voornoemde beleidspunten werd het programma het Information Security **and** Control Program genoemd.

Het vaststellen van verantwoordelijkheden voor informatie security was van groot belang voor het programma. Deze verantwoordelijkheden zijn - op basis van organisatorische positie en invloed op geautomatiseerde informatieverwerking - toegewezen aan individuen binnen de organisatie, waarbij de volgende 3 posities binnen het programma van cruciaal belang zijn:

1. de eigenaar van de gegevens	is verantwoordelijk voor het vaststellen van: - de gevoeligheid van de gegevens; - de access-privileges; - het beveiligingsniveau.
2. de eigenaar van een applicatief systeem	is verantwoordelijk voor: - het identificeren van controles; - de verwerking binnen het applicatiesysteem; - het identificeren van geautoriseerde gebruikers van de applicaties; - het definiëren van de noodzakelijke operating-omgeving.
3. de eigenaar van de computerfaciliteiten	is de bewaker van de gegevens en is verantwoordelijk voor het beschermen van die gegevens volgens de specificaties van de eigenaar van de gegevens en die van de eigenaar van het applicatiesysteem.

Het vaststellen van de minimale security-vereisten vormde een groot probleem, omdat diverse typen hardware en vele soorten applicaties in gebruik waren. Als oplossing werd besloten de minimale security-eisen te baseren op de karakteristieken van het **gebruik** van de microcomputerapparatuur in plaats van op apparatuur **type.**
De karakteristieken van drie onderdelen van het microcomputersysteem werden beschouwd - te weten gevoeligheid van de gegevens, aantal gebruikers en mate van toegangsbeheersing - waarmee de categorie, waartoe het computersysteem behoort, kan worden gevonden met behulp van onderstaand schema.



Figuur 1. US Geological Survey security category determination.

Afhankelijk van de categorie waartoe het kleine computersysteem behoort (één van de waarden 1 tot en met 6), kunnen minimale security-eisen aan het desbetreffende systeem worden gesteld.

Aan een categorie met een laag nummer worden zwaardere eisen gesteld dan aan een categorie met een hoog nummer, waarbij met (door de strategie bepaalde) eisen worden bedoeld: het uitvoeren van een risicoanalyse, het aanstellen van een security-officer, het vastleggen van een plan ten aanzien van (fysieke) beveiliging, het laten certificeren van software, etc.

De relatie (noodzakelijk, te adviseren of optioneel) tussen de categorieën van kleine computersystemen en de security-eisen kan in een matrix worden gelegd.

MICROCOMPUTERS & AUDITING
DON'T MAKE THE SAME MISTAKE FOUR TIMES
Michael Sobol

The EDP Auditor Journal 1985-Volume 1
Door L.N.M. Straathof

Steeds meer organisaties gaan over tot de invoering van microcomputers. In tegenstelling tot het gebruik van mainframes of minicomputers kan het gebruik van microcomputers vrij snel overgaan in een zekere "wildgroei".
Daar dit, uit oogpunt van interne controle, zekere risico's inhoudt, dient de accountant tijdig na te gaan welke (organisatorische) maatregelen genomen moeten worden bij de invoering van micro's.
Hij kan hierbij niet wachten totdat de micro's (reeds lange tijd) in gebruik zijn.
Onder andere de volgende maatregelen zijn van belang:

1. Indien toepassingsprogrammatuur is gekocht van een software-leverancier, is het van belang om de beschikking te hebben over de source-versie.
   Immers zodra deze leverancier geen ondersteuning meer kan verlenen, bestaat het risico dat bij het ontbreken van de source-versie de continuïteit van de geautomatiseerde gegevensverwerking in gevaar wordt gebracht.
2. Maatregelen die waarborgen dat alle gegevens juist en volledig worden verwerkt in de bestanden op microcomputers.
3. Maatregelen gericht op het voorkomen dat vertrouwelijke bedrijfsgegevens, gekochte en zelf ontwikkelde programmatuur worden gekopieerd voor "privé-gebruik".

Zodra microcomputers worden gekoppeld aan andere computers (mainframes, mini's of micro's) dient extra zorg te worden besteed aan geautoriseerde toegang tot gegevens.
Verder wordt in het artikel de nadruk gelegd op toereikende back-up-procedures voor:

- apparatuur;
- gegevens;
- programmatuur;
- documentatie.

"AUDITING MICROCOMPUTER-BASED APPLICATION SYSTEMS"
Martin A. Snow

The EDP-Auditor Journal 1985 Volume 1
Door L.N.M. Straathof

Evenals in het artikel van Michael Sobol ("Microcomputers & Auditing, don't make the same mistake four times") pleit Martin A. Snow voor voldoende en tijdige aandacht van de EDP-auditor voor de gevolgen die het gebruik van de microcomputer heeft voor de accountantscontrole. Het artikel bevat geen specifieke controlestappen of een controleprogramma. In het artikel is een opsomming van aandachtsgebieden, voor de EDP-auditor bij het gebruik van micro's, weergegeven.
Deze aandachtsgebieden betreffen:

1. Definition of the environment.
   Het vaststellen van de omgeving waarin en de werkzaamheden waarvoor een microcomputer wordt gebruikt is van groot belang voor een efficiënt en effectief controleprogramma.
2. Corporate policies.
   Ter voorkoming van wildgroei dient de bedrijfsleiding richtlijnen op te stellen inzake de aanschaf en het gebruik van microcomputers.
3. Information center development.
   De ontwikkeling van een "information center" staat in nauw verband met het gebruik van microcomputers.
   De bedrijfsleiding dient, onder andere ter voorkoming van een inefficiënt gebruik, een actieve rol te spelen bij de planning van de invoering en het gebruik van microcomputers.
4. Data integrity.
   Ten behoeve van een juiste en volledige verwerking van gegevens dienen de toepassingssystemen te zijn voorzien van voldoende controles.
   Het betreffen zowel geprogrammeerde als handmatige controles.
5. Data security.
   Toereikende beveiligingsmaatregelen zijn nodig om gegevens, programmatuur en hardware te beschermen tegen verlies en onbevoegd gebruik.
6. Data system interfaces.
   De mutaties in subsystemen (subgrootboeken) leiden veelal tot mutaties in het grootboek. De door de accountant uit te voeren controlehandelingen worden mede bepaald door de aard van de interface, die bestaat tussen het grootboek en de subsystemen. De interface kan handmatig of geautomatiseerd van aard zijn.
7. Program development.
   De gebruikers kunnen eigen programmatuur ontwikkelen op microcomputers. Toereikende ontwikkelingsprocedures zijn nodig om de betrouwbaarheid van deze programmatuur te waarborgen.

8. Procedure documentation.
   Om de continuïteit van gegevensverwerking te verzekeren dient onder andere voldoende systeemdocumentatie aanwezig te zijn.
9. Hardware compatibility.
   Een door de bedrijfsleiding vastgesteld beleid dient te waarborgen dat met behulp van de gekochte apparatuur gedurende lange tijd toepassingen kunnen worden gedraaid.
   Nieuwe ontwikkelingen, zoals bijvoorbeeld op het gebied van de datacommunicatie, mogen dit niet in de weg staan.
10. Personnel training.
    Een goede training van de gebruikers bevordert een efficiënt gebruik van microcomputers. Voorts is opleiding van belang voor de ontwikkeling van betrouwbare toepassingssystemen.
11. Disaster recovery.
    Back-up- en recovery-procedures zijn nodig om de continuïteit van de gegevensverwerking te waarborgen.
12. Ergonomics.
    In sommige landen zijn wettelijke regels opgesteld voor de werkplek waar microcomputers worden gebruikt en zijn eisen opgesteld waaraan micro's dienen te voldoen.
13. Audit involvement.
    De schrijver pleit voor een actieve rol van de EDP-auditor bij de ontwikkeling van toepassingssystemen op micro's.

De hiervoor genoemde aandachtsgebieden wijken niet veel af van die bij het gebruik van mainframes en mini's.
De ervaring heeft echter geleerd dat de microgebruikers hieraan relatief weinig aandacht besteden.

"REPORT ON THE STUDY OF EDP-RELATED FRAUD IN THE BANKING AND INSURANCE INDUSTRIES"

EDP Fraud Review Task Force.
American Institute of Certified Public Accountants (AICPA) 1984.
Door L.N.M. Straathof

Door het AICPA is een onderzoek uitgevoerd naar fraudes bij banken en verzekeringsmaatschappijen. Het onderzoek heeft zich gericht op die fraudes, waarbij de geautomatiseerde gegevensverwerking direct betrokken is geweest.
De onderzoeksgegevens zijn verkregen van:
- The Bank Administration Institute;
- The American Insurance Association;
- The American Council of Life Insurance;
- The Life Office Management Association;
- Banken en verzekeringsmaatschappijen.

Volgens de opstellers van het rapport worden de mogelijkheden van fraude vergroot door een toenemend gebruik van:
- grote geïntegreerde databases;
- microcomputers;
- draagbare "intelligente" terminals in combinatie met telecommunicatiemogelijkheden.

Verder heeft het onderzoek uitgewezen, dat de toenemende complexiteit van de computersystemen het voorkomen en het ontdekken van fraude bemoeilijkt.

Hierna zijn de belangrijkste resultaten van het onderzoek weergegeven:
- Het frauderen vond over het algemeen plaats tijdens de gewone transactieverwerking. De aard van het computersysteem speelde geen rol.
- Veel fraudeurs trokken voordeel uit zwakheden in het interne controlesysteem. Ontoereikende functiescheiding vormde een veel voorkomende leemte.
- Veel fraudes betroffen het verwerken van ongeautoriseerde transacties. In relatief veel gevallen ging de fraudeur ervan uit, dat de fraude niet ontdekt zou worden ten gevolge van het grote aantal transacties en dientengevolge de onvoldoende controle op de mutatieverwerking.
- Bij de banken kwamen de fraudeurs vooral voor bij data-entry-functionarissen en functionarissen, die werkzaam waren op het gebied van de kredietverlening.
  Bij de verzekeringsmaatschappijen kwamen de fraudeurs veel voor onder medewerkers, die waren belast met de behandeling van polissen en claims.

Een derde van de bekend geworden fraudes is ontdekt door interne en externe controle. Eveneens een derde gedeelte is ontdekt door bijzondere gebeurtenissen, zoals bijvoorbeeld ongewone handelingen van de fraudeur.
Het grootste gedeelte van de fraudes is bemerkt door collega's van de fraudeurs, waaronder interne accountants.
Bij de banken is circa 25 procent van de fraudes aan het licht gekomen door klachten van cliënten. Bij de betrokken verzekeringsmaatschappijen is dit bijna niet voorgekomen, daar de verzekerden niet op de hoogte waren van frauduleuze handelingen met hun polis. Bovendien zijn fraudes gepleegd met fictieve polissen.

"REPORT OF THE JOINT DATABASE TASK FORCE"
Uitgegeven door: American Institute of Certified Public Accountants (AICPA)
Canadian Institute of Chartered Accountants (CICA)
Institute of Internal Auditors (IIA) 1983

Samengevat: door P.A.J. van der Knaap

Verkorte inhoudsopgave:

Het rapport beschrijft het effect dat een database-omgeving heeft op de beheers- en controleprocedures.
Het rapport bestaat uit drie hoofdstukken namelijk:
1. The Database Environment;
   - Overview of a Database Management System
   - Unique features of a Database Environment
   - Characteristics of a Database Management System
   - Components of the Database Environment
2. Control Considerations in a Database Environment;
3. Audit Considerations in a Database Environment.

Ad 1

Een database is te definiëren als een verzameling onderling gerelateerde gegevens, die door meerdere gebruikers, voor verschillende doeleinden wordt gebruikt. Een database-omgeving biedt de mogelijkheid tot data-onafhankelijkheid.
Dit houdt in dat niet het applicatieprogramma, maar het Data Base Management System (DBMS) het fysiek benaderen van gegevens regelt. Hierdoor is het mogelijk om te werken met één eenduidige fysieke presentatie van de gegevens.
Tevens biedt dit de mogelijkheid van Data Sharing (gemeenschappelijk gebruik van gegevens).

Omdat in een database-systeem metadata (gegevens over de opgeslagen data) zijn vastgelegd kunnen voordelen worden behaald op het gebied van programma-onderhoud en toegangsbeveiliging.
Het management dient beheer uit te oefenen over de in een onderneming gebruikte gegevens. Door middel van een eenduidige vastlegging van metadata kan men deze beheersfunctie beter uitoefenen.

Een data base management systeem bestaat onder andere uit de volgende onderdelen:
- Data Manipulation Language (DML) [ten behoeve van het uitvoeren van manipulaties op de database];

- Data Description Language (DDL) [definieert de structuur van de database];
- Storage Structure Language (SSL) [beschrijft de wijze waarop de gegevens fysiek zijn vastgelegd].

Tot de database-omgeving behoren, naast het DBMS, het Data Dictionary/Directory System en de functie Database Administrator.

Volgens het rapport is de Database Administrator, in het algemeen, verantwoordelijk voor het definiëren, organiseren, beschermen en het efficiënt gebruik van de database. Hieronder vallen ook de regels die gelden bij het toegang krijgen tot en het opslaan van de gegevens. Nadrukkelijk is in het rapport vermeld dat in sommige organisaties een onderscheid is gemaakt tussen de beheers- en beleidsbepalende functies (Data Administrator) enerzijds en de uitvoerende, technisch geaarde functie (Database Administrator) anderzijds.

Het Data Dictionary/Directory System is een geautomatiseerd documentatiesysteem dat zowel actief als passief kan zijn.
Een passief Data Dictionary/Directory System kan gebruikt worden om een verslaglegging te geven van de in een systeem opgeslagen metagegevens. Indien gebruik wordt gemaakt van een actief Data Dictionary/Directory System controleert het DBMS, op het moment dat programma's ter compilatie worden aangeboden of de gegevens, die door het programma worden benaderd, voorkomen in het subschema dat ten behoeve van het programma is verstrekt. Dit benaderen van de gegevens kan als doel hebben geautoriseerd ontlenen van informatie, het bijwerken van informatie of het doen uitoefenen van programmafuncties op een zodanige wijze dat geen gegevens verloren gaan (concurrency control).
In het door de Database Administrator verstrekte subschema, dat is opgeslagen in het Data Dictionary/Directory System, is vastgelegd welke gegevens door het programma mogen worden benaderd.

Ad 2

De controledoelstellingen zullen in een database-omgeving niet veranderen, echter de te gebruiken maatregelen van interne controle verschillen met die welke in een traditionele omgeving worden gebruikt. Het management dient gebruikmakend van de beschikbare middelen het beheer uit te oefenen over de aanwezige gegevens.

Hierbij kunnen drie aandachtsgebieden voor de interne controle worden onderscheiden, namelijk:
- toegangs- en wijzigingsprocedures;
- coördinatie van de activiteiten (aangezien het kan voorkomen dat meerdere gebruikers op een zelfde moment gebruik wensen te maken van de gegevens moet het systeem de verschillende activiteiten op de gegevens coördineren om de integriteit van de gegevens te kunnen blijven waarborgen);

- concentratie van middelen (het gegeven dat alle gegevens geconcentreerd opgeslagen zijn, legt extra nadruk op:
  - bescherming van de gegevens;
  - het gebruik van een betrouwbaar DBMS;
  - het kunnen steunen op betrouwbaar en ter zake kundig personeel, met betrekking tot het DBMS).

Ad 3

Met betrekking tot de voornoemde aandachtsgebieden geeft dit laatste hoofdstuk een overzicht van de te gebruiken mix van controletechnieken. Het hoofdstuk start met het aangeven van de fasen die moeten worden doorlopen, voordat de mix van controlemiddelen wordt vastgesteld.

De volgende fasen kunnen hierbij worden onderscheiden:
- nagaan wat de invloed is van de gebruikte database-technologie ten opzichte van een traditionele omgeving, op de keuze van controlemiddelen;
- beoordelen welke applicatiecontroles overgenomen zijn door het DBMS;
- het verkrijgen van inzicht in de wijze waarop de verschillende gebruikers gebruik maken van elkaars gegevens (data sharing). Met behulp van een overzicht waarin is vastgelegd welke gegevens door welke gebruikers gemeenschappelijk worden gebruikt kan - te samen met het overzicht waarin de verantwoordelijkheden zijn vastgelegd - worden nagegaan of de gebruiker in staat is om deze verantwoordelijkheid te dragen.

In de tabel op de volgende bladzijde, die integraal is overgenomen uit het "Report of the joint database task force", wordt een overzicht gegeven van "Control Techniques and related controlfunctions".

Onder "Co-ordination of activities" wordt in de matrix verstaan: "het coördineren van bepaalde handelingen". Dit vereist - omdat een database gebruikt wordt - een eenduidig niveau van controlehandelingen, een consistente interpretatie van de betekenis van data-elementen en een juiste timing van het bijwerken respectievelijk afbreken van transacties (ofwel verwerkingsproces).

Met "concentration of resources" is bedoeld het gegeven dat "alle gegevens/programma's centraal opgeslagen zijn", waardoor extra maatregelen nodig zijn om de integriteit van de gegevens te waarborgen (zie onder ad 2).

Van ieder van de cellen - gevolgd met X - worden al naar gelang de situatie de eventueel mogelijke controlemaatregelen van de accountant kort aangeduid.

Control Techniques and Related Control Functions

Techniques	Access/ update	Co-ordination of activities	Concentration of Resources
Access/update Controls			
Restrict data resources and update functions to authorized users by passwords	X		
Restrict data resources and update functions to authorized users by sub-schema	X		
System Design Controls			
Implement application systems using a systems development life cycle tailored to consider the use of a DBMS		X	X
Implement a standardized approach for making modifications to application systems		X	X
Automatically generate data base description by the DD/DS		X	
Develop adequate transaction trails		X	
Consider the DBMS return codes during the detailed design phase	X	X	X
Data Base Administration Controls			
Assign responsibility for data ownership	X	X	
Centralize administration of schema/sub-schema	X	X	
Maintain adequate segregation of duties	X		X
Operational Control			
Analyze internal storage structures (pointers)			X

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

COMPACT

Zomer/Herfst 1985

Automatisering Beveiliging Controle NIEUWS

door M.C. Duym, J.F.C. van Epen en drs. J. Kuipers

Automatisering

VERVANGING ACCEPTGIRO
door J. Kuipers

Volgens het eindrapport van de COMGE-werkgroep STAG "Van Stac naar acceptgiro" gaat de huidige ponskaart van de stortingsacceptgiro (stac) verdwijnen. Vervanging is nodig omdat de ponskaartapparatuur verdwijnt.
Vijftigduizend vergunninghouders verzenden jaarlijks 250 miljoen acceptgirokaarten in Nederland.
De ponskaart wordt vervangen door een optisch leesbaar slap document (zoals het bekende postgiro-overschrijvingsformulier uit het blauwe boekje).

Veranderingen aanmaak acceptgirodocumenten

Het nieuwe document biedt meer mogelijkheden door de vorm waarin het verzonden kan worden. De nieuwe acceptgiro kan bijvoorbeeld geïntegreerd worden met een ander formulier, als afscheurbaar deel aan een factuur.
Tegenover de vergroting van de mogelijkheden staan hogere kwaliteitseisen die aan de optisch leesbare stag worden gesteld. De voorbewerkingsapparatuur dient van hoge kwaliteit te zijn.
Op het ogenblik zijn er nog maar een beperkt aantal drukkerijen die aan de gestelde eisen voor bedrukking kunnen voldoen. Met de invoering van de stag zal de naam-nummercontrole door de postgiro komen te vervallen. De incassant wordt nu alleen verantwoordelijk voor de juistheid van het gironummer op de acceptgiro.
Een en ander heeft tot gevolg dat bij overgang van ponskaart naar optisch leesbare stag een zorgvuldige voorbereiding gewenst is.

Veranderingen in ontvangst van betalingen

Een van de grootste voordelen van de acceptgiro is de terugkoppeling van op het betaaldocument voorgecodeerde boekingsinformatie. Deze terugkoppeling blijft bestaan bij aanlevering van betaalgegevens op tape en dergelijke.

Indien gewenst kunnen alle betalingen, onafhankelijk van waar de opdracht werd aangeboden, via één financiële instelling worden afgewikkeld. De betalingen via de bank en de postgiro kunnen of door de bank of door de giro in één bedrag aan de incassant worden overgemaakt.
Naast de aanlevering van betaalgegevens op borderellen, kan aanlevering op een magnetisch medium plaatsvinden, waarbij tevens de betaalkenmerken worden overgenomen.
De retournering van originele betaalopdrachten zal echter steeds verder teruggedrongen worden.

Gevolgen voor de organisatie

De steeds verdergaande vervanging van formulieren door tapes, disketten en dergelijke vereist een aanpassing van de interne controle, omdat de betaalinformatie gemakkelijker manipuleerbaar wordt.
De hoge kwaliteitseisen die aan het optisch leesbare schrift gesteld worden, houden in dat de organisatie voldoende ingesteld moet zijn op deze hogere eisen, opdat de acceptgiro's tijdig verzonden kunnen worden en geen vertraging ondervinden bij de verwerking door de financiële instellingen.

Verdere informatie is te verkrijgen bij de secretaris van COMPACT.

AUTOMATISERING BELASTINGAANGIFTE
door M.C. Duym

Kluwer was in het vroege voorjaar een van de eerste uitgevers, die naast de almanak ook een computerprogramma voor het verrichten van aangiften te koop aanbood. Dit programma draaide op enkele van de meest verkochte home computers, dus duidelijk gericht op de particuliere markt.

Dit najaar zal een andere "almanakken gigant", Elsevier- NDU's kleindochter Annoventura op de markt komen met het "Elseviers belasingaangifte systeem", dat bestemd is voor de zakelijke markt. Als doelgroepen worden genoemd belastingconsulenten, alsmede accountants- en administratiekantoren. Het pakket maken zij samen met de maatschap van belastingadviseurs Loyens & Volkmaars.

Naar aanleiding van artikel uit Computable.

IBM KOMT MET UNIX EN AI PAKKETTEN
door M.C. Duym

In de eerste helft van dit jaar heeft IBM een aantal annonceringen gedaan voor pakketten, die in eerste instantie gericht zijn op de wetenschappelijke markt en de speur- en ontwikkelingsafdelingen van bedrijven. Het betreft hier het besturingssysteem IX/370 welke gebaseerd is op UNIX versie V 0.2, een implementatie van de taal Prolog alsmede programma's voor het opbouwen en raadplegen van kennisbanken. Alle genoemde programmaprodukten draaien onder VM.

Daar wij menen, dat deze produkten ook in de nabije toekomst voor de zakelijke markt van belang zijn, besteden wij hieraan aandacht.

IBM is van plan enkele exemplaren van het besturingssysteem in december 1985 te gaan leveren. Doelgroep is vooral de UNIX-gebruiker die nog niet over IBM hardware beschikt. Ook speelt mee, dat diverse overheidsinstellingen in de USA alsmede General Motors al bij veel kontrakten bedingen, dat UNIX het besturingssysteem moet zijn.

Door het gebruik van UNIX bij bovengenoemde instellingen en bedrijven, zal een verdere uitbreiding van de gebruikersbasis naar de zakelijke markt niet lang meer op zich laten wachten. Dit als gevolg van de drang om programma-ontwikkeling (waartoe UNIX uitermate geschikt is) en meer wetenschappelijke toepassingen óók de financieel administratieve verwerking onder hetzelfde besturingssysteem te verrichten.

IX/370 ontmoet op de markt als concurent de UNIX implementatie van Amdahl onder de naam UTS. Dit pakket wordt al sinds 1982 verkocht. Nadere testen van de produkten moeten uitwijzen welke de beste koop is. In deze vergelijking zal ongetwijfeld ook CMS een rol spelen, omdat dit IBM programmaprodukt ten aanzien van het ontwikkelen van software een soortgelijke rol als UNIX speelt.

Er zijn twee belangrijke verschillen ten aanzien van de afhandeling van het terminal verkeer tussen UNIX en de IBM 370 besturingssystemen. Ten eerste maakt UNIX gebruik van ASCII terminals in plaats van EBCDIC (3270). Ten tweede biedt het in principe applicaties de mogelijkheid op een karakter voor karakter basis de verwerking uit te voeren. Van deze karakter-gewijze verwerking maken diverse UNIX applicatieprogramma's gebruik.

Voor genoemde terminalproblemen is door IBM de oplossing gezocht in het toepassen van Series/1 computers als Front End Processors. Amdahl heeft een en ander opgelost middels de 4705 I/O controller (dit is een equivalent van IBM's 3705).

VM-Programming in Logic is de naam waaronder IBM haar Prolog implementatie op de markt brengt. Het is daarmee naast de IBM implementatie van LISP, de tweede taal die IBM voor het ontwikkelen van kunstmatige intelligentie toepassingen levert.

Expert Systems Development Environment/VM en Expert Systems Consultation Environment/VM zijn de twee programmaprodukten voor het opbouwen en raadplegen van kennisbanken. Voor een bepaald vakgebied wordt een kennisbank opgebouwd door experts. Door het raadplegen van de kennisbank kunnen vervolgens niet (zulke grote) experts worden geleid in hun beslissingen. Een voor een bepaalde toepassing ontwikkelde kennisbank met de raadpleeg software wordt wel een expert system genoemd.

Er zijn in de wereld al diverse expert systems ontwikkeld. In de komende jaren zal dit aantal naar onze mening een sterke vlucht nemen en zullen ook de accountants er mee worden geconfronteerd. Wat dacht u van een expert system voor het beoordelen van de kredietwaardigheid of voor de beoordeling en evaluatie van het stelsel van interne controle. Zie ook het artikel van A. van der Drift in Compact 85/2 getiteld "Knowledge based systems: een stap vooruit in de beheersbaarheid van administratieve processen".

Beveiliging

CAUGHT IN THE ACT
door J. Kuipers

In Datamation nummer 12 van 15 juni 1985 verscheen onder deze titel een artikel, waarin de strafbaarheid van het illegaal kopiëren van software in de Verenigde Staten wordt behandeld.
Het kopiëren en gebruiken van software zonder toestemming van de ontwikkelaar is veelal in strijd met de copyright-wetgeving en software-licentie-overeenkomsten.
In de laatste anderhalf jaar zijn software-ontwikkelaars steeds vaker bereid harde juridische acties te nemen tegen het ongeautoriseerd kopiëren van software.
Als voorbeeld: in januari 1984 dient Lotus een claim van $ 10,000,000 tegen Rixon Corp. in wegens het breken van de copyright-wet en de Lotus-licence-overeenkomst. Rixon had minstens 13 kopieën van het pakket Lotus-1-2-3 verspreid over haar filialen.
In januari 1985 vervolgt MicroPro het bedrijf American Brand Inc. wegens het ongeautoriseerd kopiëren van onder andere WordStar, MailMerge en SpellStar.
De Association for Data Processing Service Organisation (ADAPSO) stelt dat voor elk verkocht pakket één illegale kopie in omloop is.
Omdat de zogenaamde copy protected-diskettes feitelijk toch te kopiëren zijn en dus geen oplossing bieden, zoeken de ontwikkelaars hun toevlucht tot harde juridische sancties.

Onder de copyright act is het maken van een kopie voor back-up-doeleinden wel toegestaan.
De copyright act wordt zodanig uitgelegd dat het downloaden vanuit een centrale computer naar diverse PC's eveneens gezien wordt als een overtreding.
Naar analogie van de uitspraak dat het thuis opnemen van tv-programma's op video te beschouwen is als "fair use" kan gesteld worden dat het thuis maken van software-kopieën niet strafbaar is.

Naast bescherming door de copyright-wetgeving is bij de aanschaf van veel pakketten ook sprake van bescherming door licentie-overeenkomsten.

Deze overeenkomsten worden ook wel "tear-me-open" of "shrink wrapped"-overeenkomsten genoemd. Bij het verwijderen van de plastic verpakking wordt de overeenkomst gesloten geacht.
Meestal beperkt deze "krimpplastic"-overeenkomst het gebruik tot één PC.
Op dit moment zijn nog geen rechtszaken over de afdwingbaarheid van "krimpplastic-overeenkomsten" bekend.
Hoewel over de rechtsgeldigheid van deze bijgesloten overeenkomsten nog twijfels bestaan is duidelijk dat de belanghebbende ontwikkelaars zich meer van juridische verdedigingsmiddelen aan het voorzien zijn.
Daarnaast legt het ADAPSO nadruk op voorlichting aan een breed publiek waarom het kopiëren van software illegaal is.

Controle
(Deze keer stellen we een waarderingskwestie - geënt op Amerikaanse verhoudingen - aan de orde)
door M.C. Duym

FASB STATEMENT VOOR VERANTWOORDING SOFTWAREKOSTEN

Per augustus 1985 is door de Financial Accounting Standards Board de Statement of Financial Accounting Standards No. 86 uitgebracht. De statement behandelt de verantwoording van kosten die gemaakt zijn voor computer software, voorzover deze wordt verkocht, ver-leased of op een andere manier wordt aangeboden.
Het voorstel houdt in, dat de kosten van het vaststellen van de technologische haalbaarheid van het produkt als last worden genomen wanneer zij worden gemaakt en worden verantwoord als kosten van speur- en ontwikkelingswerk. De kosten voor het maken van produktie masters die worden gemaakt nadat de technologische haalbaarheid is vastgesteld, moeten worden geactiveerd. Deze geactiveerde kosten houden ook in de kosten voor programmering en testen gemaakt na het vaststellen van de technologische haalbaarheid.
Als bewijs, dat de technologische haalbaarheid is vastgesteld, moet een onderneming een van de volgende groepen van activiteiten hebben verricht:

1. Indien het proces van creëren van het computer software produkt een gedetailleerd programma ontwerp bevat:
   a. Het produkt ontwerp en het gedetailleerd programma ontwerp moeten compleet zijn en de onderneming moet hebben vastgesteld, dat de nodige vaardigheden, hardware- en software-technologie in de onderneming aanwezig zijn om het produkt te produceren.
   b. De volledigheid van het gedetailleerd programma-ontwerp en de overeenkomst daarvan met het produkt-ontwerp moet bevestiging vinden in documentatie en moet worden vastgesteld door het afstemmen van het gedetailleerd programma-ontwerp met de produkt specificaties.
   c. Het gedetailleerd programma ontwerp moet zijn onderzocht ten aanzien van de ontwikkelingskenmerken met een hoog risico (bijvoorbeeld nieuw, uniek, ...) en alle onzekerheden ten aanzien van de onderkende risico's moeten zijn opgelost door middel van programmering en tests.

2. Indien het proces van creëren van het computer software produkt geen gedetailleerd programma-ontwerp bevat met de onder 1 beschreven kenmerken:
   a. Een produkt-ontwerp en een werkend model van het software produkt moeten gereed zijn.
   b. De volledigheid van het werkend model en haar overeenkomst met het produkt ontwerp moeten zijn bevestigd door tests.

Het activeren van kosten moet stoppen zodra het produkt beschikbaar is voor de algemene verkoop aan klanten.

Indien de bedoelde software niet zelf wordt ontwikkeld, maar wordt gekocht en deze software geen alternatieve toekomstige aanwendingsmogelijkheden heeft, moeten de aankoopkosten op eenzelfde wijze worden behandeld als voor eigen ontwikkelde software. Maakt de aangekochte software bijvoorbeeld onderdeel uit van een produkt waarvan de technologische haalbaarheid al is vastgesteld, dan moeten deze volledig worden geactiveerd.

Heeft de aangekochte software ook nog een alternatieve toekomstige aanwendingsmogelijkheid, dan moet het daarmee gemoeide deel van de kosten worden geactiveerd en in de toekomst naar gelang die aanwending als last worden genomen.

Nu bovengenoemde statement er ligt, zal naar verwachting het besluit van de Security and Exchange Commission van augustus 1983 worden vernietigd, waarbij genoteerde ondernemingen werd verboden kosten te activeren van computer software die intern is ontwikkeld en geproduceerd met het doel het te verkopen, ver-leasen of op een andere manier aan te bieden, indien van deze handelswijze al niet voor het moment van de SEC beslissing was gebleken. Dit besluit was in afwachting van FASB richtlijnen genomen, om de groeiende diversiteit in accounting practices tegen te gaan.

Verwacht wordt, dat als gevolg van bovengenoemde ontwikkelingen veel Amerikaanse softwarebedrijven over het lopende jaar een hogere winst zullen tonen dan over 1984 als gevolg van het activeren van meer kosten. Volgens een artikel in Computable van 23 augustus, verwachten Management Science of America (MSA) en Applied Data Research (ADR) een winsttoename in de orde van 15 tot 25 procent. Ook Cullinet verwacht een winsttoename. Echter voor IBM zal een lichte winstdaling gelden. Dit omdat zij altijd al een groot deel van de ontwikkelingskosten activeerden; meer dan nu toegestaan. In 1983 activeerde IBM 47 procent van 588 miljoen dollar aan software ontwikkelingskosten en in 1984 40 procent van 803 miljoen dollar.

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

Minister Korthals Altes installeert Commissie Computercriminaliteit

Nieuwe strafbepalingen nodig tegen misbruik van computers

JU – Justitie is niet geheel machteloos tegen crimineel gebruik van computers. Toch zijn de bestaande strafbepalingen niet voldoende toegesneden op misdragingen die door de ontwikkelingen van de informatietechnologie zijn mogelijk gemaakt. Zo schetste minister Korthals Altes de huidige situatie bij de installatie van de Commissie Computercriminaliteit. De commissie, onder voorzitterschap van mr. H. Franken, werd geïnstalleerd op 20 november. Zij zal een studie moeten verrichten naar lacunes in de wetgeving.

Mijnheer de Voorzitter, geachte aanwezigen! – In de memorie van toelichting op de rijksbegroting voor 1986 heb ik aangekondigd dat een commissie zal worden ingesteld, die een verkennend onderzoek uitvoert naar probleemgebieden in het materiële en formele strafrecht op het gebied van de opslag, verwerking en uitwisseling van gegevens met behulp van daartoe vervaardigde apparatuur. Deze commissie zou tevens dienen te adviseren over de wenselijkheid van wetswijziging.
Ik ben verheugd dat ik de voorzitter en de leden van de commissie bereid heb gevonden om deze taak op zich te nemen. Vandaag is het moment aangebroken dat u met uw werkzaamheden van start kunt gaan.
Daarmee is een einde gekomen aan een periode van twijfel waarin enerzijds werd verdedigd dat de bestaande wettelijke bepalingen voldoende mogelijkheden zouden bieden om tegen crimineel misbruik van computers op te treden, anderzijds werd gesteld dat deze bepalingen niet zijn toegesneden op misdragingen die de ontwikkelingen in het vak van de informatietechnologie mogelijk hebben gemaakt. Zonder te willen stellen dat de justitie met de bestaande wetgeving machteloos is tegen crimineel gebruik van computers, meen ik dat er inmiddels voldoende grond is om een studie te verrichten naar mogelijke lacunes in de wetgeving. Deze lacunes zouden onder meer daarin kunnen liggen dat aan de bescherming van informatie een ander gewicht moet worden toegekend nu de technische mogelijkheden om deze te manipuleren exponentieel zijn gegroeid en nog groeien.
Het valt te verwachten dat de recente en in gang zijnde ontwikkelingen in het vlak van de informatietechnologie in de komende eeuwen, terugblikkend in historisch perspectief, als één van de kenmerkende eigenschappen van het eind van de twintigste eeuw zullen worden gezien.
Het is begonnen met rekenapparatuur. Dit is ook de letterlijke betekenis van het woord 'computer'. Inmiddels zijn er echter bijgekomen de tekstverwerkers, de gegevensbanken, kunstmatige intelligentie, het computer-ondersteunde industriële ontwerp en de geautomatiseerde besturing van industriële processen, waaronder de robotica.
Ook in de afwikkeling van verkeersstromen in de lucht, te water en op het land, is de geautomatiseerde gegevensvergaring en -verwerking niet meer weg te denken. Bij al deze vormen van gebruik van informatietechnologie gaat het niet alleen om gegevens die ten opzichte van de apparatuur een uitwendige functie hebben, met andere woorden een bepaald voor de mens kenbaar resultaat opleveren, maar ook om gegevens die de inwendige processen besturen, dus de computerprogramma's en andere besturingsgegevens. De vele vormen van gegevensverwerking zouden niet zo kwetsbaar zijn, indien niet ook de telecommunicatie een enorme vlucht had genomen. Datanetwerken met daaraan gekoppelde terminals, straalverbindingen en communicatiesatellieten hebben de ruimtelijke barrières in de beschikbaarheid van informatie geslecht en hebben de plaatsbepaling van een voorhanden gegeven tot een nagenoeg verouderd begrip gemaakt.
Inmiddels neemt de snelheid van de technische ontwikkelingen niet af. De overheid houdt zich daarbij niet meer afzijdig, maar heeft uitdrukkelijk besloten tot een stimulerende rol ten opzichte van het bedrijfsleven. Binnen de Europese Gemeenschap zijn verschillende projecten ter bevordering van de informatietechnologie gestart. Ik noem slechts de codenaam Esprit en Race. In een ander verband hebben de Europese landen zich rondom het project Eureka geschaard, dat zich niet beperkt tot informatietechnologie, maar deze mede omvat. Op Nederlands niveau is er het informaticastimuleringsplan (ISP) onder de verantwoordelijkheid van mijn ambtgenoten van Onderwijs en Wetenschappen en van Economische Zaken gelaneerd.

Strafrecht

Al deze technische ontwikkelingen hebben ook hun weerslag op het recht. Dit kwam aanvankelijk tot uitdrukking in de ongerustheid over de geautomatiseerde verwerking van persoonsgegevens. De bescherming van de persoonlijke levenssfeer is inmiddels een grondwettelijk beschermd recht, dat onder meer zijn uitwerking vindt in een wetsvoorstel over persoonsregistraties, dat onlangs mede onder mijn verantwoordelijkheid bij de Tweede Kamer is ingediend. In dit wetsvoorstel speelt het strafrecht een marginale rol. Daarnaast spelen in de sfeer van het ordeningsrecht allerlei ontwikkelingen, onder meer op het terrein van mijn ambtgenoten van Verkeer en Waterstaat en van Welzijn, Volksgezondheid en Cultuur, onder wie de P.T.T. respectievelijk de omroepen ressorteren. Het valt niet uit te sluiten dat zij zullen komen tot gedragsregels waarvan de naleving strafrechtelijk moet worden afgedwongen. Ook binnen de sfeer van het strafrecht in meer enge zin, dat tot mijn verantwoordelijkheid behoort, doen zich ontwikkelingen voor. De procureurs-generaal bij de gerechtshoven hebben een werkgroep ingesteld, die onder de leiding van mr. Van Brummen bezig is een handleiding te ontwerpen ten behoeve van de rechterlijke macht voor de aanpak van computercriminaliteit op basis van het bestaande recht. Op internationaal niveau heeft eveneens de verhouding van het strafrecht tot de ontwikkelingen in de informatietechnologie de aandacht. Zo is binnen de Organisatie voor economische samenwerking en ontwikkeling (OESO) een rapport hierover inmiddels nagenoeg gereed. In dit verband lag het accent op de bescherming van de economische belangen in het internationale handelsverkeer. De Raad van Europa neemt eerstdaags het onderwerp in studie. Aldaar zal het onderwerp waarschijnlijk meer in het strafrechtelijk perspectief en in zijn verhouding tot uitleverings- en rechtshulpverdragen worden bezien.

Deze ontwikkelingen in het juridische vlak hebben inmiddels wel duidelijk gemaakt dat een meer gerichte studie naar eventuele aanpassingen van het materiële en formele strafrecht onontkoombaar is. De juridische ontwikkelingen, waaronder die in het legislatieve vlak, behoeven niet noodzakelijkerwijs hetzelfde koortsachtige tempo te hebben als de technische. Het is echter duidelijk dat een verduidelijking, toespitsing of aanpassing van bestaande wettelijke bepalingen, dan wel enige nieuwe strafrechtelijke bepalingen in overweging moet worden genomen. Een aantal voorbeelden om dit te illustreren, geef ik in het volgende aan.
Op 12 maart van dit jaar heb ik mondeling in de Tweede Kamer, in antwoord op vragen, al geopperd dat zou moeten worden bezien in hoeverre het zogenaamde inbreken in een computer, ten einde daar kennis te nemen van vertrouwelijke gegevens, zou moeten worden strafbaar gesteld. Tot dusver is dit alleen het geval ingevolge artikel 98c, eerste lid, onder 2°, van het Wetboek van Strafrecht waar het gaat om een gegeven waarvan de geheimhouding door het belang van de staat wordt geboden, kortom spionage. Overigens betreft deze bepaling de pogingen om kennis te nemen van vertrouwelijke gegevens, ongeacht de vraag of deze zijn geautomatiseerd of niet.

Geheimhoudingsplicht
Voor het overige wordt vertrouwelijke informatie tot dusver slechts beschermd door de geheimhoudingsplicht van de arts, de notaris, de ambtenaar enz. Op hem rust de plicht, die juridisch nog niet uitdrukkelijk heeft vorm gekregen, materiaal waarop vertrouwelijke gegevens zijn vastgelegd, weg te bergen. Is aan deze plicht voldaan, dan zal men in de regel niet zonder zaaksbeschadiging (het openen van een kast) of lokaalvredebreuk van deze gegevens kunnen kennisnemen. Laat de geheimhouder echter de gegevens slingeren of is hij daarmee anderszins onzorgvuldig, dan is kennisneming daarvan niet onrechtmatig. Zelfs zou men kunnen bepleiten dat zulks valt onder het verdragsrechtelijk gewaarborgde grondrecht om inlichtingen te vergaren zoals omschreven in artikel 10 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en in artikel 19 van het Internationaal verdrag inzake burgerrechten en politieke rechten. Een inperking van het recht op kennisneming van gegevens, zou dan moeten voldoen aan de criteria die deze verdragen aan zulke inperkingen stellen. Ik wijs terloops op het vraagstuk in verband met de gelijkstelling, die sommigen bepleiten, van informatie en eigendom. Het wegnemen van eigendom, van een 'goed' in de zin van het Wetboek van Strafrecht, is strafbaar als diefstal, ongeacht de zorg die de rechthebbende, in casu de geheimhouder, heeft betracht.
In dit verband rijst tevens de vraag of er nog zinvol een onderscheid kan worden gemaakt tussen gegevens die zich op één plaats bevinden en gegevens die onderweg zijn van de ene plaats naar een andere. Daarmee komt men op het onderscheppen van gegevensverkeer, de strafbaarstelling waarvan in de artikelen 139a en volgende van het Wetboek van Strafrecht zich tot dusver beperkt tot het afluisteren van telefoongesprekken die met een technisch hulpmiddel worden afgeluisterd. Ten slotte wil ik nog wijzen op artikel 441 van het Wetboek van Strafrecht dat strafbaar stelt het openbaar maken van een via de ether ontvangen bericht, indien dit bericht niet voor de ontvanger is bestemd. U zult moeten onderzoeken of deze en dergelijke bepalingen bruikbaar en toereikend zijn in het licht van de komende informatiemaatschappij.
Heb ik tot dusver aangestipt de ongeautoriseerde kennisneming van gegevens, in het verlengde hiervan ligt de manipulatie ervan. De indruk bestaat dat veel vormen van gegevensmanipulatie reeds worden gedekt door strafbepalingen. Die vormen die bij voorbeeld vermogensverschuivingen tot gevolg hebben, zullen met de klassieke bepalingen kunnen worden aangepakt die ook voor fraude worden gebruikt. Eén van uw taken zal echter zijn om na te gaan of hierin toch niet lacunes zich bevinden van dien aard dat een aanvullende strafbaarstelling nodig is.

Platleggen
Zijdelings verband hiermee houdt het zogenaamde platleggen van een automatiseringssysteem. Gezien de toenemende afhankelijkheid van dergelijke systemen is de samenleving op dit punt kwetsbaar geworden. Een breed scala van motieven kan aan dergelijke gedragingen ten grondslag liggen. Waar het gaat om terroristische acties, zullen weinigen de staat het recht ontzeggen daartegen op te treden. Ook lijkt het onomstreden dat chantage langs deze weg strafbaar moet zijn. Eén van de vragen is echter of de artikelen 317 en volgende van het Wetboek van Strafrecht die spreken over 'bedreiging met geweld' of 'smaadschrift' hierin voorzien. Ook andere bepalingen komen mogelijk in aanmerking. Onzeker is echter of zich niet toch lacunes voordoen. Problematischer wordt het vraagstuk van het platleggen van een computersysteem, indien dit gebeurt in het kader van een arbeidsgeschil. Ik kan mij voorstellen dat u, zonder met een uitgewerkt voorstel te komen, toch een richting wijst waarin zou kunnen worden gegaan.

Joy-computing
Een laatste vraagstuk van geheel andere aard dat ik in dit verband wil aanstippen is het ongeautoriseerde gebruik van een computer. In het Nederlands recht is in het algemeen het gebruik van eens anders goed zonder diens toestemming, niet strafbaar. De kraakproblematiek is hiervan een duidelijk voorbeeld. De Wegenverkeerswet kent op deze regel een uitzondering, te weten de zogenaamde joy-riding. Er zijn stemmen opgegaan om naar analogie daarvan 'joy-computing' eveneens strafbaar te stellen. In beide gevallen betreft het immers voor het publiek makkelijk toegankelijke goederen, waarbij van de eigenaar bezwaarlijk kan worden verlangd dat hij, zoals overigens voor zijn goederen, maatregelen neemt om het ongeautoriseerde gebruik tegen te gaan. Werd joy-riding, vóór de specifieke strafbaarstelling in de Wegenverkeerswet, vervolgd wegens diefstal van benzine, zo is denkbaar joy-computing te vervolgen wegens de diefstal van elektriciteit. Afgezien van de oneigenlijke constructie en de mogelijke wanverhouding tussen het telastgelegde delict en de aangerichte schade, is het de vraag of steeds wel meer elektriciteit wordt verbruikt dan zonder joy-computing het geval zou zijn geweest.

Strafvordering
Tot dusver heb ik gesproken over het materiële strafrecht: welke gedragingen zouden strafbaar moeten zijn en in hoeverre is daarin reeds voorzien. Daarmee hangt uiteraard samen de uitoefening van strafvorderlijke bevoegdheden. Het heeft geen zin wettelijke bepalingen in het leven te roepen die niet kunnen worden gehandhaafd. Derhalve behoort ook het formele strafrecht tot uw takenpakket. Het kennisnemen van informatie

door de politie, de officier van justitie en de rechter-commissaris is in het Wetboek van Strafvordering thans summier geregeld. De artikelen 105 en volgende gaan uit van voorwerpen. Blijkens artikel 107, tweede lid, wordt daarbij tevens gedacht aan informatiedragers. Van dergelijke voorwerpen kan de uitlevering worden gevorderd, doch de desbetreffende bepalingen bevatten ruime uitzonderingsgronden. Deze stoelen voor een deel op het belangrijke beginsel dat van de verdachte niet de medewerking aan zijn veroordeling kan worden verlangd. Afgezien van de ethische lading van het beginsel, stuit de doorbreking ervan ook op praktische bezwaren. Een verdachte die iets heeft te verbergen zal onder omstandigheden liever de sanctie van niet-medewerking riskeren, dan meehelpen aan het ontdekken van een gedraging die hem een veel zwaardere sanctie oplevert. De uitzonderingen op dit beginsel zijn daarom schaars. Wederom is het de Wegenverkeerswet, die gezien het maatschappelijk belang en de massaliteit van het wegverkeer hierin voorop loopt. Uw commissie zal dienen te bezien of overeenkomstige overwegingen dienen te gelden voor de computercriminaliteit dan wel of andere oplossingen uitweg bieden.
In dit verband mag de internationale strafrechtelijke samenwerking niet onvermeld blijven, hoewel uw commissie hieraan slechts zijdelings aandacht zal hoeven te schenken, gelet op het reeds geëntameerde overleg op internationaal niveau. De reeds aangestipte mogelijke vervaging van het begrip 'locus delicti' in de sfeer van de computercriminaliteit en het daarmee veelal verbonden toepasselijke rechtsstelsel, maken een aantal van de bestaande verdragsrechtelijke instrumenten onbruikbaar.
De artikelen 552h en volgende van het Wetboek van Strafvordering regelen op nationaal niveau de uitvoering van internationale verzoeken om rechtshulp. Wat betreft de uitlevering aan andere landen van personen, is de Uitleveringswet van toepassing. Het lijkt mij dat uw commissie dit onderwerp niet uitputtend zal kunnen behandelen gezien het pas kort geleden begonnen internationaal overleg. Zoudt u hierover desondanks een aantal beschouwingen kunnen leveren, dan zou ik dit op prijs stellen.

Omvangrijke taak
Mijnheer de voorzitter, geachte aanwezigen, ik realiseer mij dat, hoezeer ik ook getracht heb uw taakopdracht te beperken tot het strafrecht, en daarbij allerlei deelgebieden van het recht terzijde heb gesteld, u desondanks voor een omvangrijke taak staat. Ik ben mij er van bewust dat vele instanties en personen uw werkzaamheden aandachtig zullen volgen en mogelijk daaraan ook een bijdrage zullen willen leveren.
In de samenstelling van uw commissie is ook bewust gestreefd naar beperking. Zo zijn daarin, hoezeer dat wellicht ook vóór de hand zou hebben gelegen, geen vertegenwoordigers van andere departementen opgenomen. Zou op dit uitgangspunt een uitzondering zijn gemaakt, dan zou uw commissie vele malen groter zijn geweest en daarmee, vrees ik, hebben ingeboet aan slagvaardigheid. Ik vertrouw er echter op dat u de ruime deskundigheid en de vele verlangens die ook buiten uw kring leven, hun weg zult laten vinden in de rapportage aan mij. Ik hoop dat u erin zult slagen op het gebied van wat in de wandeling wel wordt aangeduid als computercriminaliteit, een basis te leggen voor het verdere werk aan onze strafwetgeving, zodat dit een betrouwbaar baken zal blijven in een zich veranderende maatschappij.
In 1986 zal de herdenking plaatsvinden van het 100-jarig bestaan van het Wetboek van Strafrecht. Eén van de verschillende symposia die hieraan zullen zijn gewijd, is het symposium 'Strafrecht in de informatiemaatschappij', dat zal worden gehouden op 22 april 1986 te Amsterdam. Zo duurzaam en flexibel als het Wetboek van Strafrecht is gebleken te zijn, zo duurzaam en flexibel mogen uw voorstellen worden, bestand tegen vele technische ontwikkelingen gedurende in ieder geval een aantal decennia. Uw voorstellen zullen daarom enerzijds een zekere afstand moeten hebben tot de huidige stand der techniek en meer functioneel moeten omschrijven, ongeacht de daaraan ten grondslag liggende technische middelen, welke gedragingen in de informatiemaatschappij als zodanig onoirbaar en schadelijk moeten worden beschouwd dat strafbaarstelling behoort plaats te vinden. Anderzijds zal de omschrijving van deze gedragingen zo bepaald moeten zijn dat een ieder weet waaraan hij zich heeft te houden en in welke gevallen hij de aanraking met de justitie riskeert.
Bij deze moeilijke taak wens ik u en uw commissie veel wijsheid. Want de computer lijkt wel snel te kunnen denken, maar in wijsheid onderscheidt de mens zich nog steeds van de computer.

COMPACT

Zomer/Herfst 1985

Antwoord voorzitter Franken:

Waken voor overcriminalisatie en voor ondercriminalisatie

Ook in de bestrijding van computerfraude en computermisbruik geldt de stelling dat het strafrecht een sluitstuk vormt van de inspanningen ter beteugeling van schadelijk gedrag. Gewaakt moet worden voor de gedachte dat het strafrecht de panacee kan zijn voor alle kwalen. Net als bij vele andere criminaliteitsvormen zullen preventieve maatregelen van technische, sociale en organisatorische aard voorop moeten staan. Met deze uitspraken relativeerde de voorzitter van de nieuwe Commissie Computercriminaliteit de verwachtingen die men van het strafrecht kan hebben. Mr. Franken waarschuwde voor het gevaar van zowel overcriminalisatie als van ondercriminalisatie. De commissie moet het juiste evenwicht vinden.

Geachte minister! – U kwalificeerde de taak waar de commissie voor staat als 'moeilijk'. Even daarvoor sprak u van een omvangrijke opdracht, die moet leiden tot, zo wetswijziging nodig lijkt, voorstellen met een draagwijdte van decennia. Toch dient de commissie in één jaar haar werkzaamheden te voltooien. Daaruit spreekt een groot vertrouwen in de slagvaardigheid van en de samengebrachte deskundigheid binnen de commissie, misschien wel van een overdadig optimisme. Doch dat zal aan het einde van de rit pas kunnen blijken. Veel zal afhangen van de mate waarin het zal lukken een op technologie georiënteerde denktrant zinvol te verbinden met strafrechtelijk denken. Daarbij zal de commissie snel moeten werken, waarbij een evenwicht gevonden moet worden tussen enerzijds een voldoende bijdrage van personen en instanties die niet een directe lijn naar de commissie hebben, en anderzijds een vruchtbare ontwikkeling der gedachten binnen de beperkte kring der commissieleden.
Met genoegen mag ik vaststellen dat het gelukt is een commissie te vormen uit personen waarvan verscheidene leden zich geruime tijd al bezig hebben gehouden met het verschijnsel van computermisbruik. Uit hun geschriften, alsook uit andere literatuur, komt naar voren dat de elektronische revolutie mede heeft geleid tot de totstandkoming van schadelijke gedragingen die moeilijk of helemaal niet zijn te vangen met tot het juridische instrumentarium behorende kwalificaties. De mogelijkheden van de automatisering betekenden ook nieuwe perspectieven voor kwaadwillenden. Als willekeurig voorbeeld noem ik het door een persoon in land A teweeg brengen van illegale vermogensverschuivingen in land B via land C.

Witte-boordendelicten
In sommige landen, waar de automatisering eerder dan hier grote vlucht nam, is gebleken dat de nieuwe gelegenheidsstructuren inderdaad meer dan incidenteel tot misbruik leidden. Gesproken kan worden van typische witte-boordendelicten, waarbij de schade nogal eens honderdduizenden, zo niet miljoenen guldens bedraagt. Maar ook in Nederland is al niet meer sprake van alleen incidenteel misbruik. Hoewel het niet makkelijk is hieromtrent betrouwbare opgaven van slachtoffers te krijgen, komt uit onderzoek toch naar voren dat het misbruik een duidelijke verbreiding kent.
De vraag waarvoor u de commissie stelt, is in hoeverre het strafrecht aanpassing behoeft gezien de ontwikkelingen bij geautomatiseerde gegevensprocessen en het misbruik daarbij. Het is wellicht nuttig stil te staan bij de rol die het strafrecht speelt bij het tegengaan van bedoeld misbruik.
Zoals in het algemeen geldt, is ook hier de stelling van toepassing dat het strafrecht een sluitstuk vormt van de inspanningen ter beteugeling van schadelijk gedrag. Gewaakt moet worden voor de gedachte dat het strafrecht de panacee kan zijn voor alle kwalen. Net als bij vele andere criminaliteitsvormen zullen preventieve maatregelen van technische, sociale en organisatorische aard voorop moeten staan. Hiermee relativeer ik de verwachtingen die men van het strafrecht kan hebben. De functie van het strafrecht op dit nieuwe terrein is er mijns inziens in belangrijke mate in gelegen, dat duidelijke normen worden gesteld, dat expliciet wordt gemaakt wat maatschappelijk als zodanig onoirbaar geldt dat het zware geschut van vervolging en bestraffing in stelling kan worden gebracht.

Evenwicht
Het spreekt vanzelf dat daarbij gewaakt moet worden voor zowel overcriminalisatie als voor ondercriminalisatie. Immers, overcriminalisatie zou inhouden dat zo'n breed scala aan gedragingen onder de werking van het strafrecht wordt gebracht, dat van handhaving onvoldoende terecht komt. Daarmee wordt het wapen van het strafrecht bot en wordt aan geloofwaardigheid ingeboet. Anderzijds, een wel zeer enge omschrijving van strafbaar gestelde gedragingen zou inhouden dat de overheid onmachtig is op te treden tegen bepaalde duidelijke schadelijke gedragingen. Het is het vinden van een bevredigend evenwicht dat voor de commissie een grote uitdaging zal vormen.
Daarbij zal de commissie zich niet kunnen onttrekken aan de vraag van de handhaafbaarheid. Ten aanzien daarvan lijkt het ook van gewicht dat op het praktische niveau van het ontwikkelen van specifieke automatiseringsdeskundigheid en het creëren van bijzondere faciliteiten ten behoeve van de opsporing en de vervolging het nodige gebeurt. Uiteindelijk zal het van dergelijke maatregelen afhangen of het strafrecht ook in de praktijk van de automatisering zinvol wordt gehanteerd.

Duidelijkheid
Het met eventueel aangepaste bepalingen scheppen van duidelijkheid waar die voorheen ontbrak is niet alleen zinvol tegenover degenen die schadelijk gedrag tentoonspreiden, ook voor slachtoffers en potentiële slachtoffers is het goed te weten tot op welke hoogte ze bescherming van het strafrecht genieten. In ieder geval, zo maakte ik al duidelijk, blijven buiten de sfeer van het strafrecht vele gewichtige taken