KPMG Klynveld EDP Audit Services

87/2
zomer 1987

COMPACT

Uit de inhoud

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

INHOUDSOPGAVE

Nummer 44 **Zomer 1987**
ISSN 0920-1645

COMPACT

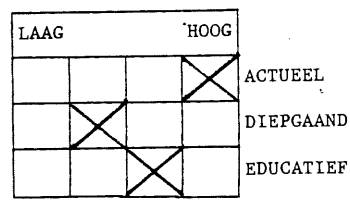
Zomer 1987

VAN DE REDACTIE

Het thema van dit zomernummer betreft moderne betaalvormen. Een drietal hoofdartikelen behandelen een aantal facetten van dit boeiende onderwerp.

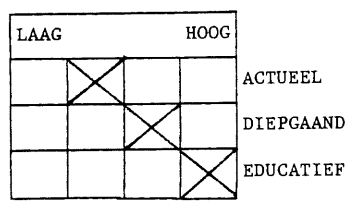
In het volgende Compact-nummer zal de problematiek vanuit andere gezichtspunten worden besproken.

Consequenties voor de beheersbaarheid
ten gevolge van
nieuwe technologische ontwikkelingen
door A.W. Neisingh



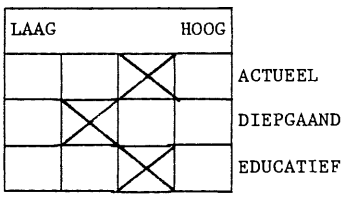
Het toepassen van nieuwe informatietechnologie kan organisaties bloot stellen aan nieuwe bedreigingen. Door de leiding van een organisatie dient bij de introductie van nieuwe informatietechnologie op deze bedreigingen te worden geanticipeerd met het treffen van beveiligingsmaatregelen. Dit artikel behandelt een aantal moderne betaalvormen en geeft daarbij aan welke bedreigingen aanwezig zijn en welke maatregelen daarbij van belang zijn. Hierbij is uitgebreid verwezen naar de thans beschikbare internationale standaards op dit gebied.

Betalingsorganisatie en automatisering
binnen de organisatie
door J. ten Wolde



Op degelijke wijze wordt in dit artikel een overzicht gegeven hoe geautomatiseerde betalingen kunnen worden beheerst binnen een organisatie. Aandacht wordt gegeven aan activiteiten van de BGC en Postbank met betrekking tot de wijze van aanlevering van de betalingsopdrachten.

Electronic banking-systemen in de praktijk
door drs. D.M. Swagerman



Ten behoeve van het bedrijfsleven en het publiek hebben zich de afgelopen twee jaar een aantal ontwikkelingen voorgedaan met betrekking tot het opvragen van saldo-informatie, het aanleveren van betalingsopdrachten en het ontvangen van dagafschriften. Banken stellen hun cliënten produkten beschikbaar om deze informatie met behulp van datacommunicatie uit te wisselen. Dit artikel geeft een overzicht van de situatie in Nederland.

Redactiewisseling

Sedert 1985 heeft Aad H.C. Koedijk een rol gespeeld bij de totstandkoming van Compact.
In die periode viel het uitbrengen van de jubileumbundel "24 over EDP-auditing", waaraan hij een belangrijke bijdrage heeft geleverd.
Door zijn vertrek naar KPMG Klynveld Bosboom Hegener raakt de redactie een ervaren redacteur kwijt. Wij zijn verheugd dat Hans Weerd zijn plaats heeft ingenomen.

Bedankt Aad; succes Hans.

Dick Steeman
Dries Neisingh
Henk van der Wielen.

Zomer 1987

COMPACT (R) is een uitgave van
KPMG Klynveld EDP Audit Services

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

Redactie:
A.W. Neisingh
Prof. D. Steeman
H. Weerd
H.J.M. van der Wielen (secr.).

Kopij kunt u inleveren bij de
secretaris van de redactie.
Adres:
Prinses Irenestraat 59,
1077 WV Amsterdam.
Toekomstig adres:
World Trade Center
Strawinskylaan 1257
Toren D 11e etage
1077 XX AMSTERDAM
Postadres:
Postbus 7137
1007 JC Amsterdam.

ISSN 0920-1645

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

Deze keer het zoeklicht op een tweetal recent verschenen boeken beide uitgebracht door KPMG Klynveld Bosboom Hegener.

"KIJK OP ORGANISATIES*"
onder redactie van D. Boom, J. Fennema, L.C.J. van den Hoek
door mevrouw drs. A. Klaver

"Kijk op organisaties" is een bundel artikelen over management, organisatie en informatieprocessen. De bundel bevat een selectie van artikelen door KBH-medewerkers geschreven met het doel een zo breed mogelijk beeld te geven van het werkterrein van een organisatie-adviseur. Deze selectie is onderverdeeld in een aantal groepen van artikelen met ieder hun eigen thema, te weten: management, omgeving, structuur, beheersing, informatie, automatisering, overheid, teams, opleidingen, advisering. Wij hebben ter bespreking een artikel gekozen uit het hoofdstuk dat als thema automatisering heeft.

Dit artikel heet: "Automatisering voor de rechterhersenhelft", door A. Kranendonk RA.
Onze hersenen bestaan uit twee helften, een linker- en een rechterhersenhelft. De linkerhersenhelft is analytisch ingesteld. In deze helft is de logica en het denken in details gezeteld. De rechterhersenhelft overziet het geheel en bevat verder onze creativiteit.

De huidige automatiseringsaanpak is gericht op de linkerhersenhelft, alleen de technische aspecten worden veelal in de besluitvorming betrokken. De aanpak van automatiseringsprojecten die in het artikel voorgestaan wordt (de zogenaamde STAA-methode) geeft aandacht aan zowel de technische als de sociale aspecten van automatisering binnen organisaties. Bij het ontwikkelingsproces dienen alle betrokkenen te participeren en niet alleen de technische automatiseerders.

De afkorting "STAA" staat voor "Socio-Technische Aanpak van Automatisering".
De socio-technische aanpak ziet zich voor drie opgaven geplaatst: rekening houden met de sociale dimensie van het informatiesysteem, een oplossing van samenwerkingsproblemen bij de ontwikkeling en het besef van de invloed van de huidige situatie binnen het bedrijf. STAA is te scheiden in het STAA-produkt en het STAA-proces.
Aan het STAA-produkt (het te ontwikkelen geautomatiseerde informatiesysteem) zijn bepaalde eisen te stellen. Deze eisen worden ontleend aan een bepaalde kijk op organisaties. In deze visie bestaat een organisatie uit elkaar wederzijds beïnvloedende componenten, zijnde taken, structuur, mens en technologie. Wanneer in één van deze componenten iets verandert (bij-

* Uitgeverij Stenfert Kroese; ISBN 90 207 1543 7.

voorbeeld in de technologie, door de ontwikkeling van een geautomatiseerd informatiesysteem) dient met de invloed van en op de andere componenten rekening gehouden te worden.

De mens in de organisatie manifesteert zich in drie rollen: hij is niet alleen de uitvoerder van een concrete taak (zoals hij binnen de technische aanpak gezien wordt) maar ook een behartiger van zijn eigen belangen en een burger met eigen normen en waarden.

Met het bovenstaande in het achterhoofd zijn bepaalde eisen aan het STAA-produkt te stellen. Enkele van deze eisen zullen de automatiseerder van de oude stempel opruiend in de ören klinken: de gebruikers mogen niet te afhankelijk worden van het systeem en het systeem mag niet alle operationele beslissingen overnemen. Er moet vrijheid in het werk overblijven. Verder moet het systeem bijvoorbeeld ruimte voor nieuwe mogelijkheden overlaten, omdat de mens en de organisatie behoefte hebben aan creativiteit.

Ook aan het STAA-proces zijn bepaalde eisen te stellen.
Het ontwikkelingsproces moet geen multi- maar een interdisciplinaire aanpak inhouden. In andere woorden gesteld: de verschillende disciplines moeten elkaar niet aanvullen, maar geïntegreerd werken. Hiertoe is een effectieve samenwerking vereist, waarvoor een leerproces noodzakelijk is. Daarom legt STAA een grote nadruk op de eerste fasen van het proces. Deze fasering gaat vooraf aan de fasen die gebruikelijk aan systeemontwikkeling gesteld worden. Deze fasen vallen uiteen in een algemene introductie (een "snuffelfase") een minder vrijblijvende voorwaarden scheppende fase (bevat bijvoorbeeld confrontaties tussen de waarnemingen van de adviseur en de conclusies van de deelnemers) en een fase van contract en werkafspraken. Pas hierna komt het gehele traject van informatie- en automatiseringsbeleid en het uitvoeren van concrete projecten.

STAA vraagt veel extra tijd in de beginfasen. Wat is hier nu het rendement van? Het rendement van STAA ligt in het vermijden van dure mislukkingen en in het verbeteren van het klimaat voor automatisering.

"ONDERNEMEN MET INFORMATIETECHNOLOGIE*"
onder redactie van drs. A.H.J.B. Schotgerrits en anderen
door mevrouw drs. A. Klaver

In deze publicatie, die als ondertitel heeft "een commerciële strategie voor bedrijven en overheden" wordt uiteengezet dat de informatie technologie van een passief hulpmiddel naar een actief instrument voor ondernemers evolueert. De informatie technologie heeft invloed op de produkten en diensten zelf, op de distributie en promotie en op alle andere elementen van de marketing-mix.

* Samsom Uitgeverijen; ISBN 90 14 03778 3.

Voorbeelden van deze informatietoepassingen met strategische aspecten zijn er te over. Zo kan men in een eenvoudig geval denken aan software ter optimalisatie van voorraadposities. Als gecompliceerdere voorbeelden geven de schrijvers het inbrengen van stuurinformatie in auto's en electronic banking. De informatiesystemen tussen verschillende organisaties zijn het belangrijkst. Hierbij valt te denken aan de klant die per terminal informatie ontvangt over de prijzen van zijn leverancier.

De primaire invalshoek van management bij het gebruik van strategische toepassingen is het verbeteren van de concurrentiepositie. Hiertoe kunnen verschillende basisstrategieën gevolgd worden. Zo kan het voordeel in concurrentiepositie bereikt worden door kostenverlaging, door produktdifferentiatie of zelfs door diversificatie. De methode die past bij dit type automatiseringsprojecten is er een van prototyping. De bijdrage van het management in deze is het opsporen van de strategische systemen door middel van brainstormsessies.

Door de opkomst van de informatietechnologie dient er een verandering op te treden in het strategisch denken van ondernemingen. Het is niet langer voldoende te denken in produkt/marktcombinaties, er moet gedacht worden in produkt/markt/technologie combinaties. Het vermogen van een onderneming zich met haar produkt/markt/technologiecombinaties te onderscheiden van andere ondernemingen, bepaalt haar succes. Het management zal bij haar strategische beleidsvorming de ontwikkelingen in de informatietechnologie in het oog moeten houden. Het management zal moeten samenwerken met deskundigen op het gebied van de informatie technologie, zal de noodzaak tot een permanente aandacht moeten onderkennen en in het personeelsbeleid rekening moeten houden met het vereiste hoge kennisniveau.

Bij het vaststellen van het strategisch management kan de organisatie inspelen op technologische trends. Het gaat hierbij om trends in communicatietechnologie, in expertsystemen, in produktie-automatisering en nieuwe diensten en produkten zoals nieuwe technieken voor beeld- en gegevensopslag.

Het vierde hoofdstuk van het boek behandelt enkele praktijkvoorbeelden van toepassingen van informatietechnologie.

In het vijfde hoofdstuk wordt ingegaan op de methoden die het management kan gebruiken om mogelijkheden voor strategische informatietoepassingen te vinden. Zo kan de manager bijvoorbeeld aansluiting zoeken bij de informatie-intensiteit. Deze valt uiteen in het informatiegehalte van het produkt (hoeveel informatie heeft de afnemer nodig om het produkt te verkrijgen en te gebruiken) en de informatie intensiteit in het bedrijfsproces. Een voorbeeld van het gebruik maken van het informatiegehalte van het produkt is het digitaal vastleggen van wasprogramma's in wasmachines. Dit bevordert eenvoud in het gebruik en maakt een grote variatie in programma's moge-

lijk. In het vijfde hoofdstuk worden nog meer methoden besproken om mogelijkheden voor strategische informaticatoepassingen te vinden. Daarop wordt in deze bespreking niet ingegaan.

Het zesde hoofdstuk behandelt een fasegewijze aanpak van strategische toepassingen.

In het zevende hoofdstuk wordt ingegaan op de gevolgen van informatie technologie voor organisaties. Zo zal bijvoorbeeld de technologie leveranciers en afnemers met elkaar verbinden.
Medewerkers in bedrijven moeten ermee leren omgaan dat alle werk tijdelijk is en zij steeds omgeschoold zullen moeten worden.

Het laatste hoofdstuk behandelt de invloed van strategische toepassingen op informatieplanning.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Zomer 1987

CONSEQUENTIES VOOR DE BEHEERSBAARHEID TEN GEVOLGE VAN NIEUWE TECHNOLOGISCHE ONTWIKKELINGEN [1)]

door A.W. Neisingh

Inleiding

Organisaties staan bloot aan bedrijfsrisico's.
Met betrekking tot geautomatiseerde gegevensverwerking kunnen risico's met de navolgende consequenties optreden:
- Discontinuïteit;
- Onjuiste beslissingen ten gevolge van fouten;
- Fraude;
- Vertraagde invoering systemen;
- Wetsovertredingen (bijvoorbeeld ten aanzien van privacy).

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

Ingeval opnieuw beslist moet worden over wijzigingen in de toegepaste informatietechnologie, zal moeten worden vastgesteld of het beveiligingsbeleid moet worden bijgesteld en wat de invloed is op het geïmplementeerde beveiligingssysteem. Het heeft bijvoorbeeld geen zin om te investeren in encryptie-apparatuur voor de datacommunicatieverbindingen als afdelingspersoneel met triviale password/username-combinaties kan binnenkomen in het systeem.

Dat wil zeggen met als uitgangspunt het geldende beveiligingsbeleid behoort het management te anticiperen op de consequenties van de introductie van nieuwe technologieën door bijstelling/actualisering van de overall beveiligings-policy.

---

1) Dit artikel is gebaseerd op de lezing "New opportunities and new risks in security and control" die door A.W. Neisingh is gehouden op het Payment Systems International (PSI) 10th anniversary symposium on Banking's Triple Challenge: New Technology, New Competition, New Marketing, November 10 to 13, 1985 in Copenhagen.
In verband met nieuwe ontwikkelingen is het artikel geactualiseerd.

Ontbreekt zo'n beveiligingsbeleid dan zullen afdelingen en/of individuen veelal op ad-hoc basis beveiligingsmaatregelen treffen. Risico hiervan is dat een beveiligingszeef in plaats van een -schild rond een bedrijf wordt gelegd.

Overduidelijk manifesteren de bedreigingen en de invloed van toegepaste informatietechnologie zich in het betalingsverkeer in het algemeen en bij banken in het bijzonder.

Hierna wordt ingegaan op bedreigingen met betrekking tot communicatie, alsmede op de zogenaamde bankkaarttoepassingen.
Onder "bankkaarten" wordt hier verstaan: plastic kaarten, die als identificatiemiddel voor bankdiensten worden gebruikt.
Als voorbeelden van bankkaarttoepassingen zullen worden behandeld:
- betaalautomaten (Electronic Funds Transfer at the Point Of Sales, of wel EFTPOS);
- gelduitgifte-automaten (Automated Teller Machines, of wel ATM's).

Tevens wordt een overzicht gegeven van de internationale (ISO) standaards met betrekking tot bankkaarttoepassingen en wordt ingegaan op elektronisch bankieren te zamen met audit-aspecten van dergelijke toepassingen.

Communicatie

Een van de meest risicogevoelige aspecten van de hedendaagse technologie is communicatie.

Zo is bijvoorbeeld de internationale bankwereld meer dan ooit afhankelijk van elektronische informatie-overdracht. Hoewel nieuwe technieken, zoals fiber en satellietverbindingen het onderscheppen van informatietransport moeilijker hebben gemaakt, blijft het zaak attent te zijn op de kwetsbaarheid van communicatielijnen in een bankomgeving.
Hierbij zij aangetekend, dat bij alle aandacht die de beveiliging van gegevens- en telexverbindingen krijgt, andere zoals vocale communicatie dikwijls wordt verwaarloosd.

Elke communicatielijn is in aanleg kwetsbaar voor bedreigingen zoals:
a. Het vrijkomen van de inhoud van berichten.
   Dit gebeurt wanneer informatie uit een verzonden boodschap uitlekt of door een indringer in het systeem wordt gestolen.
b. Analyse van het berichtenverkeer.
   Hieronder wordt verstaan het zich toeëigenen van informatie door een indringer, waarbij deze analyseert wanneer en waarheen boodschappen door het systeem worden verzonden.
c. Wijzigingen in de berichtenstroom.
   Dit is het wijzigen van een bericht tussen twee knooppunten of systemen in.

d. Weigering van een bericht.
   Hierbij wordt door een indringer een boodschap geblokkeerd, waardoor de verbinding wordt verstoord.
e. Blokkeren van een bericht.
   Dat is verstoring van het berichtenverkeer ten gevolge van door een indringer veroorzaakte vertraging in de aflevering van berichten.
f. Masquerade.
   Hierbij heeft de ontvanger van de boodschap onvoldoende zekerheid ten aanzien van de identiteit van de afzender.

Onder andere de International Organisation of Standardisation (ISO)[2]) heeft getracht een definitie te geven van beveiligingsfuncties die een veilige informatie-overdracht tussen open systemen mogelijk maken. Zij stelt hierbij dat het uiteindelijke doel van de beveiliging van gegevensverkeer is de kosten van de verkrijging of wijziging van gegevens hoger te maken dan de mogelijke waarde van het verkrijgen of wijzigen van de gegevens. Omdat in de ISO standaardisatie-organisaties uit zo'n 100 landen zijn vertegenwoordigd, duurt het vaak lang voordat concrete afspraken ten aanzien van standaardisatie zijn gemaakt. Een bijkomend nadeel is het gebrek aan formele zeggenschap dat van de ISO uitgaat.

Electronic Funds Transfer at the Point Of Sale (EFTPOS) als voorbeeld van de interrelatie tussen de risicogebieden

De zwaarste eisen ten aanzien van veilige transacties binnen een groot commercieel netwerk treffen we waarschijnlijk aan bij een EFTPOS-systeem. We zullen de interrelatie tussen de reeds eerder genoemde risicogebieden toelichten door als voorbeeld een EFTPOS-model te bekijken, met aandacht voor de transactiestructuur en de netwerkfuncties.

Een EFTPOS-transactie bestaat uit drie fasen, te weten de autorisatie van het verzoek, het op gang brengen van de transactie en het vastleggen van de gegevens. Elke fase bestaat uit een aantal activiteiten, die door netwerkfuncties moeten worden uitgevoerd.

1. Autorisatie kan verder worden onderverdeeld in vier verschillende subfuncties, te weten:
   - een verzoek om toegang: de kaartverstrekker controleert de geldigheid van de terminal, de authenticiteit van de transactie en de identiteit van de kaarthouder;
   - het verlenen van toegang: de kaartverstrekker geeft de voorwaarden aan waarop hij toegang verleent, de beperkingen die gelden ten aanzien van de transactie en de eerste vereisten waaraan dient te worden voldaan;

2) ISO: working draft addendum to ISO 7498 to cover security architecture (1984).

- een onderhandelingsfase: in deze fase worden tussen partijen (namelijk de kaarthouder en de detaillist) afspraken gemaakt over details van de transactie;
- een overeenstemmingsfase met toestemming van de partijen om door te gaan op basis van deze overeenkomst.

Het Persoonlijk Identificatienummer (PIN) dient de kaarthouder tot machtiging en mag alleen ter verificatie van berichten worden gebruikt nadat overeenstemming is bereikt.

2. Na verlening van de machtiging vindt de eigenlijke fysieke transactie plaats, die eindigt met een journaalboeking van de transactie en een kwitantie. Hier kan de transactie niet meer worden teruggedraaid omdat de consument de winkel heeft verlaten. Het is nu de taak van het EFTPOS-systeem de transactiegegevens vast te leggen en verder te verwerken.

3. Zo'n vastlegging van gegevens bestaat uit twee bewerkingen: de onvertraagde vastlegging van de gegevens op ("recoverable") disk of tape en, vervolgens, het doorsturen van de details van de transactie naar de betrokkenen.

   Ten behoeve van de integriteit van de gegevens dient van alle transacties de rechtmatige herkomst te worden vastgesteld en wel: door een netwerkfunctie met behulp van de PIN-code van de kaarthouder.
   Deze transacties moeten worden bevestigd: door een netwerkfunctie met gebruikmaking van de bevestigingscode van de bank van de detaillist.
   De bevestigingen moeten worden erkend: door een netwerkfunctie met behulp van een bevestigingscode die hoort bij de terminal van de detaillist.
   Na positieve bevestiging gaat de verantwoordelijkheid voor de transactiegegevens, met inbegrip van de recovery en de integriteit, over van de detaillist op zijn bank. De detaillist kan nu zijn kopie van deze transactiegegevens uitwissen.

   De verdere verwerking van de transactiegegevens door het bancaire systeem is voor het netwerk van geen belang; de transactiestructuur en de inhoud van het bericht dienen echter een geautomatiseerde en efficiënte afstemming te ondersteunen en een niet weerlegbare basis voor een audittrail te vormen.

De algemene netwerkstructuur bevat de drie elementen van de belangrijkste netwerkfuncties als afzonderlijke onderdelen.

De algemene netwerkstructuur voorziet in:
1. een eindgebruiker interface en controle in de terminal van de detaillist;

2. data recovery, controle van transacties en routing in het knooppunt waar gegevensvastlegging plaatsvindt;
3. het transporteren van boodschappen;
4. gateway functies tussen de EFTPOS-terminal en de gastheersystemen;
5. een autorisatiesysteem ten behoeve van de gebruiker;
6. een kaartuitgevende instelling die optreedt ten behoeve van de detaillist;
7. netwerkbeheersfuncties.

Door nu de functies van één of een aantal componenten samen te voegen kunnen veel verschillende netwerkimplementaties worden gecreëerd. Al deze implementaties zijn feitelijk afleidingen van de algemene netwerkvorm.
Het knooppunt waar gegevensvastlegging plaatsvindt, de gegevenstransporten de netwerkbeheersfuncties worden gedeeld door de detaillist, de kaartuitgevende instelling en de bank van de detaillist.
Deze gedeelde functies beïnvloeden de systeembeveiliging, maar juist omdat ze gedeeld worden hebben de drie bovengenoemde partijen er geen directe zeggenschap over. Vandaar dat de beveiliging dusdanig moet worden aangepakt dat het gezamenlijk gebruik van het EFTPOS-systeem mogelijk is zonder dat dit een bedreiging vormt voor de betrokken partijen.
Zo'n aanpak dient een vereiste te zijn voor het EFTPOS-systeem. De besluiten ten aanzien van het ontwerp dienen op deze aanpak te worden afgestemd.

Alhoewel er veel beveiligingsmaatregelen kunnen en zullen worden genomen ten einde de kans op, respectievelijk de omvang van geldverlies te verminderen, is het niet mogelijk alle risico's van verlies uit te sluiten.

Hier belanden we bij een van de grootste problemen van elektronisch geldverkeer: de acceptatie door de consument. Er bestaat onder consumenten nogal wat verwarring en scepsis ten aanzien van het functioneren van computers in het algemeen en van elektronisch geldverkeer in het bijzonder.
Als de consument duidelijk gemaakt wordt welke beveiligingsmaatregelen er in EFTPOS-systemen genomen zijn, zal dit wantrouwen waarschijnlijk afnemen. Een volgende stap zou kunnen zijn het ontwikkelen van een soort verzekering die de consument van allerlei mogelijke financiële verliezen zou kunnen vrijwaren. Hierbij dient ook te worden gedacht aan aantasting van de privacy van de consument. [3]

Het gebruik van standaards bij EFTPOS-systemen

Bij de EFTPOS-systemen zijn standaards onontbeerlijk, niet alleen om voortgang te boeken in de ontwikkeling van deze systemen (compatibiliteit), maar ook omdat ze van groot belang zijn voor het creëren van internationaal

3) Richards, R.M. and Guynes, J.L.
A strategic plan for reducing consumer anxiety about EFT security.
ACM/SIGSAC, spring 1986.

aanvaarde beveiligingsvoorwaarden welke in de EFTPOS-omgevingen in aanmerking dienen te worden genomen.

De International Organisation of Standardisation (ISO) te Genève heeft al een aantal standaards voor EFTPOS-systemen en voor daaraan verwante gebieden ontwikkeld of is daar nog mee bezig.

1. Standaards voor plastic kaarten [4]

Deze standaards hebben betrekking op de fysieke en chemische eigenschappen van de kaart en op de magneetstripcodering. De sporen 1 en 2 bevatten informatie (onder andere de naam en het nummer van de kaarthouder) die niet overschreven dient te worden. Spoor 3 kan worden gebruikt bij zowel on-line als off-line toepassingen. Deze informatie kan wel overschreven worden.

4) ISO 4909 : Bank cards - Magnetic stripe content for track 3
ISO 7810 : Identification cards - Physical characteristics
ISO 7811/1: Identification cards - Recording technique
part 1: Embossing
ISO 7811/2: Identification cards - Recording technique
part 2: Magnetic stripe
ISO 7811/3: Identification cards - Recording technique
part 3: Location of embossed characters on ID-1 cards
ISO 7811/4: Identification cards - Recording technique
part 4: Location of read-only magnetic tracks - tracks 1 and 2
ISO 7811/5: Identification cards - Recording technique
part 5: Location of read-write magnetic track - track 3
ISO 7812 : Identification cards - Numbering system and registration procedure for issuer identifiers
ISO 7813 : Identification cards - Financial transaction cards.

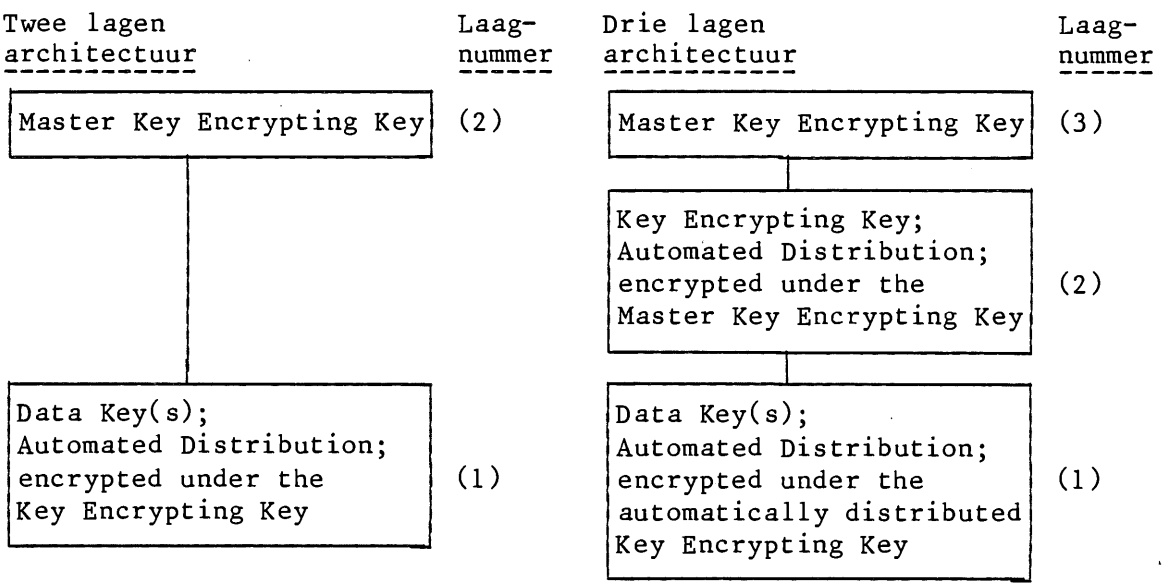
2. Standaards voor verificatie [5]

Deze standaards hebben betrekking op het (geautomatiseerde) key management en beveiligingskenmerken van verificatie-algoritmen. Verificatie is een belangrijk EFTPOS-gegeven omdat:

- zij garandeert dat het ontvangen bericht identiek is aan het verzonden bericht (validatie van de boodschap);
- zij het bewijs levert dat het afkomstig is uit de bron van waaruit het zegt afkomstig te zijn en dat deze bron gemachtigd is de ontvangen opdrachten te geven (autorisatie van de boodschap).

Eén van de doelstellingen is de key management procedures te automatiseren (zonder handmatige tussenkomst), waarbij de sleutels ook versluierd zijn en zodoende in openbare netwerken kunnen worden getransporteerd.

Volgens ISO/DP 8732 dient de architectuur van het systeem van geautomatiseerd key management uit twee of drie lagen te bestaan (zie figuur 1).



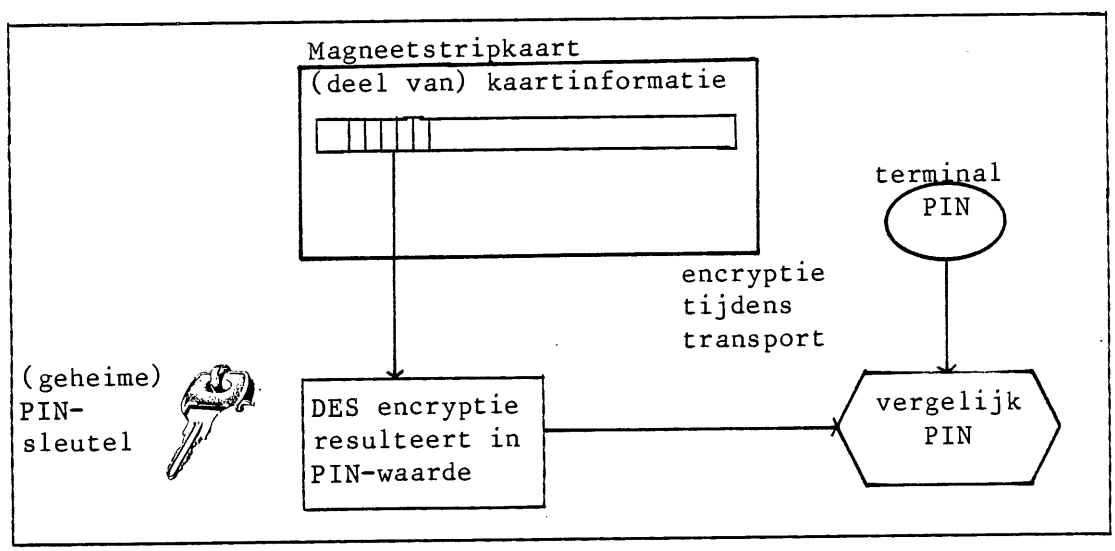
Figuur 1. Key distribution architecture.

5) ISO/DIS 8730 : Banking - Requirements for standard message authentication
ISO/DP 8732 : Banking - Key management (wholesale)
ISO/DIS 8731/1: Banking - Approved algorithms for message authentication part 1: DEA - 1 algorithm
ISO/DIS 8731/2: Banking - Approved algorithms for message authentication part 2: message authenticator algorithm.
ANSI X9.9.1982 Financial Institutions message authentication (wholesale).
ANSI X9.17-1985 Financial Institutions Key Management (wholesale)
ANSI X3.92-1981 Data Encryption Algorithm
ANSI X3.106-1982 Modes of Operation of DEA

3. Standaards voor PIN-management [6]

Deze standaards voorzien in een beschrijving van de uitwisseling van PIN-gegevens tussen financiële instituten en specificeren een aantal technieken voor het management en de beveiliging tijdens de levensduur van de PIN. Hierbij zij aangetekend dat de meeste procedures nog steeds manuaal geschieden. Zoals overal waar mensen in procedures met geheime gegevens zijn ingeschakeld, betekent dit een verzwakking ten aanzien van de beveiliging.

Een van de methoden voor PIN-generatie en verificatie is aangegeven in figuur 2. De PIN wordt hier gegenereerd op basis van (een deel van) de informatie die tevens in de kaart wordt opgeslagen, onder gebruikmaking van het DES-algoritme en een PIN-sleutel.
PIN-verificatie vindt plaats door herhaling van de operatie. De ontvanger vergelijkt deze uitkomst met de door de consument ingetoetste PIN. Locale PIN-verificatie is mogelijk wanneer gebruik wordt gemaakt van één PIN-sleutel, die in alle transactieterminals is opgeslagen. In een ATM-omgeving is dit algemeen gebruik, omdat deze apparatuur (fysiek) relatief veilig is.
In EFTPOS-systemen is het echter beter om de PIN centraal te verifiëren, bijvoorbeeld in de computer van de bank, omdat de betaalautomaat fysiek relatief minder veilig is. Hierbij dient de PIN versluierd over de lijnen van het netwerk verzonden te worden.



Figuur 2. PIN-generatie en -verificatie

6) ISO DP 9546/1: Banking - Personal identification number management and security, part 1 - PIN protection principles and techniques.
ISO DP 9546/2: Banking - Personal identification number management and security, part 2 - Approved Algorithm for PIN encypherment.

4. Standaards voor het formaat van berichten [7])

Dit betreft berichten die door een plastic kaart worden geïnitieerd.

5. Standaards voor geïntegreerde schakelingen (chip-kaarten) [8])

Deze standaards bevinden zich nog in een pril stadium. Momenteel is een werkgroep van het ISO hiermee bezig. Eén van de eerste problemen waarover zij zich dienen te buigen is de plaats waar de chip dient te worden aangebracht op de kaart.

Andere nieuwe technologieën zoals gelduitgifte-automaten brengen ook aanverwante risico's met zich mee

De gelduitgifte-automaat (Automated Teller Machine = ATM) maakt deel uit van het nieuwe dienstenpakket van banken en ook van andere organisaties. ATM's kunnen worden gebruikt voor de eigen bankdiensten dan wel gemeenschappelijk (gastgebruik) worden gebruikt. De ATM kan met een computer worden verbonden dan wel stand-alone worden gebruikt. In eerste instantie kan contant geld worden verkregen uit een gelduitgifte-automaat; verder zijn GEA's geschikt voor het uitvoeren van eenvoudige banktransacties, opvragen van saldi en storten van geld.

De PIN kan in de automaat met de kaartidentiteit worden vergeleken wanneer de PIN aan het rekeningnummer is gerelateerd; andere kaartgegevens kunnen worden gecontroleerd door een algoritme, bijvoorbeeld het gebruik van een cijfer met een geheime sleutel. Het feit dat men de relatie laat afhangen van een geheime PIN-sleutel die voor alle ATM's dezelfde is, houdt een risico in omdat deze code op zoveel plaatsen is geïnstalleerd.
Bekend raken van de key maakt het hele systeem onveilig, omdat een outsider dan zijn eigen kaarten kan maken en de PIN die daarbij past kan bepalen. De fysieke beveiliging rondom een ATM maakt het onwaarschijnlijk dat de geheime sleutel door inbraak zal worden ontdekt.

7) ISO/DIS 8583: Bank card originated messages - Interchange message specifications for financial transactions.

8) ISO/DIS 7816: Identification cards - Integrated cricuit(s) cards with contacts - Part 1 Physical characteristics.
ISO/DP 7816/3: Identification cards - Integrated circuit(s) cards with contacts.
Part 3: Electronic signals and exchange protocols.
Idem addendum 1: Structure and processing of commands in an asynchroneous transmission.
ISO/TC 97/sc 17/WG 4N229: Identification cards - Integrated circuit(s) card with contacts - Part 4: Interindustry commands for Interchange.

Een zwak punt in de beveiliging is de manier waarop de sleutel in de ATM wordt geladen. De sleutel kan het resultaat zijn van een berekening die gebaseerd is op gegevens uit verschillende bronnen, of het algoritme kan complex zijn en verschillende sleutels verlangen. Het is zo te regelen dat niemand toegang heeft tot alle gegevens die men nodig heeft om de sleutel in de ATM te laden.

De sleutels worden op twee plaatsen in het systeem gebruikt, namelijk bij de ATM's, ter controle op de relatie tussen de PIN en het rekeningnummer en andere kaartgegevens, en bij bijvoorbeeld het hoofdkantoor van de bank, waar de PIN's worden berekend ter verspreiding onder de cliënten van de bank. De beveiliging van de sleutel is in het centrale gebied waarschijnlijk het moeilijkst te realiseren. Risico's terzake komen in de een of andere vorm bij elk on-line systeem voor, ongeacht welke methode men centraal gebruikt voor het management van en de controle op de PIN's.
Daarom kan het extra risico bij een off-line ATM-systeem doordat de PIN-controles in iedere automaat worden uitgevoerd gering zijn wanneer het systeem goed wordt ontworpen.
De fysieke beveiliging van de ATM's vormt een wezenlijke factor bij deze beschouwing.

Personal Identification Number (PIN) management is tevens het onderwerp van een U.S. National Standard [9]. Drie typen PIN's worden onderscheiden, te weten:
- assigned derived PIN;
- assigned random PIN;
- customer-selected PIN.

Voor de gebruiker is het enig waarneembare verschil dat tussen een door de bank opgegeven (assigned) PIN en een PIN, die de gebruiker zelf kan kiezen.

De dialoog voor een on-line ATM dient ten minste de ATM-identificatie, de offsetwaarde en de PIN (versluierd) te bevatten.
De offsetwaarde (ook wel correctiewaarde genoemd) wordt gehanteerd om de PIN door een cliënt te laten wijzigen en/of bij verschillende systemen (betaalautomaat of geldautomaat) dezelfde PIN te kunnen hanteren.

In het geval van gezamenlijk gebruikte ATM-systemen doet zich een probleem voor: de door de verschillende banken gebruikte methoden om de PIN's met de kaartidentiteit te verifiëren zullen van elkaar verschillen; daarom kan geen enkele autonome algoritmebewerking in een ATM de PIN's van al zijn ATM-klanten verifiëren. Vandaar, dat de PIN-verificatie centraal door de respectieve kaartverstrekkers dient te geschieden; alle ATM's dienen on-line te zijn wanneer zij de klant van andere banken bedienen en alle ATM-processors van alle banken dienen met elkaar verbonden te zijn door middel van een communicatienetwerk.

9) ANSI X9.8 (1982) Personal Identification Number (PIN) management and security

Op ATM-gebied bestaan er drie grondvormen van fraude, namelijk:
- het onbevoegd gebruik van toegangsmiddelen. Bankkaarten of informatie ten aanzien van bankkaarten en PIN's kunnen worden verkregen door een onbevoegd gebruiker. Een dagelijkse opnamelimiet kan ertoe bijdragen de verliezen te beperken;
- fraude door een bevoegde kaarthouder. Kaarthouders kunnen ontkennen dat transacties hebben plaatsgevonden die hun eigen rekeningen betreffen;
- manipulatie door insiders. Personeel van de bank of van haar leveranciers kan bankkaarten stelen, geld onttrekken aan de ATM's, met rekeningen knoeien of één of andere elektronische aanval uitvoeren.

Ten slotte een paar opmerkingen ten aanzien van de wettelijke aspecten van ATM's.

Wanneer gebruik wordt gemaakt van gelduitgifte-automaten kunnen zich twee situaties voordoen waarbij sprake is van internationale gegevensoverdracht, namelijk:

1. wanneer men een ATM die zich in het buitenland bevindt in werking stelt met als resultaat een internationale overdracht van gegevens zoals de namen van de bij de transacties betrokken partijen, het bedrag en de aard en datum van de transactie;

2. wanneer een plaatselijke ATM in werking wordt gesteld voor een zuiver binnenlandse transactie, hetgeen kan betekenen dat de betrokken gegevens één of meerdere grenzen passeren omdat de gegevensstroom vanaf de bankfilialen op het hoofdkantoor is geconcentreerd.

Deze financiële gegevens zijn persoonlijke gegevens in de zin van een aantal Europese wetten ter bescherming van de persoonlijke levenssfeer omdat de gegevens informatie betreffen over een geïdentificeerd dan wel een identificeerbaar subject.

Deze privacy-wetten bevatten voorschriften die de internationale stroom van dergelijke gegevens naar landen die zulke gegevens geen gelijkwaardige bescherming bieden, beperken. In het bijzonder gegevensstromen naar de U.S. zijn aan die beperkingen onderworpen.

Men dient zich derhalve van het bestaan van deze voorschriften bewust te zijn en ook van de nationale wetten van alle doorgangslanden alsmede de landen van bestemming wanneer men gebruik maakt van een internationaal EFT-systeem of wanneer men een internationaal net gebruikt voor het overbrengen van persoonlijke gegevens. Het is daarom wellicht nuttig zich tot juridisch

adviseurs dan wel de plaatselijke autoriteiten belast met de bescherming van gegevens te wenden om erachter te komen of er zulke voorschriften zijn en, zo ja, wat hiervan de inhoud is.

Tot de nieuwe ontwikkelingen in de kaarttechnologie behoren ook de "supercard" en de "lasercard".
De supercard behoort tot de vierde generatie van de smart cards. De kaart bevat een eigen (klein) toetsenbord en beeldscherm, hetgeen autorisatie mogelijk maakt zonder dat hiervoor verdere apparatuur op het verkooppunt aanwezig is.
De lasercard bevat een optisch geheugen van maximaal 2 Mb. Verdere vergroting van de geheugencapaciteit is te verwachten. Dit geheugen kan zowel tekst als andere persoonlijke informatie, zoals foto's, vingerafdrukken of röntgenfoto's bevatten. Hierdoor worden nieuwe mogelijkheden geboden voor persoonlijke identificatie. De ontwikkeling van de lasercard is nog gaande.

"Front Office Automation" is een aspect van de nieuwe technologie dat een aantal nieuwe risico's inhoudt met betrekking tot de onbevoegde toegang tot informatie

Enerzijds maakt "Front Office Automation" het mogelijk de klanten meer privacy binnen de bank te bieden. Zij kunnen hun financiële aangelegenheden met bankpersoneel aan een bureau doorpraten in plaats van door kogelvrij glas. Maar, anderzijds, houdt "Front Office Automation" in dat het personeel in grotere mate toegang zal hebben tot persoonlijke informatie van de klant.

Laten we eerst eens vaststellen wat "Front Office Automation" inhoudt.

Allereerst is "Front Office Automation" een middel om de kwaliteit van het door banken aangeboden dienstenpakket te verbeteren. Dit betekent, bijvoorbeeld, dat het bankpersoneel de klanten een advies zal kunnen geven dat op hun financiële omstandigheden is toegesneden. De daaruit voortvloeiende betere en snellere dienstverlening kan resulteren in een groter marktaandeel en meer winst.
Dit kan worden bereikt door het geld- en gegevensverkeer op grote schaal te automatiseren.

Teneinde de bankbediende in staat te stellen de identiteit van een klant vast te stellen, dient de klant een kaart te overleggen en een Persoonlijk Identificatie Nummer, PIN-code genaamd, in te toetsen. De bankbediende zal via het beeldscherm toegang hebben tot de persoonlijke gegevens van de klant en diens financiële gegevens zoals saldi van rekeningen, kredietlimieten, effecten, opties, verzekeringen en dergelijke.

Het zal duidelijk zijn dat onder dergelijke omstandigheden een aantal interne controle- en beveiligingsmaatregelen dient te worden genomen. De infrastructuur van applicatieprogrammatuur en de computerinstallatie dient toereikend te zijn.

Het netwerk dat het filiaal met de centrale computer verbindt moet "waterdicht" zijn.

De organisatie van het filiaal dient adequaat te zijn, hetgeen inhoudt dat er ten aanzien van de omgeving voorschriften dienen te komen die de toegang tot de terminals, de toegang tot de netwerkprocessor etc. regelen. Dit betekent gebruik maken van functiescheidingen, ondersteund door aanvullende procedures.

Ook vereist "Front Office Automation" controle op de identificatiekaarten van de personeelsleden waarmee de functiescheiding binnen het filiaal op een bepaald tijdstip wordt weergegeven. En nog belangrijker is de functiescheiding binnen de transactiekringloop binnen het filiaal.

Er dienen voorschriften te komen ten behoeve van de klanten die geen gebruik wensen te maken van de PIN-codes. Dit tast de veiligheid van het systeem aan omdat zulke voorschriften het filiaalpersoneel meer kansen biedt het systeem te misbruiken.

Elektronisch bankieren (thuisbankieren) *)

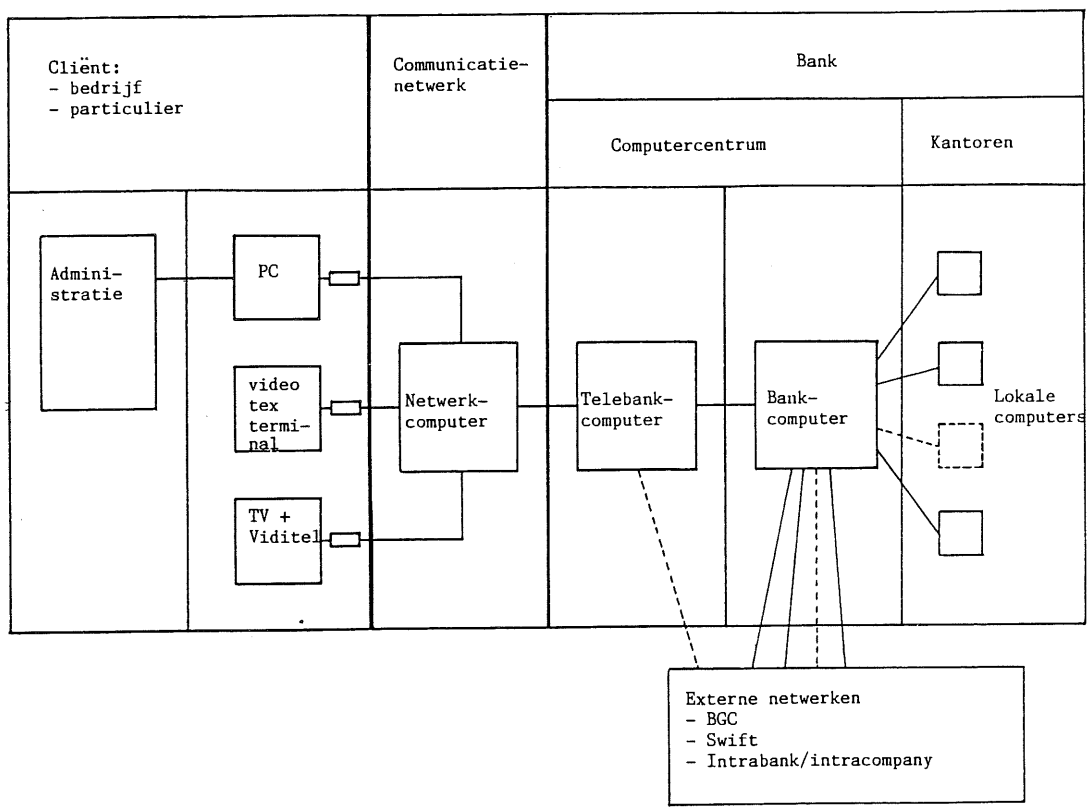
Als laatste verschijningsvorm van nieuwe technologieën kan het thuisbankieren worden genoemd. Deze elektronische bankdienst is nauw verwant met de eerder in dit artikel behandelde diensten.
Het verschil is met name gelegen in het feit dat de terminal waarvan de gebruiker zich bedient, bij deze gebruiker thuis gestationeerd is. Hierdoor is geen controle mogelijk op het gebruik van de terminal, noch door de bank zelf zoals bij front office automation, noch door een derde zoals bij EFTPOS.
De gebruiker kan vanuit zijn thuisomgeving (c.q. bedrijfsomgeving) toegang krijgen tot het netwerk waarop ook zijn bank is aangesloten.
Eenmaal "binnen" in de (tele-)bankcomputer heeft hij de mogelijkheid allerlei informatie op te vragen, bijvoorbeeld betreffende zijn saldi en heeft hij de mogelijkheid transacties te initiëren.

Het is uiteraard van essentieel belang om een zodanige afscherming van gegevens (dat wil zeggen gebruikers onderling respectievelijk gebruikers/bank) te realiseren, dat de betrouwbaarheid en de privacy gewaarborgd blijven. Het zal onmogelijk gemaakt dienen te worden dat, al dan niet opzette-

*) Voor een uitgebreide behandeling van dit onderwerp zij verwezen naar het artikel van drs. D. Swagerman elders is dit nummer.

lijk, gegevens van anderen kunnen worden gelezen of gemuteerd, of dat andere frauduleuze handelingen kunnen worden verricht.
De terminal bij de cliënt dient op adequate wijze te zijn beveiligd. Dit betekent dat tenminste een goed systeem van identificatie van zender en ontvanger, alsmede van autorisatie van transacties geïmplementeerd dient te zijn.
Hiernaast valt te denken aan een additionele beveiliging voor het terminal-gebruik, in de vorm van een magneetstripkaart of een chip-kaart.

Als voorbeeld is in figuur 3 een mogelijke configuratie van een thuisbankiersysteem geschetst.
Afhankelijk van het type systeem zal een werkelijke configuratie uit (delen van) dit algemene schema zijn samengesteld. Door het aanbrengen van enkele wijzigingen voldoet dit figuur ook aan de globale karakteristieken van een EFTPOS- respectievelijk een ATM-systeem.



Figuur 3. Mogelijke configuratie van een thuisbankiersysteem.

Uit figuur 3 is af te leiden dat we binnen een thuisbankiersysteem een aantal subsystemen kunnen onderscheiden:
- het cliëntsysteem;
- het netwerksysteem;
- het bancaire systeem (intern/extern).

Als we willen komen tot een overall-beveiliging van een thuisbankiersysteem, dan dienen de systeemeisen ten aanzien van beveiliging en de bedreigingen voor elk subsysteem te worden bepaald vanuit het gezichtspunt van elk der participanten van het thuisbankiersysteem, i.c. de drie subsystemen.

Figuur 4 geeft aan in welke fasen het proces van het definiëren van beveiligingsmaatregelen uiteen valt.

	Systeemeisen			bedreigingen gerelateerd aan systeemeisen	beveiligingsmaatregelen per (groep van) bedreiging(en)	additionele (overall-) beveiligingsmaatregelen
participant / subsysteem	cliënt	netwerkbeheer	bank			
cliënt-systeem						
netwerk-systeem						
bank-systeem						
	Fase 1			Fase 2	Fase 3a	Fase 3b

Figuur 4. Het definiëren van beveiligingsmaatregelen ten aanzien van een thuisbankiersysteem.

In de eerste fase vindt inventarisatie plaats van de systeemeisen.
Deze eisen worden door elke groep systeemgebruikers (cliënt, netwerkbeheer en bank) ten aanzien van elk subsysteem geformuleerd.

In fase 2 worden op basis van deze inventarisatie per subsysteem de bedreigingen onderkend gerelateerd aan de systeemeisen.
De bank zal bijvoorbeeld als systeemeis voor het netwerksubsysteem hebben geformuleerd, dat een juiste, volledige en tijdige overdracht van gegevens over het netwerk dient plaats te vinden (uiteraard gespecificeerd naar detailpunten).
De hierbij te formuleren bedreigingen zouden dan kunnen zijn de zes bedreigingen, zoals deze in de paragraaf "Communicatie" in dit artikel zijn genoemd.

In fase 3a word(t)en per bedreiging de mogelijke beveiligingsmaatregel(en) opgesomd.

Omdat het uiteindelijk gaat om de overall-beveiliging van het systeem worden in fase 3b de eerder genoemde maatregelen in hun onderlinge samenhang bezien en worden eventuele additionele maatregelen opgesomd respectievelijk worden elkaar overlappende maatregelen uit het ontwerp weggelaten.
In elk geval dient duidelijk in het schema te zijn vastgelegd welk subsysteem verantwoordelijkheid draagt voor welke beveiligingsmaatregelen.

De analyses en resultaten dienen tenslotte te worden teruggekoppeld naar de systeemgebruikers ter goedkeuring.

Audits zijn vereist ten einde te bevestigen dat de invoering van nieuwe technologie door effectieve controles wordt afgedekt

Een grondige controle dient alle relevante risicogebieden te omvatten hoewel zowel de interne als de externe accountant zich goed bewust dient te zijn van de omvang van zijn controlewerkzaamheden. Deze omvang wordt beïnvloed door afspraken en contracten tussen de EFTPOS-deelnemers waarin de verplichtingen en wettelijke aansprakelijkheden zullen zijn neergelegd.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Zomer 1987

BETALINGSORGANISATIE EN AUTOMATISERING BINNEN DE ORGANISATIE *)

door J. ten Wolde

1. Inleiding

In toenemende mate speelt automatisering een rol bij de totstandkoming van betalingsopdrachten dan wel bij de uitvoering van deze opdrachten.

Nu worden er tal van zaken geautomatiseerd zonder dat er een reden is om een artikel te schrijven. Waarom leent de automatisering van de betalingen zich wel voor een schriftelijke overpeinzing?

1. De betalingen vormen een belangrijke schakel in de betalingsorganisatie die op haar beurt een belangrijk onderdeel vormt van de administratieve organisatie en het systeem van interne controle.

2. Als we het waardekringloopproces symbolisch voorstellen als een "gesloten" circuit, dan vormen de betalingen een schakel naar de buitenwereld waardoor waarden het bedrijf kunnen verlaten. Daar deze waarden zowel uiterst fungibel zijn en in het algemeen gesproken "schaars" zijn, bestaat er een zekere voorkeur voor het in het bezit verkrijgen van deze waarden.
   Voor bepaalde mensen is geen inspanning of risico te groot om deze voorkeur te concretiseren.

3. Automatisering kan het systeem van interne controle ondergraven zonder dat betrokkenen zich dat bewust zijn. Vergelijk de volgende twee situaties maar eens:
   a. Een crediteurenadministrateur schrijft met de hand betalingsopdrachten. Deze legt hij te zamen met de daarbij behorende facturen voor aan de procuratiehouder. Deze "doorloopt de facturen", tekent de opdrachten en vergelijkt eventueel desgewenst gegevens van de factuur met de opdracht. Op weg naar huis doet hij, of zijn secretaresse, de envelop met de betalingsopdrachten in een brievenbus.
   b. Het computercentrum maakt een tape voor de Bankgirocentrale (BGC) en/of de Postbank alsmede een recapitulatie waarop het totaalbedrag en een telling van de rekeningnummers worden afgedrukt. De crediteurenadministrateur neemt deze twee tellingen over op een begeleidend schrijven aan de BGC en/of de Postbank.
      Dit schrijven, alsmede de tape legt hij voor aan de procuratiehouder. De procuratiehouder zet (bedachtzaam) zijn handtekening. De interne post verzorgt de rest.

*) Dit artikel is in belangrijke mate gebaseerd op een artikel gepubliceerd in het MAB, november 1978, onder dezelfde titel.

De bedachtzaamheid van de procuratiehouder vloeit wellicht voort uit zijn (onder-)bewustzijn van het feit dat er iets schort aan het systeem van interne controle.

Dit artikel gaat nader in op mogelijke c.q. noodzakelijke wijzigingen van het systeem van interne controle ingeval de betalingen worden geautomatiseerd, waarbij het noodzakelijk is tevens in te gaan op de organisatie en interne controle buiten de eigenlijke betalingsorganisatie.
Alvorens dit te doen wordt het gezegde "de keten is zo sterk als zijn zwakste schakel" in herinnering gebracht. Een interne controleschakel sterker maken dan de zwakste is niet zinvol. Bovendien ontstaat dan het risico van het (veelal ten onrechte) hebben van een gevoel van veiligheid.

Verder is het wellicht goed stil te staan bij het doel van interne controle in het algemeen. Dit doel is:
- primair: het voorkomen van "fouten";
- secundair: het tijdig ontdekken van "fouten".

In de praktijk ziet men wel dat soms te veel nadruk wordt gelegd op het bereiken van het primaire doel (met hoge kosten).
Het secundaire doel wordt veelal met lagere kosten bereikt; een voorwaarde is uiteraard dat de fout herstelbaar c.q. de geleden schade verhaalbaar moet zijn.
De volgende schakels (x) kan men bij de betalingsorganisatie onderscheiden:

	Gebruikers-organisatie/ invoervast-legg. e.d.	Computer-centrum	Gebruikers-organisatie/ nacontrole e.d.
A. Variabele gegevens: facturen (onder andere crediteurensaldi)	x	x	x
B. Stamgegevens: NAW (onder andere rekeningnummers)	x	x	x

Hierbij geldt
voor A: beginsaldo + nieuwe facturen - betalingen = eindsaldo;
voor B: dat zij niet van hetzelfde niveau is als A., doch dat, daar zij met name betrekking heeft op het essentiële onderdeel "betalingen" van A., de schakels hierbij van groot belang zijn.

Dit artikel is verder als volgt ingedeeld:
2. Uitgangspunten en conclusies
3. Wat doen de BGC en Postbank c.q. wat kunnen zij doen?
4. Voorterrein - gebruikersorganisatie
5. Computercentrum
6. Naterrein - gebruikersorganisatie
7. Rol van de accountant
8. Tendenzen en nieuwe ontwikkelingen
9. Ter afsluiting.

In een bijlage is een voorbeeld schematisch uitgewerkt.

Hoewel in dit artikel alle aandacht is gericht op betalingen aan crediteuren, zij nadrukkelijk vermeld dat voor andersoortige betalingen zoals bijvoorbeeld nettosalarisbetalingen dezelfde problematiek geldt.

Meer en meer bieden naast de Postbank ook andere banken buiten de BGC om faciliteiten op het gebied van geautomatiseerde betalingen. Deze zullen niet afzonderlijk in dit artikel aan de orde worden gesteld. Als reden hiervoor geldt dat er wezenlijk geen verschil bestaat met de door de BGC/Postbank geboden faciliteiten, aangenomen dat de individuele overige banken dezelfde interne controlemaatregelen bieden.

2. Uitgangspunten en conclusies

Uitgangspunten

1. De leiding van het bedrijf is verantwoordelijk voor de keuze van maatregelen van interne controle en de mate waarin zij in de dagelijkse praktijk worden toegepast. Vandaar ook dat de leiding betrokken dient te worden bij het opzetten dan wel wijzigen van het systeem van interne controle ingeval de betalingen geautomatiseerd worden. Bovendien een, uit kostenoogpunt, niet afgedekt risico in de betalingsorganisatie kan tot grote consequenties leiden.

2. Indien niet alle risico's (juist) worden onderkend bestaat de kans dat de keten van interne controle onevenwichtig wordt gesmeed: een schakel wordt sterker gemaakt dan de zwakste. Het is derhalve noodzakelijk dat een systematische risico-analyse plaatsvindt.

Conclusies

1. De risico's met betrekking tot het automatisch betalen mogen niet worden onderschat.
2. De organisatie en interne controle bij geautomatiseerde betalingen aan crediteuren zijn kwetsbaar; veelal kwetsbaarder dan in de "oude situatie".
3. Derhalve zijn aanvullende maatregelen van interne controle noodzakelijk.
4. Deze aanvullende maatregelen worden in belangrijke mate beïnvloed door het feit of de interne controle binnen het computercentrum al dan niet aan de - niet geringe - minimumeisen voldoet.
5. Als de interne controle zich richt op het, met honderd procent zekerheid, voorkomen van een fout zullen de maatregelen soms zo veelomvattend zijn dat aan de rationaliteit van het automatisch betalen getwijfeld zou kunnen worden.

   In dit artikel is getracht alle foutmogelijkheden te inventariseren en de maatregelen van interne controle die deze fouten voorkomen (of tijdig signaleren) aan te geven. Met een dergelijke inventarisatie wordt ongetwijfeld bij een enkele lezer de indruk gewekt dat

er van een spokenjacht sprake is, hetgeen stellig niet de bedoeling is. De bedoeling is wel de lezer kennis te laten nemen van de mogelijke risico's en wat daaraan te doen is, om daarmede tot een afweging van de risico's en een gefundeerde keuze van maatregelen te kunnen komen in zijn eigen situatie.

6. De hoofdlijnen van de opzet (en werking) van de betalingsorganisatie (functiescheidingen en registratie op basis van functiescheidingen) zijn van belang voor de accountant bij zijn controle van de jaarrekening.
7. Een systeemgerichte controle door de accountant, gericht op het ontdekken van omissies in de opzet of werking die eventueel kunnen leiden tot een foutieve betaling, is in het kader van de controle van de jaarrekening zelden noodzakelijk.
8. Indien de leiding van de onderneming het oordeel van de accountant wil leren kennen met betrekking tot de details van de betalingsorganisatie in geval van automatisering zal zij de accountant een EDP audit-opdracht dienen te verstrekken.

3. Wat doen de BGC en Postbank c.q. wat kunnen zij doen?

De BGC en Postbank accepteren betalingsopdrachten op:
a. magneetbanden, diskettes en magneetbandcassettes;
b. optisch leesbare formulieren (OLA).

Ad a.

Deze vorm wordt het meest toegepast. De toepassing is snel en accuraat. De band (diskette, cassette) gaat vergezeld van een geleidebrief (standaard-opdrachtbrief), waarin onder meer is opgenomen:
- totaalbedrag;
- rekeningnummer;
- gewenste verwerkingsdatum;
- som rekeningnummers (facultatief);
- aantal opdrachten;
- contactpersoon (bij opdrachtgever);
  alsmede technische gegevens (beschrijvingsdichtheid, labeling enz.).

Annuleringen (niet: wijzigingen!) zijn mogelijk mits de informatiedrager, de geleidebrief en het annuleringsverzoek één dag voor de gewenste verwerkingsdatum zijn aangeleverd.

Betaaldiskettes zijn geen nieuw produkt, maar worden wel steeds vaker toegepast. De diskette met betaalopdrachten kan met een tekstverwerker eenvoudig worden aangepast.
Het op zichzelf staand gebruik van betaaldiskettes vereist goede procedures gericht op het voorkomen van ongeautoriseerde wijzigingen van de opdrachten.

Binnen het interbancaire overleg is deze problematiek onderkend. Met behulp van het project authenticiteitscontrole wordt beoogd te komen tot maatregelen met behulp van cryptografische technieken om een eenduidige overdracht van verantwoordelijkheid tussen de procuratiehouder en de bank mogelijk te maken.
Thans ontbreekt deze mogelijkheid, hetgeen als een leemte kan worden gekenschetst. Hierbij gevoegd de eenvoudige fout- en manipulatiemogelijkheden van PC's, is terughoudendheid bij het geven van een oordeel geboden.

Ad b.

Op standaardformulieren van circa 25 regels worden deze opdrachten verwerkt. De toepassing is relatief traag met een grotere mate van storingen. De machines dienen absoluut storingvrij (geen scheve of zwakke letter en dergelijke) te zijn. De formulieren dienen zowel vóór als na de bewerking met zorgvuldigheid behandeld te worden. Elk formulier heeft een totaaltelling (alleen van bedragen), dient van een handtekening voorzien te worden en bevat de naam en het nummer zowel van de begunstigde als van de opdrachtgever. Annuleringen zijn niet mogelijk.

De volgende controles worden in geval a. en b. verricht:

1. Bestaanbaarheid rekeningnummers (BGC: 11-proef; bestaanbaarheid nummerserie). Opdrachten met niet bestaanbare rekeningnummers kunnen niet worden uitgevoerd. Hierover wordt door de BGC met de opdrachtgever contact opgenomen; de Postbank storneert deze opdrachten soms zonder nader overleg.
2. Som van bedragen (som van mutaties = totaaltelling in header = totaalbedrag geleidebrief).
   Wanneer het totaal van de mutaties afwijkt van de totaaltelling (in header of trailer) en/of van het totaal in de geleidebrief wordt de batch niet verwerkt en wordt contact opgenomen met de in de geleidebrief genoemde contactpersoon. Op verzoek van de opdrachtgever kan deze melding worden gericht aan een controle-instantie van het bedrijf in plaats van aan de contactpersoon.
3. Som van de rekeningnummers.
   Gecontroleerd wordt altijd of de som van de rekeningnummers van de begunstigden gelijk is aan de som zoals deze is opgenomen in het controlerecord (totaalrecord, header).
   Indien op de geleidebrief de laatste vijf (BGC) of zeven (Postbank) cijfers van de som van de rekeningnummers worden opgenomen dan wordt dit controletotaal ook gecontroleerd. Bij een eventueel verschil wordt de contactpersoon/controle-instantie *) hiervan telefonisch/schriftelijk *) op de hoogte gesteld.
   De verwerking (clearing) heeft dan bij de BGC meestal al plaatsgevonden, zodat een direct onderzoek naar de oorzaak van het verschil noodzakelijk is om in overleg met de bank en begunstigde bank eventueel acties te ondernemen om uitbetaling te vermijden.
   De Postbank heeft altijd overleg met de opdrachtgever alvorens de opdrachten worden verwerkt.

*) De gewenste mogelijkheid dient op de geleidebrief te worden aangegeven.

Door het ontbreken van een geleidebrief en sluitrecord bij de optisch leesbare formulieren vindt geen controle plaats op de telling van de rekeningnummers.
Daar het verwerkingssysteem van de BGC en Postbank zich richt op nummers wordt er geen relatie gelegd met de namen. De BGC past fiatcontrole toe: zij vraagt de bank van de opdrachtgever telefonisch akkoord voor verwerking. Deze bank past (eventueel) handtekeningcontrole en limietcontrole toe.
De Postbank past bij toepassing van tapes en dergelijke altijd handtekeningcontrole toe: als limiet geldt het creditsaldo op de rekening.

4. Voorterrein - gebruikersorganisatie

In de gebruikersorganisatie in casu het voorterrein wordt de input verzorgd van:
A. variabele gegevens: facturen;
B. stamgegevens: crediteuren NAW-gegevens (onder andere rekeningnummers).

Indien de interne controle bij deze schakels zwak is kan:
a. een factuur worden ingebracht waarvan de contraprestatie niet juist en/of niet geautoriseerd is;
b. een factuur niet of niet tijdig worden ingebracht;
c. een foutief NAW-gegeven worden ingebracht waardoor betaling niet aan de juiste persoon of instelling geschiedt.
Hierbij kan nog onderscheid gemaakt worden tussen "slepen" (crediteuren later betalen en het liquiditeitsverschil lenen) en "de greep uit de kas" (bedrag overmaken op eigen/bevriende rekening en vertrekken).

Ad a. en b.

Hoewel de organisatie met betrekking tot deze fase geen direct verband houdt met de betalingsorganisatie, zal, om een volledig beeld te schetsen, deze fase wel globaal worden uitgewerkt.
Hierbij is van belang:

1. bestelprocedure/autorisatie en registratie van bestellingen:
   - vastlegging bestelling
   - ontvangstmelding
2. ontvangst van goederen/diensten:
   - controle met bestellingen
   - opboeking in Kantoorvoorraadadministratie (KVA), kosten e.d.
   - tegenboeking Te ontvangen facturen
3. ontvangst van facturen:
   - primaire registratie alvorens facturen "het bedrijf ingaan" (doorlopende nummering)
   - controle met bestelling en ontvangst/levering, alsmede narekenen van facturen
   - opboeking Crediteuren
   - boeking eventueel prijsverschil
   - afboeking Te ontvangen facturen

4.	bewaring/registratie van crediteuren:	- analyse saldo Te ontvangen facturen - analyse van Crediteuren (crediteurenlijst op ouderdom, "afloopcontrole", aansluiting met grootboek) - saldobiljettencontrole (eventueel)
5.	betalingsfiattering:	- als voorpost van de procuratiehouder, die in een later stadium voor de feitelijke betaling zal tekenen, zal de betalingsfiatteur facturen vrijgeven voor betaling. De fiatteur zal functioneel gescheiden dienen te zijn van de goederenbestelling, -bewaring en -registratie en van de crediteurenregistratie. Hij zal, als intern de ad 1., 2. en 3. genoemde handelingen zijn verricht, de betalingsblokkade opheffen. Het computercentrum kan enkele dagen voor de betalingsdatum een opgave aan de fiatteur verstrekken van die facturen waarvan de vervaldatum is bereikt doch waarvan de betalingsblokkade nog niet is opgeheven. De fiatteur kan dan hiervan de reden nagaan.

Ad c.

Het zal duidelijk zijn dat het crediteurenbestand (waarin veelal de rekeningnummers zijn opgenomen) een kritisch bestand is. Dit bestand - voortaan rekeningnummerbestand genoemd - verdient derhalve grote aandacht en bewaking.
Mutaties in dit kritische rekeningnummerbestand dienen voorbehouden te worden aan één persoon. Deze beheerder van het rekeningnummerbestand, verder kortweg bestandsbeheerder genoemd, die verder buiten de crediteuren- en betalingsorganisatie staat, zal op grond van externe bescheiden zoals facturen en eventueel tevens op grond van een mededeling van de inkoopafdeling dat het een nieuwe relatie betreft, een mutatie aanbieden (in de vorm van ponsconcepten of met behulp van een terminalverbinding).

Het rekencentrum zal slechts van hem deze mutaties c.q. door hem geautoriseerde mutaties accepteren. (Een on-line-systeem zal op grond van een gebruikersidentificatie c.q. password en op basis van vooraf gedefinieerde bevoegdheidsregels slechts van hem mutaties mogen accepteren.) Deze mutaties worden als voorlopig beschouwd: zij mogen slechts worden gehanteerd nadat controle door een controlefunctionaris heeft plaatsgevonden.

5. Computercentrum

Het computercentrum verzorgt de geautomatiseerde verwerking van:
A. facturen;
B. crediteuren NAW-gegevens (rekeningnummers);
alsmede het vervaardigen van:
C. betalingstape;
D. print-out van deze tape.

Van essentiële betekenis voor de aard en de omvang van de te nemen maatregelen van interne controle met betrekking tot de gebruikersorganisatie, nadat verwerking heeft plaatsgevonden (het naterrein) is de vraag: Hoe sterk is de interne controle in het computercentrum of meer in het bijzonder: hoe sterk is de interne controle in het computercentrum voor zover zij een rol speelt bij de betalingsorganisatie?
In de praktijk wordt onvoldoende erkend dat werkzaamheden op het computercentrum met betrekking tot de betalingsorganisatie kritisch zijn. De verwerking van de salarissen geniet veelal veel meer aandacht (privacy) dan het vervaardigen van een betalingstape.
Minimale eisen die hierbij een rol spelen:

a. strikte functiescheiding tussen systeembouw (systeemanalyse en programmering) en produktie;
b. acceptatie- en overdrachtsprocedures van programma's (waaronder updateprogramma's van crediteurensaldi en rekeningnummerbestand, programma dat tape en listing verzorgt), waarbij onder meer het testen door daarvoor verantwoordelijke gebruikers, van belang is;
c. bewaring van programma's, zodanig dat het ongeautoriseerd wijzigen onmogelijk is c.q. tijdig kan worden opgemerkt, gekoppeld aan een wijzigingsprocedure. (Wie mag programma's wijzigen? Op grond waarvan? Goedkeuring programma na wijziging?);
d. bewaring van bestanden, zodanig dat ongeautoriseerde mutaties onmogelijk zijn c.q. tijdig worden opgemerkt;
e. controle op autorisatie (door de juiste gebruiker) van de te verwerken (verwerkte) mutaties;
f. controle op het verwerkingsproces zelf;
g. de betalingstape en print-out dienen direct na totstandkoming van het computercentrum verwijderd en afgegeven te worden aan de (assistent van de) procuratiehouder.

Indien de organisatie van het computercentrum niet aan deze minimumeisen kan voldoen als gevolg van bijvoorbeeld een relatief geringe omvang van de personele bezetting of beperkingen in de architectuur van de computerapparatuur en systeemprogrammatuur, dient het naterrein alle mogelijke risico's af te dekken, hetgeen soms zal moeten leiden tot een integrale controle aldaar (controle van alleen grote bedragen is dan onvoldoende: zie 6.B.1.).
Daar in de praktijk het computercentrum c.q. de automatiseringsorganisatie veelal niet aan deze hoge eisen kan voldoen zal veel aandacht aan het naterrein besteed dienen te worden.

Indien de interne controle niet aan vorengenoemde minimumeisen voldoet, bestaat de mogelijkheid dat:

a. een onjuiste en/of niet geautoriseerde factuur kan worden verwerkt (prestatie niet in overeenstemming met de factuur);
b. een factuur niet of niet tijdig wordt verwerkt;
c. een foutief rekeningnummer in het rekeningnummerbestand wordt verwerkt, waardoor betaling niet aan de juiste persoon of instelling geschiedt. Indien er sprake is van opzet (diefstal) zal van deze mogelijkheid veelal gebruik worden gemaakt;
d. op de betalingstape een bedrag bij een verkeerd rekeningnummer (verkeerde naam) staat;
e. op de betalingstape een foutief rekeningnummer wordt opgenomen;
f. op de betalingstape foutieve tellingen staan;
g. de afdruk kan afwijken van de tape ten aanzien van rekeningnummer;
h. idem als g. ten aanzien van bedrag;
i. idem als g. ten aanzien van totaaltellingen.

Ad a. en b. het verwerken van een onjuiste en/of niet geautoriseerde factuur en het niet of niet tijdig verwerken van facturen

Verwezen kan worden naar hoofdstuk 4, ad a. en b. Een eventuele fout wordt direct opgemerkt en is lokaliseerbaar als de gebruiker direct in staat is zijn input (output) te controleren, bijvoorbeeld door voortellingen te maken c.q. nieuw saldo te bepalen en deze te vergelijken met de output. De mogelijkheid dat een onjuiste factuur verwerkt wordt en deze evenmin op de output voorkomt, is aanwezig. Als de programma's goed getest zijn, zal er sprake zijn van opzet en zal de aandacht van de fraudeur tevens gericht zijn op het opnemen van een frauduleus rekeningnummer (zie c. en e.).

Ad c. een foutief rekeningnummer verwerken

Ook nu kan verwezen worden naar hoofdstuk 4 (ad c.).
Tijdens batch-gewijze bijwerken zal van het nieuwe bestand een telling dienen te worden gemaakt. Bij een on line-/real time-verwerking zal regelmatig het bestand doorgeteld dienen te worden. Mutatieverslagen en tellingen dienen afgegeven te worden aan een controlefunctionaris (zie 6.A.a.). Attentie: als de controle uitsluitend gelegd wordt bij de bestandsbeheerder ontstaat daar een zwakke plek in het systeem van interne controle: hij kan dan namelijk geheel zelfstandig rekeningnummers invoeren en wijzigen.
Het verwerken van een foutief nummer in een bestand zonder dat hiervan een afdruk ontstaat c.q. doorgegeven wordt aan de gebruiker is mogelijk. In dat geval zal dit nummer ook niet opgenomen worden in de telling. De ongeautoriseerde mutatie in het bestand kan ook plaatsvinden direct vóór de gereedmaking van de betalingstape op de vervaldatum van een (eventueel frauduleus ingebrachte) factuur. Daarom verdient het aanbeveling bij de vervaardiging van de tape een telling van het rekeningnummerbestand te laten afdrukken en deze te vergelijken met de controletelling (zie 6.A.a.). Zie ook e.

Ad d. op de betalingstape een bedrag bij een verkeerd rekeningnummer (verkeerde naam)

Als het programma dat tot doel heeft het vervaardigen van de tape ten aanzien van dit punt zorgvuldig is vervaardigd en getest, kan het bedrag slechts bij een foutief rekeningnummer (en een foutieve naam) vermeld zijn ingeval bij de input van de factuur een foutief crediteurennummer is gehanteerd.
Controle op een juiste codering en verdere verwerking is daarom van belang. De codering (deze zal bijvoorbeeld plaatsvinden bij de inschrijving in facturenboek en het toekennen van een intern volgnummer) zal gecontroleerd dienen te worden, bijvoorbeeld bij controle met bestelling of bij het narekenen.
Controle op de juiste verwerking kan plaatsvinden door middel van voortellingen of bij een on line-systeem door middel van naamcontrole: bij het inbrengen van een crediteurennummer koppelt het systeem de naam terug die vergeleken dient te worden met de factuur.

Ad e. op de betalingstape een foutief rekeningnummer

Als, ten gevolge van een zwakke interne controle, het mogelijk is op de betalingstape een foutief rekeningnummer op te nemen (tijdens of na de totstandkoming van de tape), kan slechts een volledige controle in het naterrein op juistheid van rekeningnummers deze leemte geheel opheffen (zie 6.B.1.).

Ad f. en i. foutieve tellingen op tape of afdruk

Bij verwerking constateren de BGC en de Postbank dat de som van de rekeningnummers gelijk is aan de totaaltelling van de tape en van de geleidebrief (= tellingen van afdruk).

Ad g. afwijking tussen tape en afdruk ten aanzien van rekeningnummer

Afwijkingen tussen tape en afdruk kunnen bij een normale (zorgvuldige) totstandkoming van het programma slechts voorkomen als, mogelijk gemaakt door een zwakke interne controle, opzet in het spel is. De tape zal dan een foutief rekeningnummer bevatten (zie e.), terwijl de afdruk een geautoriseerd rekeningnummer laat zien. Betalingen aan personeel (salaris/onkostenvergoeding e.d.) scheiden van crediteurenbetalingen. Indien niet het geval staat de benodigde BGC-rekening reeds op de tape en is het een kwestie van een programma, dat alle bedragen verlaagt tot f 1,-- en het verschil bij de fraudeur bijtelt!
Daar de telling op de afdruk dezelfde dient te zijn als op de tape (de BGC en de Postbank controleren dit) zal de som van de rekeningnummers op de afdruk ongelijk zijn aan de daaronder vermelde telling.
De conclusie is dan ook dat rekeningnummers (de laatste cijfers) nageteld dienen te worden om te kunnen signaleren dat de tape een ander nummer bevat dan op de afdruk vermeld wordt.

Ad h. foutief bedrag op tape of afdruk

Ten aanzien van bedragen geldt eveneens dat de totaaltellingen van de tape door de BGC en de Postbank gecontroleerd worden met de geleidebrief. Mogelijk is dat op de tape een hoger bedrag wordt vermeld bij een crediteur dan op de afdruk staat vermeld.
Dit te hoge bedrag kan ten laste komen van andere op de tape vermelde crediteuren (verschuiven, waardoor de telling gelijk blijft) of de verhoging wordt begrepen in de telling van de tape. Als op de afdruk ook deze telling afgedrukt wordt is de som van de bedragen van de afdruk niet gelijk aan deze telling. Deze te hoge betaling vindt echter plaats aan een geautoriseerd rekeningnummer.
Indien geacht wordt dat dit risico aanwezig is en dat terugvordering (verrekening) niet mogelijk is,
- zullen de op afdruk vermelde bedragen gecontroleerd dienen te worden met facturen, saldilijsten, factuurvervangende documenten of iets dergelijks (zie 6.B.3.);
- zal deze telling gecontroleerd dienen te worden.

6. Naterrein - gebruikersorganisatie

A. Indien de organisatie binnen het computercentrum voldoet aan de minimumeisen zal de gebruikersorganisatie, in het bijzonder het naterrein, het volgende omvatten:
   a. De controlefunctionaris van het rekeningnummerbestand ontvangt doorgenummerde mutatieverslagen van het bestand, alsmede de telling van het nieuwe bestand. Aan de hand van de bescheiden die hem ter hand zijn gesteld door de bestandsbeheerder zal hij:
      - de telling OS + mutaties = NS controleren;
      - de mutaties met bescheiden controleren en vastleggen;
      - de mutaties vrijgeven voor verwerking in het werkbestand.
   b. De procuratiehouder (of zijn assistent) vult aan de hand van de afdruk de geleidebrief in. Na ondertekening van deze brief - soms ook van een brief aan de eigen bankrelatie waarop hetzelfde bedrag vermeld staat - verzendt hij de tape alsmede deze brief (brieven). Een kopie van de afdruk en opdrachtbrieven zendt hij naar de hoofdadministratie.
   c. De van de bank ontvangen dagafschriften met bijlagen dienen rechtstreeks naar de hoofdadministratie gestuurd te worden. De hoofdadministratie:
      - vergelijkt de afmutaties met de kopie-opdrachtbrieven en afdruk (totaalbedragen);
      - boekt de totaalbedragen op Crediteuren, Te betalen salarissen enz.;
      - stuurt de bijlagen en de kopie van de afdruk van de betalingstape naar de crediteurenadministratie, salarisadministratie enz.

d. De crediteurenadministratie:
   - vergelijkt het totaalbedrag van de van de bank ontvangen specificatie met de afboeking op het crediteurensaldibestand;
   - geeft aan computercentrum opdracht om de (kopie-)betalingstape (met datum en nummer van dagafschrift) te verwerken in crediteurenbestand;
   - verwerkt aan de hand van overige bijlagen de eventueel handmatig verrichte betalingen.

   De vraag is of de banklijst in detail vergeleken dient te worden met de afdruk van de betaaltape. Deze controle zou kunnen dienen om vast te stellen dat:
   1. de inhoud van de tape in overeenstemming is (geweest) met de afdruk. Indien de interne controle hierop reeds gericht is, door de interne controle op het computercentrum of in het naterrein, kan deze controle achterwege blijven. Als deze, eventueel steekproefsgewijze, vergelijking toch wordt toegepast, bijvoorbeeld ter versteviging van de interne controle elders (als gesteund wordt op interne controle in computercentrum of indien interne controle in het naterrein met behulp van steekproeven wordt verricht) diene men zich te realiseren dat deze maatregel gericht is op tijdige ontdekking van fouten en niet op voorkoming daarvan.
   2. de bank en de Bankgirocentrale de instructies juist hebben uitgevoerd. Gezien echter het feit dat:
      - de bank en de Bankgirocentrale verantwoordelijk en aansprakelijk zijn voor frauduleuze handelingen verricht door haar functionarissen,
      - door middel van de totaalcontrole wordt vastgesteld dat de bank de instructies tijdig heeft uitgevoerd,
      - de geringe kans dat fouten worden gemaakt op het uitvoeringstraject bij de Postbank en de bank(girocentrale) zonder dat dit zichtbaar wordt in het totaalbedrag,

      lijkt een detailcontrole om deze redenen niet rationeel. Als een detailcontrole toch zinvol wordt geacht, kan dit geschieden door de crediteurenadministratie (op de Postbank-lijst staan alleen nummers en bedragen; namen kunnen worden opgevraagd).

e. Tot slot dient vermeld te worden dat een aantal maatregelen, genoemd in hoofdstuk 4, het systeem van interne controle sluitend maakt:
   - aansluiting van de subadministratie crediteuren met het grootboek;
   - analyse van de ouderdom van de nog te betalen posten;
   - eventueel: saldobiljetten versturen;
   - eventueel: controle op de afloop van de saldi (volledigheidscontrole).

B. Indien de interne controle binnen het computercentrum (betreffende de betalingsorganisatie) niet voldoet aan de daaraan te stellen eisen zullen, naast de ad A. genoemde, nog de volgende maatregelen in het naterrein genomen dienen te worden:
   1. De rekeningnummers op de afdruk dienen gecontroleerd te worden aan de hand van een bestand dat door de controleur wordt bijgehouden, of aan de hand van facturen of factuurvervangende documenten (zie ook suggestie C.6.).
      Slechts de rekeningnummers controleren bij de grote bedragen is niet voldoende: het foutieve nummer kan op de afdruk bij een klein bedrag staan en op de tape bij een groot bedrag.
   2. De telling van de rekeningnummers (de laatste cijfers daarvan) dient te worden gecontroleerd. Het foutieve nummer kan wel opgenomen zijn op de tape doch niet op de afdruk, hetgeen tot een foutieve totaaltelling van de nummers leidt.
   3. Indien er een risico bestaat dat een foutieve (te hoge) betaling wordt verricht die niet hersteld kan worden door verrekening of terugvordering: controle van de bedragen aan de hand van facturen of factuurvervangende documenten, saldilijsten en dergelijke.
      Dit zal in het algemeen slechts het geval zijn als er betalingen plaatsvinden aan crediteuren waarmede een korte relatie bestaat c.q. zal bestaan (zie C.2.).

C. Versterking van het systeem van interne controle is mogelijk indien één of meer van de volgende punten verwezenlijkt kan worden.
   1. Het computercentrum vervaardigt, naast de afdruk van de tape, betalingsspecificaties per crediteur. Hierop staat per specificatie vermeld:
      - NAW-crediteur;
      - factuurnummer;
      - factuurdatum;
      - bedrag;
      - totaalbedrag;
      - (waarschijnlijke) datum waarop bedrag tegemoet gezien kan worden.

      De (assistent-)procuratiehouder verzendt deze specificaties aan de crediteuren. Zij weten dan wat zij verwachten kunnen en hebben daarvan een specificatie. Indien, per betaling, een aantal facturen betaald dient te worden is een dergelijke specificatie geen luxe: de specificatieruimte op de tape (c.q. op het overschrijvingsformulier) is namelijk beperkt.
      De som van deze specificaties dient uiteraard gelijk te zijn aan het totaalbedrag van de tape (afdruk).
      Een kopie van deze specificaties kan als controle/naslag dienen voor de crediteurenadministratie.
   2. Het verdient soms aanbeveling alle betalingen met een bijzonder (bijvoorbeeld vreemde valuta) of eenmalig karakter niet te automatiseren: het risico op fouten en fraude is hier het grootst. Boven-

dien leiden deze transacties tot veel mutaties in "vaste" gegevens (rekeningnummerbestand, NAW, VV-tegenwaarde) en veelal tot opblazen (meeslepen van niet meer te gebruiken gegevens) van bestanden.

3. Indien het afdrukken (en natellen) van de tape met zorg wordt omringd is veel controlewerk overbodig: de controle ad B.1. kan dan beperkt worden tot de rekeningnummers van de grotere bedragen en de controle ad B.2. (natellen van rekeningnummers) kan vervallen.
   Genoemde "zorg" kan als volgt omschreven worden:
   - laat afdruk niet geïntegreerd plaatsvinden, doch maak van het afdrukken van de tape een afzonderlijke activiteit;
   - een functionaris die geen bemoeienis heeft met de verwerking/totstandkoming van de tape zal deze actie uitvoeren (met behulp van eenvoudige standaardprogrammatuur ten behoeve van het afdrukken van tapes);
   - het programma dat deze afdruk (en natelling) verzorgt blijft onder beheer van deze functionaris;
   - de tape mag tijdens deze verwerking niet meer gemuteerd worden (wegnemen schrijfring).

   Bovenstaande is met een standaard-retrieval-pakket eenvoudig te realiseren.
4. Op het moment dat de totaaltape wordt vervaardigd, wordt van alle rekeningnummers in het geraadpleegde bestand een telling gemaakt. Deze telling wordt aangesloten met het standenregister van de bestandsbeheerder, waardoor meer zekerheid wordt verkregen dat van het juiste bestand gebruik is gemaakt.
5. Het computercentrum vervaardigt twee identieke tapes. Eén tape wordt, met geleidebrief, ter betaling verzonden en één tape wordt naar een ander computercentrum ter controle gezonden. Dit computercentrum controleert:
   - de tellingen van de tape met de tellingen van de kopie-geleidebrief;
   - de nummers met een schaduwbestand. Dit bestand wordt bijgehouden aan de hand van kopie-mutatie-opdrachten (zie 4. ad c.). Update-verslagen met tellingen worden verzonden aan de controlefunctionaris van het bedrijf (zie 6.A.a.).

   De beslissing welke tape naar dit computercentrum wordt gezonden dient genomen te worden door een functionaris die functioneel onafhankelijk is van het eigen centrum, bijvoorbeeld de procuratiehouder of de controlefunctionaris. De controle door een ander centrum kan op basis van reciprociteit plaatsvinden.
6. Het computercentrum vervaardigt een betalingsvoorstel (= selectie van goedgekeurde facturen waarvan de vervaldatum nadert). Dit betalingsvoorstel wordt voorgelegd aan de crediteurenadministratie. Deze maakt aan de hand van de betreffende facturen een voortelling van de rekeningnummers en geeft aan, na overleg met treasurer, welk maximumbedrag van de bank kan worden afgeschreven; eventueel wordt de betaling van enkele facturen uitgesteld. Voornoemde voortelling dient aan te sluiten met de telling van de rekeningnummers van de (definitieve) betalingstape (-output).

7. Indien in het crediteuren-NAW-bestand de datum van de laatste betaling wordt genoteerd kan het bestand periodiek geschoond worden: verwijderen van crediteuren (rekeningnummers) aan wie gedurende ... maanden geen betaling is verricht.
8. De tape dient direct nadat zij gereed is buiten het computercentrum gebracht te worden.
9. De crediteurenadministratie houdt handmatig met behulp van totaaltellingen het (totaal)saldo crediteuren bij:
   - bijmutaties aan de hand van (recapitulaties van) inkoopboeken;
   - afmutaties aan de hand van totalen van betalingen.

   Door dit saldo te vergelijken met het saldo volgens het grootboek wordt zekerheid verkregen dat alle betalingen ook ten laste van de rekening Crediteuren zijn geschied. Controle (analyse) van de crediteurenlijst per een bepaalde datum geeft dan zekerheid of er foutieve betalingen hebben plaatsgevonden.
10. Hoewel geen maatregel van interne controle kan de fraudeverzekering niet onvermeld blijven. Het is echter zeer de vraag of en in welke mate deze verzekering kan leiden tot minder controlewerkzaamheden: de verzekeraar stelt namelijk ook eisen met betrekking tot de administratieve organisatie en interne controle.

7. Rol van de accountant

De verantwoordelijkheid voor een adequate opzet en werking van een organisatie ligt uiteraard bij de leiding van de onderneming. De accountant wordt geconfronteerd respectievelijk kan geconfronteerd worden met de organisatie uit hoofde van:

Zijn controlefunctie

Bij de controle van de jaarrekening dient de accountant:
a. een onderzoek in te stellen naar de opzet van de administratieve organisatie - met name van het systeem van interne controle - voor zover van belang en noodzakelijk voor zijn controle van de jaarrekening;
b. een onderzoek in te stellen naar de werking van de onder a. genoemde opzet;
c. de daarbij aan het licht getreden leemten in de opzet en werking
   - te evalueren op de consequenties voor zijn controle (aanvullende alternatieve controles? wijziging van oordeel?);
   - te rapporteren aan de leiding, en

   desgevraagd
   - met betrekking tot verbeteringen te adviseren (= adviesfunctie).

De hoofdlijnen van de opzet (en werking) van de betalingsorganisatie (functiescheidingen en registratie op basis van functiescheidingen) zijn van belang voor de accountant bij zijn controle van de jaarrekening. Derhalve zullen de opzet en werking hiervan bij zijn controle-onderzoek worden betrokken.

De details van de opzet en werking zijn slechts van belang voor de accountant als hij wil vaststellen dat:
a. betaling aan de juiste crediteur is geschied;
b. de betaling terecht heeft plaatsgevonden.

Indien het systeem van registratie op basis van functiescheidingen (zie 6.C.4.) zekerheid geeft dat alle daarvoor bestemde betalingen verwerkt worden op de rekening Crediteuren, heeft de accountant - wil hij bovenstaande punten a. en b. vaststellen - de mogelijkheid dit te doen door een systeemgerichte of door gegevensgerichte controle. Daar een systeemgerichte controle (in detail) van de opzet en daarbij behorende toetsingswerkzaamheden in dit geval omvangrijk zullen zijn, en het risico van niet direct gesignaleerde doorbreking, in het bijzonder in het rekencentrum, relatief groot blijft, zal de accountant uit oogpunt van doelmatigheid èn doeltreffendheid c.q. zekerheid kiezen voor een gegevensgerichte controle.
Zo zal de accountant de op de balans voorkomende post Crediteuren kunnen controleren door controle met saldobiljetten en controle aan de hand van de betalingen in de volgende periode, waarbij van belang is dat de accountant kan vaststellen aan wie betaald is. Deze controle geeft hem in samenhang met alle andere controlehandelingen achteraf voldoende (denk aan de tolerantie) inzicht of al dan niet gedurende de controleperiode onrechtmatige betalingen hebben plaatsgevonden. Een uitgebreide systeemgerichte controle met als doel het ontdekken van omissies die kunnen leiden tot een foutieve betaling is daarom in het kader van de controle van de jaarrekening zelden noodzakelijk.

Zijn adviesfunctie

Indien de leiding, zich bewust zijnde van de kwetsbaarheid van de (ten dele geautomatiseerde) betalingsorganisatie en zich tevens bewust zijnde dat de accountant in zijn functie van controleur van de jaarrekening geen detailonderzoek naar de opzet en werking van de betalingsorganisatie zal verrichten en eventuele onregelmatigheden derhalve pas achteraf constateert, de accountant om advies vraagt c.q. hem vraagt een diepgaand systeemgericht onderzoek te verrichten teneinde een (interne) sluitende controle vóór betaling te verkrijgen, zal de accountant zeker goede diensten kunnen verlenen. Zijn kennis van de administratieve organisatie en interne controle en zijn automatiseringskennis kunnen hem in staat stellen een dergelijk onderzoek doelmatig en doeltreffend te verrichten en hierbij te adviseren.

8. Tendenzen en nieuwe ontwikkelingen

In het geautomatiseerd betalingsverkeer kunnen momenteel twee nieuwe ontwikkelingen worden onderkend die zich in de toekomst naar verwachting zullen uitbreiden, te weten:
a. De veranderingen in transportmiddelen voor geautomatiseerde betalingsopdrachten.
b. Het interactief kunnen aanbieden van individuele betalingsopdrachten.

Ad a.

De veranderingen doen zich hierbij voor in twee richtingen. Enerzijds tenderen de veranderingen in het gebruik van (met name 5,25 inch) diskettes in plaats van de eerder genoemde (en als voorbeeld gestelde) tapes.
Anderzijds wordt meer en meer gebruik gemaakt van datacommunicatiefaciliteiten tussen de opdrachtgever en bancaire instelling(en).

Weliswaar verdient het opslagmedium niet direct specifieke aandacht. Echter doordat voor deze media relatief goedkopere en in een bredere laag van de organisatie (zo niet samenleving) benodigde apparatuur (zoals home/personal computers) beschikbaar is, neemt het risico van ongeautoriseerd benaderen c.q. manipuleren toe. Derhalve dient verhoogde aandacht te worden geschonken aan de fysieke beveiliging van deze opslagmedia en zullen preventieve maatregelen zoals genoemd in hoofdstuk 6. (Naterrein, met name voor wat betreft de maatregelen genoemd onder C.5.) noodzakelijk blijken.
Gelet op de momenteel op ruimere schaal beschikbare apparatuur kan worden geconstateerd dat het risico toeneemt dat betalingsopdrachten buiten het computercentrum om worden aangemaakt en verzonden.

Met behulp van een directe koppeling tussen de computer van de opdrachtgever en die van een bancaire instelling zullen meer en meer betalingsopdrachten worden overgebracht. Een magnetisch/optisch leesbaar medium voor transport is hierbij geëlimineerd.
Hierdoor zal in toenemende mate moeten worden gesteund op de maatregelen van interne controle binnen het computercentrum omdat niet alle preventieve maatregelen in het naterrein meer mogelijk zijn.
De betekenis van de controlemaatregelen, zoals uitgevoerd door de bancaire instelling(en), op basis van onder meer de geleidebrief neemt eveneens in belangrijke mate toe.
Hiernaast zullen additionele (hier niet nader uitgewerkte) maatregelen op het gebied van een betrouwbare datacommunicatie (ten aanzien van bevoegdheid, juistheid en volledigheid) noodzakelijk zijn.

Ad b.

In de voorafgaande alinea's is met behulp van datacommunicatie alsnog sprake van batch-gewijze verwerking van betalingsopdrachten. Heden ten dage is het echter ook mogelijk door middel van datacommunicatie tussen de opdrachtgever en de bancaire instelling (zoals de Postbank met het GIROTEL-systeem) postgewijs betalingsopdrachten aan te bieden. Of al dan niet een directe verwerking binnen de bancaire instelling plaatsvindt (on line/real time dan wel data entry) wordt verder buiten beschouwing gelaten.
Bepaalde tot dusver beschreven interne controlemaatregelen kunnen ten gevolge van de verandering van batch- naar postgewijze aanbieding niet meer worden uitgevoerd. Deze betreffen met name die maatregelen die gericht zijn op de volledigheid en juistheid van de opdrachten met behulp van op onder meer de geleidebrief vermelde (batch)totalen.
Het autorisatie-aspect speelt hierbij - voornamelijk door het ontbreken van de geleidebrief - een nog grotere rol. Vast dient te staan dat niet alleen de terminal maar met name de persoon gemachtigd is betalingsopdrachten te geven.

Dit betekent:
- stringente maatregelen in de gebruikersorganisatie (toekennen, wijzigen, geheim houden codes);
- een sterke automatiseringsorganisatie (voldoende en blijvende functiescheidingen);
- stringente maatregelen binnen de automatiseringsorganisatie (wijzigen programmatuur, tabellen en dergelijke).

Wellicht gaat dit aspect bij betalingsorganisaties de grenzen van automatiseren bepalen. Als het goed is, is automatiseren van handelingen een kosten-nut-vraagstuk. Aan de kostenzijde dienen de risico's te worden begrepen. De vraag rijst dan of de ontwikkelingskosten enz. èn het risico het nut - het niet behoeven uit te schrijven van betalingsopdrachten - overtreffen.
Wellicht zal de eerste grote geautomatiseerde greep uit de geautomatiseerde kassa - mits daaraan in de media voldoende aandacht wordt besteed - de waardering voor een stukje origineel handwerk doen stijgen.
Een te constateren verschijnsel hierbij is echter dat het risico toeneemt dat betalingsopdrachten onafhankelijk van het computercentrum worden aangeboden.

9. Ter afsluiting

Zoals dat wel vaker het geval is, vormt automatisering een aanleiding om de organisatie en interne controle aan een nader onderzoek te onderwerpen. Dat onderzoek leert dan meestal dat, wil men na de automatisering een sluitende interne controle bereiken, de procedures aangepast dienen te worden. Soms komt men dan tot de conclusie dat het oude systeem van interne controle niet sluitend was.
Het vorenstaande is veelal van toepassing als overwogen wordt de betalingen aan crediteuren te automatiseren: de betalingsorganisatie, inclusief een deel van het voorterrein, wordt aan een nader onderzoek onderworpen.
(De situatie dat de procuratiehouder zonder herbezinning of aanpassing van de organisatie en/of procedure "gelukkig" geleidebrieven aan de Postbank/BGC blijft tekenen, wordt "onbestaanbaar" geacht.) In dit artikel is getracht alle mogelijke risico's en de mogelijkheden deze (volledig) af te dekken te analyseren. Deze analyse heeft zeker niet tot doel beren op de weg te jagen c.q. een (wellicht soms onwerkbare) procedure te propageren die alle risico's volledig afdekt. Het doel is wel geweest aan te geven dat er risico's zijn, welke risico's er zijn en wat daaraan gedaan kan worden, om zodoende materiaal te hebben om in een concrete situatie een gefundeerde beslissing te kunnen nemen.

Bij de beslissing of en zo ja welke wijzigingen in de organisatie of het systeem van interne controle genomen dienen te worden is van belang:
- voor de leiding van de onderneming:
  a. Het verrichten van betalingen is een kritische schakel in de organisatie, waarbij het risico van fraude ten opzichte van andere onderdelen van de organisatie relatief groot is.

b. De leiding dient op de hoogte te zijn van alle mogelijke risico's.
c. De leiding dient op de hoogte te zijn van de mogelijke risico's die niet worden afgedekt met maatregelen van interne controle, bijvoorbeeld ten gevolge van de daaraan verbonden kosten (in relatie tot het mogelijke risico), de geringe personeelsbezetting en dergelijke.

Met andere woorden: de verantwoordelijkheid voor de risico-analyse en de uitkomsten daarvan en de daarop volgende maatregelen ligt bij de leiding, niet bij het hoofd computercentrum, de procuratiehouder, de afdeling organisatie enz., alhoewel die hieraan zeer zeker een bijdrage kunnen leveren.
Een gevaar van onderschatting van het probleem is hier zeker aanwezig.

- voor de accountant:
  a. Wat zijn de consequenties voor de controle (controlefunctie).
  b. Is de leiding voldoende op de hoogte van de risico's en van de maatregelen die wel (of gefundeerd niet) genomen zijn ter afdekking daarvan (adviesfunctie).

Appendix

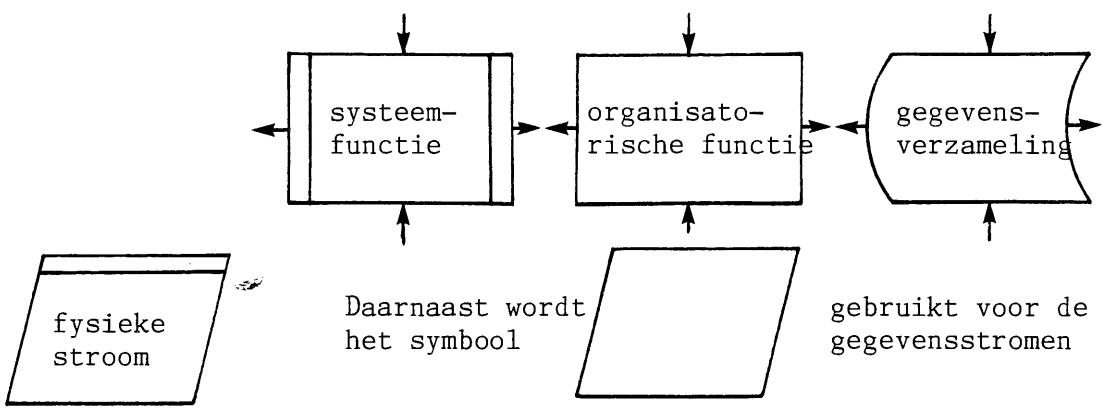
Uitgewerkt (schematisch) voorbeeld

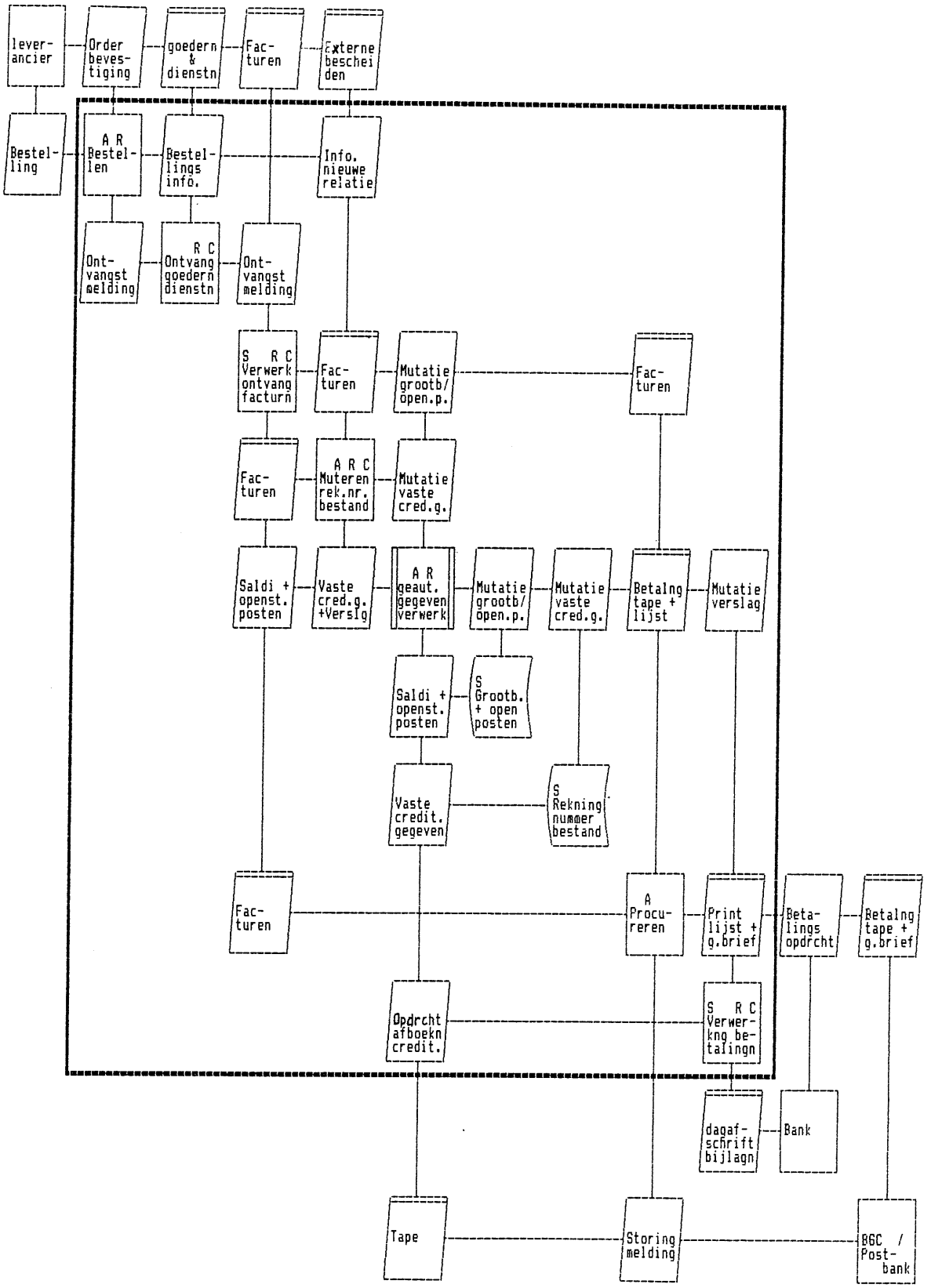
De in deze appendix toegepaste schema's zijn gebaseerd op PRISMA, een methode voor het beschrijven van organisaties en hun informatiesystemen. Een brochure is op aanvraag leverbaar. De PRISMA-methode wordt ondersteund door een geautomatiseerd documentatiesysteem met de welluidende naam PALET. Dit systeem biedt de mogelijkheid om de verschillende PRISMA-schema's grafisch in te voeren en af te drukken op papier.

Het pakket PALET dat op een micro met grafische kaart kan worden verwerkt is leverbaar tegen daarvoor vastgestelde vergoeding.
De sectie Support & Programming van Klynveld EDP Audit Services wil - desgewenst - gaarne inlichtingen verschaffen. Ook demo's zijn mogelijk.
(U belt met telefoonnummer 020 - 5461174 of 5461560.)

Met betrekking tot de schematechniek gelden onder meer de volgende conventies:
- de organisatorische en externe functies, de systeemfuncties en de gegevensverzamelingen staan op de diagonaal van de matrix;
- door functies opgeleverde (= uitgaande) gegevensstromen worden weergegeven op de regels van het schema (of wel: horizontaal);
- door functies ontvangen (= ingaande) informatiestromen staan in de kolommen van het schema (of wel: verticaal).

Schematisch als volgt:





Compact is een uitgave van

KPMG Klynveld EDP Audit Services

COMPACT

Zomer 1987

ELECTRONIC BANKING-SYSTEMEN IN DE PRAKTIJK

door drs. D.M. Swagerman*)

1. Inleiding

In de afgelopen twee jaar is de Nederlandse markt geconfronteerd met de introductie van een veelheid aan Electronic Banking-systemen. Deze introductie is gepaard gegaan met grote promotionele activiteiten van de verschillende banken. In eerste instantie lijkt de markt voor de potentiële gebruiker erg ondoorzichtig. Wij hopen met dit artikel een goed en objectief beeld te geven van de huidige stand van zaken. Bovendien wordt ingegaan op een aantal gebruikerstoepassingen.

Er bestaat een grote diversiteit onder de aangeboden Electronic Banking-systemen. Het ene systeem is niet aanwijsbaar beter dan het andere, omdat het is gebaseerd op verschillende gebruikerswensen die per afdeling en per soort organisatie uiteenlopen. De systemen richten zich duidelijk op een bepaald segment van de markt.

Vele ondernemingen voldoen nog niet aan de eisen waaraan een onderneming moet voldoen om succesvol een Electronic Banking-systeem te kunnen implementeren. Het is voor bedrijven van belang te werken aan het intern ontwikkelen van de treasury-functie en de daarbij behorende interne treasury-informatiesystemen.

Het artikel is als volgt opgebouwd. Allereerst wordt ingegaan op het aanbod van de systemen en de toepassingsmogelijkheden. Ter verduidelijking van het aanbod van Electronic Banking is het goed ook de vraagzijde te belichten. Dit zal geschieden door middel van de reacties van enige feitelijke gebruikers. Hiertoe zijn gesprekken gevoerd met een aantal gebruikers. Op grond daarvan wordt geschetst voor welk type bedrijven de Electronic Banking-systemen geschikt zijn. Het artikel zal worden afgesloten met enkele conclusies omtrent de confrontatie tussen vraag en aanbod en met enige beschouwingen over de voorzienbare ontwikkelingen.

---

*) Drs. D.M. Swagerman MBA is als partner verbonden aan KPMG Klynveld Bosboom Hegener, organisatie-adviseurs. Binnen KBH geeft hij (mede) leiding aan de Adviesgroep Financieel Economische Beheersing.

2. De aanbodzijde

Voordat er zal worden ingegaan op de systemen zelf, zullen in het kort twee ontwikkelingen worden aangestipt in het licht waarvan ons inziens Electronic Banking moet worden geplaatst. De eerste ontwikkeling is de trend naar "fee-based" banking. De andere ontwikkeling is die naar "paperless banking society".

Electronic Banking is in beide ontwikkelingen een stap voorwaarts. Enerzijds betekent Electronic Banking voor de banken een stap naar kostenverlaging en verhoging van accuratesse en betrouwbaarheid, anderzijds is het een "income generating" produkt.
Electronic Banking is een belangrijke mijlpaal in deze ontwikkeling.

Definitie van Electronic Banking

Voor dit artikel wordt Electronic Banking gedefinieerd als: "informatie-uitwisseling via datacommunicatie tussen bank en bedrijf, waarbij gebruik wordt gemaakt van door of voor de bank ontworpen software".

Door deze definitie worden een aantal zaken afgeschermd, die in een aantal gevallen ook tot Electronic Banking worden gerekend, maar die in dit artikel niet verder aan de orde zullen komen, zoals de verschillende reeds bestaande geautomatiseerde betalingsmogelijkheden (tapes en diskettes) en "netting-systemen". Tevens worden een aantal zaken buiten beschouwing gelaten die niet primair op de financiële functie van een bedrijf zijn gericht, zoals gelduitgifte-automaten (GUA's), betaalautomaten (BEA's) en daarbij behorende magneetstrip- of chipkaarten.

Er wordt in dit artikel gesproken van het begrip Electronic Banking en niet van treasury management-systemen, aangezien niet alleen de geldstroombeheerders, maar ook de debiteuren- en crediteurenadministraties en mogelijk ook andere afdelingen van deze systemen gebruik kunnen maken. Hierbij kan worden gedacht aan bijvoorbeeld de verkoopafdeling.

De interpretatie van het begrip Electronic Banking verschilt per aanbieder. Marktinformatie en electronic mail zijn bijvoorbeeld toepassingen van Electronic Banking die niet door alle banken in hun systemen zijn verwerkt.

Onderdelen van Electronic Banking

Het is moeilijk om duidelijk inzicht te verkrijgen in het aanbod van Electronic Banking-systemen, doordat de verschillende systemen een mix van diverse categorieën produkten zijn. Deze categorieën zijn hardware, software, datacommunicatie en ten slotte de data zelf, dat wil zeggen de inhoud van de communicatie.

In de categorie hardware kunnen de personal computers worden geplaatst, te denken valt aan terminals en modems, maar ook aan de telex en de mainframes. Aangezien de banken hier niet als aanbieders optreden, wordt hierop niet verder ingegaan. De categorie software omvat het eigenlijke aangeboden bankprodukt, maar ook produkten als Viditel en electronic mail.

In de categorie datacommunicatie vallen een aantal mogelijk te gebruiken netwerken. Deze zijn als volgt te categoriseren:
- de public networks, zoals die van de PTT;
- de commercial networks, zoals Viditel, Geisco of NDC (National Data Corporation);
- de interbank networks, zoals S.W.I.F.T. en de BGC;
- de intrabank networks, zoals het DCN van de Amrobank;
- de intracompany networks, zoals multinationals deze gebruiken.

Bij de data kan worden gedacht aan transactie-informatie, mutatie-informatie, informatie over de wereldmarkten, "new-abstracts" en open berichten in beide richtingen.

De keuze van de mix van deze produktcategorieën en data in het aangeboden systeem is sterk bepalend voor het uiteindelijke resultaat. Juist dit laatste aspect maakt het aanbod zo ondoorzichtig.

Systeemaanbod

Om een indruk te geven van het aanbod van Electronic Banking zullen wij nu de systemen aan de orde stellen, zoals deze door de verschillende banken worden aangeboden.

De systemen op de huidige Nederlandse markt zijn op verschillende wijzen in te delen in een aantal categorieën.
Een van de gangbare classificeringsmethoden maakt onderscheid in terminalsystemen en workstation-systemen.
Zowel bij terminal- als de workstation-systemen worden door banken data aangeleverd aan een centrale computer via een eigen netwerk of een service-bureau dan wel via een ander internationaal netwerk.

In de terminal-systemen kan de gebruiker via een telefoonlijn verbinding zoeken met een internationaal netwerk en zodoende gegevens opvragen uit de centrale computer. Hierbij worden geen manipuleerbare data overgezonden, doch gehele rapporten.

De volgende systemen vallen ons inziens onder deze categorie:

Terminal-systemen

NCB Bank	- Infocash
NCB Bank	- Vidibanking
Credit Lyonnais Bank Nederland	- Telelion

Credit Lyonnais Bank Nederland	- Lioncash
Bank Mees en Hope	- Meesnet
ABN Bank	- Balance Reporting
Postbank	- Girotel

De terminal-systemen zijn op zich onder te verdelen in systemen die al of niet van Viditel gebruik maken. Viditel is een semi-commercieel netwerk dat door de PTT wordt onderhouden. Elk bedrijf kan informatie verzenden via Viditel. Om de betreffende informatie uit het systeem te halen moet het bedrijf op Viditel zijn aangesloten. Electronic Banking via Viditel heeft het voordeel dat het voor bedrijven als stand alone-toepassing gemakkelijk is om door middel van dit datacommunicatiesysteem elektronisch te gaan bankieren. Een nadeel is dat de verdere mogelijkheden tamelijk beperkt zijn.

De NMB-Bank bereidt zich voor om op middellange termijn een breed scala aan Electronic Banking produkten te brengen, gericht op de zakelijke markt, met name het midden- en kleinbedrijf. Op dit moment wordt in de NMB-Bank hard gewerkt aan het realiseren van de noodzakelijke infrastructurele voorzieningen. Nog dit jaar zal de NMB-Bank op verzoek van grote cliënten, die een Electronic Banking-systeem van een andere bankier hebben afgenomen, data aanleveren via een internationaal netwerk.

De Rabobank zal nog dit jaar op de markt komen met een systeem dat gericht is op de grotere relaties van de Rabobank. Na deze introductie zal men zich ook op de middenmarkt richten. In de systemen zal de filosofie van de Rabobank over Electronic Banking tot uitdrukking komen. In deze visie is de informatieverstrekking via Electronic Banking een taak van de bank. Hierop zullen de produkten van de Rabobank zich primair richten. Het ontwikkelen van beslissingsondersteuningsgerichte software is in deze visie gezien de specifieke eisen en wensen een taak van de organisatie zelf. De bank zal daarbij ondersteunend kunnen optreden.
Wij verwachten dat er ook ontwikkelingen zullen komen van Staal Bankiers, Bank Mendes Gans en van Van Lanschot Bankiers.

De systemen die in onze visie onder deze workstation-categorie vallen zijn de volgende:

Workstation-systemen

NCB-Bank	- Microstation
Bank of America	- Microstar
AMRO-Bank	- AMRO Treasury Manager

Het onderscheid tussen terminal- en workstation-systemen is voor de gebruiker om een aantal redenen van belang. De prijsstellingen van aanschaf en gebruik verschillen sterk en de mogelijkheden data op te slaan of verder zelf te verwerken lopen uiteen. De workstation-systemen kunnen, in tegenstelling tot de terminal-systemen, files aanmaken. Om deze reden kan de gebruiker met een workstation-systeem doorgroeien en aansluiting maken met de administratieve systemen en met zelf ontwikkelde decision support-systemen.

Terminal- en workstation-systemen worden ook wel eerste respectievelijk tweede generatiesystemen genoemd. Ons inziens is het risico van deze indeling in generaties, dat bij de potentiële koper de indruk zou kunnen worden gewekt dat de tweede generatiesystemen moderner zijn dan de eerste generatiesystemen. Ten onrechte, want alleen de wijze van toepassing is verschillend.

Multibank- en monobanksystemen

Bij het monobanksysteem kan alleen informatie worden uitgewisseld met betrekking tot rekeningen die worden aangehouden bij de bank die het Electronic Banking-systeem heeft geleverd.

Bij multibanksystemen is het theoretisch mogelijk informatie van rekeningen bij andere banken in te winnen. Echter, niet alle banken zijn bereid, of technisch in staat, om deze informatie aan te leveren. Een aantal Nederlandse banken is gewoon nog niet zover dat zij dit soort informatie in één systeem kunnen rapporteren. Daarnaast wordt, wanneer de technische mogelijkheden er zijn, niet altijd alle benodigde informatie geleverd.
Er is bijvoorbeeld een bank die wel boeksaldi maar geen valutaire saldi rapporteert.

Real time

Een aantal Electronic Banking-systemen biedt technisch de mogelijkheid om real time te rapporteren. Echter, een groot aantal van de te rapporteren data is afkomstig van buiten de bank. Een deel van deze bronnen, zoals de BGC, werkt niet real time, zodat deze gegevens ook niet meer op real time-basis in het Electronic Banking-systeem kunnen worden gerapporteerd. Deze real time-systemen hebben dus slechts beperkte real time-toepassingen.

Informatie van bank naar cliënt

De informatie die door de bank aan de klant wordt gestuurd betreft primair de typische dagafschriftinformatie zoals boeksaldi, valutaire saldi en transactie-informatie.

Daarnaast wordt in verschillende systemen de mogelijkheid geboden informatie in te winnen van geld-, kapitaal-, effecten- en zelfs van goederenmarkten. Soms blijft dit beperkt tot de prijzen waartegen de systeemleverende bank bereid is zaken op deze markten te doen.

Informatie van cliënt naar bank

Alle informatie die door de klant aan de bank wordt gezonden ligt in de instruerende sfeer.

Allereerst bieden een aantal systemen de mogelijkheid tot open berichtgeving waarmee instructies kunnen worden gezonden. Dit vervangt de telex-, telefax- of telefoonberichten, doch is geen wezenlijke Electronic Banking.

Binnen de bank moet de instructie nog steeds worden geïnterpreteerd, beoordeeld, gefiatteerd en uitgevoerd.

Vervolgens bieden een aantal systemen de mogelijkheid om voorgeformatteerde instructies te verzenden. Weliswaar neemt de bedrijfszekerheid van het systeem hierdoor toe, doch er is nog steeds geen sprake van werkelijke Electronic Banking-systemen. Deze categorie systemen hebben wij in ons overzicht aangeduid met de term "telex".

Ten slotte is er de echte transactie-initiatie. Hierbij wordt de instructie aan de bank door de computer geïnterpreteerd, beoordeeld, gefiatteerd en uitgevoerd.
Alle Electronic Banking-systemen hebben gemeen dat zij de kwaliteit van de informatie verbeteren. De via Electronic Banking aangeleverde data zijn betrouwbaarder en sneller beschikbaar dan de traditioneel aangeleverde informatie. Ook past Electronic Banking en met name de workstation-systemen in de ontwikkeling van werkplekautomatisering en persoonlijk computergebruik.

Een methode die het mogelijk maakt systemen ten behoeve van de gebruiker te rangschikken, is de weergave van de lijst met functionele specificaties van de systemen. Wij hebben hiertoe een gedetailleerd overzicht opgesteld, waarin de eigenschappen van de op dit moment op de markt actief aangeboden systemen worden weergegeven.

Dit overzicht is tot stand gekomen op basis van gesprekken die wij hebben gevoerd met de voor Electronic Banking verantwoordelijke functionarissen van de betreffende banken. Tevens hebben wij gesproken met twee Nederlandse banken die nog geen systeem op de markt aanbieden, te weten de NMB-Bank en de Rabobank.

SYSTEEM INVENTARISATIE

Omschrijving van aangeboden Electronic Banking systemen	ABN Bank	AMRO Bank	Bank Mees & Hope		Bank of America	Credit Lyonnais Bank Nederland		Nederlandse Credietbank			Postbank
	Balance Reporting	ATM	Meesnet Quik Comm.	Meesnet Multi Bank Reporting	Microstar	Lioncash	Telelion	Vidibanking	Infocash	Microstation	Girotel
1 Mono/Multibank	Multi	Multi	Mono	Multi	Multi	Multi	Mono (wordt Multi)	Mono (NCB)	Multi	Multi (vanaf eind april 1987)	Mono
2 Workstation/Terminal	Terminal	Workstation	Terminal (elec. mail)	Terminal (workstation toekomstig)	Workstation	Terminal	Terminal	Terminal	Terminal	Workstation	Terminal
3 Realtime/niet realtime *	Beperkt	Beperkt	Beperkt	Niet	Beperkt	Niet	Mono: realtime (Multi Beperkt)	Niet	Niet	Beperkt	Niet
intraday/niet intraday *	Beperkt	Medio '87 Beperkt	Beperkt	Beperkt	Beperkt	Niet	Beperkt	Niet	Beperkt	Beperkt	Niet
4 Opslag en verwerking gegevens	ARC (100% ABN)	NDC	Geisco & Mees	NDC	BAMTRAC of cliënt-PC	GEISCO	Telelion-computer	IBM Databank	IDC	IDC	Girotel-computer
5 Netwerk:											
- Banken —— Bank	Swift of aan NDC	Swift of aan NDC	N.v.t.	NDC (Swift toekomstig)	Diversen	Banklink of NDC	(Swift & NDC)	N.v.t.	Diversen	Diversen	N.v.t.
- Verw.centrum —— klant	GEISCOMARK III	GEISCOMARK III	Mailbox bij GEISCO	GEISCOMARK III		GEISCOMARK III	Videotex/ telefoon	Telefoonlijn	Telefoonlijn + Chase Access System		Telefoon/ Videotex
6 Benodigde hardware (afgezien van printers)	Terminal/PC & modem of telex	PC & modem	PC met modem, ook mainframe, terminal, of telex mogelijk		PC & modem	Telex, terminal, PC & modem, of mainframe	PC & modem of terminal (Viditel)	PC & modem of terminal (Viditel)	PC & modem of terminal	PC & modem	PC & modem of terminal (Viditel)
7 Data van Bank naar Klant											
A. Mutatie-informatie											
. valutadatum	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	= boekdatum
. omschrijving	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
. selecteren	ja	ja	neen	ja	ja	ja	ja	neen	neen	ja	ja
. betalingsadv.	neen	ja	ja	ja	ja	neen	neen	indien geboekt	indien geboekt	indien geboekt	neen
. bevestigingen transacties	neen	ja	neen	neen	apart systeem	neen	neen	neen	neen	ja (forex/ forward)	neen
B. Positie-informatie											
. valutair saldo	ja	ja	ja	ja		ja	ja	ja	ja	ja	= boeksaldo
. val. saldo toekomst	ja	ja	uitsplitsing float	toekomstig	ja	ja	ja	ja	neen	ja	neen
. bank/totalen	ja	ja	n.v.t.	ja	ja	ja	ja	n.v.t.	ja	ja	n.v.t.
. munt/totalen	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	n.v.t.
. lopende leningen	neen	wel door	neen	neen	wel door	ja,	ja,	ja,	neen	ja	neen
depots	neen	klant zelf	neen	neen	klant zelf	als	als	als	neen	ja	neen
termijncont.	neen	in te voeren in Adm. Fin. Contracten	neen	neen	in te voeren in Adm. Fin. Contracten	rekening	rekening	rekening	ja	ja	neen

Blad 1 * Deze systemen zijn (soms gedeeltelijk) real-time en intraday. Externe databronnen zijn dit vaak niet.

SYSTEEM INVENTARISATIE

	Omschrijving van aangeboden Electronic Banking systemen	ABN Bank	AMRO Bank	Bank Mees & Hope		Bank of America	Credit Lyonnais Bank Nederland		Nederlandse Credietbank			Postbank
		Balance Reporting	ATM	Meesnet Quik Comm.	Meesnet Multi Bank Reporting	Microstar	Lioncash	Telelion	Vidibanking	Infocash	Microstation	Girotel
7	C. Prijsinformatie			Aparte Module: Fin. Alert								
	. rente	neen	ja	ja	ja	neen	neen	komt	neen	ja	ja	alleen
	. valuta	ja	ja	ja	ja	neen	neen	komt	neen	ja	ja	informatie
	. tijdigheid	dagel. fixing	10 x per dag	realtime	realtime	-	-	-	-	9 x per dag	wordt 9 x p/d	over
	. commodities	neen	neen	neen	neen	neen	neen	neen	neen	neen	neen	postbank-
	. effecten	neen	neen	neen	neen	neen	neen	komt	neen	neen	neen	produkten
8	Data van Klant naar Bank											
	. betalen (TI/Telex)*	toekomstig(TI)	ja (TI)	ja (telex)	ja (telex)	ja (TI)	ja (telex)	komt (TI)	komt (rep.)	ja (rep.)	ja (TI)	ja (TI)
	. bevestiging	onbekend	neen	neen	neen	neen	neen	neen	neen	neen	neen	neen
	. depots	neen	neen		neen	instructies zijn	neen	neen	neen	neen		(alleen inleggen)
	. lenen	neen	neen	niet als standaard-scherm	neen	als standaard-scherm	neen	neen	neen	neen	niet als standaard-scherm	(alleen opnames en inleggen)
	. effecten	neen	AMROS	wel	neen	te	neen	komt	neen	neen	wel vrij	neen
	. forward	neen	neen	vrij via Mailbox	neen	verzenden	neen	neen	neen	neen	via electronic mail	neen
	. forex	neen	neen		neen		neen	neen	neen	neen		neen
	. doc. kredieten	neen	neen	ja	ja	apart systeem	ja	komt	neen	neen	standaard-scherm	neen
9	. vervalkalenders	neen	ja	neen	toekomstig	ja	neen	neen	neen	neen	ja	neen
	. cash flow prognoses	neen	prognose/ meting	neen	neen	ja	neen	neen	neen	neen		eenvoudig model voor budgettering
	. rendementsanalyses	neen	ja	neen	neen	ja	neen	neen	neen	neen	ja	neen
	. forex simulatie	neen	via Fintech	neen	neen	ja	neen	neen	neen	neen	aparte modules FX/rente	neen
	. koppeling met spreadsheet of Database	toekomstig	ja	neen	toekomstig	ja	neen	toekomstig	neen	neen	ja	neen
10	Taal	Engels of NL	Engels of NL	overw. Engels	overw. Engels	Engels	Engels/Frans	Engels of NL	Nederlands	Engels	Engels	Nederlands

Blad 2

* TI: automatische debitering
Telex: verzenden instructie ter debitering

Toelichting

In de eerste rij ziet u de aanbiedende bank, in de tweede rij de naam van het aangeboden systeem.

In de derde rij geven wij aan of het systeem een monobank- of een multibank-systeem is. Bij een monobank-systeem is het alleen mogelijk gegevens te ontvangen over de rekeningen bij de bank waar rekeningen worden aangehouden. Bij een multibank-systeem is het technisch mogelijk ook gegevens van andere banken te ontvangen.

In de vierde rij geven wij aan of het een workstation- of een terminal-systeem betreft.

In de vijfde rij geven wij aan in welke netwerkcomputer de opslag en voorbewerking van de aan te leveren data plaatsvindt.

In de laatste rij geven wij de mogelijkheid van transactie-initiatie aan. Bij een aantal systemen kan via het systeem worden betaald, of wordt dit binnenkort mogelijk. De term "telex" geeft aan dat het hier geen directe transactie-initiatie betreft, maar een vorm waarbij feitelijk alleen de betalingsopdracht via datacommunicatie wordt verzonden; deze doorloopt dan gewoon de normale verwerkings- en fiatteringsgang bij de bank. Deze vorm levert voor het bedrijf geen wezenlijke versnelling van de betaling op.

Voor wat de prijsstelling van Electronic Banking-systemen betreft, blijkt het dat per aanbiedende bank en per toepassing de kosten nogal uiteenlopen. Bij een terminal-systeem zijn er bijvoorbeeld meestal geen softwarekosten. De prijsstelling is momenteel hevig in beweging, voorlopig is er nog geen rust op de aanbiedersmarkt. Er is een trend naar prijsverlaging waarneembaar.
In dit overzicht zijn de nieuwe betalingsprodukten van de AMRO-Bank voor het midden- en kleinbedrijf niet verwerkt.

3. Toepassingsmogelijkheden

De huidige toepassingsmogelijkheden van Electronic Banking-systemen laten zich als volgt omschrijven:

Middelenbeheer

Bij middelenbeheer gaat het om liquiditeiten-, saldo- en geldstroombeheer. Hierbij is de mogelijkheid een valutair saldo te genereren van groot belang.

Wanneer het systeem real time-mogelijkheden kent, zal dit voornamelijk interessant zijn, wanneer de gebruiker veel data hanteert die buiten de BGC-batch-verwerking om worden verwerkt.

Transactie-initiatie kan voor de middelenbeheersfunctie waarde hebben, wanneer de treasurer zekerheid heeft over het tijdstip waarop de via het systeem geïnitieerde betalingen worden uitgevoerd.

Debiteurenbeheer

Het beheer van de debiteuren met behulp van een Electronic Banking-systeem heeft twee invalshoeken.

In de ene invalshoek staat de ondersteuning van of zelfs de integratie met de debiteurenadministratie centraal.

In de andere invalshoek komen meer verkoopgerichte toepassingen aan de orde, zoals beslsissingen of nieuwe orders van een cliënt kunnen worden aangenomen dan wel bestellingen kunnen worden uitgeleverd.

Crediteurenbeheer

Crediteurenbeheer speelt alleen een rol wanneer het systeem ook transactie-initiatie biedt, dan wel de mogelijkheid om betalingsdiskettes aan te maken. Juist voor het middelgrote bedrijf kan transactie-initiatie door middel van Electronic Banking interessant zijn, omdat zij moeilijk toegang hebben tot de zeer geavanceerde betaalvormen.

Een aantal systemen biedt verschillende vormen van beslissing-ondersteunende modules. Dit varieert van eenvoudige modellen tot ingewikkelde programma's. Het betreft saldo-cashflow-voorspellingen, koersanalyses en koersprognoses, modules voor "what-if" analyses en modules voor contractadministratie. Wij denken dat vooral op dit terrein de software-houses activiteiten zullen gaan ontwikkelen en de banken zullen terugdringen naar hun oorspronkelijke positie van informatieleverancier.

4. De vraagzijde

De toenemende vraag naar Electronic Banking-toepassingen is een illistratie van de voortschrijdende professionalisering van de financiële functie binnen bedrijven, die reeds enige tijd aan de gang is.

De steeds verdergaande administratieve automatisering heeft een verstrekkende invloed gehad op het bestuurlijke informatieproces. De toenemende professionalisering leidde tevens tot een steeds grotere know-how op bancair gebied, ook binnen kleinere organisaties.

De know-how op het gebied van zowel automatisering als treasury-vraagstukken stelt de banken in de gelegenheid de treasurer een zeer geavanceerde "toolkit" te bieden in de vorm van een Electronic Banking-systeem.

De "Wet van de remmende voorsprong" kan bij een organisatie aanleiding zijn voor de vervanging van de huidige administratieve systemen. Ons inziens zal de treasurer er goed aan doen te sturen naar een nieuw systeem dat een geïntegreerde toepassing van Electronic Banking en een Treasury Informatie Systeem mede mogelijk maakt en hiermede een voorsprong verwerft.

Natuurlijk is het na de aanschaf van een Electronic Banking-systeem primair de verantwoordelijkheid van de gebruiker om het interne deel van zijn Treasury Informatie Systeem te ontwikkelen.

Wij hebben de gebruikers van Electronic Banking-systemen vragen op een aantal terreinen gesteld.

De "trigger", die heeft geleid tot de aanschaf van een Electronic Banking-systeem, is niet altijd gemakkelijk te achterhalen. Wij hebben de indruk gekregen dat gerichte marketing-inspanningen van de bank hierbij een rol spelen.

Bij de selectie van een Electronic Banking-systeem wordt dan ook niet altijd even gericht te werk gegaan. Wij hebben de indruk, dat tijdens het selectieproces van een meer volledig overzicht van de mogelijkheden van de Electronic Banking-markt meestal nog geen sprake is.

Het is ons in de interviews opgevallen dat bij veel van onze gesprekspartners ten tijde van de introductie van het systeem de, voor multibank-systemen foutieve, gedachte leefde dat het gebruik van een Electronic Banking-systeem van een bepaalde bank, ook betekent dat het merendeel van de in- en uitgaande betalingen over die bank moet worden geleid. Deze vermeende ombuigingen van de geldstromen werden door de geïnterviewden om twee redenen als een groot bezwaar gezien.

Ten eerste was bij al onze gesprekspartners sprake van een jarenlange relatie met een hoofdbankier, die men niet zomaar wilde verstoren.

Ten tweede bleek men terug te deinzen voor de vrij forse interne operatie, die over het algemeen nodig is om de geldstromen substantieel over een andere bank te gaan leiden.

Met deze twee bezwaren in het achterhoofd zal men, wanneer de hoofdbankier een op het eerste gezicht bevredigend systeem aanbiedt, minder snel onderzoeken welke andere mogelijkheden van Electronic Banking er zijn.

De mogelijkheid een bepaald systeem op proef te krijgen, blijkt achteraf bij de uiteindelijke aanschaf zwaar te hebben gewogen. Uit de interviews blijkt, dat het gebruikersgemak van het systeem bij de keuze een belangrijk element is. Wanneer men voor het eerst achter het scherm plaatsneemt en snel het gevoel heeft het systeem te begrijpen en te kunnen bedienen, zal dit de keuze positief beïnvloeden. Eerdere gebruikservaring met de hardware van een systeem (Viditel, PC of terminal) is hierbij van belang.

Men is doordrongen van het feit dat kosten-/batenanalyses van het systeem zeker vooraf moeilijk zijn te maken. Vaak wordt een wat globale berekening gemaakt. Men gaat er doorgaans vanuit, dat de implementatie van het systeem geen substantiële wijzigingen in de personele bezetting of in de indirecte kosten teweeg zal brengen. Op basis van de te behalen tijdwinst in het verkrijgen van de saldi- en transactie-informatie maakt men vervolgens een schatting van de kosten en baten.

Waar beslissingen ten aanzien van automatisering in organisaties soms grootschalige en moeizame processen zijn, blijkt de beslissing tot aanschaf van een Electronic Banking-systeem relatief eenvoudig te worden genomen.

De implementatie van het Electronic Banking-systeem verloopt doorgaans redelijk eenvoudig. Alle gesprekspartners waren te spreken over de wijze waarop de betreffende bank dit proces begeleidde. Meestal was een dag installatie en demonstratie door een of twee medewerkers van de bank voldoende om de gebruikers in te werken. De meeste banken bieden daarnaast een "hot-line"-service, die soms ook buiten kantooruren bereikbaar is, voor gebruikers die vastlopen of brandende vragen hebben.

5. Voor wat voor type bedrijven is Electronic Banking nu eigenlijk geschikt?

In het algemeen kan gesteld worden dat de huidige "state of the art" in Electronic Banking op dit moment interessant is voor die groep van bedrijven die voldoen aan de volgende kenmerken:

- er moet een zeker volume zijn in betalingen van en aan het bedrijf;
- tijdigheid van het hebben van financiële informatie moet van belang zijn;
- de factor kapitaal moet in het bedrijf een zekere dominantie hebben;
- binnen het bedrijf moet de bereidheid/ambitie leven om actief betrokken te zijn bij nieuwe (technologische) ontwikkelingen;
- het hebben van meerdere bankrelaties kan van belang zijn;
- een belangrijk deel van in- en verkoop verloopt via vreemde valuta;
- een zeker volume aan letters of credit bestaat;
- het hebben van een zeer groot aantal verschillende debiteuren en/of crediteuren.

Het voldoen aan slechts enkele van deze karakteristieken kan voor een bedrijf reeds een reden zijn om een Electronic Banking-systeem aan te schaffen.
Gezien de huidige stormachtige ontwikkelingen zijn wij van mening dat Electronic Banking steeds sneller voor een steeds grotere groep organisaties toepasbaar zal blijken te zijn.

Als we nu wederom kijken naar de twee typen van Electronic Banking-systemen, te weten terminal- en workstation-systemen die een eigen specifieke toepassing hebben in de markt, dan kan verder globaal worden aangegeven voor welk type bedrijven deze twee typen van toepassingen geschikt zijn.

- Workstation-systemen zullen vooral geschikt zijn voor grotere bedrijven, maar ook voor kleinere bedrijven, waarvoor één van de voornoemde karakteristieken zo zwaarwegend is, dat een workstation-systeem wenselijk is.

- Terminal-systemen kunnen het best worden toegepast in een gecentraliseerde treasury-omgeving, maar ook kan dit systeem worden gebruikt door bedrijven die een niet erg intensief gebruikte stand-alone-toepassing overwegen.

Het ene type systeem is niet beter of slechter dan het andere type, alleen de toepassingsmogelijkheden zijn verschillend.

Deze passage is begonnen met het aangeven van typen bedrijven, waarvoor Electronic Banking geschikt is. In wezen wordt de toepasbaarheid van een bepaald Electronic Banking-systeem bepaald door de wijze van organisatie van de treasury-functie van een bedrijf.

Workstation-systemen zijn in aanschaf duidelijk duurder dan de terminal-systemen. De grotere flexibiliteit van workstation-systemen, de betere mogelijkheid tot integratie in de eigen administratieve systemen, en de bij intensief gebruik relatief lagere datacommunicatiekosten kan voor bepaalde bedrijven dermate belangrijk zijn, dat een workstation-systeem toch de voorkeur verdient. Tevens bieden workstation-systemen de mogelijkheid van uitbouw met meer terminals in een "local area network".
Alle Electronic Banking-systemen hebben gemeen dat zij de kwaliteit van de financiële informatie verbeteren.

De aangeleverde data zijn betrouwbaarder en sneller beschikbaar dan de informatie die op een traditionele wijze naar de bedrijven wordt gezonden.

6. Beveiliging

Wij willen apart aandacht besteden aan het beveiligingsaspect van Electronic Banking-systemen. De beveiligingsaspecten gaan steeds zwaarder wegen.

De eisen inzake beveiliging en interne controle die in het algemeen aan geautomatiseerde systemen zijn te stellen, zijn geheel van toepassing op Electronic Banking-systemen. De eisen die gelden ten aanzien van integriteit, autorisatie, beheersbaarheid, continuïteit en controleerbaarheid van de data in het dataverwerkend proces gelden zodoende onverkort. Wel is het zo dat de eisen ten aanzien van interne controle en beveiliging zwaarder wegen wanneer het Electronic Banking-systeem op een meer geavanceerde of geïntegreerde wijze wordt toegepast.

Het is van belang om voldoende functiescheiding en preventieve interne controle in de organisatie rondom Electronic Banking in te bouwen.

Naast de operationele waarde van een goede beveiliging, heeft de wijze van beveiliging ook een marketing-waarde. De aanbiedende bank kan hierin een verkoopargument vinden, door te stellen dat haar Electronic Banking-systeem beter is beveiligd dan de systemen van de concurrentie.

Ook vanuit maatschappelijk oogpunt wordt steeds meer nadruk gelegd op de noodzaak om geautomatiseerde systemen goed te beveiligen.

7. Vergelijking van vraag en aanbod

Aan het einde van dit artikel een confrontatie tussen de vraag naar Electronic Banking-systemen en het aanbod van Banken daarvan.
Deze vergelijking van vraag en aanbod van Electronic Banking-systemen levert het volgende op.

De aanbieders zijn druk bezig hun systemen te verbeteren en geschikt te maken voor diverse groepen cliënten. In de toekomst zullen er meer aanbieders tot de markt toetreden. Niet alleen banken, maar ook softwarehouses zullen de software gaan leveren. De toepassingen van de softwarehouses zullen vermoedelijk meer gericht zijn op het opzetten van een intern Treasury Informatie Systeem en zullen waarschijnlijk de integratie met bestaande administratieve systemen binnen de bedrijven vergemakkelijken.

Potentiële gebruikers reageren afwachtend. De aanschaf van een Electronic Banking-systeem stellen zij uit tot het aanbod verder is uitgekristalliseerd. Tot dat moment zullen de bedrijven in vele gevallen hun aandacht besteden aan het opzetten en verbeteren van de treasury-organisatie. Het is heel goed mogelijk om een flexibele, stand alone-toepassing van een Electronic Banking-systeem te creëren, eventueel met gebruikmaking van een proefperiode zoals die door een aantal banken wordt aangeboden. Ook rijst soms de vraag of de kosten die op dit moment moeten worden gemaakt om tot een goed Electronic Banking-systeem te komen opwegen tegen de baten. Op termijn is het wel zo dat Electronic Banking binnen het bereik van steeds grotere groepen van (potentiële) gebruikers zal komen.

8. Voorzienbare ontwikkelingen

Dit artikel zal worden afgesloten met een korte schets van de door ons voorzienbare ontwikkelingen.

Als eerste zullen wij aangeven welke ontwikkelingen op korte termijn op het gebied van Electronic Banking te verwachten zijn:
- over enige tijd pas zal de prijsstelling van Electronic Banking-systemen tot rust komen.
  De huidige neerwaartse trend zal nog even doorgaan;

- er zullen nog meer aanbieders van Electronic Banking-systemen op de markt komen.
  Softwarehouses zullen in plaats van banken software proberen aan te bieden;
- in de technische sfeer zullen verdere ontwikkelingen optreden, real time-systemen zullen meer toegepast worden. Transactie-initiatie zal belangrijker worden evenals de multibank-systemen;
- integratie met interne Treasury Informatie Systemen en met andere administratieve systemen zal steeds vaker worden toegepast;
- het beveiligingsaspect zal meer en meer worden benadrukt;
- de standaardisatie zal tussen de banken ten aanzien van systemen en informatie-uitwisseling tot stand komen.

Wanneer de Electronic Banking-ontwikkeling in een wat ruimer kader wordt geplaatst, dan denken wij dat de volgende ontwikkelingen te voorzien zijn:
- Electronic Banking is een belangrijke stap in de richting van "the office of the future" waarin papier tot het minimum is beperkt;
- ook denken wij dat Electronic Banking in relatie tot werkplekautomatisering een belangrijke ontwikkeling zal zijn;
- ten slotte verwachten wij allerlei interessante mogelijkheden zoals:
  . zou S.W.I.F.T. misschien direct toegankelijk worden voor het bedrijfsleven;
  . komt er een BGC-netwerk computer;
  . hoe staat het met "homebanking";
  . wanneer komt elektronisch betalen.

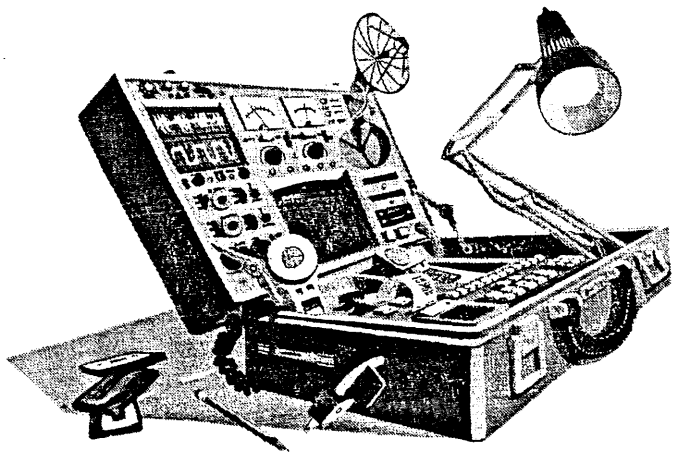
Het lijkt ons goed om ook hier nogmaals te stellen dat door de steeds verder voortschrijdende informatietechnologie op zeker moment het tijdstip zal zijn aangebroken dat Electronic Banking zal zijn toegepast in vrijwel iedere organisatie. De "paperless banking society" is dan aangebroken.

Kortom, wij denken dat er een interessante tijd zal aanbreken in de relatie tussen cliënt en bank.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Zomer 1987



DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

INTRODUCTIE VAN DE APPLE MACINTOSH IN DE KPMG-ORGANISATIE

Waarom Apple Macintosh?

Het voormalige KMG Computer Audit Sub Committee heeft met het op de markt verschijnen van de IBM PC alle member firms aanbevolen het computergebruik in de controle te standaardiseren op IBM PC en compatible micro's, die werken met MS DOS. De onder auspiciën van de CASC voor gemeenschappelijk gebruik door member firms ontwikkelde toepassingen zijn voor die combinatie gemaakt.

Peat Marwick International is een andere weg ingeslagen door vanaf de introductie direct met de Apple Macintosh in zee te gaan.

Het is duidelijk dat er, nu de fusie tussen KMG en PMI is gerealiseerd, tussen beide micro's gekozen moest worden. Het is technisch mogelijk voor gemeenschappelijk gebruik toepassingen te ontwikkelen die op beide typen micro's kunnen worden gebruikt. Het grote bezwaar is echter dat dit een aanzienlijke verzwaring met zich mee brengt van opleiding en ondersteuning en dat uitwisseling tussen controleploegen die verschillende micro's gebruiken ernstig wordt bemoeilijkt. Standaardiseren op één type is dus noodzakelijk.

Uiteindelijk is de keuze gevallen op de Apple Macintosh.

Gebleken is dat dit voor velen in de voormalige KMG-organisatie toch wel als een verrassing is gekomen. Enige toelichting is dus wel op zijn plaats.

Het besluit is voorbereid in de Computer Audit Joint Task Force, één van de vele Task Forces die het Executive Committee van KPMG heeft geadviseerd over het KPMG business plan en budget.

Specialisten uit de PM ontwikkelgroep en uit de KKC ontwikkelgroep hebben intensief kennis genomen van elkaars software en de wijze van ontwikkelen. Gezamenlijk werd een bezoek gebracht aan Apple.

De hieruit verkregen informatie leidde tot de conclusie dat de Apple Macintosh duidelijke voordelen biedt ten opzichte van op MS DOS gebaseerde micro's. Speciaal het gebruik in een controle verloopt met minder technische problemen.
Een belangrijke oorzaak daarvan is dat de in de Apple toegepaste technologie veel beter aan de gebruiker aangepaste toepassingen mogelijk maakt.

Uiteraard werd tevens geïnformeerd naar de plannen van IBM terzake. Na de nieuwe recente aankondigingen is inmiddels gebleken dat de voordelen van de Apple Macintosh in het gebruik voor controletoepassingen niet zijn aangetast.

Nadat in KPMG verband begin maart 1987 de beslissing was gevallen om de Apple Macintosh als standaardmachine in de controlepraktijk te gaan gebruiken, moest worden beslist op welke termijn de introductie van de Macintosh binnen KKC diende plaats te vinden.

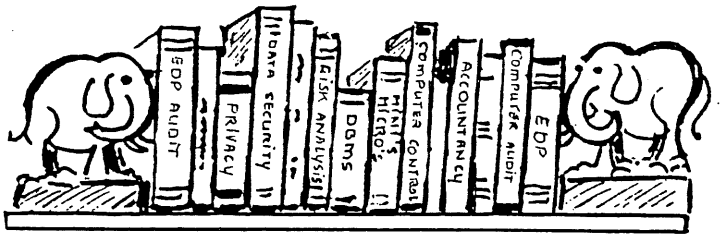
Alle voor- en nadelen afwegend hebben we gekozen voor een introductie, in een zo ruim mogelijke opzet, nog vóór de zomervakantie 1987. Hoewel de door KKC ontwikkelde software zoals FAT/FMT en Palet vooralsnog niet op de Macintosh beschikbaar was, is het belangrijk geacht om zo gauw mogelijk door de, gelukkig niet al te, zure Apple heen te bijten en de apparatuur reeds toen te demonstreren en te verspreiden met de thans reeds vanuit PMI beschikbare software.

De introductiedagen voor vennoten vaktechniek en microbeheerders vonden eind juni 1987 plaats, gevolgd door regionale dagen in de eerste weken van juli.

De acceptatie van de Macintosh was boven verwachting. De bereidheid van zelfs de meest fervente MSDOS-gebruikers om de Mac te leren kennen, geeft ons goede hoop op een verdere invoering van de microcomputer in de accountantscontrole, waar ze reeds nu nog nauwelijks valt weg te denken.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services



Zomer 1987

Boeken

door drs. P. Westdijk, ing. J.C. van Winkel en J.A.W. Winterink

The international handbook on computer crime,
Auteur: Ulrich Sieber
Uitgever: John Wiley & Sons, 1986

De auteur

Ulrich Sieber is verbonden aan de universiteit van Freiburg (BRD), waar hij zich bezig houdt met strafrechtelijke aspecten van "computercriminaliteit". Op dit gebied heeft hij diverse studies uitgevoerd in nationaal en internationaal verband.

Het boek

In het boek wordt eerst beschreven wat computercriminaliteit is; vervolgens worden vele voorbeelden uit de internationale literatuur gegeven.

Daarna wordt de juridische problematiek behandeld, zoals bewijsvoering, strafbaarstelling en geldend recht (strafrecht of privaatrecht bijvoorbeeld). Hierin komt een veelheid van (internationale) wet- en regelgeving gedetailleerd aan de orde.
In deze bespreking zal slechts aandacht worden besteed aan de aanbevelingen; geïnteresseerden worden naar het boek zelf verwezen.

Sieber geeft vervolgens aan hoe een systeem van adequate beveiligingsmaatregelen in een organisatie dient te worden ingevoerd en welke aspecten door dat systeem dienen te worden afgedekt.

Afsluitend wordt enige aandacht besteed aan de problematiek van het vervolgen van computercriminaliteit.

In twee appendices geeft Sieber verder uitgebreide opsommingen van beschikbare literatuur en wetteksten.

1. Computercriminaliteit

Door een toenemende automatiseringsgraad binnen organisaties nemen de gevolgen van fouten en criminele handelingen binnen een computersysteem in belangrijkheid toe.

Sieber definieert computercriminaliteit als "any illegal, unethical or unauthorized behaviour involving automatic data processing and/or transmission of data". Deze ruime definitie maakt het mogelijk dezelfde werkhypotheses en -modellen te hanteren voor de diverse vormen.

Computercriminaliteit wordt door Sieber onderverdeeld in drie hoofdgroepen:
1. economische criminaliteit (wat, hoe, door wie);
2. inbreuk op persoonlijke belangen (privacy);
3. inbreuk op "superindividual interests" (nationale veiligheid, grensoverschrijdend gegevensverkeer e.d.).

Ad 1. Economische criminaliteit

Fraude door manipulatie van computersystemen heeft meestal betrekking op immateriële activa, zoals banksaldi (elektronisch betalen, geldautomaten), salaris, gewerkte uren e.d. Fraude met boekingen, waardoor materiële zaken kunnen worden verduisterd komt minder frequent voor.

Manipulatie vindt plaats gedurende het gehele traject van verwerking: incorrecte invoer, beïnvloeden van verwerking (ongeoorloofde wijziging van programmatuur bijvoorbeeld), aanpassen van de output en tijdens gegevenstransport.

Verhoudingsgewijs wordt door DP-specialisten minder en door leken meer gefraudeerd. De verwachting hierbij is dat meer niet-personeel bij fraudes betrokken zal zijn (onder andere hacking). Ook samenspanning werd in dit kader genoemd.

Juridische aspecten

Sieber beveelt aan de intentie een persoon of organisatie te benadelen strafbaar te stellen. Hierdoor blijven onopzettelijke fouten buiten de strafrechtelijke sfeer.

Spionage heeft met name betrekking op programmatuur (illegale kopieën) en minder op bedrijfsinformatie.

Het kopiëren van bestanden is de meest gebruikte methode: door infiltratie, corruptie en het manipuleren van personeel wordt dit mogelijk gemaakt. Hacking en het aftappen van terminal-aansluitingen om passwords te onderscheppen zijn nieuwe technieken hiervoor.

Gebruikers, dealers en niet-loyaal personeel zijn de hoofdgroepen die zich met illegaal kopiëren bezig houden. Beloning door concurrerende bedrijven komt hierbij veelvuldig voor.

Juridische aspecten

Gegevens zijn niet tastbaar, waardoor wettelijke bescherming bemoeilijkt wordt. Voor programmatuur zouden contractbepalingen, handelsgeheim, patenten en copyrights als regelgeving kunnen dienen.

Sabotage kan betrekking hebben op het beschadigen van gegevens of apparatuur.

De fysieke beschadiging is het meest verbreid. Logische beschadiging kan plaatsvinden door een tijdbom, een programma dat een of meerdere bestanden na het verstrijken van een bepaalde tijd volledig wist.

Naast terroristen en concurrenten is ontevreden personeel een risicofactor.

Juridische aspecten

Fysieke beschadiging valt in principe onder de reguliere wetgeving. Sieber stelt voor het opzettelijk/bewust beschadigen van gegevens strafbaar te stellen; probleem blijft hierbij de bewijslast.

Diefstal van computertijd is op het eerste gezicht niet zeer nadelig voor de toepassingen en veiligheid van de eigen organisatie. Er is echter sprake van gemiste opbrengst; in extreme gevallen kan een hoge bezettingsgraad van de computer leiden tot onterechte vervanging door een grotere machine.

Juridische aspecten

Sieber stelt dat ongeautoriseerd computergebruik strafbaar moet worden gesteld indien benadeling wordt beoogd. Hierbij zal de bewijslast echter problemen kunnen geven; toegangsbeveiliging zal hierin een rol kunnen spelen.

Ongeoorloofde toegang zoals hackers dat uit hobbyisme doen, noemt Sieber "korte-broeken-criminaliteit", waardoor meestal geen schade optreedt omdat er geen financieel motief aanwezig is. Als er schade ontstaat, wordt dat als "toeval" aangeduid. In een aantal gevallen heeft hacking geleid tot betere beveiligingsmaatregelen.

Juridische aspecten

Sieber stelt voor ongeoorloofde toegang en aftappen van lijnen strafbaar te stellen via speciaal daarvoor opgestelde wetgeving.

Als voorbeeld van **traditionele criminaliteit** waarbij nu de computer als hulpmiddel is gebruikt, voert Sieber het bekende voorbeeld van Equity Funding aan, waarbij een verzekeringsmaatschappij voor miljoenen onechte polissen als verkocht rapporteerde.
Fraude inzake belastingen kan eveneens in deze worden genoemd.

Juridische aspecten

Internationaal dient te worden gestreefd naar een harmonisatie op het gebied van boekhouding/administratie, belastingen en douaneformaliteiten.

Ad 2. Inbreuk op persoonlijke belangen (privacy)

Het privacy-vraagstuk beslaat meer aspecten dan alleen criminologische; er is veel anders gerichte publieke discussie over de afweging van diverse belangen.

Als vormen van inbreuk op persoonlijke belangen worden genoemd:
- verstrekken en gebruiken van onjuiste informatie;
- onwettige verspreiding en misbruik van juiste gegevens;
- onwettig verzamelen en opslaan van gegevens;
- inbreuk op privacy-wet- en regelgeving.

Juridische aspecten

De OECD heeft de volgende aanbevelingen gedaan:
- beperkt gegevens vastleggen, alleen met medeweten van subjecten;
- alleen relevante gegevens, accuraat en compleet;
- specificatie van het doel van de gegevensverzameling;
- beperking van het gebruik tot het gespecificeerde doel;
- adequate beveiliging;
- openheid ten aanzien van ontwikkelingen en beleid rond de verzameling;
- subject heeft toegang tot en invloed op de gegevens.

Sieber voegt hieraan toe: internationale harmonisatie. Op internationaal niveau (bijvoorbeeld EEG) dient overeenstemming te worden bereikt over de basisprincipes, waarna een duidelijke en eenduidige lijst met strafbare feiten en bijbehorende bestraffing daarin kan worden opgenomen.

Ad 3. Inbreuk op "superindividual interests" (nationale veiligheid, grensoverschrijdend gegevensverkeer e.d.

Dit aspect wordt niet nader uitgewerkt.

Omvang en ontwikkelingen

De omvang van het aantal gevallen van computercriminaliteit is niet exact bekend; Sieber geeft in dit kader voor een aantal landen in Europa en de USA schattingen (niet alle bekende gevallen vallen onder bestaande wetgeving; verder blijft een aantal gevallen onontdekt).

De schade die bij computercriminaliteit optreedt is vaak groter dan in meer traditionele fraudes e.d. omdat het manipuleren met een groot bedrag soms even makkelijk is als manipuleren met een klein bedrag.

Toename van het aantal computertoepassingen in met name financiële sfeer betekent dat de omvang van de computercriminaliteit zal toenemen (mits maatregelen worden getroffen).

2. Beveiligingsmaatregelen

Om computercriminaliteit te voorkomen is een stelsel van adequate beveiligingsmaatregelen vereist. Doelen van een dergelijk stelsel zijn:
- afschrikken van personen met frauduleuze bedoelingen;
- voorkomen van succesvolle manipulaties;
- ontdekken van manipulaties en stoppen van verdere uitvoering;
- minimaliseren van gevolgen van manipulaties;
- vervullen van wettelijke bepalingen.

Hierbij zijn een aantal bedreigingen te onderkennen:
- computercriminaliteit zoals hiervoor aan de orde is geweest;
- verwaarlozen van procedures;
- menselijke fouten en onbekwaamheid van personeel;
- natuurrampen;
- stakingen.

Beveiliging dient in een organisatie beleidsmatig te worden aangepakt. Een Task Force zou het proces projectmatig kunnen sturen. Eerst wordt bepaald wat beveiligd moet worden, met andere woorden een inventarisatie van "waarden". Risico-analyse kan daarna gebruikt worden om te bepalen waartegen de waarden beveiligd moeten worden. Een kosten/batenanalyse van de verschillende mogelijkheden geeft aan hoe beveiligd zal worden.

De beveiliging dient daarna te worden getest (scenario's, "inbraakgroepen"). Tegenmaatregelen kunnen zijn opgenomen in de applicatie, systeemprogrammatuur of anderszins technisch opgelost. Na implementatie dient het stelsel van maatregelen adequaat te worden beheerd.

Als belangrijke elementen van beveiligingsbeleid worden de volgende gebieden genoemd:
- personeel en opleiding (selectiecriteria, screening, job rotation, ontslagprocedures, goede werksfeer e.d.);
- fysieke maatregelen (brandwerende materialen, airconditioning met ruime capaciteit e.d.);
- organisatie en technische maatregelen.

Dit laatste gebied wordt als volgt verder uitgewerkt in een algemeen en een specifiek deel.

Algemeen:
- automatiseringsorganisatie direct onder de leiding;
- functiescheiding in automatiseringsorganisatie en systeemontwikkeling, ondersteund door beveiligingspakket;
- aanwijzen verantwoordelijke gebruikers;
- onafhankelijke controle op verwerking;
- procedures rond foutafhandeling;
- recovery-plan.

Specifiek:
- inputcontrole (onder andere organisatie rond brongegevens, automatische checks, controletotalen, check digits e.d.);
- communicatie (encryptie, verzegelen tapes, aanlog-procedures);
- verwerking (audit operating system, overdrachtsprocedures);
- opslag/bestandsbeheer;
- programmabeheer;
- EDP audit;
- verzekeringen;
- goede en duidelijke contracten;
- scenario's voor gerechtelijke stappen in geval van computercriminaliteit.

Gerechtelijke vervolging

Van computercriminaliteit ontbreekt in een aantal gevallen elk spoor door wissen van het bewijs. In andere gevallen is het bewijs voor de reguliere opsporingsambtenaren niet leesbaar. Het verdient dan ook aanbeveling het opsporingsapparaat op te leiden in automatisering om te komen tot een adequate opsporing en vervolging.

Conclusie

Het boek geeft de indruk van een gedegen studie en kan tevens dienen als naslagwerk op grond van de vele voetnoten.

Zomer 1987

Managing Computer Risk A guide for the policy maker
Auteurs: G.M. Ward en J.D. Harris (Price Waterhouse)
Uitgever: John Wiley & Sons

Dit boek met een omvang van 182 pag. is met name geschreven voor functionarissen die betrokken zijn bij het management van geautomatiseerde systemen. In dit verband worden met name genoemd de "financial executive, senior manager, policy maker, auditor and data security officer".

Het boek bestaat uit twee delen:
1. The policy maker's perpective (hoofdstuken 1 tot en met 6).
   Hierin wordt in het algemeen behandeld welke veranderingen er plaatsvinden op het gebied van de automatisering en wat hiervan de consequenties zijn voor het management van deze systemen. Hoe bouw ik beheersbare systemen en welke acties zou ik als manager in mijn organisatie kunnen nemen om controle te kunnen blijven uitoefenen over de door mij gedelegeerde taken. Hierbij wordt ook gesproken over de taak en de plaats van een interne (EDP-)audit-afdeling.
2. Understanding the technology (hoofdstukken 7 tot en met 12).
   In dit deel worden in een vogelvlucht allerlei "technische" zaken behandeld, zoals gedistribueerde gegevensverwerking, DBMS, datacommunicatie, e.d.

Vanwege het zeer globale karakter van het boek wordt hier slechts ingegaan op hetgeen op de omslag wordt genoemd als de "tien moeilijkste problemen met betrekking tot data security".
Oordeelt u zelf of u zich hierin kunt vinden:
Het blijkt hierbij te gaan over 10 vragen die men zich kan stellen bij het inventariseren van de mate waarin er sprake is van "computer security", teneinde de gebieden te onderkennen waar nog (extra) aandacht aan beveiliging moet worden gegeven.
1. Have written corporate policies regarding data security been distributed to employees.
2. Does a data security function exist and to whom does it report.
3. Do internal auditors really have EDP auditing (including data security review) capabilities.
4. Are data processing, data security, EDP auditing and user departments working together or at loggerheads.
5. Is there an adequate reporting system.
6. Has a security software strategy been developed and is it being followed.
7. Is your data security system active or passive.
8. Is the password and user-id system serious or trivial.

9. When were corporate data security controls last reviewed by top management.
10. Is top management really interested in data security.

Dit laatste punt wordt door de auteurs - terecht - als het meest belangrijke onderkend.

Conclusie

Dit overigens zeer leesbare werk is te globaal van opzet om als serieus handboek te worden beschouwd voor een (aankomend) EDP auditor. Het betekent dat het boek voor degenen met nog weinig kennis op het gebied van beveiliging en controle een aardige "binnenkomer" zou kunnen betekenen.
De meeste onderwerpen met betrekking tot beveiliging en controle worden wel aangeroerd, maar van een methode van aanpak van deze problemen is geen sprake.
Voor het hogere management is dit boek mijns inziens inderdaad bruikbaar, zoals door de auteurs wordt gesteld. Het zal zeker een goede bijdrage kunnen leveren aan de bewustwording van het management van haar verantwoordelijkheden ten aanzien van computerbeveiliging en van de instrumenten die zij hierbij zou kunnen hanteren.
De stelling dat dit boek ook door auditors en data security officers gelezen zou dienen te worden, kan op grond van onze studie niet worden onderschreven. Het is voor organisaties te hopen dat genoemde functionarissen de in het boek aangereikte kennis reeds in hun bagage hebben.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Zomer 1987

TIJDSCHRIFTEN

door mw. D. Jansen Heijtmajer, mw. drs. A. Klaver en J.L.H. Kooijman

"A comparison of judgement, skills and prompting effects between auditors and systems analysts". S.V. Grabski, J. Hal Reneau, S.G. West *)

De drie bovengenoemde heren hebben een onderzoek verricht naar het nut van inschakelen van "auditors" bij het ontwerpproces van geautomatiseerde systemen. Het inschakelen van accountants zou verbetering van het stelsel van interne controlemaatregelen moeten opleveren. Uit kostenoogpunt is opnemen van interne controlemaatregelen tijdens de bouw verre te prefereren ten opzichte van latere inbouw van deze maatregelen. Het lijkt daarom logisch accountants tijdens het ontwerpproces in te schakelen en uit een recente inventarisatie blijkt dit ook in negentig procent van de gevallen te gebeuren.

In het onderzoek van de heer Grabski en zijn collega's wordt nagegaan wat nu het daadwerkelijke effect is van het inschakelen van accountants bij het ontwerpproces. Hiertoe hebben zij een aantal algemene accountants, een aantal EDP auditors en een aantal systeemanalisten aan de tand gevoeld.
Met behulp van cases werd onderzocht of deze vogels van verschillende pluimage ook inderdaad verschillende kwaliteiten aan de dag legden bij het onderkennen van zwakheden in de interne controle en het zoeken van de juiste interne controlemaatregelen bij gegeven situaties. De verschillen tussen de drie groepen met betrekking tot deze vaardigheden bleken statistisch niet significant. Wat echter wel bleek, was dat alle drie de groepen veel betere resultaten behaalden wanneer zij gebruik konden maken van checklists, dan wanneer zij de maatregelen zelf moesten verzinnen.

De heer Grabski en zijn collega's menen hieruit te moeten concluderen dat de rol van de accountant teruggebracht kan worden tot het verstrekken van checklists. Hier zijn echter enkele vragen bij te stellen. De onderzoekers zelf geven twee kanttekeningen bij hun onderzoek. Ten eerste kan de compacte geringe informatie, die bij de cases verstrekt werd, invloed gehad hebben op het verschijnsel dat zulke geringe verschillen gevonden werden tussen de vertegenwoordigers van de vergeleken vakgebieden. Ten tweede is het effect van synergie buiten beschouwing gebleven. Groepsbesluitvorming geeft andere resultaten dan individuele besluitvorming. Het onderzoek was geënt op individuele besluitvorming, terwijl groepsbesluitvorming zich in de werkelijkheid voordoet.

*) Bron: "MIS quarterly" juni 1987.

Wij zouden willen ingaan op het eerste bezwaar. In werkelijkheid is er geen sprake van een gestructureerde probleemsituatie. De kwaliteit van een accountant ligt in het "zoeken van de krenten uit de pap".
Uit een spervuur van ongestructureerde, door ruis omgeven, informatie, dient hij die stukjes te zoeken die bijdragen tot het verkrijgen van een goed beeld van de situatie. Deze situatie sluit niet aan bij het hier besproken onderzoek, waarbij de krenten keurig op een bordje geserveerd worden. De onderzoeksresultaten doen daarom geen recht aan de specifieke vaardigheden van de accountant.

"Computer fraud detection techniques: design and use", Mercer *)

Dit artikel behandelt drie manieren waarop de accountant door de techniek geassisteerd computerfraudes op het spoor kan komen.

De eerste methode waarop de schrijver ingaat is het onderzoeken van bestanden met behulp van audit-programmatuur. Het voordeel van audit-programmatuur in vergelijking met handmatig onderzoek is de grote aantallen gegevens die zonder veel moeite op een bepaald criterium getoetst kunnen worden. Een voorbeeld hiervan is bijvoorbeeld het zoeken van een dubbel voorkomende naam of fiscaal nummer op een loonlijst. Een ander voorbeeld is het zoeken van slapende rekeningen die plotseling actief geworden zijn door verschillende generaties van een bestand te vergelijken. Voor dit soort onderzoeken kan audit-programmatuur zoals het bij KKC op microcomputers beschikbare pakket File Analysis Tool (FAT) gebruikt worden.

De tweede techniek die de heer Mercer aanbeveelt is die van de regressieanalyse. Zoals bekend is regressie-analyse een wiskundige methode om het statistisch verband tussen twee (enkelvoudige) of meer (multiple regressieanalyse) variabelen vast te stellen in een testset. Waarnemingsparen uit een te onderzoeken bestand kunnen aan het gevonden verband, de regressielijn, getoetst worden. Waarnemingsparen die te ver van de gevonden regressielijn afwijken, nodigen uit tot een nader onderzoek. Hier zou fraude in het spel kunnen zijn. Een voorbeeld dat de schrijver geeft, is het verband tussen het loonbedrag en de omzet van een filiaal in een winkelketen. Als een filiaal sterk afwijkt met zijn cijfers van het gevonden regressieverband, is het mogelijk dat niet alle verkopen verantwoord worden. De analyse kan niet alleen tussen verschillende filialen op één tijdstip (cross sectional) maar ook op verschillende tijdstippen van één filiaal uitgevoerd worden (time series). De schrijver wijst op enkele gevaren van deze statistische techniek. Ten eerste geldt het gevonden lineaire verband vaak alleen voor waarnemingen die zich dicht in de buurt van de onderzochte range bevinden. Daarnaast wordt gewaarschuwd dat een statistische samenhang nog geen causale relatie betekent en dat een bepaalde variabele vaak van meer dan één factor afhankelijk is. Het gevonden verband is daarom niet altijd even betrouwbaar. Ook al ontneemt een statistisch pakket de accountant de

*) Bron: "The accountants magazine" juni 1987.

last van het rekenwerk, toch zal hij het een en ander van de wiskundige achtergrond moeten weten om de techniek met verstand te kunnen gebruiken. Het is daarom wat optimistisch dat de schrijver stelt "common sense and a little basic reading should enable the auditor to start trying regression".

De derde techniek die in het artikel besproken wordt is die van onderzoek van system logs. Twee nadelen zijn verbonden aan system logs: zij zijn onleesbaar omdat zij niet afgestemd zijn op gebruik door auditors en ook een system log zelf kan aan fraude onderhevig zijn. Met behulp van system logs kan bijvoorbeeld het gebruik van gevoelige programma's of data opgespoord worden.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Zomer 1987

Automatisering
Beveiliging
Controle
NIEUWS

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

Automatisering

Verdere schaalvergroting

In het vorige Compact-nummer vermeldden wij de overname van SKK en de Cambridge group, bouwers en houders van verkooprechten van ACF2, door Uccel. Thans kunnen we melding maken van de overname van Uccel door Computer Associates. Deze overname werd geëffectueerd door een aandelenruil van meer dan 1,5 miljard gulden. CA is hiermee na IBM de grootste software-producent ter wereld geworden.

Het verschil in omzet is echter groot. De vergrote CA zal een omzet van tussen de 650 à 700 miljoen dollar krijgen. De software-poot van IBM daarentegen heeft een omzet van 5,5 miljard dollar.

Een verdere concentratie van producenten van software utilities in de IBM-omgeving is met deze fusie een feit geworden.

Referentie: De Automatisering Gids van 5 juni 1987 en latere persberichten.

Beveiliging

Te weinig back-up-tijd beschikbaar

Het Engelse onderzoekbureau Xephon heeft 39 MVS-computercentra ondervraagd naar hun back-up-praktijken. Het blijkt dat met de komst van steeds meer on-line-systemen het spanningsveld tussen een extra-shift en tijd voor back-up toeneemt. 40% van de respondenten maakte gelijktijdig met het on-line-werk back-ups ten koste van de response. 25% zei de back-up-procedures wegens gebrek aan tijd in het geheel over te slaan.

Een van de door het onderzoekbureau aangedragen oplossingen bestaat uit het gebruik van cartridge-eenheden (bijvoorbeeld de IBM 3480) waardoor de back-up-procedure versneld kan worden.

Commentaar

De vermelde praktijk maakt de noodzaak tot het regelmatig controleren van de werking van de back-up-procedures duidelijk.

Referentie: Computable 3 april 1987.

Tweede hands, voorzien van gegevens

In het Verenigd Koninkrijk ontdekte een koper van een tweede hands micro-computer dat de harde schijf nog personeelsgegevens bevatte van de Roual Signals and Radar Establishment van het Ministry of Defense.

Commentaar

Het zal duidelijk zijn, dat voorafgaand aan afstoting van geheugenmedia deze gewist moeten worden door ze in het geheel te beschrijven met bijvoorbeeld blanks. Ook in het gewone gebruik kan dit geen kwaad. Toegangsbeveiligingspakketten bevatten veelal een optie die het overschrijven van vrijgegeven ruimte mogelijk maakt. Ook zijn hiervoor diverse utilities te verkrijgen. Ook voor gebruik op de PC.

Referentie: Edpacs april 1987.

Wat gebeurt er tijdens de nachtdienst?

In Edpacs werden een aantal praktijksituaties van de bezigheden van medewerkers tijdens de nachtdienst genoemd. Enkele hiervan nemen wij hier over.

- Een operator van het California Department of Justice gaf gegevens uit strafregisters en autoregistraties door aan drugsdealers die deze informatie gebruikten voor het screenen van potentiële cliënten.
- Een verveelde operator doodde de tijd door in twee overheids-databases in te breken en een programma te schrijven dat de gegevens hieruit combineerde.
- De chef van de nachtploeg van een verzekeringsbedrijf met het grootste gedeelte van zijn staf gebruikte de computer voor de administratie van hun gokbedrijf.
- Twee programmeurs van een ziekenhuis die 's avonds werkten selecteerden uit een database met informatie over patiënten die een abortus hadden gehad, de alleenstaande vrouwen van bepaalde leeftijd, gewicht en ras. Deze werden vervolgens telefonisch benaderd voor afspraakjes.

Commentaar

Maatregelen om dergelijke praktijken tegen te gaan bestaan uit het:
- incidenteel bezoeken van het computercentrum tijdens de nachtdienst;
- controleren en aftekenen van de log (natuurlijk moeten er ook maatregelen zijn getroffen om te waarborgen dat de log compleet is).

Referentie: Edpacs maart 1987

Controle

Fouten in onderhoudsprocedure bij Australische Bank

Bij het uitvoeren van onderhoud aan het besturingssysteem deden zich problemen voor. Het elektronisch betalingsverkeersysteem dat op de desbetreffende mainframe draaide werd hierdoor zodanig beïnvloed, dat klanten met behulp van betaalautomaten meer dan de daglimiet van 200 Australische dollars konden opnemen. Deze mogelijkheid stond zels open voor mensen met onvoldoende saldo.

De problemen, die zich met name voordeden tijdens perioden met hoge transactievolume, noodzaakte de bank alle betaalautomaten en POS-systemen voor bijna een dag te sluiten. In die tijd is de voorgaande versie van het besturingssysteem weer operationeel gemaakt.

De bank beweert, dat geen directe financiële schade is geleden.

Commentaar

Dit is na de problemen bij een Amerikaanse bank als gevolg van hogere transactievolumes dan verwacht de tweede keer dat een soortgelijke situatie zich voordoet. In het eerste geval betrof het duidelijk het applicatiesysteem. Tevens werd in dat geval wel een directe schade geleden, namelijk intrestverlies.

Ter voorkoming van dergelijke problemen is het vooraf testen van een systeem met een beperkt aantal transacties niet toereikend. Het vereist een tweede systeem, dat de nodige transacties genereert en de afhandeling daarvan controleert. Een geweldige investering in software. In een dergelijk geval zullen ook grote investeringen in de hardware moeten worden gedaan, omdat bij grote gesimuleerde transactievolumes ook grote bestanden en een zekere netwerkinfrastructuur horen. Deze hardware-investeringen hebben echter ook een alternatieve aanwending in de vorm van back-up-voorziening.

Een risico-analyse zal moeten uitwijzen of dergelijke investeringen gerechtvaardigd zijn.

Referentie: EFTPOS International Bulletin June 1987.

Administratief systeem met bijzondere gebruiksmogelijkheid

In het Verenigd Koninkrijk zijn een certified accountant en een systeemanalist veroordeeld voor het maken en verkopen van een inventaris- en boekhoudpakket met een bijzondere extra. Het pakket,"Movieman" voor videoverhuurbedrijven, bevatte een geheime routine die gebruikt kon worden om een gedeelte van de dagomzet te verbergen. De gebruiker kon zelf het percentage van de gewenste omzetvermindering bepalen.

Niet alle gebruikers waren op de hoogte gesteld van deze geheime routine. Het werd, zo nodig, alleen gebruikt om een potentiële koper over de streep te halen.

Door middel van een wachtwoord konden de gebruikers een overzicht krijgen van hun echte of verminderde omzet.
Zowel de omzet- als inkomstenbelasting waren aanzienlijk gedupeerd. Het bestaan van de routine kwam aan het licht door een anonieme tip. Het duurde twee weken voordat deskundigen van de belastingdienst de desbetreffende code hadden geïdentificeerd.

Commentaar

Hoe kan een accountant of belastinginspecteur dergelijke codes vermoeden? Het is te moeilijk de volledigheid van de opbrengsten van een videoverhuurwinkel te bepalen. Naast het feit dat de omvang van het bedrijf geen functiescheiding toelaat zijn nog een aantal redenen aan te wijzen:

- Het aantal keren dat een tape gedraaid kan worden voordat deze als onverhuurbaar kan worden aangemerkt fluctueert sterk en kan zelfs in hoge mate worden beïnvloed. (Welke kwaliteit is nog acceptabel?)
- Er zitten grote verschillen in de omloopsnelheid van de tapes.
- Het is moeilijk te bepalen hoe de goedlopers en slechtlopers over het assortiment zijn verdeeld.
- Er kunnen zelf gemaakte kopieën in omloop zijn. Ook kan de leeftijd van een originele tape worden "verlengd" door middel van een kopie.

De enige controlemogelijkheid bestaat nog uit inventarisatie en een vergelijking met de aanschaflijst en de verhuurlijst. Indien de aanschaflijst ook door hetzelfde admnistratiesysteem wordt bijgewerkt, moet deze van een eerdere datum zijn dan de verhuurlijst. Hierdoor kan worden voorkomen, dat tapes die op het afdrukmoment tot de niet geregistreerde omzet behoren, op geen van beide lijsten worden vermeld.

Daarnaast is een goede speurdersneus in deze gevallen een onontbeerlijke controletechniek.

Referentie: Edpacs, April 1987.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services