KMG Klynveld Kraayenhof & Co.
Automatisering & Controle-groep

COMPACT 8/43

Nummer 36 11e jaargang herfst 1984

COMPACT

COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE

nummer 36 11e jaargang herfst 1984

Herfst 1984

VAN DE REDACTIE

Het is voor de redactie soms een hachelijke zaak om tot een kernachtige typering van het voorliggende Compactnummer te komen.

Voor dit herfstnummer 1984 is het

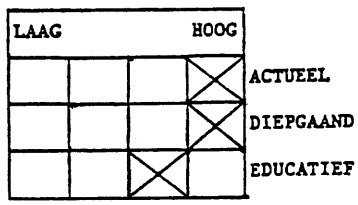
"Na het onderkennen van Risico's komen tot Beveiligingsbeleid"

"Via een theoretisch model naar praktische toepassingen bij S/38 en bij Netwerken".

Na de boekaankondiging onder de kop Actualiteit volgen een drietal hoofdartikelen over bovengenoemd thema.

"Data Base & Accountant", nieuw uitgegeven.

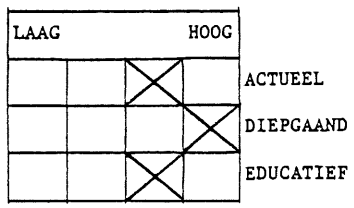
A.H.C. Koedijk et al.
Volledig herschreven druk van dit boek.
Boekaankondiging door de redacteur.



Het boek geëvalueerd

Security management: from the past to the future

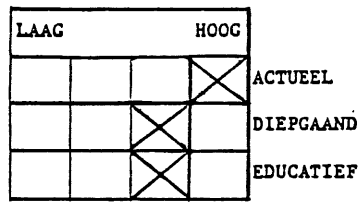
door drs. H.C. Kocks



Een gezond risicobeleid is voorwaarde voor het adequaat functioneren van de onderneming. Het nemen van risico's is immers inherent aan het ondernemerschap. Om de omvang van mogelijk nadelige gevolgen binnen aanvaardbare grenzen te houden is een beveiligingsplan vereist.
Ook automatisering doet zijn invloed daarop gelden.
Dit artikel wil een aanzet zijn voor bezinning.

"De organisatie rond een Systeem/38"

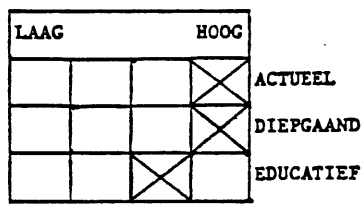
door H.J. Lijnes, organisatie-adviseur.



Bij de opzet van een organisatie rondom een Systeem/38 dient men een verdeling van taken en verantwoordelijkheden toe te passen die een goede waarborg bieden voor de beheersing en controle van de automatiseringsactiviteiten. Het is niet noodzakelijk dat dit een excessieve groei betekent van het aantal medewerkers van de automatiseringsafdeling, zoals meestal het geval is in grote automatiseringsorganisaties. Dit artikel tracht de weg daartoe aan te geven en doet suggesties omtrent de wijze waarop men tot een betere benutting kan komen van de mogelijkheden van een Systeem/38.

"Beveiligingsaspecten in netwerken:
Theorie en Praktijk"

door ing. C.J.M. Gielen en H. Weerd



Het artikel bestaat uit twee delen:
a. de uiteenzetting van een theoretisch model voor beveiliging;
b. het S.W.I.F.T.-netwerk.
   Hierbij is ingegaan op het doel en functies van S.W.I.F.T., de verhouding van het S.W.I.F.T.-netwerk tot het OSI-model en de voorzieningen die bij het S.W.I.F.T.-netwerk in de application- en transportlayer zijn getroffen.

Rubrieken

De rubrieken vormen soms en zeker in dit nummer het spiegelbeeld van de hoofdartikelen.
Reden hiervoor kan zijn dat ontwikkelingen op verschillende plaatsen tegelijk ontstaan.
Het is op zichzelf een wonder dat bij vergelijking steeds nieuwe facetten blijken.

Voor opbouwende kritiek is steeds ruimte beschikbaar in ons blad.
U kunt uw commentaar inzenden aan onze secretaris.

Zoals u weet vonden de soldaten van Napoleon een belangrijke steen in Egypte: "de steen van Rosette".
Het vormde de sleutel voor het ontraadselen van het hiërogliefenschrift. Op de steen staat namelijk een en dezelfde tekst in drie talen waarvan er twee bekend waren en het hiërogliefenschrift de andere tekst vormt.

Kortgeleden is gebleken dat vergeten is op de achterzijde te kijken.
Zie hieronder een specimen van de tekst.

SANSKRIT

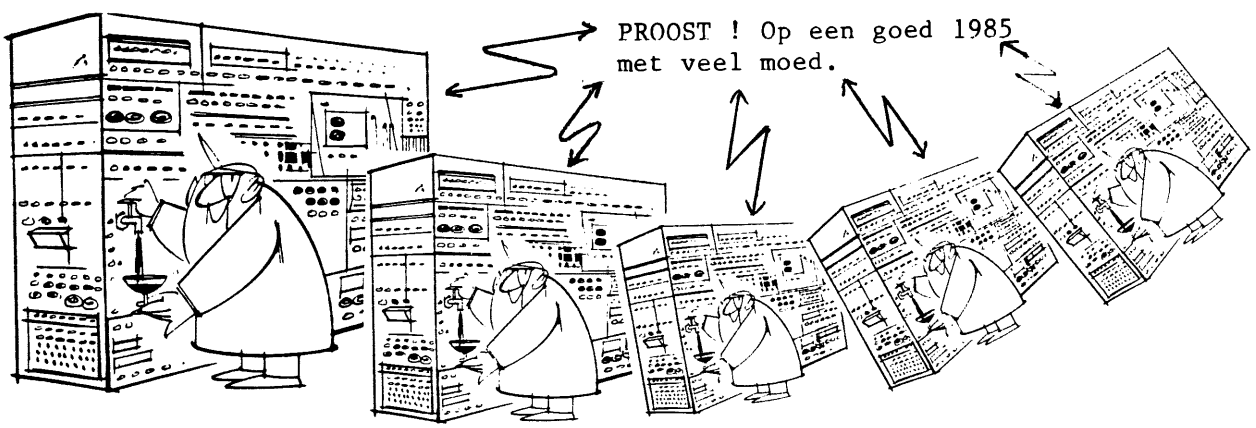
AMHARIC

HIEROGLYPHICS

Hieruit blijkt duidelijk dat in de oudheid de micro-computer ook reeds bekend was.
Waarvan akte. Blijkbaar werd het gebruikt in de buurt van water en vogels.

Tot zover onze Oudheidskundige.

Met bovenstaande zinsnede beëindigen wij als redactie dit herfstnummer 1984. Tot na de feestdagen.



Modern sternetwerk

Herfst 1984

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

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

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

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

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

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

ACTUALITEIT

"DATA BASE & ACCOUNTANT"*, NIEUW UITGEGEVEN

Rond deze tijd, december 1984, verschijnt bij Samsom een volledig herschreven druk van dit bekende boek. Onder redactie van A.H.C. Koedijk is het boek thans geheel samengesteld door medewerkers van de AC-kern van Klynveld Kraayenhof & Co. Overige auteurs zijn:
A. van der Drift, J.E. Huizenga, A. Kamstra en J.L.H. Kooijman; voor Compactlezers alle vijf geen onbekenden.
Het boek is primair bedoeld voor algemene (niet in automatisering gespecialiseerde) accountants, die wel verondersteld worden over basiskennis van automatisering te beschikken. Het is geen handboek voor de praktijk, doch het bedoelt accountants zodanig inzicht te verschaffen, dat zij met praktijksituaties kunnen omgaan.

Hieronder volgt een korte beschrijving van de hoofdstukken.

1. Inleiding

In dit hoofdstuk wordt aangegeven waarom besturingssystemen, waaronder data base management systemen, object van onderzoek kunnen zijn voor accountants. Het motief daartoe wordt gezocht in de "migration of controls" vanuit organisatie en applicatiesystemen naar besturingssystemen.

2. Het beheersen van geavanceerde gegevensverwerking

In dit hoofdstuk wordt een tweetal functionele modellen beschreven:
a. de "systeemfuncties" in een data base-omgeving (conceptueel, intern en extern schema);
b. de organisatorische functies (gebruikers, gegevensbeheer, data base administration, systeembeheer, systeemontwikkeling, verwerking en security).

De relaties vanuit het gezichtspunt van beheersbaarheid tussen de twee soorten functies worden aangegeven.
Het belang van de modellen moet vooral worden gezocht in:
a. het dienen als referentiekader bij de later te behandelen "techniek". Als zodanig vormen de modellen de "rode draad" van het boek;
b. het op een conceptuele manier uiteen zetten hoe een data base-omgeving eruit zou moeten zien, waardoor ze als toetsingsmodel kan worden gebruikt bij het beoordelen van een concrete situatie.

3. Opslagstructuren van gegevens

De technische verschijningsvormen van data bases worden behandeld. Hierbij wordt onderscheid gemaakt tussen twee hoofdgroepen: pointer-systemen (in het bijzonder netwerksystemen) en relationele systemen. De behandeling geschiedt getrapt:

3.1 Algemene inleiding tot data bases (definitie; motivatie: verminderen van redundantie - en daarmee inconsistentie - en beschikbaar stellen voor gemeenschappelijk gebruik).
Algemene inleiding tot pointer systemen (3.1.4) en tot relationele systemen (3.1.5).

3.2/3 Meer diepgaande behandeling van de twee soorten systemen.

De technische diepgang is zoveel mogelijk beperkt gehouden en gericht op: wat moet bekend zijn om de te beschrijven mogelijke interne controlemaatregelen te kunnen begrijpen. Allerlei technische details, bijvoorbeeld op het gebied van performance, zijn weggelaten.

Het hoofdstuk besluit met een afzonderlijke paragraaf Interne Controle (3.5), waarin de mogelijkheden op een rijtje worden gezet. Aan het eind worden de relaties met de modellen uit hoofdstuk 2 gelegd.

4. On-line verwerking

De behandeling van dit onderwerp in een boek over data bases is bijna onontkoombaar, niet in de laatste plaats omdat een aantal relevante "technische bouwstenen" van het externe schema uit het beheersbaarheidsmodel in de tele-processing software kunnen worden aangetroffen. Ook dit hoofdstuk besluit met een paragraaf Interne Controle (4.3).

5. Data dictionary directory systemen

Nadat het toenemend belang ervan (gegevensbeheer!) reeds in hoofdstuk 2 is geïntroduceerd, worden hier de DDD-systemen met hun mogelijkheden in kort bestek behandeld. Ook voor accountants, zoals in hoofdstuk 6 verder zal blijken, zijn deze systemen van groot belang.

In de inleiding wordt het verschil tussen dictionary functie en directory functie uiteengezet.
In paragraaf 5.2 worden de relaties met verschillende organisatorische functies uit hoofdstuk 2 gelegd.
In paragraaf 5.3 wordt ingegaan op de relatie tussen informatie in de dictionary, in de directory en de besturing van computerprocessen.

6. Accountantscontrole

Het hoofdstuk gaat uit van een keuzemogelijkheid tussen systeemgericht dan wel gegevensgericht controleren. Hoe tot deze keuze wordt gekomen blijft buiten beschouwing. Alleen de mogelijkheden bij elk van beide opties zijn toegelicht.
De behandeling van "CAAT's" (bestandsonderzoeken) is kort.
Het accent ligt in dit hoofdstuk op de systeemgerichte controle. Hier ligt dan ook een verschil met de vorige versie van Data base & Accountant.

7. Distributed data base

Belangrijke elementen in dit hoofdstuk zijn:
- soorten van distributie (7.1);
- overwegingen die hierbij een rol spelen (7.2).

Tot besluit worden in par. 7.3 de controle-aspecten belicht.

8. Data base machines

Dit hoofdstuk heeft uitsluitend een informatief karakter. Het pretendeert niet meer dan de lezer te vertellen wat een dbm is en waarom een dbm nodig is.

9. Report generatoren, query-talen, vierde generatietalen

Hoewel bedoelde programma-ontwikkelingshulpmiddelen ook voor de accountant in het kader van bestandsonderzoeken hun nut kunnen hebben (beperkte "audit-packages"), is dit niet de invalshoek van het hoofdstuk.
Het hoofdstuk gaat in op de consequenties van deze hulpmiddelen op de beheersbaarheid van de geautomatiseerde gegevensverwerking, in het bijzonder de consequenties van de verhoogde service aan en de grotere mogelijkheden voor gebruikers.
Met andere woorden, de nadruk ligt op de interne controle-aspecten.

10. Microcomputer, data base en accountant

Dit hoofdstuk heeft een tweeledig karakter. Paragraaf 10.2 sluit aan bij de voorgaande hoofdstukken en behandelt de mogelijke vormen van microcomputergebruik alsmede de invloed hiervan op de beheersbaarheid. Paragraaf 10.1 staat meer op zichzelf en gaat in op het gebruik van de microcomputer in de accountantscontrole.

---

* Data base & Accountant/A.H.C. Koedijk (red.); m.m.v. A. van der Drift ... (et al.); Samsom Alphen aan den Rijn, 1984; ISBN 90 14 034385, ca. 170 blz., ca. f 55,--.

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

SECURITY MANAGEMENT: FROM THE PAST TO THE FUTURE

door drs. H.C. Kocks

INTRODUCTION

Along with the development of electronic information processing (1), the 'security' aspects of that processing have also received attention. But taking the rapid development of information processing into account it is doubtful whether this attention to security has kept pace with the EDP-development.
Because of this doubt it seems desirable to look into the following questions:

- What is the state-of-the-art of EIP and of the related security aspects? Has the objective of the experts been achieved, or are the results disappointing?

- What will the future be? Should we continue to follow the road we have taken so far or is it necessary to adopt new methods?

The first part of this paper, which aims at dealing with these questions, contains an analysis of the past and arrives at a conclusion. The second part gives an approach to Security Management. This approach is submitted for critical evaluation and comments.

The paper comprises the following sections

(1) In this paper the abbreviation EIP will be used for Electronic Information Processing.
(2) Deze bijdrage is eerder behandeld op de IFIP-TC 11 Working Conference "Informatics security management" 24-25 May 1984.

1.0 SECURITY MANAGEMENT: A THEORETICAL MODEL

In the introduction reference was made to 'EIP and security', but nowadays the term 'security management' is increasingly used. This means that security is considered in a much broader framework, but it also emphasizes that the attention to security as a consequence of EIP is in the first place a concern of management.
Further, it would seem that the term security management speaks for itself, but the truth is to the contrary. In professional literature various - and also inconsistent - definitions are used. In order to avoid further misunderstanding, a schematic description is given in figure 1.

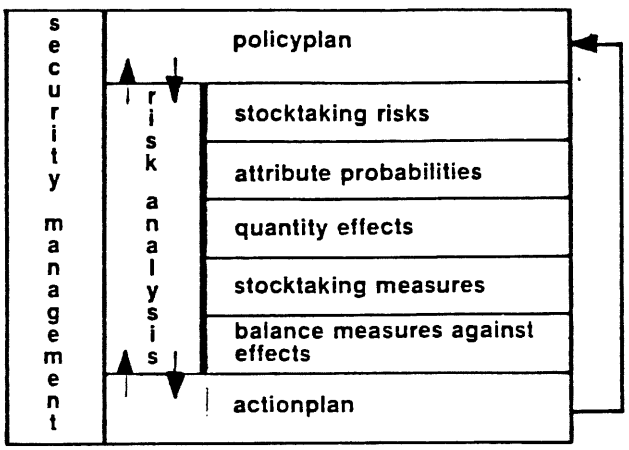


Figure 1: Security Management

This figure gives a theoretical model, in which three main activities are laid down:
* defining and drawing up a policy plan;
* making a risk analysis;
* defining and drawing up an action plan.

The first of these main activities, defining and drawing up a policy plan, is a task of management in an organization.
Apart from pronouncing the necessity to undertake action in order to recognize dangers and to react appropriately to them, the policy plan should also contain starting points, norms and boundaries as guidelines for making a risk analysis.
The activities for making a risk analysis consist of drawing up a list of all possible risks, probable events to which risks might be linked and subsequently quantifying the consequences of these hazards as well as possible.
Further, it must be laid down which measures (preventive, damage reducing and damage corrective) must or can be taken to reduce the risks and their consequences to an acceptable level. Finally the costs of the measures must be determined.
This information should be presented to management in the form of a draft security plan.

Management checks the draft security plan and compares it with the guidelines given before. Upon completion management will decide which choices are made from the alternative measures provided in the draft security plan. Then instruction will be given for the third main activity: defining and drawing up an action plan. This activity closes the circle.
Permanent adjustment on the basis of the results of the periodically undertaken risk analysis - as foreseen in the action plan - will contribute to a well-balanced security policy.

2.0 THEORY VERSUS PRACTICE

What happens more often in reality is that the theory is not in concurrence with practice. That is the case here as well. At first sight it seems simple to fill in the theoretical model, but in practice it is not simple at all. In the following some reasons will be given for the (continuing) gap between theory and practice.

2.1 Responsibility of management

It should be emphasized once again that management has the responsibility for an adequate security policy. However, neither the 'theoreticians' nor the 'practitioners' have ever furnished management with the tools to develop such a policy. Policy plans aimed at security related to the application of EIP in general do not exist in practice. On the one hand - as said before - this must be ascribed to the lack of adequate tools, and on the other hand it is due to the nature of the phenomenon itself.
For management EIP is usually not a primary, but more often a secondary area of attention. It is no more than an instrument to achieve the primary objectives of the organization. These objectives require management's full attention and consequently owing to the increasing importance of EIP, to which inadequate attention is paid, it may become a threat to the realization of the main objectives of the organization. Very often management is insufficiently familiar with the phenomenon of EIP. Due to the lack of a sound policy plan, the strategy of management with regard to EIP and security is unknown to workers in the organization. Furthermore, the guidelines, norms and boundaries for adequate security of the organization are usually lacking.
So it is doubtful whether investments in this respect will produce the proper results.
If no norms are provided, the main activities two and three - risk analysis and action plan - will in most cases lead to wrong conclusions and recommendations.

2.2 Risk analysis

Risk analysis is the main activity which follows upon completion of the policy plan and in literature it is often referred to as the backbone of security management.
Yet it should be stressed that risk analysis is only a technique for making an inventory of risks and weighing cash of them.

The choice of starting points and the determination of probabilities is a matter of subjective consideration, though it does determine the recommendations finally given to improve the situation.
Hereafter the following aspects of risk analysis will be discussed:
a. the methods;
b. the performers.

a. The methods
The first step in the process of risk analysis - the inventory of risks - is extremely important. This is done in the first place by determining the 'completeness' of the risks. It is therefore interesting to see which methods can be applied. In professional literature three are offered.

I Assets approach.
In applying this method an inventory of assets - in the broadest sense - is made. Upon completion of this, each asset is considered in the light of existing risks.
The entire area may be divided into sub-areas in order to further simplicity and increase transparency of the activities.

II Threats approach.
For a well-defined entity (situation/department) an indication is given regarding the possible dangers. In order to determine the possible damage (loss), for each hazard the assets, which represent a risk, are aggregated. This approach, via the 'backdoor', seems opposite to the 'front-entrance' assets approach. It looks, however, that the results will be similar.

III Systems approach.
This method approaches the dangers and risks from a limited number of (so not all) operational applications. Interested parties determine which applications are relevant in their functions and which are the risks and dangers inherent to those applications. This approach, because of its limitations, cannot be considered as an integral risk analysis method to prepare or adjust a security plan.

Whether the results of an assets approach and a threats approach indeed are similar will largely depend upon the degree of certainty with regard to the completeness of the basic material.
With the assets approach concrete monetary means, goods and materials form the starting point. With the threats approach on the other hand 'possible events' form the basis. The completeness of the assets can indeed be determined, but with regard to 'possible events' this is much more difficult. In this respect it is more likely to be incomplete than complete.

The choice of method to be applied requires a certain amount of expertise, and furthermore, the results may differ in each case.

b. The performers

The performers of risk analysis can be divided into two categories. On the one hand there are the 'experts' who are involved full-time in security activities and on the other hand there are the 'amateurs', who are professionally involved in EIP and - convinced of the usefulness of security - in that capacity are charged to deal with it. The category of experts is usually found among external business consultants.

'Experts' often apply methods developed by themselves, which they for reasons of competition keep secret. Experts are called in at the request of management to make a risk analysis. This job completed, management will receive a usually confidential report and an action plan. The recommendations, however, cannot be confidential. This way of working implies that the execution of the action plan is not a simple job, because so far all activities have been carried out at management level, while the workers in the organization have not been involved. Yet they are supposed to accept security measures as soon as the action plan is put into practice. It is obvious that such a procedure is not conducive to the object of making the entire organization 'security minded'. And so:
- security measures will be accepted only with great difficulty;
- the effectiveness of the measures will not be very great, because the measures and procedures are bound to be neglected.

The category of 'amateurs' often uses the commercially available methods, put out in the form of checklists. These methods pretend that risk analysis is such a simple job that it can be done after following a course of only a few days. How to use the checklists is the content of the learning exercise.
In practice personnel of operational level will be charged with risk analysis, but it is doubtful whether recommendations based upon such a risk analysis can produce a balanced system of security measures.

In general it may be said that the undertaking of a risk analysis by either category has certain drawbacks.

- There is the possibility of drawing up a 'static' risk analysis. A snapshot is made of a real situation and on the basis of this, recommendations are formulated for management. Nothing, however, is more dynamic than an EIP-using organization. There are continuous changes and these entail that the organization must be supervised and adapted permanently.
  Periodical risk analysis, however, should not be recommended either, because changes might take place during the intervals and consequently the level of security might drop below the norm.
- It is doubtful whether on the basis of a 'static' risk analysis correct conclusions can be drawn as a basis for recommendations (and possible investments).

2.3 Action plan

The action plan is based on the results of the risk analysis with an aim at improving the situation.
The following problems often present themselves in practice.

- The workers in the organization do not accept the measures because they have not been involved in security management. The measures are imposed and consequently the effectiveness might be questionable.
  Security fully depends on acceptance by all sections of the organization. Therefore in practice much more attention should be paid to the 'why' and the necessity for security measures. Well-founded arguments - not only the argument that the measure has to do with EIP - will make the organization security minded. Education and training of personnel is therefore necessary.
- The existing and proposed measures do not produce a 'balanced situation'. Emphasis is put on the protection of 'data' while measures are usually taken in the physical area. This is understandable because this area is familiar and also because the risks are often found in this area (e.g. fire, etc.).
  Balance in the dose of measures is a requirement in the achievement of a balanced security system. ('The chain is only as strong as its weakest link'.)
- As already said, the action plan is based upon a 'static' risk analysis. The real danger exists in management's assuming that after the execution of the action plan the security is satisfactory according to the defined norm, while EIP in the meantime has changed. The reality then can be:
  . that incorrect investments have been made;
  . that the security does not comply with the required norm, taking the situation into consideration;
  . that management is not aware of the existing risks.

3.0 RESULTS

The conclusion is that there is no balance between approach and measures in security management. In the period behind us the emphasis was laid on responsibility of management, vague risks and parts of the security area, without a possibility on providing:
- training and education facilities for responsible management (what risk is connected with EIP);
- training and education facilities for security specialists;
- an adequate set of tools with:
  . approaches;
  . methods;
  . techniques.

Another aspect is that until now - in the frame of security management - attention has merely been paid to the EIP function. The relation between the functions of the organization and the importance of EIP for the continuity of these functions is often neglected.
Until now too much priority has been given to EIP instead of to the safeguarding of continuity of the vital functions of the organization. These functions have often been neglected altogether.

In short, the pioneering phase has not paid enough attention to:
- the increasing importance of EIP for the continuity of the organization;
- the dynamic aspect of security following the rapid changes in EIP;
- the impact of security measures within the organization, whereby the degree of acceptance has not kept pace with that of security;
- an 'overall' approach.

How to alter this course will be discussed in the second part of this paper.

4.0 SECURITY POLICY

As a critical comment on the present situation it was mentioned that security in practice has been oriented towards sub-areas. Physical security was the one which received most attention.
The set of areas of EIP for which security measures have to be taken, can be divided into connected subsets each of them with its own characteristics (figure 2). In security management the whole area must be covered. The measures taken will have to be balanced as much as possible, for each subset as well as for the whole.

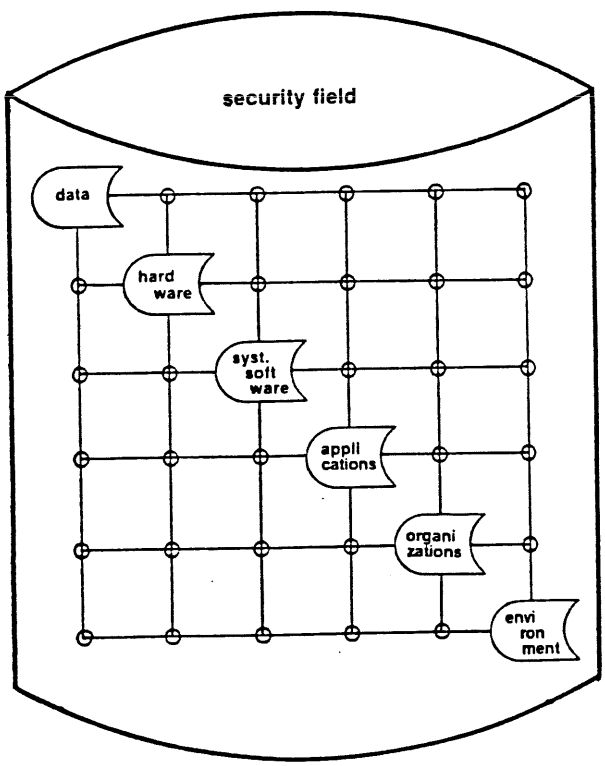


Figure 2: Security Field

The names of the subsets are self-explanatory, each one consists of a number of components. The subset 'data' for example, may comprise the following components (sub-subsets)(figure 3).

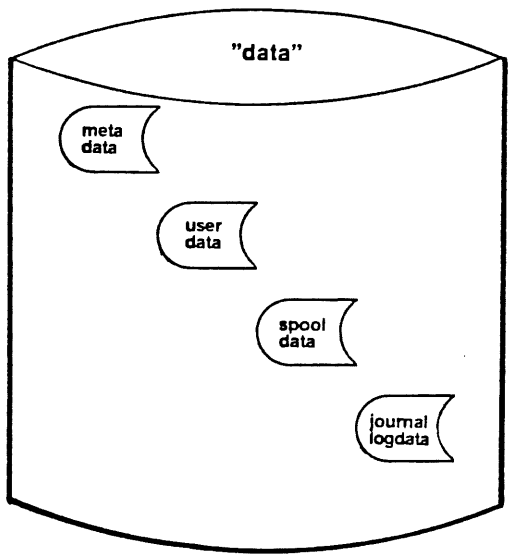


Figure 3: Subset 'data'

5.0 THE FUNCTIONAL APPROACH

The first step in the theoretical model of Security Management is called 'development of a policy plan'. The necessity of guidelines and norms has been emphasized. Because such a policy plan often does not exist in practice, efforts are made to determine the norms in a practical manner.
Determination of norms and related activities as discussed hereafter are directed towards the continuity requirements of organizations.
In an EIP environment the norms are determined by the maximum acceptable delay in an essential business function as a consequence of a failure of the EIP function.
The continuity of the functions of an organization is the main object and for that reason one may call it the functional approach.

Once the norms are determined, the actual situation will be considered thoroughly (the risk analysis). The objective of this is to check whether the actual situation is in accordance with the norms set by management. The ways and means to be applied will be discussed later.

Upon completion of the risk analysis a balanced action plan which can be composed of two parts will be set up:
- actions to be taken immediately, due to the fact that the actual situation deviates from the norms;
- an emergency plan.

Up till now only the 'static' situation has been discussed. In order to change 'static' into 'dynamic' it is necessary to introduce the security function. This function is responsible for the permanent monitoring of the balance between norms and reality. Later in this paper further consideration will be given to this point.

In the following chart the functional approach, which will be elaborated in detail later, is given (figure 4).

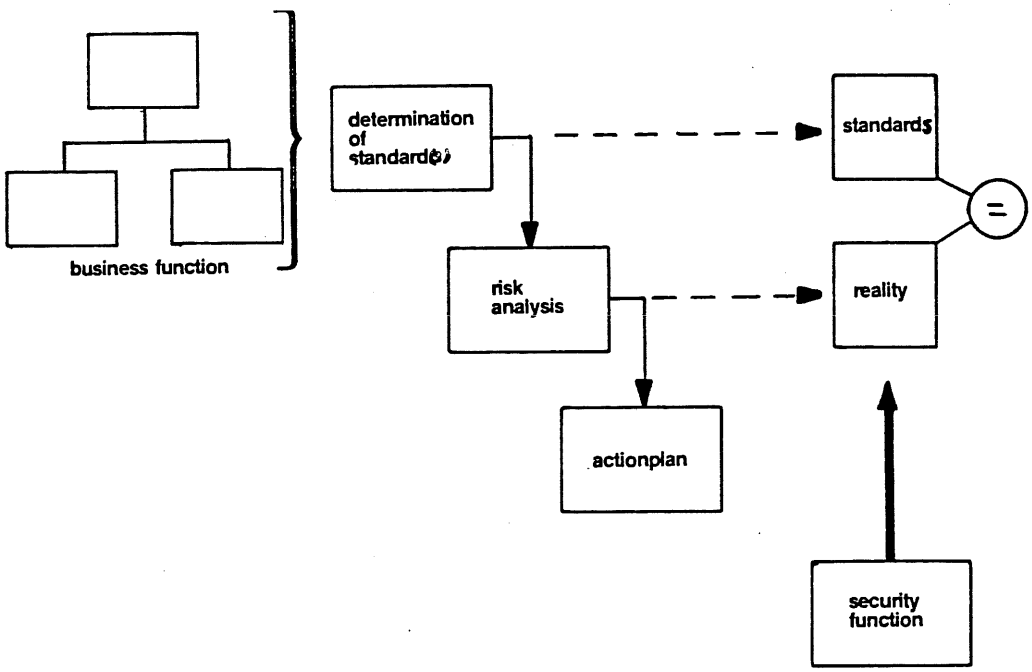


Figure 4: Functional Approach

6.0 DETERMINATION OF THE STANDARDS

For its continuity not every activity of an organization is equally dependent upon the application of EIP. For one activity a continuous availability may be required, whilst for another activity EIP will hardly be needed.

The starting point in this approach is that the norms are determined by the main activities of the organization which are essential for its continuity and which are mostly dependent on EIP. This refers to the level of security of EIP which is minimally required in order to avoid the vital activities running danger and thus safeguarding the continuity of the organization. This means that the drop-out time of the vital functions of the organization may not exceed a defined time. Thus the norm consists of a time factor which may not be exceeded. The determination of the time factor is explained in figure 5.

Explanation
Determine for the organization concerned the most important function which is dependent on EIP, and make an inventory of what 'output' is provided by means of EIP as 'input' for the vital function of the organization. This inventory should be based on normal conditions. 'Output' should comprise not only information on paper, but also on visual displays etc. This being done also the frequency of information output supply must be defined (eliminating irrelevant output).
(See next page.)

By this a table can be made with frequency categories, e.g.:
P = permanent
1h = every hour
4h = every 4 hours
D = daily
W = weekly
M = monthly
However, this table (figure 5) should not yet be applied because further consideration has to be given as to delay in the outputsupply is acceptable.

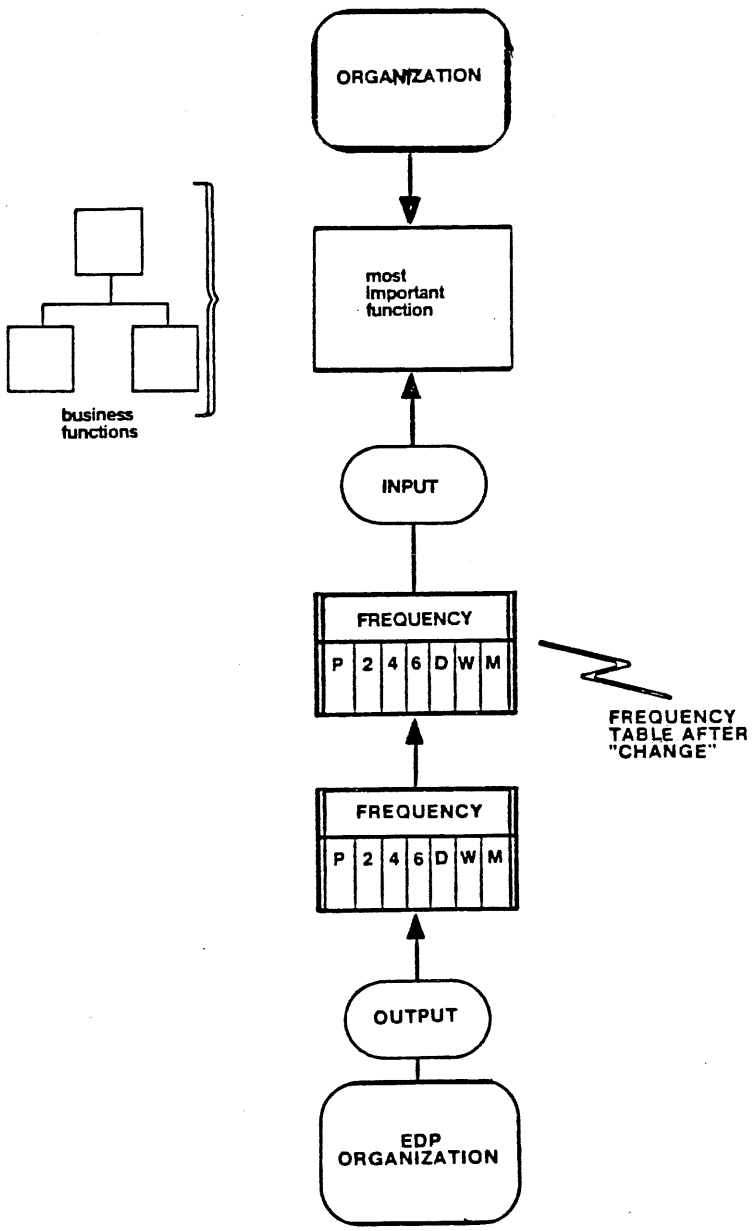


Figure 5: Determination of the time factor

An example in illustration
Assume that the output is being provided daily, but with the restricting requirement that it must always be available at 4.00 p.m. It is then necessary to change from frequency category D to P; 2 or 4h is consequently required. The result of this exercise is a corrected frequency table.

Starting from this corrected frequency table the normal execution time of the vital activity should be set up. This being done it will be necessary to determine per output frequency what the consequences are of a delay in the output supply by the EIP department and at what costs/loss of income.
The maximum delay in output supply by the EIP department - by which the vital activity is not hampered - is the acceptable delay time, "the norm". The security of the EIP should thus be such that the drop-out time will not be exceeded.

The norm can only be determined by intensive co-operation with the responsible staff of the organization itself. Furthermore, it produces at the same time appropriate information for management as to what losses will be caused by exceeding the drop-out time.
Through this exercise the user's organization as well as management will become aware of the importance of EIP which in turn will result in a more positive attitude towards the security measures to be taken.

7.0 RISK ANALYSIS

This activity can start simultaneously with the previous one determination of the norms to be applied because a risk analysis exercise should start with an inventory of the actual situation. This inventory should be carried out according to the assets method.
The risk analysis hereafter described consists of the following steps:
- availability (7.1);
- the 'feeding' problem (7.2);
- software configuration (7.3);
- hardware configuration (7.4);
- automation plan (7.5).

7.1 Availability

The aim of this step is to determine:
- whether 'assets' are available according to the norms, in case of emergency, when breakdowns/calamities and/or loss of assets occur;
- to what threats are the assets exposed;
- which measures have been taken;
- which risks exist and which financial consequences are involved.

Figure 6 shows the way in which the objectives can be reached.

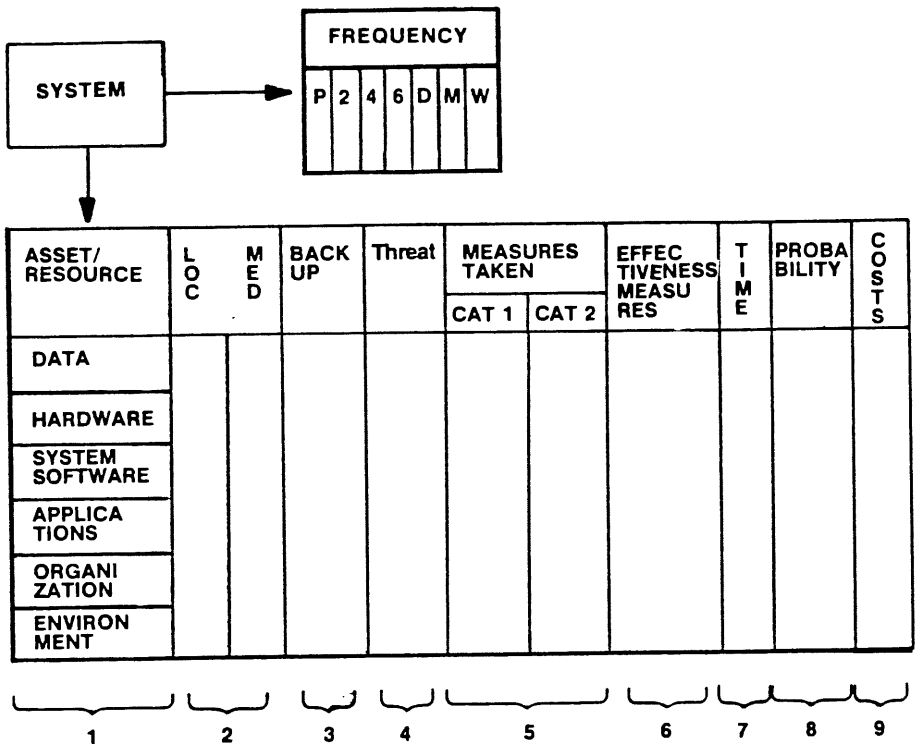


Figure 6: Determination of availability

Explanation

1. The asset resource
   The output supplied to vital firm or company activities is the result of one or more applications (systems). These applications can only 'work' safely by the grace of 'assets'.
   In order to obtain an overall view of the risks all assets used for producing the output have to be itemized. The subsets are indicated: data, hardware, etc.

2. Location/medium (Loc/Med)
   Indication of where the 'assets' are situated (location) and if necessary on what kind of medium the assets are recorded (fixed and/or removable disk).

3. Back up
   Indicate by means of an asterisk (*) in this column if it is a 'back up' of an asset. (This indicates also whether there is a balance between the 'back up' measures.)

4. Threat
   Decide by asset to which threats they are exposed.

5. Measures taken
List the measures already taken to limit the risks. These 'measures' can be split into two categories. Category 1 comprises those which may be ranked as assets themselves and are thus also exposed to risks, which risks have to be limited as well. All other measures fall under category 2.
Two examples in illustration
Category 1: The fire risk has been reduced by the installation of a firedetector and -extinguisher (measure). The installation itself is exposed to risks as well: what measures have been taken to reduce these?
Category 2: A procedure has been developed whereby daily at 18.00 hrs back up copies of all the files have to be brought to a back up safe.

6. Effectiveness measures
We have to determine whether the measures taken are really effective. The existence of a procedure is not sufficient. Its effectiveness has to be checked as well.

7. Time
Here it has to be indicated how long it takes - in case of loss - to be operational again. From this column we can read whether the norm-time has been exceeded. The availability of the assets does not say anything about them being operational or not.

8. Probability
Indicate what the probability of a risk is. Mathematical methods and techniques can be used to this end. However, the so-called 'Fingerspitzen-gefühl' (intuition) together with some expertise appeal much more to the author. Each situation is different.

9. Costs
The costs entailed by the loss of assets have to be calculated.
The above-mentioned practice leads to the following results:
- Insight in the risks which are still being run, despite the measures taken.
- It becomes clear for which subsets measures have been taken and on which subsets the emphasis lies; the measures within and between the subsets have to be in balance.
- The time is indicated within which assets - in case of loss - will be available again (not operational yet).
- Insight into the costs incurred through loss of assets.

The above-mentioned picture may already lead to an intermediate report to management, because the conclusion may be that improvement of the situation is absolutely necessary.

7.2 The 'feeding' problem

The aim of this step is to determine whether the data file, from which the vital function of the enterprise obtains its 'output', is brought up-to-date ('feeding') so that there is no the danger of going beyond the norm (time limit).
A function will seldom obtain its information from an isolated data file with only one update-frequency. As the latter increases the 'feeding' takes place by means of mutation streams and other files. Therefore it is necessary to check the way in which this works and whether the enterprise's vital function can dispose of the correct information in time.
This can be portrayed schematically as shown in figure 7.

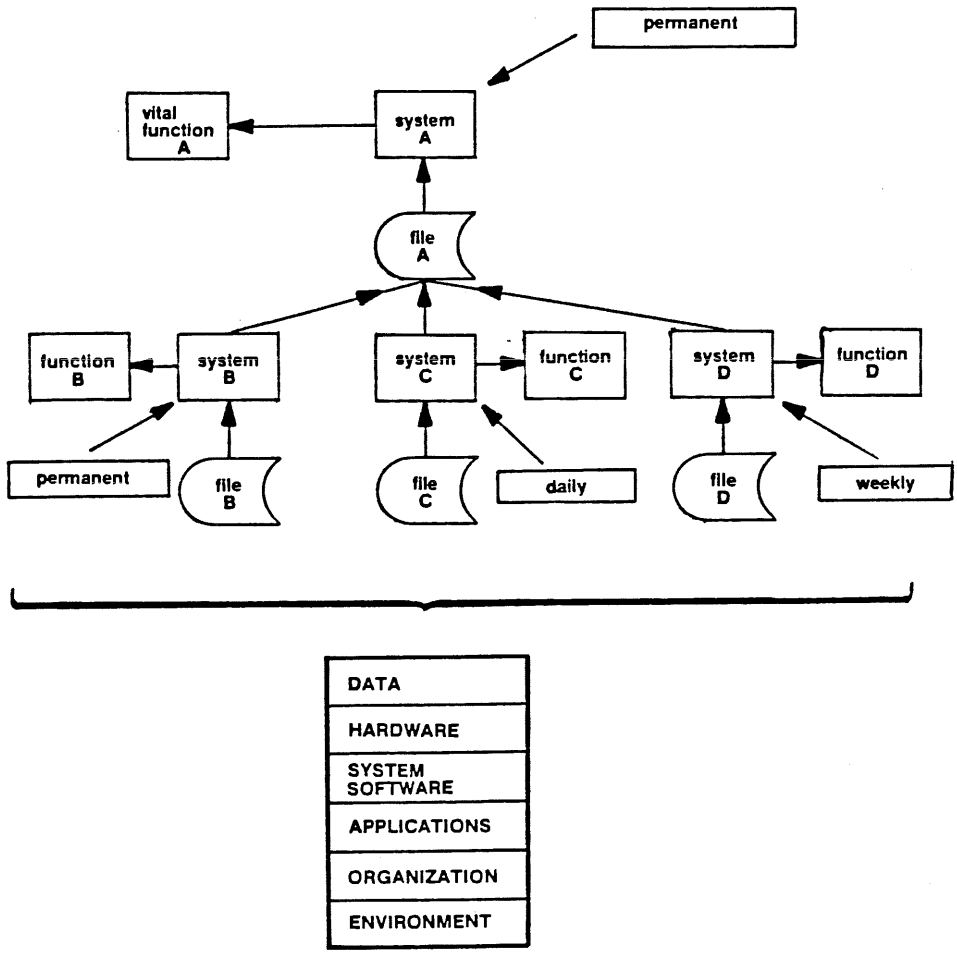


Figure 7: 'Feeding'

Explanation
Check which data files system A makes use of, and determine from which files those belonging to system A are fed. Determine also with which frequency this happens. The scheme file A is fed permanently from B, daily from C and weekly from D. Maybe it is necessary to do the same for B and/or C and/or D. These proceedings have to be carried on until an 'isolated' area has been obtained. In fact, 'system A' will thus be extended to include systems B, C and D. These systems can make use of data, hardware, etc. Therefore it is necessary to install a feedback and to complete step 1 (availability) for this more complicated situation. (It is possible to perform this step first and determine the availability later on.)

This step leads to insight into whether the maximum acceptable delay is exceeded by 'feeding' from other systems. It will become clear to what extent the vital function of the enterprise depends on or is coupled to other functions of the enterprise.

7.3 Software configuration

The foregoing in 7.1 and 7.2 has produced insight in:
- the availability of assets within a certain lapse of time;
- which assets have to be considered.

Yet this is not all. The next step will be to determine the influence which the dropping out of a software component would have on one or more other software components.

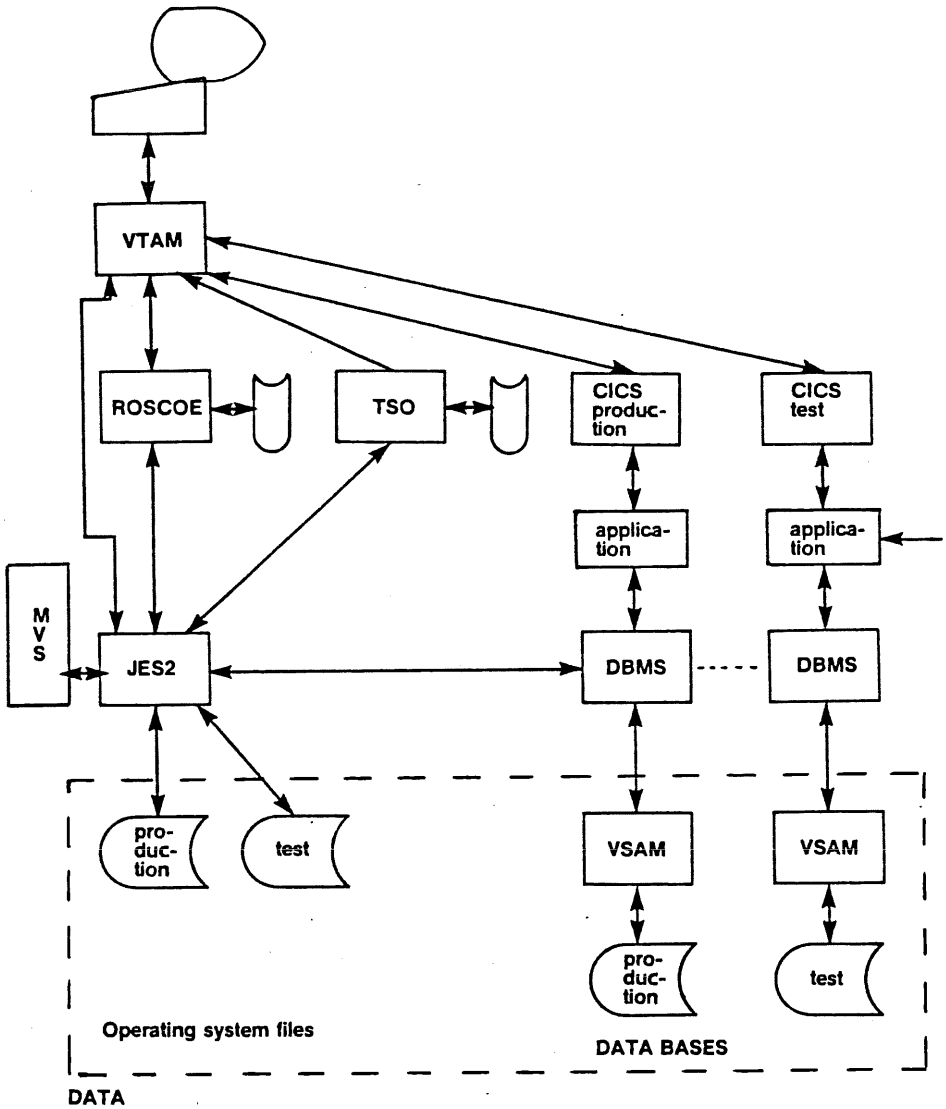


Figure 8: Software Configuration

In other words: if one software component drops out, what is then:
- its influence on another component;
- the time necessary to locate the error;
- the correction time.

These three factors also indicate whether or not the continuity norm has been exceeded.
To this end it is necessary to establish a software scheme (figure 8).

Explanation
All essential software has to be embodied in the scheme after which - progressively - the question has to be asked: if ... then. For each question there has to be an indication of:
- possible influence on other components;
- the time needed for locating errors;
- the correction time.

7.4 Hardware configuration

The same method can be applied here as in 7.3 for software. The influence of the dropping out of a hardware component on the continuity norm has to be determined. Therefore it is necessary to establish a hardware configuration scheme (see figure 9) with the necessary (indicated in 7.2) hardware components. Here too, one has to ask the question:
if ... then.

Hardware has an influence not only on hardware components but sometimes also on software components. Therefore for each question the following points have to be indicated:
- the time necessary to locate an 'error';
- possible influence on other hardware components;
- possible influence on software components;
- correction time: hardware ...
  software ...
  ---
  total ...

The total correction time is not necessarily the aggregate of adding up the hardware and software correction times.

The conclusion which can be drawn from 7.4 is that, despite the availability of the assets, the correction time goes beyond the continuity norm.
In that case additional measures have to be taken or the norm has to be adjusted.

7.5 Automation plan

Before starting the action plan (scheme) it might be advisable to obtain insight into possible 'automation plans' of the enterprise. It does not matter whether these have been laid down in a plan or not. The conclusions drawn from the risk analysis can indicate the direction with regard to which measures should or must be taken.

The plans in the field of data processing may cross this course. (When the software and hardware are changed it might be necessary to repeat steps 3 (7.3) and 4 (7.4). In that event it would be wise to look into the automation plans before taking step 3.)

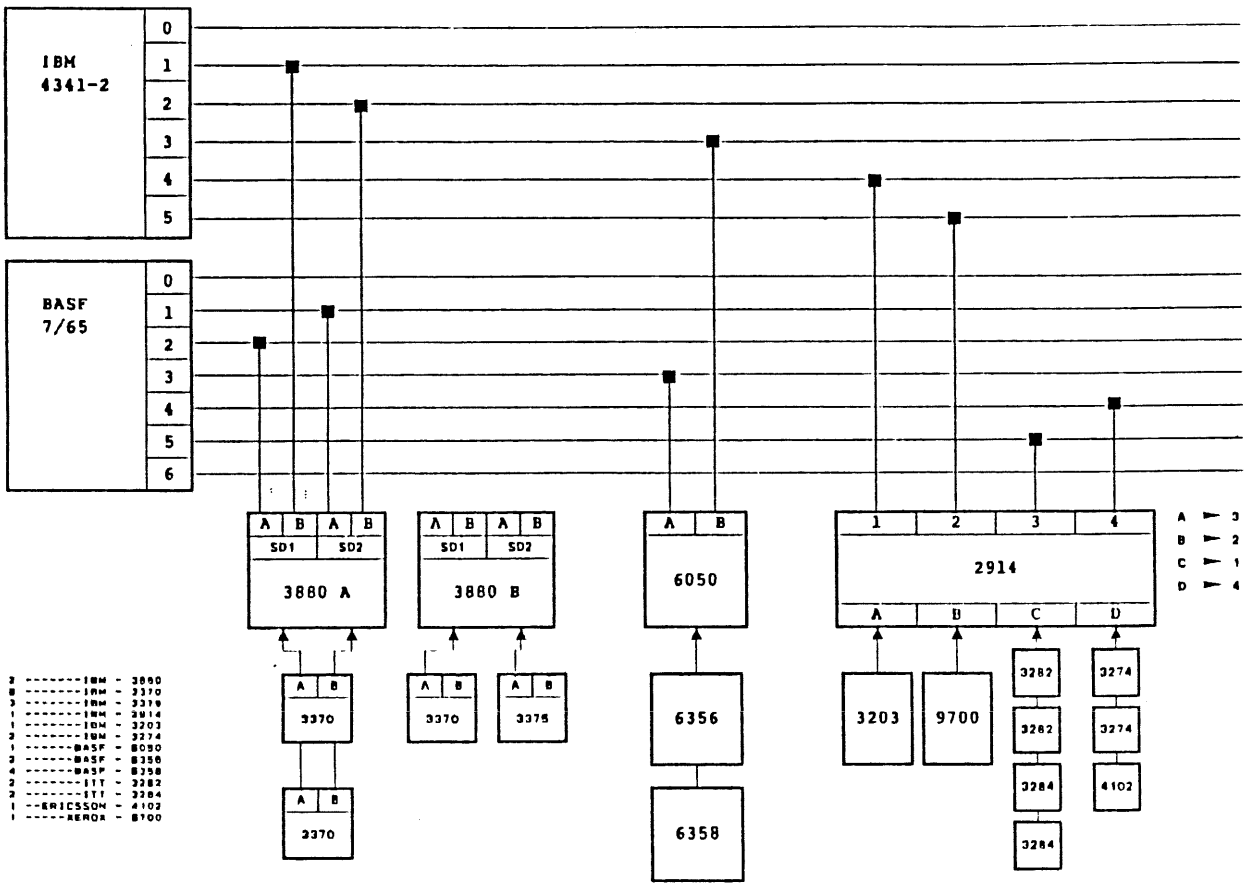


Figure 9: Hardware Configuration Scheme

8.0 THE ACTION SCHEME

The findings and the recommendations are laid down in a report to management who will have to decide whether:
1. the actual situation will be adapted to the norm (requirement);
2. the norm will be adapted to the actual situation;
3. an alternative has to be found between 1 and 2.

Finally, an action scheme - if adaptation is necessary - will be drawn up, and seeing the involvement of the whole organization in the entire operation, these measures will be effective.

9.0 STATIC VERSUS DYNAMIC (Security Function)

The actions which have been taken up to now have a static character (except the influence of the data processing scheme). The actual situation has been studied and from this 'instantaneous snapshot' measures have been recommended as though there will be no change in the situation in the future.

If the continuity of the enterprise or organization strongly depends on data processing, this static approach is in fact not acceptable. A periodic risk analysis has to be discouraged as well, because the time interval will be too great.

Hopefully, it has been made clear that changes in one of the subsets (data, hardware, etc.) may subsequently require adaptation of the measures. Actually, this happens frequently. Therefore, it is necessary - in order to maintain a permanent balance between normative and actual situation - to introduce a security function. The task of the person in charge will be to maintain a permanent balance. Only then will dynamic risk analysis be attained.
This illustrates that quite some knowledge and expertise is needed for proper execution of the security function. Training is necessary. The aspect 'training' will not be discussed in this article.

10.0 THE SECURITY FUNCTION

Chapter 9.0 dealt, among others, with the security function. However, only one aspect of it has been covered. The entire function consists of two elements viz.: the 'management' and the 'operational' part. The former is responsible for 'security management' whilst the latter 'translates' and carries out what that management considers necessary.

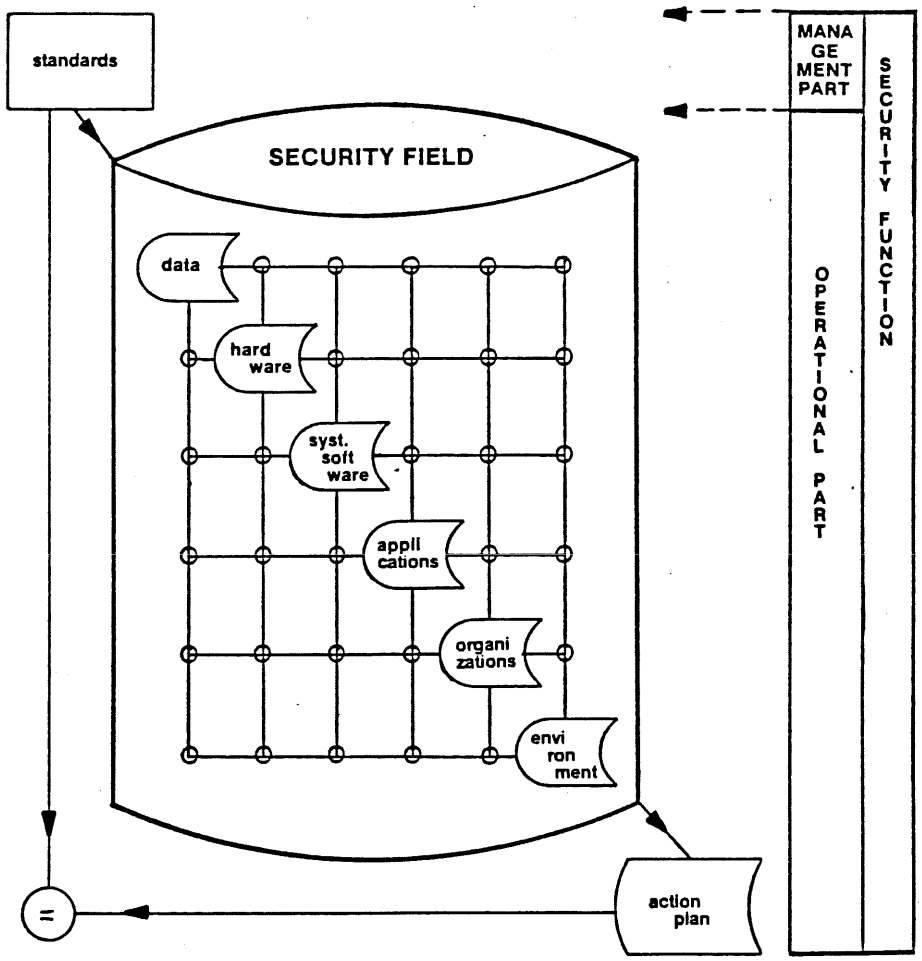


Figure 10: Relation security function - security field

The management part falls within the scope of top management, whereas the operational part can be placed on different levels - dependent on the size and structure - within the entity.

The management part of the security function has to see to developing a security management and establishing guidelines, prior conditions and norms. The operational part has to translate this into a security organization in such a way that the norm will be in balance with the actual situation (the reality). A security organization does not only mean the installing of procedures and guidelines, etc, but also the controlling and checking of their correct functioning. The relation between the security function and the 'security field' is shown schematically in figure 10.

11.0 CONCLUSION

In the first part of this article 'security management' was discussed, and a theoretical model was developed. Only when the dynamic aspect is present one can speak of management. The functions existing within an organization have to be directed towards a specific goal, viz.: security. This contribution aims at furthering that objective.

Another objective of this article has been to encourage thought about the present status of security, with which the author is indeed not happy. Hopefully, a basic concept has been given for the future.

This is the first article on this concept. A so called 'overall view'. Some aspects of this concept have not been filled in. That will be done in the near future. Some of these aspects are:

- training aspects of (security) managers and security officers;
- the place of the security function in the organization;
- the role of an external advisor in security management;
- how to carry out a security audit and what experience and knowledge is required for it.

Naschrift van de Redactie

Onder het hoofd Risk Analysis maakt de schrijver een onderscheid tussen twee categorieën "Performers":
- de "experts";
- de "amateurs".

Zoals een goede schrijver betaamt heeft hij het gelijk aan zijn kant: Risico-analyse dient te geschieden door deskundigen uitgaande van het bedrijf in kwestie rekening houdend met de interne en externe factoren die mogelijk risico's zouden kunnen veroorzaken.
Het is een bouwwerk van binnenuit. Niet een snel oordeel op grond van vragenlijsten met als regel een algemeen toepasbare strekking.

Als aanvulling op het bovenstaande meent de redactie dat niet onvermeld mag blijven het grote nut van het zeer specifieke controlegereedschap dat samengevat kan worden onder het begrip "AC-vragenlijst".

Ook "experts" hebben deze vragenlijsten nodig als "aide de mèmoire" bij hun eindevaluatie.
Redactie.

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

DE ORGANISATIE ROND EEN SYSTEEM/38

door H.J. Lijnes, organisatie-adviseur

1. Inleiding

Met de ingebruikneming van een IBM Systeem/38 in organisaties, waar men voorheen gebruik maakte van een IBM Systeem/34 en/of 36, behoort een betere beheersing en controle van de automatiseringsactiviteiten niet slechts tot de mogelijkheden, maar wordt zelfs een noodzaak.

De na een eerste gewenningsperiode toch wel betrekkelijk eenvoudige wijze waarop men gebruik kan maken van het Systeem/38, veroorzaakt in vele gevallen een ongebreideld gebruik van de ter beschikking staande mogelijkheden. Dit leidt, en zal leiden, tot het optreden van knelpunten in het Systeem/38. Deze knelpunten zullen zonder een gerichte organisatie van functies, taken en bevoegdheden, alsmede de invoering van enige methodiek en standaards, uitmonden in een, niet altijd strikt noodzakelijke, uitbreiding van het Systeem/38.

Bij de opzet van een organisatie rondom een Systeem/38, dient men daarom een verdeling van taken en verantwoordelijkheden toe te passen die een betere waarborg zijn voor de beheersing en controle van de automatiseringsactiviteiten. Het is niet noodzakelijk dat dit een excessieve groei betekent van het aantal medewerkers van de automatiseringsafdeling, zoals meestal het geval is in grote automatiseringsorganisaties.

Dit artikel tracht de weg daartoe aan te geven en doet suggesties omtrent de wijze waarop men tot een betere benutting kan komen van de mogelijkheden van een Systeem/38.

2. Personele bezetting

In veel organisaties die gebruik maakten, en maken, van een Systeem/34 of 36, wordt slechts een minimale functiescheiding toegepast. De automatiseringsorganisatie kent in veel gevallen slechts het verschil tussen de systeembediening en programmering en in sommige organisaties wordt dit onderscheid zelfs niet gemaakt.

Nieuwe toepassingen worden op een "informele" wijze ontwikkeld, waarbij het contact tussen eindgebruiker en de betreffende programmeurs direct en "ongedocumenteerd" plaatsvindt.

Deze werkwijze zal aanvankelijk niet zo snel tot problemen leiden, echter, wanneer het aantal toepassingen in de loop der tijd toeneemt, er sprake is van personeelsverloop op de Automatiseringsafdeling en wanneer de toepassingen aan wijzigingen toe zijn, begint de ontevredenheid. De oorzaak hiervan is, in praktisch alle gevallen, de lange tijd die nodig is voor het aanbrengen van wijzigingen alsmede de lange responsetijden die optreden bij het gebruik van de toepassingen.

Wil men komen tot een betere beheersing van de produktiviteit, systeemcapaciteit en de kwaliteit van de toepassingen, dan dient men naast de diverse methoden en procedures ook te beschikken over een doelmatige verdeling van taken en verantwoordelijkheden.

2.1 Onderscheiden functies

In een Systeem/38 omgeving worden de volgende functies onderscheiden:

a. Beveiligingsbeheer (Security Officer).
Het (mede) opzetten en bewaken van beveiligingsprocedures ter voorkoming van onbevoegd gebruik van apparatuur, programmatuur en gegevensverzamelingen, alsmede het beheren van gebruikersprofielen ("user profiles") en -wachtwoorden ("passwords").

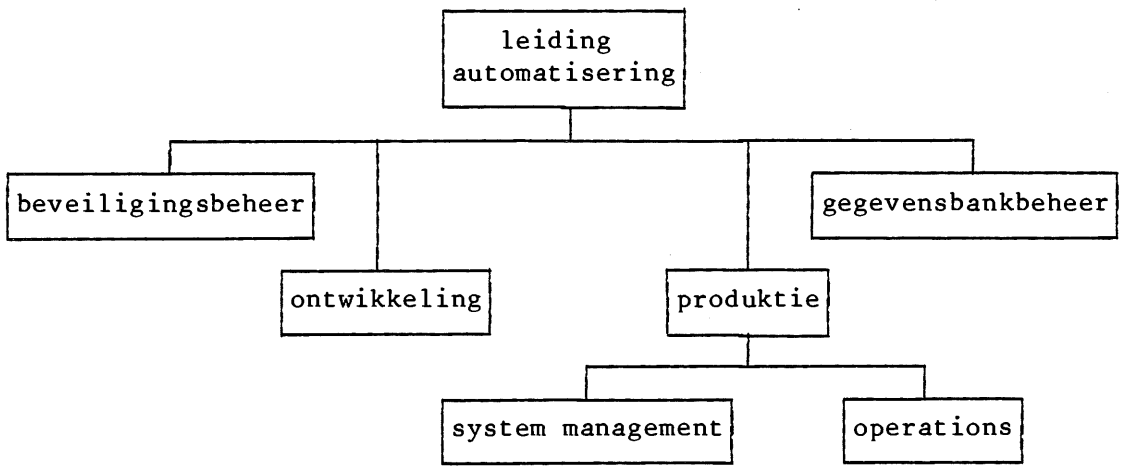
b. Gegevensbankbeheer (Data Base Administration).
Het definiëren, structureren en opzetten van gegevensverzamelingen ("Physical" en "Logical Files"), het bewaken van de integriteit en het gebruik ervan, alsmede de relaties tussen de diverse gegevens en van de data dictionary, waarin gedefinieerde begrippen zijn opgenomen ("Field Reference Files").

c. Produktie (System Management and Operations).
Het bewerkstelligen van een tijdige, volledige, juiste, betrouwbare, geautoriseerde en continue verwerking, alsmede het nemen van maatregelen ter bevordering van een doelmatig gebruik van apparatuur en programmatuur.

d. Ontwikkeling (Systems Analysis and Programming).
Het voorbereiden, ontwikkelen, testen, invoeren en onderhouden van nieuwe en gewijzigde geautomatiseerde informatiesystemen, alsmede het stimuleren van de betrokkenheid van gebruikers bij de ontwikkeling en invoering, op een zodanige wijze dat overdracht van kennis plaatsvindt.

e. Leiding (management).
Het geven van algemene leiding aan de voorbereiding en uitvoering van de geautomatiseerde informatiesystemen, het voorbereiden van het informatie- en automatiseringsbeleid/plan, alsmede het in samenwerking met de betrokkenen uitvoeren van het vastgestelde informatie- en automatiseringsbeleid/plan.

Schematisch weergegeven ziet de ideale organisatie van een Automatiseringsafdeling met een Systeem/38 er als volgt uit.



2.2 Taakverdeling en combinatie van functies

Het is niet zonder meer noodzakelijk dat elk van de genoemde functies wordt ondergebracht in een afzonderlijke organisatorische eenheid (positie). De verschillende functies laten zich, uit het oogmerk van functiescheiding, op een toelaatbare wijze met elkaar combineren.

Hierbij valt te denken aan de volgende combinatie van functies:

- Beveiligings- en gegevensbankbeheer;
  het samenvoegen van beide functies in een afzonderlijke organisatorische eenheid (positie).

- Ontwikkeling en gegevensbankbeheer;
  het als deeltaak vervullen van de gegevensbankbeheerfunctie door een van de ontwikkelaars.

- Leiding ontwikkeling en gegevensbankbeheer;
  het als deeltaak vervullen van de gegevensbankbeheerfunctie door de eventuele leidinggevende functionaris van de ontwikkelingsfunctie.

- Leiding automatisering en beveiligingsbeheer;
  het laten vervullen van de beveiligingsbeheerfunctie door de leidinggevende functionaris van de automatisering.

De combinaties van beveiligingsbeheer en ontwikkeling, of van beveiligingsbeheer en produktie moeten worden afgewezen indien men enige betekenis wil toekennen aan functiescheiding.

2.3 **Bevoegdheden functies**
De aan elke onderscheiden functie toe te wijzen specifieke mogelijkheden van het Systeem/38, dienen te worden afgeschermd tegen het gebruik door onbevoegden.

Deze afscherming wordt gerealiseerd door het toewijzen van de specifiek bij een bepaalde functie behorende gebruiksmogelijkheden, welke tot uitdrukking komen in de commando's van de bij het Systeem/38 behorende besturingstaal, en het vervolgens toewijzen van de noodzakelijke autorisaties met betrekking tot het gebruik ervan, door anderen.
Deze toewijzing is alleen noodzakelijk voor de kritische commando's, zoals bijvoorbeeld het creëren van nieuwe bibliotheken, dat tot de exclusieve taken van beveiligingsbeheer kan behoren.

De toegewezen autorisaties zullen afwijken van de door IBM initieel verschafte bevoegdheden in de systeemprogrammatuur. Deze afwijkingen dienen te worden opgenomen in een speciaal daarvoor bestemd programma (in de besturingstaal) dat, na het installeren van nieuwe releases, dient te worden uitgevoerd om de gewenste situatie te herstellen.

3. Systeemontwikkeling

3.1 **Procedures systeemontwikkeling**
Het is, voor een goed inzicht in de werkzaamheden en een goede afstemming met de gebruikers, noodzakelijk dat eenduidige procedures aanwezig zijn met betrekking tot:
- de acceptatie van (nieuwe) opdrachten tot ontwikkeling van toepassingen;
- de uitbreiding of wijziging van bestaande toepassingen;
- het testen en accepteren van nieuwe en gewijzigde toepassingen door gebruikers;
- de systeemontwikkeling door derden;
- de overdracht van (al dan niet door derden) ontwikkelde toepassingen.

3.2 **Standaards ontwikkeling toepassingen**
Het is voor een goede beheersing en controle eveneens van belang, dat standaards voor het ontwikkelen van toepassingen worden vastgesteld.

De standaards dienen onder andere betrekking te hebben op:

A. De aanpak van de voorkomende onderdelen in een systeemontwerp, zoals:
   - de opzet van de database-structuur, gebaseerd op
     . het soort gebruik van de gegevens;
     . de gebruiks- en toegangsfrequentie;
     . de omvang van de voorkomende gegevensverzamelingen;
     . de voorkomende bevoegdheden tot toevoeging, verwijdering en/of wijziging van de in de database voorkomende gegevens.
   - de opzet van de toepassingsstructuur, gebaseerd op
     . de interactieve onderdelen;
     . de door interactieve onderdelen geïnitieerde batch-onderdelen, welke asynchroon kunnen worden uitgevoerd;
     . de batch-onderdelen, die volgens een vast tijdschema kunnen worden uitgevoerd.
   - de opzet van de back-up en recovery-maatregelen, gebaseerd op
     . de tijdstippen en de wijze waarop back-up-bestanden dienen te worden vervaardigd;
     . de verantwoordelijkheden van de eindgebruikers in deze;
     . criteria voor het vastleggen van "audit trails" ("journaling");
     . criteria voor de herstelprocedures in geval van niet geplande onderbrekingen tijdens de interactieve verwerking ("commitment control").
   - de opzet en het hanteren van noodprocedures, gebaseerd op
     . de kritische onderdelen van de toepassing;
     . het al dan niet handmatig kunnen voortzetten van de werkzaamheden.

B. De te volgen gefaseerde ontwikkelingsprocedure.

C. De in de ontwikkelingsprocedure voorkomende controlemomenten.

D. De wijze van programma-opbouw, taalgebruik, het hanteren van beschrijvingen ("comments") in programma's.

E. De systematische naamgeving van bibliotheken, gegevens, bestanden, programma's, etc.

F. De uniforme basisopzet van beeldschermindelingen en "print layouts".

G. De uniforme indeling van menu's en het gebruik van "Command Function Keys".

H. Etc.

3.2.1 **Eisen aan opzet en structuur van toepassingen**

Er dienen standaards te worden vastgesteld voor de ontwikkeling van toepassingen, welke aansluiten op de verdeling van verantwoordelijkheden en taken. Om zo dicht mogelijk aan te sluiten bij de mogelijkheden van het Systeem/38, dient het uitgangspunt bij de ontwikkeling van toepassingen te zijn:

> "Het minimaliseren van de noodzaak tot interventie door een centrale functie. De beheersing en controle van de uitvoering van toepassingen dient plaats te vinden vanaf de werkplek, door de gebruikers van de toepassing. Centrale interventie blijft beperkt tot het veiligstellen van gegevensverzamelingen en het afdrukken van grote hoeveelheden uitvoer".

Veel van de operationele toepassingen op een Systeem/38 zijn oorspronkelijk afkomstig van Systeem/34 of Systeem/3. Veel van deze toepassingen zijn rechtstreeks geconverteerd met de daarvoor ter beschikking staande hulpmiddelen. Deze toepassingen kunnen allerminst worden beschouwd als ideale Systeem/38-toepassingen.

Veel toepassingsonderdelen vervaardigen overzichten op decentraal opgestelde afdrukapparatuur en worden interactief uitgevoerd hetgeen resulteert in lange blokkeringstijden van beeldschermapparatuur. Het in (asynchrone) batch uitvoeren van deze onderdelen is in een Systeem/38-omgeving een betrekkelijk eenvoudig uit te voeren oplossing.

De geautomatiseerde conversie van Systeem/34-programmatuur veroorzaakt vrij diepgaande "Call"-structuren met een onevenredig groot aantal zogenaamde "Control Language" (CL) programma's. Deze veroorzaken een niet onaanzienlijk deel van de "overhead" van het Systeem/38.

De aanwezigheid van de programmeertaal RPG III suggereert een uitwisselbaarheid van programmeurs, die getraind zijn in RPG II.
Wil men echter een optimale toepassing van de nieuwe programmeertaal RPG III, dan zal men zijn RPG II programmeurs grondig dienen te herscholen. Het gebruik van de gestructureerde operaties in RPG III vereist een totaal andere aanpak bij het vervaardigen van programma's in vergelijking met de traditionele "indicator" en "RPG cycle" gestuurde oplossingen in RPG II.

Indien onvoldoende aandacht wordt besteed aan het opleidingsaspect, bij het in gebruik nemen van een Systeem/38, zullen de nieuwe toepassingen dezelfde kenmerken vertonen, als de toepassingen in de vroegere Systeem/34- of Systeem/3-omgeving.

3.2.2 Toepassingsdocumentatie

De toepassingsdocumentatie is nog steeds één van de meest verwaarloosde onderdelen van geautomatiseerde informatiesystemen. Er worden soms indrukwekkende hoeveelheden, goed ogende, documentatie vervaardigd, doch wanneer men na het verstrijken van enige tijd de inhoud daarvan vergelijkt met de werkelijkheid, vertoont deze tal van afwijkingen. Hierdoor ontstaan extra vertragingen bij het aanpassen of wijzigen van toepassingen, terwijl in die gevallen dan ook maar wordt afgezien van het bijwerken van de documentatie.

Bij het opzetten van een toepassingsdocumentatie dient men zich te realiseren welke inspanningen men zich moet getroosten om deze bijgewerkt te houden. Minder ambitieuse, maar actuele documentatie, verdient verreweg de voorkeur.

Het Systeem/38 biedt veel mogelijkheden voor het verkrijgen van een inzicht in de samenstelling van toepassingen. Deze mogelijkheden aangevuld met eigen beschrijvingen van de niet door het Systeem/38 verschafte inzichten, in combinatie met beschikbare hulpprogrammatuur (pakketten), leveren een actuele en bruikbare toepassingsdocumentatie. De daarvoor te maken kosten wegen ruimschoots op tegen het nut en de geringe hoeveelheid tijd die men daaraan moet besteden.

Het is daarvoor echter noodzakelijk dat men regels vaststelt ten aanzien van vorm en inhoud van de noodzakelijke toepassingsdocumentatie - zowel systeem-, als gebruikers- en operationeel georiënteerd - in combinatie met de te gebruiken hulpmiddelen.

Onderdelen van de toepassingsdocumentatie zijn:

1. Een algemeen overzicht van de toepassing in de vorm van een schema, met de daarin voorkomende subsystemen, en de belangrijkste daarin voorkomende bestanden alsmede een korte verbale beschrijving van de voornaamste functies van de diverse onderdelen van de toepassing.

2. Een overzicht van de onderlinge samenhang tussen de in de toepassing voorkomende bestanden. Het gaat hier met name om de relaties tussen logische en fysieke bestanden en de relaties tussen bestanden (logisch en fysiek) en programma's waarin deze bestanden worden gebruikt.

3. Een overzicht van de rubriek- en recordbeschrijvingen van de in een toepassing voorkomende bestanden.

4. Een overzicht van de onderlinge samenhang en structuur van de in de toepassing voorkomende programma's.

5. Een overzicht van de menustructuur van de toepassing met de daarin voorkomende beeldschermindelingen (de keuzemenu's).

6. Per in de toepassing voorkomend programma een korte verbale beschrijving van de functies en de in het programma voorkomende beeldscherm- en printindelingen.

Als voorbeeld van een documentatiehulpmiddel kan ABSTRACT/38 worden genoemd dat, indien het wordt gebruikt in combinatie met Text Management van IBM, een inzichtelijke en bijgewerkte toepassingsdocumentatie oplevert.

De gebruikelijke handleidingen voor eindgebruikers van toepassingen kunnen worden geïntegreerd in de zogenaamde "HELP"-functie. Deze functie biedt de mogelijkheid om door middel van het indrukken van de HELP-toets op het toetsenbord van het beeldschermstation instructies op het beeldscherm te projecteren. In de toepassingsprogrammatuur dienen hiertoe voorzieningen te zijn getroffen, die echter gering van omvang zijn. Het toepassen van, met behulp van Text Management vervaardigde, handleidingen als "HELP"-tekst in programma's kan het gebruik van traditionele "geschreven" gebruikershandleidingen overbodig maken.

De geschreven handleidingen zijn immers vaak zo omvangrijk, dat zij gedoemd zijn hun leven te slijten in een kast of de onderste lade van een bureau, zonder dat er frequent gebruik van wordt gemaakt.

Indien men op de eerder genoemde manier handleidingen vervaardigt, wordt het de gebruiker eenvoudiger gemaakt, zeker indien men de betreffende "HELP"-teksten laat aansluiten op het onderdeel van de toepassing waar de gebruiker op dat moment mee bezig is.

4. Beveiligingsbeheer

De beveiligingsbeheerfunctie ("Security Officer") vervult in het concept van het Systeem/38 een sleutelpositie. De mogelijkheden tot beveiliging in het Systeem/38 behoeven niet te worden beperkt tot het handhaven van de bevoegdheden ten aanzien van het gebruik van programmatuur en gegevensverzamelingen (bestanden), doch kunnen eveneens worden gehanteerd voor het afdwingen van de te volgen procedures.

Er zijn organisaties waarin elk van de afzonderlijke ontwikkelaars de beschikking heeft over de bevoegdheden van "Security Officer". Behalve het aspect van de functiescheiding tussen Ontwikkeling en Produktie kan deze handelwijze een nadelige invloed hebben op de prestaties van het Systeem/38, door onvoldoende afstemming ten aanzien van de wijze waarop men van het Systeem/38 gebruik dient te maken.

In organisaties waar men wel bepaalde vormen van bevoegdheidsverdeling toepast, komt het vaak voor dat men zelden of nooit de eenmaal vastgestelde wachtwoorden ("passwords") verandert, zodat na verloop van tijd deze wachtwoorden als "algemeen bekend" mogen worden verondersteld.

De oorzaak kan worden gevonden in de gekozen bevoegdheidsregeling, die bij een toename van het aantal toepassingen moeilijk te handhaven blijkt door de daaraan noodzakelijkerwijs te besteden tijd in combinatie met een gebrek aan adequate hulpmiddelen.

Een doelmatige uitvoering van de taken die tot het beveiligingsbeheer worden gerekend kan worden bevorderd door het vervaardigen van procedures en hulpmiddelen, gericht op:
- de uitgifte en regelmatige wijziging van "passwords" aan gebruikers van het Systeem/38;
- het installeren van door derden ontwikkelde toepassingspakketten. Deze installatiewerkzaamheden bestaan onder andere uit:
  . controle van de volledigheid van de toepassingsprogrammatuur,
  . controle van de programmatuur op constructies die strijdig zijn met de geldende bevoegdheidsregelingen,
  . het inpassen van de toepassingsprogrammatuur in de geldende bevoegdheidsregelingen;
- de migratie van toepassingsobjecten tussen de Ontwikkelings-, Acceptatie- en Produktie-omgevingen;
- de inrichting van omgevingen en toewijzing van de noodzakelijke bevoegdheden voor nieuwe gebruikers van het Systeem/38;
- het eventueel herroepen van bevoegdheden;
- de controle van inbreuken op de bevoegdheden;
- de uitvoering van "saves" met de bijbehorende noodzakelijke registraties.
- etc.

5. Gegevensbankbeheer

De geleidelijke wijze waarop men een gegevensbank kan samenstellen uit fysieke en logische bestanden heeft als risico dat het evenwicht geleidelijk kan worden verstoord. Hiermee wordt bedoeld, de geleidelijke verandering die kan optreden in het gebruik van de onderscheiden bestanden, die deel uitmaken van de gegevensbank. Indien er geen wijzigingen worden aangebracht in de tot de gegevensbank behorende fysieke bestanden, zullen de responsetijden hierdoor in toenemende mate negatief worden beïnvloed.

Wijzigingen in toepassingen kunnen, ondanks het gebruiksgemak van het Systeem/38, leiden tot het opnieuw creëren van fysieke en logische bestanden en hercompilatie van de samenhangende programmatuur.

Een doelmatige uitvoering van de taken die tot het gegevensbankbeheer worden gerekend kan worden bevorderd door het vervaardigen van procedures en hulpmiddelen, gericht op:
- de beschrijving van gegevensrubrieken in zogenaamde "Field Reference Files";
- de vervaardiging van diverse "where used" overzichten;
- de beschrijving van bestanden ("Data Description Specifications") in "Source Physical Files";
- het gezamenlijk gebruik van toegangspaden tot gegevens in bestanden door verschillende gebruikers ("access-path sharing");
- de regels ten aanzien van validiteit, consistentie en juistheid van gegevens;
- het reorganiseren van de gegevensverzamelingen.
- etc.

6. Produktie

De Produktie-functie kan worden onderscheiden in het beheren van het Systeem/38 en zijn systeemprogrammatuur (System Management) en de bediening (Operations), die noodzakelijk is voor de dagelijkse uitvoering van de toepassingen.

6.1 **System Management**

Onder System Management wordt verstaan, de functie of verzameling van functies die ten doel heeft het Systeem/38 op de meest optimale wijze te laten functioneren, door het scheppen, beheersen en controleren van de meest doelmatige organisatie rondom het Systeem/38, alsmede de operationele inrichting van het Systeem/38 zelf.

Taken die onder System Management kunnen worden gerekend zijn, onder andere:
- de voorbereiding en invoering van opeenvolgende versies van het besturingssysteem en overige systeemprogrammatuur;
- de bevordering van een doelmatig gebruik van apparatuur, data communicatievoorzieningen en programmatuur (capaciteitsbeheersing en prestatiemetingen).

Met name de bevordering van het doelmatig gebruik (waaronder mede kan worden verstaan de "performance") is een gebied dat om goede procedures en hulpmiddelen vraagt. Het ligt immers niet binnen het bereik van iedere organisatie om daarvoor een gespecialiseerde medewerker aan te trekken, zoals dat gebruikelijk is in grote automatiseringsorganisaties (Systeemprogrammeur).

De noodzaak daarvoor in een Systeem/38-omgeving is trouwens niet altijd aanwezig, mits men over de juiste hulpmiddelen beschikt en over voldoende kennis van zaken, voor wat betreft de voornaamste knelpunten die kunnen optreden bij het gebruik van het systeem.

Punten van aandacht hierbij zijn:
- de wijze waarop men gebruik maakt van het Systeem/38, aangeduid als de operationele omgeving;
- de manier waarop men tot een betere beheersing kan komen van de prestaties van het systeem (de "performance");
- de methodes om het externe geheugengebruik (schijfruimte) binnen redelijke normen te houden.

6.1.1 Inrichting Operationele Omgeving Systeem/38

Het is uit een gezichtspunt van beheersbaarheid en controle gewenst een onderscheid te maken tussen een Ontwikkel-, een Test- (of Acceptatie-) en een Produktie-omgeving.
Het ontwikkelen en wijzigen van toepassingsprogrammatuur vindt alleen plaats in de Ontwikkel-omgeving, het testen van toepassingsprogrammatuur door gebruikers in de Test- of Acceptatie-omgeving, en de uitvoering van toepassingsprogrammatuur door gebruikers (en Operators) in de Produktie-omgeving.

Deze indeling is te realiseren door de toewijzing van separate groepen bibliotheken, waartoe slechts door daartoe geautoriseerde personen toegang kan worden verkregen.

De overgang van objecten vanuit de ene omgeving naar een andere dient aan de hand van procedures en met behulp van daartoe geeigende hulpmiddelen te worden geregeld door de beveiligingsfunctie.

Een verdere onderverdeling van de bibliotheken in de Test- en Produktie-omgeving wordt toegepast per toepassing (per afdeling), waarbij programma's, display files, etc. (de meer statische objecten) en databases files en data areas (de meer dynamische objecten) in aparte bibliotheken worden ondergebracht.

Back-up-procedures kunnen hierdoor beter worden afgestemd op de wijzigingsfrequentie van de objecten in de bibliotheken.

Iedere gebruiker van het Systeem/38 krijgt een "user profile" toegewezen. Gebruikers kunnen de beschikking hebben over meerdere "user profiles", afhankelijk van het aantal verschillende toepassingen dat door hen wordt gebruikt. Meerdere gebruikers van eenzelfde afdeling worden bovendien samengevoegd tot een "group profile".

Aan "user profiles" wordt tevens een "job description" gekoppeld, waarin onder andere de bibliotheken worden aangegeven waartoe de betreffende gebruiker toegang heeft gedurende zijn of haar werkzaamheden ("library list").

6.1.2 **Beheersing Performance Systeem/38**

Ter bevordering van de beheersing van de performance van Systeem/38 is het noodzakelijk dat gebruik wordt gemaakt van daarop gerichte hulpmiddelen. Sommige hulpmiddelen, de eenvoudige, kunnen zelf worden vervaardigd, de meer complexe dienen te worden aangeschaft.

Het betreft hulpmiddelen:
- voor het verkrijgen van een inzicht in de gebruiksfrequentie alsmede het soort gebruik van bestanden door toepassingen. Hierdoor wordt het mogelijk de reorganisatie van bestanden beter af te stemmen op het meest frequente (en soort) gebruik;
- voor het vervaardigen van overzichten met betrekking tot het gebruik van het Systeem/38. Deze informatie kan worden gebruikt om tot een eventuele doorbelasting van kosten te komen, terwijl tevens een inzicht wordt verkregen omtrent eventueel optredende knelpunten in het systeemgebruik. Met name dit laatste punt is van belang voor eventuele maatregelen ter verbetering van de Systeem/38 performance;
- voor het localiseren en analyseren van verdere knelpunten in de performance van het Systeem/38, op een meer gedetailleerd nivo (software monitor).

6.1.3 **Extern geheugengebruik**

Door de gebruikseenvoud van het Systeem/38 ontstaat in vele gevallen een onzorgvuldig gebruik van de externe geheugenruimte. Een externe geheugenbezetting die groter wordt dan 50 tot 60%, oefent in toenemende mate een nadelige invloed uit op de totale prestatie van het Systeem/38. Het is daarom noodzakelijk, dat een aantal maatregelen worden genomen om verspilling van externe geheugenruimte tegen te gaan.

Deze maatregelen, vast te leggen in procedures, zijn onder andere:
- het regelmatig uitvoeren van een "Initial Micro Program Load" (IMPL), waardoor overmatig grote "Spool Buckets" kunnen worden vermeden;
- het opslaan van de "sources" van produktieprogrammatuur op externe gegevensdragers (diskette, tape), gekoppeld aan een procedure (en programmatuur) voor het beschikbaar stellen van te wijzigen sources;
- het regelmatig verwijderen van niet meer gebruikte objecten uit de diverse bibliotheken (schonen);
- het regelmatig reorganiseren van frequent muterende bestanden ten behoeve van het opnieuw beschikbaar stellen van de ruimte die in beslag genomen wordt door "deleted" records;

Dit reorganiseren heeft tevens een positief effect op de responstijden van het Systeem/38, indien hierbij tevens rekening wordt gehouden met de meest frequent gebruikte volgorde van de te reorganiseren bestanden;
- het is tevens aan te bevelen, in die gevallen waarbij de externe geheugenbezetting groter is dan 60%, op gezette tijden een complete "save" van het systeem uit te voeren en vervolgens het systeem te "restoren". Hierdoor worden met name de aanwezige bestanden op een meer evenwichtige wijze over de beschikbare schijfruimte verdeeld (aaneensluitend);
- het met behulp van speciale programmatuur verwijderen van de zogenaamde "program templates" van produktieprogramma's, hetgeen besparingen kan opleveren van 40 tot 60% in de ruimte die nodig is voor het opslaan van deze programma's.

6.2 **Operations**

In het ontwerp van nieuwe toepassingen dient men te streven naar een zo automatisch mogelijk verloop van de werkzaamheden op het Systeem/38. De bediening van de centraal opgestelde apparatuur zal hiermee tot een minimum kunnen worden beperkt, waardoor bedieningstaken wellicht kunnen worden gecombineerd met een andere aanwezige functie.

Taken die tot operations worden gerekend zijn onder andere:
- bediening en bewaking van de (centraal) opgestelde apparatuur;
- het bedrijfsklaar maken van het Systeem/38;
- het afsluiten van de werkzaamheden op, en het uitzetten van het Systeem/38;
- de registratie en bewaring van gegevensdragers (diskettes, tapes);
- het registreren en aanvullen van de papiervoorraden;
- de nabewerking van lijstuitvoer (splitsen, distribueren, etc.);
- etc.

7. Handboek Systeem/38

Het is gewenst, zoniet noodzakelijk, de organisatie, taken en verantwoordelijkheden, de procedures, het gebruik van de hulpmiddelen, regels, aanbevelingen, etc., vast te leggen in een handboek.

Ervaringen hebben aangetoond, dat in automatiseringsorganisaties met een kleine personele bezetting, de continuïteit erg kwetsbaar is. In geval van ziekte en optredend verloop, komt de uitvoering van de werkzaamheden in gevaar door het ontbreken van duidelijke instructies. In deze kleine organisaties is het uitermate belangrijk, dat het waarnemen van werkzaamheden van anderen ondersteund wordt door uitgebreid gedocumenteerde procedures en instructies.

Het handboek kan worden ingedeeld als volgt:

1. Een algemeen deel met gegevens over de organisatie, functies en taken, alsmede de distributie en het onderhoud van het handboek.
2. Een deel met een complete beschrijving van de aanwezige apparatuur, de locaties, de bekabeling van aangesloten werkstations met hun adressering ("hardware"), alsmede een opsomming van de geïnstalleerde systeemprogrammatuur, de daarop aangebrachte veranderingen, en een (schematische) vastlegging van de gebruikte operationele inrichting (Sub Systems, Job Descriptions, Output Queues, etc.).
3. Een deel met gedetailleerde instructies met betrekking tot de bedieningsaspecten van het systeem.
4. Een deel met op het beveiligingsbeheer toegespitste procedures, instructies en hulpmiddelen.
5. Een deel met op het gegevensbankbeheer toegespitste procedures, instructies en hulpmiddelen.
6. Een deel met op het "System Management" gerichte procedures, instructies en hulpmiddelen, zoals:
   - "Job Accounting" procedures en hulpmiddelen;
   - de uitvoering van prestatiemetingen;
   - beschrijvingen van speciaal ten behoeve van operations vervaardigde programmatuur;
   - etc.
7. Een deel waarin de te volgen ontwikkelingsprocedures staan beschreven, alsmede de standaards, instructies en aanbevelingen die gelden voor de te ontwikkelen toepassingen.
8. Een deel waarin de samenstelling van de toepassingsdocumentatie staat aangegeven, alsmede de procedures en instructies rond de hulpmiddelen, die bij het samenstellen worden gehanteerd.
9. Een deel met door operations uit te voeren werkzaamheden die verband houden met de uitvoering van toepassingen.

Verder kunnen nog alle voor de automatiseringsactiviteiten belangrijke adressen van contactpersonen worden vastgelegd in een adreslijst.

Ervaringen hebben aangetoond dat, bij het optreden van de reeds eerder genoemde situaties, de aanwezigheid van een actueel handboek goede diensten kan bewijzen.

8. Tot besluit

De mogelijkheden van het Systeem/38 kunnen op effectieve wijze worden aangewend bij het handelen naar de te volgen procedures. Het is tevens een systeem dat door zijn structuur de mogelijkheid geeft tot verregaande automatisering van de automatiseringswerkzaamheden zelf.

Er zijn tal van dit soort hulpmiddelen beschikbaar die, in vergelijking met gelijksoortige produkten voor de "grote" systemen, tegen aanzienlijk geringere kosten verkrijgbaar zijn.

Het is daarom aan te bevelen zich eens te oriënteren op deze markt, zodat men een inzicht krijgt op welke wijze men, met deze hulpmiddelen in combinatie met een meer gestructureerde opzet van de automatiseringsorganisatie, een grotere produktiviteit van de automatiseringsinspanning kan bereiken.

9. Literatuur

1. Beheersing, beveiliging en controle van het IBM Systeem/38
   A.H.C. Koedijk Compact 10e jaargang nummer 31 Lente 1983

2. Abstract/38 User Guide
   Advanced Systems Concepts, Inc.

3. Anchor/38 Produkt Informatie
   SSP Systems Support & Products.

4. Diverse IBM System/38 Manuals.

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

Herfst 1984

BEVEILIGINGSASPECTEN IN NETWERKEN: THEORIE EN PRAKTIJK

door ing. C.J.M. Gielen en H. Weerd*)

1. Inleiding

In dit artikel worden zowel de theorie als de praktijk ten aanzien van beveiligingsaspecten van netwerken behandeld.
Allereerst zal worden ingegaan op de theoretische aspecten.
Hierbij zullen worden behandeld: een algemeen model waarin de bedreigingen ten aanzien van netwerken kunnen worden gegroepeerd, link oriented versus end-to-end protocollen, data encryption en hoe de bedreigingen in netwerken kunnen worden afgedekt. Bij de behandeling van deze onderwerpen is gezien de beperkte ruimte geen volledigheid nagestreefd. Getracht is om de belangrijkste aspecten zo compact mogelijk weer te geven. Voor lezers die dieper op de betreffende onderwerpen willen ingaan en/of meer achtergrondinformatie willen, verwijzen wij gaarne naar de literatuurlijst waarvan vooral [1] is aan te bevelen.
In het tweede gedeelte zal worden ingegaan op een praktisch voorbeeld: het S.W.I.F.T.-netwerk. Hierbij zal worden ingegaan op: het doel en de functies van S.W.I.F.T., de verhouding van het S.W.I.F.T.-netwerk tot het OSI-model en de voorzieningen die bij het S.W.I.F.T.-netwerk in de application en transport layer zijn getroffen.

Onderdeel theorie

2. Bedreigingen ten aanzien van netwerken

De datacommunicatie heeft de afgelopen jaren een enorme vlucht genomen. De informatie die over de netwerken wordt getransporteerd zal voor de ene organisatie meer en voor de andere organisatie minder kritisch en/of waardevol zijn. In dit artikel zal de noodzaak tot het beveiligen van die informatie als uitgangspunt worden aangenomen.
De bedreigingen die in een netwerk kunnen vóórkomen, worden in de volgende vijf groepen gerangschikt:

1. Vrijkomen berichtinhoud.
2. Analyseren berichtenstroom.
3. Wijzigen berichtenstroom.
4. Blokkeren en/of vertragen van berichten.
5. Heimelijk initiëren van een verbinding.

*) Dit artikel is onder de titel "Security in high level network protocols: theorie en praktijk" in een eerdere versie gepubliceerd door ASI ETV in de syllabus "Informatie over communicatie", serie voordrachten gehouden op 24 oktober 1984 aan de TH Delft.

De eerste twee bedreigingen zijn passief: er wordt slechts informatie afgeluisterd. Bij het actief indringen in een netwerk wordt de berichtenstroom behalve afgeluisterd tevens gewijzigd of beïnvloed (dat wil zeggen de bedreigingen 3 tot en met 5).

Het vrijkomen van de inhoud van een bericht vindt plaats indien de informatie in een bericht bekend wordt (bijvoorbeeld door het aftappen van een communicatiekanaal) aan een daartoe ongeautoriseerde persoon of entiteit (bijvoorbeeld een proces).

Het analyseren van de berichtenstroom is het ongeautoriseerd observeren van de berichtenstroom in het netwerk. Hierbij is meestal additionele informatie noodzakelijk. Indien een indringer bijvoorbeeld ziet dat er veel berichten worden uitgewisseld tussen de componenten van twee bedrijven dan zou hij daaruit kunnen afleiden dat de twee bedrijven onderhandelen. Dit gegeven alleen is echter niet zo interessant, men zou al moeten weten waarover de twee bedrijven eventueel zouden kunnen zijn gaan onderhandelen.

Onder het wijzigen van de berichtenstroom valt naast het (letterlijk) wijzigen van de inhoud van een bericht (inclusief het adres van zender of ontvanger) hertransmissie van berichten, het toevoegen van informatie, het verwijderen van informatie en het opnieuw ordenen van blokken waarin een bericht is opgesplitst.

Bij heimelijk initiëren van een verbinding wordt getracht een verbinding aan te gaan onder een valse identiteit of door hertransmissie van een reeds eerder verzonden berichtenstroom.

Het hierboven beschreven model kan worden gebruikt voor het specificeren van algemene security eisen ten aanzien van netwerken. Het model is gebaseerd op de logische structuur van een netwerk, op security aspecten ten aanzien van de fysieke structuur zal in dit artikel niet worden ingegaan (zie daarvoor [2]).

De lezer merke op dat passieve aanvallen (dat wil zeggen aanvallen waarbij informatie slechts wordt afgeluisterd) kunnen worden voorkomen ondermeer door vercijfering (zie paragraaf 4).
Actieve aanvallen daarentegen, waarbij de informatie kan worden gewijzigd, kunnen niet worden voorkomen, doch slechts worden gedetecteerd tenzij het gehele netwerk inclusief lijnen, knooppunten e.d. fysiek beveiligd zou kunnen worden.

3. Link oriented versus end-to-end protocollen

Ten aanzien van beveiligingsmaatregelen in netwerken zijn er twee basisbenaderingen:
1. link-oriented;
2. end-to-end.

Link oriented

Het belangrijkste voordeel van link-oriented maatregelen is dat het gehele bericht dat over een datacommunicatie-link gaat vercijferd kan worden. Ook het adres van de zender en de ontvanger zijn derhalve gemaskeerd. Daar de informatie slechts op de communicatie-links is beschermd dienen de knooppunten in het netwerk allemaal veilig te zijn. Naast het feit dat dit zeer kostbaar is en moeilijk toe te rekenen is aan de verschillende gebruikers van het netwerk, is het de vraag of alle gebruikers van het netwerk wel zullen willen vertrouwen op beveiligingsmaatregelen die door de autoriteiten van het netwerk zijn geïmplementeerd en worden onderhouden. Zeker in geval van een public netwerk (big brother is watching you) zal dit laatste zwaar wegen. In het algemeen mag daarom worden gesteld dat link-oriented maatregelen niet goed toepasbaar zijn voor publieke netwerken.

End-to-end

End-to-end maatregelen modelleren het netwerk als een medium waarop het berichtenverkeer op een veilige manier van afzender tot bestemming kan plaatsvinden. Ze kunnen geheel door de gebruikers zelf worden geïmplementeerd en worden onderhouden. Indien één van de tussenliggende links bij een transport niet veilig is kan toch een veilig transport plaatsvinden.
Naarmate de maatregelen dichter bij de terminalgebruikers worden gelegd kan een groter gedeelte van het traject door het protocol worden beschermd. De hard- en software die een en ander moet ondersteunen neemt echter toe.

4. Data encryption

Alle beveiligingstechnieken tegen de bedreigingen die in paragraaf 2 zijn gedefinieerd zijn gebaseerd op data encryption. In dit hoofdstuk zullen allereerst enige definities worden gegeven. Vervolgens zal kort worden ingegaan op crypto-analyse (het ontcijferen van geheimschriften). In de laatste twee paragrafen zullen de belangrijkste aspecten van respectievelijk de Data Encryption Standard (DES) van het National Bureau of Standards en public key cryptosystemen worden beschreven. Het ontwerp van encryption algoritmes valt buiten de scope van dit artikel.

Definities

De cryptologie (leer van het geheimschrift) [3] is opgesplitst in de:
- cryptografie: het ontwerpen van geheimschriften;
- crypto-analyse: het ontcijferen van geheimschriften.

Met betrekking tot de automatische gegevensverwerking kunnen drie toepassingsmogelijkheden van de cryptografie worden gegeven:
1. gegevenstransport over netwerken;
2. gegevensopslag in bestanden of data bases;
3. authentificatie van gebruikers en/of berichten.

Alleen op de punten 1 en 3 zal in dit artikel worden ingegaan.

Figuur 1 **Conventioneel systeem**

Klare tekst kan met behulp van een cryptografisch systeem worden vercijferd. Hierbij wordt meestal een bepaalde sleutel gebruikt. De aldus verkregen tekst wordt cijfertekst genoemd. Voor het ontcijferen dient een inverse operatie beschikbaar te zijn. In conventionele systemen werd voor het ver- en ontcijferen dezelfde sleutel gebruikt. Een dergelijke sleutel mag alleen bekend zijn aan geautoriseerde gebruikers. Het algoritme dat wordt gebruikt voor het ver- en ontcijferen wordt een cijfer genoemd (zie figuur 1).
Bij de meer moderne technieken - de public key systemen - zijn er voor het vercijferen (de public key) en het ontcijferen (de geheime sleutel) aparte sleutels.

Twee klassen van cryptografische systemen kunnen worden onderscheiden:
1. Blokcijfers: deze versluieren hele blokken onder controle van een sleutel. Ze zijn equivalent aan de klassieke substitutie algoritmen. Indien een blok correspondeert met een karakter is het eenvoudig om een dergelijk algoritme te breken. De enige oplossing hiervoor is om de blokgrootte te verhogen en mixing transformaties te gebruiken. Het DES-systeem kent hier een voorbeeld van. Onder mixing transformaties wordt verstaan het van plaats verwisselen van delen van het blok.
2. Stroomcijfers: hierbij worden delen van de klare tekst vercijferd met behulp van een deel van de sleutelstroom. Deze gedeelten variëren van een tot acht bits. De sleutelstroom heeft hierbij - in tegenstelling tot blokcijfers - altijd dezelfde lengte als de klare tekst.

Verscheidene technieken kunnen worden toegepast om de sleutelstroom te genereren. Deze technieken bepalen of wijzigingen in de cijfertekst al dan niet worden voortgeplant in andere delen van ontcijferde tekst. In het laatste geval bestaat het gevaar dat voorspelbare wijzigingen kunnen worden aangebracht in de ontcijferde tekst.

De kunst bij cryptografie is om systemen te ontwerpen die zeer moeilijk te breken zijn. Een cryptografisch systeem dat iedere aanval kan doorstaan ongeacht de computertijd en capaciteit wordt onconditioneel of theoretisch betrouwbaar genoemd. Een cryptografisch systeem is praktisch betrouwbaar indien de kosten om het systeem te breken de baten te boven gaan.

Crypto-analyse

Drie niveaus van crypto-analyse kunnen worden onderscheiden:

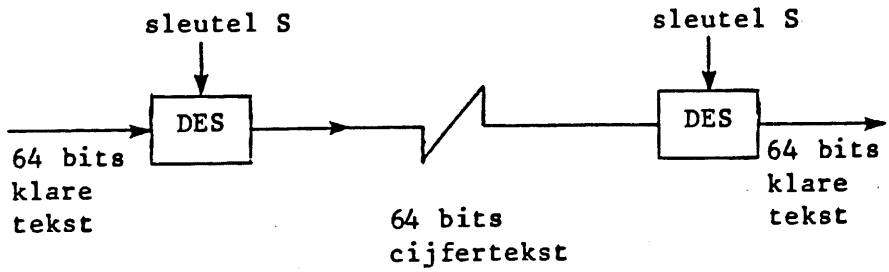
1. ciphertext only attack: hierbij is alleen de vercijferde tekst beschikbaar aan de crypto-analist. Om het cryptosysteem te breken maakt de crypto-analist gebruik van de kennis van statistische eigenschappen van de taal, zoals de relatieve frequentie van bepaalde letters en waarschijnlijke woorden zoals standaardafsluitingen in brieven e.d.;
2. known plaintext attack: hier is zowel een klare tekst als de bijbehorende vercijferde tekst bekend;
3. chosen plaintext attack: de crypto-analist heeft hierbij de beschikking over zelf gekozen klare tekst en de bijbehorende cijfertekst. Dit is uiteraard de meest krachtige methode. Public key systemen moeten hiertegen bestand zijn om de eenvoudige reden dat de manier van vercijferen openbaar is, zowel wat betreft het algoritme als de sleutel waarmee het bericht wordt vercijferd.

Data Encryption Standard

De DES definieert een aantal standaardtechnieken voor encryption. Hierbij komen zowel blok- als stroomcijfers voor. In de volgende subparagrafen zullen de verschillende technieken in het kort worden besproken.

Electronic Code Book (ECB)

De meest fundamentele techniek is een blokcijfer met 64-bits blokken en een 56-bits sleutel (zie figuur 2).



Figuur 2 **ECB**

Ieder bit in de vercijferde tekst is een functie van de klare tekst en de 56-bits sleutel. De voortplanting van een wijziging binnen een blok is derhalve hoog, daarbuiten nihil (met het reeds genoemde nadeel dat mogelijk voorspelbare wijzigingen kunnen worden aangebracht).
Identieke klare tekst levert identieke vercijferde tekst. Men zou dus een lijst kunnen aanleggen van overeenkomstige klare tekstcijferparen. Misschien kunnen zo fragmenten van de tekst worden ontcijferd. Een dergelijke lijst hoeft niet eens zo heel lang te zijn. Bijvoorbeeld in Engelse tekst zijn niet 2**64, maar slechts 2**12 groepen van 64 bits met niet verwaarloosbaar kleine frequentie.

Cipher Block Chaining (CBC)

Bij de CBC-techniek wordt een bericht opgedeeld in blokken. Bij het eerste blok wordt modulo 2 een zogenaamde Initialisatie Vector (IV) opgeteld. Vervolgens wordt het resultaat vercijferd. De resulterende cijfertekst wordt verzonden en daarnaast als input gebruikt voor de modulo 2-optelling (in de eerste slag werd hiervoor de IV gebruikt) van het tweede blok etc. (zie figuur 3).

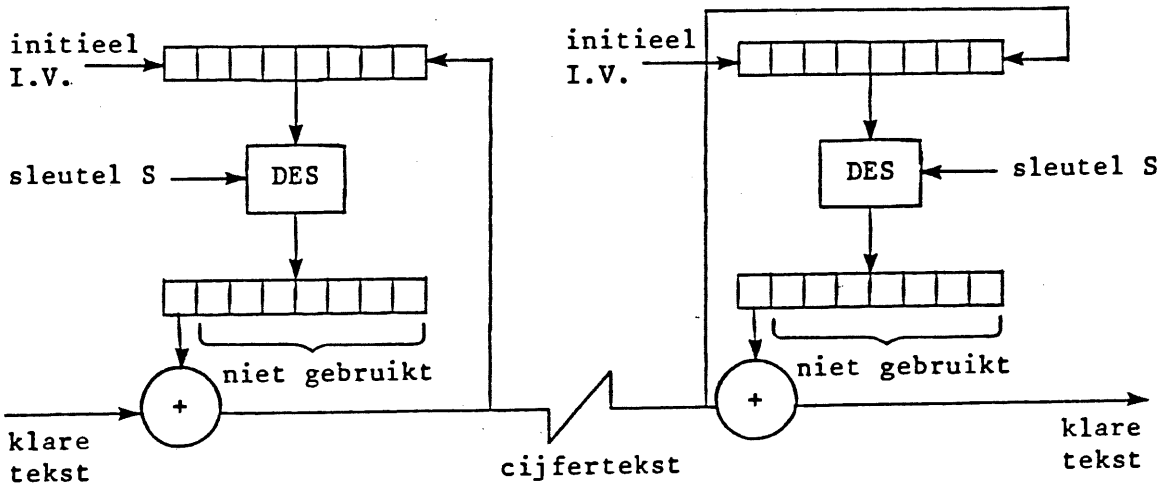
Figuur 3 **CBC**

Een wijziging in de cijfertekst werkt slechts door in twee blokken (voor de ontvanger).

Cipher FeedBack (CFB)

Bij deze laatste techniek wordt DES zodanig gebruikt dat de vercijferde tekst wordt gebruikt voor sleutelstroomgeneratie.
Zowel bij de zender als bij de ontvanger wordt gestart met dezelfde Initialisatie Vector. Van de vercijferde tekst worden slechts de eerste acht bits gebruikt voor een modulo 2-optelling met de eerste acht bits van de te versluieren tekst.

Deze acht bits worden zowel verzonden als gebruikt om te worden toegevoegd aan de IV. Daar vallen de eerste acht bits van weg etc. (zie figuur 4).



Figuur 4 CFB

Kritiek op DES

De publicatie van het voorstel DES (door IBM ontwikkeld) als standaard te accepteren heeft tot een storm van kritiek geleid.
Het voorstel is echter uiteindelijk ongewijzigd aangenomen.
De twee belangrijkste punten van kritiek betroffen:

1. de sleutelgrootte: in het oorspronkelijke voorstel van IBM had DES een sleutel van 128 bits. Deze lengte zou uitputtend onderzoek van de sleutel voor lange tijd onmogelijk maken. De lengte van de sleutel is gewijzigd in 56 bits (plus acht parity bits). Bij deze sleutellengte wordt (zoals reeds bij de ECB is aangegeven) uitputtend onderzoek binnen een tiental jaren mogelijk geacht [4];
2. het ontwerp van het algoritme: dit is niet bekend gemaakt. Hierdoor is het voor personen buiten IBM en het National Bureau of Standards onmogelijk te controleren hoe goed het algoritme werkelijk is.

Public key algoritmen

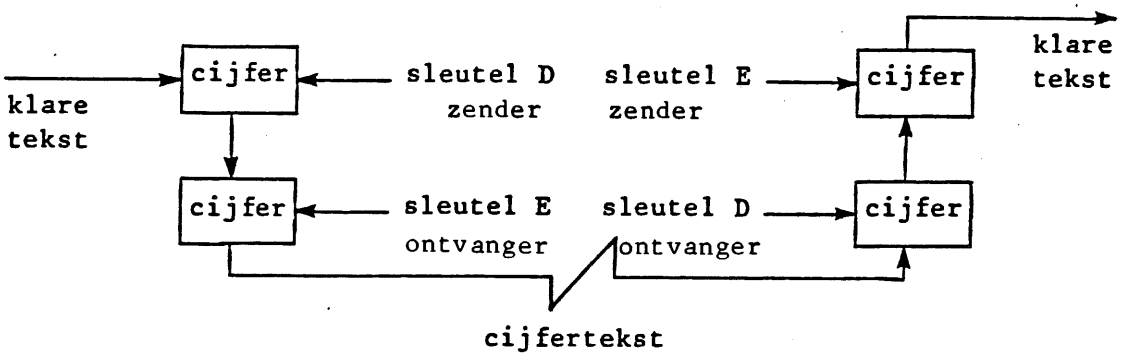
De conventionele cryptografische systemen bevatten een tweetal aspecten die het gebruik ervan op grote schaal hebben beperkt:

1. sleutelbeheer en -distributie: de kwetsbaarheid van het berichtenverkeer wordt verplaatst naar de gebruikte sleutels. Dit is geen gering probleem, voor 1000 gebruikers zijn bijna 500.000 sleutels nodig;

2. de onmogelijkheid om berichten te ondertekenen.

Als oplossing voor deze problemen zijn twee trends te onderscheiden:
a. Public key distributiesysteem: hierbij kunnen zender en ontvanger zonder tussenkomst van enige andere partij, via het openbare kanaal een sleutel overeenkomen voor het gebruik in een conventioneel cryptosysteem;
b. public key cryptosystemen, die hieronder zullen worden behandeld.

Bij public key algoritmes wordt onderscheid gemaakt tussen de mogelijkheid om een bericht onder een bepaalde sleutel te vercijferen of te ontcijferen. Hiervoor worden paren (E, D) van sleutels uitgegeven. Deze sleutels definiëren een paar van transformaties (die eenvoudig te berekenen moeten zijn) die ieder hun inverse zijn en waarbij geen van de twee afleidbaar is van de andere. Iedere gebruiker heeft een paar sleutels. De ene (E) is openbaar (the public key) en wordt gebruikt om berichten voor die gebruiker te vercijferen. De andere sleutel (D) wordt geheim gehouden en gebruikt door de betreffende ontvanger om voor hem bestemde berichten te ontcijferen.
Identificatie van de zender kan plaatsvinden door het bericht eerst te vercijferen onder de geheime sleutel van de zender en daarna onder de openbare sleutel van degene voor wie het bericht is bedoeld. De ontvanger kan het bericht ontcijferen door allereerst zijn eigen geheime en vervolgens de openbare sleutel van de zender op het bericht los te laten (zie figuur 5).



Figuur 5 **Public key cryptosysteem**

De identificatie van het bericht door de zender met behulp van zijn geheime sleutel kan in datacommunicatiesystemen de handtekening gaan vervangen die we in het dagelijks leven op allerlei documenten zo gewend zijn als bewijs voor het feit dat het document inderdaad van de veronderstelde zender afkomstig is.

Een functie die voldoet aan alle eigenschappen als hierboven beschreven behalve de mogelijkheid tot het signeren van een bericht wordt een "trap-door one-way function" genoemd [5]. "One-way" omdat de functie in de ene richting heel gemakkelijk te berekenen is en in de andere richting zeer moeilijk; "trap-door" (valluik) omdat de inverse functie met de enige geheime (de geheime sleutel D) informatie zeer eenvoudig is. Heeft de functie ook de mogelijkheid tot signeren dan wordt ze "trap-door one-way permutation" genoemd.
Dit wordt wel samengevat met (zie [6]): een public key cryptosysteem is een verzameling valluiken.
Het ontwikkelen van een public key cryptosysteem start met het zoeken naar geschikte one-way functions (of permutations) waarin een trap-door kan worden ingebouwd.
In 1977 werden er tussen geleerden van Stanford en M.I.T. $100 weddenschappen afgesloten met betrekking tot het breken van trap-door one-way functions (die van M.I.T. is een permutation). Inmiddels veelbesproken is het innen van een $100 cheque door Shamir, een Israëli, die in 1982 de trap-door one-way function van Stanford kraakte.
Hiermee is het public key concept echter niet van de aardbodem weggeveegd. De geheime codes zullen in de toekomst nog verbeterd worden. Bovendien is de trap-door one-way permutation van M.I.T. waar Shamir zelf aan heeft meegewerkt nog steeds niet gekraakt.

5. Tegenmaatregelen bedreigingen

In dit hoofdstuk zullen maatregelen worden beschreven tegen de bedreigingen die in hoofdstuk 2 zijn gepresenteerd. Hierbij zal worden uitgegaan van end-to-end protocollen; met name zal worden uitgegaan van DES.

Vrijkomen berichtinhoud

Het gedeelte van het bericht wat door encryption kan worden beschermd hangt af van de laag waarin encryption wordt toegepast. Echter encryption in de netwerklaag in plaats van in de transportlaag geeft geen extra beveiliging daar de informatie in de netwerklaag door zijn aard (namelijk met betrekking tot netwerk adressering en identificatie van de ontvanger) zichtbaar moet zijn voor het netwerk. De transportlaag is dus de laagste laag waarin we end-to-end encryption kunnen toepassen.

Zoals reeds in hoofdstuk 4 is aangegeven is bij ECB het risico dat de crypto-analist er in slaagt de sleutel te vinden relatief groot omdat identieke blokken klare tekst een identieke cijfertekst opleveren.

Bij CBC is dit probleem opgelost. De vercijferde tekst is een functie van alle voorgaande blokken. Hierdoor levert hetzelfde blok klare tekst in verschillende berichten een verschillende cijfertekst op. Alleen twee geheel identieke berichten (alle blokken moeten dan in dezelfde volgorde worden aangeboden) leveren hetzelfde resultaat op. Dit probleem kan worden opgelost door ieder bericht (dat met dezelfde sleutel wordt vercijferd) met een andere prefix (bijvoorbeeld een oplopend volgnummer) of Initial Vector te laten beginnen (een en ander is dan nog afhankelijk van het feit of de blokken al dan niet in de juiste volgorde aankomen).
Hierdoor wordt de vercijferde tekst van het eerste blok en daardoor van alle opvolgende blokken uniek.

Bij CFB is de problematiek nog iets gecompliceerder dan bij CBC. Hiervoor verwijzen wij naar [1].

Analyseren berichtenverkeer

Om analyse van het berichtenverkeer tegen te gaan moeten frequentie, lengte en afzender/bestemming patronen worden verborgen. Zoals reeds eerder is aangegeven is dit bij link encryption technieken geen probleem aangezien daar het hele bericht vercijferd kan worden. Dit is niet zo bij end-to-end technieken. Host-level patronen zullen altijd zichtbaar blijven (het laagste niveau waarop bij end-to-end technieken encryption kan worden toegepast is de transportlaag). Hetzelfde geldt globaal voor frequentie en lengte patronen. In de meeste gevallen is het toepassen van encryption op de transportlaag een voldoende beveiliging. Wordt dat echter onvoldoende geacht dan zouden eventueel dummy-berichten kunnen worden toegevoegd in het berichtenverkeer. Dit zou echter een aanzienlijke extra belasting voor het netwerk betekenen. Samenvattend kan worden gezegd dat maatregelen tegen het analyseren van de berichtenstroom wel mogelijk zijn doch boven een bepaald niveau omslachtig en kostbaar worden.

Wijzigen berichtenstroom

Deze bedreigingen kunnen worden onderverdeeld in bedreigingen met betrekking tot: integriteit, authenticiteit en ordening.
Integriteit houdt in dat een bericht niet wordt gewijzigd gedurende het transport in het netwerk. Authenticiteit houdt in dat het bericht daadwerkelijk is verzonden door de entiteit die men aan de andere kant van de verbinding veronderstelt. Ordening houdt in dat van alle blokken waaruit een bericht bestaat de juiste plaats kan worden bepaald.

Applicatieprogramma's kunnen zelf ook maatregelen nemen tegen het wijzigen van de berichtenstroom. Beveiligingen in het protocol maken het echter overbodig dat iedere applicatie alles zelf moet controleren. Dit laatste zou een niet geringe belasting betekenen bij het ontwikkelen, wijzigen, testen etc. van de applicaties.
Het verdient derhalve de voorkeur de maatregelen tegen het wijzigen van de berichtenstroom in het protocol op te nemen.

De integriteit van berichten kan worden gewaarborgd door ieder blok een error detection code mee te geven. Hiermee zouden wijzigingen aan de vercijferde tekst kunnen worden gedetecteerd (en met behulp van een error correcting code zelfs kunnen worden hersteld); op deze wijze kunnen actieve aanvallen worden ontdekt. Een probleem waar bij een dergelijke code rekening mee moet worden gehouden is de voortzetting van een verandering in een bit van de vercijferde tekst in de ontcijferde tekst. Bij sommige encryption technieken kan namelijk een wijziging in een bit van de vercijferde tekst 50% van de bits in de ontcijferde tekst wijzigen.
Een error detection code alleen is te weinig. Bij opzettelijke inbraken zou de code opnieuw kunnen worden berekend. Daarom moet de error detection code altijd in samenhang worden gezien met de toegepaste encryption techniek.

Berichtenauthenticiteit kan worden gewaarborgd door iedere verbinding tussen een zender en een ontvanger een unieke identificatie en richtingsindicator (in verband met hertransmissie van blokken met een juist volgnummer die eerder in de tegenovergestelde richting zijn verzonden) toe te kennen. Indien voor iedere verbinding een verschillende vercijferingssleutel wordt gebruikt houdt dit impliciet een unieke identificatie in. Indien meerdere verbindingen dezelfde sleutel gebruiken, moet binnen die groep van gebruikers nog een locale identificatie worden toegepast. Het gebruik van een aparte sleutel voor iedere verbinding kan worden toegepast in een public key distributiesysteem. Een andere benadering zou zijn om iedere verbinding met een aparte Initialisatie Vector te laten starten.

Berichtordening kan worden gewaarborgd door aan ieder blok een uniek volgnummer toe te kennen. Hierbij treedt een probleem op indien het hoogste volgnummer is bereikt. Dit kan worden opgelost door:
1. een voldoende groot veld voor het volgnummer te nemen, dit kost echter veel ruimte, of een variabel veld;
2. een nieuwe identificatie toe te kennen aan de verbinding en opnieuw met nummeren te beginnen. In plaats van een nieuwe identificatie zou men ook een nieuwe sleutel aan de berichtenstroom kunnen toekennen. Hierdoor wordt automatisch verzekerd dat een sleutel slechts een beperkt aantal malen wordt gebruikt.

Berichtenauthenticiteit steunt op maatregelen die zijn genomen ten aanzien van berichtintegriteit. Berichtordening steunt op maatregelen die zijn genomen ten aanzien van berichtintegriteit en -authenticiteit.

Vertragen en blokkeren van berichten

Om te ontdekken of berichten worden geblokkeerd of vertraagd is er een request-response mechanisme nodig waarmee periodiek wordt gekeken of het pad waarover het transport plaatsvindt nog open is. Dit mechanisme kan worden geïmplementeerd in de transport of een hogere layer.
Voor het request-response mechanisme is aan iedere zijde van de verbinding een timer nodig die periodiek een request verzendt.
Blijft de response uit dan moet actie worden genomen.

Heimelijk initiëren van een verbinding

Hieronder vallen:
- het initiëren van een verbinding onder een valse identiteit;
- hertransmissie van een reeds verzonden berichtenstroom.

Het vercijferen van de berichten geeft een zekere mate van authenticiteit omdat alleen de zender en ontvanger de sleutel (behoren) te kennen. Bij public key systems kan er zelfs een signering plaatsvinden door de zender. Hier komt echter weer het probleem van het sleutelbeheer en -distributie om de hoek kijken.

Hertransmissie van reeds verzonden berichtenstromen kan worden voorkomen door middel van verificatie dat de verbinding in real-time wordt gelegd. Hierbij kan gebruik worden gemaakt van een challenge-response mechanisme (equivalent aan het request-response mechanisme). Dit mechanisme moet worden toegepast voordat de echte verzending begint. Iedere zijde van de verbinding moet hierbij aan de andere zijde een "challenge-bericht" (bijvoorbeeld de tijd) verzenden. Hierop moet worden geantwoord (response met een transformatie op het challenge-bericht).

Onderdeel praktijk: het S.W.I.F.T.-netwerk

1. Doel en functies van S.W.I.F.T.

S.W.I.F.T. is de afkorting van "Society for Worldwide Interbank Financial Telecommunication", een internationale coöperatie van banken gevestigd in La Hulpe (België). Deze organisatie heeft tot doel het opzetten en onderhouden van een telecommunicatienetwerk ten behoeve van het ontvangen, tijdelijk vastleggen, doorleveren en afleveren van berichten in een standaardformaat ten behoeve van de bij de coöperatie aangesloten banken.
Er zijn per juli 1984 1529 banken bij de coöperatie aangesloten verdeeld over 39 landen.

Het huidige S.W.I.F.T.-netwerk is uit de volgende componenten samengesteld:
- schakelcentra;
- internationale lijnverbindingen;
- concentrators;
- het S.W.I.F.T.-applicatiesysteem;
- besturingsprogrammatuur;
- lijnverbindingen naar de banken.

De te verzenden berichten van de banken worden per land verzameld met behulp van de concentrators.
Het schakelcentrum ontvangt berichten van concentrators, voert tests uit op het formaat en bestaanbaarheid van de bestemming, bepaalt de routing en verricht de functie van tijdelijke opslag van de berichten voor navraagdoeleinden.

Het huidige S.W.I.F.T.-systeem wordt ultimo 1985 geleidelijk vervangen door een nieuw systeem: SWIFT-II. De architectuur van dit systeem is volgens het OSI-model opgezet.

Het SWIFT-II systeem wordt samengesteld uit een hypernetwerk van slices onder supervisie van twee System Control Centres (SCC).

Een slice is een verzameling elementen die in staat zijn om, in geval van een periode van isolatie van de andere slices, hun locale functies uit te voeren zonder onderbreking van de locale gegevensverwerking.

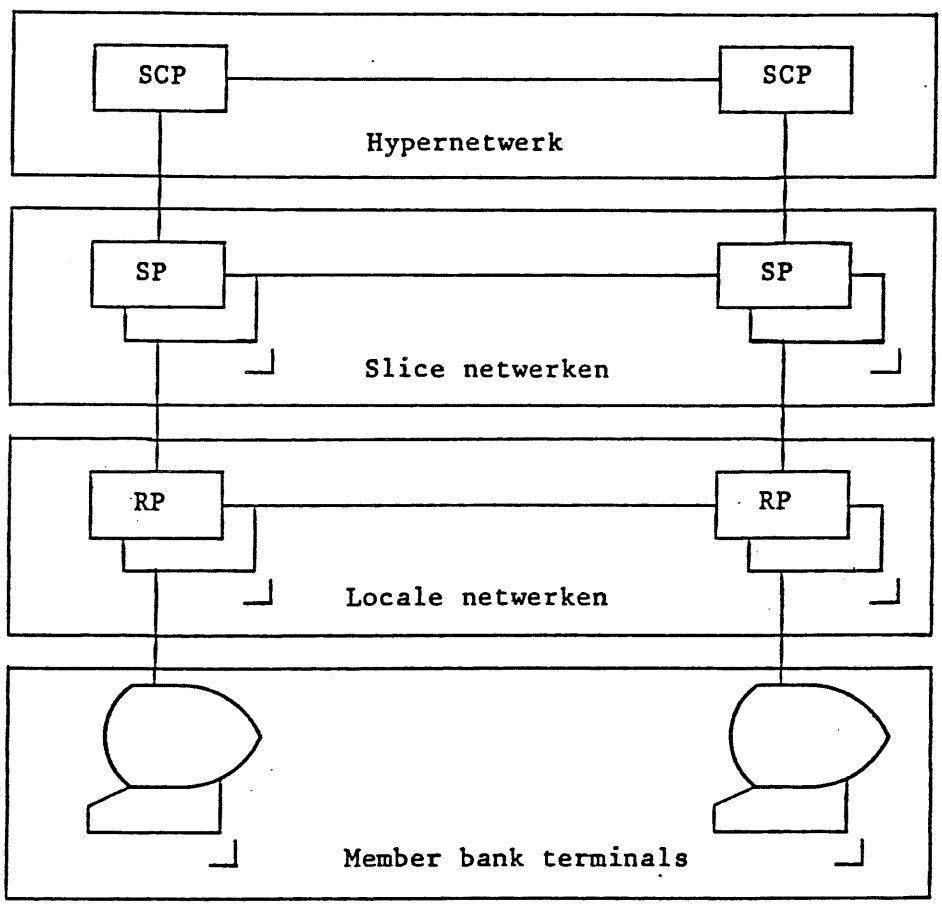
Een slice is samengesteld uit:
- een Slice Processor (SP) voor de uitvoering van de transactieverwerking;
- een of meer Regional Processors (RP) voor het omzetten van locale protocollen naar de SWIFT-protocollen;
- een Slice Network (SN) voor het verbinden van de SP met de RP's.

De SP's worden op de locaties van de SCC's geïnstalleerd.

De besturing van een SN wordt uitgevoerd door een System Control Processor (SCP).

De slices worden met elkaar verbonden via een hypernetwerk onder besturing van de SCP's, die op de locaties van de SCC's worden geïnstalleerd en bediend.

De SCC's zijn gepland om de enige bemande centra van het systeem te worden.



Overzicht SWIFT-II-systeem

2. Het OSI-model en S.W.I.F.T.

Het ISO referentiemodel voor Open Systems Interconnection beschrijft een geordende set van subsystemen voor datacommunicatie.

In dit hoofdstuk wordt een uiteenzetting gegeven over security voorzieningen zoals deze zijn opgenomen in het S.W.I.F.T.-netwerk. De uiteenzetting beperkt zich tot de lagen 7 tot en met 4 van het OSI-model. Hierbij ligt het accent op de end-to-end voorzieningen.

Een aantal van de principes en uitgangspunten van de huidige voorzieningen blijft in de application layer van het nieuwe systeem gehandhaafd.

De bestaande voorzieningen van het huidige S.W.I.F.T.-systeem zijn beschreven bij laag 7 (application layer hoofdstuk 3). Hierbij is tevens aangegeven welke functies in de application layer ten behoeve van het nieuwe SWIFT-II-systeem worden opgenomen.

Laag 6 (presentation layer) is voor S.W.I.F.T. niet van toepassing omdat uitsluitend berichten in standaardformaat worden verwerkt. Van de mogelijkheid die het OSI-model biedt om in deze laag gebruik te maken van end-to-end vercijfering voor het gegevenstransport wordt geen gebruik gemaakt.

Laag 5 (session layer) is voor S.W.I.F.T. niet van toepassing omdat de voorzieningen in laag 4 vooralsnog voldoende zijn voor de geplande toepassingen. Een toepassing die aanvullende ondersteuning van de session layer behoeft betreft: file-transfer.

De functies en security voorzieningen zoals deze zijn gepland voor laag 4 van het nieuwe SWIFT-II-systeem zijn beschreven bij de transport layer (hoofdstuk 4).

3. Functies en security-voorzieningen in de application layer

In de application layer worden ten behoeve van het nieuwe SWIFT-II system onder andere de volgende functies opgenomen:

a. In de member bank user processen:
   - verzoek voor het starten en stoppen van sessies;
   - genereren van ISN-volgnummers;
   - controleren van OSN-volgnummers;
   - zenden van transacties;
   - ontvangen van transacties;
   - zenden van bevestigingen voor ontvangst;
   - genereren van controletotalen;
   - controleren van controletotalen;
   - uitvoering van resynchronisatie.

b. In de SWIFT-II gedistribueerde systeemprocessen:
   - controleren van sessie-parameters;
   - ontvangen en vastleggen van transacties;
   - sessie-uitvoering;
   - controle ISN-volgnummers;
   - genereren van OSN-volgnummers;
   - zenden van transacties;
   - controleren van controletotalen;
   - acceptatie van berichten;
   - zenden van bevestiging voor ontvangst;
   - afwijzen van berichten;
   - uitvoering van resynchronisatie.

3.1 Log-in/log-out-procedure

Om te voorkomen dat berichten door anderen dan de aangesloten banken worden verzonden of ontvangen, worden door de S.W.I.F.T.-organisatie log-in-tabellen aan de banken beschikbaar gesteld. Met behulp van de in de tabellen vastgelegde codes wordt toegang verkregen tot het S.W.I.F.T.-netwerk.
Indien zich gedurende de berichtenuitwisseling onregelmatigheden voordoen wordt de verbinding met het S.W.I.F.T.-netwerk vanuit de S.W.I.F.T.-organisatie verbroken (automatische log-out). Voor de log-in-tabellen wordt onderscheid gemaakt in drie sets van tabellen:
- normal table;
- fallback table;
- emergency table.

In het algemeen wordt gebruik gemaakt van de normal version van de log-in-tabel. Deze tabel bevat 600 codes en dient steeds door de bank te worden besteld. Als na bestelling niet op tijd een nieuwe tabel wordt ontvangen en ook wanneer de normal table in het ongerede mocht zijn geraakt, kan de emergency table worden gehanteerd.

Voor bijzondere gevallen, bijvoorbeeld uitvallen van de lijnverbinding of storing in een schakelcentrum wordt gebruik gemaakt van de fallback table, om toegang te krijgen tot een ander schakelcentrum.

Elke set tabellen bestaat uit twee delen die te zamen de sequence nummers en de daarbij behorende log-in-keys vormen voor de log-in-procedure.

Bij de log-in-procedure kan gebruik worden gemaakt van de time-option. Hierdoor is het mogelijk om vooraf afspraken te maken op welke tijdstippen de gegevensuitwisseling zal plaatsvinden.

Tevens kan gebruik worden gemaakt van de state-option. Hierdoor is het mogelijk om vooraf afspraken te maken over het ontvangen en/of verzenden van berichten.

In het SWIFT-II-systeem wordt gebruik gemaakt van het toekennen van sessienummers per log-in of poging tot log-in. Met behulp van deze voorziening wordt een controleerbare vastlegging gecreëerd van pogingen tot inbraak in het systeem.

3.2 ISN/OSN volgnummers van transacties

Om de volledigheid van de berichtenoverdracht tussen een bank en het S.W.I.F.T.-netwerk te kunnen vaststellen wordt gebruik gemaakt van ISN-OSN-volgnummercontrole.

Input Sequence Numbers (ISN)
De bankorganisatie dient haar uitgaande berichten te voorzien van een volgnummer dat door S.W.I.F.T. wordt gecheckt op aansluiting. Onjuist genummerde berichten worden niet geaccepteerd. Indien door S.W.I.F.T. wordt geconstateerd dat berichten niet met een opeenvolgend ISN worden ontvangen, wordt hiervan melding gemaakt en dienen, afhankelijk van de foutsituatie, door de bankorganisatie acties te worden genomen.

Output Sequence Numbers (OSN)
S.W.I.F.T. kent aan ieder bericht dat aan een bankorganisatie wordt verzonden een volgnummer toe. De nummeraansluiting van inkomende berichten van het S.W.I.F.T.-netwerk naar de bankorganisatie dient door de bankorganisatie te worden vastgesteld. Indien wordt geconstateerd dat er berichten met een niet opeenvolgende OSN worden ontvangen, dienen afhankelijk van de aard van de foutsituatie acties door de bankorganisatie te worden genomen.

3.3 Acceptatie van berichten

Ieder bericht dat wordt ingevoerd, wordt door het systeem op geldigheid gecheckt. Ter zake van de feitelijke inhoud van het bericht wordt alleen nagegaan of de indeling overeenkomt met de gestandaardiseerde vereisten. Bij non-acceptatie wordt een foutmelding afgegeven met omschrijving van de aard der fout, waarna het bericht in verbeterde vorm weer kan worden ingevoerd.
Berichten met fouten worden nimmer via het netwerk naar de gebruiker/ontvanger doorgezonden.
Indien het bericht is geaccepteerd, volgt een erkenning (logical-acknowledgement) ten teken van correcte invoer.

3.4 User-to-user ontvangstbevestiging

De te verzenden berichten dienen van een prioriteitscode te worden voorzien. Deze code is bepalend voor het type bevestiging dat zal worden verstuurd. De volgende codes worden gehanteerd:

Prioriteit 01: Spoedbericht, waarbij de zendende bank een bevestiging voor aflevering ontvangt en eventueel een waarschuwing indien aflevering van een bericht niet binnen 15 minuten kan plaatsvinden.

Prioriteit 02: Normaal bericht, waarbij de zendende bank geen bevestiging voor aflevering ontvangt en eventueel wel een waarschuwing indien aflevering niet binnen 15 minuten kan plaatsvinden.

Prioriteit 11: Spoedbericht, waarbij de zendende bank alleen een waarschuwing ontvangt indien aflevering niet binnen 15 minuten kan plaatsvinden.

Prioriteit 12: Normaal bericht met een bevestiging voor aflevering aan de zendende bank.

Indien geen prioriteit wordt opgegeven wordt prioriteit 02 toegekend.

3.5 User-to-user authenticator-key-procedures

Om de rechtmatige herkomst van de ontvangen berichten te kunnen vaststellen wordt gebruik gemaakt van de authenticator-key-procedures. Deze procedures zijn uit de volgende elementen samengesteld:

- een authenticator-key;
- de inhoud van een bericht;
- een algoritme;
- een authenticator-key-resultaat.

Authenticator-keys worden tussen banken onderling uitgewisseld. Met behulp van de authenticator-key en de inhoud van een bericht wordt door het algoritme een authenticator-key-resultaat bepaald. Dit resultaat wordt aan het te verzenden bericht toegevoegd door de zendende bank. Bij ontvangst dient de procedure te worden herhaald door de ontvangende bank. Hierbij dient vervolgens het berekende resultaat te worden vergeleken met het bij het bericht vastgelegde resultaat. Met de uitvoering van deze procedure worden tevens eventuele vermin-king, verschuiving of verlies van gegevens ontdekt door de ontvanger.

Een nieuwe methode ten behoeve van het vaststellen van de rechtmatige herkomst van berichten is thans in voorbereiding voor SWIFT-II.

3.6 Opslaan en opvragen van berichten

De berichten worden gedurende 14 dagen op de magneetschijven van de schakelcentra opgeslagen. De berichten zijn gedurende deze tijd direct toegankelijk voor degene die ze heeft geïnitieerd.
De 15e dag worden de berichten op magneetband opgeslagen. Gedurende een periode van 4 maanden kunnen berichten dan nog slechts worden geraadpleegd.
De berichten worden in vercijferde vorm opgeslagen.

3.7 Resynchronisatie

Het SWIFT-II-systeem bevat een resynchronisatie-mechanisme dat bijvoorbeeld in werking treedt indien een aantal ISN's of OSN's niet worden bevestigd. Dit mechanisme kan door een member bank gebruikersproces of een S.W.I.F.T.-systeemproces worden opgestart. De informatie die bij dit mechanisme wordt uitgewisseld geeft aan welke controle-informatie (onder andere ISN en OSN) bij het hervatten van de berichtenuitwisseling gebruikt moet worden.
Deze voorziening beoogt de noodzaak voor het creëren van duplicaten van berichten te voorkomen.

4. Functies en security-voorzieningen in de transport layer

In de transport layer worden ten behoeve van het SWIFT-II-systeem onder andere de volgende functies opgenomen:
- starten van transportsessies;
- beëindigen van transportsessies;
- end-to-end flow control;
- berichten segmentatie;
- reassembly van berichten;
- end-to-end error control.

4.1 End -to-end flow control

De ontvanger beschikt over de mogelijkheid om de omvang van het berichtenverkeer van de zender te beperken. Deze mogelijkheid is gebaseerd op een credit-mechanisme. De ontvanger voorziet de zender van krediet voor het zenden van berichten afhankelijk van zijn beschikbare bufferruimte.

4.2 End-to-end sequencing

Voor het geval dat de omvang van de berichten of de netwerk-packets verschillen wordt segmentatie of reassembly toegepast.

In dit subsysteem worden voorzieningen opgenomen die dienen te garanderen dat de berichten worden afgeleverd aan de ontvanger in dezelfde volgorde als ze zijn verzonden aan de transport layer door de zender.

Elk blok van een bericht wordt geïdentificeerd met twee volgnummers:
- het nummer van het blok binnen het bericht;
- het nummer van het bericht waar het blok bij behoort.

De ontvanger onderhoudt een teller waarin het eerste volgnummer van een segment dat wordt verwacht wordt opgeslagen.

4.3 End-to-end error control

Indien segmenten van berichten worden ontvangen die niet aan de verwachte volgorde voldoen, worden deze berichten in de transport layer - indien mogelijk - in de juiste volgorde gerangschikt.

Indien segmenten niet in een juiste volgorde kunnen worden gerangschikt, worden deze genegeerd. In deze situatie dient hertransmissie plaats te vinden.

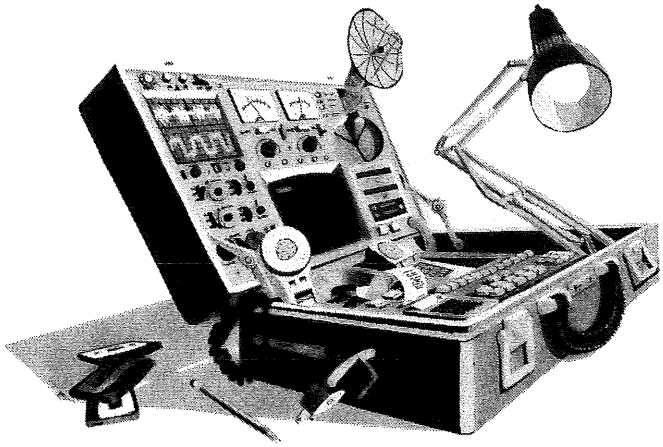
5. Link-to-link-vercijfering van het gegevenstransport

Voor het gegevenstransport binnen het SWIFT-II-systeem zal vercijfering worden toegepast. Voor het gegevenstransport tussen de member banken en het SWIFT-II-systeem kan door de banken desgewenst vercijfering worden toegepast.

Literatuurlijst

[1] V.L. Voydock en S.T. Kent, "Security Mechanisms in High-Level Network Protocols," Computing Surveys, Vol. 15, No. 2, June 1983.
[2] D.M. Nesset, "A Systematic Methodology for Analyzing Security Threats to Interprocess Communication in a Distributed System," IEEE transactions on communications, Vol. com-31, No. 9, September 1983.
[3] H.C.A. Tilborg, "Inleiding cryptosystemen," Cursus Cryptografie, Mathematisch Centrum, Amsterdam 1983.
[4] P.J. Hoogendoorn, "Public key cryptografie," Cursus Cryptografie, Mathematisch Centrum, Amsterdam 1983.
[5] R.L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, January 1983, Vol. 26, No. 1.
[6] A.E. Brouwer, "De Data Encryption Standard," Cursus Cryptografie, Mathematisch Centrum, Amsterdam 1983.

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



DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

Het is al weer bijna een half jaar geleden dat wij u berichtten over de invoering van de microcomputer in de KKC-controlepraktijk. Wat is er nu gebeurd sinds die vermaarde negentiende juni, toen de eerste dertig Hyperion micro's aan de microbeheerders werden meegegeven.
Ik moet u zeggen: heel wat!
Op de eerste plaats is het aantal draagbare microcomputers bij KKC in de afgelopen periode de honderd gepasseerd. Dit komt er in concreto op neer dat op iedere vestiging in Nederland momenteel minimaal één, maar meestal een groter aantal draagbare microcomputers beschikbaar is.
Vertellen wat er allemaal kan op zo'n micro zou wat te ver voeren, maar wat er door ons KKC'ers op gedaan wordt is mijns inziens wel vermeldenswaard.
Het meest populair is het geautomatiseerde 14-kolommenpapier, ook wel spreadsheet genoemd. Met het programma, dat daarvoor beschikbaar is gekomen, namelijk Multiplan, zijn ondertussen al legio toepassingen gerealiseerd. Om KKC Multiplan te leren, is een tweedaagse cursus ontwikkeld, welke in de eerste helft van dit jaar aan iedere microbeheerder is gegeven.
De microbeheerders hebben vervolgens, met de opgedane kennis gewapend, de "rest van Nederland" opgeleid. De mate waarin deze spreadsheet-opleiding is gevorderd, varieert per vestiging.
Maar, zult u zeggen, hoe zit het nou met dat bestandsonderzoekprogramma van je?
Goed dat u dat vraagt: dan zal ik daar nu wat meer over vertellen.
Dat programma FAT (File Analysis Tool), hetwelk door de AC-microgroep van KKC speciaal voor de accountantscontrole is ontwikkeld, groeit gestadig. Evenals trouwens de hoeveelheid toepassingen. Gebleken is dat, nu de Multiplan-opleiding achter de rug is, men ook eens voorzichtig wil proberen hoe dat FAT nu eigenlijk werkt.

Uit de reacties van de microbeheerders, welke het afgelopen najaar voor de eerste maal bijeen zijn geweest, blijkt dat, door gebrek aan een goede FAT-opleiding, de mogelijkheden van het pakket niet voldoende bekend zijn. Hierdoor moet nog regelmatig door de AC-kern worden bijgesprongen tijdens het ontwikkelen van toepassingen. Wij hopen dat hier in 1985 verandering in zal komen.

Hieronder een voorbeeld van een bestaande FAT-toepassing:
een cliënt is bereid haar grootboekmutaties maandelijks op een diskette te zetten. Deze diskette wordt verzonden naar kantoor Amsterdam, waar de diskette wordt omgezet naar het door onze micro te lezen formaat. De diskette wordt vervolgens teruggestuurd, waarna de controleploeg het bestand met FAT te lijf gaat. Allereerst vindt controle op volledigheid plaats, of wel: "heeft de klant ons wel het goede bestand geleverd". In dit geval wordt een saldibalans uitgedraaid om deze controle uit te kunnen voeren. Vervolgens wordt per dagboek een matrix vervaardigd van de saldi per rekening; daar op deze lijst een aantal maanden naast elkaar worden afgedrukt, is ze uiterst geschikt ten behoeve van cijferbeoordeling. De uiteindelijke selectie van "interessante posten" vindt hierna plaats. In ons geval wil de controle alle investeringen boven de f 10.000,-- zien, evenals een overzicht van de bijzondere baten en lasten.

Wat zegt u? u wist niet dat dat allemaal kon?
In dat geval adviseer ik u contact op te nemen met uw microbeheerder, zodat ook u effectiever kunt controleren en de kwaliteit van de controle kunt verhogen.

Tenslotte nog wat nieuws over de activiteiten van de AC-microgroep.
De groep zal vanaf januari 1985 uit 16 personen bestaan. De helft hiervan is in dienst van KKC, terwijl de rest bij KKC stage loopt of, als logisch gevolg van een eerdere stage, bij ons afstudeert.
Door deze groei is een verdere professionalisering van de ontwikkelomgeving een pure noodzaak geworden. Daartoe zijn strakke programmeringsprocedures opgesteld, waarvan de naleving geautomatiseerd wordt gecontroleerd.
Tevens is afgestapt van de IBM-PC als ontwikkelcomputer. Momenteel wordt met meer terminals aan één multi-user-computer gewerkt. De computer is voorzien van het UNIX-besturingssysteem, waaronder alle software-gereedschappen als editors, compilers, debuggers en bibliotheken voorhanden zijn. Wat snoevend kan ik dit melden omdat ook pakketten als LOTUS en Symphony op een dergelijke wijze worden ontwikkeld.

Herfst 1984

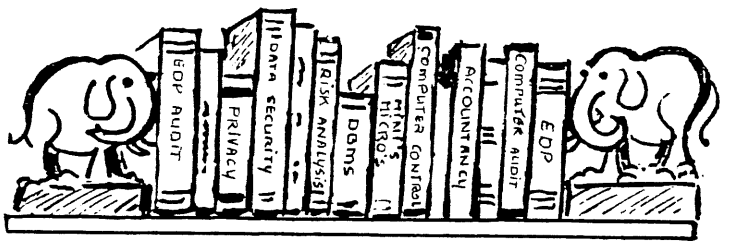
Er wordt gewerkt in projectgroepen, waarvan de volgende vermeldenswaard zijn:

FAT: het verder uitbreiden van het bestandsonderzoekprogramma;

FCT: het ontwikkelen van het File Conversion Tool. Met behulp van dit pakket zal disketteconversie niet langer door specialisten hoeven gebeuren;

APS+: het volledig automatiseren van de schematechniek voor het in beeld brengen van organisaties en het ondersteunen bij de beoordeling van die organisatie.

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



Boeken

Boekbespreking
Titel: The IBM-PC in the Corporation
Xephon User Survey
Uitgegeven door: Xephon Technology Transfer LTD
September 1984
Aantal bladzijden: 44, prijs: £ 30
Besproken door: J.C. Boer

Het rapport is te splitsen in twee delen. Het eerste deel betreft een korte beschrijving van de IBM-PC hardware en de beschikbare software. Deze beschrijving wordt gevolgd door de uitwerking van een schriftelijke enquete onder de gebruikers van IBM-mainframes in Europa (hoofdzakelijk Groot Brittannië).

De algemene beschrijving van de hardware (PC, PC XT, PC XT/370, 3270 PC) wordt afgesloten met de conclusie, dat de architectuur geen revolutionaire zaken in zich heeft. Alleen ten aanzien van de 3270 PC wordt opgemerkt, dat dit een machine is met een eigen identiteit. De 3270 PC was echter op het moment van de enquete niet algemeen verkrijgbaar.
Uit de inleiding blijkt, dat volgens Xephon het markt succes van de IBM-PC voortkomt uit de voorkeur van de automatiseringsafdelingen om de PC's van de mainframe-leverancier af te nemen. Hierbij spelen (verwachte) koppelingsmogelijkheden met het mainframe en de verwachting dat IBM zich tot een standaard in PC zal ontwikkelen een rol. Tot het moment, dat de IBM-PC op de markt verscheen zijn de centrale automatiseringsafdelingen weinig betrokken geweest bij het gebruik van PC in de organisatie. De introductie van de IBM-PC is ervaren als het beschikbaar komen van een betrouwbare machine die een onderdeel vormt van de totale geautomatiseerde informatieverwerking binnen de onderneming.

De weergegeven onderzoekresultaten zijn gebaseerd op een schriftelijke enquete waarop 53 Europese IBM-mainframe-gebruikers hebben gereageerd (waarvan 39 uit Groot Brittannië).

De vraagstelling richtte zich op de wijze waarop grote organisaties die gebruik maken van een IBM-mainframe omgaan met Personal Computers. De enquete had betrekking op:

- de penetratie van de PC binnen de organisatie. Naast de huidige situatie had de enquete ook betrekking op de verwachting ten aanzien van de komende 5 jaar;
- de kwaliteit van de PC. Uit dit onderdeel komen de sterke en de zwakke punten van het PC gebruik naar voren, zoals deze ervaren zijn door de ondervraagde bedrijven;
- de PC-hardware-configuratie. De informatie die uit deze vragen naar voren komt heeft betrekking op de combinaties van IBM hardware met de hardware van onafhankelijke fabrikanten en de verbinding met andere systemen (vooral de gebruikte printers blijken dikwijls niet van IBM afkomstig te zijn);
- de "compatibility" met andere PC's. Op deze vraag zijn zeer uiteenlopende antwoorden gegeven. Op de problemen wordt echter niet in detail ingegaan;
- de applicaties. Uit de antwoorden blijkt, dat meer dan 50% van de gebruikers geen gebruik maakt van programmeertalen. Deze gebruikers maken slechts gebruik van applicatiepakketten (bijvoorbeeld Lotus 1-2-3);
- het bedrijfsbeleid.

Uit de reacties op de laatste groep vragen blijkt dat indien er sprake is van een beleid, dit over het algemeen betrekking heeft op de selectie van PC's. Een beleid gericht op het dagelijks gebruik van de PC's is slechts in beperkte mate gedefinieerd. Slechts 20% van de geënqueteerde bedrijven heeft beleidsrichtlijnen ten aanzien van het muteren van data opgeslagen onder beheer van het mainframe.
Wanneer ik deze bevinding combineer met de verwachting, dat in 1989 80% van de geplaatste PC's zal communiceren met het mainframe dan blijkt de noodzaak tot het spoedig formuleren van beleidsrichtlijnen ten aanzien van gebruik van PC's. Het uitblijven van een beleid ten aanzien van het gebruik zal ondermeer leiden tot een aantasting van één van de fundamenten onder een - uit het gezichtspunt van interne controle en beveiliging - betrouwbare informatieverwerking.

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

TIJDSCHRIFTEN

Herfst 1984

Evaluating the Risks of Computer Fraud and Error
Andrew D. Warren
Computers & Security 2, 1983

In dit artikel wordt een nieuwe methode beschreven voor de evaluatie van fraude- en foutenrisico's in computersystemen.

Samenvatting

Veel oudere methoden voor de evaluatie van fraude- en foutenrisico's zijn volgens Warren ineffectief en kosten te veel tijd. Dit komt doordat de ontwikkeling van de methoden niet in de pas gebleven is met de ontwikkeling van de techniek.
In het onderhavige artikel wordt een alternatieve evaluatiemethode beschreven.

De redenen van een nieuwe benaderingswijze:
1. De voortgaande ontwikkeling van steeds ingewikkelder systemen voor algemeen toepasbaar gebruik.
2. Veel bestaande technieken zijn niet fijn genoeg voor de evaluatie van de controles.
3. Er is behoefte aan methodes die efficiënt uit te voeren zijn.

De doelstellingen van de nieuwe methode zijn:
- de methode dient geschikt te zijn voor alle soorten computersystemen;
- een sluitende evaluatie voor de beoordeling van fraude- en foutenrisico's dient te worden bereikt;
- de methode moet doelmatig zijn voor het bereiken van een betere communicatie tussen EDP-accountants en algemeen accountants.

De methode is gebaseerd op de schatting van fraude- en foutenrisico's voor financiële systemen die zijn geautomatiseerd.

Bij het onderzoek van het financiële systeem wordt onderscheid gemaakt tussen administratieve functies.
Voor het opsporen van de risico's moet worden nagegaan hoe de administratieve functies en de beheersfuncties verdeeld zijn over de gebruiker en de computer.

Voor een goede schatting van de fouten- en frauderisico's is het nodig dat wordt nagegaan waar in het systeem gesteund wordt op de automatisering voor administratieve of beheersfuncties.
Hierop wordt de controlebenadering van het systeem gebaseerd.
Voor de beoordeling van risico's dient er een helder inzicht te zijn in de wijze waarop het financiële systeem afhankelijk is van de computer.
Ofwel voor welke functies vertrouwt men op het geautomatiseerde systeem voor een foutloze uitvoer van die functie zonder bloot te staan aan ongeautoriseerde beïnvloeding. Warren noemt deze functies EDP dependent.
Voor het onderkennen van risico's wordt gezocht naar EDP dependent functions omdat daarop volledig vertrouwd wordt.
De EDP dependent functie kan ook een handmatig uitgevoerde functie zijn, hoofdzaak is dat daarbij gebruik wordt gemaakt van (de uitkomsten van) het geautomatiseerde systeem.

De benaderingswijze voor de evaluatie van de controles in het geautomatiseerde financiële systeem is in drie stappen te verdelen.
Ten eerste het onderzoek van het administratieve systeem voor het onderkennen van EDP dependent functies.
De tweede stap zijnde een voorlopige evaluatie dient om na te gaan of verdergaand onderzoek zinvol is.
De laatste stap omvat de evaluatie van de EDP-procedures en een beoordeling van de toereikendheid van de controles.
Blijkt uit de tweede stap dat een gedetailleerde evaluatie niet zinvol is dan wordt in deze fase gestopt.

Onderzoek van het administratieve systeem begint met het opsporen van de EDP dependent functies. Dit deel van het onderzoek kan door een niet-gespecialiseerde accountant worden verricht omdat alleen aangegeven hoeft te worden welke administratieve en controlefuncties afhankelijk zijn van het geautomatiseerde systeem.
Het verdere onderzoek blijft beperkt tot de EDP dependent functies wat het voordeel heeft dat het aantal onderzoeksgebieden wordt beperkt.
Van de EDP dependent functie wordt vastgesteld of de risico's beheerst kunnen worden binnen de functie. Daarnaast wordt nagegaan of de functie beschermd wordt door een voldoende functiescheiding.
Voor het laatste wordt vastgesteld wie ongecontroleerde toegang hebben tot het gebruik van de EDP dependent functie.
Bij de beoordeling van de toereikendheid van de controles en de toegangsbeveiliging wordt gebruik gemaakt van twee vragenlijsten waarop aangegeven wordt welke personen welke mate van toegang tot het systeem hebben.

Conclusie

De aanpak van Warren wordt uiteindelijk toegespitst op access-controls en de daarop gebaseerde "counter" controls (tegen- of nacontrole). Daarbij gaat hij met name na welke personen toegang hebben tot de EDP dependent functies en door wie deze personen op hun beurt worden gecontroleerd.

> "At the completion of the evaluation of access controls the EDP-auditor is in a position to identify any people who have uncontrolled access to the system or whose duties make them a Sensitive Person."

De activiteiten van een Sensitive Person zullen - aldus Warren - nader moeten worden onderzocht. Hoe dat verder in z'n werk gaat is niet toegelicht.

Op zich is de methode niet nieuw. Ook in de Nederlandse praktijk zijn methoden ontwikkeld waarmee wordt vastgesteld "wie wat mag met welke gegevens" en via een scala van controlemiddelen kan worden nagegaan of handelingen (ook van Sensitive Persons) conform de voorschriften zijn verricht, gerapporteerd en gecontroleerd.

Rejuvenate your old systems
Tools to rejuvenate your old systems
EDP Analyzer (March, April 1984)

De maart en aprilnummers van EDP-analyzer handelen over de mogelijke werkwijzen om tot een verjonging van de verouderde informatieverwerkende systemen te komen. Doordat het automatiseringsbeleid vooral gericht is op de ontwikkeling van nieuwe systemen, raken de oude systemen in verval. Door dit verval is een verantwoord onderhoud niet meer mogelijk. Er komt een moment dat het systeem "versleten" is. Dit kan grotendeels voorkomen worden door een beleid gericht op het bouwen van systemen met een gestandaardiseerde structuur, het beheren van data als activa, het technisch bij de tijd blijven en het actief voeren van een sterk onderhoudsbeleid (dus niet alleen het minimaal noodzakelijke).

Om de oude systemen aan te passen aan de vereisten kan in plaats van het geheel opnieuw ontwikkelen van de systemen gekozen worden voor een verjonging van de huidige systemen. De verjonging (rejuvenation) wordt gedefinieerd als "using an existing system as the basis for a new strategic system".

Om hiertoe te komen worden een viertal fasen doorlopen:
1. vaststellen van de potentiële waarde van het oude systeem voor de onderneming;
2. het oppoetsen van het bestaande systeem (met name op programmaniveau);
3. het efficiënter maken van het systeem;
4. het systeem zijn belangrijke rol binnen de onderneming laten vervullen.

Dit laatste is mogelijk omdat het systeem weer volledig onderhoudbaar is en snel aangepast kan worden aan de veranderende bedrijfsomstandigheden.
De kracht van de verjongingsstrategie is gelegen in de tijdbesparing ten opzichte van de conventionele systeemontwikkeling. De punten waarop de verjonging kan worden gericht zijn:
- het installeren van gekochte pakketten;
- uitbreiding van het bestaande systeem met een:
  - input process,
  - data manipulation process,
  - interactive query capabilities,
  - output process;
- renoveren van het oude systeem door het herstructureren van de coding. In de V.S. is een bedrijf hierin gespecialiseerd. Voor enkele deelfuncties zijn pakketten (tools) op de markt verkrijgbaar;
- iteratief ontwikkelen van het nieuwe systeem.

Commentaar

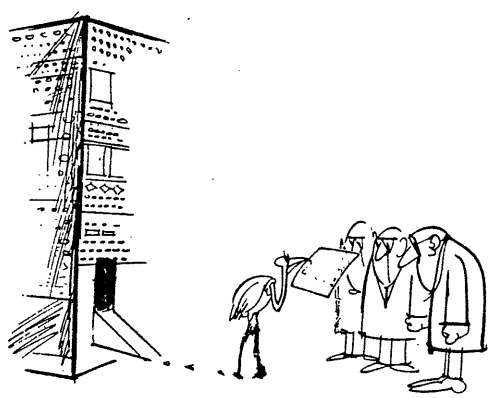
De geschetste werkwijze maakt op ruime wijze gebruik van de mogelijkheden die de vierde generatie talen bieden (prototyping, performance verbetering van programmeurs, inschakeling van de gebruikers). Als kanttekening wordt naar voren gebracht dat de organisatie wel rijp moet zijn voor gebruik van de vierde generatie talen.

Gezien door de bril van de accountant kunnen een tweetal opmerkingen gemaakt worden ten aanzien van het voorgestelde verjongingsproces.

Ten eerste zullen er maatregelen getroffen moeten worden, opdat de in de systemen aanwezige maatregelen van interne controle niet verloren gaan. De uitbreidingen die aan het systeem worden toegevoegd kunnen uitbreiding van de controlestructuur noodzakelijk maken.

De tweede opmerking komt voort uit het gebruik van vierde generatie talen en is niet specifiek verbonden aan de verjonging van het systeem. Het gebruik van vierde generatie talen brengt met zich mee, dat niet-automatiseringsspecialisten zich bezighouden met de programma-ontwikkeling. Door het zich niet realiseren van het belang van geprogrammeerde controles kan het betrouwbaarheidsniveau van de programmatuur aangetast worden. De signalering hiervan door de organisatie is niet gewaarborgd omdat de ontwikkeling over het algemeen niet volgens een fasegewijze methodologie met kwaliteitsbewakingspunten plaats zal vinden (bijvoorbeeld door vervanging functiescheiding tussen de systeemontwikkeling en de gebruikers verliest de acceptatietest aan waarde).

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



COMPACT

Automatisering
Beveiliging
Controle
NIEUWS

Herfst 1984

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

Automatisering

Iedere Nederlander krijgt een administratienummer

Onder deze titel vinden we in de Nederlandse Staatscourant van 23 November 1984 een artikel naar aanleiding van het congres "Gemeenten en informatiebeleid" dat de dag daarvoor werd gehouden. Op dit congres hield de staatssecretaris van Binnenlandse Zaken, de heer Van Amelsvoort, een inleiding over de mogelijke invoering van persoonsadministratienummers ten behoeve van persoonsregisters van de overheid. De staatssecretaris formuleerde het aldus: "gezien vanuit de optiek van het totale persoonsinformatiebeleid denk ik dat het op termijn invoeren en gebruiken van één nummer om doelmatigheidsredenen verreweg de voorkeur verdient".

In zijn toespraak gaf de staatssecretaris aan dat de "oude" wetgeving uit respectievelijk 1887 (Wet op de bevolkings- en verblijfsregistraties) en 1938 (Besluit bevolkingsboekhouding) weliswaar nog steeds bestaan, maar dat er door de invoering van de automatisering bij de gemeenten uiteenlopende oplossingen zijn ontstaan. Dit veroorzaakt onder meer afstemmingsproblemen bij de overdracht van persoonsgegevens tussen de verschillende gemeentelijke administraties en er worden vaak dubbele administraties gevoerd.
Inmiddels is uit diverse inventarisaties en studies een aantal nota's ontstaan, zoals de Structuurschets voor de persoonsinformatievoorziening, de ambtelijke discussienota LBA (Landelijke bevolkingsadministratie) en de notitie GBA (Gemeentelijke Bevolkingsadministratie) welke laatste op 1 november jongstleden door de staatssecretaris aan de tweede kamer is gezonden.
Deze nota's vormen de uitgangspunten voor het Persoonsinformatiebeleid van de overheid. Een aantal hoofdpunten hieruit zijn:
- optimale waarborgen voor de bescherming van de persoonlijke levenssfeer van de burger;
- optimalisering van de toegankelijkheid van de persoonsinformatie;
- optimalisering van de doelmatigheid en doeltreffendheid van de informatie door bundeling van gelijksoortige persoonsinformatie;
- bevorderen van de multifunctionaliteit van de persoonsinformatie (ofwel: voorkomen dat identieke informatie op verschillende plaatsen door verschillende instanties wordt opgeslagen).

Een verdere uitwerking van deze uitgangspunten heeft geleid tot aanbevelingen die neerkomen op een gedecentraliseerde benadering:
- verzameling en beheer van persoonsgegevens zo dicht mogelijk bij de bron;
- de gemeentelijke bevolkingsboekhouding blijft de basisregistratie voor bevolkingsgegevens, hetgeen impliceert dat de gemeenten verantwoordelijk zijn voor het informatiebeheer en dat andere overheidsorganen geen bevolkingsgegevens in eigen beheer zullen verzamelen, indien de voor de uitoefening van hun taken benodigde gegevens op doelmatige wijze kunnen worden betrokken uit de basisregistratie;
- duplicatie van verzameling, vastlegging, verwerking en opslag van persoonsgegevens moet worden voorkomen, tenzij doelmatigheidsredenen dit noodzakelijk maken;
- samenwerking van de betrokkenen op het gebied van persoonsinformatievoorziening is nodig om tot een zo doelmatig en doeltreffend mogelijke organisatie van de informatievoorziening te komen;
- centrale regelgeving voor de vaststelling van de inhoud van de basisregistratie is nodig om de gewenste afstemming van de informatie te waarborgen.

Het beleid inzake de persoonsinformatie zal zich derhalve concentreren op de Gemeentelijke Bevolkingsadministratie (GBA). Getracht is de problematiek nader te regelen met inachtneming van de tekortkomingen op het terrein van de regelgeving.
Samengevat:
- het in de GBA-wet nader regelen van de persoonlijke levenssfeer van de burger met inachtneming van de eisen die gesteld worden in de komende wet op de persoonsregistraties;
- decentraal informatiebeheer;
- automatisering van de Nederlandse bevolkingsboekhouding, waardoor de persoonskaartadministraties overbodig worden;
- informatie-uitwisseling zal volledig geautomatiseerd plaatsvinden met behulp van een datacommunicatienetwerk;
- herziening van de inhoud van de bevolkingsadministratie;
- het vervangen van het huidige, inmiddels sterk verouderde, stelsel van wet- en regelgeving;
- het in overleg met de gemeenten samenstellen van een functioneel ontwerp voor de GBA.

Invoering zal over ongeveer 8 jaar kunnen plaatsvinden. Gedurende deze vrij lange overgangsperiode zullen de administraties grotendeels op de oude voet worden voortgezet, waarbij de staatssecretaris zal trachten het bijhouden van de persoonskaarten op korte termijn op te schorten. De gemeenten wordt toegestaan "eigen" systemen te ontwikkelen, gegevens uit te wisselen en dergelijke onder de beperkende voorwaarden dat:

1. het binnen gemeentelijk gebruik van bevolkingsgegevens gereglementeerd dient te geschieden en
2. er sprake moet zijn van gebruik van de gegevens binnen de gemeentelijke organisatie.

Het uiteindelijk te realiseren systeem zal een beperkt aantal kenmerken dienen te bevatten, om een persoon in dat systeem te identificeren. Een administratienummer zal daarvan de kern vormen.
Een "strategische beleidsnota" over de nummerproblematiek zal binnenkort aan het Kabinet worden voorgelegd.
Ook zal op korte termijn een adviserende Raad voor de persoonsinformatievoorziening worden ingesteld.

Commentaar

De zekerheid die de titel van het hiervoor verkort weergegeven artikel suggereert is nog geen feit; het geheel is nog in studie. De aanpak lijkt ons, uit automatiseringstechnisch gezichtspunt, veelbelovend. De realisatie zal echter mede dienen af te hangen van de invoering van een privacy-wet, waarvan kortgeleden een geheel nieuw wetsontwerp is gereed gekomen. Daarop vooruitlopend zijn ons inziens voor de waarborging van de privacy goede uitgangspunten geformuleerd. Naleving zal echter krachtens een wet afgedwongen en gecontroleerd dienen te worden.

Beveiliging

Eind oktober is bij het Nederlands Genootschap voor Informatica (NGI) een brochure uitgegeven over Computerbeveiliging. De auteur is de heer H.R.F. von Seydlitz Kurzbach.
De uitgave is voorbereid door de Sectie Beveiliging van het NGI.

De schrijver heeft het grootste deel van de tekst eerder gepubliceerd in het Handboek Schadepreventie (uitgave Samsom Uitgeverij, Alphen aan den Rijn). Gezien de specifieke lezerskring van dit Handboek, waartoe slechts weinig NGI-leden zullen behoren, werd een heruitgave overwogen. De auteur heeft daartoe enkele aanvullingen aangebracht, die het geschrift tot een zelfstandige uitgave maakte.

In vogelvlucht (ruim 60 pagina's) wordt een beeld gegeven van de aspecten van de computerbeveiliging, of zoals de schrijver het in zijn inleiding zegt: "Dit overzicht beoogt voor de leiding van een onderneming een wegwijzer te zijn in de doolhof van de computerbeveiliging". En even verder: "Mogelijk kan het ook in bredere kring zijn diensten bewijzen, waarbij wordt gedacht aan architecten- en ingenieursbureaus, adviseurs, hoofden van rekencentra, security-functionarissen, accountants en dergelijke".

Wij merken hierbij op dat een dergelijk beknopt boekwerkje nimmer kan aangeven hoe computerbeveiliging in een gegeven situatie zal moeten worden gerealiseerd, wel geeft het aan waaraan gedacht dient te worden en waarom. De doelgroep van deze brochure is het management zoals in de titel staat aangegeven. De nadere uitwerking van het beveiligingsplan vereist naast leiding de inzet van deskundigen zowel wat betreft het opstellen ervan als de realisering. Wij verwijzen naar het artikel van H.C. Kocks in deze Compact.

SMF-beveiligingen

In De Computerkrant (nummer 9, oktober 1984) wordt melding gemaakt van een beveiligingspakket voor de (IBM-) SMF-log file. Dit betreft het pakket SMF-EXPRESS dat als voornaamste doelstelling heeft het afvangen van automatisch wissen of overschrijven van de SMF log file ingeval deze vol is en daarvoor geen tegenmaatregel is getroffen.

Volgens het artikel zou SMF-EXPRESS de volgende functies hebben:
- zonder handmatig ingrijpen automatisch dumpen van de SMF-file bij het vollopen daarvan;
- vergelijken van de op tape gedumpte en de oorspronkelijke file;

- volledig beschrijven van de tapes door middel van Multi-file;
- parametrisering voor het eenvoudig terugvinden van bepaalde gegevens;
- selecteert verlangde SMF-records, welke eventueel gecombineerd kunnen worden.

Laatstgenoemde eigenschappen zouden ook voor controlefuncties nuttig kunnen zijn.

Controle

Reeds meerdere malen maakten wij melding van een artikel uit het kwartaaltijdschrift The EDP Auditor, uitgave van The EDP Auditors Foundation in de Verenigde Staten van Amerika. Deze keer troffen wij in het exemplaar van het derde kwartaal 1984 een interessant artikel aan, namelijk een bespreking van "Guidelines for Computer Security Certification and Accreditation", een uitgave van het U.S. National Bureau of Standards (Federal Information Processing Standard Publication 102). Een klein gedeelte uit de inleidende tekst laten wij nu volgen, ten einde de lezer bekend te maken met de doelstelling van de uitgave.

> This guideline was developed as a basic reference document for general use in establishing and carrying out a certification and accreditation program for computer security. The document recommends that certification and accreditation should be performed for applications that process sensitive data, or that could cause loss or harm from improper operations, or deliberate manipulation of the application.
>
> **Objective**
> This Guideline describes how to establish and carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive application to see how well it meets security requirements. Accreditation is the official management authorization for the operation of the application, and is based on the certification and accreditation program benefits and organization by improving management control over computer security, and increasing awareness of computer security throughout the organization.

Het eerste gedeelte van de "Guideline" wordt in het genoemde tijdschrift afgedrukt teneinde een indruk te geven van de aard van de betreffende uitgave. Dit deel start met de samenvatting die wij U evenmin willen onthouden:

> The best way to view computer security certification and accreditation is as a form of quality control for the computer security of sensitive applications (i.e., applications with a significant potential for loss). The critical decisions regarding the adequacy of security safeguards in sensitive applications must be made by authorized managers, and must be based on reliable technical information. As defined in this document, security certification is a technical evaluation for the purpose of accreditation, and uses security requirements as the criteria for that evaluation; security accreditation is management's approval for operation, and is based on that technical evaluation, and other management considerations. It should be noted that computer certifica-

tion and accreditation are one aspect of a general certification and accreditation activity that should be performed to assure that a computer application satisfied all its requirements. This guideline tells:

a. how to establish a program for computer security certification and accreditation,
b. how to perform such certifications and accreditations.

Daarna geeft het artikel een samenvatting van de "guideline" met verwijzing naar de vindplaats in de tekst.

De beide onderdelen: a. opstellen van het werkprogramma;
b. uitvoeren van het werkprogramma,
worden kort toegelicht aan de hand van attentiepunten.
Dan volgt de complete weergave van het eerste hoofdstuk, Introduction. Daaruit blijkt onder meer dat de Guidelines zijn gericht op het beoordelen en certificeren van "gevoelige"*) computertoepassingen en dat het uit het onderzoek voortkomende rapport het veiligheidsbewustzijn van het management kan bevorderen. Iets waaraan ook in de Nederlandse lectuur meer en meer aandacht wordt besteed. Ook wordt aandacht gegeven aan Risico-analyse, de beperkingen daarvan, alsmede aan de overeenkomst met de door de EDP-audit-functie te verrichten onderzoeken en de mogelijkheid de evaluatie van het security-onderzoek te vergelijken met de uitkomsten van de EDP-audit.

*) Onder "gevoelig" in dit verband te verstaan: kritisch voor het functioneren van de onderneming.

Commentaar Redactie

Het voorgaande onder Controle geeft een afspiegeling van zienswijzen zoals deze in Amerika tot stand zijn gekomen.
Het is waard deze opvattingen te vergelijken met die zoals deze in Nederlandse verhoudingen zijn geformuleerd.
Wij noemen de volgende bronnen:

- "Beheer en controle van en in Besturingssystemen" Workshop sectie EDP-auditing van het NGI 14, 15 en 16 mei 1984. Enkele artikelen zijn in Compact opgenomen.
- "Internationaal symposium over controle in een geavanceerde, complexe geautomatiseerde omgeving".
  Symposium georganiseerd door het NIVRA 10, 11 en 12 september 1984. Kort verslag in De Accountant van december 1984, pag. 248.
- "Certificering van software".
  Symposium georganiseerd door het NGI sectie EDP-auditing op 8 november 1984.
- "Security management": from the past to the future".
  Voor dit artikel van de hand van drs. H.C. Kocks verwijzen wij naar het hoofdartikel in dit blad.

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

ONDERWIJS

Managen van Datacenters

Het leidinggeven aan een rekencentrum omvat vele facetten. Een aantal daarvan zijn zeer specifiek in relatie tot het rekencentrum, andere facetten ontmoeten we ook bij het leidinggeven aan overige bedrijfsafdelingen.

De door Raet c.v. georganiseerde driedaagse cursus onder de titel "Managen van Datacenters" geeft aan de cursisten een overzicht van de meest relevante aspecten van het leidinggeven aan een operationeel rekencentrum. Ook waar het algemene zaken betreft zoals personeelsbeleid, omdat daaraan vanuit de specifieke eigenschappen van het rekencentrum vaak andere eisen moeten worden gesteld.

De behandeling van de stof geschiedt vanuit de optiek van het "grote" rekencentrum. Dit wil echter niet zeggen dat zij, die een rekencentrum van een geringere omvang leiden, er geen baat bij zullen hebben. In veel situaties blijven de problemen gelijk, alleen de omvang ervan verschilt.

Aan de orde komen onder meer onderwerpen als:
- organisatie van het datacenter;
- personeelsbeleid;
- planning van de produktie;
- werken in shifts;
- doorberekeningsmethoden;
- change management;
- computerbeveiliging;
- risico-analyse;
- betrouwbaarheid van programmatuur;
- EDP-audit.

De laatstgenoemde vier onderwerpen worden gegeven door een der EDP-auditors van Klynveld Kraayenhof & Co. De overige door functionarissen van Raet c.v., die elk die onderwerpen behandelen, die onderdeel uitmaken van hun dagelijkse werkzaamheden. Zo wordt bereikt dat de stof steeds door docenten wordt aangeboden, die praktijkervaring met de stof hebben.

Herfst 1984

Deze cursus is bestemd voor diegenen, die nu of in de toekomst, leiding (zullen) geven aan de geautomatiseerde gegevensverwerking binnen hun organisatie, dan wel bij het leidinggeven mede betrokken zullen worden.
Ook voor hen, die betrokken zullen zijn bij (management-)audits van automatiseringsorganisaties, kan deze cursus van nut zijn.

De eerstvolgende keer dat de cursus "Managen van Datacenters" wordt gegeven is in mei 1985. Deze cursus zal ook worden vermeld in de KKC-cursusbrochure en inschrijvingen ervoor zijn derhalve ook via KKC mogelijk.

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