compact

COMPUTER EN ACCOUNTANT

Klynveld Kraayenhof & co
ACCOUNTANTS

NUMMER 13 6E JAARGANG ZOMER 1979

compact

VAN DE REDACTIE

Het zomernummer van 1979 is vertraagd van de pers gerold.

In dit nummer zijn een tweetal hoofdartikelen opgenomen:

- "EDP Audit". Onder deze titel starten J.H. Urbanus en J. Verheul het eerste deel van hun artikel. Het slot volgt in een van de volgende uitgaven van Compact.
- "De invloed van de privacy-wetgeving op de organisatie en geautomatiseerde systemen" is van de hand van A.W. Neisingh.

Behalve deze twee artikelen zijn de vaste rubrieken ABC-Nieuws en Literatuuroverzicht aanwezig alsmede aan artikel over een computer-controletoepassing met een IMS-Data Base van de hand van H. Weerd.

Compact is een uitgave van de groep Automatisering en Controle van Klynveld Kraayenhof & co.

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

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

Redactie:
A.W. Neisingh, J. Philippo en D. Steeman.
Adres: Pr. Irenestraat 59, Amsterdam

Bijzondere EDP onderzoeken (I)

door: J.H. Urbanus en J.M. Verheul

1. Inleiding; doelstellingen

Het opschrift geeft al aan dat in deze bijdrage niet het algemene fungeren van de accountant als controleur van de jaarrekening aan de orde is, maar een fungeren in bijzondere opdrachten op het gebied van de administratieve automatisering. Ook andere dan accountantskantoren kunnen daarvoor zijn geëquipeerd.

In zijn algemene functie kan de accountant te maken hebben met, niet zelden ernstige, communicatiestoornissen tussen de directie en het automatiseringsmanagement. De oorzaak ligt veelal in een onvoldoende begrip voor elkaars verantwoordelijkheid ten aanzien van zaken zoals: management- en organisatieproblematiek, projectorganisatie, ontwikkeling en beheer van systemen, verwerkingscapaciteit.
Door de veelzijdige in accountantskantoren aanwezige kennis, die zich mede uitstrekt tot de genoemde gebieden, vervult de accountant naast de rol van beoordelaar ook vaak die van "vertaler" en zal hij relatief veelvuldig door opmerkingen en aanbevelingen (met name in Management Letters) tot verbetering hebben bij te dragen.
Het opvolgen van aanbevelingen door het management leidt menigmaal tot aanvullende opdrachten ter verkrijging van een nader oordeel op specifieke punten en/of het doen uitwerken van voorstellen tot verbetering.

De hierboven aangeduide "afstand" tussen hogere leiding en automatisering doet voorts bij eerstgenoemde nogal eens de behoefte opkomen aan een onafhankelijk oordeel over doeltreffendheid en doelmatigheid van de automatiseringsorganisatie.
De topleiding kan, als eindverantwoordelijke voor automatisering, met tussenpozen van enige jaren, of periodiek, naar aanleiding van belangrijke investeringsaanvragen, omvangrijke kostenstijgingen, en dergelijke, een (meestal korte) doorlichting doen uitvoeren.
Het gaat hierbij niet om een audit welk wordt gevolgd door een oordeel over de situatie van een moment, maar om een prospectief gericht onderzoek van algemene aard, waarvoor de term review of doorlichting meer geëigend is.
Ook het vrijwel ontbreken van normen voor een geheel objectieve meting van doeltreffendheid en doelmatigheid leidt tot een voorkeur voor de benamingen review en doorlichting (1).

Los van het eerder gestelde rijst vaak de vraag, ook bij het automatiseringsmanagement, of men met de automatisering geheel op de goede weg is.
Voor het verkrijgen van een oordeel kan in een doorlichting het automatiseringsgebeuren in brede zin (beleid èn uitvoering) aan de orde komen. Zie het volgende onderdeel van deze bijdrage.

De vraagstelling kan ook minder algemeen zijn en zich bijvoorbeeld richten op:

- de doelmatigheid van de taakverdeling en procedures in rekencentra
- de doelmatigheid van programmatuur en/of het computergebruik
- vraagstukken inzake de beveiliging
- aspecten als de tijdigheid, de bruikbaarheid en het feitelijk gebruik van computeruitvoer, en op verdere kosten/nut verhoudingen in een bepaald informatiesysteem. Zie onderdeel 3 van dit hoofdstuk.

Voor een verder overzicht wordt verwezen naar de literatuurlijst, (2) t/m (5).

Externe en interne EDP auditors beschikken reeds over zoveel kennis van de betreffende organisatie en haar systemen, dat zij een belangrijk aandeel kunnen leveren aan deze doorlichtingen.

Het verdient overigens de aandacht dat de automatiseringsproblematiek meer en meer wordt herkend als een probleem van brede en diepe structurering van overleg en communicatie, waarop ter oplossing socio-technische en andere methoden van organisatie-ontwikkeling van toepassing zijn.
Onderzoek en begeleiding vergen hier het optreden van daartoe geëquipeerde adviesbureaus, waaronder zich ook organisatie-afdelingen van accountantskantoren bevinden.
Hier moet worden volstaan met de geïnteresseerde lezer te verwijzen naar de literatuuropgave (6).

2. De algemene doorlichting

Ten einde een indruk te geven van de onderwerpen en facetten, die in een doorlichting aan de orde kunnen komen, wordt als voorbeeld een algemene doorlichting in gedachten genomen. Daarin richt men zich op de doelmatigheid en doeltreffendheid van de totale automatiseringsinspanning, veelal ter verkrijging van een antwoord op de vraag: zijn wij in alle opzichten op de goede weg?
Het ligt voor de hand dat beschouwing van het feitelijk gevoerde informatie- en automatiseringsbeleid als uitgangspunt dient. Via onderzoeken van de organisatie- en management-aspecten van de automatisering, alsmede de wijze waarop informatiesystemen feitelijk tot stand komen, worden ingevoerd, gebruikt en beheerd, mondt de doorlichting uit bij de electronische verwerking.

Een en ander wordt nader uitgewerkt in de hieronder genoemde onderdelen van deze bijdrage:

2.1 Bestuurlijke en beleidsaspecten
2.2 De organisatie van de automatiseringsfunctie
2.3 Het management van automatiseringsafdelingen

2.4 De bemanning van de automatiseringsafdelingen
2.5 Gebruikersparticipatie en - satisfactie; projectorganisatie
2.6 De systeemontwikkeling; het systeem- en programma-onderhoud
2.7 De electronische informatieverwerking
2.8 Rapportage van bevindingen en aanbevelingen.

In een korte algemene doorlichting gaat het wezenlijk om een beknopte verkenning van dezelfde zaken. De minder belangrijke daarvan komen dan slechts summier aan de orde.
Een korte doorlichting, welke één of twee weken in beslag kan nemen, levert veelal een voor de topleiding goed bruikbare indicatie van sterke punten, onevenwichtigheden en belangrijke tekorten.
De onderzoektijd wordt grotendeels in beslag genomen door interviews met de betrokken topleiding en verdere leidinggevenden, alsmede met vertegenwoordigers van gebruikers van informatiesystemen.
Een algemene doorlichting zal zich overigens als regel niet uitstrekken tot de afzonderlijke informatiesystemen.

In bijzondere EDP onderzoeken zijn voor een belangrijk deel onderwerpen aan de orde die reeds in algemene EDP audits de aandacht hebben.
Te dezer plaatse is de aandacht evenwel anders gericht (nadruk op doelmatigheid/doeltreffendheid in plaats van op betrouwbaarheid/continuïteit).
Ten einde doublures te vermijden, worden de beide laatstgenoemde aspecten niet opnieuw aan de orde gesteld, hoewel zij ook in het bijzonder EDP onderzoek punt van aandacht zijn.

Voorafgaande aan een doorlichting wordt aan betrokkenen een beknopte schriftelijke vastlegging gevraagd van gegevens waarvan de beschikbaarheid van belang is voor de planning van het onderzoek, zoals

- schema van de organisatiestructuur van de totale organisatie en de automatiseringsafdelingen, met indicatie van bezetting, vacatures en toekomstige sterkte
- automatiseringsplan
- personele opbouw naar bekwaamheden en ervaring; globale verdeling van aan systeemontwikkeling en onderhoud bestede tijd; ziekte en verloop
- schema van de computer-configuratie; aantal en plaats van terminals, e.d.; voorgenomen wijzigingen en uitbreidingen
- overzicht van besturings-, diensten- en hulpprogramma's
- gemeten computertijd voor produktie, tests, conversie e.d.
- samenstelling van de automatiseringsbudgetten van de laatste jaren
- belangrijkste gegevens van bestaande en in ontwikkeling zijnde informatiesystemen.

Inzage wordt gevraagd van functie-, taak- en procedureschrijvingen, documentatievoorschriften, standaards en richtlijnen, e.d. rapporten inzake hardware-selectie, actuele toepasbaarheidsstudies.
De organisatorische voorbereidingen van onderzoeken vallen buiten het bestek van dit artikel.

2.1 Bestuurlijke en beleidsaspecten

De accountant is uiteraard op de hoogte van tal van aangelegenheden die van invloed waren of zijn op de administratieve automatisering, zoals groei, concurrentieverhoudingen, personeelsvoorziening, rendementsontwikkelingen.
Het feitelijk gevoerde beleid en de historie van de automatisering zijn hem eveneens bekend.
Niettemin is het noodzakelijk in interviews met de verantwoordelijke hoogste leiding en andere managers de beleidsaspecten en de rol van de hoogste leiding in beschouwing te nemen.
Doelstelling van dit onderdeel van het onderzoek is een beeld te verkrijgen van het algemene bestuurlijke kader waarin de automatisering staat en zal staan, de automatiseringshistorie, alsmede de mate van aandacht en satisfactie van het verantwoordelijke hogere management.
De voornaamste vraag- en attentiepunten zijn:

- aanleiding tot de doorlichting
- achtergronden en doelstellingen van de automatisering in verleden, heden en toekomst; informatie en automatiseringsplanning
- rol van de hoogste leiding, andere stuurorganen en ondernemingsraad in beleidsvorming, planning, investeringsbeslissing, toepasbaarheidsonderzoeken
- meest gehanteerde beslissingscriteria, waaronder eisen inzake rendement en payback
- bereikte resultaten; eerdere evaluaties
- aandacht voor de vervulling van basisvoorwaarden voor automatisering
- voornemens ten aanzien van organisatie-ontwikkeling en -verandering; samenhang met de toepassing van management-technieken ten aanzien van plannen en beheersen; tendensen ten aanzien van centralisatie en decentralisatie; gespreide informatieverwerking
- groeiverwachtingen; flexibiliteitsbehoefte
- aandeel van automatiseringskosten in administratiekosten en totale kosten; verhouding van automatiseringskosten tot andere grootheden, bijvoorbeeld de omzet; ontwikkeling en beheersing van automatiseringskosten
- standpunt ten aanzien van externe bijstand waar onder die van accountantszijde; uitbesteding; make of buy; mixed hardware

- innovatiestreven in de automatisering
- voorlichting van en verbreding van automatiseringskennis onder het personeel
- standpunt ten aanzien van doorberekening van kosten van automatisering.

Het is van belang de resultaten van het automatiseringsbeleid weer te geven door feiten respectievelijk verwachtingen betreffende de voornaamste geautomatiseerde informatiesystemen en geplande systemen naar verschillende gezichtspunten te rubriceren.

Aldus kan inzicht worden gegeven in (schematisch):

- jaar van gereedkomen en algehele herziening; idem ten aanzien van geplande ontwikkelingen en herzieningen; prioriteitenstellingen indien een tijdplanning nog ontbreekt; levensduur
- de automatiseringsgraad in verschillende functionele onderdelen van de organisatie
- de aard van de functies waarin automatisering een grotere of kleinere rol speelt; bestuur, beheer, bewaring, registratie
- de afdelingen en de aantallen functionarissen die bij de systemen zijn betrokken ten opzichte van het geheel van afdelingen en mankracht
- geïnvesteerde bedragen; begrotingsoverschrijdingen; kosten op jaarbasis verdeeld in afschrijving, exploitatie en onderhoud; zichtbare besparingen; verwachtingen inzake kosten en baten
- wijzigingsfrequentie
- indicatie van het bedrijfsbelang
- technische gegevens zoals documentatiegraad, aandeel in de bezetting van de computer, toegepaste programmeertaal en bestandsorganisatie, voornaamste informatiedragers, flexibiliteit, onderhoudbaarheid, uitbreidbaarheid
- indicatie van eventueel achterstallig onderhoud, komende conversies, e.d.

De overzichten geven een globale indruk van de mate waarin van een gezonde en evenwichtige ontwikkeling sprake is.

2.2 De organisatie van de automatiseringsfunctie (algemeen)

Het begrip organisatie wordt hier breed opgevat en omvat het geheel van mensen, structuren, methoden, procedures en andere middelen, die in en buiten de automatiseringsafdelingen een rol spelen in de planning, voorbereiding en uitvoering van het automatiseringsgebeuren.
Uit hetgeen hiervoor is opgemerkt inzake het ontbreken van voldoende normen voor een objectieve meting van de doelmatigheid

en doeltreffendheid van de activiteiten in een automatiseringsorganisatie, volgt dat er behoefte bestaat aan een indirecte benadering van de genoemde aspecten.

Het onderzoek betreft dan allereerst de kwaliteit van de organisatie (het vermogen om haar doelstellingen te bereiken). Een positief oordeel over die kwaliteit, met name over de aandacht voor doelmatigheid en doeltreffendheid, mag in eerste instantie de verwachting vestigen, dat ook de resultaten goed zullen zijn.

Een "omgevingsonderzoek", bij de hoogste leiding (2.1) en de gebruikers van informatiesystemen (2.6), leert in hoeverre het automatiseringsgebeuren de belangen van de verdere organisatie dient en kan leiden tot bijstelling van in de vorige zin genoemde verwachting.
De indirecte benadering neemt de vorm aan van een conditie-onderzoek, waarin wordt nagegaan of de juiste condities worden geschapen en in stand gehouden voor een goede systeemontwikkeling, welke in overeenstemming is met de in de overige organisatie geldende doelstellingen, en voor een goede computerexploitatie.

De onderstaande vraag- en attentiepunten zijn van algemene aard. In de volgende paragrafen vindt enige verdere uitdieping plaats

- structuur van de automatiseringsorganisatie
- leiding en toezicht; span of control; periodieke rapportage aan de topleiding
- beschrijving en toedeling van alle te vervullen functies; functiehiërarchie; afwezigheid van ongewenste vermenging of cumulatie van verantwoordelijkheden
- aanwezigheid van een automatiseringshandboek.

2.3 Het management van automatiseringsafdelingen

In interviews met de leiding van automatiseringsafdelingen zijn de belangrijkste vraag- en attentiepunten, naast ter zake reeds genoemde

- toepassing van management-technieken bij plannen, begroten, delegatie, toewijzen van mensen en middelen, voortgangscontrole, financiële controle, kwaliteitscontrole
- beoordelingsfrequentie van produktieregistratie; onderzoek naar incidenten en opvallende afwijkingen van de planning, klachtenbehandeling
- produktiviteit en efficiency-bewaking
- rol in de automatisering van de hoogste leiding en de gebruikers
- interne en externe communicatie; overleg; coördinatie

- periodieke rapportage aan de hogere leiding
- beschikbaarheid van plaatsvervangers en opvolgers
- besluitvoorbereiding en beslissingsprocedures in aangelegenheden van apparatuur, programmatuur, informatiesystemen; de voornaamste daarbij gehanteerde rendements- en andere criteria. Toepasbaarheidsonderzoeken
- aanschaffings- en acceptatieprocedures
- standpunt ten aanzien van standaardprogramma's, leverancierskeuze, gebruik hogere talen, comptabiliteit, overdraagbaarheid
- rol ten aanzien van risk-management en verzekeringen.

2.4 De bemanning van de automatiseringsafdelingen

De voornaamste vraag- en attentiepunten zijn:

- beschrijvingen van (kern)functies, verantwoordelijkheden en taken, functie-eisen
- evenwichtigheid van taakbundelingen
- opbouw van het personeelsbestand naar verschillende gezichtspunten (zoals ervaring, vorming, doorstromingsmogelijkheid, leeftijd)
- methoden van selectie en vorming
- gebruik van tijdelijke krachten
- opvangmogelijkheden bij ziekte, vakantie en vertrek
- externe contacten; deelname aan seminars en dergelijke
- ontwikkeling van de sterkte in de laatste jaren

2.5 Gebruikersparticipatie en -satisfactie; projectorganisatie

Inleiding

Al vanaf de opkomst van de computer, als opvolger van electromechanische apparatuur, heeft het sterk technische en complexe karakter van de administratieve automatisering een vrij grote scheiding teweeg gebracht tussen de automatiseringsspecialisten en de zo geheten gebruikers.
Een toereikende participatie van de zijde van de gebruiker, eventueel binnen het kader van een projectorganisatie, is derhalve van grote betekenis voor het bereiken van de gemeenschappelijke doelstelling.
Hoewel er veelal samenhang bestaat tussen participatie en satisfactie zal naar dit laatste toch afzonderlijk dienen te worden geïnformeerd.
De betreffende vraag- en attentiepunten vormen het tweede deel van deze paragraaf.

Participatie

Het onderzoek naar de gebruikersparticipatie is gericht op het verkrijgen van een oordeel over de mate waarin de participatie de totstandkoming van betrouwbare, efficiënte en effectieve informatiesystemen bevordert, en de gebruiker echte verantwoordelijkheid kan dragen voor de materiële inhoud van het systeem, de beveiliging van de gegevens en de voorzieningen tegen verstoringen van de normale exploitatie van de systemen.

Vraag- en attentiepunten betreffende gebruikersparticipatie

- historie van de gebruikersparticipatie
- organisatie van de inbreng van gebruikers van informatiesystemen in informatie- en automatiseringsplanning, toepasbaarheidsonderzoeken, analyse, testen, invoering
- zorg voor vervulling van de basisvoorwaarden voor automatisering
- autorisatie- en acceptatieprocedures
- vaststelling van het niveau van interne controle en beveiliging
- gebruik en wijziging van passwords, en dergelijke
- planning van verwerking; onderhoudsplanning; systeembeheer in het algemeen
- evaluatie van informatiesystemen; periodieke herhalingen.

Projectorganisatie

Zoals gezegd kan de gebruikersparticipatie voor een deel bestaan uit deelname aan de projectorganisatie.
Inzake dit belangrijke onderwerp kan in hoofdzaak worden verwezen naar de in de litaratuur voorkomende vragenlijsten (7).
Voor het doel van dit artikel valt de nadruk op de onderstaande punten

- fasegewijze aanpak
- bewaking van voortgang, kwaliteit en kosten via opdrachten, rapportage en evaluatie per fase
- fasegewijze opbouw van de systeem- en programmadocumentatie
- algemene afspraken met interne en externe accountant omtrent de door deze uit te voeren beoordelingen (vooraf, achteraf en op tussenliggende kritische momenten).

Het onderzoek naar de satisfactie van gebruikers betreft de algemene ervaringen van gebruikers in de omgang met automatiseringsspecialisten.
In een korte algemene doorlichting kan geen evaluatie van afzonderlijke informatiesystemen plaatsvinden en ook in een langer durende algemene doorlichting zullen vaak geen systeemonderzoeken van enige omvang zijn begrepen.

Nochtans berust de satisfactie van de gebruiker voor een belangrijk deel op ervaringen met "hun" informatiesysteem.
De ervaring leert dat, uit gesprekken met gebruikers toch een beeld kan worden verkregen van de algemene relatie automatiseringsorganisatie - gebruiker, aan de hand waarvan andere bevindingen kunnen worden getoetst en eventueel beter kunnen worden geïnterpreteerd.

In het algemeen bestrijkt de ondersteuning en dienstverlening door de automatiseringsorganisatie alle fasen en aspecten, vanaf het opkomen van ideeën en probleemstellingen, waaruit tenslotte informatiesystemen voortkomen, tot en met het exploiteren en onderhouden van die systemen.

De gesprekken betreffen dan ook de algemene ervaringen van de gebruiker met betrekking tot

- prioriteitenstelling
- toepasbaarheidsonderzoek
- projectdefinitie, -planning, -voorbereiding en -beheer
- opstelling functionele eisen en specificatie, detail-analyse
- programmering, opstellen testgevallen, testen, overdracht aan gebruikers, instructie van gebruikers, gebruikers-documentatie
- conversie van oud naar nieuw; invoering, begeleiding
- nazorg; evaluatie
- aanpak van en verantwoordelijkheid voor controle en beveiliging
- exploitatieplanning; levering uitvoer; exploitatiekosten
- systeembeheer, onderhoud van systemen en programma's
- klachtenbehandeling
- overleg en communicatie van algemene aard; voorlichting.

2.6 De systeemontwikkeling; het systeem- en programma-onderhoud

De onderstaande vraag- en attentiepunten vormen ten opzichte van de voorgaande onderdelen een specifiek op het onderwerp gerichte aanvulling:

- de aanwezigheid van methoden en procedures met betrekking tot schema-technieken, formulierengebruik, structureren, documenteren, autoriseren, programmeren, testen, overdragen
- verhouding tot project-management, gebruikers, systeemprogrammeurs, systeembeheerders, formulierbeheerder, organisatie-afdeling, interne accountant
- aandeel van systeemanalisten en programmeurs in de systeemtest, in de opstelling van gebruikersinstructies, in conversies, in de invoering
- organisatie van trouble-shooting
- tijdsbesteding aan ontwikkeling versus onderhoud
- tijdsbesteding aan analyse, programmering, testen en documenteren, in onderlinge verhouding.

Een vooraf verkregen overzicht van bestaande systemen, onderhanden projecten en onderhoudswerkzaamheden, en hun samenhang, vormt een goed hulpmiddel in de te voeren gesprekken.
Hetzelfde geldt voor de resultaten van een inzage vooraf van de systeem- en programmadocumentatie van informatiesystemen die typerend worden geacht voor de periode waarin zij zijn ontstaan.

2.7 De electronische informatieverwerking

Als aanvulling op de hiervoor opgenomen en voor het onderhavige onderdeel relevante vraag- en attentiepunten worden genoemd

- methoden en procedures van planning; scheduling; voorbehandeling; werkvoorbereiding; operating; voortgangscontrole; produktiecontrole; nabehandeling; bestandsbeheer; bibliotheekbeheer; datalijnenbeheer; voorraadbeheer informatiedragers; beheer van het archief van printlogs, console-prints en andere verslagen; samenstelling en beheer van de produktiedocumentatie (run-books, stoplists, en dergelijke)
- verhouding tot systeem-programmering; functie en werkwijze van systeemprogrammeurs
- registratie van het computergebruik voor produktie, overdraaien, testen, dumpen; stilstandsregistratie
- registratie van abnormale stops, herstarts, storingen, andere incidenten
- periodieke samenvattingen van registraties ten behoeve van automatiseringsmanagement
- planning en organisatie van het testen; testprocedures
- acceptatieprocedures inzake aangeboden programmatuur en toepassingsprogramma's
- methoden en technieken van eigen tests en onderhoud van hardware en informatiedragers; regeling van het preventief onderhoud door leveranciers.

Tot de middelen van onderzoek behoren naast interviews het inzien van produktiedocumentatie, het bestuderen van produktieregistraties en periodieke samenvattingen daarvan, het bijwonen van werkzaamheden gedurende een of meer representatieve shifts.

Het bezien van samenstelling, capaciteit en bezetting van de apparatuur vormt uiteraard een belangrijk onderdeel van een doorlichting, welke is gericht op doelmatigheid en doeltreffendheid van de electronische verwerking.

De voornaamste middelen van onderzoek zijn de configuratiebeschrijving en de shiftsgewijze registratie van het gebruik van de voornaamste computercomponenten.

De EDP auditor zal nagaan of er aanwijzingen zijn voor de aanwezigheid van dure overcapaciteit en zich rekenschap geven van ernstige ongelijkmatigheden en onevenwichtigheden in de bezetting van computercomponenten resulterend in omvangrijke onbenutte capaciteiten.
Zulks vereist, mede gezien de kans op verborgen leegloop, enig inzicht in de werking van de systeem- en hulpprogrammatuur, de voornaamste toepassingen, de daarbij toegepaste methoden van bestandsorganisaties en bestandsbenadering, alsmede een globaal oordeel over de doelmatigheid van een en ander.

Sterke afwijkingen van een ideaal bezettingspatroon en -niveau zullen vaak in belangrijke mate kunnen worden verklaard uit hoofde van omstandigheden zoals:

- tijdsaspecten in de gebruikersbehoeften
- niet te spreiden piekbehoeften
- doorwerking van de configurering van voorgaande computers
- doorwerking van achterhaalde opvattingen ten tijde van de bouw van oudere informatiesystemen
- niet voorspelbare en wisselende belastingen in on-line toepassingen
- capaciteitsredundantie in verband met de gevolgen van storingen
- anticipatie op groei en nieuwe (rendabele) toepassingen
- vertragingen of uitstel van geplande toepassingen
- overige technisch-economisch onvermijdelijke of geboden overcapaciteiten.

Computer-aanschaffingen betreffen de infra-structuur van de organisatie. Daarmee wordt geanticipeerd op investeringsbeslissingen met betrekking tot informatiesystemen.
In beide soorten beslissingen spelen belangrijke imponderabele overwegingen een rol en min of meer ernstige fouten zijn in deze complexe materie haast onvermijdelijk.

De gelegenheid tot het snel effecteren van eenvoudige maatregelen waardoor een doelmatige computerconfiguratie zou worden bereikt, doet zich evenwel aanzienlijk minder vaak voor dan sommige publikaties doen vermoeden.

In een doorlichting kan de EDP auditor in aangelegenheden van hardware en software samenwerken met andere specialisten.
Er zijn goede ervaringen in het samenwerken van EDP auditors met raadgevende ingenieurs voor automatisering en softwarehouses.
De nodige apparatuurkennis zal overigens vaak aanwezig zijn in de aan de grotere accountantskantoren verbonden organisatie-adviesafdelingen.

2.8 Rapportage van bevindingen en aanbevelingen

In de rapportage wordt onder meer rekening gehouden met:

- het prospectieve karakter van de doorlichting. Het gaat om de vooruitzichten voor het op goed niveau bereiken of behouden van een bevredigend evenwicht tussen doelstellingen, middelen en resultaten
- een mogelijk gebrek aan onderling begrip en communicatie tussen de hogere leiding en het automatiseringsmanagement alsmede tussen de automatiseringsafdelingen en de gebruikende afdelingen
- de veelal aanwezige noodzaak tot het verbeteren van de algemene grondslagen voor een goede informatievoorziening, op een breed front in de gehele organisatie en
- de complexiteit van de materie, waardoor als regel vrij veel opmerkingen zijn te maken, hetgeen echter een verkeerde indruk kan vestigen. Door minder belangrijke aangelegenheden in bijlagen op te nemen wordt de aandacht gevestigd op de werkelijk ter zake doende punten.

Het prospectieve karakter van een doorlichting vergt dat ernstige problemen en belangrijke kosten uit hoofde van een (vervroegde) vervanging of uitbreiding van apparatuur en systemen worden gesignaleerd. Voorbeelden zijn omvangrijke herprogrammeringen en wijzigingen in bestandsorganisaties, alsmede on-line toepassingen.
Een complicerende factor is dat door snelle technologische ontwikkelingen en prijsdalingen het steeds minder vanzelfsprekend is dat een "groter familielid" als opvolger van de aanwezige computer zal worden gekozen.
De ontwikkelingen in het decentraal gebruik van kleine computers en daarmede al dan niet verband houdende on-line toepassingen kunnen de aanbevelingen eveneens beïnvloeden.

In het voorgaande zal duidelijk zijn geworden dat er gevallen zijn waarin een algemene doorlichting, en nog minder een korte doorlichting, niet op alle punten tot een afgerond en stellig oordeel over de aspecten doeltreffendheid en doelmatigheid zal kunnen leiden.
De rapportage na een algemene doorlichting kan aanleiding geven tot onderzoeken op deelgebieden waaraan management verdergaande aandacht wil wijden.
Die onderzoeken vallen niet steeds, of in alle opzichten, binnen de mogelijkheden van een EDP auditor, bijvoorbeeld omdat zij een diepergaande kennis van organisatievraagstukken, programmering, systeemprogrammatuur en apparatuur vereisen. Uit paragraaf 2.7 (slot) blijkt hoe ook dan een onderzoekteam kan worden samengesteld.

In een volgende aflevering van COMPACT zal deze bijdrage worden afgesloten met de bespreking van het onderwerp "De bijzonder review van een geautomatiseerd informatiesysteem".

Literatuurlijst

1. Begrip en praktijk van EDP-Auditing door D. Steeman en J.H. Urbanus (Informatie, september 1975).

2. EDP-Analyzer (uitg. Canning Publ. Inc.).
   Are we doing the right things (mei 1975).
   Are we doing things right (juni 1975).
   Do we have the right resources (juli 1975).

3. EDP-auditing; een bijdrage tot beheerst computergebruik, door L.C. van Zutphen (de Accountant, februarie 1975).

4. EDP-Audit, een veel-zijdig instrument, door drs. F.J.G. Fransen (informatie, maart 1979).

5. Het beheer van computer (een verzameling monografieën in losbladige vorm) Uitg. Samsom.

6. Socio-technische aanpak van de automatisering, door B.S. Drent (GIDOR-bulletin jan./febr. 1978, uitg. Ministerie van Binnenlandse Zaken).

7. Project control manual, door Sven R. Hed (Uitg. Hed, Geneve, 1973, losbl.).

8. Bepaling van de informatiebehoefte, door J. Ganzevoort (GIDOR-bulleting nov./dec. 1977, uitg. Ministerie van Binnenlandse Zaken).

9. Computer Output Review, door A. Kranendonk (GIDOR-bulleting jan./febr. 1978, uitg. Ministerie van Binnenlandse Zaken).

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

DE INVLOED VAN DE PRIVACY-WETGEVING OP DE ORGANISATIE EN OP DE GEAUTOMATISEERDE INFORMATIESYSTEMEN

door A.W. Neisingh

I Inleiding

In de zeventiger jaren heeft zich een ontwikkeling in het maatschappelijk denken afgetekend onder meer gericht op de bescherming van de persoonlijke levenssfeer.
De wetgevers in de Verenigde Staten van Noord-Amerika en in Europese landen hebben op deze tendens ingehaakt en wettelijke regelingen aan de parlementen aangeboden.
In Europa zijn landen als Zweden (1973), West-Duitsland (1977) en Frankrijk (1978) voorlopers geweest; andere landen zijn gevolgd.
Protectionistische trekjes zijn ons in de wetgeving niet bespaard gebleven. Op de problematiek, die hierdoor kan ontstaan in het geval van grensoverschrijdend gegevensverkeer [1] zal in deze bijdrage niet worden ingegaan.

Ons land schaart zich met bijvoorbeeld België in de rij van de "nakomers" bij het van kracht worden van een privacy-wetgeving.
Zoals bekend heeft de "Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties" (zogenaamde Commissie Koopmans) in 1976 tot slot van zijn werkzaamheden een Eindrapport uitgebracht.
In het Eindrapport zijn onder meer opgenomen een voorstel voor een wettelijke regeling en de schriftelijke reakties op het in 1974 uitgebrachte interimrapport Privacy en persoonsregistratie.
Het in het Eindrapport opgenomen voorstel voor een wettelijke regeling is (nog?) niet door de regering overgenomen. De verwachting is dat omstreeks eind 1979/begin 1980 een Ontwerp van Wet kan worden tegemoet gezien.

In deze bijdrage zal aandacht worden besteed aan de mogelijke invloed van privacy-wetgeving zoals die reeds in enige landen van West-Europa van kracht is op de organisatie en op de geautomatiseerde informatiesystemen.
Aan het genoemde Eindrapport zal uiteraard niet worden voorbijgegaan.

In de literatuur die met betrekking tot de bescherming van de persoonlijke levenssfeer verschijnt wordt aandacht besteed aan de begrippen:

- privacy en
- data security

1) Van grensoverschrijdend gegevensverkeer is onder meer sprake indien gegevensverwerking in een ander land plaatsvindt of indien bij uitwijk van een computer in een ander land gebruik wordt gemaakt.

Het privacy-begrip behandelt welke gegevens geheim te houden, vertrouwelijk te behandelen of ongeautoriseerde verspreiding daarvan te voorkomen en welke gegevens men over andere personen mag hebben.
Regels met betrekking tot de privacy-bescherming zijn ontwikkeld ten behoeve van het beschermen van personen.

(Onder persoonsgegevens wordt vooral verstaan hetgeen de persoonlijke levenssfeer betreft en daarom niet "iedereen" regardeert: inkomen, ziektegeschiedenis, lidmaatschappen, e.d.)

Data security betreft het vraagstuk hoe gegevens kunnen worden beveiligd tegen ongeautoriseerde toegang, modificatie en kennisneming zodra deze geautomatiseerd zijn.
Data security behandelt de bescherming van gegevens.
Op deze plaats zal niet worden ingegaan op het complex van maatregelen, waarmee data security kan worden gerealiseerd.

Regels die dienen te gelden ten behoeve van de bescherming van gegevens beantwoorden normaliter ook aan de verlangens op grond van de bescherming van de privacy.
Er kunnen echter enige maatregelen worden onderkend, waarbij maatregelen ten behoeve van data security strijdig zijn met privacy verlangens en omgekeerd.
Een voorbeeld ter verduidelijking:

- data security versus privacy: het extern bewaren ten behoeve van reconstructiedoeleinden van een kopie van een belangrijk "privacy-gevoelig" bestand roept een privacy-risico op!
- privacy versus data security: uit oogpunt van privacy-bescherming verdient het aanbeveling de geautomatiseerde gegevensverwerking van de salarissen altijd door dezelfde operators te laten uitvoeren (geheimhouding gemakkelijker te waarborgen en te controleren).
  Uit een oogpunt van interne controle is een dergelijke situatie echter ongewenst te achten (mogelijkheid van ongeoorloofd ingrijpen in de verwerking, continuïteit in de bezetting (bij ziekte e.d.).

Het spreekt welhaast vanzelf dat ook bij privacy-gevoeligheid de noodzaak van het bestaan alsmede de handhaving en naleving van algemene maatregelen ter zake van de betrouwbaarheid en de continuïteit van de gegevensverwerking in de organisatie van de automatisering en in geautomatiseerde systemen onveranderd aanwezig blijft.

Uit een beoordeling van privacy-wetgeving en (voor)ontwerpen blijkt dat daarvan een belangrijke invloed kan uitgaan op:

- de organisatie van de onderneming
- de organisatie van de automatisering
  te weten

. de ontwikkeling van geautomatiseerde informatiesystemen
. de organisatie van de gegevensverwerking

- de gegevensbeveiliging.

Op deze onderwerpen zal achtereenvolgens worden ingegaan.

II Invloed op de organisatie van de onderneming

Voordat zal worden ingegaan op de invloed van de privacy-wetgeving op de organisatie van de automatisering is het gepast een ogenblik stil te staan bij de gevolgen die deze wetgeving kan hebben op de organisatie als geheel.

De Duitse privacy-wet "Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz: BDSG)" gaat op dit punt vrij ver door te stipuleren dat in bepaalde omschreven gevallen een zogenaamde Datenschutzbeauftragter moet worden benoemd (artikel 28 lid 1 en 2 BDSG), alsmede zijn organisatorische plaats (lid 3 en 4).
Artikel 29 BDSG vermeldt vervolgens welke taken door hem dienen te worden verricht.
Daarnaast vermeldt de Anlage zu Paragraph 6 Abs. 1 Satz 1 BDSG onder meer ".... die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle)".*
De Technische en organisatorische Massnahmen in paragraaf 6 worden in zoverre afgezwakt, dat:
"Erforderlich sind Massnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht".

In een voorontwerp van een Belgische wet wordt eveneens een persoon verantwoordelijk gesteld voor de databank en naleving van de wettelijke regelingen.

Vanzelfsprekend is in alle wetten en (voor-)ontwerpen voorzien in toezichthoudende staatsorganen.
In Nederland wordt hiertoe gedacht aan een Registratiekamer [2)]
(vgl. Eindrapport), die "bevoegd is inlichtingen in te winnen, apparatuur, programmatuur, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen vertonen, voor zover dit redelijkerwijs voor de vervulling van zijn taak nodig is" (artikel 9 lid 1 Ontwerp van Wet in Eindrapport).

* Voorzover (delen van) buitenlandse wetteksten worden geciteerd, worden deze ter voorkoming van voornamelijk interpretatieverschillen in de oorspronkelijke taal overgenomen.

2) Zweden: Data Inspection Board; West-Duitsland: Bundesbeauftragter für den Datenschutz; Frankrijk: La Commission Nationale de l'informatique et des libertés.

Van deze stellingname zal een positieve invloed uitgaan op de organisatie.

Het Nederlands Instituut van Registeraccountants heeft in haar brief d.d. 25 juni 1974 aan de Staatscommissie naar aanleiding van het interim-rapport van de Commissie Koopmans naar mijn mening terecht kritische kanttekeningen geplaatst bij de rol van de Registratiekamer.
Uit de brief [3] citeer ik punt 4:
"In principe is het huidige Nederlandse accountantsberoep geëquipeerd om de bedoelde onafhankelijke controletaak op zich te nemen. Men bedenke, dat de apparatuur die voor de persoonsgegevensverzameling wordt gebruikt goeddeels dezelfde is als de apparatuur, die in ruime mate voor de - reeds onder accountantscontrole vallende - administratieve verslaglegging wordt gebruikt. Men bedenke ook, dat de organisatorische beveiligingsmaatregelen die voor persoonsgegevensverzamelingen nodig zijn, geen andere zijn dan de maatregelen die reeds sinds jaar en dag voor de beveiliging van administratieve gegevens worden toegepast en door accountants worden gecontroleerd.
Zodra een wettelijke regeling tot stand is gekomen, zullen onafhankelijke registeraccountants dan ook in staat zijn het bedoelde toezicht uit te oefenen en ten behoeve van het bevoegde gezag verklaringen te geven omtrent het voldoen aan die eisen, respectievelijk het op bepaalde aangegeven onderdelen niet voldoen".

De reeds in ondernemingen van enige omvang aanwezige interne accountantsdiensten, interne controlefunctionarissen, en zogenaamde security officers zullen een belangrijke rol kunnen spelen bij de controle op de naleving van de regelingen, zoals die in hun onderneming dienen te gelden.

III Invloed op de organisatie van de automatisering

A. De ontwikkeling van geautomatiseerde informatiesystemen

In deze paragraaf zal aandacht worden besteed aan de invloed van de privacy-wetgeving op de ontwikkelingsorganisatie van geautomatiseerde informatiesystemen (ontwerp, analyse en programmering).
Vanzelfsprekend zijn de opmerkingen slechts van toepassing op die systemen die persoonsgegevens zullen verwerken.
In de behandeling zal aandacht worden besteed aan overwegingen, die voorafgaan aan en maatregelen, die tijdens de ontwikkeling dienen te worden genomen. Mogelijke gevolgen van de wetgeving op ontwerp, analyse en programmering komen vervolgens ter sprake.
Tenslotte zal worden ingegaan op belangrijke instructies en

voorschriften die bijvoorbeeld ten aanzien van het onderhoud

van operationele programmatuur en het documenteren van deze systemen dienen te gelden.

Het is zeer gewenst in een vroegtijdig stadium te beschrijven welke acties zijn toegestaan, wie daartoe geautoriseerd zijn en welke gegevens daarbij nodig zijn.
Reden voor deze "positieve" benadering is dat zeer moeilijk en nagenoeg nooit limitatief kan worden beschreven wat niet is toegestaan, respectievelijk wat onder misbruik dient te worden verstaan.
Hiertoe is het nodig vast te leggen welke gedragslijn dient te gelden ten aanzien van:

a. het verzamelen van gegevens
b. het vastleggen van gegevens
c. het verspreiden
d. het gebruik en
e. de controle door een geautoriseerde gebruiker.

Het is uiteraard van belang na te gaan welke wettelijke bepalingen ten aanzien van de onderneming en het specifieke systeem gelden.
In de Duitse BDSG worden met betrekking tot de ontwikkeling van systemen de volgende controles beschreven, waaraan onder de reeds vermelde voorwaarde "Erforderlich sind Massnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu den angestrebten Schutzzweck steht" moet worden voldaan:

1. Speicherkontrolle
2. Zugriffskontrolle
3. Uebermittlungskontrolle
4. Eingabekontrolle
5. Transportkontrolle [4].

Over de interpretatie van deze voorschriften is overigens in West-Duitsland het laatste woord nog niet gesproken.
Het zal evenwel duidelijk zijn dat de "Kontrolles" gemakkelijker zijn gedefinieerd dan geïmplementeerd!

In wetten en (voor-)ontwerpen van wet is voorzien in een inzagerecht en correctierecht voor degene van wie persoonlijke gegevens zijn opgeslagen en een recht te weten wie in een bepaalde periode persoonsgegevens heeft opgevraagd.
In artikel 69 lid 2 van het Ontwerp van Wet (zie Eindrapport) wordt gesteld: "indien gegevens betreffende de persoon van de verzoeker in het registratiesysteem zijn opgenomen stelt de houder hem, desverlangd in schriftelijke vorm een volledig en eenvoudig te begrijpen overzicht van deze gegevens ter beschikking".

4) Voor de volledige tekst wordt verwezen naar bijlage 1.

De consequentie hiervan kan zijn dat speciale maatregelen in systemen nodig zullen blijken te zijn.
Afhankelijk van de frequentie van inzage en verbetering is het misschien noodzakelijk de bestandsorganisatie aan te passen.
Dit recht op inzage en verbetering zal in vele systemen ook leiden tot uitbreidingen (van de systemen).
Programmatuur zal moeten worden ontwikkeld om aan de Wet te voldoen ("in schriftelijke vorm een volledig en eenvoudig te begrijpen overzicht" en op grond van andere in de artikelen 69 t/m 74 genoemde condities [5]).

Artikel 35 BDSG behandelt "Berichtigung, Sperrung und Löschung von Daten".
Uit lid 2 van het artikel vloeit onder meer voort dat de datum van initiële inbreng vastgelegd dient te worden, omdat zij aan het einde van het vijfde kalenderjaar na de datum van inbreng dienen te worden geblokkeerd.
In een voorontwerp van de Belgische privacy-wetgeving is ooit opgenomen geweest (paragraaf 26 lid 2), dat aan betrokkenen "de identiteit van de derden aan wie in de loop van de twaalf maanden die aan het verzoek voorafgaan, gegevens zijn medegedeeld" moet kunnen worden gemeld.

Dit betekent méér dan een audit trail!

De door de Zweedse wetgever ingestelde Data Inspection Board heeft zelfs de bevoegdheid voorschriften te geven (indien noodzakelijk) met betrekking tot:

- de verkrijging van informatie
- het inlichten van de persoon waarover gegevens zijn vastgelegd
- de openbaarmaking van informatie.

Van deze bevoegdheid kan een belangrijke invloed uitgaan op de ontwikkeling en het onderhoud van geautomatiseerde informatiesystemen, omdat deze voorschriften dienen te worden opgevolgd.
Er is bovendien een ontwikkeling gaande te komen tot de vastlegging van zogenaamde privacyreglementen. In deze reglementen zal ongetwijfeld een rem worden gezet op te ongebreidelde "verzamel- en vastleggingswoede" van automatiseerders.

Deze paragraaf zou ik willen besluiten met de suggestie:
"Ontwerp een geautomatiseerd informatiesysteem op basis van wat is toegestaan".

5) Voor de volledige tekst van de artikelen 69 t/m 74 wordt verwezen naar bijlage 2.

Uit de voorgaande bespreking zal duidelijk zijn geworden dat een privacy-wetgeving gevolgen zal hebben op ontwerp, analyse en programmering van geautomatiseerde informatiesystemen waarin persoonsgegevens worden verwerkt.
Dat wil zeggen er zullen beperkingen worden opgelegd aan de tot nu toe bestaande vrijheid van handelen (lees: ontwerpen) van onder meer automatiseerders.

De navolgende aspecten kunnen worden onderkend:

1. Verplicht gebruik van data encryption technieken ter voorkoming van ongeoorloofde kennisneming van de vertrouwelijke gegevens.
   (Deze technieken ook te gebruiken bij - uit beveiligingsoverwegingen - extern bewaarde kopieën van persoonsgegevens verzamelingen.)

2. Toekennen van classificatiecodes aan uitvoer, zowel op papier als op andere informatiedragers.
   Hierbij behoren tevens voorschriften met betrekking tot de vernietiging van geclassificeerde stukken.

3. De implementatie van technieken gericht op de controle van de bevoegdheden en de identificatie van de gebruiker; het gebruik van wachtwoorden ter bescherming tegen ongeautoriseerde toegang tot (delen van) bestanden, eventueel gecombineerd met een automatisch log-off mechanisme indien terminals gedurende een bepaalde periode niet zijn gebruikt.
   Vastleggingen dienen te worden opgebouwd van pogingen tot toegang van beschermde/geclassificeerde bestanden.

4. Ontwikkeling van programmatuur ten behoeve van het opvragen van informatie.
   Het ligt in de lijn der verwachting dat een aantal van degenen waarvan persoonsgegevens zijn opgeslagen inzage in deze gegevens zal verlangen. Dit zal niet uitsluitend dienen ter informatie/ter controle van deze gegevens; men zal eveneens wensen op de hoogte te worden gesteld van het gebruik dat van de gegevens werd gemaakt.

5. Geautomatiseerde systemen zullen de mogelijkheid moeten bieden foutieve gegevens terstond te corrigeren respectievelijk te verwijderen of zo nodig voor gebruik te blokkeren.

6. Ontwikkeling van monitoring mechanismes (surveillance) ten behoeve van een voortdurende controle van de gehele gegevensverwerking.

7. Limiteren van de integratie van gegevensverzamelingen.

8. Gescheiden opslag van belangrijke gegevens opdat het risico dat bij elkaar behorende (persoonsgegevens) uitlekken wordt verkleind.

9. Overwogen kan worden onder besturing van het betreffende toepassingsprogramma waarschuwingen op de uitvoer af te drukken (zowel op de eerste als laatste regel van een pagina):
"Attentie! Openbaarmaking van deze gegevens is in strijd met artikel .. Wet Privacybescherming".

10. Eveneens zou het gelijktijdig afdrukken van meerdere rubrieken van persoonsgegevens kunnen worden voorkomen. Voorbeeld: de koppeling tussen naw-gegevens van een personeelslid en zijn salaris, beoordelingscijfer e.d. kan slechts met behulp van het personeelsnummer geschieden.

11. De verplichting tot het vervaardigen van protocollen.

Na de behandeling van enige aspecten ter zake van mogelijke gevolgen van privacy-wetgeving op ontwerp, analyse en programmering, waarbij niet kan worden voorbijgegaan aan administratief-organisatorische maatregelen, past tot slot van deze paragraaf een korte bespreking van belangrijke instructies en voorschriften in de automatiseringsorganisatie.

Het zou te ver voeren op deze plaats op het belang en de noodzaak van vastgelegde instrukties, voorschriften en procedures in te gaan. Steeds vaker kan worden waargenomen dat het automatiseringsmanagement ook los van de verwerking van persoonsgegevens de betekenis en de noodzaak ervan onderkent en een en ander gesystematiseerd laat onderbrengen in een zogenaamd handboek automatisering.
Bij de behandeling van de onderhavige problematiek springen enige instructies, procedures en voorschriften in het oog die van bijzondere betekenis zijn.
Achtereenvolgens zullen de revue passeren:

a. programma-onderhoudsprocedure
b. reconstructie en herstart
c. documentatie
d. programmeringsstandaarden
e. maatregelen van interne controle.

ad a. programma-onderhoudsprocedure.
De procedure bij het modificeren van operationele programmatuur dient erop gericht te zijn uit te sluiten dat ongeautoriseerde wijzigingen in operationele programmatuur worden aangebracht.

Ten aanzien van operationele programmatuur waarmee persoonsgegevens worden verwerkt zal bijzondere aandacht

dienen te worden geschonken aan:

- de afhandeling van programmadumps, omdat de gemaakte afdruk van het computergeheugen persoonsgegevens kan bevatten
- de controle op de juistheid van de aangebrachte programmawijziging
  (Voorkomen dient te worden dat de getroffen beveiligingsmaatregelen ten gevolge van het doorlopen van een bepaald - tijdens het onderhoud gemodificeerd-programma-onderdeel teniet worden gedaan.)
- het testen van het gewijzigde programma. Indien het testen geschiedt met behulp van kopieën van geclassificeerde gegevens dienen waarborgen te worden getroffen dat deze testuitvoer niet openbaar wordt.

Voor zogenaamde "midnight-changes" zullen vanzelfsprekend zeer stringente beveiligingsmaatregelen moeten worden getroffen.

ad b. reconstructie en herstart.
Na een calamiteit dienen gegevensverzamelingen in hun laatste (consistente) stand te worden teruggebracht, waarna de gegevensverwerking kan worden herstart.
In dit kader is het van belang:

- die delen van het geheugen van de computer die zijn gebruikt ten behoeve van het uitvoeren van de reconstructie en herstart "schoon" te maken, opdat niet door een toevalligheid privacy-gevoelige gegevens ongecontroleerd beschikbaar komen
- vast te stellen dat de gegevensverzamelingen correct zijn nadat de benodigde werkzaamheden zijn uitgevoerd.

ad c. documentatie.
Vanzelfsprekend dient een goede documentatie van geautomatiseerde systemen te worden opgebouwd.
Op de aan de inhoud te stellen eisen van de diverse te onderkennen documentatiedelen, te weten systeemdocumentatie, programmadocumentatie, gebruikers- en operating/werkvoorbereidingdocumentatie alsmede controledocumentatie zal hier niet worden ingegaan.
Een belangentegenstelling kan worden onderkend, waarover hierna meer.
Documentatie dient als vertrouwelijk stuk te worden aangemerkt, omdat hierin onder meer eigen know-how is gestoken. De verantwoordelijke leiding zal maatregelen nemen dat (kopieën van) documentatie niet aan onbevoegden ter inzage wordt verstrekt, respectievelijk kan worden meegenomen.

Uit artikel 40 Ontwerp van Wet (Eindrapport) volgt dat slechts een vergunning voor een vergunningsplichtig systeem kan worden afgegeven indien het privacy-reglement (dit is inclusief de documentatie van het informatiesysteem) en een beschrijving van de technische en organisatorische maatregelen ter beveiliging van het systeem aan de Registratiekamer is overlegd.

In Nederland zijn mij geen wettelijke bepalingen bekend met betrekking tot het documenteren van geautomatiseerde systemen. In West-Duitsland is daarentegen sprake van de zogenaamde Grundsätze ordnungsmässiger Speicherbuchführung (GoS) [6]; hierin wordt onder meer aandacht besteed aan de documentatie van geautomatiseerde systemen en de controleerbaarheid van de gegevensverwerking.

ad d. programmeringsstandaarden.
Standaardisatie in de programmering betekent onder meer uniformiteit in het gebruik van een programmeertaal. Hiermede kan (onder meer) worden voorkomen dat programma-fouten ontstaan, die resulteren in ongewenste modificatie van persoonsgegevens, de vernietiging, dan wel de openbaarmaking ervan.

ad e. maatregelen van interne controle.
Deze maatregelen hebben ten doel de volledigheid, juistheid en tijdigheid van de gegevensvastlegging, -verwerking en -verstrekking te verzekeren. Aan de controle op de bevoegdheden van de aanbieder van gegevens, respectievelijk de aanvrager van informatie dient voldoende aandacht te worden besteed.
Een greep uit deze maatregelen:

- zodanige invoercontroles dat geen "logisch" foutieve gegevens in het systeem verwerkt kunnen worden
- zodanige controles op de (volledigheid van de) gegevensverwerking dat onjuiste en onvolledige gegevensverwerking in een vroegtijdig stadium worden onderkend
- versluiering van wachtwoorden, opdat onbevoegden geen kennis kunnen krijgen van de codes gebruikt bij de beveiliging van bestanden, programmatuur e.d.

6) Zie bespreking in Datenschutzberater van 15-8-1978 (pagina's 120 t/m 124).

B. De organisatie van de gegevensverwerking

Ook aan de organisatie van de gegevensverwerking (dit is het computercentrum) gaat de privacy-wetgeving niet ongemerkt voorbij.
De Zweedse wetgever gaat zelf zó ver dat "zonodige richtlijnen met betrekking tot de gegevensverwerking kunnen worden gegeven" door de Data Inspection Board en kan worden aangegeven "welke apparatuur dient te worden gebruikt".
Enige controles zoals genoemd in de Anlage zu Paragraph 6 Abs. 1 Satz 1 BDSG (zie bijlage 1) zijn van toepassing op de organisatie van de gegevensverwerking zoals:

1. Speicherkontrolle
2. Transportkontrolle
3. Benutzerkontrolle
4. Uebermittlungskontrolle.

De controles 1 en 4 zijn ook van betekenis bij de ontwikkeling van een toepassing.
Wil men op afdoende wijze voorzien in de oplossing van de problemen die hiervoor zijn gedefinieerd, dan is een afgerond stelsel van algemene maatregelen van interne controle en beveiliging vereist.
Genoemd kunnen worden:

- functiescheiding
- screening van personeel
- procedures en voorschriften in het bijzonder ten aanzien van documentatie, programma-onderhoud, testen, overdracht van programmatuur, betrokkenheid van de gebruiker

De hiervoor genoemde maatregelen gelden ook ten aanzien van de ontwikkelingsorganisatie

- onderhoud aan de computer terwijl deze gedeeltelijk in bedrijf blijft of geheugens on-line blijven
- maatregelen met betrekking tot de betrouwbaarheid van de gegegevensverwerking
- de beveiliging van datacommunicatielijnen
- controle op het gebruik van de computer
- controle op het gebruik van de laatst geautoriseerde versie van programma's.

Aanvullende maatregelen hebben in het bijzonder ten doel de vertrouwelijkheid van persoonsgegevens te waarborgen zoals de beveiliging van computeruitvoer tegen ongeautoriseerde openbaarmaking/kennisneming door:

. de gegevensverwerking bij te wonen en na beëindiging van de verwerking de uitvoer door een geautoriseerde gebruiker te laten meenemen
. gebruik te maken van carbonloze kopieën

- toe te zien op het vernietigen van gegevens opgeslagen op SPOOL-files, tijdelijke bestanden en dergelijke (bij erasure wordt slechts de pointer verwijderd; de gegevens blijven dus ongemodificeerd bereikbaar)
- het verzegeld verzenden van geclassificeerde uitvoer
- het vernietigen van foutieve uitvoer en van verouderde microfiches
- geclassificeerde uitvoer gedurende de avond- en nachtshiften beveiligd te bewaren
- in geval van een zogenaamde panic dump (bijvoorbeeld ten gevolge van een stroomstoring) het gedeelte van de SPOOL-file waarop de gehele geheugeninhoud wordt gedumpt tegen ongeautoriseerde toegang te beschermen
- de tijdens de verwerking opgebouwde logtape met before en/of after images en/of mutaties beveiligd op te bergen.

Het belang van een procedurehandboek, waarin alle getroffen maatregelen, te ondernemen acties en verplichtingen van het personeel van het computercentrum zijn beschreven in geval persoonsgegevens worden verwerkt, moet niet worden onderschat.
De vertrouwelijkheid van de persoonsgegevens vereist echter eveneens dat de beschrijving van deze maatregelen niet in brede kring bekend moeten zijn.

Een dergelijke vastlegging geeft de bevoegde instanties een beeld van de zorgvuldigheid waarmee de gegevensverwerking is omkleed.
De vastlegging kan daarnaast dienen als uitgangspunt bij de controle van de handhaving en naleving van de beschreven instructies.
Voor de rol van de accountant hierin wordt nogmaals verwezen naar het reeds gememoreerde commentaar van het NIvRA op het interim-rapport van de Commissie Koopmans.

IV Invloed op de gegevensbeveiligingn

Een onderneming dient maatregelen te nemen dat de gegevensverwerking (binnen redelijke grenzen) in geval van een calamiteit kan worden gecontinueerd.
Dit betekent dat onder meer maatregelen dienen te worden getroffen ter voorkoming van, respectievelijk ter beperking van de gevolgen van Acts of God (brand, wateroverlast en dergelijke), diefstal van informatiedragers, misbruik van de computer of van informatie en dergelijke.
Concreter uitgewerkt betekent dit, dat zal moeten worden voorzien in:

- de fysieke beveiliging van het computercentrum.
  De Zugangskontrolle (BDSG) heeft hierop betrekking.

. andere beveiligingsmaatregelen, inclusief de beveiliging van programmatuur en bestanden, uitwijkprocedures en dergelijke.

Een zwakke plek in de beveiligingsorganisatie ontstaat nogal eens ingeval zich bijzondere omstandigheden voordoen.
Hierop dient in eerste instantie de automatiseringsleiding attent te zijn.

Enige praktische tips met betrekking tot de gegevensbeveiliging mogen niet ontbreken:

1. Berg persoonsgegevens achter slot en grendel op wanneer zij niet voor verwerking benodigd zijn.
2. Voorzie alle media waarop persoonsgegevens zijn vastgelegd van labels.
3. Voorzie media waarop persoonsgegevens zijn vastgelegd van gekleurde stikkers, zodat het opvalt wanneer zij worden gebruikt.
4. Houd de bestandenregistratie in het bijzonder ten aanzien van informatiedragers waarop persoonsgegevens zijn opgenomen voortdurend up-to-date.
5. Leg de bewaarplaats van genoemde informatiedragers vast.
6. Controleer alle persoonsgegevens zorgvuldig na bijvoorbeeld een computerstoring.
7. Verbied/voorkom bij de uitvoering van incidentele werkzaamheden het ophangen of opzetten van informatiedragers met persoonsgegevens omdat "het programma erom vraagt", maar bindt dit aan een opdracht van gebruikers.

In geval de verwerking van persoonsgegevens niet in het eigen computercentrum plaatsvindt, dienen zodanige maatregelen van beveiliging te worden getroffen dat anderen geen inzage kunnen krijgen in, respectievelijk de beschikking kunnen krijgen over deze persoonsgegevens (codering, encryption en dergelijke).

V Tot slot

In deze bijdrage heb ik aangegeven dat een nationale privacy-wetgeving van niet te onderschatten invloed kan zijn op de organisatie van de onderneming, de organisatie van de automatisering en de geautomatiseerde informatiesystemen.
In verschillende buurlanden is reeds wetgeving van kracht en uit de aangehaalde passages blijkt dat deze een belangrijke invloed doen gelden op (onder meer) het automatiseringsgebeuren.
Willen de Nederlandse ondernemers (inclusief hun automatiseerders) voorkomen dat zij in een te strak keurslijf worden gedrongen, dan "past" grondige bestudering van het te verwachten Ontwerp van Wet

en reageren op te vergaande beperkingen.
Een laatste opmerking:
De verzekeraars in West-Duitsland hebben een gat in de markt ontdekt: zij bieden de helpende hand bij Datenunfälle met hun Computer Missbrauch Versicherung.

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

Anlage zu § 6 Abs. 1 Satz 1

Werden personenbezogene Daten automatisch verarbeitet, sind zur Ausführung der Vorschriften dieses Gesetzes Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. Personen, die bei der Verarbeitung personenbezogener Daten tätig sind, daran zu hindern, daß sie Datenträger unbefugt entfernen (Abgangskontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. die Benutzung von Datenverarbeitungssystemen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden, durch unbefugte Personen zu verhindern (Benutzerkontrolle),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können (Übermittlungskontrolle),
7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu gewährleisten, daß bei der Übermittlung personenbezogener Daten sowie beim Transport entsprechender Datenträger diese nicht unbefugt gelesen, verändert oder gelöscht werden können (Transportkontrolle),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

§ 9. *Inzage en verbetering*

Artikel 69. 1. De houder van een registratiesysteem deelt aan een ieder die daarom verzoekt mede of gegevens betreffende de persoon van de verzoeker zijn geregistreerd.

2. Indien gegevens betreffende de persoon van de verzoeker in het registratiesysteem zijn opgenomen stelt de houder hem, desverlangd in schriftelijke vorm een volledig en eenvoudig te begrijpen overzicht van deze gegevens ter beschikking.

3. De Registratiekamer kan ten aanzien van een registratiesysteem bepalen, dat de in de leden 1 en 2 bedoelde informatie niet of slechts onder bepaalde omstandigheden in schriftelijke vorm mag worden verstrekt. In dat geval bepaalt de Registratiekamer, de houder gehoord, op welke wijze het inzagerecht kan worden uitgeoefend.

4. Bij reglementsplichtige en vergunningsplichtige registratiesystemen wordt in het reglement geregeld op welke wijze aan de verplichting van de leden 1 en 2 toepassing zal worden gegeven.

5. De houder van het registratiesysteem draagt zorg dat voldoende waarborgen bestaan voor de identificatie van degene die verzoekt om mededeling of inzage overeenkomstig de leden 1 en 2.

6. De houder kan voor de inzage een kostenvergoeding verlangen, die niet hoger mag zijn dan een bij of krachtens algemene maatregel van bestuur vast te stellen bedrag. Deze vergoeding moet worden teruggegeven wanneer de houder vervolgens op verzoek van de geregistreerde tot verbetering overgaat overeenkomstig artikel 70, of daartoe ingevolge artikel 72 een bevel van het gerechtshof krijgt.

Artikel 70. 1. De houder is verplicht op verzoek van een persoon wiens gegevens het betreft over te gaan tot verbetering van de gegevens op de in het verzoek aangegeven wijze of tot verwijdering ervan, indien de gegevens onjuist zijn of, gezien de doelstelling van het systeem, niet ter zake doende, dan wel in strijd met het reglement zijn opgenomen of niet verwijderd.

2. Eveneens is hij verplicht, indien gegevens ontbreken die ingevolge het reglement vermeld hadden kunnen zijn, over te gaan tot aanvulling van gegevens op de in het verzoek aangegeven wijze, voor zover dit met de inrichting van het registratiesysteem te verenigen is.

Artikel 71. 1. De houder van het registratiesysteem geeft aan de verzoeker binnen twee maanden na ontvangst van een overeenkomstig het vorige artikel gedaan verzoek schriftelijk bericht of hij daaraan voldoet.

2. Een weigering van de houder is met redenen omkleed.

Artikel 72. 1. Indien de houder van het registratiesysteem na verloop van twee maanden niet heeft bericht dat hij aan een overeenkomstig artikel 70 gedaan verzoek voldoet, kan de verzoeker zich tot het gerechtshof te ..... wenden om de houder te bevelen aan het gedane verzoek te voldoen.

2. Het verzoek moet bij het gerechtshof worden ingediend binnen twee maanden na de verzending van de weigering van de houder, of, indien de houder niet binnen de gestelde termijn heeft gereageerd, binnen twee maanden na afloop van die termijn.

3. Indien de verzoeker zich binnen de in het vorige lid bedoelde termijn van twee maanden tot de Registratiekamer heeft gewend met het verzoek te bemiddelen of te adviseren in zijn geschil met de houder, dan verklaart het gerechtshof de verzoeker nog ontvankelijk indien hij zich tot het gerechtshof heeft gewend binnen twee maanden nadat de Registratiekamer hem heeft bericht geen stappen meer in de zaak te willen doen.

4. Het gerechtshof wint het advies van de Registratiekamer over het verzoek in tenzij het reeds aanstonds oordeelt dat het verzoek niet ontvankelijk is, of de Registratiekamer reeds overeenkomstig het derde lid bemoeienis met de zaak heeft gehad.

5. Het gerechtshof wijst het verzoek toe indien de weigering van de houder in strijd is met artikel 70.

6. De twaalfde titel van het Eerste Boek van het Wetboek van Burgerlijke Rechtsvordering met uitzondering van artikel 429d, derde lid, is voor procedures naar aanleiding van een verzoek als bedoeld in het eerste lid van toepassing.

7. Van de eindbeschikking van het gerechtshof staat beroep in cassatie open.

Artikel 73. 1. De houder van een registratiesysteem die overeenkomstig artikel 70 of 72 aan een verzoek van de geregistreerde voldoet, is verplicht om aan hen van wie hij kan nagaan dat zij in het jaar voorafgaand aan het verzoek en in de sinds dat verzoek verstreken periode onjuiste, niet ter zake doende of onvolledige gegevens hebben ontvangen, mededeling te doen van verbetering, verwijdering of aanvulling van gegevens.

2. Het eerste lid geldt niet, indien de verzoeker te kennen heeft gegeven op het doen van mededeling geen prijs te stellen.

Artikel 74. Indien de rechter een verzoek als bedoeld in artikel 72 heeft afgewezen, kan de verzoeker gedurende één jaar na het onherroepelijk worden van de afwijzende beschikking in volgende verzoeken bij het gerechtshof ten aanzien van dezelfde gegevens uit hetzelfde registratiesysteem niet worden ontvangen.

EEN COMPUTER-CONTROLETOEPASSING MET EEN IMS-DATA BASE

door H. Weerd

Achtergrond van de toepassing

Met ingang van 1970 wordt bij een van onze cliënten gebruik gemaakt van een aantal computerprogramma's als hulpmiddel bij de accountantscontrole. Aan de hand van een aantal door de controlegroep opgestelde wensen zijn door de AC-groep computerprogramma's ontwikkeld, waarmee per kwartaal de volgende informatie wordt verstrekt:

1. een saldibalans die is samengesteld uit de mutaties op de grootboek-rekeningen;
2. een overzicht van geselecteerde posten uit de mutaties, die voor de controle van belang zijn.

Het ontwikkelen van deze computerprogramma's heeft destijds ca 250 uur gekost. Per kwartaal worden de hierboven genoemde overzichten op de computer van de cliënt, onder toezicht van de AC-programmeurs vervaardigd.
Voordelen voor de controlegroep waren:

a. geen zoekwerk meer in het grootboek van de cliënt voor de te controleren posten;
b. zekerheid dat alle mutaties in de eindtotalen zijn opgenomen en dat alle mutaties de selectiezeef passeren;
c. beoordeling van de eindtotalen, voordat er gecontroleerd wordt, maakt de controle doeltreffender.

Doordat dat de saldibalans in gecomprimeerde vorm werd afgedrukt, was de papiermassa beduidend kleiner.
Van het voorgenoemd programma is 8 jaar zonder noemenswaardige verandering gebruik gemaakt.

Wijziging in het systeem

Door belangrijke wijzigingen in het informatiesysteem van de cliënt per 1 januari 1978 waren wij genoodzaakt onze computerprogramma's aan te passen. Onze cliënt ging gebruik maken van een programmapakket voor de registratie en verdere verwerking van de grootboek-gegevens.
Het betreft hier het "General Ledger and Financial Reporting System" van de leverancier "Software International".
Voor de gegevensopslag van de grootboek-gegevens wordt in deze toepassing van het programmapakket gebruik gemaakt van onder andere een IMS-data base.

Data base aspect bij onze toepassing

Voor de overdracht van gegevens tussen een toepassingsprogramma en een data base is het noodzakelijk dat er vooraf een beschrijving wordt gemaakt van het desbetreffende deel van de data base, waarop gegevensoverdracht zal plaatsvinden.
Met behulp van de in deze beschrijving opgenomen informatie komt vervolgens op het moment van uitvoering de koppeling plaats tussen het toepassingsprogramma en het data base management systeem. Vervolgens kan de gegevensoverdracht tussen het toepassingsprogramma en de data base worden uitgevoerd.
Bij een IMS-data base vindt de hierboven genoemde beschrijving plaats met behulp van een "Program Specification Block" (PSB).

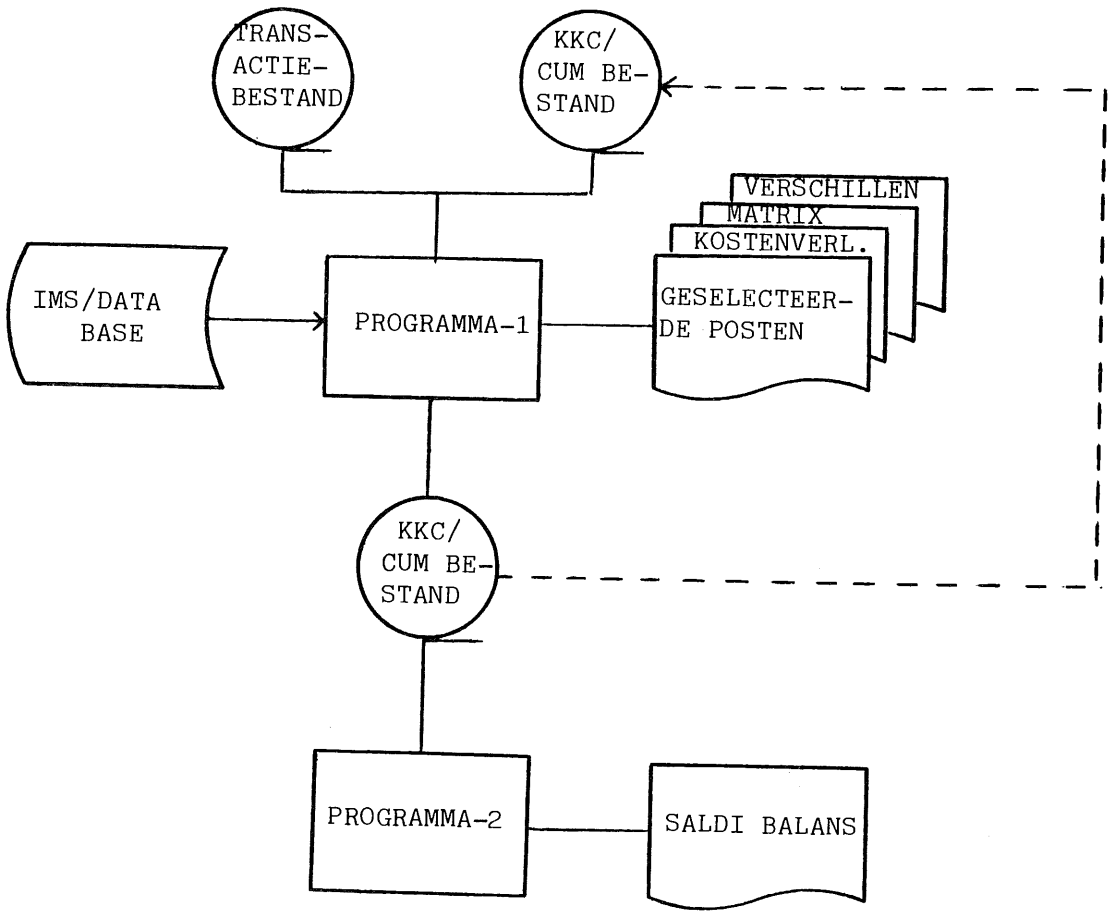
Na overleg met de cliënt bleek dat wij voor onze toepassing gebruik konden maken van een PSB dat reeds voor een ander toepassingsprogramma - van de cliënt - beschikbaar was.

Met behulp van het ons beschikbaar gestelde PSB hebben wij voor onze toepassing uitsluitend lees-toegang tot bepaalde segmenten in de data base. Hierdoor kunnen wij de gegevens uit de segmenten selecteren en op overzichten laten afdrukken.

Wijzigingen in de controle-toepassing

Naast het aanbrengen van de noodzakelijke wijzigingen heeft tevens een uitbreiding plaatsgevonden. Door de computerprogramma's wordt nu vastgesteld of alle mutaties, die in het geautomatiseerde systeem van de cliënt zijn vastgelegd, hun weerslag hebben gevonden in de cumulatieve totalen per rekeningnummer. Dit wordt bereikt door het in ons beheer houden van een magneetband met totalen per rekening. Bij de verwerking van een volgende periode worden de transacties van de desbetreffende periode per rekening geteld bij de cumulatieve totalen van onze magneetband. Het resultaat van deze optelling wordt vergeleken met de in de IMS-data base vastgelegde totalen van de desbetreffende rekening. Eventuele verschillen worden op een overzicht afgedrukt. Een magneetband met totalen per rekening tot en met de verwerkte periode wordt vervolgens weer in ons beheer gehouden.
Tevens wordt van een aantal kostensoorten (salarissen en algemene kosten) zogenaamde matrices vervaardigd, aan de hand waarvan deze kunnen worden beoordeeld en zonodig nadere controlemaatregelen kunnen worden genomen.
In de matrices worden de kostensoorten per aangegeven grootboekrekening per maand afgedrukt en de cumulatieve totalen per kwartaal.
Van de voorgaande kwartalen worden de gegevens vastgehouden, zodat aan het eind van het jaar een 13-perioden-overzicht ontstaat.

In het onderstaande schema is een weergave gegeven van de beschreven controle-toepassing.



Systeemstroomschema van de controletoepassing.

Kosten en voordelen van de toepassing

Het aanbrengen van de wijzigingen en aanvullingen heeft in totaal ca 370 uur in beslag genomen.

De jaarlijkse besparing op de bestede controletijd is moeilijk exact te bepalen, omdat naast minder werk (tellen en doorchecken van posten is komen te vervallen en minder zoekwerk) de kwaliteit van de controle is verbeterd. Een globale benadering van de bereikte besparing kan gesteld worden op 10 à 12 weken per jaar, voornamelijk werkzaamheden van een junior assistent.

LITERATUUROVERZICHT

door B.M. de Vries

In de A.C.-bibliotheek opgenomen boeken

AC 209 Data Security Design Handboek - IBM.

Trefwoord: B 4H (beveiliging, A 4H (systeem realisatie).

Before date protection measures can be determined, a thorough knowledge of the threats and deficiencies that affect computer installations is essential. A detailed study of errors and omissions, that is, unintentional threats to data security, was conducted in Sweden, with the aim of creating a foundation for the design of suitable protective measures in computer installations. Information was collected from 800 cases of unintentional threats in nine different installations, and classified into 72 categories.
From this data, the deficiencies that caused the threats were analyzed.

Using this material as a basis, IBM has developed practical instructions on how to identify individual problems and take appropriate measures, and published the Data Security Design Handbook. Even though the initial study covered only unintentional threats, the handboek also deals with intentional threats.

The Data Security Design Handbook provides a foundation for the implementation of a systematized data security project. But resources must be available to implement this project, which means that top-level executives in the companies concerned must be aware of the problems that exist.

It is essential that management know the status of its own data protection. The study that formed the basis for the recommendations in the Data Security Design Handbook indicated clearly that computerized information processing is exposed to threats. These threats tend to be trivial, everyday events with minor negative consequences in themselves but taken together, they constitute an unnecessary, and avoidable risk to the company.

A methodical and target-oriented data security project can create a sound data security system that costs less than the damage costs that the system can attempt to eliminate.

AC 211 Composite/Structured design - Glenford J. Myers.
Van Nostrand 1978 (Engels 174 blz.)

Trefwoorden: A 22 (gestructureerd ontwerp).

Composite/Structured Design presents an program design methodology with the goal of producingg programs of higher reliability and extensibility. Composite design (also know as structured design) is explained in this book by discussing the underlying theory and then using procedureal examples, case studies, and exercises to illustrate the concepts. The relationships to such areas as other programming methodologies, the "Jackson design method", and programming languages, are discussed.

Composite/Structured Design gives the programmer or systems analyst a set of objectives and methods to design the structure of medium- or large-sized programs. Although the book is oriented to the design of aplication programs, the ideas also have been used in the designs of system software (e.g. operating systems, compilers) and microprograms.
This book is an extension and refinement of the author's first book on this subject, Reliable Software Through Composite Design (Petrocelli/Charter, 1975).

Composite/Structured Design is must reading for every programmer, systems analyst, programming project manager, and computer science student. The design of highly reliable, maintainable, and extensible programs is fundamental to the economics of computing systems and data processing.

UIT DE TIJDSCHRIFTLITERATUUR

Grensoverschrijdend informatieverkeer vereist nationale en internationale regels. - G. Russell Pipe

- S 299

uit: Automatiseringsgids 31 mei 1979

Trefwoord: E 30, E 31, (wettelijke regelingen ten aanzien van informatie), K 40 (privacy).

Een belangrijk gevolg van de snelle technologische ontwikkelingen op het gebied van de informatieverwerking en de telecommunicatie is, dat de beweeglijkheid van informatie toeneemt. Informatiestromen passeren in toenemende mate de nationale grenzen als gevolg van de onderlinge betrekkingen van landen, internationale organisaties en multinationale ondernemingen. Deze toename van internationale informatiestromen, ofwel grensoverschrijdend informatieverkeer, heeft natuurlijk nog al wat consequenties op gebieden als: nationale souvereiniteit, staatsveiligheid, eigendomswetgeving, gegevensbescherming en dergelijke. G. Russell Pipe bekijkt in dit artikel met name de juridische, economische en sociaal-culturele aspecten van grensoverschrijdend informatieverkeer.

The protection of computer facilities and equipment: physical security - T.E. Diroff

- S 259

Uit: Data base Summer 1978

Trefwoord: B 40 (algemene computerbeveiliging).

Alhoewel iedere beveiliging van geautomatiseerde gegevensverwerking in principe doorbroken kan worden, blijft het van eminent belang risico's, die de voortgang van de geautomatiseerde gegevensverwerking bedreigen, zoveel mogelijk te beperken.
Binnen de organisatie behoren een of meerdere van andere functies onafhankelijke personeelsleden met de verantwoordelijkheid van de security te worden belast. Deze functionaris dient direct onder de topleiding te ressorteren.
Grondslag van het beveiligingsplan dient te zijn een risico-analyse, bevattende

1. mogelijke gevaren, waaraan de computerinstallatie blootgesteld is of wordt.
2. schatting van de kosten, die het zich voordoen van deze gevaren met zich meebrengen
3. schatting van de kans, dat deze gevaren zich voordoen.

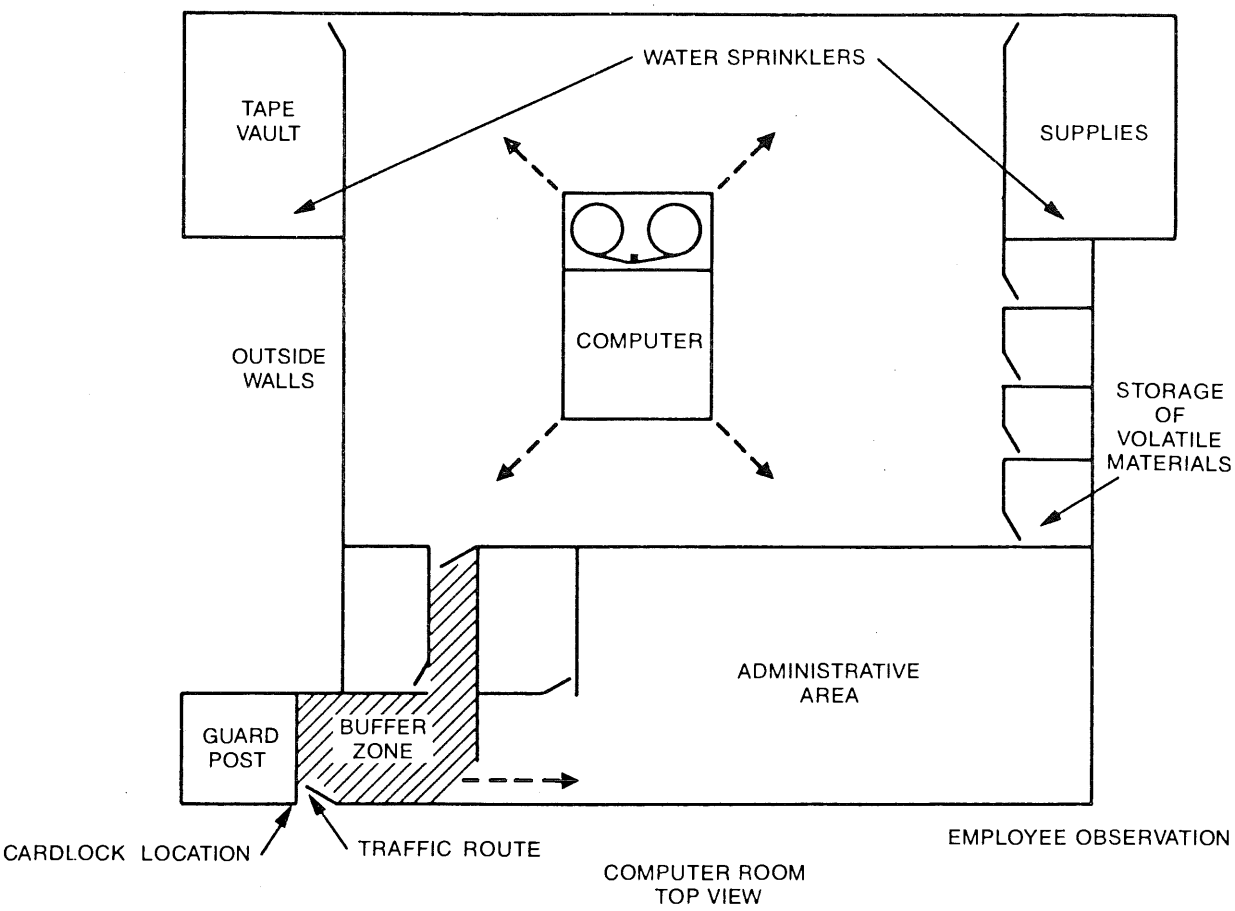
Voor wat betreft de fysieke beveiliging in 't kort de volgende aanbevelingen: (zie figuur)

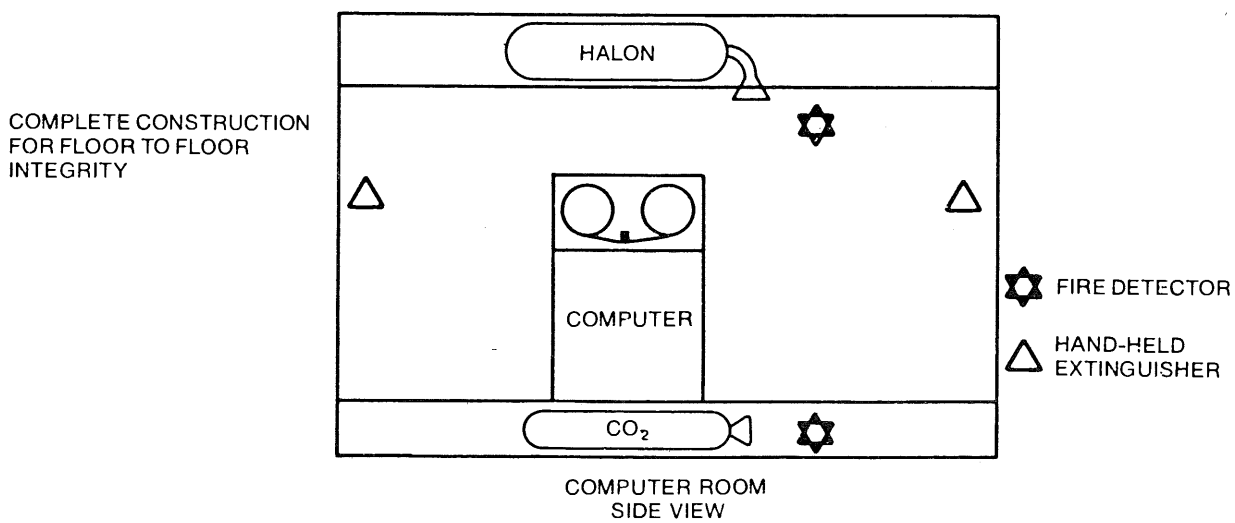
- situeer de computerinstallatie in een afzonderlijk gebouw vanwege de daardoor onstane grotere beveiligingsmogelijkheden
- zet de computerinstallatie in het midden van de computerzaal omdat
  1. een locatie dicht bij muren en ramen een grotere trefkans op gevaren van buitenaf heeft
  2. het centrum van een ruimte door het personeel beter geobserveerd kan worden.
- Eventuele brand bij een computerinstallatie kan met Halon-apparatuur het meest effectief besteden worden. Halon is echter ten opzichte van CO_2 en water erg duur.
  Opslagplaatsen van tapes, papiervoorraden en dergelijke worden daarentegen uitgerust met spinklers (water).
- branddetectie-apparatuur zowel in het plafond als onder de vloer (ten behoeve van kabels). De branddetectors, die reageren op rookontwikkeling door middel van ionisering verdienen de voorkeur vanwege de snelheid van melding.
- een goed uitgewerkt en getest noodvoorzieningenplan.
- de toegang tot de computerzaal beveiligen door een samenstel van de volgende maatregelen:
  - identificatie van de persoon
  - passwords
  - sleutel of toegangskaart met gemagnetiseerde strip
  - bewakingsdienst
  - buffer zones
  - toegangsdetectors (7 soorten worden aangeduid).
- uitwijkfaciliteiten goed regelen; bijvoorkeur op andere locatie.
- adequate verzekering.

Het samenstel van maatregelen op het gebied van de fysieke beveiliging dient regelmatig onderzocht te worden op

- effectiviteit
- geschiktheid
- optimale kosten-nut verhouding
- snelheid van reactie.

Naast een regelmatige beoordeling is een goede planning essentieel.





Computer Room Equipment Placement

DATA BASE SUMMER 1978

The computer service center: should it be visited? - A. Ussher

Uit: the South African Chartered Accountant (december 1978) -P 282

Trefwoord: E 92 (controle van serviceverwerking).

Service bureau revenue in South Africa has been growing at about 25-30 percent each year, but the industry itself is far from stable. Small bureaus open and close with startling frequency. Bigger bureaus are subject to mergers and acquisitions.

Small businesses often use service bureaus because they cannot justify the cost of installing their own computer hardware. Because a bureau enjoys the economies of scale associated with large, powerful computers, larger businesses may find it offers a cost saving. No matter what type of service is provided, it seems certain that the business world will make more use of service bureaus. As a result, auditors will become increasingly involved with clients that use service bureaus.

The fact that a bureau is involved in financial processing does not change an organization's requirement to generate and control information. Assets and financial records must be adequately safeguarded.
However, use of a bureau does add a step to the processing procedures and involves a legally separate organization in the record-keeping process. This kind of involvement may affect the scope of the auditors examination.

Auditors must learn to cope with some of the problems associated with the use of service bureaus. These include:

- Gaining access to client files and records which are physically and legally controlled by an outside party
- A third party now deeply involved in the audit
- Processing techniques used by the bureau which may not be familiar to either the auditor or his client.

In spite of these problems, an auditor's approach must be basically the same as if an in-house computer was used. Internal controls must be evaluated. The review of these controls must include both client and bureau procedures.

Very little of the evaluation of service bureau controls is being undertaken by auditors in South Africa. A questionnaire about auditor involvement was sent to all service bureaus. Based on the returns, it appears that only three percent of client auditors ask for access to the bureau to observe their client's processing. About 18 percent of the auditors look at administrative controls or documentation relating to the processing of their client's records.

To carry out his duties, the auditor must know something about the service bureau and its operations. This information can be obtained only by:

- Reviewing the contract
- Visiting the service bureau
- Studying the bureau's documentation
- Examining a report from an independent auditor engaged to review the center's operating procedures.

In a given set of circumstances, all four of these information sources may not be available. When this happens, the auditor must rely on a combination of the available sources in order to assess the reliability of the bureau. Among the factors to be evaluated are:

- Financial stability of the bureau (Dependence on one or two major clients may be a problem. Loss of one such client could cause the bureau to fail.)
- Arrangements for coping with a power or hardware failure
- Integrity of the bureau's management in maintaining the quality of its personnel (Staff turnover rates should be reviewed.).

The auditors decision not to visit the service center may be correct, but it might be based upon the wrong reasons. Under some conditions, the bureau must be visited.
The article lists a number of such conditions such as:

- When a center process several client systems
- When the bureau exercises critical controls (e.g., batch ba- - lancing)
- When computer assisted audit techniques are to be employed.

Basically, if reliance is to be placed on controls and procedures at the service center, it is the auditor's duty to ensure that these controls and procedures are adequately performed.

Even if an audit visit to the bureau is not required, it may be of service to the client. The auditor should try to convince the client that he should make such visits on his own on a periodic basis.

The concept of service bureau visits presents some very real problems. The service centers may not want to cooperate with such visits. They may feel the amount of income they derive from the auditor's client does not justify the time they would have to spend in cooperating with a visit.
Further, the visit itself may be a violation of the center's own security. In particular, this might be the case when the bureau runs a specialized industry application package for many users. A bureau with 200 or more clients might simply not have the time to deal with many different sets of auditors.

To relieve this problem, the concept of a third-party auditors has evolved. This auditor would review and report upon the controls over the center's processing. The client auditors would consider the thirdparty auditor's work in determining the scope of their work. Client auditors would have to evaluate the data that serves as input to the center's processing. Some of the problems of the third-party audit concept, as listed in the article, include:

- It would take extensive work to satisfy the requirement of all the user auditors. Most of this work would be beyond that for the service center's normal audit.
- Report timing might not satisfy all users.
- User and third-party auditors might have different audit approaches.
- There are no established standards for control reviews and reporting.

CONCLUSION

When a client uses a service center for processing accounting records, the auditor has additional responsibilities. The surveys mentioned in the article indicate that auditors do not always accept this responsibility. As a result, the fraud deterrent aspects of an audit are greatly reduced.
Computer professionals have a low opinion of auditors' expertise in EDP. In part, this opinion is based upon the auditors' obvious reluctance to visit service centers.

The situation revealed by the survey is a serious one. A major fraud in a service center is likely to bring charges of audit negligence. If the auditor never visited the center, it will be difficult for him to defend against these charges.

What makes a system reliable? - George A. Champine

Uit: Datamation (september 1978) - verkorte weergave 0 161

Trefwoord: A 90, A 42, B 53.

Unreliability in a commercial aircraft is completely unacceptable. It is not tolerated. In computer systems, unreliability is an accepted way of life. This is an intolerable situation. We should begin to expect perfection from our computer systems.

FAIL-SOFT SYSTEMS

Failure in an interactive computer system can have a serious impact on users.
Systems must be designed so that they are fail-soft-- the failure of a component will degrade, but not halt, processing.
Some of the common fail-soft techniques are:

- Redundancy of system units
- Automatic reconfiguration (i.e., work around the element that failed)
- Automatic recovery following transient faillures
- Error correction codes to fix main storage failures
- Automatic retry of instructions that failed.

Systems recovery planning should be based upon realistic mean time between failures (MTBF) data, but this is often difficult to obtain. Hardware salesmen do not like to discuss failure rates.

The author cites an example of an important interactive system that was only able to remain operational 76 percent of the time. The main problem was the combined reliability of the ten nonremovable mass storage devices. By fine tuning, the careful matching of component, and adding a spare, vendor factory personnel were able to bring availability up to 96 percent.

Vendor and user personnel must work together to achieve a satisfactory level of system reliability and efficient recovery. Under normal field conditions, a typical large scale computer may be unavailable from two to five percent of the time. At the same time, one large time-sharing service has its system available 99.5 percent of its scheduled time. The difference can be largely attributed to management's dedication to reliability and continuing pressure on the vendor's customer engineers.

COMPONENT RELIABILITY

All systems are constructed from a wide range of component. Ultimately, each component will fail. Failure rates are common early in a system's life and peak again as the system nears the end of its life cycle.
Early failures are usually caused by manufacturing defects and late failures by old age.

SYSTEM RELIABILITY

Two additional terms must be defined in order to discuss reliability. Mean time to repair (MTTR), as a term, is quite descriptive. However, it must also include time for reruns and

file or data base reconstruction. Availability can be expressed as MTBF divided by MTBF plus MTTR. The author expands on these topics by describing how the availability of individual components must be concidered when determining overall systems availability.

SYSTEMS INTEGRITY

If the integrity of the data produced by a system is questionable, the system is worthless. The systems must be able to detect errors and keep them from contaminating the data files. Comprehensive error detection is essential in any system that requires high availability.

SYSTEM MAINTAINABILITY

Vendors are changing their approach to systems maintenance and repair. The use of on-site maintenance personnel is rapidly becoming prohibitively expensive. Other techniques must be employed.

Most maintenance alternatives involve the use of additional hardware. One approach is based on providing two or more of every system component. If a component fails, another takes its place.

REMOTE MAINTENANCE

In this approach, the maintenance processor is at a vendor facility and accesses the user's equipment via a telecommunications facility. Used since 1975, remote maintenance seems to be working well.

REDUNDANT SYSTEMS

Two forms of redundant systems are common: standby systems and multiprocessor systems. With a standby system, a complete second system is installed. The secondary system handles batch processing tasks while the primary system is on-line. If the primary system fails, the secondary system takes over.

The multiprocessor approach uses a single system that has two or more of each component, including central processors. When a component fails, the system is automatically reconfigured to work around the unit that failed. The system will continue processing, but performance will be degraded.

SOFTWARE RECOVERY FROM HARDWARE ERRORS

A number of different types of software recovery are available:

- Correcting or rereading data errors from mass storage devices
- Generating duplicate copies of files to provide backup
- Generating an error log
- Establishing checkpoints during long jobs so a restart, if required, will not have to go back to the beginning of the job.

The original article contains a longer list of software recovery techniques.

The author also provides a longer discussion of software recovery of a data base after a hardware failure. When data base management software (DBMS) is used in a system that furnishes on-line processing of transactions, recovery problems can become quite complex. Most DBMS packages provide for recovery from mainframe errors, but software errors or physical damage to the mass storage media can create very difficult recovery problems.

SOFTWARE RELIABILITY

A very helpful table of software reliability parameters is included in the article.
It gives characteristic values for factors like average number of initial program errors and average computer time to fix an error.

One negative development has also appeared. The use of on-line terminals to write and debug programs can encourage sloppy programming. By relying so heavily on the computer, the programmer may develop careless work habits. This can serve to decrease program reliability.

FUTURE SYSTEMS RELIABILITY

Future systems will be more complex, so reliability will be more important and more difficult to achieve. The author presents a brief case to illustrate his point.

Since the reliability of each component has an impact on overall reliability, planning must consider the characteristics of each device.

Data security - A "Common sense" approach pays off
- F.W. Miller

uit Infosystems (augustus 1978) - verkorte weergave P 278

Trefwoorden: B 42, B 43, B 44 (gegevensbeveiliging).

A commonsense approach is the best way to look at data and computer security.
Management wants to know: "What am I protecting and how much will it cost?" To answer these questions, a cost/benefit analysis must be used to assess risk and select security meausures.

In a data processing shop, security can be divided into two sectors - (1) protection of the physical equipment and the computer room, and (2) protection of the data from misuse and abuse.

It might be assumed that most DP installations are protected against unauthorized intrusion and natural disasters. However- the author cites a bombing incident that shows this assumption may be invalid.

Data security, which should be of primary importance in most computer installations, is simply the protection of data, a valuable corporate asset, from destruction, modification, or disclosure. In setting up a data security program, the problems caused by a suspension of DP services are sometimes overlooked. Recently, some groups have been thinking about this problem. They are exploring the possibility of joinly-funded emergency backup sites for large systems users.

A group in Southern California is planning a backup facility that subscribers could use in case of a disaster, but which might als be available to handle overload work. The group is also developing reciprocal agreements with similar groups elsewhere in the country. These agreements would serve as an additional safeguard in case of a widespread physical disaster in the Los Angeles area.

A sixteen-company group in the New York City area has hired a Big-Eight public accounting firm to conduct a feasibility study of a shared EDP contingency center.
The study will include developing compatible equipment configurations and establishing operational procedures.

The biggest threat to data security is accidental misuse of information or systems by authorized users. Since data is a

valuable corporate asset, management should realize it must protect that data. In practice, most security measures are not expensive, but they do take time.

Computer crime seems to be becoming a serious threat. Preventing the unauthorized use of data involves certain basic controls:

- Assign responsibility for the finite data elements in the system.
- Maintain a separation of duties between those who use the system and those who change the system.
- Limit physical access to the facility.
- Assign accountability for data.
- Require the use of journals or logs to record alle system activity.
- Track system variances to make sure they are resolved.

At a bank auditors' conference, an IBM representative outlined some steps to take in evaluating data security:

- Identify what will be protected.
- Identify the hazards that each resource must face.
- Assign a dollar cost or value to each exposure.
- Determine the expected probability of an exposure's occurrence. (The number of people who can cause a particular kind of damage is a large factor in determining this probability.)

  Once the annual cost of a risk has been determined, one of three different protective measures can be taken:

  - Tolerate the exposure by doing nothing.
  - Lower the dollar impact if the loss occurs.
  - Lower the probability of the loss occurring.

  Data security also involves considering the use of encryption techniques. Typically, encryption is applied to data transmitted over communication lines. When communications facilities are being employed, they are largely outside the control of the using organization. The threat of wire-tapping is a real one.

  To demonstrate the problem, at a recent computer show engineers from Motorola exhibited an electronic device they had assembled from $ 600 of parts purchased at a computer hobby store. Their passive wiretap unit was able to monitor and display messages between a terminal and a simulated host computer. When a data encryption device was placed on both ends of the communications line, the wiretap produced only unintelligible data. A number of firms are now manufacturing data encryption devices.

Management may look upon data security as a complex problem, which it is, but a commonsense approach will reduce the problem to a manageable size. As advances in technology encourage the concentration of EDP resources in new ways, installations become more susceptible to individual hazards. At the same time, this concentration makes it possible to apply economies of scale to protective measures.

Automatisering
Beveiliging
Controle
NIEUWS

door H.C. Kocks

Automatisering

Grote vertraging bij aflevering IBM's 38 systemen

Aldus de kop van een artikel in de Automatisering-gids van 6 september 1979. Naast het feit dat in het artikel wordt ingegaan op de oorzaak van de vertraging vraagt de schrijver zich af of aankondiging van nieuwe systemen in een prematuur ontwikkelingsstadium wel verantwoord is en of de gebruiker ermee gediend is.

IBM Nederland heeft vorige maand per brief zijn klanten medegedeeld dat de eerste afleveringen van de in oktober 1978 geannonceerde nieuwe computersystemen 38 aanmerkelijk zijn vertraagd. Hoewel het de bedoeling was dit najaar met de eerste installaties te beginnen, verwacht IBM nu dat de eerste leveringen pas medio 1980 zullen plaatsvinden, wat op zich een vertraging is van zes tot negen maanden.

Deze mededeling van IBM is de eerste sinds mensenheugenis, dat de maatschappij de door haar gestelde afleveringsdatum van een nieuw ontwikkeld computersysteem niet kan waarmaken. De problemen bij de 38 liggen voornamelijk bij de ontwikkeling van het nieuwe besturingssysteem voor de 38, de Control Program Facility.
De CPF zou volgens IBM bij de annoncering van de 38 ervoor zorgen dat veel werk dat verbonden is aan het besturen van systeemtaken en de systeemelementen van de gebruiker naar de computer zouden worden verlegd. Het systeem 38 zou daarbij een viermaal zo groot vermogen hebben dan een van zijn voorgangers, zoals het systeem 3. Op dit moment blijkt dat de 38 qua vermogen gelijk of iets boven dat van het systeem 3 ligt.
Om deze problemen op te lossen werken thans in de Amerikaanse plaats Rochester, Minn. meer dan 400 programmeurs/systeemanalisten aan de problematiek rond de 38, terwijl daarnaast nog eens 300 man zijn ingezet voor de ontwikkeling van het database systeem van de 38.
Volgens berichten in de Amerikaanse pers zouden deze mensen momenteel 10 tot 20 uur per week overwerken om sneller uit de problemen te komen.

Wat de financiële gevolgen zijn voor IBM is moeilijk na te gaan. Wel is bekend dat IBM volgens Amerikaanse marktanalisten voor de 38 zo'n 32.000 opdrachten heeft gekregen, die in koopprijzen variëren van 100.000 tot 600.000 dollar. Deze marktanalisten hadden de verwachting dat IBM in de eerste vijf jaar van levering wel eens 82.000 systemen 38 zouden installeren met een totale geraamde waarde van 30 miljard dollar. Bij deze

aantallen vallen de eerste 1400 afleveringen voor dit najaar, die nu pas medio 1980 zullen aanvangen in het niet.
Een van de grootste konkurrenten om van deze vertragingen te profiteren is IBM zelf. De 38 wordt namelijk op de markt gebracht door de General Systems Div., terwijl een van de belangrijkste konkurrenten van de 38, de kleinere modellen zijn in de begin 1979 door IBM's Data Processing Div. geannonceerde 4300 serie computers.
Wel blijft bij dit alles, dat de gebruiker met dit soort ontwikkelingen niet is gediend. Hoewel IBM in zijn brief aan klanten zegt, "dat de extra tijd die nodig is voor het integreren en uittesten van de nieuwe software-technologie die deel uitmaakt van het systeem 38 en waardoor het als uitgangspunt genomen prestatieniveau kan worden gehandhaafd, het belang van de toekomstige gebruiker wordt gediend", zou men zich beter kunnen afvragen of gebruikers eigenlijk wel zijn gediend met aankondigingen van nieuwe systemen, die nog in zo'n prematuur ontwikkelingsstadium zijn, dat zelfs de leverancier de daarbij optredende problemen niet goed heeft onderkend, en/of heeft opgelost. Zonder deze vroegtijdige annonceringen, die overigens niet alleen door IBM worden gedaan, zouden gebruikers wellicht een meer verantwoorde keuze kunnen maken uit werkelijk bestaande goed werkende systemen om hun automatiseringsproblemen op een zo adequaat mogelijke wijze op te lossen.

De komst van de 4300 serie van IBM heeft veel teweeggebracht in de automatiseringswereld. Dat de 4300 duidelijk verschilt van haar voorgangers blijkt wel uit het feit dat de aanpak van het systeemonderhoud door IBM is gewijzigd. Het volgende artikel geeft een goed beeld van de "nieuwe aanpak".

Gelijk met de annoncering van het nieuwe 4300 systeem heeft IBM een belangrijke wijziging aangekondigd in de aanpak van zijn hardware- en software-service. Een service-processor en een via telefoonlijnen te raadplegen databank zijn de nieuwe hardware-service ontwikkelingen. Op software-service gebied gaat IBM door de komst van de 4300 serie zijn support-organisatie ook drastich veranderen. De belangrijkste schakel in de nieuwe organisatie zal dan het Support Centrum worden.

De nieuwe aanpak is mogelijk geworden door de nieuwe programmatuurfilosofie, die heeft geleid tot een grotere zelfstandigheid van de gebruiker op het gebied van systeembeheer, programma-ontwikkeling en systeemgebruik, en daarmee tot een ruimere keuze in servicepakketten met de mogelijkheid tot kostenbesparingen.

HARDWARE-SERVICE

Als in het verleden een fout optrad in de hardware van een systeem, moest de technicus ter plaatse de fout rekreëren om deze te lokaliseren en te repareren. Bij het IBM 4300 systeem wordt een snellere en meer efficiënte methode gebruikt, die mogelijk is dank zij de aanwezigheid van een zogenaamde service-processor. De service-processor verzamelt

automatisch maximaal 1300 bytes aan informatie over de hardware-fout. Hij voert een "Log-Analysis"-programma uit, dat meestal resulteert in het beschikbaar komen van een referentiekode. Deze kode geeft aan waar de fout zit en welke printplaat moet worden vervangen. Daarmee vervalt in de meeste gevallen het rekreëren van de fout en het lokaliseren van het defekte onderdeel.

Een belangrijk voordeel van het gebruik van een service-processor is dat nu veel gemakkelijker intermitterende fouten gelokaliseerd en verholpen kunnen worden. Ook als het systeem weer goed funktioneert bij de komst van de technicus, kan deze de intermitterende fout opsporen en repareren.

Als de technicus, ondanks de hulp van de service-processor, de fout niet snel genoeg kan vinden, kan hij via de operator-konsole de hulp inroepen van de Retain/370 Databank. Dit betekent ook dat via de telefoon te allen tijde een beroep kan worden gedaan op verschillende IBM-deskundigen via de RSF (Remote Support Facility).

RETAIN/370 DATABANK

De Retain/370 Databank is een wereldomspannend netwerk met vier centra, in Europa, de Verenigde Staten, Australië en Japan, die via satellieten in rechstreekse verbinding met elkaar staan. Het netwerk is verbonden met alle branchekantoren van de dienst en bovendien met produktspecialisten die zich op IBM laboratoria en fabrieken bevinden. Het netwerk bestaat uit een data base en circa tweeduizend beeldschermterminals en twaalfhonderd afdrukeenheden.

Een technicus die moeilijkheden ondervindt bij het lokaliseren van een hardware-fout, kan nu via RSF contact opnemen met een produktspecialist in eigen land. Deze specialist kan de volgende handelingen verrichten:

- hij kan de console bedienen en aflezen, alsof hij ter plaatse aanwezig is,
- hij kan de foutgegevens analyseren (Log Analysis)
- hij kan diagnostische programma's starten en
- hij kan microcodeverbeteringen overzenden.

Deze procedure is in vele opzichten beveiligd. Alle gegevens die op het scherm van de produktspecialist verschijnen, worden tegelijkertijd weergegeven op de console van de gebruiker, zodat deze controle kan uitoefenen op de gegevens die worden overgebracht. Daarbij komt dat de service-processor, die een belangrijke rol speelt bij het lokaliseren van de fout, alleen toegang geeft tot het hoofdgeheugenn en niet tot de bestanden. Als extra zekerheid beschikt de gebruiker over een "operator"-schakelaar, waarmee hij op ieder moment onmiddellijk de overdracht van informatie kan beëindigen.

De telefoonaansluiting voor deze vorm van serviceverlening, die bekend staat als Remote Service Facility (RSF) staat onder beheer van de gebruiker. Deze verbinding dient buiten de huiscentrale om te lopen, om

te voorkomen dat tijdens een RSF-procedure de verbinding kan worden verbroken door de telefoniste. De RSF-procedure kan worden afgewikkeld zonder dat het normale produktiewerk moet worden onderbroken.

Als ook het servicecentrum in het eigen land geen oplossing kan bieden voor de gerezen problemen, kan een beroep worden gedaan op andere produktspecialisten in Europa (Mainz) of de Verenigde Staten.

De faciliteiten van de Retain/370 Databank staan ook ter beschikking bij het zoeken van oplossingen voor software-fouten.

SOFTWARE-SERVICE

Tot dusver heeft de software-service van IBM een gelaagde structuur. De Customer Engineer (CE), die zich ziet geplaatst voor programmatuurproblemen waarvoor hij ter plaatse geen oplossing kon vinden, neemt in eerste aanleg contact op met het CE Branche Office in Amsterdam, Zoetermeer of Arnhem, afhankelijk van het rayon waarin de gebruiker woont. Het betrokken CE Branch Office kan dan op zijn beurt de Field Support Group in Amsterdam raadplegen. Kan ook deze groep geen adequate oplossing vinden, dan is de volgende stap het consulteren van het Area Field Support Center in Mainz. In laatste instantie kan dan een beroep worden gedaan op de verschillende Central Programming Support Groups, die verantwoordelijk zijn voor de ontwikkeling en het onderhoud van de betreffende software-componenten. Deze opzet heeft soms tot gevolg dat bij moeilijke software-fouten veel tijd verloren gaat, voordat de oplossing is gevonden.

De nieuwe software support-organisatie, die nu in opbouw is en in december 1979 volledig operationeel moet zijn, heeft een geheel andere structuur. De kern van de nieuwe organisatie zal het IBM support centrum zijn. Een gebruiker die een programmatuurprobleem heeft kan zelf via een telefoonverbinding het support centrum consulteren.
Hij zal dit pas doen als de sterk verbeterde mogelijkheden om zelf, door middel van een dialoog met het systeem, programmatuurfouten, op te sporen en te verhelpen, niet tot het gewenste resultaat hebben geleid.

Het IBM support centrum kan zo nodig rechtstreeks contact opnemen met de Central Programming Support Groups. In dit geval zitten het lokale CE Branch Office en het Area Support Center er dus niet meer tussen. Vermindering van het aantal "lagen" leidt uiteraard tot een snellere procedure.

CENTRALE PROGRAMMATUURONDERSTEUNING

Een ander gevolg van de nieuwe opzet van de software-service is een betere preventieve service. Daaronder verstaan we het verbeteren van programma's ten aanzien van fouten die nog niet eerder zijn opgetreden bij de meeste gebruikers.
Dit gebeurt door middel van "service update tapes", die alle verbeteringen bevatten voor de programmatuur die door de klant wordt gebruikt.

Deze tapes worden automatisch vanuit de Europese Programmabibliotheek (EPL) rechtstreeks naar de relatie gestuurd.
Verder bestaat de centrale programmatuurondersteuning uit het behandelen van foutmeldingen (APAR's) door de IBM ontwikkelingslaboratoria en het produceren van verbeteringen, de zogenaamde PTF-banden.

RUIMERE KEUS UIT CONTRACTMOGELIJKHEDEN

In de nieuwe opzet van de software-serviceverlening kan de gebruiker rechtstreeks contact opnemen met het nieuwe Support Centrum. De enige kosten die hieraan zijn verbonden, zijn die van een kort telefoongesprek met het support centrum, want dit centrum zal na het inleidende telefoongesprek en consultatie van de R/370 data base terugbellen. Zelfs de telefoonkosten zijn dus voor rekening van IBM.
Deze mogelijkheid om "vrijwel gratis" zoveel assistentie van deskundigen te krijgen als nodig is voor het oplossen van het probleem, plus de grotere zelfstandigheid van de gebruiker bij het oplossen van zijn eigen problemen als gevolg van de mogelijkheid in dialoog met het systeem te treden, hebben tot gevolg dat er minder behoefte zal bestaan aan bezoek van een customer engineer.

Dit betekent niet dat er nooit meer een CE aan huis zal komen. Ook bij de nieuwe opzet blijft het mogelijk een CE tegen het geldende uurtarief te laten komen voor het assisteren bij probleemdeterminatie. De probleemdiagnose en correctie, het aanbrengen van verbeteringen (PTF-banden), het ontwikkelen van een lokale fix of bypass of het prepareren van een foutmelding (APAR) blijft behoren tot de taken van de CE.

Daarnaast blijft de mogelijkheid bestaan contracten af te sluiten, waarbij de zojuist genoemde werkzaamheden door een CE aan huis worden verricht. Er zijn afzonderlijke contracten voor:

- systeembesturingsprogramma's (SCP's) onder de naam ABPS en
- gelicentieerde programma's (LP's) onder de naam ABPL.

Als dergelijke contracten zijn afgesloten, zijn alle genoemde werkzaamheden van de CE gratis, op voorwaarde dat de gebruiker de service update tapes heeft aangebracht binnen drie maanden na de verzending daarvan.

Gebruikers met meer dan een systeem kunnen deze contracten afsluiten tegen een gereduceerd tarief. De voordelen van de nieuwe opzet van de Software-service voor de gebruiker zijn:

- directe telefonische toegang tot het support centrum en Retain/370 Databank, en daarmee tot een keur van produktspecialisten;
- keus uit verschillende servicemogelijkheden;
- de mogelijkheid tot kostenbesparing;
- verbeterde beschikbaarheid van het systeem als gevolg van de snellere service;
- verhoogde produktiviteit van de systeemprogrammeurs;

- nieuwe "tools" en "aids".

De volgende systeembesturingsprogramma's ondersteunen het IBM 4300 systeem en vallen daarmee onder de nieuwe programmatuurondersteuning (met ingang van 1980):

DOS/VSE,
VM/370 Release 6, en
OS/VS1 Release 7.

De Automatisering-gids, 12 juli 1979

DOOR PROGRAMMEERFOUTEN IN HECHTENIS

Hoewel in de inleiding wordt gesteld dat het hier niet om een voorspelling of een griezelverhaal gaat komt een dergelijke "kop" ongeloofwaardig over tenzij het om frauduleuze handelingen gaat. De wettelijke aansprakelijkheid van programmeurs voor fouten in hun programma's gaat in de Verenigde Staten gestalte krijgen (volgens recente uitgave van het Computer Law and Tax Report).

Geldboetes of zelfs gevangenisstraf voor een programmeerfout. Dit is geen voorspelling uit George Orwell's "1984" of een griezelverhaal uit de Russisiche propagandamachine, maar de keiharde realiteit van vandaag de dag. Programmeurs kunnen wettelijk aansprakelijk worden gesteld voor fouten, die in hun programma's voorkomen. Een en ander blijkt uit een recente uitgave van het "Computer Law and Tax Report" (CLTR).

De sankties op programmeerfouten staan in het steeds groeiende aantal wetten, dat jaarlijks wordt uitgevaardigd door de afzonderlijke staten in de Amerikaanse federale overheid. Het CLTR adviseert iedereen die met gegevensverwerking te maken heeft, zich terdege op de hoogte te stellen van de verschillende wetten, om te voorkomen, dat zij zich onbewust in een strafbare positie manoeuvreren. Om deze situatie te vermijden, moeten programmacorrecties worden aangebracht en moeten de foutzoekprocedures intensiever worden. Een van de wetten die kortgeleden van kracht is geworden, heeft betrekking op de automatisering in de geneesmiddelenindustrie. De nieuwe wet stelt, dat een ieder die zich schuldig maakt aan het op onjuiste wijze vervaardigen van geneesmiddelen, gestraft kan worden met een boete tot 1000 dollar of gevangenisstraf van maximaal een jaar. Onder "onjuiste manier", of zoals letterlijk in de wet staat "vervalsing", wordt het volgende verstaan: "De bij de fabrikage gebruikte methoden, hulpmiddelen of regeleenheden c.q. verpakking, verwerking of opslag die niet voldoen aan algemeen aanvaarde normen".

In de wet op de geneesmiddelen wordt een aparte paragraaf gewijd aan het gebruik van de computer bij de fabrikage hiervan. Als computerapparatuur wordt gebruikt, dan eist de "Food and Drug Administration" (FDA)

dat aan de volgende voorwaarden wordt voldaan:

- De routinematige afstellingen, inspecties en controles moeten worden uitgevoerd aan de hand van speciaal ontwikkelde programma's die een waarborg zijn voor goed werk.
- Van iedere uitgevoerde inspectie, afstelling of controle moet een schriftelijk rapport worden bijgehouden.
- Aanvullend zal degelijk moeten worden gecontroleerd, dat veranderingen in het fabrikageproces slechts worden aangebracht door daartoe bevoegd personeel.
- Van alle in het systeem aanwezige gegevens moet een "back-up" worden gemaakt.
- Van de back-upgegevens zal op de een of andere manier een "hard-copy" gemaakt moeten worden, ten einde te voorkomen, dat de gegevens bij ongeluk worden gewist.

De Automatisering-gids, 4 oktober 1979.

Beveiliging

In Computable van 20 juli 1979 stond het volgende:

"Onder de kop "Privacy eindelijk ook voor regeringszijde erkend" en "Maatregelen tegen misbruik van persoonlijke gegevens" lezen wij: "De mededeling van oud-staatssecretaris (en huidige minister van Onderwijs) Van Veen, dat er gewerkt wordt aan een wet ter bescherming van de burger tegen de mogelijkheid in een computer over hem opgenomen gegevens te achterhalen werpt weer eens het zoeklicht op het vraagstuk privacy". Dat bovenaangehaald citaat afkomstig is uit Computable is niet zo verwonderlijk: Wèl verwonderlijk is de datum van het nummer van Computable waarin dit artikel staat, namelijk oktober 1971. Waar blijft de tijd. En waar blijft de privacywetgeving?"

Terecht wordt besloten met "En waar blijft de privacywetgeving?" Dat het uitblijven van de privacywetgeving in Nederland als een gemis wordt ervaren blijkt uit het feit dat bepaalde instanties zelf regels gaan opstellen. De volgende twee artikelen gaan over "ad hoc" regelingen op min of meer vrijwillige basis wegens het uitblijven van een wettelijke regeling.

VNG GEEFT REGELS VOOR REGISTRATIE PERSOONSGEGEVENS

De burger zal in de nabije toekomst zijn gemeentebestuur kunnen controleren op het juiste gebruik van zijn persoonlijke gegevens. Tenminste, als die gemeentebesturen de ideeën overnemen van de Commissie Privacy van de Vereniging van Nederlandse Gemeenten (VNG).

Onder voorzitterschap van drs. W. Lemstra, gemeentesecretaris van Amsterdam, heeft een studiecommissie van de VNG zich gebogen over de problematiek van de bescherming van persoonsgegevens in het belang van de persoonlijke levenssfeer van de burgers.

Een aantal gemeenten had, mede door de resultaten van de Staats-Commissie-Koopmans, al een begin gemaakt met het opstellen van regels. De VNG heeft gemeend de draad verder te moeten opnemen. In nauw overleg met het Samenwerkingsverband voor de Overkoepeling van de Automatisering bij de Gemeenten (SOAG) heeft de VNG eind 1977 de zogeheten Commissie Privacy ingesteld.

De Commissie heeft zich niet willen beperken tot de geautomatiseerde informatiesystemen. Zij meent dat ook regels kunnen worden opgesteld voor niet-geautomatiseerde systemen zoals kaartregisters, persoonsdossiers en dergelijke. De commissie heeft wel een begrenzing aangebracht in het onderwerp. Zij heeft zich gericht op de persoonsgegevens die worden verwerkt in het proces van de bestuurlijke informatievoorziening in de gemeentelijke administratie. Men is uiteindelijk gekomen tot het opstellen van een aantal regels voor het verzamelen, opslaan, verwerken en verstrekken van persoonsgegevens.

De commissie geeft een aantal mogelijkheden aan, die de burger in staat stellen na te gaan of de gegevens over hem juist zijn en ook volgens de regels worden gebruikt. De burger kan in een openbaar register zien welke gegevensverzamelingen er worden bijgehouden. Hij krijgt een inzage- en correctierecht. Als de burger meent dat zijn gegevens niet goed behandeld worden, kan hij in beroep gaan bij de gemeenteraad. Daarnaast geeft de commissie aan hoe toezicht uitgeoefend kan worden.

Aan het rapport zijn twee modellen voor een privacyverordening toegevoegd. Het ene model voorziet in de instelling van een afzonderlijke commissie van toezicht; het andere laat de toezichtsfunctie bij de gemeenteraad. Bij de opstelling van de modellen is rekening gehouden met de voorstellen van de Staatscommissie-Koopmans. Daarmee wordt bereikt dat de gemeenten al zoveel mogelijk en voor zover nodig hun bevoegdheden kunnen aanwenden in de door die commissie aangegeven richting.

De VNG geeft het rapport en bijbehorende modellen van de Commissie privacy gebundeld in een boekje onder de titel: "Gemeente en privacy".

De Automatisering-gids, 13 september 1979

AMSTERDAM KRIJGT PRIVACY-VERORDENING

Burgemeester en wethouders van de hoofdstad hebben een privacy-verordening laten opstellen, die beoogt de persoonlijke levenssfeer te beschermen van de Amsterdammers, over wie gegevens zijn opgenomen in gemeentelijke registraties. Dit werd medegedeeld tijdens de officiële opening van het nieuwe pand, twee weken geleden, voor het Amsterdamse gemeentelijke centrum voor electronische informatieverwerking (GCEI). Iedere Amsterdamse burger zal in de toekomst zelf kunnen kijken welke persoonsgegevens van hem in de verzameling zijn opgenomen en kan deze eventueel wijzigen of aanvullen wanneer er fouten in zijn geslopen.

De door het gemeentebestuur opgestelde privacy-verordening wordt op 21 juni aanstaande behandeld in de commissie van bijstand voor de bestuursinformatie en na de zomervakantie komt de verordening ter bespreking in de gemeenteraad.

AANLEIDING

Sinds de volkstelling van 1971 staat de bescherming van de persoonlijke levenssfeer in de publieke belangstelling. Door de Staatscommissie-Koopmans is in 1976 een ontwerp van de Wet op de persoonsregistraties gepubliceerd. Naar wordt verwacht zal deze wet omstreeks 1982 kunnen gaan gelden.

Burgemeester en wethouders van Amsterdam hebben gemeend vooruit te moeten lopen op deze Wet, in verband met de vele gemeentelijke registraties waarin gegevens over personen zijn opgenomen. In de derde Nota Automatisering (1977) is gesteld dat het privacybeleid ten aanzien van de geregistreerden het noodzakelijk maakt de instelling en het functioneren van registratiesystemen met bestuurlijke waarborgen te omkleden. De Amsterdamse verordening is in de eerste plaats gericht op de geautomatiseerde registraties. Dit is voornamelijk gedaan uit praktische overwegingen, daar beschrijvingen van de geautomatiseerde registraties reeds vastliggen in de systeemdocumentatie van het gemeentelijk centrum voor electronische informatieverwerking. De verordening voorziet echter in de mogelijkheid regels die gesteld worden aan geautomatiseerde registraties tevens van toepassing te verklaren op niet-geautomatiseerde verzamelingen van persoonsgegevens.

INHOUD VERORDENING

In principe vallen alle gemeentelijke gegevensverzamelingen met persoonsgegevens onder de verordening. Voor sommige registraties zou dat echter een onnodige reglementering betekenen omdat deze niet "privacybedreigend" zijn. Voor andere worden openbaarheid en andere waarborgen reeds in wetten geregeld. Daarom worden een aantal registraties uitgezonderd.

De verordening voorziet in een onafhankelijke controle. Hiermee wordt een aparte commissie (registratiecommissie) belast, die een eigen verantwoordelijkheid heeft ten aanzien van de bescherming van de persoonlijke levenssfeer.

De registratiecommissie kan zich laten bijstaan door ambtenaren van de gemeentelijke accountantsdienst of door andere deskundigen. Over de uitoefening van de bevoegdheden legt de registratiecommissie verantwoording af aan de gemeenteraad, zodat een politieke controle mogelijk blijft.

De geautomatiseerde registratiesystemen moeten worden ingeschreven in een openbaar register, waarbij de registratiecommissie nagaat of de registraties voldoen aan de gestelde eisen.

Burgemeester en wethouders wordt opgedragen voor alle geautomatiseerde registraties reglementen vast te stellen. In deze reglementen is vastgelegd met welk doel de registraties zijn opgezet, door wie en waarvoor de gegevens mogen worden gebruikt, wie wel en wie geen gegevens mag ontvangen.

Er worden waarborgen gegeven voor het samenvoegen van registraties en het koppelen van persoonsgegevens met gegevens uit andere registraties.

De bewerker, dat is degene die is belast met het beheer van de apparatuur en de programmatuur, is gebonden aan regels. Er mogen door hem uit eigen beweging geen bewerkingen worden uitgevoerd of gegevens aan derden worden verstrekt.

De geregistreerde heeft recht op inzage en verbetering, verwijdering of aanvulling van de eigen gegevens.
Voor een aantal registraties heeft de beheerder een zogenaamde protokolplicht. Dat is de plicht om bij te houden wie bepaalde gegevens zijn verstrekt gedurende een zekere termijn. De beheerder is in het algemeen verplicht een geregistreerde op zijn verzoek inzage te geven in het protokol, voor zover dat op hem betrekking heeft. Als een beheerder niet voldoet aan een verzoek tot inzage of verbetering, kan de geregistreerde in beroep gaan bij burgemeester en wethouders.

De Automatisering-gids, 11 juni 1979.

De registratiecommissie kan zich laten bijstaan door ambtenaren van de gemeentelijke accountantsdienst of door andere deskundigen. Over de uitoefening van de bevoegdheden legt de registratiecommissie verantwoording af aan de gemeenteraad, zodat een politieke controle mogelijk blijft.

De geautomatiseerde registratiesystemen moeten worden ingeschreven in een openbaar register, waarbij de registratiecommissie nagaat of de registraties voldoen aan de gestelde eisen.

Burgemeester en wethouders wordt opgedragen voor alle geautomatiseerde registraties reglementen vast te stellen. In deze reglementen is vastgelegd met welk doel de registraties zijn opgezet, door wie en waarvoor de gegevens mogen worden gebruikt, wie wel en wie geen gegevens mag ontvangen.

Er worden waarborgen gegeven voor het samenvoegen van registraties en het koppelen van persoonsgegevens met gegevens uit andere registraties.

De bewerker, dat is degene die is belast met het beheer van de apparatuur en de programmatuur, is gebonden aan regels. Er mogen door hem uit eigen beweging geen bewerkingen worden uitgevoerd of gegevens aan derden worden verstrekt.

De geregistreerde heeft recht op inzage en verbetering, verwijdering of aanvulling van de eigen gegevens.
Voor een aantal registraties heeft de beheerder een zogenaamde protokolplicht. Dat is de plicht om bij te houden wie bepaalde gegevens zijn verstrekt gedurende een zekere termijn. De beheerder is in het algemeen verplicht een geregistreerde op zijn verzoek inzage te geven in het protokol, voor zover dat op hem betrekking heeft. Als een beheerder niet voldoet aan een verzoek tot inzage of verbetering, kan de geregistreerde in beroep gaan bij burgemeester en wethouders.

De Automatisering-gids, 11 juli 1979.

Controle

THE RISE AND RISE OF COMPUTER CRIME

Aldus de titel van een artikel in International Management van juli 1979.

Naast de drie slogans:

Computerization has opened new doors to criminals that companies have been slow to close.

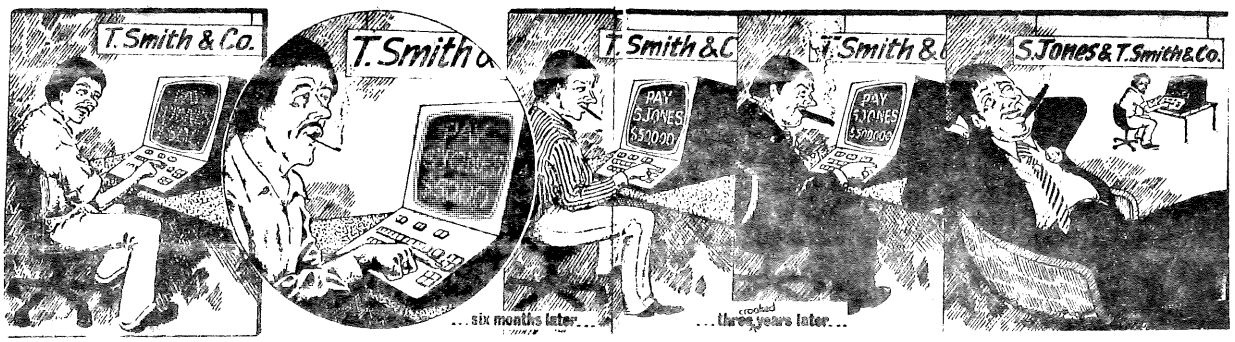
Auditors are reluctant to accept responsibility for detecting computer frauds.

Most crimes stem from a dissatisfaction with an employer.

Geeft het artikel in tabelvorm:

- "Environments that lead to computer crime" en
- How to avoid computer crime.

Het geheel dat hieronder is opgenomen is op passende wijze gelardeerd (ook uit International Management juli 1979).



ENVIRONMENTS THAT LEAD TO COMPUTER CRIME

- Low staff morale. Personnel in data processing and computer user departments show a lack of discipline in observing security precautions and in maintaining a tidy and systematically run operation.
- Poor documentation. System documentation is incomplete, out-of-date and untidy. Only the system designer has a complete idea of what the system does.
- Unnecessarily hard-working staff. Staff have little leave or absence, remain in the same function for a long period and seldom take a holiday. Once a fraud is in operation the criminal often needs to maintain continuous vigilance to avoid detection.
- Expensive habits. Individual members of staff or whole groups suddenly adopt new improved life-styles.
- Lack of duty segregation. Programmers are allowed to input data, operations staff are involved in programming, data preparation staff are involved in data control.
- Poor operation management. No documentary control and authorization procedures governing system changes and alterations to data files. General lack of systematic control.
- High level of computer error. Errors created through poor system design lead staff and managers to accept errors that can be "blamed on the computer".

Indien de accountant een toestand aantreft als in de "Environments that lead to computer crime" zal hij maatregelen dienen te treffen. Wellicht kan het volgende staatje haar/hem daarbij helpen.

HOW TO AVOID COMPUTER CRIME

- Set up task force to establish and monitor computer security procedures. The task force must include representatives from the data processing department, security, auditors and user departments.
- Perform a systematic risk analysis covering potential loss through accident as well as intentional crimes.
- List computer applications and identify possible opportunities for computer crimes; develop a system of defences.
- Establish site inspections and interviews covering:
  Physical state of computer room
  and user departments
  Access control
  Documentation
  Segregation of duties
  Unnecessary or excessive
  over-working by staff
  General personnel environment
- Give special attention to accounting information. Most computer fraud concerns the following areas:
  Purchase orders and invoices
  Inventories
  Sales
  Pay-roll
  Pensions
- Avoid:
  Reliance on one person for vital functions
  Chances for collusion
  Periodic repetition of security checks; rely on ad hoc spot checks instead
  Unsupervised work, particularly late at night; slack staff recruitment, appraisal and termination procedures
  Reduction of security in moving from manual to computer system.