COMPUTERBEVEILIGING

door Drs. R. A. M. Pruijm

DE KOST GAAT VOOR DE BAAT UIT

1 Inleiding

Alhoewel de problematiek rond computerbeveiliging op het eerste gezicht verre van de taakuitoefening van de accountant verwijderd schijnt, blijkt dit bij nader onderzoek een probleem te zijn dat de accountant direct betreft.

Door de automatisering van de informatieverwerking zien we drie tendenties optreden.

Ten eerste het in toenemende mate overnemen van voorheen door de mens verrichte werkzaamheden door de computer: de functionele concentratie.

Ten tweede zien we dat bovengenoemde overname gepaard gaat met concentratie van voorheen op diverse lokaties uitgevoerde werkzaamheden in de computer: de geografische concentratie.

Aangezien de computer een informatieverwerkend apparaat is, gaat de overname van werkzaamheden eveneens gepaard met het in toenemende mate opslaan van de hiervoor benodigde informatie bij de computer: concentratie van informatie-opslag. Voorbeelden zijn allerlei bestanden (debiteuren, voorraden, etc.), bedrijfsinformatie (personeelsgegevens, omzetstatistieken, etc.) en computerprogramma's.

Het gevolg van al deze factoren is dat het computercentrum steeds meer het zenuwcentrum vormt van het gehele informatieverwerkend proces bij vele ondernemingen.

Het uitvallen van de computer door allerlei oorzaken kan dan ook ernstige repercussies hebben voor de verdere bedrijfsuitoefening en deze in sommige gevallen zelfs onmogelijk maken.

Wat te denken van een onderneming:

- met een facturerings- en debiteurenprogramma waarin 20.000 cliënten zijn opgenomen met een totale waarde van 2 miljoen gulden
- die de salarissen van haar 35.000 werknemers berekent en uitbetaalt met behulp van een gecompliceerd salarisprogramma
- met een door de computer verzorgde produktieplanning, inkoop- en voorraadadministratie
- en die tenslotte door personeelsverloop weinig employé's meer in dienst heeft die zich herinneren hoe elk van de genoemde werkzaamheden nog manuaal gedaan moeten worden?

Wat zou er met deze onderneming gebeuren als door de een of andere calamiteit, zoals bijvoorbeeld brand, het computercentrum vernietigd wordt? Harold Weiss typeert deze situatie met de veelzeggende benaming „total corporate amnesia", of wel totale verlamming van het bedrijfsgebeuren. Het

zijn niet alleen de juistheid en volledigheid van de informatie, maar ook de tijdigheid en continuïteit van de informatie welke van belang zijn voor het bedrijfsgebeuren.

Het komt ons voor dat vanuit dit licht bezien beide laatste aspecten van belang zijn voor de accountant in het kader van de beoordeling van de interne controle.

2 Gebiedsafbakening

Onder computerbeveiliging wordt door ons verstaan:

„Het geheel van maatregelen gericht op het beschermen van de automatische informatieverwerking, tegen alle factoren welke de continuïteit van het informatieverwerkend proces kunnen verstoren."

Dit hele complex van maatregelen valt uiteen in twee onderdelen:

1 Preventieve maatregelen.
2 Maatregelen tot herstel.

ad 1 Hieronder worden verstaan alle maatregelen gericht op het minimaliseren van het risico dat de continuïteit van het informatieverwerkend proces door een of andere calamiteit wordt verbroken.

ad 2 Hieronder worden verstaan alle maatregelen gericht op het minimaliseren van de tijd gepaard gaande met het reactiveren van het informatieverwerkend proces, indien dit door een calamiteit tot stilstand is gebracht.

3 Invloedsfactoren

Welke zijn nu de factoren waartegen men zich dient te beschermen?

Hieronder volgt een summiere selectie van enkele praktijkgevallen

- Bij de bezetting van een grote chemische onderneming door een groep anti-Vietnam-betogers gewapend met magneten werd voor 100.000 dollar aan magneetbanden vernield. De waarde van de informatie die de banden bevatten was een veelvoud van het schadebedrag.
- Bij een brand, veroorzaakt door een molotov-cocktail, in het computercentrum van een Amerikaanse universiteit ging voor 2 miljoen dollar aan apparatuur verloren.
- Een ontevreden tape-beheerder verwisselde voor zijn vertrek alle etiketten op tape-reels en cassettes; er wordt aan getwijfeld of het mogelijk is de onderneming nog voort te zetten.

De volgende risico's zijn te onderscheiden:

- ongeautoriseerde toegang, met als gevolg diefstal, sabotage, vernielingen, brandstichting en dergelijke;
- brandschade;
- waterschade door lekkende daken, gebroken waterleidingen, grondwater-

overlast, lekkage van bluswater of waterschade door Sprinkler-blussystemen, overstroming;
- schade aan het gebouw door storm, blikseminslag, aanslagen, opstootjes, een vliegtuigramp en dergelijke;
- uitvallen van de elektriciteit;
- diefstallen, sabotage-daden, bezetting, onoplettendheid en dergelijke van het eigen personeel.

4 Beveiligingsmaatregelen

De te nemen beveiligingsmaatregelen zijn te verdelen in:

A. Beveiliging tegen ongeautoriseerde toegang
B. Beveiliging tegen brand en andere calamiteiten
C. Beveiliging tegen storing in de energievoorziening
D. Beveiliging van gegevens
E. Personeelsbeveiliging

A. Beveiliging tegen ongeautoriseerde toegang

De maatregelen richten zich vooral op de beperking van het aantal toegangswegen, alsmede de versterking van de controle op het gebruik hiervan door alleen hiertoe bevoegde personen.

Beperking van het aantal toegangswegen is een vraagstuk van bouwtechnische aard. Het gaat erom de computerruimte zo te construeren dat toegang alleen mogelijk is via de hiervoor bestemde route. Dit houdt in beperking van het aantal toegangen tot zo mogelijk één, hetgeen niet wil zeggen dat er maar één deur is. Het is heel goed mogelijk deuren te construeren die alleen van binnen uit geopend kunnen worden en waarvan de sleutel in geval van nood onmiddellijk bereikbaar is.

Ook de verdere constructie van de computerruimte dient erop gericht te zijn toegang te bemoeilijken; dit kan inhouden ramen van gewapend glas voorzien van tralies of stalen rolluiken, vermijden van ligging gelijkvloers aan de straat, etc.

Tevens kan men detectie-apparatuur installeren om ongewenst bezoek te signaleren.

Controle op geautoriseerde toegang kan op velerlei manieren geschieden. De meest gehanteerde methode is het situeren van een portier of waker bij de toegang tot de computerruimte.

Autorisatie van toegang kan geschieden op vertoon van een speciale pas of een insigne met een speciale kleur of code.

Bezoekers dienen in een bezoekersregister te worden ingeschreven en bij de portier te worden afgehaald en teruggebracht door degene voor wie zij komen.

Met toegangsbeveiliging kan men zeer ver gaan; er bestaan systemen waarbij de bezoeker in een sluis komt, afgesloten door 2 deuren. Hij moet dan het juiste pasje, sleutel of insigne ter visuele inspectie aan de portier tonen (al of niet door middel van een televisiecamera) of zijn pasje in een speciale lezer stoppen, alvorens de deur opengaat.

Een dergelijke sluis kan tevens van detectie-apparatuur worden voorzien ter signalering van eventueel meegebrachte magneten.

Ook is het mogelijk magneetbanden en schijven van onverwijderbare etiketten te voorzien waarop in de sluis aangebrachte detectoren kunnen reageren en de doorgang blokkeren, zodat op deze wijze diefstal van informatiedragers voorkomen wordt.

Veelal gaat men ertoe over bovengenoemde controlemaatregelen toe te passen in combinatie met een zogenaamde „closed shop", hetgeen wil zeggen dat alleen degenen belast met de bediening van de computer toegang hebben tot de eigenlijke computerruimte.

Alle te verwerken informatie wordt aan een balie afgeleverd, waar ook na verwerking de resultaten kunnen worden afgehaald. Afdracht en ontvangst geschiedt tegen afgifte van hiertoe bestemde ontvangst- c.q. afgiftebewijzen.

Kort samengevat zijn de voornaamste beveiligingsmaatregelen tegen ongeautoriseerde toegang het beperken van de toegangsmogelijkheden, de beperking van het aantal geautoriseerde personen die toegang tot het computercentrum hebben en als laatste controle op het zich verschaffen van toegang.

B. Beveiliging tegen brand en andere calamiteiten

Beveiliging tegen brand kan worden bewerkstelligd door snelle detectie van het ontstaan ervan en een onmiddellijk hierop volgende bestrijding. Als detectie-apparatuur hanteert men veelal detectoren welke reageren op geïoniseerde deeltjes in de lucht, afgegeven door oververhitte voorwerpen.

Plaatsing geschiedt veelal onder de verhoogde vloer in de computerruimte en tegen het plafond.

Als bestrijdingsmiddelen voor brand kunnen worden gebruikt blus-installaties met water (Sprinkler-systeem), CO_2 of Halon 1301, al of niet gekoppeld aan detectie-apparatuur, en handblussers.

Halon 1301 is een gas dat als blusmiddel twee voordelen bezit boven CO_2 en water; het is in tegenstelling tot CO_2 ongevaarlijk voor de mens en laat na blussing geen schadelijke residuen achter op de apparatuur zoals laatstgenoemde blusmiddelen.

Ter voorkoming van de verspreiding van brand zien we in moderne centra ook vaak de toepassing van automatische branddeuren welke zich sluiten na brandmelding. Deze deuren zijn aan te bevelen voor het papiermagazijn, de tape-kluis en de toegangswegen.

Ter bescherming tegen bluswateroverlast van hoger gelegen verdiepingen is het raadzaam passende dekzeilen voor de apparatuur in of bij de computerruimte op te slaan, alsmede de ruimte te voorzien van een draineringssysteem ter afvoering van bluswater.

Tevens kan het plafond boven de computerruimte worden afgedicht ter voorkoming van lekkage.

Naast hulpmiddelen voor branddetectie en -bestrijding dient men de kans op brand zoveel mogelijk te beperken door maatregelen van meer huishoudelijke aard.

Voorbeelden hiervan zijn: een stringent rookverbod in de computerruimte, beperking van het in de ruimte opgeslagen papier tot datgene beno-

digd voor één dag produktie, prullemanden van metaal voorzien van een deksel, geen opslag van brandbare schoonmaakmiddelen in de ruimte, etc.

In dit kader werden wel eens de volgende hoofdregels genoemd:

- wat niet direct en dringend nodig is in de computerruimte, moet verwijderd worden
- in de computerruimte vindt geen enkele activiteit plaats, die niet net zo goed elders kan geschieden.

Andere calamiteiten zoals grondwateroverlast, stormschade, blikseminslag, waterschade door gebroken ruiten en dergelijke kunnen worden voorkomen door maatregelen van bouwtechnische aard.

Ook het gevaar van brand kan door dergelijke maatregelen worden beperkt. Te denken valt aan het gebruik van brandwerende scheidingswanden en deuren, metalen meubilair, etc.

C. Beveiliging tegen storing in de energievoorziening

Voor automatische informatieverwerking is elektriciteit nodig, zowel voor de computer als voor de airconditioning-apparatuur welke de computerruimte op de juiste vochtigheidsgraad en temperatuur houdt.

Er wordt geadviseerd bij temperaturen hoger dan 22 à 23° C de computer uit te schakelen om de kans op fouten te vermijden. Bij 60° C gaat hij slecht functioneren en bij 100° C en hoger is de computer onherstelbaar vernietigd.

Het is duidelijk hoe belangrijk elektriciteit voor de computer zelf is. Uitvallen ervan betekent zonder meer het stilhouden van de verwerking en het verloren gaan van informatie.

Het gaat hierbij echter niet alleen om een ongestoorde stroomvoorziening, maar ook om beveiliging tegen al te grote fluctuaties in de stroomspanning.

In Brabant doen zich met name bij het begin van de „suikercampagne" veel storingen in computercentra voor, veroorzaakt door fluctuaties in de stroomvoorziening door het opstarten van de suikerfabrieken.

Ter verzekering van een ongestoorde stroomvoorziening zijn noodaggregaten verkrijgbaar welke automatisch aanslaan bij uitval van stroom. Ook is er apparatuur welke stroomfluctuaties reguleert.

De kosten van dergelijke apparatuur zijn echter hoog; toepassing ervan zien we dan ook tot nu toe alleen gerealiseerd bij de zeer grote rekencentra.

Door de lagere prijs zien we zogenaamde „accubatterijen" meer toegepast. Deze zijn echter alleen maar in staat uitval van de elektriciteit voor korte tijd te compenseren. Gedurende deze tijd is het dan mogelijk de informatieverwerking geleidelijk aan te beëindigen zonder dat gegevens verloren gaan of dat informatie wordt verminkt. Men spreekt dan van „graceful degradation".

D. Beveiliging van gegevens

Bij geautomatiseerde informatieverwerking zijn vier soorten gegevens te onderscheiden:

1 invoergegevens in voor de computer leesbare vorm, zoals rekeningcourant mutaties, verkooporders, etc.
2 bestanden, zoals het bestand voorraden, debiteuren, etc.
3 programma's in voor de computer begrijpbare vorm (source deck) ge-

schreven in een programmeertaal welke eerst vertaald (gecompileerd) moet worden in voor de computer uitvoerbare vorm (object deck)

4 documentatie; hieronder zijn te verstaan programmabeschrijvingen met blokdiagrammen en/of beslissingstabellen, indelingen van invoergegevens en bestanden, voorbeelden van de te bedrukken formulieren, bedieningsvoorschriften voor de operators, etc.

De eerste drie soorten gegevens treft men aan op ponskaart, magneetband, magneetschijf, magneetkaart of magneettrommel.

Zij zijn niet alleen onmisbaar bij de feitelijke gegevensverwerking, maar voor de programma's geldt bovendien dat zij vaak zeer grote investeringen vergen. Ter illustratie: het reserveringssysteem van een grote luchtvaartmaatschappij kostte alleen aan programmatuur al 7 miljoen dollar.

De te nemen beveiligingsmaatregelen vertonen een gelijkenis met de organisatie rond de opslag van goederen in een gesloten magazijn. Alle gegevens dienen in een aparte ruimte opgeslagen te zijn onder beheer van een aparte functionaris, die als enige toegang tot deze ruimte heeft.

Alle informatiedragers dienen van etiketten te worden voorzien, waarop onder andere vermeld: het nummer, bestandsnaam, versienummer, etc. De beheerder houdt een aparte administratie bij van alle in- en uitgaande informatiedragers.

Uitgifte geschiedt alleen op schriftelijke opdracht van de afdeling Werkvoorbereiding.

Direct na beëindiging van de werkzaamheden dienen de betreffende informatiedragers weer in de bibliotheek te worden opgeborgen. Ter controle hierop zien we vaak de toepassing van een dubbele registratie van de informatiedragers en wel een registratie van de informatiedragers naar programma waarbij ze gebruikt mogen worden en een registratie van de informatiedragers naar nummer.

In de eerste registratie worden de data van ontvangst en uitgifte vastgelegd, in de tweede registratie worden per informatiedrager alle gegevens geregistreerd over het gebruik, zoals: datum in gebruikname, aantal malen gebruikt, voorgekomen lees- of schrijffouten en dergelijke. De ruimte waarin de opslag van informatiedragers geschiedt dient zo mogelijk te bestaan uit een waterdichte en brand- en inbraakvrije kluis.

De documentatie van zowel lopende als gereedgekomen projecten dient na beëindiging van de werkzaamheden eveneens in een waterdichte, brand- en inbraakvrije kluis te worden opgeborgen. Het belang van de projectdocumentatie voor de continuïteit wordt veelal onderschat, maar zij is onmisbaar bij onderhouds- of revisiewerk. Verlies ervan betekent dat deze werkzaamheden ernstig kunnen worden bemoeilijkt of zelfs moeten worden stopgezet.

Indien men bedenkt dat 60 tot 80% van de programmeurswerkzaamheden bestaan uit onderhoud en revisie, is beveiliging van de documentatie van groot belang voor de continuïteit.

E. Personeelsbeveiliging

De factor personeel kan op 2 manieren stagnatie in de informatieverwerking veroorzaken.

Ten eerste kan zij schade toebrengen aan de apparatuur, programma's en bestanden door onoordeelkundig optreden, sabotage, etc. of de onderneming schade toebrengen door diefstal van programma's, bestanden of informatiedragers.

Ten tweede kan de informatieverwerking stagneren door het ontbreken van voldoende bedienend personeel door ziekte, staking, personeelsverloop, etc.

De eerste factor komt nog steeds veel voor; zelfs bij de moderne apparatuur is menselijke interactie zeer belangrijk en kan onjuiste bediening ernstige gevolgen hebben.

Voorbeelden zijn: onjuiste montering of behandeling van de magneetbanden of de kwetsbare schijveneenheden, waardoor deze beschadigen en niet meer bruikbaar zijn (helaas ook de erin opgeslagen informatie niet), of het verloren gaan van bestanden door gebruik ervan bij de verkeerde programma's.

Veel aandacht voor de opleiding, toezicht op de naleving van procedures en geprogrammeerde controles welke foutieve handelingen signaleren en de verdere verwerking onmogelijk maken, kunnen erger voorkomen.

De maatregelen ter voorkoming van de tweede factor liggen meer in de sfeer van het personeelsbeleid.

Uitvallen van personeel door ziekte kan alleen worden opgevangen door het overnemen van hun werkzaamheden door anderen.

Mogelijke oplossingen zijn het aanhouden van wat overcapaciteit in de voor de verwerking kritieke functies, zoals bediening, werkvoorbereiding en dergelijke, of uit andere functies personeelsleden opleiden als invaller.

Sabotage, staking en dergelijke zijn te voorkomen door veel zorg te besteden aan de handhaving van de kwaliteit en de motivatie van het personeel.

Dit impliceert een scherpe selectie bij de aanname, alsmede de zorg voor goede werkomstandigheden en beloning. In dit opzicht geldt nog steeds het aloude gezegde: „De beste employé is de tevreden employé". Gezien de indrukwekkende mogelijkheden welke automatiseringspersoneel tot sabotage hebben is dit inderdaad de beste beveiliging.

Hieronder volgen 2 illustraties van de inventiviteit van ontevreden employé's:

- Een operator die de dienst was opgezegd, hing voor zijn vertrek een paperclip op een nogal onbereikbare plek in het geheugen van de computer.
  Telkens als bij de verwerking de betrokken geheugensectie werd gebruikt, veroorzaakte de paperclip kortsluiting, waardoor informatie werd verminkt of verloren ging.
  Vanwege het intermitterende karakter van de storing duurde het zeer lang voor de fout door de leverancier was opgespoord; schade 250.000 dollar.

- Een programmeur bouwde in het door hem geschreven programma een instructie in waardoor na zijn vertrek de velden van een bestand, waarin de

in voorraad zijnde hoeveelheden artikelen waren opgeslagen, werden gevuld met random-getallen.

Ter voorkoming van dergelijke acties dient men er zorg voor te dragen dat degenen van wie men vermoedt of kan vermoeden dat zij een zekere wrok tegen de onderneming koesteren nauwlettend geobserveerd worden, zodat men kan ingrijpen voordat iemand tot sabotage overgaat. Het is in dit verband eerder aan te raden bij het geven van ontslag dit dadelijk te doen ingaan met behoud van salaris voor de nog resterende periode, dan de persoon in kwestie zijn tijd te laten uitdienen.

5 Maatregelen tot herstel

Alle te nemen maatregelen tot herstel zijn samen te vatten onder het begrip „Company Disaster Plan". Hieronder wordt verstaan: „Het geheel van maatregelen gericht op het minimaliseren van de tijd gepaard gaande met het reactiveren van het informatieverwerkend systeem indien dit door een calamiteit (disaster) wordt gestagneerd of tot stilstand gebracht".

Als uitgangspunt voor het Company Disaster Plan dient men vast te stellen:
1 wat men voor de betreffende onderneming onder een disaster dient te verstaan;
2 welke prioriteiten men aan de door het systeem gegenereerde output wenst toe te kennen.

ad 1 Onder het begrip disaster valt het hele gamma van tijdelijke werkvertraging tot complete stilstand van het informatieverwerkend systeem.

Bij de definiëring van wat voor de betreffende onderneming een disaster is, dient men met drie factoren rekening te houden, namelijk apparatuur, programmateur en bezettingsgraad.
- Apparatuur: het kapotgaan van een magneetbandeenheid heeft minder consequenties dan het „opblazen" van de centrale verwerkingseenheid.
- Programmatuur: de betekenis voor de onderneming van het verloren gaan van een statistisch programma dat eens in de maand wordt verwerkt, zinkt in het niet bij het verloren gaan van een programma dat voor de dagelijkse facturering wordt gebruikt.
- Bezettingsgraad: het begrip disaster is voor een onderneming met een voor 40% bezette computer totaal verschillend van dat voor een onderneming met een voor 90% bezet systeem.

Na bestudering van deze factoren zal men bijvoorbeeld tot de volgende omschrijving van een disaster kunnen komen. Een disaster is voor onze onderneming:
- het verloren gaan van ons IBM 360/25 systeem, of
- het verloren gaan van onze IBM 370/145 in gebruik voor ons on-line real time reserveringssysteem, alsmede
- het verloren gaan van de hierbij behorende programma's en de programma's Reserveringen en Routeplanning.

m a b blz. 167

ad 2 Nauw samenhangend met het vorige punt is het toekennen van prioriteiten aan de door het systeem opgeleverde output. Na stagnatie zal de achterstand dienen te worden ingehaald. Welke programma's hierbij voorrang hebben hangt af van de prioriteit welke de door hen gegenereerde output bezit. Bij uitwijk naar een ander systeem zal men maar de beschikking hebben over een deel van de gebruikelijke verwerkingstijd; ook hier rijst dan de vraag welke programma's moeten dan minimaal gedraaid worden. Bepalend hiervoor is dan de prioriteit welke hun uitvoer bezit.

Heeft men vastgesteld wat voor de betreffende onderneming het begrip disaster kan inhouden en welke prioriteiten men aan de gegenereerde gegevens dient te stellen, dan kan men overgaan tot het opstellen van het eigenlijke disasterplan.

Voor automatische informatieverwerking zijn drie zaken onmisbaar, namelijk
1 programma's (produktieprogramma's, besturingsprogramma's, vertaalprogramma's en dergelijke)
2 data (transactiegegevens en bestanden)
3 apparatuur (de computer met randapparatuur).

Zoals in het voorgaande is vermeld kan door allerlei oorzaken schade worden toegebracht aan deze drie elementen, waardoor stagnatie of stilstand in de informatieverwerking optreedt.

Het disasterplan is er dan ook op gericht de toegebrachte schade zo spoedig mogelijk te verhelpen door voor vervanging of reconstructie van genoemde onderdelen te zorgen, of in geval van onherstelbare schade aan apparatuur de uitwijk naar een andere computer mogelijk te maken. In de Amerikaanse terminologie spreekt men van de zorg voor een adequate software en hardware back-up.

6 Programmatuur en data back-up

Men kan de toegebrachte schade aan programmatuur en data herstellen door reconstructie of vervanging.

Bij reconstructie spreekt men veelal over het bekende grootvader-vader-zoon concept, een reconstructietechniek voor bestanden. Deze techniek is echter niet bruikbaar voor de overige bij automatische informatieverwerking noodzakelijke programmatuur en data. Hiervoor dient men in het disasterplan zorg te dragen voor de aanmaak van reserve-exemplaren ter vervanging van beschadigde exemplaren.

Het gaat hierbij om reserve-exemplaren van de volgende soorten programmatuur, gegevens en dergelijke:
1 Systeemdocumentatie
2 Programmadocumentatie
3 Bedieningsinstructies (run manuals)
4 Programma's in onvertaalde of vertaalde vorm (de zogenaamde source of object decks)

5 De benodigde job control voor produktieprogramma's
6 Besturingssystemen
7 Invoergegevens in machinaal leesbare vorm
8 Formulierenvoorbeelden
9 Noodvoorraad voornaamste voorgedrukte formulieren
10 Besturingsbandjes voor de afdrukeenheid.

ad 1 Systeemdocumentatie
Hierin bevinden zich:
- een diagram van een toepassing waarin alle bestanden, programma's en overzichten voorkomen, alsmede een beschrijving in verhaalvorm van het systeem
- een schema waaruit voor ieder programma blijkt waaruit de in- en uitvoer bestaat
- een beschrijving van het doel en de functies van het programma met voorbeelden van alle vervaardigde bestanden en de te genereren overzichten.

ad 2 Programmadocumentatie
Deze bevat een blokdiagram waarin de belangrijkste verwerkingsstappen voor ieder programma zijn vastgelegd en een detailblokschema waarin de logica van het programma is vastgelegd.

Tevens is hier een door de computer vervaardigde afdruk van de programma-instructies opgenomen zoals deze door de programmeur zijn opgesteld.

ad 3 Bedieningsinstructies (run manuals)
Deze bevatten werkinstructies voor de operateurs, zoals de te gebruiken bestanden, soort papier (bijvoorbeeld 1- of 2-voud), uit te voeren handelingen op grond van meldingen op de bedieningsconsole, etc.

ad 4 Programma's in onvertaalde of vertaalde vorm (source of object decks)
Onder een source deck verstaan we een programma geschreven in een programmeertaal (COBOL, FORTRAN en dergelijke) dat door een speciaal vertaalprogramma (de compiler) in een voor de computer begrijpelijke vorm dient te worden omgezet; de resultante van dit vertaalproces is het object deck. Het is duidelijk dat het programma een onmisbaar onderdeel is van een disasterplan.

ad 5 De benodigde job control voor produktieprogramma's
Dit zijn opdrachten aan de computer, geschreven in een speciale taal - de job control language - waarin wordt medegedeeld welk programma moet worden uitgevoerd, waar de invoer te vinden is en waar de uitvoer gebracht moet worden.

ad 6 Besturingssystemen
Dit zijn door de fabrikant geleverde programma's welke de gebruiker in staat stelt de door hem ontwikkelde programma's op de computer te verwerken.

Dit systeem regelt bijvoorbeeld het verkeer tussen de verschillende perifere eenheden, het sorteren, het tegelijkertijd uitvoeren van meerdere programma's, het besturen van magneetbandeenheden en dergelijke.

ad 7 Invoergegevens in machinaal leesbare vorm
Het grootvader-vader-zoon principe berust op de gedachte dat uit het vorige bestand (de vader) met behulp van de vorige mutaties het nu gebruikte bestand (de zoon) kan worden gereconstrueerd. Het is in dit verband dan ook raadzaam de vorige mutaties in machinaal leesbare vorm te bewaren, opdat deze reconstructie snel kan geschieden.

ad 8 Formulierenvoorbeelden
Dit zijn voor de drukker bestemde lay-outs van de formulieren waarop de computer zijn gegenereerde gegevens afdrukt. Op deze lay-outs staan de kopgegevens, vlakverdeling en dergelijke.

ad 9 Noodvoorraad voornaamste voorgedrukte formulieren
Ook dit zijn elementaire zaken benodigd voor de informatieverwerking. Te denken valt aan voorgedrukte salarisstroken, facturen, rekening-courant-overzichten, etc.

Bij vernietiging van de aanwezige voorraad door een calamiteit kan niet direct voor aanvulling gezorgd worden, zodat het aanhouden van een kleine buffervoorraad van essentiële formulieren een goede voorzorgsmaatregel is.

ad 10 Besturingsbandjes voor de afdrukeenheid
Dit zijn bandjes waaruit de computer door middel van ponsingen kan bepalen hoever hij het blad op moet schuiven alvorens bepaalde regels te drukken.

Alle genoemde programmatuur, gegevens, hulpmiddelen en dergelijke kunnen nodig zijn voor de heropbouw van de informatieverwerking indien deze door een calamiteit is verstoord.

Om te voorkomen dat de reserve-exemplaren door dezelfde calamiteit vernietigd of beschadigd worden als die welke de originele programmatuur, gegevens en dergelijke heeft getroffen, dienen zij op een veilige plaats opgeborgen te worden.

Hierbij dient men de voorkeur te geven aan een lokatie welke niet dezelfde is als die waarin het computercentrum is gehuisvest. Het spreekt vanzelf dat deze lokatie adequaat beveiligd dient te zijn.

Gaat men over tot het aanhouden van dergelijke back-up exemplaren, dan gaat het erom dat men de uiterste zorg besteedt aan het continu bijhouden van de reserve-exemplaren, zodat deze steeds zijn aangepast aan de actuele werksituatie. Het zou bijvoorbeeld bijzonder vervelend zijn als men de salarissen ging berekenen met een back-up salarisprogramma van 2 jaar oud.

Het up to date houden van de back-up exemplaren is bepalend voor het daadwerkelijk kunnen continueren van de informatieverwerking nadat zich een disaster heeft voorgedaan.

7 Hardware back-up

Een plan tot hardware back-up valt uiteen in 2 delen:

1 een plan tot continuering van de informatieverwerking door middel van een alternatieve verwerkingsmogelijkheid, de zogenaamde „alternate site".
2 een plan tot reconstructie van het bestaande rekencentrum of de bestaande installatie.

ad 1 Alternate site

Bij het zoeken naar een geschikte alternatieve verwerkingsmogelijkheid dient men met de volgende punten rekening te houden:

- Is de beschikbare tijd voldoende voor het verwerken van de door ons vereiste informatie?
- Is de installatie op een dusdanig tijdstip beschikbaar dat wij, gezien onze informatiebehoefte, tijdig over de informatie kunnen beschikken?
- Is de apparatuur op de alternate site compatibel met onze apparatuur? Men dient te denken aan de grootte van het geheugen, voldoende magneetband- of schijveneenheden en dergelijke.
- Kunnen onze programma's verwerkt worden onder het bij de alternate site in gebruik zijnde besturingssysteem?
  Men dient rekening te houden met een afwijkende versie of opties welke kunnen betekenen dat de programma's niet zonder meer op de andere computer verwerkt kunnen worden.
  In dat geval zullen de programma's aangepast moeten worden en dient men rekening te houden met de hiermede gepaard gaande kosten en vertraging in geval van nood.
- Wat voor soort overeenkomst kunnen wij met de wederpartij sluiten? Te denken valt aan een wederzijdse overeenkomst, waarbij de betrokken computercentra elkaars back-up zijn.
  Heeft men in dat geval capaciteit genoeg op het eigen systeem?
  Kan men tot een overeenkomst komen over een vast aantal uren verwerkingstijd of laat men dit van de omstandigheden afhangen?
- Zijn er op de alternate site mogelijkheden tot opslag van onze kopieprogramma's en bestanden?
- Is men in staat de alternate site „bij" te houden?
  Men dient met de alternate site een systeem van communicatie op te zetten ten einde op de hoogte te blijven van alle veranderingen in apparatuur en besturingssystemen, beschikbare tijd en dergelijke, opdat vastgesteld kan worden op welk moment de alternate site niet langer geschikt meer is om als uitwijkmogelijkheid te kunnen fungeren.

Gegeven een goed uitgewerkt en bijgehouden back-up systeem en een weloverwogen keuze van de alternate site, is het mogelijk althans een deel van de informatieverwerking te continueren indien zich een disaster heeft voorgedaan. Tegelijkertijd dient men tot reconstructie van de bestaande installatie over te gaan.

ad 2 Plan tot reconstructie
Er zijn hierbij verschillende alternatieven te onderkennen.
a. Herstel van de beschadigde apparatuur. Een dure oplossing; veelal zal men aan het volgende alternatief de voorkeur geven.
b. Vervanging van apparatuur door identieke (al of niet nieuw) of
c. vervanging door modernere apparatuur.

Veelal zal men tot alternatief *c.* besluiten, om op deze manier „van de nood een deugd te maken".

De keuze zal dan bijna altijd vallen op apparatuur van dezelfde leverancier. Conversie naar andere apparatuur kost immers veel tijd en geld, omdat de bestaande programma's niet zonder meer op systemen van andere leveranciers verwerkt kunnen worden.

Het verdient aanbeveling zich, behalve over bovengenoemde alternatieven, eveneens te beramen over de relocatie van apparatuur.

Beschikt men over meerdere systemen in 1 rekencentrum, dan kan men besluiten deze te spreiden over meerdere centra, „to separate the eggs into more baskets".

8 Verzekering

Zoals uit het voorgaande blijkt kan de schade toegebracht aan automatische informatieverwerkende systemen belangrijke financiële consequenties hebben voor de onderneming.

De verzekeringsmaatschappijen bieden de mogelijkheid voor computergebruikers zich te verzekeren tegen de financiële gevolgen welke voortvloeien uit schade aan de computerinstallatie.

Deze computerverzekeringen dekken enkele uit calamiteiten voortvloeiende schaden, zoals:

- De kosten voor reparatie/vervanging van beschadigde apparatuur, alsmede de bijbehorende fysieke vervanging van de informatiedragers (waarbij de hierin opgeslagen informatie buiten beschouwing wordt gelaten). De uitkering kan geschieden op basis van de historische uitgaafprijs of de vervangingswaarde.
- De kosten welke verband houden met het werken op een elders opgestelde computer, wanneer het eigen systeem op „storing staat", zoals huur-, transport-, overwerk-, reis- en verblijfkosten.
- Kosten voor het uitwijken naar een andere computer door stilstand van het eigen systeem ten gevolge van schade aan de airconditioning-installatie.
- De kosten verbonden aan het converteren van programma's ten einde op elders opgestelde apparatuur te kunnen werken.
- De kosten voor het reconstrueren van gegevens op informatiedragers.
- De kosten om de uitoefening van het bedrijf mogelijk te maken tijdens dit reconstrueren.
- De schade voortvloeiende uit het niet of slechts gedeeltelijk functioneren van het bedrijf (de zogenaamde bedrijfsschade).

m a b blz. 172

In principe zijn deze verzekeringsvormen toepasselijk op zowel gehuurde als gekochte apparatuur.

De premie zal van geval tot geval worden vastgesteld, veelal na inspectie van het rekencentrum.

Van veel belang voor de premiehoogte zijn de bepalingen in de huur- c.q. onderhoudscontracten, de bouwaard van het pand, de genomen beveiligingsmaatregelen en de maatregelen tot back-up.

9 Conclusie

De onderneming zal zich door een complex van maatregelen dienen te beschermen tegen alle factoren welke de continuïteit van het informatieverwerkend proces kunnen verstoren, ter handhaving van de tijdigheid en continuïteit van de informatievoorziening.

De hiertoe te nemen maatregelen zullen gericht moeten zijn op zowel preventie van calamiteiten als op herstel van aangebrachte schade en dekking tegen de uit de schade voortvloeiende financiële consequenties. De kosten gepaard gaande met het uitvoeren van deze maatregelen zullen hoog zijn. De rechtvaardiging van deze kosten is te vinden in de schade welke door stagnatie in de informatievoorziening aangericht kan worden. Na een grondige studie van zowel „costs" als „benefits", zal men vaak inzien dat ook hier geldt: „De kost gaat voor de baat uit".

Literatuur

Burt, K. H., *Computer Center Security: Protecting the Achilles Heel.* The Magazine of Bank Administration, April 1970.

Browne, P. S., *Computer Security - A Survey.* Data Base, April 1973.

EDP Analyzer, December 1971, Vol. 9, No. 12. *Security of the Computer Center.*

EDP Analyzer, January 1972, Vol. 10, No. 1. *Computer Security: Back-up and Recovery Method.*

Farr, M. A. L. e.a., *Security for Computer Systems.* National Computing Centre Limited, 1972. Quay House, Quay Street, Manchester M3 3HU.

Hallinan, A. J., *Internal Audit of a Computer Disaster Plan.* The Internal Auditor, 1970.

Scoma, L., *Protecting your EDP.* The Office, September 1971.

Tassel, D. van, *Computer Security Management.* Prentice-Hall Inc. 1972. Englewood Cliffs, New Jersey.

Verba, J., *Protecting your EDP Investment.* Management Services, September-October 1970.

Wasserman, J. J., *Plugging the Leaks in Computer Security.* Harvard Business Review, September-October 1969.

Voorts ten aanzien van nieuwe ontwikkelingen en ervaringen:

- EDPACS. The EDP Audit Control and Security Newsletter. Publ. Harold Weiss, Automation Training Center, 1930 Isaac Newton Square East, Reston, Virginia 22090. USA. Vol. I 1973/74. Maandblad in eenvoudige vorm; de afleveringen omvatten circa 20 A-4-pagina's. [Zie ook: De Accountant, *80* (1974), nr. 7 (maart), blz. 326.]