EDP-audit bij middelgrote systemen

Drs. W. F. de Koning

In de literatuur over EDP-audit wordt overwegend aandacht besteed aan grote computersystemen (mainframes). Daaruit zou de conclusie getrokken kunnen worden dat middelgrote en kleine computers (mini- en microcomputers) niet interessant zijn voor een EDP-auditor. De overgrote meerderheid van de geplaatste computersystemen behoort echter tot de laatste twee categorieën. In de groep minicomputers zijn de afgelopen jaren enkele systemen verschenen, die technisch gezien voldoende mogelijkheden hebben om een goede vorm van interne controle te realiseren. Daarbij kan gedacht worden aan de AS/400 van IBM, de (Micro)VAX van DEC en verschillende computers met het besturingssysteem UNIX System V. In dit artikel wordt ingegaan op voor een controlerend accountant interessante aspecten van de beveiliging van dergelijke systemen. In een appendix wordt toegelicht hoe de beveiliging in een concreet geval, namelijk de AS/400 van IBM, op zijn goede werking getoetst kan worden.
Het beoordelen van het niveau van beveiliging in en rond computersystemen vereist een behoorlijke kennis van de gebruikte apparatuur en bijbehorende besturingssystemen. Het is dan ook niet verstandig dat algemene accountants zelf dergelijke beoordelingen uitvoeren. Zij zullen echter wel op de hoogte moeten zijn van de doelstellingen en de werkwijze van de EDP-auditor. Op basis daarvan kan de waarde worden bepaald die aan de uitkomsten van een EDP-audit moet worden toegekend.

Aandachtsgebieden van de accountant

Een accountant, die controleert in een geautomatiseerde omgeving (welke omgeving is dat tegenwoordig niet?), zal aandacht moeten besteden aan interne controles in de geautomatiseerde systemen. De diepgang waarmee deze interne controles worden beoordeeld hangt af van de controlebenadering van de accountant. Een belangrijke vraag daarbij is in hoeverre gesteund wordt op de interne controle, dat wil zeggen in hoeverre een systeemgerichte controlebenadering wordt gekozen.
Het is zinvol onderscheid te maken tussen:
- algemene beheersingsmaatregelen (general controls);
- beheersingsmaatregelen in toepassingen (application controls).

De toepassingsprogrammatuur is vaak een verlengstuk van de administratieve organisatie. Een accountant zal zich daar altijd in meer of mindere mate in moeten verdiepen. Besluit de accountant bij zijn controle in belangrijke mate te steunen op de geautomatiseerde gegevensverwerking, dan zullen ook de algemene beheersingsmaatregelen beoordeeld moeten worden. Vastgesteld moet dan worden dat de toepassingen zich in een veilige omgeving afspelen. Een beoordeling van de algemene beheersingsmaatregelen kan ook uitgevoerd worden op verzoek van de leiding van de organisatie of in het kader van een ruime controleopdracht, waarin een beoordeling van de interne procedures uitdrukkelijk is opgenomen.

Algemene beheersingsmaatregelen
Bij het beoordelen van de interne controle zijn vooral de volgende categorie- en beheersingsmaatregelen van belang:
- fysieke beveiliging;
- logische (toegangs)beveiliging;

Drs. W. F. de Koning, registeraccountant, is vennoot van Paardekooper & Hoffman Registeraccountants en als zodanig verantwoordelijk voor EDP-auditing. Hij is tevens als docent verbonden aan de postdoctorale opleiding EDP-auditing van de Erasmus Universiteit.

– functiescheidingen rond de computer;
– systeemontwikkelingsprocedures;
– continuïteitsvoorzieningen.

Fysieke beveiliging, waaronder toegangsbeveiliging tot de computerruimte, heeft lange tijd een belangrijke plaats ingenomen bij de beoordeling van de interne controle. Door het toenemend gebruik van transactiegewijze verwerking met behulp van werkstations, die bij eindgebruikers zijn opgesteld, heeft deze beveiliging aan betekenis ingeboet. Daartegenover is een toenemende belangstelling voor logische beveiliging ontstaan. Onder logische beveiliging wordt verstaan het beperken van de toegang die via werkstations tot bestanden en programma's kan worden verkregen. Aan gebruikers worden autorisaties toegekend waarmee geregeld wordt welke acties wèl en welke niet zijn toegestaan.
Eén van de fundamenten van interne controle is functiescheiding. Met behulp van autorisatiecontroles kan (bij goed geautomatiseerde systemen) functiescheiding op een eenduidige en controleerbare manier gerealiseerd worden. Het niveau van interne controle kan daardoor verbeterd worden, waar een accountant uiteraard gebruik van kan maken.
Systeemontwikkelingsprocedures moeten betrouwbare en onderhoudbare toepassingen waarborgen. In dit artikel zullen deze procedures alleen zijdelings aan de orde komen. Zij zijn grotendeels onafhankelijk van de gebruikte apparatuur.
Continuïteitsvoorzieningen bestaan onder meer uit backup- en herstelprocedures, mutatielogging en uitwijkregelingen. Langzamerhand begint de opvatting veld te winnen dat een accountant zich ook hierover een oordeel moet vormen.

Opzet en werking
Vanaf NIvRA-geschrift nr. 13 wordt onderscheid gemaakt tussen het beoordelen van de opzet van de interne controle en het toetsen van de werking daarvan. De literatuur over interne controle in een geautomatiseerde omgeving beperkt zich in veel gevallen tot een beschrijving van de wenselijk geachte opzet van de interne controle. Voor een accountant is het echter van groot belang, dat vastgesteld kan worden dat een gekozen opzet ook daadwerkelijk is gerealiseerd en gedurende de controleperiode is gehandhaafd.

Om de werking te beoordelen moet 'audit-evidence' verkregen worden. Deze bewijsmiddelen zullen voor een belangrijk deel bestaan uit informatie die uit het systeem kan worden opgevraagd. Het gaat daarbij vooral om parameterinstellingen, toegekende autorisaties en diverse vormen van logging van het systeemgebruik. De mogelijkheden om deze informatie te verkrijgen verschillen van systeem tot systeem.
In steeds meer systemen zijn mogelijkheden aanwezig voor door de gebruiker te definiëren rapportages. De controlewaarde, die aan dergelijke rapportages kan worden toegekend, neemt af met de flexibiliteit van de rapportagevormen. Het wordt dan een aantrekkelijke optie voor de accountant om zelf van deze rapportagemogelijkheden gebruik te maken. Dat opent de mogelijkheid om direct de in het systeem opgeslagen gegevens te controleren en niet meer afhankelijk te zijn van afgeleide informatie.

Fysieke beveiliging

– *toegangsbeveiliging*
Bij grote computersystemen (mainframes) is veelal sprake van een afzonderlijk rekencentrum met bijbehorende toegangscontrole. Middelgrote computers zullen in de meeste gevallen gewoon op de werkvloer bij gebruikers zijn opgesteld. Het belangrijkste probleem dat daardoor ontstaat, is de mogelijkheid dat ongeautoriseerden via het bedieningsconsole toegang krijgen tot het systeem. Een console biedt vaak verdergaande mogelijkheden dan een gewoon werkstation. Bij het opstarten van het systeem kunnen bijvoorbeeld parameterinstellingen worden gewijzigd, waardoor het beveiligingsniveau kan worden beïnvloed. Op sommige systemen is het mogelijk ieder willekeurig werkstation tot console te benoemen. Het is duidelijk dat de bedieningsfuncties dan alleen door daartoe geautoriseerden mogen worden uitgevoerd. Er moet tegen gewaakt worden dat de bedieningsconsole onbeheerd aan blijft staan.

Het in- en uitschakelen van het systeem is een kritische handeling. Is het mogelijk het systeem met een schakelaar aan of uit te zetten, dan mag deze schakelaar zeker niet voor iedereen toegankelijk zijn.

Sommige computers zijn uitgerust met een schakelaar, waarmee de beveiliging kan worden gewijzigd. Deze schakelaar dient met name voor onderhoudswerkzaamheden. De sleutel waar deze schakelaar mee bediend wordt, moet op een veilige plaats, bijvoorbeeld in een kluis bij de directie, worden opgeborgen en mag alleen tijdens onderhoud aan het systeem worden uitgegeven.

– *omgevingsfactoren*
Hoewel minicomputers geen airconditioning meer vereisen, blijft het zinvol de computerruimte te beschermen tegen al te grote temperatuurschommelingen en een hoge vochtigheidsgraad. Bij tropische temperaturen worden de verwerkingsresultaten soms onvoorspelbaar.
De stroomvoorziening in Nederland functioneert redelijk storingsvrij. Toch komt een tijdelijke onderbreking van de stroomvoorziening, vooral in industriegebieden, wel eens voor. Voor de meeste minicomputers is een voorziening waardoor het systeem, na stroomuitval, nog enkele minuten op een accu kan doorwerken zeer wenselijk. Een onderbreking van de spanning kan ertoe leiden dat bestanden verminkt raken, bijvoorbeeld doordat indexbestanden niet meer overeenstemmen met de gegevensbestanden. Het systeem moet de mogelijkheid hebben om op reguliere wijze zijn bestanden af te sluiten.

– *overige beschermingsmaatregelen*
Speciale inbraakbeveiliging voor de ruimte waar de computer staat opgesteld verdient zeker overweging. Het komt voor dat complete computersystemen gestolen worden. Door de beperkte omvang van de huidige computers wordt het ontvreemden eenvoudiger. Diefstal van een compleet computersysteem ondermijnt de continuïteit van de gegevensverwerking, maar leidt er tevens toe dat vertrouwelijke gegevens in verkeerde handen komen.
De laatste tijd verschijnen berichten over de mogelijkheid computerapparatuur elektronisch af te luisteren. Elektromagnetische straling kan met relatief eenvoudige apparatuur op afstand opgevangen worden, waarna gegevens in leesbare vorm op een beeldscherm geprojecteerd kunnen worden. Terminals en kabels zijn af te schermen voor deze straling.
Backup-bestanden moeten beveiligd worden. In theorie is het mogelijk backup-kopieën te manipuleren, waardoor na een geforceerde herstelloperatie gebruikers over andere autorisaties beschikken. Ook uit het oogpunt van een goede continuïteitswaarborg is het gewenst backupmedia zorgvuldig op te bergen. Daartoe moet gebruik gemaakt worden van speciale datasafes, die een hoge mate van brandbeveiliging bieden. Magnetische gegevensdragers zijn gevoeliger voor temperatuurverhoging dan bijvoorbeeld papier. Data-safes maken brandblusapparatuur overigens niet overbodig.

Logische toegangsbeveiliging

– *gebruikerscodes*
Wanneer op één systeem meerdere gebruikers actief zijn, zullen de gebruikers geïdentificeerd moeten worden met een gebruikerscode. Uit het oogpunt van toegangsbeveiliging is het zonder meer noodzakelijk dat de identiteit van de gebruiker door het systeem wordt geverifieerd. In de meeste gevallen wordt daartoe gebruik gemaakt van wachtwoorden. Soms worden andere verificatiemidelen gebruikt, zoals bijvoorbeeld 'cardkeys' of fysieke sleutels.
Gebruikerscodes moeten op een zinvolle en eenduidige manier worden samengesteld. Codes als 'Piet' of 'Marie' zijn bij de controle erg hinderlijk. Een code kan bijvoorbeeld worden samengesteld uit een afkorting van de afdeling, waar de gebruiker werkzaam is, met een volgnummer. Het is gewenst dat iedere gebruiker zijn eigen gebruikerscode heeft. Eén code voor een hele afdeling maakt het onmogelijk acties van individuele gebruikers te volgen.

Krakers van computersystemen maken weleens gebruik van default-gebruikerscodes, die bij

oplevering van het systeem worden meegeleverd. Het gaat daarbij vaak om codes met een hoge autorisatie, die benodigd zijn voor de installatie van het systeem. Deze codes, in ieder geval de bijbehorende wachtwoorden, moeten zo snel mogelijk gewijzigd worden.

– *wachtwoorden*
Het is wenselijk dat gebruikers in staat zijn zelf hun wachtwoorden te wijzigen. Wachtwoorden worden vaak in versleutelde vorm in het systeem opgeslagen. Zelfs de systeembeheerder is dan niet in staat wachtwoorden op te vragen. Een gebruiker kan echter zijn wachtwoord vergeten. Het is daarom gebruikelijk dat de systeembeheerder in staat is wachtwoorden te overschrijven.
Aan wachtwoorden moet de eis gesteld worden dat zij een minimale lengte hebben (bijvoorbeeld zes posities). Hoe langer het wachtwoord, hoe moeilijker het wordt een wachtwoord te raden of via een computer te genereren. Veel systemen hebben de mogelijkheid de noodzakelijke minimale lengte af te dwingen. In de recente versies van het besturingssysteem Unix wordt zelfs de eis gesteld, dat het wachtwoord minimaal één cijfer of speciaal teken bevat. Het 'kraken' van versleutelde wachtwoorden wordt daardoor bemoeilijkt.
Wachtwoorden worden bij voorkeur regelmatig gewijzigd. Een wachtwoord kan na verloop van tijd ook aan niet-geautoriseerden bekend worden, bijvoorbeeld door het over de schouder meekijken bij het intoetsen van het wachtwoord. Er zijn systemen die het regelmatig wijzigen van wachtwoorden kunnen afdwingen.
Om het uitproberen van wachtwoorden te voorkomen is het wenselijk dat het systeem signaleert wanneer een gebruiker meerdere malen een onjuist wachtwoord invoert. Het aantal toegestane foutieve aanmeldpogingen wordt dan bij voorkeur op niet meer dan drie gesteld. Bij overschrijding van dit aantal sluit het systeem het werkstation af en geeft een melding op het console of in een logbestand.
Een bijzondere vorm van toegangsbeveiliging is het koppelen van gebruikers aan (adressen van) werkstations. Wanneer deze faciliteit voorhanden is, kan daarvan gebruik gemaakt worden om bijvoorbeeld gebruikers met hoge autorisatie slechts toe te laten vanaf daartoe aangewezen werkplekken. De flexibiliteit van het gebruik wordt daardoor evenwel verminderd.

– *autorisatie per transactie*
Het computergebruik van eindgebruikers beperkt zich veelal tot het uitvoeren van applicatieprogramma's. De beveiligingsmaatregelen kunnen daar op inspelen door aan dergelijke eindgebruikers dan ook niet meer mogelijkheden te bieden dan het opstarten van applicaties. Dat kan in veel systemen bereikt worden door de gebruikers een verplicht startprogramma of startmenu toe te kennen. Dat biedt een goede bescherming tegen computermisbruik door eindgebruikers, mits zij niet in staat zijn met functietoetsen en andere systeemcommando's aan het keurslijf van de verplichte programma's of menu's te ontkomen. De programma's moeten op een deugdelijke wijze opgebouwd zijn en mogen bijvoorbeeld niet zelf om systeemcommando's vragen of in foutsituaties een uitgang naar het systeem bieden.
Op de meeste systemen zijn hulpprogramma's voor bestandsmanipulatie aanwezig. Ook deze hulpprogramma's moeten in voldoende mate voor eindgebruikers zijn afgegrendeld.
Door een zorgvuldige toewijzing van menu's, waaruit toegestane programma's gekozen kunnen worden, is een goede vorm van functiescheiding tussen eindgebruikers te realiseren. Alleen die programma's mogen in het menu ter beschikking gesteld worden, die gebruikers voor de uitoefening van hun functie nodig hebben.
Bij voorkeur wordt gebruik gemaakt van menu's voor groepen gebruikers. De functiescheidingen worden daardoor overzichtelijker en beter beheersbaar. De functiescheiding tussen eindgebruikers kan bijvoorbeeld bij een handelsonderneming als volgt geregeld zijn:
De verkoopafdeling mag alleen voorraden raadplegen en orders invoeren. De inkoopafdeling mag voorraden raadplegen en daarnaast inkooporders invoeren. Het magazijn krijgt de beschikking over programma's voor het invoeren van goederenontvangsten en het gereedmelden van verkooporders. De administratie mag kredietlimiten inbrengen, de facturering opstarten en finan-

ciële boekingen invoeren. Als de omvang van de administratie het toelaat is nog een verdere functiescheiding te realiseren door bijvoorbeeld onderscheid te maken in autorisaties voor de debiteuren-, crediteuren- en grootboekadministratie.
Functiescheiding tussen groepen gebruikers of afdelingen is 'harder' dan functiescheiding tussen personen. Personen gaan op vakantie of kunnen om andere redenen afwezig zijn, in welk geval een ander de functie zal waarnemen. Binnen een afdeling is vervanging eenvoudiger te regelen.
Menubeveiliging zal alleen worden toegepast voor eindgebruikers. Het is praktisch gesproken niet mogelijk operators en programmeurs met menu's te laten werken. Ook is het niet mogelijk om op deze manier de mogelijkheden die opvraagtalen en tekstverwerkingspakketten soms bieden om bestanden te wijzigen voldoende af te schermen. In deze gevallen wordt autorisatie op bestandsniveau noodzakelijk.

– *bestandsbeveiliging*
Bestandsbeveiliging omvat het toekennen van toegangsrechten tot bestanden aan (groepen van) gebruikers. De toegangsrechten worden doorgaans onderscheiden in:
- rechten met betrekking tot bestanden als object, zoals rechten om bestanden aan te maken, te verplaatsen en te verwijderen (objectautorisatie) en
- rechten met betrekking tot de gegevens in de bestanden, zoals rechten om gegevens in een bestand te lezen, te wijzigen en te verwijderen (gegevensautorisatie).

Een programma is ook een bestand. Lees- of uitvoeringsautorisatie voor een programma betekent het recht het programma te gebruiken.
Een aantal besturingssystemen, waaronder Unix en VMS, maakt gebruik van hiërarchische bestandssystemen, waarbij bestanden worden ingedeeld in directories en subdirectories. In dat geval kunnen zowel per (sub)directory als per bestand toegangsrechten worden gedefinieerd. Autorisaties per directory zijn objectautorisaties. Een leesautorisatie voor een directory betekent bijvoorbeeld dat opgevraagd kan worden welke bestanden in de directory zijn opgenomen. Een schrijfautorisatie voor de directory houdt de mogelijkheid in bestanden toe te voegen en – bij Unix – te verwijderen. VMS kent een afzonderlijke autorisatie voor het verwijderen.
De toegangsrechten worden daarbij verdeeld in rechten voor de eigenaar van het object, rechten voor de groep waartoe de eigenaar behoort en rechten voor overige gebruikers (de 'world' in VMS-termen). Om een goede vorm van functiescheiding te realiseren is het dan zaak de gebruikers op een handige manier in groepen in te delen.
Het besturingssysteem van de AS/400 (OS/400) kent geen hiërarchisch bestandssysteem met directories. Zowel de objectautorisaties als de gegevensautorisaties moeten per bestand worden aangegeven, waarbij de autorisaties kunnen gelden voor afzonderlijke gebruikers, voor groepen van gebruikers dan wel voor alle gebruikers. Deze autorisaties kunnen opgenomen worden in gebruikers- of groepsprofielen, maar kunnen ook geregistreerd worden in autorisatielijsten per bestand.

OS/400 kent wel de mogelijkheid bestanden te groeperen in biliotheken. De toegangsrechten voor deze bibliotheken kunnen op dezelfde wijze als voor bestanden worden gedefinieerd en omvatten dus tevens de gegevensautorisatie voor de bestanden in de bibliotheek.
Zowel Unix als VMS kennen de mogelijkheid om, naast de in de directories vastgelegde autorisaties, per bestand aanvullende autorisaties voor individuele gebruikers te definiëren.

Het is van belang de autorisaties per bestand overzichtelijk te houden. Een té gedetailleerd gebruik van alle mogelijkheden om variaties in de toegangsbeveiliging per bestand te regelen leidt snel tot een niet meer te beheersen geheel. Bij voorkeur worden gelijksoortige bestanden in bibliotheken of directories gegroepeerd en wordt de toegangsbeveiliging op dat niveau geregeld. Alleen voor kritische bestanden (bijvoorbeeld een bestand waaruit betalingsopdrachten worden aangemaakt) is een verdergaande beveiliging zinvol.

Er moet rekening mee worden gehouden, dat één of meer gebruikers zullen beschikken over faciliteiten om beveiligingen te omzeilen. Ieder systeem zal een systeembeheerder ('super-user' of 'security-officer') hebben, die vergaande privileges heeft binnen het systeem. Ook aan andere gebruikers kunnen bijzondere bevoegdheden worden toegekend. Deze verdergaande bevoegdheden kunnen zijn opgenomen in autorisatietabellen of in het gebruikersprofiel. Ook is het mogelijk dat bij uitvoering van programma's tijdelijk een andere (doorgaans hogere) autorisatie wordt verkregen.

– *tijdelijke autorisaties*
Het is soms noodzakelijk dat een gebruiker met een programma een bestand muteert, terwijl de gebruiker geen schrijfrechten heeft voor dat bestand. Deze situatie kan zich onder meer voordoen, wanneer een eindgebruiker de beschikking heeft over een opvraagtaal om overzichten uit bestanden aan te maken. Om met een applicatieprogramma een bestand, bijvoorbeeld het voorraadbestand, te muteren, moet de gebruiker in principe schrijfbevoegdheid hebben voor dat bestand. Heeft de gebruiker daarnaast de mogelijkheid met een opvraagtaal (die vaak ook mogelijkheden heeft om bestanden te muteren) voorraadoverzichten aan te maken, dan is het gewenst dat de schrijfbevoegdheid alleen toegekend wordt wanneer het bestand via het applicatieprogramma wordt benaderd.

Dat kan gerealiseerd worden door het tijdelijk overnemen van de autorisatie van het programma door de gebruiker. Dat wordt wel 'adopted authority' (OS/400) of 'set user id' (UNIX) genoemd. Deze faciliteit heeft een nogal negatieve klank gekregen, omdat daarmee in de praktijk wel gemanipuleerd is om ten onrechte een hogere autorisatie te verkrijgen dan is toegestaan. Er bestaat bijvoorbeeld het risico van 'Trojaanse paarden', dat wil zeggen programma's die ongemerkt door een geautoriseerde gebruiker worden opgestart en vervolgens zijn autorisatie gebruiken. Gebruikt het programma dat zijn autorisatie overdraagt bijvoorbeeld 'call'-instructies, dan zou een 'call' gedaan kunnen worden naar een 'Trojaans paard', dat daarmee de gewenste autorisatie verkrijgt.
Belangrijk is, dat programma's die hun autorisatie overdragen een niet te hoge autorisatie hebben (wat bij standaardpakketten nog weleens voorkomt), zo weinig mogelijk gebruik maken van 'call'-instructies en goed in elkaar zitten.

Functiescheiding rond de computer

De gebruikers van een middelgroot computersysteem zijn te verdelen in de volgende groepen:
– de systeembeheerder(s);
– eindgebruikers;
– programmeurs;
– operators.

Soms ontbreekt de groep programmeurs. Er wordt dan alleen gebruik gemaakt van door derden ontwikkelde applicaties, dat wil zeggen standaardpakketten of door een systeemhuis geschreven maatwerkprogramma's. Voor de beveiliging is dat een gunstige situatie.
Vaak ontbreekt de groep operators. De bedieningstaken worden dan uitgevoerd door de systeembeheerder(s), door programmeurs of door eindgebruikers. Dat is een minder gunstige situatie. In al deze gevallen treedt functievermenging nog het minst op, wanneer een systeembeheerder de operatorfuncties uitoefent. Soms is de systeembeheerder tevens programmeur of eindgebruiker. Beide combinaties zijn ongewenst.

– *de systeembeheerder*
De systeembeheerder (de 'super-user' of 'security-officer') is oppermachtig in het systeem. Hij of zij is in staat om autorisatiecontroles te ontwijken en om aan andere gebruikers (en zichzelf) bijzondere autorisaties toe te kennen. De organisatie dient zich bewust te zijn van deze zwakte in de interne controle. De toepassingen dienen aan eindgebruikers mogelijkheden te bieden de gegevensverwerking in voldoende mate te controleren, bijvoorbeeld door middel van totaalcontroles of met behulp van analytische overzichten. Kritische transacties (bijvoorbeeld uitgaande betalingen) moeten met aanvullende controles omgeven zijn.

Aan de selectie van een systeembeheerder dient de nodige aandacht besteed te worden. Bij voorkeur is deze functionaris niet gedetailleerd op de hoogte van alle administratieve procedures.
In kritische situaties is het mogelijk, zij het niet zonder bijzondere inspanningen, aanvullende controles uit te oefenen op de handelingen van de systeembeheerder. Daartoe kan bijvoorbeeld een interne-controlemedewerker worden ingeschakeld. Eventuele loggingsfaciliteiten kunnen gebruikt worden om na te gaan welke acties de systeembeheerder heeft uitgevoerd. Bovendien zullen de toegekende autorisaties dan regelmatig gecheckt moeten worden.
Soms biedt de besturingsprogrammatuur mogelijkheden met meer systeembeheerders te werken, die ieder een beperkt gedeelte van het systeem onder hun beheer hebben. Daarvan kan gebruik gemaakt worden om een hiërarchie onder systeembeheerders te realiseren. De hoogste systeembeheerder zal dan meer een coördinerende functie hebben. De dagelijkse beheersactiviteiten worden door lager geplaatste systeembeheerders uitgevoerd. Het is duidelijk dat een organisatie voldoende omvang moet hebben om deze functiescheiding te kunnen realiseren.
In het geval dat in de organisatie slechts één systeembeheerder aanwezig is, moeten maatregelen genomen worden voor vervanging bij vakantie en andere afwezigheid. Bij voorkeur wordt daartoe een tweede gebruikerscode met systeembeheerbevoegdheden op het systeem gedefinieerd. Deze gebruikerscode wordt alleen in noodgevallen gebruikt. Het wachtwoord van deze gebruikerscode wordt op een veilige plaats, bijvoorbeeld in de kluis van de directie bewaard. Het wachtwoord wordt, indien nodig, aan een vervanger kenbaar gemaakt en na terugkomst van de systeembeheerder zo snel mogelijk door hem of haar gewijzigd. Aan de hand van de systeemlogging kan nagegaan worden welke acties tijdens de vervanging zijn uitgevoerd.
Een reserve-gebruikerscode kan tevens gebruikt worden voor het geval de systeembeheerder zijn wachtwoord vergeten is. Veel systemen zijn zo goed beveiligd, dat alleen met behulp van technici van de leverancier de gebruikerscode van de systeembeheerder achterhaald kan worden.

– *eindgebruikers*
Eindgebruikers worden zoveel mogelijk beperkt tot het uitvoeren van applicatieprogramma's. In het voorgaande is al aangegeven dat bij het gebruik van keuzemenu's een goede functiescheiding tussen eindgebruikers is te realiseren.
Wanneer het centrale systeem tevens voor tekstverwerking wordt gebruikt is het noodzakelijk aan gebruikers afzonderlijke directories of libraries toe te kennen waar de tekstbestanden kunnen worden opgeslagen. De produktiebestanden moeten voor hen afgegrendeld worden.
Het direct benaderen van produktiebestanden met opvraagtalen en report-writers door eindgebruikers moet uit beveiligingsoogpunt zoveel mogelijk vermeden worden. Bovendien kan het leiden tot overdadig beslag op het systeem.

– *programmeurs*
In veel gevallen hebben programmeurs te grote bevoegdheden op het systeem. Voor het ontwikkelen van programma's zijn geen speciale autorisaties nodig. Het is van belang de programmeeromgeving zorgvuldig te scheiden van de produktie-omgeving. Dat kan bereikt worden door aan programmeurs afzonderlijke bibliotheken of directories toe te kennen. Onder Unix is het mogelijk een volledig gescheiden werkomgeving te creëren door gebruik te maken van 'protected subsystems'.
Het toevoegen van programma's aan produktiebibliotheken vereist over het algemeen een hoge autorisatie. Het in produktie brengen zal daarom voorbehouden moeten zijn aan de systeembeheerder of een speciale applicatiebeheerder. Programma's worden pas in produktie gebracht als zij volledig uitgetest zijn (ook door de betrokken eindgebruikers), voldoende gedocumenteerd zijn en bij voorkeur doorgenomen zijn door een andere programmeur ('peer-review'). De uitgeteste programma's worden opnieuw gecompileerd. Ook de operationele bronprogramma's worden in een beveiligde bibliotheek opgeslagen.
Het installeren van nieuwe versies van standaard besturings- of applicatieprogrammatuur is voorbehouden aan de systeembeheerder. Vastge-

steld moet worden dat de nieuwe versies uit onverdachte bron afkomstig zijn. Het is wel voorgekomen, dat zij 'Trojaanse paarden' bevatten.

– *operators*
Juist in een minicomputer-omgeving is de functie van operator minder noodzakelijk. Veel van de operatortaken worden door het systeem of door gebruikers uitgevoerd. Het opstarten van het systeem of het maken van backup-kopieën blijft echter een kritische handeling, die bij voorkeur niet door eindgebruikers of programmeurs wordt uitgevoerd. In de meeste gevallen zal dat een taak van de systeembeheerder zijn.

Overige aandachtspunten

– *datacommunicatie*
Datacommunicatie leidt tot beveiligingsrisico's. Deze risico's moeten zoveel mogelijk beperkt worden. Wanneer via kieslijnen toegang tot de computer kan worden verkregen verdient het aanbeveling gebruik te maken van automatische terugbelfaciliteiten.

Bij voorkeur wordt aan gebruikers van andere systemen niet zonder meer toegang verleend tot het systeem, maar wordt eerst de identiteit geverifieerd (met een wachtwoord). Het is wenselijk aan 'buitengebruikers' alleen toegangsrechten voor daartoe aangewezen directories of bestanden toe te kennen. File-transfer is altijd gevaarlijk en kan beter via een 'mailbox'-systeem geleid worden.
De datacommunicatieverbindingen moeten op veiligheid (onder meer tegen elektronisch afluisteren) beoordeeld worden.
Het koppelen van lokale netwerken aan het systeem kan bijzondere risico's met zich meebrengen. De gegevensstroom die via het netwerk verloopt is vaak op eenvoudige wijze te onderscheppen.
Voor datacommunicatie kan encryptie van gegevens overwogen worden. Het DES-algoritme voor encryptie biedt voldoende beveiliging. Het beheer van de vercijferingssleutel vraagt in dat geval bijzondere aandacht. Encryptie is overigens niet aan te bevelen voor gegevensbestanden op de computer. In de praktijk geeft dat te veel problemen.

– *wormen en virussen*
Kwaadwillenden scheppen er wel eens genoegen in de goede werking van computers en netwerken te ondermijnen met wormen en virussen. In beide gevallen is sprake van bijzonder hinderlijke programma's, die een computer of een netwerk volledig kunnen blokkeren. Wormen verspreiden zichzelf. Virussen hechten zich aan andere programma's en verspreiden zich op die manier. Verdachte programma's en programma's uit openbare bronnen moeten zoveel mogelijk vermeden worden. Het laden van bestanden op de computer moet met de nodige voorzorgen omgeven zijn.

Continuïteitsvoorzieningen

– *backup-kopieën*
Het is noodzakelijk regelmatig (in de meeste gevallen dagelijks) kopieën te maken van de gegevensbestanden. De backup-kopieën worden in minimaal drie generaties vastgehouden. Eén van de drie sets wordt bij voorkeur buitenshuis opgeslagen. De overige worden in datasafes bewaard. Daarnaast is het verstandig met een ruimer interval (bijvoorbeeld maandelijks) een extra kopie te vervaardigen en die langer te bewaren.
Het is noodzakelijk ook de systeembestanden, configuratiebeschrijvingen, autorisatieregels en dergelijke te kopiëren. Bij het herstellen van bestanden dienen deze gegevens beschikbaar te zijn.
Het opnieuw laden van bestanden bij reconstructies kan gevolgen hebben voor de geldende autorisatieregels. Het kan nodig zijn bij hersteloperaties eerst de autorisaties voor bestanden te herstellen of aan te passen.

– *mutatielogging*
De meer geavanceerde systemen beschikken over faciliteiten om alle mutaties op bestanden in logbestanden of journalen vast te leggen. Deze faciliteit moet doorgaans afzonderlijk geactiveerd worden en wordt vaak niet gebruikt, omdat het extra opslagcapaciteit kost.

Zijn er geen faciliteiten voor mutatielogging of wordt daarvan geen gebruik gemaakt, dan zal bij het verloren gaan van bestanden een backupkopie geladen moeten worden en zullen alle mutaties na het moment waarop de backupkopie is vervaardigd opnieuw ingevoerd moeten worden. De basisgegevens moeten in dat geval reconstrueerbaar zijn en daartoe bijvoorbeeld op invoerdocumenten vastgelegd worden.
Wordt mutatielogging wel gebruikt dan kan, in geval van een calamiteit, met behulp van backups en journalen de situatie tot vlak voor de calamiteit gereconstrueerd worden.
Het gebruik van mutatielogging stelt eisen aan de applicatie-programmatuur. Wanneer met één transactie meerdere mutaties in bestanden worden aangebracht, is het belangrijk dat deze mutaties gelijktijdig worden verwerkt ('commitment control'). Is dat niet het geval dan kunnen bij reconstructie inconsistente bestanden het gevolg zijn.
Bij gebruik van mutatielogging kan het aantal backups worden teruggebracht. Dagelijks kunnen bijvoorbeeld alleen de mutaties worden gekopieerd en wekelijks de complete bestanden.

– *uitwijkregelingen*
Door een toenemend gebruik van geïntegreerde systemen worden ook kleinere organisaties steeds meer afhankelijk van de beschikbaarheid van hun computersystemen. In de meeste gevallen bestaan er geen formele uitwijkregelingen voor het geval de computer geheel verloren gaat of gedurende langere tijd niet meer beschikbaar is. Het is noodzakelijk aan de hand van een risicoanalyse vast te stellen welke schade de organisatie leidt bij uitval van het systeem gedurende langere tijd. Blijkt eventuele uitval tot grote schade te leiden, dan zullen maatregelen genomen moeten worden om uitwijk naar een andere computer te regelen. Vaak zijn er mogelijkheden uitwijkregelingen met collega-bedrijven of leveranciers te treffen. Schriftelijke afspraken daarover verdienen de voorkeur. De te ondernemen acties in geval van uitwijk zullen in een draaiboek beschreven moeten worden en er zal regelmatig met een sloepenrol getest moeten worden of de uitwijk daadwerkelijk te realiseren is.

Controle op de werking

Toetsingswerkzaamheden
Om een oordeel te verkrijgen over het niveau van beveiliging in en rond de computer zal gesproken moeten worden met de systeembeheerder(s), programmeurs en operators (indien aanwezig) en enkele eindgebruikers. Daarnaast zullen functie- en taakbeschrijvingen, procedurebeschrijvingen, en andere instructies doorgenomen moeten worden. De ervaring leert echter dat in kleinere organisaties weinig van deze zaken op schrift staan. Wel beschikt de accountant vaak over een beschrijving van de administratieve organisatie.
Een belangrijk onderdeel van de audit is het beoordelen van de kwaliteit van het systeembeheer. De systeembeheerder heeft voor een belangrijk deel dezelfde belangen als de accountant en kan door de accountant ondersteund worden in zijn beherende functie. Is de systeembeheerder voldoende op de hoogte van de beveiligingsaspecten van het besturingssysteem en is in de organisatie de wil aanwezig om de beveiliging goed te regelen, dan zal het onderzoek minder diepgang behoeven te hebben. Het zal dan meer het karakter krijgen van een toetsing op de uitgevoerde beveiligingsmaatregelen.

Beoordeling functiescheidingen
Om een oordeel te verkrijgen over de gerealiseerde functiescheiding tussen eindgebruikers zullen de gebruikersprofielen of autorisatietabellen worden opgevraagd. Blijkt daaruit dat de gebruikers inderdaad beperkt zijn tot het uitvoeren van applicaties, dan kan door het rubriceren van menu's en programma's naar (groepen van) eindgebruikers een goed inzicht verkregen worden in de toegekende mogelijkheden transacties uit te voeren.
Belangrijk is het beoordelen van de mogelijkheden die aan programmeurs zijn toegekend. Vaak wordt aan programmeurs geen enkele beperking opgelegd. Dat is onaanvaardbaar en zal moeten leiden tot een advisering aan het management daar verbetering in aan te brengen. Programmeurs mogen niet in staat zijn produktiebibliotheken of -directories te benaderen. Ook voor 'trouble-shooting', dat wil zeggen het oplossen van

problemen met operationele programma's, moeten goede procedures bestaan.
De betrouwbaarheid van de applicatieprogrammatuur kan vanwege het tijdrovende karakter daarvan slechts marginaal worden beoordeeld. Een code-review van enkele programma's, gecombineerd met een beoordeling van de documentatie en interviews met programmeurs, geeft een indruk van de wijze en het niveau van programmeren.

Toetsingen aan het systeem
Om de beveiliging te toetsen zullen enkele acties op het systeem uitgevoerd moeten worden. Omdat voor de meeste opvragingen uit systeembestanden een hoge autorisatie noodzakelijk is, is aan te bevelen deze opvragingen als auditor niet zelfstandig uit te voeren, maar in samenwerking met de systeembeheerder. Met andere woorden, de systeembeheerder toetst onder toeziend oog van de EDP-auditor de opvraaginstructies in.
Bij het onderzoek aan het systeem zal onder meer aandacht besteed moeten worden aan:
- de wijze waarop het besturingssysteem is geïnstalleerd (parameterinstellingen);
- de activering van beveiligingsmogelijkheden;
- het blokkeren van default-gebruikerscodes;
- de wijze waarop toegang tot bestanden is geregeld (met name bij kritische bestanden);
- het afschermen van produktiebibliotheken of -directories;
- de aanwezigheid van gebruikers met bijzondere privileges;
- de aanwezigheid en autorisatie van programma's die hun autorisatie overdragen;
- informatie uit logbestanden, bijvoorbeeld aanmeldingen op ongebruikelijke tijdstippen;
- informatie uit logbestanden over 'gevoelige' acties, zoals beveiligingsovertredingen;
- gelogde mutaties op kritische bestanden;
- schriftelijke acceptaties voor produktieprogramma's, volgens de laatste wijzigingsdata in programmabibliotheken.

Los van de systeembeoordeling is het zinvol na te gaan welke mogelijkheden er voor de accountant bestaan bij de controle gebruik te maken van opvraagtalen of rapportgeneratoren.

APPENDIX

Controle bij een AS/400

In deze appendix wordt ingegaan op de mogelijkheden die een AS/400 biedt om de beveiliging van het systeem te beoordelen.

installatie
Op het bedieningspaneel is een beveiligingsschakelaar aangebracht. Nagegaan moet worden dat deze schakelaar in de stand 'secure' of 'auto' staat. De sleutel waarmee de schakelaar bediend wordt, moet op een veilige plaats zijn opgeborgen (bijvoorbeeld in een kluis bij de directie).
Wat betreft de wijze van installatie van het systeem zijn de volgende opvragingen zinvol:
- Het beveiligingsniveau kan opgevraagd worden met het commando: DSPSYSVAL QSECURITY. De niveaus 10 en 20 duiden op een onvoldoende gebruik van de beveiligingsmogelijkheden. Het niveau moet 30 zijn!
- Van de – bij aflevering aanwezige – standaard gebruikerscodes (QSYS, QUSRSYS, en dergelijke) moet nagegaan worden of de standaard wachtwoorden gewijzigd zijn.
- DSPOBJD OBJ(QSYS/QHST*) OBJTYPE (*FILE) geeft een overzicht van alle logbestanden op het systeem.
- QHSTLOSIZ toont de maximale omvang van de logbestanden.
- WRKJRNA toont de journalen die in gebruik zijn en de bestanden waarvoor journalering wordt gebruikt. Daarbij gecontroleerd worden of de relevante programma's op een juiste wijze van 'commitment control' gebruik maken.
- Het commando: DST Display Checksum Configuration toont of de checksumbescherming geïmplementeerd is. Checksumbescherming biedt aanvullende faciliteiten voor herstel van bestanden bij calamiteiten (maar legt wel beslag op schijfcapaciteit).

autorisaties
Om de operationele autorisaties in beeld te brengen zijn de volgende commando's beschikbaar:
- DSPAUTUSR toont per gebruikersprofiel de

datum van laatste wijziging van het wachtwoord, het van toepassing zijn van een groepsprofiel e.d.
- Met DSPUSRPRF USRPRF (gebruikerscode) TYPE (*ALL) kan een compleet gebruikersprofiel worden opgevraagd; bijzondere aandacht moet gegeven worden aan hoge autorisaties als *ALLOBJ en *SERVICE en gebruikerscategorieën als *SECOFR, *SEDCAM e.d., die per definitie hoge autorisaties op het systeem hebben; ook moet gelet worden op de verplichte startmenu's en de parameter 'begrenzing toegangsmogelijkheid', waarmee systeemcommando's afgegrendeld kunnen worden.
- DSPOBJAUT OBJ(object) toont de autorisatieregels per object.
- Met DSPAUTL AUTL(naam) kan een autorisatielijst (lijst van autorisaties per object) worden opgevraagd.
- DSPPGMADP toont de programma's die hun autorisatie tijdelijk overdragen (adopted authority); daarbij moet gelet worden op bijzondere autorisaties.

Per gebruikersprofiel moet nagegaan worden welke programma's in de startmenu's en volgmenu's zijn opgenomen en welke mogelijkheden deze programma's bieden.

produktieprogramma's
- Om een overzicht van produktiebronprogramma's te verkrijgen moet het commando DSPFD gebruikt worden. Getoond worden de programma's met invoerdatum, aantal records en laatste wijzigingsdatum. Aan de hand van deze laatste wijzigingsdatum kan gecheckt worden of de acceptatieprocedures gevolgd zijn.
- De bibliotheek met objectprogramma's kan opgevraagd worden met DISLIB. De daarin voorkomende objecten worden opgevraagd met DSPOBJ.

Voor de produktiebestanden en -programma's moet vastgesteld worden dat zij niet direct door eindgebruikers en in het geheel niet door programmeurs te benaderen zijn.
Let ook op dubbel voorkomende programmanamen, dat zou op 'Trojaanse paarden' kunnen duiden.

logbestanden
De in het systeem bijgehouden log- en mutatiebestanden kunnen gebruikt worden om na te gaan hoe het systeem daadwerkelijk wordt gebruikt. De AS/400 heeft uitgebreide faciliteiten om het systeemgebruik in controleerbare vorm vast te leggen.
Het historiebestand houdt alle systeemboodschappen vast. Ook ongeautoriseerde toegangspogingen worden daarin geregistreerd. De systeembeheerder ('security-officer') heeft de bevoegdheid het historiebestand te verwijderen. Nagegaan moet worden dat het verwijderen pas plaats vindt nadat het log afgedrukt, geanalyseerd en gearchiveerd is.
Uit een aanwezig logbestand kunnen allerlei selecties gemaakt worden. Voorbeelden daarvan zijn:
- DSPLOG LOG (QHST) PERIOD (2000 031090)) (2400 031090). Deze opvraging geeft een overzicht van alle systeemboodschappen tussen 8 en 12 uur 's avonds op 10 maart 1990;
- DSPLOG LOG (QHST) PERIOD (0800 031090) (2400 031090)) MSGID (CPF2200) geeft alle systeemboodschappen met code CPF2201 tot CPF2299. De meeste 'security-messages' liggen in deze range.

De journalen waarin mutaties op bestanden worden vastgelegd kunnen eventueel gebruikt worden om transacties op kritische bestanden te analyseren. Mutaties op een bepaald bestand kunnen als volgt worden opgevraagd:
- DSPJRN JRN(bibliotheek/journaal) FILE(bibliotheek/bestand)

Wanneer gebruik gemaakt wordt van jobaccounting kan het jobaccounting journal (QACGJRN) gebruikt worden om na te gaan welke gebruikers op het systeem actief zijn en welke bestanden zij benaderen.

Gebruik opvraagtalen

De AS/400 beschikt over een relationele data-

base. Wanneer een accountant besluit om zelf bestandsonderzoeken uit te voeren, zou de database uitgelezen kunnen worden en (na een filetransfer) ingelezen kunnen worden in de computer van de accountant. In veel gevallen zal er echter de voorkeur aan gegeven worden de bestanden op het systeem zelf te onderzoeken. Op de AS/400 zijn daarvoor (optioneel) de volgende opvraagtalen beschikbaar:
- Query/400,
- SQL/400,
- Data File Utility.

De meeste opvragingen zijn hiermee te realiseren. Wanneer de accountant(sassistent) zelf de opvragingen op het systeem definieert, heeft hij of zij de autorisatie nodig om de betreffende bibliotheken of bestanden te kunnen benaderen. Het is noodzakelijk dat daarbij alleen opvraagautorisatie (*USE) wordt verleend.

Literatuur

Beveiliging algemeen:
W. Hartman e.a., *Bevordering Betrouwbaarheid Informatiesystemen*, 2e druk, Kluwer, 1988.
AICPA, *Audit and Control Considerations in a Minicomputer or Small Business Computer Environment*, 1981.

Beveiliging AS/400:
W. F. de Koning en J. H. Matto, *Beveiliging en controle in een AS/400 omgeving*, P&H-Groep, 1989.
W. H. Murray, *Security Audit and Control Considerations of AS/400*, EDPACS p. 7 ev., november 1988.

Beveiliging UNIX:
X/Open Security Guide, Prentice Hall, 1989.
S. A. Kakilow en G. A. Wilson, *Unix Security*, EDPACS p. 1 ev., december 1989.

Beveiliging (Micro) VAX:
G. J. C. Heikamp, *Beveiligingsaspecten van VAX/VMS*, Compact p. 47 ev., 1990/1.

Determinanten van de vermogensstructuur

Drs. Kees Cools

'How do firms choose their capital structures? We don't know.'

Stewart Myers (1984)

1 Inleiding [1]

Hoe bepalen ondernemingen hun financiële structuur? Sinds Franco Modigliani en Merton Miller in 1958 hierover hun beroemde arikel publiceerden is dit een centrale vraag in het vak ondernemingsfinanciering.[2] Niettemin gaf Stewart Myers 26 jaar later als antwoord op de gestelde vraag: 'We don't know.' Dit wellicht teleurstellende antwoord kan ten dele worden verklaard uit de aard van de bedrijfseconomie als een tak van de sociale wetenschappen. Menselijke gedragingen zijn immers soms onvoorspelbaar. Bovendien is elke onderneming in zijn soort tot op zekere hoogte uniek. Daarom mag men ook niet verwachten gemakkelijk universele wetmatigheden ter verklaring van de (optimale) vermogensstructuur te kunnen vinden. Toch is de financieringstheorie in staat gebleken enkele factoren aan te geven, die mede bepalend zijn voor de financiële structuur van een onderneming.
Als eerste in een reeks van drie geeft dit artikel een kort overzicht van drie decennia vermogensstructuurtheorie. In een volgende bijdrage zal de financiering van Nederlandse beursondernemingen worden geanalyseerd voor de periode 1977-1988. Daarmee krijgen we een indruk van de

Drs. C. Cools studeerde economie, filosofie en accountancy en is verbonden aan de vakgroep bedrijfseconomie, sectie financiering van de Katholieke Universiteit Brabant.