KPMG Klynveld EDP Audit Services

87/3
herfst 1987

COMPACT

Uit de inhoud

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

INHOUDSOPGAVE

Nummer 45 **Herfst 1987**
ISSN 0920-1645

COMPACT

Herfst 1987

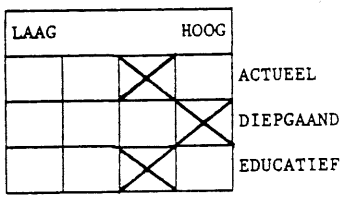
VAN DE REDACTIE

De gecompliceerdheid van betalingsorganisaties in het huidige tijdsgewricht dwingt ons ertoe slechts langzaam door te dringen in de problematiek en de daarvoor te kiezen oplossingen uit hoofde van automatisering en controle. Reden waarom dit nummer niet over betalingsorganisaties in hun moderne vorm handelt. Maar ... "Wat in het vat zit verzuurt niet!" Waarvan akte.

Toch bevat dit nieuwe nummer veel onderwerpen die met de omgevingsvoorwaarden te maken hebben die vervuld moeten zijn wil een hechte betalingsorganisatie überhaupt kunnen bestaan.

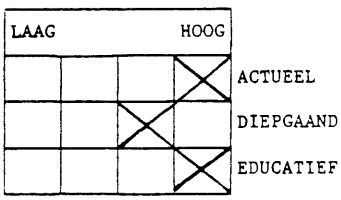
Wij behandelen achtereenvolgens.

Escrow-depot voor computersoftware in Nederland
door Mr. V.A. de Pous



Victor de Pous is free lance journalist tevens meester in de Rechten.
Hij schrijft onder eigen verantwoordelijkheid, die we ook niet kunnen overnemen. Victor de Pous houdt zich bezig met juridische aspecten van de informatietechnologie. Het artikel is geheel voor verantwoordelijkheid van de auteur.
Het onderwerp is belangrijk genoeg om aandacht aan te besteden. Lezing is van harte aanbevolen.

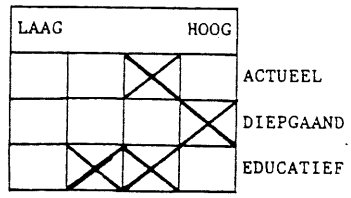
Beveiligen tegen computermisbruik
door A.W. Neisingh en drs. J. Vossen



Tot voor enige tijd konden facturen en vrachtbrieven nog handmatig worden geschreven. Inmiddels is de tijd aangebroken dat deze administratieve handelingen, mede ten gevolge van een toegenomen bedrijfsomvang, niet meer handmatig mogelijk zijn. Het toenemende gebruik van de automatisering en de voortschrijdende technische mogelijkheden ervan zoals integratie en distributie van apparatuur, programmatuur en gegevensverzamelingen maken de organisatie kwetsbaar. Deze kwetsbaarheid noodzaakt de organisatie tot het nemen van maatregelen om de geautomatiseerde gegevensverwerking te beheersen.

In dit artikel zal in het bijzonder worden stilgestaan bij opzettelijke fouten. Dat wil zeggen, die handelingen waarbij kan worden gesproken van computercriminaliteit. Aangegeven wordt op welke wijze een organisatie zich kan beveiligen tegen de bedreigingen van computermisbruik.

Geïntegreerde gegevensverwerking:
structuur van controle- en beveiligingsmaatregelen
in een ADR/DATACOM DB-DC-omgeving
door J.A.W. Winterink en drs. R.G.A. Fijneman

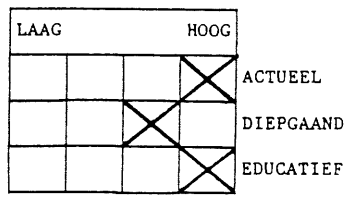


In het in Compact 87/1 verschenen artikel "Geïntegreerde gegevensverwerking" behandelt collega Kocks vanuit een basisconcept de ontwikkelingen en invloeden als gevolg van toenemende geavanceerdheid van de automatisering behandeld, alsmede gevolgen ervan voor de interne controle.

Met het basisconcept als uitgangspunt wordt in dit artikel ingegaan op de structuur van controle- en beveiligingsmaatregelen die voor de beheersbaarheid van de gegevensverwerking in een ADR/datacom DB-DC omgeving zijn vereist.

Een beschrijving van de ADR-progammatuur, alsmede de (noodzakelijke) samenhang ertussen, vormt de grondslag voor de beschrijving van met behulp van deze produkten te realiseren interne controlemaatregelen. Aansluitend daarop wordt vervolgens geëvalueerd wat hiervan de betekenis is op de controle- en beveiligingsmaatregelen met betrekking tot respectievelijk de gebruikersorganisatie, de automatiseringsorganisatie en de organisatie van de automatisering.

Belangrijke functies van een toegangs-
beveiligingspakket
door M.C. Duym



In dit artikel worden de functionele eisen behandeld die aan een toegangsbeveiligingspakket gesteld moeten worden. Na een opsomming en korte toelichting van de eisen wordt eerst ingegaan op de registraties (bestanden) die zo'n pakket voor haar functioneren nodig heeft. De beschrijving van de inhoud van een aantal van deze bestanden dient namelijk als basis voor een verdere uitdieping van het functionele eisenpakket.

Verder slechts enige van de gebruikelijke rubrieken, waaronder Actualiteiten over het seminar EDP-auditing volwassen en de conclusie van de NIvRA-commissie CAV in verband met de opleiding EDP auditors.

COMPACT

Herfst 1987

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

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

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

ISSN 0920-1645

Indien u belangstelling heeft voor meerdere exemplaren kunt u deze aanvragen bij de secretaris van de redactie, evenwel zolang de voorraad strekt (telefoon 020 - 5461912).

ACTUALITEITEN

EDP-auditing volwassen [1]

Op 31 december 1987 zal de heer J.H. Urbanus uittreden uit de maatschap KPMG Klynveld EDP Audit Services. Dan zal één van de grondleggers van het EDP audit beroep in Nederland terugtreden uit de actieve beroepsuitoefening. Sinds de jaren zeventig heeft hij zich op velerlei fronten ingezet voor de ontwikkeling van de EDP audit in brede zin zowel als aparte discipline. Gememoreerd kunnen worden zijn werkzaamheden in dezen bij het NGI (mede-oprichter van de sectie Beveiliging waaruit de sectie EDP Audit is voortgekomen) en het NIvRA. Een dergelijke voorvechter voor de EDP audit laat men niet zomaar afscheid nemen. Daarom zal op 9 december 1987 middels een conferentie – georganiseerd door het NGI in samenwerking met KPMG EDP Audit Services – op waardige wijze afscheid genomen worden van J.H. Urbanus. Hij zal samen met zijn zes collega-vennoten van KPMG Klynveld EDP Audit Services een overzicht geven van de huidige stand van zaken met betrekking tot de EDP audit in Nederland. Meer gedetailleerde informatie inzake de presentaties vindt u elders in deze brochure.

DOELGROEP

Deze conferentie is bestemd voor:
- functionarissen werkzaam – van beleid tot uitvoering – op het gebied van de automatisering c.q. beveiliging met betrekking tot automatisering
- (aankomend) EDP auditors
- functionarissen werkzaam op een afdeling interne controle c.q. interne accountantsafdeling
- registeraccountants werkzaam als intern of openbaar accountant

09.00 - 09.15 uur
Ontvangst deelnemers, koffie

09.15 - 09.30 uur
Opening door de dagvoorzitter
J. Hekkelman

09.30 - 10.10 uur
EDP audit
door: J.H. Urbanus

Een aantal jaren geleden is in het Handboek Accountancy een artikel verschenen dat is geschreven door Han Urbanus en Joop Verheul. Sinds die tijd heeft het EDP audit beroep een zodanige ontwikkeling doorgemaakt dat aanpassing van het artikel noodzakelijk bleek. Tijdens de presentatie zal een schets van die ontwikkelingen worden gegeven met een blik gericht op de toekomst waardoor de deelnemer met een goed beeld van de "state of the art" huiswaarts zal keren.

10.10 - 10.50 uur
Effectiviteit en efficiency van de automatisering als object van de EDP audit
door: H.B. Moonen

Het beoordelen van effectiviteit en efficiency van de informatievoorziening is binnen de EDP audit een betrekkelijk onderontwikkeld gebied. In de praktijk heeft de EDP audit zich voornamelijk gericht op betrouwbaarheidsonderzoeken. Betrouwbaarheid is echter slechts één van de kwaliteitsaspecten van de geautomatiseerde informatievoorziening. In dat kader is het van belang dat speciale aandacht geschonken wordt aan de onderzoeks- en vastleggingstechnieken, de normen voor toetsing en andere hulpmiddelen voor de beoordeling (audit) van de doeltreffendheid en doelmatigheid van de informatievoorziening.

10.50 - 11.10 uur
Pauze

11.10 - 11.50 uur
Mededelingen over de uitkomsten van EDP audit; grondslag, strekking en vorm
door: H. Roos

Strekking en vorm van mededelingen over de uitkomsten van EDP audits worden bepaald door de daaraan ten grondslag liggende werkzaamheden en door de verwachtingen van de lezer van de mededeling. Anders dan meestal geldt voor "verklaringen" bij financiële verantwoordingen zijn deze mededelingen steeds bestemd voor een beperkte kring van belanghebbenden. Een uitzondering daarop vormen wellicht "certificaten" bij standaard software. De correcte interpretatie van een mededeling vereist bekendheid met de materie. Zelfs in kleine kring zal de aanwezigheid van materiekennis nogal variëren. Dit stelt specifieke eisen aan de vorm en de inhoud van een mededeling. Op basis van de ervaring met de hierover in NIvRA 26 gegeven richtlijnen wordt een aanzet gegeven tot een mogelijke verduidelijking naar vorm en inhoud van EDP audit mededelingen.

11.50 - 12.30 uur
Software certificering
door: A.W. Neisingh

Keuring en certificering van informatietechnologie-produkten betreffen een element van EDP audit dat recent hieraan is toegevoegd. Na een schets van de ontwikkelingen, voorlopig eindigend met de oprichting van het Instituut voor Certificatie van Informatietechnologie (ICIT), zal worden ingegaan op de begrippen keuren en certificeren zelf. Keuringen kunnen slechts worden uitgevoerd door erkende keuringslaboratoria, die gebruik maken van normen. Tevens zal op de rol van de EDP auditor in het verrichten van keuringen worden ingegaan.

12.30 - 13.30
Lunch

[1] NGI/SIC, Proceedings EDP-auditing volwassen
ISBN: 90-5005-017-4

13.30 - 14.10 uur
Beveiliging in organisatorisch perspectief
door: Drs. H. C. Kocks

Automatisering en beveiliging lijken onlosmakelijk met elkaar verbonden. Zolang de EDP audit bestaat heeft ze zich intensief bezig gehouden met de beveiligingsaspecten die de automatisering betreffen. De fysieke aspecten hebben lange tijd overheersende aandacht gekregen. Echter, steeds meer komt de nadruk te liggen op logische (dat wil zeggen software-matige) beveiliging van de geautomatiseerde gegevensverwerking. Dit alles dient in al haar complexiteit beheersbaar te blijven. Er zal worden ingegaan op de organisatorische beheersbaarheid van die beveiligingsproblematiek. Managementverantwoordelijkheid, security functie, risico-analyse, alsmede de rol van EDP audit zijn de voornaamste ingrediënten van de presentatie.

14.10 - 14.50 uur
EDP audit en onderwijs
door: Prof. D. Steeman

De belangstelling voor betrouwbaarheid en beveiliging neemt terecht nog steeds toe. Accountants zijn van oudsher in dit vakgebied werkzaam. Anders dan wat de certificering van financiële verantwoordingen betreft, hebben zij op het terrein van EDP audit niet het monopolie.
De opleiding met betrekking tot EDP audit wordt echter nog steeds gedomineerd door accountants met een 'automatiseringstik'. Het huidige opleidingsgamma vertoont dan ook een gevarieerd beeld.
Er zal onder andere worden ingegaan op de bijdrage die door automatiseringsdeskundigen geleverd zou kunnen worden. Daarnaast worden mogelijkheden aan de orde gesteld die een bredere scope van de opleiding tot standbrengen.

14.50 - 15.10 uur
Pauze

15.10 - 15.50 uur
De (on)mogelijkheden van het gebruik van de automatisering als "tool" in de controlepraktijk
door: A. M. le M. Leach

Sinds de opkomst van de micro-computer zijn de mogelijkheden, om de automatisering als hulpmiddel bij de planning en uitvoering van accountantswerkzaamheden te gebruiken, sterk toegenomen. Wat de stand van zaken nu is en wat de nabije toekomst (negentiger jaren) zal brengen, is het thema van de presentatie.

15.50 - 16.00 uur
Recapitulatie en sluiting
J. Hekkelman

Mr. J. Hekkelman

Jaap Hekkelman is directeur van de N.V. Bank voor Nederlandse Gemeenten. Hij is belast met de leiding over het gehele terrein van de dienstverlening aan gemeenten, andere publiekrechtelijke lichamen, overheidsondernemingen en instellingen die werken met enige overheidsgarantie. Deze dienstverlening omvat zowel het betalingsverkeer als de verschillende vormen van kredietverlening.
Hij was sedert de oprichting in 1979 tot 1986 lid en voorzitter van de sectie Beveiliging van het NGI en voorzitter van de werkgroep binnen de sectie die zich bezig houdt met de privacy wetgeving. Sinds najaar 1985 is hij lid van het bestuur van het NGI.

Drs. H. C. Kocks RA

Cor Kocks is lid van de maatschap KPMG Klynveld EDP Audit Services. Naast het leiding geven met betrekking tot EDP audit werkzaamheden bij een groot scala cliënten – variërend van klein tot (zeer) groot in diverse branches – is hij binnen KPMG Klynveld EDP Audit Services verantwoordelijk voor vaktechniek en opleiding. Daarnaast is hij verbonden aan de Erasmus Universiteit te Rotterdam waar hij doceert in de beheers- en audit aspecten van automatisering in relatie tot de beroepsuitoefening van de, zowel intern als openbaar, accountant.

A. M. le M. Leach CA

Tony Leach is lid van de maatschap KPMG Klynveld EDP Audit Services sinds 1987. Hiervoor werkte hij bij Peat Marwick in Amerika, België, Duitsland en Nederland. Als partner was hij belast met EDP support voor de Continental European Firm. Hij heeft brede ervaring met betrekking tot het gebruik van microcomputers in de controlepraktijk en het gebruik van micro-mainframe verbindingen. Binnen KPMG Klynveld EDP Audit Services is hij verantwoordelijk voor Support & Programming. Tevens is hij Regional Coördinator voor EDP Support binnen de KPMG Continental Europe Regional Organisation.

J. B. Moonen RA

Hans Moonen is lid van de maatschap KPMG Klynveld EDP Audit Services sinds 1983. Daarvoor was hij werkzaam als EDP audit partner bij de interne accountantsdienst van N.V. Philips. Hij is verbonden aan de Katholieke Universiteit Brabant te Tilburg waar hij doceert in het vak EDP audit. Tevens is hij bestuurslid van de EDP Auditors Association chapter Benelux.

A. W. Neisingh RA

Dries Neisingh is lid van de maatschap KPMG Klynveld EDP Audit Services. Sedert 1971 is hij werkzaam op het terrein van de automatisering en controle. Hij heeft een brede ervaring en diepgaande kennis op het gebied van (interne) controle, beveiliging, accountantscontrole met betrekking tot geautomatiseerde gegevensverwerking. Als openbaar accountant is hij in zijn specialistische rol betrokken bij de problematiek van EDP audit van vele ondernemingen waaronder een van de grote Nederlandse banken. Hij is lid van het NGI-bestuur.

H. Roos RA

Herman Roos is lid van de maatschap KPMG Klynveld EDP Audit Services. Momenteel is hij binnen KPMG Klynveld EDP Audit Services verantwoordelijk voor Research & Development van automatiserings- en controlepraktijkhulpmiddelen voor KPMG Klynveld Kraayenhof & Co. en KPMG Klynveld EDP Audit Services. Daarnaast is hij verantwoordelijk voor de coördinatie van EDP audit werkzaamheden met een verscheidenheid aan controle cliënten en is hij belast met speciale EDP audit werkzaamheden bij o.a. verzekeringsmaatschappijen, elektronica bedrijven, handelsmaatschappijen en Electronic Funds Transfer systems. Herman Roos is voorzitter van de internationale KPMG Computer Audit Advisory Committee.

Prof. D. Steeman RA

Dick Steeman is lid van de maatschap KPMG Klynveld EDP Audit Services.
Na te hebben gewerkt in de controle- en organisatie-adviespraktijk, is hij sinds de zeventiger jaren werkzaam op het terrein van de EDP audit. Sinds 1976 is hij als buitengewoon hoogleraar verbonden aan de Erasmus Universiteit te Rotterdam.

A. H. Urbanus RA

Hij is sedert 1950 werkzaam bij Klynveld Kraayenhof & Co., en heeft na accountantscontrole werkzaamheden, zich gespecialiseerd in organisatie advieswerk, met als aandachtsvelden administratieve organisatie en automatisering. Hij is sedert 1969 lid van de maatschap en sinds 1973 werkzaam bij KPMG Klynveld EDP Audit Services en bestuurslid van het ICIT.

Opleiding EDP auditor

De opleiding tot EDP-auditor heeft in de afgelopen tijd in de belangstelling gestaan. Het onderwerp is voorwerp van overleg geweest tussen het NIVRA en het Nederlands Genootschap van Informatica. Aan enkele instellingen van hoger onderwijs zijn voorts specifieke EDP-audit-opleidingen van start gegaan. Het is tenslotte duidelijk dat ook andere disciplines dan die van accountants gebruik maken van de aanduiding "EDP-auditor".

Het bestuur acht het gewenst een bijdrage te leveren aan een zo duidelijk mogelijke positiebepaling nopens de EDP-audit. Tot dit doel heeft de CAV een notitie opgesteld, die hierbij wordt gepubliceerd.
De CAV heeft zich beraden op hetgeen onder EDP-audit zou moeten worden verstaan; welke functionele eisen op dat gebied aan de accountant in de algemene functie moeten worden gesteld; welke specialisaties binnen het (brede) begrip EDP-audit kunnen worden onderscheiden. Het resultaat treft de lezer hieronder aan.

A. Wat wordt verstaan onder EDP-audit

Als uitgangspunt is de volgende definitie gekozen: EDP-auditing is het door een onpartijdig deskundige kritisch beoordelen van en adviseren over de kwaliteit van de organisatie van de automatisering, de automatiseringsorganisaties en te automatiseren c.q. geautomatiseerde informatiesystemen.

Het begrip kwaliteit omvat dan de volgende aspecten:

1. *Betrouwbaarheid*
(Engels: integrity) De mate van volledigheid, juistheid, tijdigheid en geoorloofdheid van de gegevens, de gegevensverwerking en de informatie.

2. *Doeltreffendheid (effectiviteit)*
De mate waarin wordt voldaan aan de eisen van de gebruikers, mede omvattend de mate van correctheid waarmee systeemspecificaties zijn nageleefd.

3. *Continuïteit*
De mate van zekerheid van ongestoorde voortgang, onder meer af te meten aan levensduur en onderhoudbaarheid van de gegevensverwerking.

4. *Doelmatigheid (efficiency)*
De mate waarin een snelle en economisch verantwoorde gegevensverwerking wordt gerealiseerd.

5. *Beveiliging en bescherming*
(Engels: security) De mate van preventie tegen en signalering van ongewenste ingrepen en calamiteiten en de voorzieningen tot herstel. Dit aspect omvat mede de privacybescherming en hetgeen met robuustheid (weerbaarheid) wordt aangeduid.

Zowel de aspecten afzonderlijk als de totaliteit kunnen als beoordelingscriteria voor een onderzoek worden gedefinieerd.

B. Functionele eisen voor de accountant in de algemene functie

De huidige RA moet in staat zijn om:

in zijn controlefunctie

1. de gevolgen van de automatisering voor de aanpak c.q. uitvoering van de (jaarrekening)controle te overzien;
2. al dan niet bijgestaan door gespecialiseerde collega's of assistenten, de betrouwbaarheid van de geautomatiseerde gegevensverwerking te beoordelen en te toetsen (verifiëren) ten behoeve van de concipiëring van het programma van controlewerkzaamheden ter vaststelling van de getrouwheid van de verantwoording;
   Onder concipiëring te verstaan: samenstelling van het controleplan door afweging van effectiviteit en doelmatigheid van de diverse controlemiddelen en technieken.
3. bij de inschakeling van EDP-auditors de regie en daarmede de eindverantwoordelijkheid van de opdracht te behouden;
4. automatiseringstechnische controlebevindingen te vertalen in gevolgen voor de controle en (eventueel) aanbevelingen voor het management;
5. minimaal op functioneel niveau de keuze en toepassing van computerondersteunende controlemiddelen (waaronder auditsoftware) te (doen) realiseren.

in zijn adviesfunctie

6. op beleidsniveau te adviseren over het interne controlebeleid als onderdeel van het informatie- en automatiseringsbeleid;
7. automatiseringsprojecten met betrekking tot de betrouwbaarheids-, en continuïteitsaspecten te begeleiden;
8. met betrekking tot de toepassing van interne controletechnieken in geautomatiseerde informatiesystemen te adviseren,
9. de doeltreffendheid van informatie uit geautomatiseerde toepassingen voor de gebruiker te beoordelen.

C. Welke gespecialiseerde EDP-auditors zijn te onderkennen?

Naar de mening van de CAV is het nodig de overall functie EDP-auditor te splitsen in de volgende deelfuncties (specialisaties):

- EDP-auditor/Organisatiespecialist
- EDP-auditor/Hardwarespecialist
- EDP-auditor/Softwarespecialist.

Van deze specialisaties volgt een globale functiebeschrijving.

1. *EDP-auditor/organisatiespecialist (al dan niet RA)*
Beoordelen van en adviseren over de kwaliteit respectievelijk een of meer kwaliteitsaspecten van:
1.1. de organisatie van de automatisering
1.2. de automatiseringsorganisatie (ontwikkelingsorganisatie en organisatie van de gegevensverwerking)
1.3. te automatiseren c.q. geautomatiseerde informatiesystemen.

2. EDP-auditor/hardwarespecialist (al dan niet RA)
Beoordelen van en adviseren over de kwaliteit, respectievelijk een of meer kwaliteitsaspecten van:
2.1. hardwarebeleid
2.2. selectie van hardware
2.3. hardware-architecturen
2.4. ingebouwde interne controles.

3. EDP-auditor/softwarespecialist (al dan niet RA)
Beoordelen van en adviseren over de kwaliteit respectievelijk een of meer kwaliteitsaspecten van:
3.1. softwarebeleid (als onderdeel van het automatiseringsbeleid)
3.2. selectie van software
3.3. besturingssystemen inclusief alle hulpprogrammatuur zoals compilers etc.
3.4. database managementsystemen
3.5. toegangsbeveiligingssystemen
3.6. datacommunicatiesystemen
3.7. toepassingsgerichte programmatuur. ■

Uit: de Accountant nr. 2/oktober 1987, pag. 97

Herfst 1987

Bespreking van de kpmg-brochure "de wet persoonsregistraties"

door A. Klaver

Het doel van deze brochure is cliënten te wijzen op de komende Privacy-wet en de gevolgen daarvan voor het Nederlandse bedrijfsleven en overheid.

Privacy wordt in deze brochure omschreven als het recht van individuen zelf te bepalen welke informatie over hen wordt doorgegeven aan anderen. Deze zaak is in de belangstelling omdat door de voortschrijdende automatisering het steeds eenvoudiger wordt gegevens te selecteren en met elkaar in verband te brengen (computer matching).

In de op handen zijnde wet staat de zelfregulering voorop. Daarnaast geeft de wet een raamwet voor zaken die per algemene maatregel van bestuur geregeld dienen te worden. Doel van de wet is het beschermen van de privacy van het individu.

De wet is van toepassing op geautomatiseerde en handmatige personeelsregistraties. Voor de laatste categorie moet dan wel gelden dat zij systematisch toegankelijk zijn. Bepaalde persoonsregistraties vallen buiten de werkingssfeer van de wet. Hierbij kan bijvoorbeeld gedacht worden aan politiedossiers.

Naast de wet persoonsregistraties kent ons land nog andere privacy-regelingen. Ook internationaal zijn er regels. Dit maakt de zaken complex voor geregistreerden die hun recht zoeken.

De wet normeert het opzetten en gebruik van een registratie van persoonsgegevens. Deze normering valt in drie deelgebieden uiteen.

Ten eerste is er sprake van eisen ten aanzien van de aanleg van een persoonsregistratie. De wet stelt dat deze voor een bepaald doel moet plaatsvinden waarvoor het belang redelijkerwijs aanleiding geeft en waarbij dit doel niet in strijd is met de wet, openbare orde en goede zeden.

Met betrekking tot de inhoud wordt voorgeschreven dat de gegevens rechtmatig moeten zijn verkregen en dat de gegevens in overeenstemming moeten zijn met het doel waarvoor de registratie werd aangelegd.

Gebruik dient beperkt te blijven tot doeleinden die verenigbaar zijn met het doel waarvoor de registratie is aangelegd. Verstrekking van gegevens aan derden mag alleen plaatsvinden zonder toestemming van de geregistreerde voor zover dit voortvloeit uit het doel van de registratie of wettelijk voorschrift.

De wet maakt een onderscheid tussen verschillende typen registraties. Zij onderscheidt gegevens bij overheid, gegevens bij bedrijfsleven en gegevens met een bijzondere gevoeligheid (zoals gegevens over iemands politieke voorkeur of omtrent iemands gezondheid).
De regelgeving verschilt per type registratie.

De overheid en instanties die specifiek gevoelige gegevens registreren zijn reglementsplichtig. Dat wil zeggen dat de belangrijkste kenmerken van de desbetreffende persoonsregistratie openbaar gemaakt moeten worden. Reglementsplichtige houders van registraties mogen op basis van wettelijke voorschriften persoonsgegevens afstaan. De regelgeving ten aanzien van gevoelige gegevens moet nog invulling vinden in een te nemen algemene maatregel van bestuur.

Voor de houders van persoonsregistraties in het bedrijfsleven geldt eveneens een meldingsplicht. Deze vindt zijn weerslag niet in een openbaar te maken reglement, maar in een "privacy-formulier". Dit privacy-formulier dient aan de Registratiekamer gezonden te worden.

In inhoud is er weinig verschil tussen een reglement en een privacy-formulier. In beide dient onder andere opgenomen te worden welke gegevens in de desbetreffende registraties opgenomen zijn en aan wie deze gegevens worden verstrekt.

Alle houders hebben een beveiligingsplicht ten aanzien van de registraties. Er dienen voldoende maatregelen getroffen te worden ter beveiliging tegen verlies, aantasting en onbevoegde kennisneming van gegevens.

Daarnaast hebben alle houders plichten die voortvloeien uit de rechten van de geregistreerden. Een geregistreerde heeft er recht op kennis te nemen van zijn eigen persoonsgegevens, deze te laten verbeteren of verwijderen, recht op informatie over de herkomst van de gegevens en recht op mededeling inzake de verstrekking aan derden.

Een houder die zijn verplichtingen niet nakomt, is aansprakelijk voor de hieruit voortvloeiende schade.

De brochure gaat ook in op de rol van de Registratiekamer. Deze instantie gaat zich bezighouden met advisering, controle, klachtenbehandeling en bemiddeling ten aanzien van de wet. Hiertoe heeft de Registratiekamer inzagebevoegdheid en verregaande onderzoeksbevoegdheden zoals het onderzoeken van apparatuur en programmatuur.

Sancties op het niet naleven van de wet kunnen voortvloeien uit het privaatrecht of het strafrecht. Op grond van het privaatrecht kan een betrokkene of een belangenorganisatie naar de rechter stappen. Ook kunnen zij de Registratiekamer verzoeken een onderzoek in te stellen.

Herfst 1987

Op grond van het strafrecht kan het niet nakomen van de privacy-wet in een privacy-delict resulteren. Voorbeelden van zo'n delict zijn het niet vastleggen van een reglement of formulier en het verstrekken van gegevens aan bepaalde buitenlandse instellingen.

Complicerend bij een eventuele rechtsgang is het feit dat de rechtzoekende met zoveel regelingen te maken heeft, dat hij door de bomen het bos niet meer ziet. De geregistreerde kan kiezen uit de burgerlijke rechter, de Registratiekamer, de Nationale Ombudsman en de afdeling Rechtsspraak van de Raad van State.

De brochure bespreekt enige specifieke onderwerpen inzake de privacy-wet, waaruit er hier een gekozen is. De brochure gaat in op de beveiliging van computersystemen, organisatie en voorschriften in eigen huis, computermisbruik, internationale aspecten (transborder dataflow) en een lijst van attentiepunten voor de organisatie. Op dit laatste onderwerp wordt hier kort ingegaan.

Indien u belangstelling heeft voor de brochure kan deze telefonisch worden aangevraagd (020-5461723).

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Herfst 1987

ESCROW-DEPOT VOOR COMPUTER-SOFTWARE IN NEDERLAND

door Mr. V.A. de Pous

0. Inleiding

De geautomatiseerde gegevensverwerking creëert een kwetsbare samenleving. Afhankelijkheid van computersystemen is een feit geworden. De moderne ondernemer is afhankelijk geworden van de continuïteit van zijn gegevensverwerkend systeem en hoewel de oorzaken legio zijn, blijft het gevolg pijnlijk gelijk. Als de computer "down" gaat, ligt het bedrijf stil en ontstaat er vrijwel meteen aanzienlijke schade. Dat derhalve integraal aan beveiliging in de meest ruime zin van het woord moet worden gewerkt spreekt voor zich. De praktijk is veelal anders en in dit perspectief is de rechtsbescherming van computer-software zeker onderbelicht.
Over software-bescherming wordt meestal slechts dan gesproken wanneer het gaat om de vraag of octrooirecht dan wel auteursrecht op computerprogramma's van toepassing is. Voor wat betreft dit laatstgenoemde intellectueel eigendomsrecht: het zonder toestemming van de rechthebbende kopiëren en verhandelen - formeel omschreven: verveelvoudigen en openbaar maken - van de software is dan onrechtmatig.
Echter rechtsbescherming door middel van registratie en escrow-depot biedt een ruimere, praktijkgerichte protectie en heeft behalve voor de eigenaar van rechten op de computerprogramma's ook een positieve werking voor andere betrokkenen.
Registratie ligt aan de basis van de escrow-depot, want wat op deze wijze formeel in bewaring wordt gegeven bij een notaris wordt nauwkeurig omschreven en gedocumenteerd. En dat betekent met betrekking tot software onder meer:

- de programmatuur in source of broncode op magnetische media vastgelegd (het computerprogramma in een hogere programmeertaal geschreven, hetgeen noodzakelijk is voor ontwikkeling en onderhoud);
- de listing van het computerprogramma op papier vastgelegd;
- ontwikkel- en onderhoudsdocumentatie.

Echter door gebruik te maken van louter een bewaargevingsovereenkomst zijn partijen er niet. De "escrow" [1]), die zijn basis vindt in het Anglo-Ameri-

[1]) Volgens "The Oxford Companion To Law" (1980): A written instrument evidencing obligations between two or more parties, given to a third party on the condition that he delivers it to the other party, only on the happing of a stated condition, such as payment of a price or the death of a person, which being done it takes effect as a deed. If the condition is not performed it never becomes a deed.

kaanse recht, biedt als type bewaargevingscontract (in casu een driepartijenovereenkomst) naar Nederlands recht naar redelijke waarschijnlijkheid onvoldoende rechtsbescherming voor programmatuur, omdat deze juridische constructie in het geval van zogenoemd derdebeslag rechthebbenden geen toegang tot het gedeponeerde zal geven.

1. Bedreigingen

Indien de broncode van het computerprogramma, om welke reden dan ook, niet meer voor handen is, loopt het automatiseringsproject vast en komt het voortbestaan van de onderneming op het spel te staan. Zo schrok Nederland in de zomer van 1972 wakker toen het hoofd Automatisering van een chemisch bedrijf op Rozenburg alle aanwezige tapes met computerprogramma's en gegevens, dus ook de banden voor back-up-doeleinden gemaakt, verduisterde en deze later zijn werkgever te koop aanbood. Chantage dus. En hoewel de dader werd gepakt, illustreert dit voorval in het bijzonder de kwetsbaarheid van een onderneming door de automatisering van de gegevensverwerking. Een andere bedreiging voor de gebruiker van computersystemen betreft het staken van de onderneming door de software-leverancier, bijvoorbeeld in geval van faillissement. Meestal valt er in faillissementen weinig meer te halen voor de curator, en dat geldt in het bijzonder bij software-leveranciers. De programmatuur in source-code, die onmisbaar is voor onderhoud en aanpassing, is voor hem niet toegankelijk, tenzij hij deze uit de failliete boedel weet te halen.
Toegang tot en gebruik van de sources van het computerprogramma zijn dus van levensbelang voor alle betrokkenen bij de onderneming.

2. Auteursrecht voor software

Hoewel rechtsbescherming van programmatuur als een van de oudste deelgebieden van het computerrecht kan worden aangemerkt, raken software-producent en -gebruiker maar vooral rechtswetenschapper hierover niet uitgesproken. Stapels rapporten, waarvan ook een aanzienlijk aantal van eigen bodem, hebben reeds het licht gezien en vele seminars en congressen besteedden in extenso aandacht aan dit onderwerp. Veelal te rechtvaardigen belangstelling, hoewel men zich moet afvragen tot welke in de praktijk werkbare beschermingsvorm al deze aandacht heeft geleid.

Op juridisch terrein is het geschut reeds lang in stelling gebracht en er is ook al flink mee geschoten.

Hoofddoel: het auteursrecht, zowel in binnen- als in buitenland. Computerprogrammatuur kan, algemeen gesproken, auteursrechtelijk worden beschermd indien het aan de eisen van wet en jurisprudentie voldoet.
Geen opzienbarend feit. Auteurswetten hanteren in beginsel een open sys-

teem. Zo ook in Nederland, waar slechts voorbeelden van "werken" die beschermd kunnen worden in de wet zijn opgenoemd. Ook computerprogramma's vallen volgens rechtsgeleerden en rechters dus onder het Nederlandse auteursrecht, maar dan beginnen de problemen pas. Hier scheiden theorie en praktijk.
Weliswaar gemakkelijk dat dit intellectuele eigendomsrecht van rechtswege - dus automatisch - ontstaat indien aan een idee op enigszins creatieve wijze wordt vormgegeven, echter hoe wordt bij inbreuk, bijvoorbeeld slaafse nabootsing of plagiaat, de zaak voor de rechter hard gemaakt?
De centrale vraag in dit kader luidt: voldoet software-bescherming op grond van deze vorm van geestelijk eigendomsrecht aan de (rechts)beschermingsbehoefte in de automatiseringspraktijk? Een praktijk die op dit moment om een aantal praktijkgerichte oplossingen van juridische problemen vraagt, zowel in de verhouding tussen computerleveranciers onderling als in de verhouding leverancier - gebruiker.
Het laat zich raden dat registratie en escrow-depot in dit kader goede diensten bewijzen.

3. Registratie en escrow-depot van software

3.0 Algemeen

Centraal in de procedure van registratie en escrow-depot van software staat het verschaffen van zekerheid voor de gebruiker. Weliswaar kan een computerprogramma op grond van het Nederlandse recht voor auteursrechtbescherming in aanmerking komen, maar bij inbreuk zal veelal de gang naar de rechter gemaakt moeten worden. Een proces voeren betreft een tijdrovende en kostbare bezigheid, ook indien de eiser het gelijk aan zijn kant krijgt. De trage procesgang creëert bij partijen onzekerheid terwijl het ook nog eens om voer voor specialisten gaat. Rechters en advocaten ontberen in het algemeen informaticakennis en inzicht in gewoonten en gebruiken in de automatiseringsbranche. Al gauw zullen automatiseringsdeskundigen uitkomst moeten bieden, maar wie zijn dat?
Door gebruik te maken van registratie en escrow-depot van programmatuur staat de rechthebbende in een bewijsrechtelijke sterke positie, waardoor zelfs de stap naar de rechter en de daaruit voortvloeiende problemen kan worden voorkomen, omdat men domweg over het benodigde beschikt. Registratie en escrow-depot heeft derhalve zowel preventie als repressieve beschermingskracht.

3.1 Leveranciers

Voor de leverancier in de rol van werkgever zijn er eveneens beveiligingsaspecten aan te wijzen. Registratie en escrow-depot van software betekent voor hem bescherming tegen inbreuk in de vorm van kopiëren, slaafs nabootsen en wat dies meer zij. Rechtsbescherming tegen derden (concurrenten), maar zeker niet in de laatste plaats tegenover eigen personeel.

Algemeen wordt aangenomen dat werknemers het grootste lek zijn van bedrijfsgeheimen. [De vraag kan in gemoede gesteld worden of dit waar is. Redactie] Computerprogramma's vormen hierop geen uitzondering. Of de programmeur deze nu aan de concurrent levert, of dat hij, en dat gebeurt maar al te vaak, voor zich zelf begint, registratie en escrowing van software biedt in rechte uitkomst. Bewijstechnisch kan een goed gemotiveerd en gestaafd stuk worden geproduceerd. Daarnaast strekt registratie en escrowing van software tot voordeel van de leverancier, omdat deze figuur juridisch maar vooral feitelijke overdracht van sources en listings aan de gebruiker/opdrachtgever overbodig kan maken. Immers voor dagelijks gebruik heeft hij deze niet nodig. Een "run only"-kopie voldoet geheel en hoe minder personen over de broncode kunnen beschikken, hoe beter het is. Op deze wijze wordt voorkomen dat aan de gebruikerskant maat-software zonder toestemming wordt gekopieerd en gebruikt.
Overigens is het wel zo dat eigendoms-, exploitatie- en gebruiksrechten met betrekking tot programmatuur te allen tijde schriftelijk moeten worden vastgelegd. De leverancier moet duidelijke afspraken maken met de gebruikers, zijn contractors en met zijn eigen werknemers.
Voor wat betreft de laatstgenoemde relatie is van belang dat onze auteurswetgeving bepaalt dat het auteursrecht op het door de werknemer vervaardigde werk in beginsel toekomt aan de werkgever. In beginsel, omdat partijen anders overeen kunnen komen. Met free-lance-medewerkers of gedetacheerd automatiseringspersoneel (contractors) ligt de zaak minder eenvoudig. Veelal zal in casu sprake zijn van een overeenkomst tot het verrichten van enkele diensten, dat een ander rechtsregiem heeft dan de arbeidsovereenkomst. De hoofdregel is dan niet van toepassing.
Hoewel het voor de hand ligt dat rechten met betrekking tot de eigendom van programmatuur te allen tijde contractueel moeten worden vastgelegd, wordt er in de praktijk niet altijd naar gehandeld. In dit verband moet eveneens op de situatie worden gewezen dat het auteursrecht op grond van de Auteurswet 1912 aan het software-huis zal toekomen, indien dit software-huis de programmatuur als van haar afkomstig openbaar maakt zonder de naam van de (externe) programmeurs bekend te maken.
Een laatste, maar daarom niet minder zwaarwegend voordeel betreft een puur marketing-aspect. Immers de leverancier die gebruik maakt van registratie en escrow-depot van zijn (nog te ontwikkelen) programmatuur, zal dit in de precontractuele fase de potentiële gebruikers ter kennis kunnen brengen. Bij de potentiële gebruiker zal dit feit terecht worden meegewogen in het beoordelingsproces, om met een bepaalde leverancier in zee te gaan. Continuïteit is immers de conditio sine qua non voor een geslaagd automatiseringsproces.

3.2 Gebruikers

Nadat men eenmaal met de verstrekkende gevolgen van het beëindigen van de activiteiten van de leverancier op pijnlijke wijze in aanraking was gekomen, werd er naar wegen gezocht de continuïteit van het automatiseringspro-

ces zeker(der) te stellen. Een proces, waarbij in de regel grote (financiële) belangen op het spel staan, die zo goed als mogelijk is moeten worden gediend en de daarmee verbonden risico's tot een aanvaardbaar niveau moeten worden teruggebracht.
Vaststaat dat indien de leverancier "wegvalt", de gebruiker over de sources en listings moet beschikken. Niet zozeer om het feit dat hij zelf aan de slag kan gaan om onderhouds- en "update"-werkzaamheden uit te voeren, dan wel dat het gekwalificeerde en tijdrovende werk door een ander software-huis wordt overgenomen.
Door registratie en escrow-depot van zijn programmatuur krijgt de gebruiker onder strikt omschreven voorwaarden een eigen recht van toegang tot de broncode van de software en de technische documentatie. Het toegangs- en gebruiksrecht wordt in het bijzonder geactiveerd indien het economische leven van de leverancier (software-huis, systeemhuis) op een of andere wijze wordt beeindigd. Verschillende situaties kunnen zich in dit kader voordoen: het staken van de onderneming, overlijden van de programmeur, overname van het bedrijf, geschillen over de auteursrechten van de software met concurrenten, surseance van betaling en natuurlijk ook faillissement.
Ten slotte kan nog worden overeengekomen, indien de leverancier met onderhoud stopt, bijvoorbeeld omdat het software-huis van mening is dat onderhoud en nieuwe releases voor deze bepaalde software niet meer economisch haalbaar zijn, de gebruiker toegang krijgt tot sources, zodat hij niet onmiddellijk gedwongen wordt nieuwe programmatuur te laten ontwikkelen.

4. De notariële oplossing

De voordelen van registratie en escrow-depot van computerprogrammatuur voor de betrokkenen bij het proces van ontwikkelen en gebruiken van computerprogrammatuur mogen duidelijk aanwezig zijn, maar op welke wijze kan men deze aanwenden?
Wanneer over een bewaargevingsovereenkomst wordt gesproken (het Nieuw Burgerlijk Wetboek opteert overigens voor het begrip bewaarnemingsovereenkomst) betekent dit dat iedereen partij bij dit contract kan zijn. Men hoeft geen notaris te zijn om roerende goederen in bewaring te nemen, aldus het Nederlandse recht. Echter wil men zeker zijn van het feit dat broncode en technische documentatie van de in bewaring gegeven programmatuur inderdaad buiten een eventueel beslag op goederen in geval van faillissement van de software-leverancier valt, dan is een "gewoon" bewaargevingscontract in beginsel onvoldoende, zelfs al is de notariële rechtskundige de bewaarnemer van de software.
Naar redelijke waarschijnlijkheid zijn het slechts juridische technieken, die gebaseerd zijn op het notariële recht en die alleen door een notaris op grond van de door de wet aan hem toegekende bevoegdheden opgezet en uitgevoerd kunnen worden, die erin slagen programmatuur toegankelijk te houden voor de gebruiker. De crux van de zaak is namelijk hierin gelegen dat het gedeponeerde aan het rechtsverkeer wordt onttrokken. Op grond hiervan is beslaglegging niet mogelijk.

Indien de betrokkenen rond het gehele proces van ontwikkeling, gebruik en onderhoud van computerprogrammatuur gebruik wensen te maken van registratie en escrow-depot van software als praktijkgerichte wijze van rechtsbescherming en indien zij deze juridische constructie met succes willen toepassen, dan moet er op verschillende zaken worden gelet:

- registratie en escrow-depot, hetgeen meer inhoudt dan de klassieke bewaargevingsovereenkomst, zal bij een notaris moeten plaatsvinden in zijn hoedanigheid als openbaar ambtenaar;
- in de overeenkomst zal een contractsbepaling moeten worden opgenomen, waarin wordt vastgelegd dat ook iedere mutatie in de computerprogramma's ("updates", "upgrades", nieuwe releases) moet worden gedeponeerd en gecontroleerd;
- bij de notaris zal voldoende kennis op het terrein van de geautomatiseerde gegevensverwerking aanwezig moeten zijn voor bijkomende technische details, terwijl tegelijkertijd bijzondere eisen moeten worden gesteld ten aanzien van interne en externe beveiliging, bewaringsfaciliteiten en verzekeringen.

Het belang van de continuïteit van het automatiseringsproces, de wezenlijke rol die computerprogrammatuur hierin speelt en de omvang van de investeringen die in automatiseringsperspectief zijn gedaan, rechtvaardigen dat de betrokkenen bij automatiseringsprojecten registratie en escrow-depot van software ten minste te overwegen.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Herfst 1987

BEVEILIGEN TEGEN COMPUTERMISBRUIK

door A.W. Neisingh en drs. J. Vossen

1. Inleiding

De invloed van de automatisering op de beheersbaarheid van de organisatie

Het is inmiddels niet meer voor discussie vatbaar. Bedrijven en instellingen zijn in grote mate afhankelijk van een continu beschikbare, betrouwbare, geautomatiseerde gegevensverwerking. Beheersbaarheid te vertalen als maatregelen van interne controle en beveiliging in het licht van de ongestoorde voortgang van de gegevensverwerking. Interne controle zowel gedefinieerd voor wat betreft het voorkomen, respectievelijk het tijdig ontdekken van onopzettelijke en opzettelijke fouten. Beveiliging als preventieve maatregel om onbevoegden te weren en voor het waarborgen van de continuïteit. De transformatie van een industriële naar een "informatiemaatschappij" is in volle gang.
Tot voor enige tijd konden facturen en vrachtbrieven nog handmatig worden geschreven. Inmiddels is de tijd aangebroken dat deze administratieve handelingen, mede ten gevolge van een toegenomen bedrijfsomvang, niet meer handmatig mogelijk zijn. Het toenemende gebruik en de voortschrijdende technische mogelijkheden van de automatisering zoals integratie en distributie van apparatuur, programmatuur en gegevensverzamelingen maken de organisatie kwetsbaar. Deze kwetsbaarheid noodzaakt de organisatie tot het nemen van maatregelen om de geautomatiseerde gegevensverwerking te beheersen.

In dit artikel zal in het bijzonder worden stilgestaan bij opzettelijke fouten. Dat wil zeggen, die handelingen waarbij kan worden gesproken van computercriminaliteit. Aangegeven wordt op welke wijze een organisatie zich kan beveiligen tegen de bedreigingen van computermisbruik.
De definitie van computercriminaliteit zal worden gevolgd zoals die is gedefinieerd door de Commissie Computercriminaliteit (naar haar voorzitter genoemd de Commissie Franken) en zoals weergegeven in haar eindrapport Informatietechniek en Strafrecht. Basis voor de definitie is computermisbruik.

"Computermisbruik is schadelijk gedrag met betrekking tot de opslag, verwerking en uitwisseling van gegevens door middel van daartoe vervaardigde apparatuur. Misbruik omvat alle schadelijke gedragingen; criminaliteit alleen de strafbaar gestelde."

Die opzettelijke handelingen kunnen zich voltrekken ten aanzien van:
- de computerapparatuur;
- de besturingsprogrammatuur;
- toepassingsprogrammatuur;
- de gegevensverzamelingen.

Risicobeheersing

Ervaring leert dat de schade die leemtes in de administratieve organisatie kunnen veroorzaken, vaak wordt onderschat. Bij calamiteiten kan juist de kostenpost voor het eventueel reconstrueren van computerprogramma's en winstderving bij verstoring van het produktieproces of bij de in- en verkoop een grote omvang aannemen. Veel moeilijker te meten, maar niet minder reëel, zijn de consequenties als bedrijfsgegevens in handen van de concurrentie komen. Schade aan financiële gegevens wordt vaak onderschat.
Risicobeheersing is vooral een organisatorische aangelegenheid. Zo moet allereerst een beveiligingsbeleid worden gedefinieerd, waarbij de gehele organisatie in ogenschouw wordt genomen. Vervolgens is het zaak de betrokkenen te motiveren voor de doelstellingen die in het beveiligingsplan zijn geformuleerd. Het is de verantwoordelijkheid van het management ervoor te zorgen dat het niet bij goede voornemens blijft. De beveiligingsmaatregelen zullen ook in de toekomst werkzaam moeten zijn. Om dit te bereiken dient er permanent aandacht te zijn voor veranderingen in risico's terwijl daarnaast behoefte bestaat aan een mechanisme om de effectiviteit van de maatregelen te meten. Door de kosten van de beveiligingsmaatregelen te vergelijken met de mogelijke schade en de kans daarop. Het is evenmin zinvol onevenredig dure maatregelen toe te passen op een facet van de beveiliging als andere zwakke plekken blijven bestaan.
Deze aspecten bepalen uiteindelijk of de nagestreefde risicobeheersing een succes wordt of mislukt.

"Waakhond"

In organisaties kan het wenselijk zijn een functionaris aan te stellen, belast met de beleidsvoorbereiding, coördinatie en toezicht op de uitvoering van beveiligingsmaatregelen. Deze functionaris kan tijdig manco's signaleren en als zodanig binnen het management de taak van "waakhond" vervullen. Waakzaamheid is immers één van de pijlers waarop een goed beveiligingsbeleid rust. Anders gezegd: zonder een goede beleidsmatige, organisatorische en personele ondersteuning kan zelfs het meest ingenieuze systeem waardeloos blijken te zijn.

Dit artikel is verder als volgt ingedeeld:
2. Risicogebieden
3. Vormen van computermisbruik
4. Beveiliging van geautomatiseerde gegevensverwerking
5. Meest voorkomende tekortkomingen in de computerbeveiliging
6. Functie van "EDP auditing" ten aanzien van computermisbruik.

2. Risicogebieden

De afhankelijkheid van de organisaties van de geautomatiseerde gegevensverwerking, noodzaakt tot een beheersing van de bedreigingen die een organisatie loopt.
De bedreigingen zijn afhankelijk van de automatiseringsgraad van de organisatie.

Voor de vaststelling van de automatiseringsgraad zijn van belang het samenstel van het bedrijfstype, de gevoeligheid en de betekenis van de geautomatiseerde systemen, te zamen met de wijze van gegevensverwerking en de omvang van de automatiseringsinspanning zoals deze blijkt uit de technische omgeving.

Onder bedrijfstype en specifieke wijze van gegevensverwerking verstaan we het volgende.
De aard van de bedrijfsactiviteiten (bijvoorbeeld banken, verzekeringsmaatschappijen, produktie-ondernemingen, handel en dienstverlening, overheidsdiensten en dergelijke), alsmede de specifieke wijze van gegevensverwerking (on-line, on-line real time, batch-verwerking), al dan niet met gebruikmaking van database management-systemen, zijn mede bepalend voor de betekenis die de kwaliteit van de automatisering en de beveiliging ervan voor de organisatie hebben.

De technische omgeving kan afgeleid worden uit de informatie over eigen gegevensverwerking c.q. verwerking door derden, het al dan niet verwerken door middel van meerdere eigen computers/locaties en de reden daarvan, de aard en de omvang van de eigen mainframes, mini's, micro's en terminals, alsmede de toepassing van programmeertalen (ook door gebruikers). Op grond hiervan is een indeling te maken in de categorieën grootschalige, kleinschalige en middelgrote automatisering.

Voor de systematische benadering van de bedreigingen zijn de volgende risicogebieden te onderkennen:
1. organisatie: mensen en procedures;
2. gegevens;
3. toepassingsprogrammatuur;
4. systeemsoftware;
5. hardware;
6. omgeving.

Afhankelijk van de automatiseringsgraad is per risicogebied aan te geven welke bedreigingen de organisatie loopt.
Een systematische inventarisatie van de bedreigingen is van belang voor het bepalen van de te treffen beveiligingsmaatregelen, om te voldoen aan de doelstellingen, die in het beveiligingsplan zijn geformuleerd.

Op grond van het voorgaande moge het duidelijk zijn dat de praktijk noodzaakt tot een grote variatie in de structuur van de automatisering. Deze structuur laat zich niet beschrijven door middel van een representatieve casus. Voor iedere individuele situatie zal derhalve vastgesteld moeten worden welke combinatie van beveiligingsmaatregelen, noodzakelijk wordt geacht.

3. Vormen van computermisbruik

In het navolgende wordt een overzicht gegeven van de bedreigingen, die de integriteit en continuïteit van de automatisering van de gegevensverwerking bedreigen. Hierbij zijn de bedreigingen per risicogebied aangegeven. De bedreigingen hebben betrekking op computermisbruik.
Er is niet getracht een volledige opsomming te geven van mogelijke bedreigingen, maar er is getracht de lezer een inzicht te geven in mogelijke bedreigingen per risicogebied.
Het onderkennen van de bedreigingen per risicogebied kan behulpzaam zijn bij het opstellen van het pakket van beveiligingsmaatregelen.

In het volgende stuk wordt veelvuldig gebruik gemaakt van vakjargon. Dit is zoveel mogelijk toegelicht. (Indien een wetenschap beoordeelt zou worden op het creëren van nieuwe woorden, dan zou de informatica niet slecht scoren.)

3.1 Organisatie: mensen en procedures

Verpersoonlijking (impersonation)

Een persoon neemt de identiteit van een andere geautoriseerde persoon aan. Dit geschiedt door gebruik te maken van de identificatie van die persoon. Door middel van deze impersonation kan bevoegdheid verkregen worden tot:
- toegang tot (een deel van het) gebouw, de computerruimte, het computersysteem, de gegevens- en programmatuurverzamelingen, actieve processen;
- inzage in afgedrukte uitvoer;
- in produktie nemen van programma's en bestanden;
- aanbrengen van constructies met frauduleuze bedoelingen in programmatuur.

Functiescheiding

Het achterwege laten van adequate functiescheiding bij geautomatiseerde gegevensverwerking verzwakt de interne controle.

Procedures

Leemten in c.q. het niet opvolgen van de te volgen procedures.
Hierbij kan gedacht worden aan het niet tijdig veranderen van passwords in geheimhouding van passwords.

Documentatie

Het ontbreken van adequate documentatie en registratie inzake verleende bevoegdheden en de wijze waarop deze gewaarborgd zijn.

Computerchantage

Het chanteren van de organisatie door eigen medewerkers die sleutelposities innemen of door medewerkers die gegevensdragers meenemen.

Gebruik van diensten

Gebruik van het computersysteem door mensen uit de organisatie voor andere doelen dan de doelstellingen van de organisatie. Dit kan bestaan uit het onschuldige spelletje tot en met het leveren van diensten voor derden gebruik makend van de applicaties van de organisatie of applicaties van derden.

Vandalisme

Dit neemt meestal de vorm aan van fysieke schade toebrengen aan het computersysteem en de randapparatuur. Denk aan het risico van daden door ontevreden werknemers of idem ex-werknemers.

3.2 Gegevens

Bij gegevens is soms moeilijk vast te stellen of er sprake is van computermisbruik of een misdaad met behulp van de computer. Het manipuleren van gegevens vond bij handmatige administraties reeds plaats. Dit is niet zo zeer computermisbruik, maar een administratief organisatorische fout (slechte interne controle, geen audit trail) waardoor dit mogelijk is. Anders wordt het als gegevens worden gemanipuleerd na het verkrijgen van onbevoegde toegang tot het computersysteem.

Data diddling

Het ongeautoriseerd wijzigen, vervangen, toevoegen of weglaten van gegevens tijdens de invoer of tijdens de uitvoer van het systeem. Dit kan geschieden door de wijzigingen aan te brengen op het invoermedium, uitvoermedium of direct met behulp van terminals.

Scavening

Het verkrijgen van gegevens die achtergelaten worden rondom een computersysteem na de uitvoering van een verwerking. Dit kan zowel de fysieke output zijn (in prullenbak) als het uitlezen van niet uitgewiste werkgeheugens.

Data leakage

Een methode om heimelijk gegevens van een computersysteem te verkrijgen. Dit kan geschieden door de gegevens te verbergen in reguliere output of door middel van zinslengte, waaraan een afgesproken betekenis kan worden ontleend.

Output

De verkregen output kan voorzien in de benodigde gegevens om een fraude op te zetten (bijvoorbeeld crediteurennummers).

3.3 Toepassingsprogrammatuur

Trojan horse

Het toevoegen van instructies in een geautoriseerd programma. Het veranderde programma zal goed werken, maar de toegevoegde instructies zullen ook uitgevoerd worden.

Trapdoor

Een trapdoor is een fout of kwetsbaar stuk in een programma geplaatst of erin gelaten tijdens de ontwikkelfase, om dit op een later tijdstip te activeren.

Salami techniques

Deze zijn gebaseerd op het overbrengen van kleine hoeveelheden van bezittingen van een groot aantal bronnen. Hierbij kan gedacht worden aan een renteberekeningsprogramma dat zodanig is aangepast dat alle afrondingsverschillen ten gunste van een rekeninghouder komen.
De mogelijkheid van ontdekking is geminimaliseerd, omdat geen enkel slachtoffer zulke verliezen lijdt dat hij die opmerkt.
Tevens verdwijnt er niets van het totale bedrag uit het systeem en vindt alleen een verschuiving plaats. De salami techniques vereisen een verandering van bestaande instructies in programma's of de ontwikkeling van een programma dat verwerkt kan worden op het systeem en toegang heeft tot een groot bestand van bronnen.

Logic bomb

Dit is een programma of een gedeelte van een programma dat automatisch wordt uitgevoerd om de status en inhoud van een computersysteem te testen.

Als aan alle gedefinieerde condities is voldaan wordt een ongeautoriseerde actie uitgevoerd. Het meest gunstige moment voor de illegale actie wordt op deze manier uitgekozen.

Virussen

Dit is een programma dat andere programma's kan infecteren door ze te modificeren met een (mogelijk geëvolueerd) kopie van zichzelf. Het virus verspreidt zich over het netwerk gebruik makend van de autorisatie van alle gebruikers die het geïnfecteerde programma gebruiken. De programma's van deze gebruikers worden ook geïnfecteerd met het virus, totdat alle programma's het virus bevatten. Het virus kan bestaan uit een verminking van programma's en gegevens, een programma dat gegevens kopieert naar voor de dader toegankelijke directories of een log bijhoudt wie wanneer welke kenwoorden een programma gebruikt.

Worms

Dit is een programma dat ongebruikte processors gebruikt om niet doelmatige berekeningen uit te voeren. Het beslag van de processoren kan zo groot worden dat geen andere acties meer uitgevoerd kunnen worden. Het systeem moet opnieuw opgestart worden.

Kopiëren

Het illegaal kopiëren van software. Deze illegale kopieën worden aangewend voor eigen gebruik of verhandeld.

3.4 Systeem-software

Superzapping

Het ongeautoriseerd gebruik van faciliteitenprogramma's (utilities) voor wijzigen, vernietigen, raadplegen, kopiëren en/of gebruiken van gegevens of toepassingsprogramma's.

Asynchronous attack

De meeste besturingssystemen werken asynchronisch. Meerdere verschillende processen vinden achtereenvolgens plaats zonder dat het eerste proces geheel afgehandeld is. De afgebroken processen worden tijdelijk opgeslagen totdat er voldoende resources beschikbaar zijn. De beheersing van deze asynchrone verwerking geschiedt door het besturingssysteem. Dit is een zeer complex geheel van programma's. Soms is het mogelijk de condities te veranderen tijdens de tijdelijke opslag, die door het systeem niet opgemerkt worden. Bij een asynchronous attack maakt men gebruik van de beperkingen van de beheersingsmogelijkheden van het besturingssysteem.

Controles

De meeste systeem-software bevat een beveiligingspakket, dat allerlei controles uitvoert. Door het uitschakelen van de controles en de log-faciliteit kunnen programma's en gegevens benaderd en veranderd worden zonder dat hier nog enige controle op is.

Achterdeur

Dit is een toegang tot het systeem die in het algemeen alleen bekend is bij de ontwerper van het systeem, maar soms door anderen gevonden wordt.

Systeem_crash

Misbruik maken van kwetsbaarheden die optreden na een crash van het systeem. Zo is het mogelijk dat bepaalde bestanden niet gesloten zijn en zodoende door onbevoegden benaderd kunnen worden.

3.5 Hardware

Hardware-modificatie

Ongeautoriseerde modificatie van hardware. Naast het modificeren van de hardware kan hier ook gedacht worden aan impersonation van hardware.

3.6 Omgeving

Netwerken

- Vrijkomen berichteninhoud.
  Het vrijkomen van de inhoud van een bericht vindt plaats indien de informatie in een bericht bekend wordt (bijvoorbeeld door het aftappen van een communicatiekanaal) aan een daartoe ongeautoriseerde persoon of entiteit (bijvoorbeeld een proces).
- Analyseren berichtenstroom.
  Het analyseren van de berichtenstroom is het ongeautoriseerd observeren van de berichtenstroom in het netwerk. Hierbij is meestal additionele informatie noodzakelijk. Indien een indringer bijvoorbeeld ziet dat er veel berichten worden uitgewisseld tussen de componenten van twee bedrijven dan zou hij daaruit kunnen afleiden dat de twee bedrijven onderhandelen. Dit gegeven alleen is echter niet zo interessant, men zou al moeten weten waarover de twee bedrijven eventueel zouden kunnen zijn gaan onderhandelen.
- Wijzigen van berichtenstroom.
  Het wijzigen van de inhoud, hertransmissie van berichten, het toevoegen of verwijderen van gegevens en het opnieuw ordenen van blokken waarin een bericht is opgesplitst.

- Blokkeren en/of vertragen van berichten.
- Piggyback.
  Een ongeautoriseerd persoon verkrijgt toegang tot het systeem door gebruik van een andere persoon. Dit kan bijvoorbeeld geschieden door op hetzelfde communicatie circuit te zitten. (Dit is een andere vorm van impersonation).
- Hacking.
  Het inbreken in geautomatiseerde gegevensverwerkende systemen door telecommunicatie-instrumenten. De meest toegepaste methode hiervoor is door middel van impersonation.

Tempest

Computers zenden, wanneer zij zijn ingeschakeld, continu radiogolven uit, die met behulp van een ontvangeenheid kunnen worden opgevangen en gedecodeerd.

Simulatie

Een computer kan gebruikt worden om bepaalde systemen of processen te simuleren om zodoende het effect en mogelijke succes te bepalen van een misdaad.

Diefstal

Het toeëigenen van hardware en software.

Sabotage

- Fysieke schade.
  Deze kan gepleegd worden door een ieder die dicht genoeg bij het computercentrum of datacommunicatiefaciliteiten kan komen. Fysieke sabotage omvat het opblazen van het computercentrum tot het uitschakelen van de power-knop.
- Logische schade.
  Hieronder kunnen vallen het veranderen van programma's en gegevens. Methoden hiervoor zijn onder andere superzapping en trojan horse. Deze worden hier nog eens genoemd omdat het doel hier puur sabotage is.

4. Beveiliging van geautomatiseerde gegevensverwerking

Het is niet aan te bevelen om bij het beveiligen van geautomatiseerde gegevensverwerking zich alleen te richten op de bedreigingen van computermisbruik.
Beveiliging moet in een breder perspectief gezien worden van betrouwbaarheid en beveiliging van geautomatiseerde gegevensverwerking. Waarbij computermisbruik één van de bedreigingen is.

a. Algemene maatstaven voor beveiliging

Achtereenvolgens zullen de volgende aspecten worden behandeld:
- Beleid;
- Risico-analyse;
- Noodvoorzieningenplan;
- Betrouwbaarheid van de automatiseringsorganisatie;
- Betrouwbaarheid van de geautomatiseerde informatiesystemen;
- Fysieke beveiliging;
- Beveiliging van microcomputers;
- Selectie van beveiligingsmaatregelen.

Beleid

Het definiëren van beleid, het concretiseren en het uitvoeren ervan zal uiteindelijk dienen uit te monden in de beheersing van de organisatie door het management.
Bij de navolgende beschouwing is ervan uitgegaan dat een algemeen informatie- en automatiseringsbeleid aanwezig is, zodat er een organisatorisch uitgangspunt voor het voeren van een effectief beveiligingsbeleid voorhanden is.

De introductie van automatisering in een organisatie leidt tot een concentratie van risico's, omdat de bestaande functioneel gescheiden verwerkingscircuits qua aantal zeer sterk worden ingekrompen. Deze tendens is versterkt door de ontwikkeling van grotere mogelijkheden van automatisering (als bijvoorbeeld de vervanging van de - geparcelleerde - seriegewijze gegevensverwerking door in beginsel ononderbroken postgewijze gegevensverwerking) en de sterke toename van datacommunicatie over interne en externe data-communicatienetten.

Het is dus zaak te trachten de bedreigingen door middel van risicobeheersing op een methodische wijze te benaderen. Computermisbruik is één van de bedreigingen die een organisatie met geautomatiseerde gegevensverwerking loopt.
Risicobeheersing is het bewust, integraal en dynamisch onderkennen van alle risico's (inclusief die als gevolg van automatisering) en het introduceren en handhaven van een evenwichtig samenstel van maatregelen om de risico's te beperken tot een voor het management aanvaardbaar (kosten)niveau. Deze definitie plaatst risicobeheersing in het kader van de totale organisatie en daarmede ook van de automatisering.

Het bezig zijn met de bedreigingen die een organisatie loopt, dient welbewust te geschieden. Indien dat niet het geval is zullen noodzakelijke maatregelen om risico's te kunnen beperken achterwege blijven en getroffen maatregelen als niet zinvol worden beschouwd.

Hierdoor zijn ze zeker niet als effectief aan te merken. Met het bewust bezig zijn met risicobeheersing staat of valt de acceptatiegraad van een door het management uitgestippeld beleid ten aanzien van risicobeheersing. Het is daarom niet voorbehouden aan het management of verbijzonderde security functies etc. alleen, maar het is een noodzaak voor alle geledingen van de totale organisatie. Inbedding in de organisatiestructuur (functies, procedures en voorschriften) is derhalve een voorwaarde. Onder zo'n integrale benadering moet worden verstaan de benadering die uitgaat van de totale organisatie waarbij deze kan worden gesplitst - en onderzocht - in deelgebieden zonder dat de "totaalvisie" wordt losgelaten. (Voorbeeld: geen onderzoek naar risicobeheersing ten aanzien van computermisbruik zonder dat dit geplaatst wordt in het deelgebied risicobeheersing uit hoofde van automatisering en dit weer gezien in het kader van de risicobeheersing van de totale onderneming.)

Het woord dynamisch duidt erop, dat er permanent aandacht moet zijn voor de risico's die uit welken hoofde dan ook worden gelopen. Het dynamisch aspect van risicobeheersing dient zijn voedingsbodem in de organisatie te vinden.

Slechts door het integraal en dynamisch onderkennen van risico's kan een evenwichtig stelsel van maatregelen ontstaan en worden gehandhaafd. Een niet integrale benadering zal onvermijdelijk leiden tot onevenwichtigheid in de te treffen maatregelen en daarmede ook in de risicobeheersing.
Als het management zich niet bewust is van de risico's en dat niet vertaalt in een daarop geënt beleid, hoe kan dan een bewuste uitvoering en naleving van de getroffen maatregelen door de lagere echelons worden verwacht. Risicobeheersing moet derhalve - om effectief te zijn - door het management worden vertaald in een actief beleid waaraan de organisatie als geheel is gebonden. Het beleid gericht op risicobeheersing zal duidelijke normen moeten bevatten waaraan moet worden voldaan met terugkoppelingsinformatie naar het management of aan die normen blijvend wordt voldaan.

Uit het voorgaande kan derhalve worden afgeleid, dat risicobeheersing een organisatorisch probleem is.

In dit verband kan computerbeveiliging worden gedefinieerd als dat deel van de maatregelen in het kader van de totale risicobeheersing, dat het traject van de geautomatiseerde gegevensverwerking en informatievoorziening bestrijkt. (Het beveiligen tegen computermisbruik is een automatisch gevolg hiervan.)
Het is daarom noodzakelijk, dat de leiding van een organisatie zich fundamentele opvattingen eigen maakt omtrent de eisen welke zij hieraan wenst te stellen.
Beveiliging van de geautomatiseerde gegevensverwerking en informatievoorziening is gericht op:
- het beschermen van de geautomatiseerde informatieverzorging tegen incidenten die de continuïteit van dit proces kunnen verstoren;

- het beschermen van gegevensverzamelingen en computerprogramma's tegen al dan niet opzettelijke verminking en onbevoegd gebruik;
- het beperken van schade indien deze toch dreigt te worden geleden.

Dit geheel van maatregelen dient te worden ondergebracht in een zogenoemd "Computerbeveiligingsplan". Hierin worden onder meer aangetroffen maatregelen:

- van preventieve aard, gericht op het minimaliseren der risico's. Dit is in sterke mate van toepassing op computermisbruik. De gevolgen zijn vaak desastreus en moeten voorkomen worden;
- van signalerende aard, gericht op het tijdig, of althans in een zo vroeg mogelijk stadium ontdekken van onregelmatigheden;
- van conserverende aard als rampenbestrijding, voorzieningen in noodgevallen, met inbegrip van reconstructie. Hoofddoel van deze maatregelen is dreigende schade tot het uiterste te beperken en zo enigszins mogelijk geleden schade binnen aanvaardbare tijdgrenzen te herstellen.

Met betrekking tot het in dit plan neergelegde beveiligingsbeleid zijn de belangrijkste facetten de zogenaamde toegangscontrole en de continuïteit. Op eerstgenoemd gebied zullen de te stellen eisen steeds zwaarder worden, ten einde te voorkomen dat de programmatuur en gegevensverzamelingen, of althans grote delen ervan, als het ware voor iedere gebruiker van het computersysteem bereikbaar en dus "open" is. Laatstgenoemd facet vergt de nodige aandacht met name wanneer daarbij in aanmerking wordt genomen dat niet zelden tientallen of zelfs honderdtallen gebruikers via terminals aan het computersysteem zijn gekoppeld en de benodigde gegevens slechts via terminals kunnen worden verkregen. Wanneer zich hierbij een storing voordoet zal het systeem in staat dienen te zijn zelf de laatste nog juiste stand te traceren.
Zonder de expliciete inbreng van de topleiding zullen informatie-analisten en systeemontwerpers los van elkaar betrouwbaarheids- en continuïteitseisen introduceren, zonder dat zij het geheel van de problematiek kunnen overzien, er is immers geen beleidsvisie als kader waarnaar men zich dient te richten.
Een goed beveiligingsbeleid wordt gekenmerkt door de ruimte die is toegekend aan de aanpassing aan zich wijzigende omstandigheden, met andere woorden een flexibel beleid vereist een aanpassing à tempo; ex-post oplossingen tonen veelal aan, dat het beleid niet meer adequaat kan worden genoemd en dat er mogelijk al grotere gevaren dan wenselijk hebben bestaan.

Als voorloper van het beveiligingsplan zullen de bestaande en mogelijk te ontstane risico's moeten worden geïnventariseerd en geanalyseerd. In de volgende paragraaf wordt op dit laatste nader ingegaan.

Bij de opstelling van het beveiligingsplan dient een keuze te worden gemaakt uit een scala van mogelijke beveiligingsmaatregelen, terwijl bovendien noodzakelijkerwijze daarin ook noodvoorzieningen en op reconstructie

gerichte handelingen een plaats moeten krijgen. Tenzij de organisatie de eerste schreden zet in de automatisering, zal in de praktijk vrijwel nimmer van het nulpunt behoeven te worden uitgegaan. Bij de initiëring van - ook schijnbaar onbelangrijke - wijzigingen zal het gevoerde beleid en het daaruit voortvloeiende beveiligingsplan in heroverweging moeten worden genomen.

Een beveiligingsbeleid kan niet bevredigend worden gedefinieerd zonder een gedegen beleidsvoorbereiding. Deze behelst het uitvoeren van een zogenaamde risico-analyse.

Risico-analyse

Een risico-analyse beoogt op een zo geobjectiveerd mogelijke wijze te bepalen welke risico's in welke omvang aanwezig zijn. Daarom vormt deze analyse een richtsnoer voor de praktisch te treffen maatregelen.

De risico-analyse dient te omvatten:

1. het onderkennen van de bedreigingen tezamen met een schatting van de waarschijnlijkheid van het worden tot calamiteit;
2. het begroten van de mogelijke omvang van de schade;
3. het vaststellen van de schadeverwachting per onderscheiden bedreiging (de schadeverwachting is gelijk aan het produkt van de waarschijnlijkheid van het optreden van een calamiteit binnen een gegeven periode en van de begrote omvang van de schade).

Met betrekking tot de bedreigingen gaat het uiteraard om vitale functies voor bedrijf en organisatie voor zover deze afhankelijk zijn van geautomatiseerde gegevensstromen.

Ad 1.

Bedreigingen kunnen zijn gelegen in fouten als gevolg van onbedoeld te kort schieten van mensen, in opzettelijk kwaadwillig handelen, in technische storingen en in calamiteiten als brand, explosie en wateroverlast.

Voor het opzettelijk kwaadwillig handelen wordt verwezen naar de genoemde bedreigingen in hoofdstuk 3.
De overige bedreigingen worden in het kort beschreven.

Menselijke fouten kunnen zich niet alleen voordoen bij de bediening van de apparatuur en de hantering van machinaal leesbare gegevensverzamelingen, maar evenzeer bij het maken van computerprogramma's, waardoor deze tekortkomingen vertonen die grote nadelige gevolgen kunnen hebben. Het maken van fouten geschiedt onopzettelijk. Er dienen zodanige omstandigheden te worden geschapen dat fouten menselijkerwijs gesproken vrijwel uitgesloten zijn en - als ze toch voorkomen - tijdig worden ontdekt. Desondanks vormen zij kwantitatief bezien de belangrijkste categorie bedreigingen.

Technische storingen kunnen zich bijvoorbeeld voordoen in de apparatuur, in de stroomvoorziening, in datalijnen. Calamiteiten als brand, explosie, wateroverlast en dergelijke behoeven nauwelijks toelichting, maar deze behoren wel in de analyse te worden begrepen.

Ad 2.

Na de analyse van de bedreigingen en het in kwalitatieve zin bepalen van hun mogelijke gevolgen, zal de omvang van de mogelijke schade moeten worden gewaardeerd. Het gaat hier om:

- Schade aan of verlies van materiële bezittingen (apparatuur, behuizing). De omvang van de directe schade is hier gelijk aan de vervangingswaarde van deze bezittingen.

- Schade aan of verlies van immateriële bezittingen (gegevensverzamelingen of programma's). De omvang van deze schade wordt bepaald door de kosten van reconstructie. Een dergelijke reconstructie moet geschieden van kopieën of andere gegevensverzamelingen uit, dan wel van de brondocumenten uit. Als reconstructie onverhoopt niet mogelijk is of veel tijd vergt moet rekening worden gehouden met de daarmee samenhangende bedrijfsschade.

- De hierboven bedoelde directe schade gaat meestal gepaard met indirecte schade, met inbegrip van winstderving, welke voortvloeit uit vertraging in de verwerking. Ook belangrijke storingen kunnen vertraging veroorzaken. Het optreden van vertraging in de verwerking, zal zeker na het verstrijken van een zekere tijdslimiet, vrijwel zeker tot verdere schade leiden.

  In het algemeen zal de omvang van de schade toenemen met de duur van de vertraging. Als ene uiterste zal men de tijd moeten schatten die nodig zou zijn voor de reconstructie na een totale vernietiging van de computerfaciliteiten en de bestanden.
  Als andere de min of meer normaal te achten vertraging die optreedt als storingen en dergelijke beperkt blijven tot een normale frequentie en tijdsduur. Door tussen deze uitersten nog 2 à 4 situaties te interpoleren, wordt een pad gebaand waarlangs het mogelijk is een verband te leggen tussen de tijdsduur van een vertraging en de omvang van de daarbij behorende schade.

- Een bijzondere categorie van schade ontstaat bij ontvreemding van gegevens door derden, althans onbevoegden (raadplegen, kopiëren). Afgezien van eventuele reconstructiekosten en kosten van vertraging in de verwerking zal het bedrag van de schade sterk afhankelijk zijn van de aard van de gegevens en van het gebruik dat de onbevoegde ervan maakt. Men zal moeten nagaan wat de gevolgen kunnen zijn indien bepaalde gegevens

in verkeerde handen, bijvoorbeeld die van concurrenten, zouden komen.

- Bij onvoldoende maatregelen van externe bewaring en het achterwege laten van de frequente aanmaak van back-up-kopieën, kan tevens sprake zijn van het verlies van de gegevensverzamelingen.

Ad 3.

De laatste stap in de risico-analyse is het bepalen van de schadeverwachting. Deze werd reeds gedefinieerd als de omvang van de mogelijke schade per soort bedreiging, vermenigvuldigd met de kans dat een dergelijke gebeurtenis zich binnen een gegeven periode zal voordoen. Men kan de schadeverwachting dus op jaarbasis uitdrukken in guldens. Dit zal natuurlijk nooit exact kunnen zijn of zelfs niet altijd mogelijk; de raming van de mogelijke schadebedragen en van de frequentie bevat veel subjectieve elementen, welke echter zoveel als mogelijk geobjectiveerd dienen te worden.

Gezien het grote belang van het afwegen van risico's tegen beveiligingskosten is actieve medewerking van de hoogste leiding vereist. Ten aanzien van belangrijke risico's zal de leiding op de hoogte dienen te zijn van alle overwegingen die nodig zijn om tot een eigen oordeel over de omvang van de schadeverwachting en de noodzaak tot beveiliging te kunnen komen. Indien op topniveau onvoldoende belangstelling bestaat voor de risico's en voor het treffen van beveiligingsmaatregelen, moet worden gevreesd dat grote schade kan worden opgelopen.

Het doel van beveiliging zal steeds zijn de kans op schade tegen de geringste kosten te minimaliseren. Hierin dient een maatstaf te liggen voor het toetsen van de effectiviteit en economische rechtvaardiging van in beschouwing te nemen alternatieve maatregelen.

Uit de risico-analyse moet ook naar voren komen in hoeverre het bestaande stelsel van beveiligingsmaatregelen evenwichtig is, respectievelijk in hoeverre daarbij ten onrechte de nadruk is gelegd op deelgebieden van geringere importantie. Uiteindelijk dient te worden gezorgd voor een adequaat stelsel van organisatorische, technische en in de computerprogrammatuur begrepen controle- en beveiligingsmaatregelen.

Het niet, respectievelijk niet met voldoende diepgang, uitvoeren van een risico-analyse kan er toe leiden, dat een aantal - voor de hand liggende maatregelen - uit het palet van de beschikbare wordt gekozen maar dat belangrijke leemten blijven bestaan.

Noodvoorzieningenplan

Organisaties worden steeds meer afhankelijk worden van het voortdurend beschikbaar zijn van geautomatiseerde gegevensverwerking.
Noodvoorzieningenplannen dienen, indien de in gebruik zijnde faciliteiten in het ongerede raken, om de geautomatiseerde gegevensverwerking, dan wel

belangrijke delen daarvan, met handhaving van de controlemaatregelen te kunnen herstarten binnen de vereiste tijdslimiet.

Tot voor kort waren de consequenties van een calamiteit te overzien als kopieën van programmatuur en gegevens elders werden bewaard en afspraken met andere computergebruikers waren gemaakt om de verwerking te kunnen continueren: het "noodvoorzieningenplan in de dop".
Bij de meer geavanceerde technologieën waarvan op dit moment gebruik wordt gemaakt, waarbij ingevoerde posten onmiddellijk in verschillende gegevensverzamelingen worden verwerkt en verschillende acties worden geïnitieerd (zoals het vervaardigen van produktie-orders en het uitleveren van goederen) moet in het noodvoorzieningenplan rekening worden gehouden met het probleem dat ontstaat doordat gegevens van verschillende locaties of via datacommunicatie worden aangeleverd. Verder dient men er zich van bewust te zijn dat terugkeer naar handmatige verwerking vrijwel nimmer mogelijk is.
Het vervaardigen van zo'n noodvoorzieningenplan is geen sinecure. Van elke verandering binnen de geautomatiseerde gegevensverwerking dienen de consequenties voor het noodvoorzieningenplan te worden nagegaan. De gebruiker speelt hierbij een niet weg te denken rol.

Zo'n noodvoorzieningenplan kan weliswaar technisch door de automatiseringsafdeling worden opgezet, maar de gebruikersorganisatie zal moeten aangeven in hoeverre verstoring van geautomatiseerde processen op de uitoefening van de primaire bedrijfsfunctie van invloed is. Pas dan kan een evenwichtige keuze worden gemaakt uit beschikbare maatregelen. Als een noodvoorzieningenplan eenmaal is gedefinieerd, uitgewerkt en de voorzieningen daarvoor getroffen zijn, behoeft dit niet zonder meer te betekenen, dat aan de eisen is voldaan. De praktijk heeft geleerd dat met enige regelmaat de voorzieningen daadwerkelijk moeten worden uitgetest opdat men niet wordt geconfronteerd met niet voorziene complicaties indien de nood aan de man komt.
In verschillende landen en ook in Nederland bestaan organisaties die bedrijven behulpzaam zijn bij het opzetten en frequent testen van de noodvoorzieningenplannen.
Omdat het bijna niet meer mogelijk is in geval van een calamiteit uit te wijken naar collega-bedrijven, zijn "uitwijkcentra" ontstaan die een scala van mogelijkheden bieden.
Uitgaande van de risico's die "in-house" niet zijn af te dekken (ook niet door verzekeringen) zal een beroep op die uitwijkcentra kunnen worden gedaan. Te veel komt het nog voor dat bedrijven uit het produktenscala van die centra een "aangepaste keuze" doen, die bij hun intuïtief bepaald budget past. Dit is een onderschatting van het probleem. Het is noodzakelijk dat het management erop toeziet dat alle "noodfaciliteiten" worden ingehuurd die volgens de risico-analyse beschikbaar zouden dienen te zijn.

Meestal hebben noodfaciliteiten betrekking op gebouwen, apparatuur en datacommunicatie. Ingeval van die faciliteiten gebruik moet worden gemaakt dienen de "bedrijfseigen gegevens" beschikbaar te zijn. Dat zijn dan de pro-

grammatuur en de diverse gegevens. Zonder deze gegevens is uitwijken zinloos.

Controle op de handhaving en naleving van procedures, voorschriften en dergelijke is een onmisbare zaak.

Betrouwbaarheid van de automatiseringsorganisatie

Een goede beveiliging is niet mogelijk zonder de inschakeling van deskundige personen in en buiten de automatiseringsorganisatie. Organisatorische maatregelen spelen hierbij een belangrijke rol. Bij de werving, opleiding en motivering van het personeel zal door middel van screening, cursussen enz. aan de betrouwbaarheid van het aan te stellen personeel en vervolgens aan het veiligheidsaspect bewust aandacht moeten worden geschonken. Het is van groot belang dat alle betrokkenen de waarde van een goede en ongestoorde informatievoorziening inzien en overtuigd zijn van de noodzaak tot beveiliging. Dat kan er toe leiden dat een veiligheidsfunctionaris met een volle of deeltaak wordt aangesteld voor beleidsvoorbereiding, coördinatie en toezicht op de uitvoering der genomen maatregelen.
Beveiliging en betrouwbaarheid van gegevens en programma's gaan hand in hand. Bij de organisatorische maatregelen gaat het in eerste instantie om het bereiken van een goede structuur waardoor met betrekking tot de geautomatiseerde gegevensverwerking een goede functiescheiding wordt verkregen. In dit verband is het tevens van belang dat een duidelijk onderscheid gemaakt wordt tussen enerzijds de verantwoordelijkheid voor het opzetten van het systeem (analyse en programmering) en anderzijds die voor de werking van het geautomatiseerde systeem. Binnen elk van deze hoofdactiviteiten kan men een aantal functies onderscheiden. Bij de toewijzing en het duidelijk vastleggen van taken en verantwoordelijkheden speelt ook het element van interne controle een belangrijke rol, dat wil zeggen dat er voor wordt zorg gedragen, dat tussen ontwerpers van een systeem en de operationele verwerking en de gebruikers een functionele scheiding moet worden aangebracht, opdat wordt voorkomen, dat beschikkingsmacht over een systeem (opzet, bewaring, beheer) in één of althans te weinig handen komen.

Preventieve beveiligingsmaatregelen zijn behalve functiescheiding en voorschriften ook procedures bij de gebruikers en bij de automatiseringsafdeling in hun onderlinge samenhang. Deze maatregelen en procedures effectueren in wezen de organisatorische beveiliging. Zij zijn uiteraard goeddeels afhankelijk van de aard van de geautomatiseerde toepassingen, nochtans springen de volgende algemene punten in het oog.
Er dient te worden gezorgd voor:

- een goede functie-omschrijving met een duidelijke vastlegging van de taken te verrichten door onderscheiden functionarissen respectievelijk afdelingen;
- de aanwezigheid en handhaving van een voor het gehele bedrijf geldende voorgeschreven methodiek voor systeemontwikkeling, programmering, documentatie, en test, acceptatie en overdracht van systemen;

- de permanente beschikbaarheid van up-to-date gehouden documentatie voor alle informatieverwerkingssystemen. Behalve de goed uitgewerkte gegevens omtrent de opzet en werking van de systemen dient de documentatie ook duidelijke procedurebeschrijvingen en gedetailleerde uitvoeringsinstructies te omvatten;
- een adequaat beheer van gegevensverzamelingen;
- een strak georganiseerd beheer van programmabibliotheken.

Het is van grote betekenis dat het accent wordt gelegd op het materieel effect van de procedures. Hoofddoel hiervan is het als het ware permanent bewust houden der betrokkenen van hun verantwoordelijkheid. Hierbij is het belangrijk dat een documentatie en registratie (log) van de uitvoering wordt opgebouwd en bijgehouden. Dit verschaft niet alleen de basis voor een uitvoering in overeenstemming met de daaraan gestelde eisen maar bovendien voor het afleggen van verantwoording en controle op de uitvoering achteraf.

Betrouwbaarheid van geautomatiseerde informatiesystemen

In het voorgaande is de nadruk min of meer gelegd op de expliciete maatregelen ter beveiliging. Ziende naar de betrouwbaarheid van geautomatiseerde informatiesystemen, zal er voor impliciete beveiliging dienen te worden zorg gedragen, dat wil zeggen een beveiliging welke is ingebouwd in de toepassingsprogrammatuur.

Bij niet sterk geïntegreerde informatiesystemen omvat het te doorlopen verwerkingstraject de vervaardiging van een basisdocument (input) tot en met de verwerking en de controle van de uitkomsten van de verwerking (output). Deze controle van de uitkomsten vindt in beginsel buiten de automatiseringsorganisatie plaats. De automatiseringsorganisatie controleert zelf de uitkomsten van de gegevensverwerking om vast te stellen dat de opgedragen werkzaamheden correct zijn uitgevoerd.
Naarmate de verwerkingsprocessen verdergaand worden geïntegreerd zal het aantal handmatige bewerkingen in en buiten de automatiseringsorganisatie progressief afnemen. Het basisdocument, het traditionele uitgangspunt voor de vaststelling van de juiste en volledige invoer, verdwijnt steeds vaker. De basisgegevens worden steeds frequenter direct in het systeem ingebracht, waarna de controle op plausibiliteit, aanvaardbaarheid, juistheid en blijvende volledigheid door de computer kan worden verricht, gevolgd door de eigenlijke verwerking. Ingeval bepaalde controlehandelingen door de computer worden verricht dient de noodzaak en omvang hiervan te worden gedefinieerd, om vervolgens te worden ingebouwd in de toepassingsprogrammatuur.

Het zal voor de verantwoordelijke gebruiker zichtbaar en controleerbaar gemaakt moeten worden.

Deze controle- en deels tevens beveiligingsmaatregelen zijn als het ware specifiek voor elk individueel systeem. De gebruikersorganisatie, die het systeem hanteert, zal haar eisen te dien aanzien duidelijk moeten stellen,

opdat zij in staat is de eindverantwoordelijkheid voor de juiste werking van het systeem te dragen. Er zal steeds sprake zijn van een samenstel van controlemaatregelen, waarvan uiteraard slechts een - zij het groot - deel aan de computer kunnen worden toevertrouwd. Indien zou worden besloten om in bepaalde gevallen alle controlemaatregelen naar "de automatisering" te verschuiven, wordt daarmee ook de beheersing van het systeem door de gebruiker en zijn verantwoordelijkheid voor de juiste verwerking aangetast, hetgeen uiteraard een onaanvaardbare verzwakking van de beveiliging zou inhouden. Anderzijds dient te worden opgemerkt, dat niet zelden een situatie wordt aangetroffen, waarbij de gebruiker niet in staat of bij machte is geweest zijn eisen kenbaar te maken en te doen realiseren. Dit leidt veelal tot qua betrouwbaarheid onbeheersbare systemen, waarbij kunstgrepen door de gebruikersorganisatie de leemten in het systeem zouden moeten opvullen, met alle risico's van dien.

De bouw van betrouwbare informatiesystemen is derhalve mede gebonden aan de voorwaarde dat zowel in de automatiseringsorganisatie als in de gebruikersorganisatie beschikt kan worden over voldoende deskundigheid op het gebied van de (administratieve) organisatie en van de interne controle. Voorwaarde hierbij is, dat de attitude van de topleiding ter zake van beheersing van systemen duidelijk is voor zowel de gebruikers als voor de automatiseringsorganisatie. Hierdoor weten de betrokkenen vooraf welke eisen in het algemeen worden gesteld, en dat een ieder medeverantwoordelijkheid draagt dat hieraan wordt voldaan.
Het ontbreken van door topmanagement goedgekeurde algemene eisen, kan en zal in vele gevallen leiden tot ontoereikende controlemaatregelen.

Een tweede zeer belangrijk aspect ter zake van de betrouwbaarheid van geautomatiseerde informatiesystemen is het op adequate wijze effectueren van bevoegdheden binnen de geautomatiseerde systemen. Voordat er sprake was van sterke integratie bleek uit basisdocumenten door middel van parafen en controletekens wie welke controlehandelingen had verricht op grond van schriftelijke (procedure)vastleggingen. Bij voortgaande integratie (bijvoorbeeld de uitwisseling van factureringsgegevens tussen leverancier en afnemer vindt plaats door middel van magneetband) wordt de organisatie als het ware gedwongen de bevoegdheden en beslissingsregels met betrekking tot bepaalde transacties respectievelijk transactiesoorten en de daarbij betrokken interne functies en externe lichamen in het geautomatiseerde systeem zelf vast te leggen. Het gebruik van het systeem zal alsdan bij uitsluiting aan bepaalde met name bekende functionarissen zijn toegestaan.
Dit leidt ertoe, dat met de nodige omzichtigheid van wachtwoorden, bevoegdheidstabellen en identificatiecodes gebruik moet worden gemaakt.

Ten behoeve van de bewaking van programmatuur, gegevens en gegevensstromen zijn een veelheid aan standaardpakketten op de markt, of worden aangeboden door leveranciers van computers en van besturings-software.

Bedoelde pakketten regelen de toegangscontrole tot gegevens, tot programmatuur, respectievelijk de vercijfering van gegevensstromen. In een aantal gevallen worden de faciliteiten niet als afzonderlijke pakketten aangeboden doch zijn deze in de functies van de beschikbare besturingsprogrammatuur opgenomen.
Het belang van deze pakketten is niet zozeer beschikbaarheid dan wel de optimale benutting van de mogelijkheden ter beheersing van de geautomatiseerde gegevensverwerking die deze bieden. Het laatste vergt van functionarissen in de organisatie een gedegen kennis van de mogelijkheden met een dergelijk pakket. In de praktijk blijkt evenwel dat de toepassing veelal niet dieper gaat, dan de voorbeelden die de leverancier in de documentatie heeft opgenomen, dan wel tijdens cursussen heeft gehanteerd, dit ten detrimente van de kwaliteit van de beveiliging.

Bij het gebruik van encryptie-technieken speelt uiteraard het sleutelbeheer een kritische rol in het geheel van de getroffen maatregelen. De organisatie van een onderneming dient vanzelfsprekend te voorzien in voldoende maatregelen van interne controle en beveiliging rond dit sleutelbeheer.
Het gebruik van encryptie-technieken is overigens niet voorbehouden aan grootschalige automatisering; ook gegevens op vaste schijven van microcomputers kunnen vóór opslag worden vercijferd.

Een nieuwe dimensie van problemen vormt de introductie van zogenaamde "Point of Sale"-systemen. Zoals bekend is bestaat de mogelijkheid in Zuid-Nederland bij een toenemend aantal benzinestations en op langere termijn in het gehele land af te rekenen door het invoeren van de eurocheque-kaart of bankpas voorzien van magnetische strip. Invoeren van de kaart in een lezer en vervolgens intoetsen van een personal identification number (pin) en de fiattering van het bedrag betekent dat het bedrag van de eigen bankrekening wordt afgeschreven en bijgescheven op die van de leverancier. Uiteraard zal te zijner tijd in allerlei winkels en warenhuizen op deze wijze kunnen worden afgerekend.
Bekend is dat leveranciers van computers zeer uitgebreid onderzoek verrichten naar de beveiligingsmogelijkheden van deze nieuwe vorm van betalingsverkeer, terwijl een aantal accountants betrokken is bij het beoordelen van de controle- en beveiligingsmaatregelen. Een niet te onderschatten probleem hierbij is het gedrag van de afnemer. Zolang deze niet doordrongen is van de gevaren aan zijn soms wat achteloos gedrag, zullen schades worden geleden. Een goede voorlichting ter zake lijkt noodzakelijk.

Het voorgaande zal duidelijk hebben gemaakt dat, hoewel het einde van de ontwikkeling van automatisering nog lang niet in zicht lijkt, de betrouwbaarheid van het systeem in overheersende mate afhangt van de organisatie en van het menselijk handelen (vanaf de opbouw tot en met het gebruik van systemen). Goede procedures binnen een doordachte organisatorische opzet, waarin de interne controle en de beveiliging zijn geïncorporeerd, vormen de basis van het betrouwbaar fungeren van een - overigens door de gebruiker geaccepteerd - informatiesysteem.

Fysieke beveiliging

De geautomatiseerde gegevensverwerking dient uiteraard omgeven te worden met een reeks maatregelen ter fysieke beveiliging. Ook hier zal het management uiteindelijk moeten beslissen in hoeverre maatregelen worden getroffen.

Door middel van fysieke beveiliging kan men de gebouwen, de installaties en apparatuur, de magneetbanden en -schijven waarop informatie is vastgelegd, de documentatie enz. zo goed mogelijk beschermen tegen brand, explosies, wateroverlast, diefstal en dergelijke.

Informatiedragers en documentatie behoren te worden opgeslagen in brandvrije, goed afsluitbare kasten, kopieën hiervan bij voorkeur in een ander gebouw. De toegang tot de gebouwen en in het bijzonder tot de ruimten waar de computer of daarop aangesloten in- en uitvoerstations staan opgesteld, dient behoorlijk te worden beveiligd. De in- en uitvoerstations zelf kunnen met een "sleutel" worden beveiligd. Langs deze weg wordt ook het gevaar van misbruik of sabotage verminderd. Zeer geavanceerde apparatuur en programmatuur is op de markt om een effectieve toegangscontrole tot computercentra te regelen. Daarbij kan worden zichtbaar gemaakt wie op welke momenten toegang tot welke ruimten hebben gevraagd.
Met name voor belangrijke gegevensverzamelingen kan tevens worden gedacht aan dubbele versluiting van de bewaarplaats, zoals bij een banksafe. Tot de groep van fysieke beveiligingsmaatregelen kan men voorts rekenen de aanwezigheid van een noodstroomvoorziening en een adequate, eventueel dubbel uitgevoerde airconditioning.

Een aantal van de hier bedoelde voorzieningen zal reeds vóór de bouw of het installeren van apparatuur moeten worden aangebracht omdat anders de kosten onevenredig hoog kunnen worden.

Een zwakke schakel in het geheel van te treffen fysieke beveiligingsmaatregelen blijft het personeel. Voortdurend blijkt dat ingeval de policy met betrekking tot beveiliging van computercentra niet wordt gedragen door het personeel (motivatie), de effectiviteit van de getroffen maatregelen in het geding is. Een noodzakelijk onderdeel van het beveiligingsbeleid dient ook hierbij te zijn in voldoende mate bekend maken van het beveiligingsbeleid en daarna het frequent testen van de werking van de aangebrachte voorzieningen en omtrent de uitkomsten van deze tests aan management te rapporteren.

Beveiliging van microcomputers

Wat de beveiliging van microcomputers en het gebruik ervan betreft zullen op deze plaats slechts enkele hoofdzaken de revue passeren.
Een probleem dat niet eenvoudig kan worden opgelost is het onrechtmatig kopiëren van programma's en gegevensverzamelingen bijvoorbeeld op diskette voor gebruik op een willekeurig andere microcomputer en het meenemen ervan

buiten het bedrijf ten behoeve van verkoop of illegaal gebruik. Tegen deze vorm van diefstal lijkt op dit moment weinig te doen.
De vraag is of het zelfs moet worden voorkomen nu er een tendens waarneembaar is naar steeds meer thuiswerken omdat de microcomputer via de telefoon kan worden verbonden met andere microcomputers in het bedrijf of het mainframe en het dus niet nodig is iedere dag naar de onderneming te gaan.

Het is van belang te onderstrepen dat degenen die bij een organisatie behoren als een goed huisvader/moeder met de apparatuur dienen om te gaan omdat het waardevolle machines betreft en als regel nog veel waardevoller informatie.

Een fenomeen dat inmiddels al niet meer is weg te denken uit het zakenleven is de zogenaamde elektronische brievenbus (electronic mailbox systems). Berichten van allerlei aard en formaat worden door de bezitters van microcomputers/personal computers, die voorzien zijn van een modem, in een elektronische brievenbus gezet en - indien bestemd voor henzelf - eruit gehaald. Een ongecontroleerde flow van berichten kan hiermede ontstaan.
Slechts ondersteund met discipline ten aanzien van de wachtwoorden kan worden gewaarborgd dat onbevoegden verkeerde berichten in handen krijgen of dat ondergeschikten te vroeg kennis krijgen van mededelingen, boodschappen en dergelijke die in eerste aanleg voor het management zijn bedoeld. Op de mogelijkheden het datacommunicatieverkeer en de opslag van gegevens te beveiligen door toepassing van data-encryption-technieken is hiervoor reeds ingegaan.

Selectie van beveiligingsmaatregelen

Om te kunnen bepalen welke maatregelen in een concreet geval getroffen dienen te worden, moeten de kosten worden afgewogen tegen het nut alsmede tegen niet op geld waardeerbare belangen en waarden. Het nut van de in aanmerking komende beveiligingsmaatregelen is gelegen in hun effectiviteit, in de zin van het verkleinen van de schadeverwachting in guldens op jaarbasis. Voor een goede vergelijking van kosten en nut is het gewenst ook alle kosten van beveiliging te herleiden tot jaarkosten. Daarbij kan worden aangetekend dat de specifiek aan beveiliging te relateren kosten van maatregelen soms gering zijn, omdat het vaak voorzieningen betreft die reeds voor een goed verloop van de lopende exploitatie zijn vereist.

Nu gaat het niet zozeer om het kiezen van één geïsoleerde maatregel maar wel om de selectie van een samenstel, een mix van maatregelen die ten dele overlappend zijn, maar elkaar anderzijds schragen en versterken. Het gevolg hiervan is dat het nut van zo'n samenstel in zijn totaliteit moet worden bepaald en niet als de optelsom van het nut van alle afzonderlijke maatregelen.
Vanzelfsprekend moet worden gezocht naar een zodanig samenstel van maatregelen, dat een optimale verhouding wordt bereikt tussen het niveau van beveiligingskosten en het nuttig effect.

Bij het schatten van nut en kosten spelen vele moeilijk af te wegen factoren een rol; er is een groot aantal maatregelen denkbaar, dat te zamen talloze combinatiemogelijkheden biedt. Het werkelijk optimum zal men dus wel nooit vinden; men moet zich tevreden stellen met het vinden van een zo goed mogelijke benadering van draagkracht, waarbij imponderabilia uiteraard meespelen.

Om te komen tot een zo goed mogelijk samenstel van beveiligingsmaatregelen, kan men het best beginnen met de aandacht te richten op het risico met de grootste schadeverwachting op jaarbasis.
Hiervan zal men nagaan welke maatregelen er zijn om de kans op schade te verkleinen (preventie) en welke maatregelen er zijn om bij eventueel toch voorkomende calamiteiten de omvang van de schade te beperken (signalering, bestrijding, noodvoorzieningen en reconstructie). Maatregelen met het grootste overschot van nut tegenover kosten worden gekozen.
Vervolgens wordt nagegaan, in hoeverre de gekozen maatregelen tevens leiden tot vermindering van de schadeverwachting uit hoofde van andere risico's. De aandacht wordt dan gericht op het risico met de grootste nog resterende schadeverwachting. Als ook hiervoor passende maatregelen zijn gekozen, herhaalt dit afwegingsproces zich totdat het niet langer mogelijk is maatregelen te vinden waarvan de effectiviteit in combinatie met de reeds gekozen maatregelen hoger ligt dan de kosten.

b. Detectie van inbreuken op computerbeveiliging

Signaleringsmaatregelen beogen het zodanig tijdig signaleren van onregelmatigheden dat de schade door snel ingrijpen zoveel mogelijk wordt voorkomen, althans binnen zekere grenzen blijft.
Signaleringsmaatregelen vormen een noodzakelijke aanvulling op de preventieve maatregelen, omdat deze uiteraard nooit volledige bescherming bieden.
Bij de mogelijke fysieke maatregelen moet vooral gedacht worden aan verschillende waarschuwingssystemen als brand- en rookmelders, alarminstallaties.
Hierop zal hier niet nader worden ingegaan evenmin als op sabotage en dergelijke.

De huidige computerapparatuur is doorgaans zo geconstrueerd dat storingen onmiddellijk door het besturingssysteem worden gesignaleerd. Daarnaast is afzonderlijke programmatuur beschikbaar voor het registreren van de activiteiten van het computersysteem.
Deze registratie kan men gebruiken om bepaalde ongewenste of van het normale patroon afwijkende activiteiten te signaleren.
Het signaleren van fouten door middel van geprogrammeerde controles behoort ook tot de categorie van signaleringsmaatregelen.

Voor zover de signalering van onregelmatigheden niet automatisch plaatsvindt door getroffen fysieke maatregelen of door middel van apparatuur of programmatuur, zullen controleprocedures moeten worden ontworpen om bepaalde onregelmatigheden te doen signaleren, bijvoorbeeld aan de hand van de gebruikte computertijd, de cijfermatige aansluiting tussen opeenvolgende met de computer vervaardigde overzichten en dergelijke.

Van belang is in elk geval dat de hulpmiddelen met inachtneming van de interne controle- en beveiligingsmaatregelen worden geïnstalleerd.

Voor detectie zijn nodig:
1. Een beleidsvisie van topmanagement ten aanzien van de beheersing van de organisatie, welke tevens voldoende moet zijn uitgedragen;
2. Maatregelen welke voorkomen, dat automatiseringsdeskundigen op grond van specifieke deskundigheid autonoom kunnen fungeren.

Beoordeling van de effectiviteit van getroffen maatregelen wijst uit, dat waarschijnlijk ook ten gevolge van onkunde zelfs voor de hand liggende beveiligingsmaatregelen niet worden genomen.

Wanneer geen sprake is van een adequaat stelsel van maatregelen van interne controle en beveiliging (adequaat impliceert preventie, detectie, signalering op toereikend niveau) kunnen op verschillende plaatsen leemtes in het stelsel van maatregelen voorkomen. In hoeverre getroffen maatregelen elkaar aanvullen, respectievelijk compenseren is dan niet bekend.

5. Meest voorkomende tekortkomingen in de computerbeveiliging

De uit de enquête, die in het najaar van 1986 in opdracht van de Commissie Computercriminaliteit door KMG Klynveld Kraayenhof & Co. is uitgevoerd, gebleken meest frequent voorkomende gebreken met betrekking tot computerbeveiliging kunnen als volgt worden samengevat:
1. het ontbreken van een duidelijk beleid ter zake. Risico-analyses als grondslag voor de opzet van een evenwichtig stelsel van computerbeveiligingsmaatregelen zijn eerder uitzondering dan regel;
2. onvoldoende functiescheiding in de automatiseringsorganisatie;
3. onvoldoende ondersteuning van de computerbeveiliging door de wijze waarop besturings- en andere software is geïnstalleerd. In dit verband speelt ook een rol van betekenis, dat de topleiding veelal niet in staat blijkt te zijn specialistische functies te beheersen;
4. onvoldoende kwaliteitscontrole op de bouw en wijziging van toepassingsprogrammatuur. Hierbij met name te denken aan kritische controle van programmatuur om te vermijden dat ongeoorloofde programmafuncties en dergelijke worden geïmplementeerd;
5. de geringe effectiviteit van interne controles verwerkt in toepassingsprogrammatuur, omdat deze geïsoleerd zijn getroffen of althans niet zijn ingebed in het stelsel van maatregelen;

6. slechte organisatie van de programma-overdrachtprocedure, waardoor toepassingsprogramma's in de test-, respectievelijk in de operationele fase door onbevoegden kunnen worden "benaderd". Het ontbreken/niet correct ingevoerd zijn van bibliotheekbeheersystemen speelt hierbij een cruciale rol;
7. hetzelfde geldt zeker ook voor de controle op de toegang tot gegevens. Vragen over deze problematiek zijn niet duidelijk beantwoord, hetgeen erop kan duiden, dat een "gevoelig" gebied is geraakt;
8. de functies interne controle en beveiliging zijn blijkens de gegeven antwoorden in beperkt mate aanwezig. De kwaliteit van de getroffen maatregelen blijkt duidelijk te lijden onder de afwezigheid van functies, die toezicht houden op de handhaving en naleving van het stelsel van controlemaatregelen;
9. het in veel gevallen ontbreken van - geteste - noodvoorzieningenplannen.

Niet duidelijk is geworden in hoeverre de problematiek van beheersbaarheid in het kader van zich in snel tempo ontwikkelende informatietechnologie tijdig wordt onderkend. Te denken valt hierbij aan de grote vlucht van het gebruik van microcomputer, de introductie van gelduitgifte-automaten en "point-of-sale" apparatuur.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Herfst 1987

GEINTEGREERDE GEGEVENSVERWERKING: STRUCTUUR VAN CONTROLE- EN BEVEILIGINGSMAATREGELEN IN EEN ADR/DATACOM DB-DC-OMGEVING

door J.A.W. Winterink en drs. R.G.A. Fijneman

1. Inleiding

In het in Compact 87/1 verschenen artikel "Geïntegreerde gegevensverwerking" ') worden vanuit een basisconcept de ontwikkelingen en invloeden als gevolg van toenemende geavanceerdheid van de automatisering behandeld, alsmede gevolgen ervan voor de interne controle.
Met het basisconcept als uitgangspunt wordt in dit artikel ingegaan op de structuur van controle- en beveiligingsmaatregelen die voor de beheersbaarheid van de gegevensverwerking in een ADR/datacom DB-DC omgeving zijn vereist.

Een beschrijving van de ADR-produkten, alsmede de (noodzakelijke) samenhang ertussen, vormt de grondslag voor de beschrijving van met behulp van deze produkten te realiseren interne controlemaatregelen. Aansluitend daarop wordt vervolgens geëvalueerd wat hiervan de betekenis is op de controle- en beveiligingsmaatregelen met betrekking tot respectievelijk de gebruikersorganisatie, de automatiseringsorganisatie en de organisatie van de automatisering.

Afsluitend wordt in een matrix weergegeven in welke mate de structuur van controle- en beveiligingsmaatregelen in een ADR/datacom DB-DC omgeving voldoet aan de in het basisconcept gedefinieerde eisen van interne controle voor het bereiken van de vereiste beheersbaarheid.

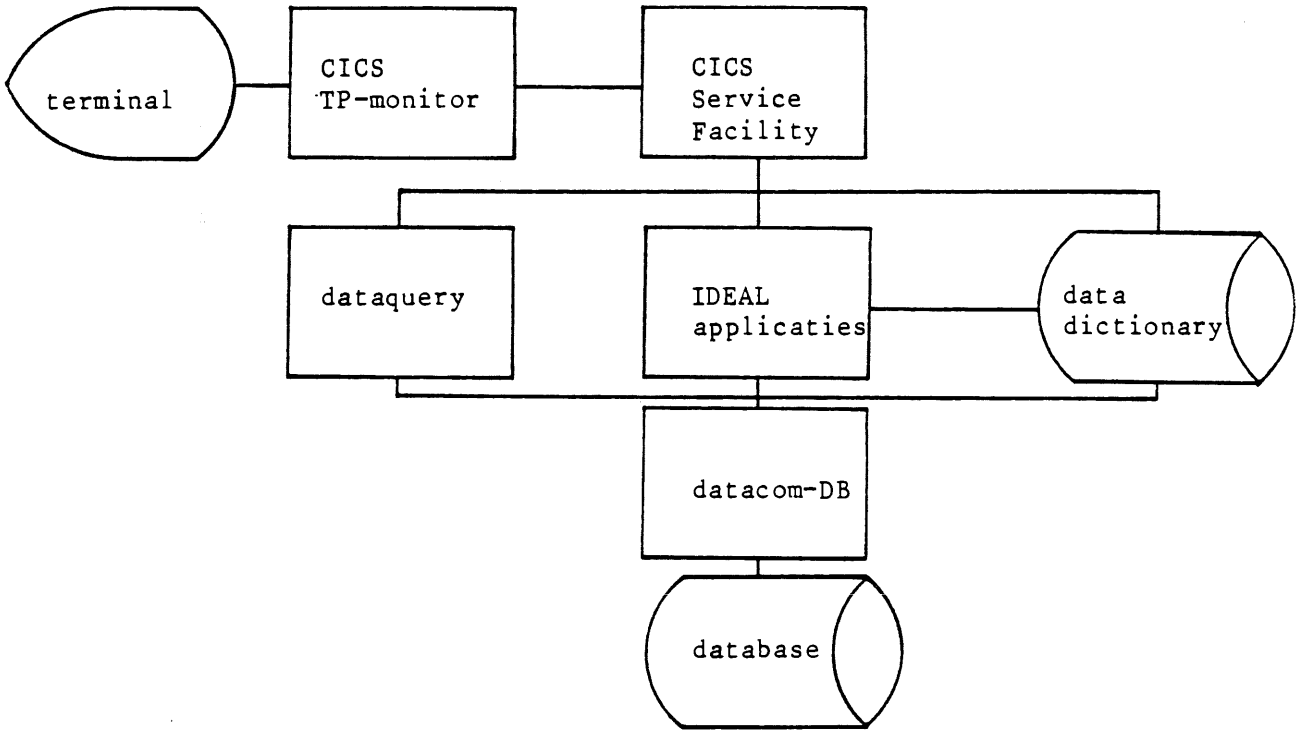
2. ADR-programmatuur

Applied Data Research (ADR), een dochteronderneming van de Amerikaanse multinational Ameritech, is één van de grote onafhankelijke software-leveranciers. In dit hoofdstuk wordt een beschrijving gegeven van de volgende pakketten die ADR met betrekking tot zijn DBMS-systeem ADR/datacom heeft uitgebracht:
- datacom-DB = Data Base Management Systeem (DBMS);
- datacom-DD = Data Dictionary;
- CICS service facility;

') Geïntegreerde gegevensverwerking" door drs. H.C. Kocks, Compact 87/1 nummer 44.

- IDEAL ') = applicatie ontwikkelsysteem;
- dataquery.

Deze programmatuur kan worden verwerkt onder MVS/XA, VSE/SP2 en multiprocessor-systemen. De samenhang tussen de pakketten kan als volgt worden weergegeven:



Figuur 1: Samenhang programmatuur

De beschrijving is gebaseerd op informatie, verkregen uit leveranciers-manuals, beschikbaar per eind 1986 en kennis verkregen bij cliënten die werken met ADR-programmatuur.

Datacom-DB

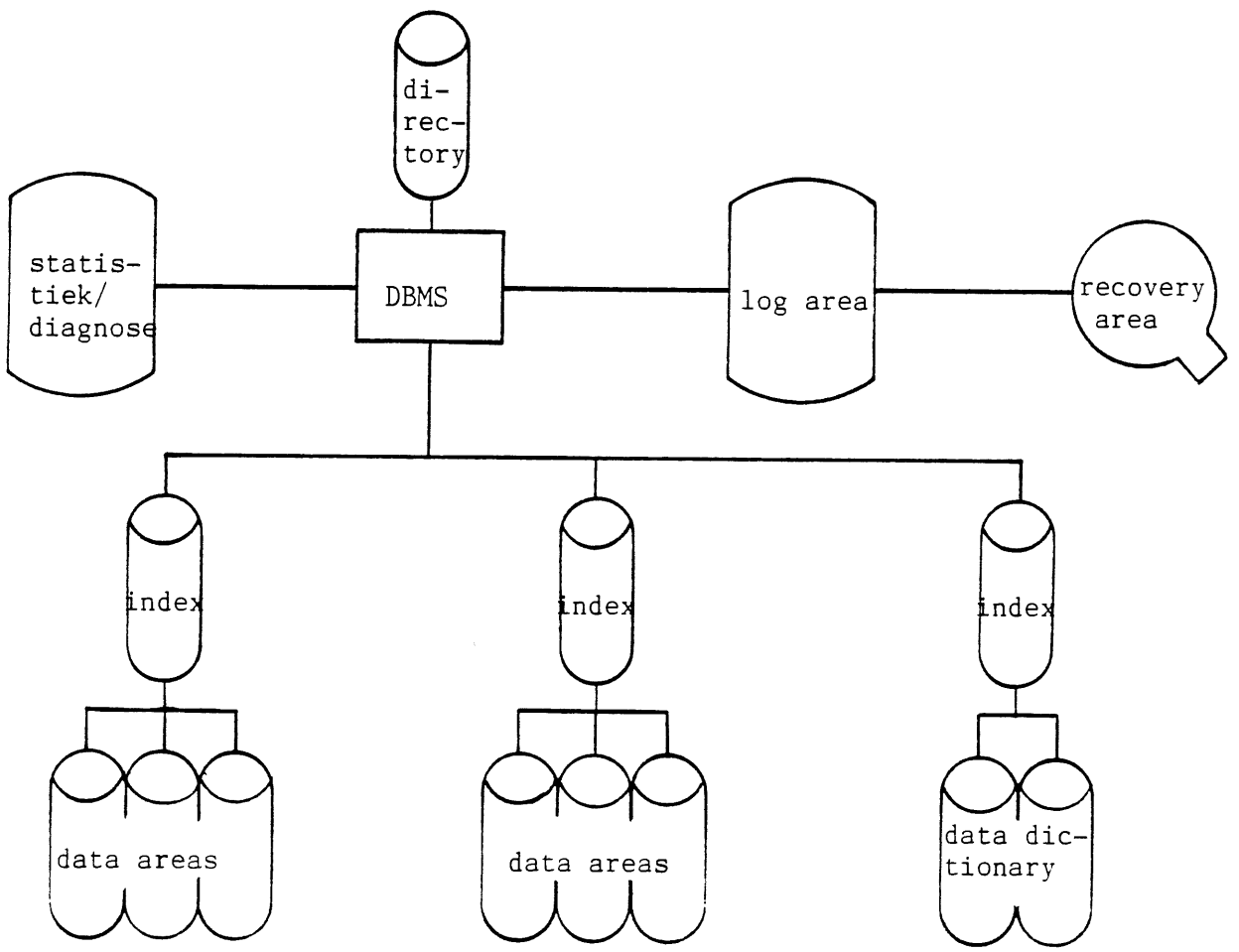
Datacom-DB, het Data Base Management Systeem (DBMS), is de centrale component in ADR's "Relational Information Management Environment". Het DBMS is gebaseerd op het relationele "flat file" concept en kan worden opgebouwd uit maximaal 999 databases (files) waarvan er één per definitie de Data Dictionary moet vormen.
Elke database kan uit maximaal 240 tabellen bestaan. Het aantal indices per database is maximaal 999.

') IDEAL
Ideal is het 4e-generatie ontwikkelsysteem dat een interactieve omgeving schept voor het ontwikkelen, onderhouden en uitvoeren van applicaties. Ideal wordt gebruikt onder de monitorfunctie van CICS en maakt gebruik van de data dictionary.

Hoewel datacom-DB dus een relationele database heet te zijn, is het feitelijk een tabellarisch georiënteerd DBMS en is het grotendeels gebaseerd op inverted file-technieken. Met behulp van indices per database wordt voor een snelle benadering van de gegevens gezorgd. In de index worden automatische relaties gelegd tussen records met overeenkomstige sleutels. De interrelatie tussen tabellen wordt gelegd op basis van sleutel-attribuutwaarde. Met behulp van de data dictionary/directory en de indices wordt random of sequentiële toegang verkregen op basis van een zoekargument.
Voor het uitvoeren van back-up en recovery-procedures werkt datacom-DB met log en recovery areas. In de log area vindt de logging voor alle veranderingen plaats aan de hand van before en after images. Regelmatig kan deze logging worden weggeschreven naar de recovery area (= tape), zodat in geval van calamiteiten logtapes ter beschikking staan voor het uitvoeren van herstelprocedures.

De logging in de statistiek- en diagnose-area bevat operationele statistieken om inzicht te krijgen in het functioneren van datacom-DB.

Functioneel kan datacom-DB als volgt worden weergegeven:



Figuur 2: Functionele elementen datacom-DB.

Datacom-DD

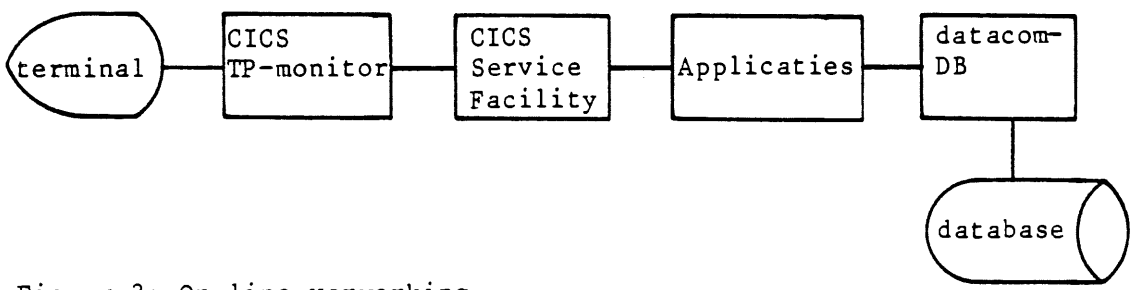
Het gebruik van de data dictionary is een vereiste voor het gebruik van zowel datacom-DB, als van IDEAL en dataquery. Daarnaast bevat de data dictionary de meta-data voor de gebruikersorganisatie, de organisatie van de automatisering en de automatiseringsorganisatie. Binnen een organisatie vormt het dus een centrale plaats voor de vastlegging en uitoefening van het beheer over de meta-data en de data.

In de data dictionary wordt door middel van het definiëren van gegevensentiteiten en relaties tussen de entiteiten het gegevensmodel voor de organisatie vastgelegd. Tevens kan de stuurinformatie voor de gehele gegevensverwerking in de data dictionary worden opgeslagen.

De data dictionary is actief, hetgeen inhoudt dat datacom-DD dynamisch het systeem onderhoudt en bewaakt. De "high-speed" directory daarentegen is semi-actief, hetgeen betekent dat aanpassingen in de data dictionary niet direct aan de directory worden doorgegeven. Deze aanpassingen dienen met een batch-functie te worden aangebracht, waarvoor adequate organisatorische maatregelen voorzien moeten zijn.

CICS Service Facility

Met behulp van de CICS Service Facility wordt datacom-DB de mogelijkheid geboden te werken met alle applicaties die werken onder de CICS teleprocessing monitor (IBM). De teleprocessing monitor beheert het verkeer van en naar de terminals. Het is de besturingsprogrammatuur die in een on-line-gegevensverwerkingssituatie de toegang tot de applicaties regelt.
Dit is schematisch weergegeven in figuur 3.



Figuur 3: On-line-verwerking

IDEAL

Ideal is het 4e-generatie ontwikkelsysteem dat een interactieve omgeving schept voor het ontwikkelen, onderhouden en uitvoeren van applicaties. Ideal wordt gebruikt onder de monitorfunctie van CICS en maakt gebruik van de data dictionary.

Dataquery

Dataquery is een vraagtaal die bestaat uit een eenvoudige set niet-procedurele commando's. Dataquery kan worden ingezet als middel om te kunnen voorzien in ad-hoc informatiebehoeften.

In tegenstelling tot wat de naamgeving van dit produkt doet vermoeden, kent dataquery een aantal update-mogelijkheden, namelijk:
a. toevoegen van records;
b. vervangen van records;
c. verwijderen van records.

De update-mogelijkheden kunnen centraal geheel worden afgeschermd, zodat gebruikers geen update-faciliteiten via dataquery worden gegeven.

3. Basisconcept interne controle

Om de beheersing van geïntegreerde gegevensverwerking te kunnen waarborgen, is een adequaat stelsel van interne controlemaatregelen vereist, dat deels in de beschikbare programmatuur en deels via organisatorische maatregelen gerealiseerd moet worden.

Uitgangspunt voor de evaluatie van de interne controlemaatregelen vormen de interne controledoelstellingen, waarvan straks in de conclusie wordt nagegaan of deze in een ADR/datacom-omgeving gerealiseerd kunnen worden.

De door ons gedefinieerde interne controledoelstellingen zijn:
- de juistheid, volledigheid en tijdigheid van data en meta-data moet tijdens de invoer, verwerking en bewaring gegarandeerd kunnen worden;
- de blijvende juistheid en volledigheid van data en meta-data moet controleerbaar zijn;
- de autorisatie tot het inbrengen, verwijderen, muteren en raadplegen van data en meta-data moet afdoende kunnen worden geregeld;
- de integriteit van de data en meta-data moet gewaarborgd blijven, ook als de verwerking ten gevolge van calamiteiten verstoord zou worden.

4. Interne controlemaatregelen in de ADR-programmatuur

De ADR-programmatuur biedt een aantal maatregelen om bepaalde aspecten van interne controle te realiseren.
Per beschreven onderdeel van de ADR-programmatuur zullen de aanwezige maatregelen uiteengezet worden, en worden gesteld tegen de ons inziens vereiste interne controlemaatregelen.
Als resultante blijven de maatregelen die in de organisatie dienen te worden getroffen respectievelijk in de applicatie.

In het kader van dit artikel is een uitputtende behandeling hier niet mogelijk. Alleen de belangrijkste maatregelen komen aan bod.

ADR/datacom-DB

Formele validiteitscontroles kunnen door het DBMS aan de hand van de beschrijving in de meta-data op een beperkte wijze worden uitgevoerd. Bovendien zijn er mogelijkheden aanwezig om per record de volledigheid van de in te voeren gegevens te kunnen garanderen.

Een van de risico's bij geïntegreerde gegevensverwerking is het voorkomen van concurrent update (meerdere gebruikers tegelijk willen hetzelfde record muteren). Datacom-DB heeft voor het voorkomen hiervan de faciliteit van de "exclusive control", hetgeen betekent dat een record pas na wijziging weer wordt vrijgegeven door de applicatie en pas dan weer voor andere gebruikers beschikbaar is. Datacom-DB verplicht echter niet tot het gebruik maken van deze faciliteit. Ingeval hiertoe om redenen van performance toch besloten mocht worden, dan betekent dit dat in de programmering van de applicatie deze maatregelen getroffen moeten worden.

Hiermee samenhangend kan een deadlock-situatie zich voordoen (twee applicaties/gebruikers wachten op elkaar). Signalering van deze deadlock is van essentieel belang. Daartoe is het noodzakelijk dat per applicatie een maximale verwerkingstijd wordt gedefinieerd. Het DBMS zal de overschrijding van deze tijd signaleren en de applicatie vervolgens afbreken, waarna de andere applicatie zijn verwerking kan vervolgen. Het DBMS kan dus alleen maar handelen, als in de applicaties de maximale verwerkingstijd wordt gedefinieerd. Met behulp van statistic reports (waarin opgenomen het aantal deadlocks, wachttijden en dergelijke) is het vervolgens mogelijk te komen tot een adequate beheersing en controle ten aanzien van optredende deadlocksituaties.

Datacom-DB beschikt over een back-up, recovery en restart-faciliteit. Essentieel is dat per tabel/file de logging-parameters (before en after images) door de data administrator gedefinieerd en door de database administrator (DBA) geïmplementeerd en bewaakt moeten worden. Checkpoints worden door het DBMS na het afronden van transacties automatisch gezet. Als checkpoints tijdens de transactieverwerking zijn vereist, dan is het noodzakelijk dat hierin door de applicatieprogrammatuur wordt voorzien. Deze checkpoints geven dan aan tot welk punt de verwerking van de transactie nog goed is verlopen. Bij een storing zorgt datacom-DB er vervolgens voor, dat de situatie wordt hersteld tot het laatst bevestigde check-point (transaction back-out aan de hand van de gelogde before-images). Daarna wordt de verwerking na autorisatie door de DBA weer opgestart.

Het handhaven van de referential integrity wordt door datacom-DB, evenals bij andere bekende relationele DBMS, niet dynamisch ondersteund. Als wijzigingen in gegevens het noodzaken dat mutaties in meerdere tabellen moeten worden doorgevoerd, dan zal hierin via de applicaties moeten worden voorzien. ADR beveelt gebruikers van haar programmatuur aan, een statische check uit te voeren op de integriteit van de tabellen door zogenaamde standaard "edit and validation" routines te koppelen aan die applicaties die mutaties in meerdere tabellen tegelijk doorvoeren. Via deze routines kunnen inhoudelijke controles, alsmede ook noodzakelijke control counts worden gedefinieerd. De routines kunnen door ADR niet standaard worden geleverd, maar zijn afhankelijk van het door de betreffende gebruiker gehanteerde gegevensmodel. Wijzigingen in het gegevensmodel noodzaken vaak ook tot aanpassingen in de routines.

ADR/datacom-DD

In de data dictionary moeten data-elementen, gebruikers, systemen en projecten gedefinieerd worden. Het DBMS zal steeds dwingend de data dictionary raadplegen alvorens toegang te verlenen tot het werken met applicaties en data.

De beschrijvingen van de meta-data in de data dictionary (DD), zijn voorzien van status- en versie-indicaties. Hierdoor is het voor de data administrator (DA) mogelijk om veranderingen in de meta-data te controleren.

Ook ten aanzien van de meta-data speelt het probleem van de referential integrity. Een velddefinitie is slechts binnen dezelfde tabel uniek en datacom-DD zorgt er niet voor dat de aanpassing in de meta-data in alle relevante tabellen automatisch wordt doorgevoerd. De DBA zal voor de aanpassing in alle tabellen moeten zorg dragen en de DA zal hierop aan de hand van het gegevensmodel in de DD controle moeten uitoefenen.

De high-speed directory is semi-actief. Wijzigingen real time doorgevoerd in de data dictionary worden niet automatisch doorgevoerd in de directory. Hiervoor is voor de directory een batch-functie beschikbaar. De consequentie hiervan is dat afwijkingen tussen de data dictionary en de directory kunnen optreden. Organisatorische procedures en een adequaat handelen van de DBA zullen het voorkomen van de afwijkingen tot het geringste moeten beperken.

De standaardentiteiten in de meta-data staan toe, dat zowel het conceptuele schema, het interne schema als het externe schema (3-schema-architectuur ANSI-SPARC) in de data dictionary worden vastgelegd. De aansluiting van deze schema's op elkaar wordt echter niet software-matig ondersteund. Via organisatorische maatregelen zullen dus waarborgen geschapen moeten worden om ervoor zorg te dragen dat de onderlinge aansluiting geregeld en bewaakt kan worden.

CICS service facility

De CICS service facility zorgt ervoor dat de CICS sign-on-tabel in datacom-DD beschreven kan worden. Per applicatie zal in de data dictionary tevens een user requirement-tabel gedefinieerd moeten worden, met daarin beschreven welke tabellen met data geraadpleegd en/of gewijzigd mogen worden. Bij het aanloggen wordt door CICS vervolgens vastgesteld of de gebruiker hiertoe bevoegd is. Tevens wordt met behulp van de CICS-log vastgelegd wie welk verzoek op welk moment heeft gedaan.

Via de CICS service faciliteit krijgen de applicaties die onder CICS werken toegang tot datacom-DB. De CICS service faciliteit biedt daarnaast mogelijkheden om bepaalde statistiekinformatie op te slaan en vervolgens te tonen (bijvoorbeeld aantal concurrent users, aantal verzoeken met I/O, wachttijden).

De DBA zal de CICS service faciliteit zorgvuldig moeten implementeren en gebruiken. De DA zal verantwoordelijk zijn voor de controle op de implementatie en het gebruik, alsmede op de wijzigingen die in de meta-data worden aangebracht.

IDEAL

Applicaties met behulp van IDEAL geschreven moeten gebruik maken van dataviews die in de data dictionary zijn opgenomen. Deze dataviews maken een beveiliging tot op elementniveau mogelijk (element = maximaal vier velden binnen een record). Voor niet IDEAL-applicaties geldt de beperking dat via de data dictionary slechts een beveiliging tot op record-niveau is te realiseren. Eventuele verdere beperkingen zullen per applicatie moeten worden gedefinieerd en geprogrammeerd.

Binnen IDEAL worden voorts verschillende functies onderkend die in de ontwikkelomgeving een beheerst gebruik van de daar ter beschikking staande mogelijkheden moeten garanderen.

Essentieel is dat IDEAL geen mogelijkheden biedt om de toegang tot de program source, program object en program load versies van de programmatuur op een adequate wijze te beveiligen. Hiervoor is ondersteuning met behulp van een toegangsbeveiligingspakket aan te bevelen.

Dataquery

Dataquery kent een geheel eigen wijze van beveiligen en maakt daarmee een beveiliging tot op veldniveau mogelijk. Zowel de in de data dictionary gedefinieerde velden als de gebruikers krijgen ieder hun eigen profielcodes toegekend. Een gebruiker is bevoegd tot gebruik (raadplegen en/of wijzigen) van het veld als zijn profielcode overeenkomt met die van het veld.

De beschreven beveiliging bij IDEAL laat - zoals duidelijk mag zijn - geen 1 op 1 vertaling toe op de situatie bij dataquery. De gebruikers van ADR-programmatuur moeten zelf in mogelijkheden voorzien om de beveiliging vanuit één centraal autorisatieprofiel op een uniforme wijze voor beide produkten te realiseren.

Zoals reeds eerder bij de produktbeschrijving gememoreerd is, biedt dataquery ook mogelijkheden tot het wijzigen van data. Deze mogelijkheid dient vermeden te worden en kan centraal (DBA) onmogelijk gemaakt worden. Enquiry-beveiliging is evenmin in een batch-omgeving goed te realiseren. Dataquery zal alleen real time/on line (RT/OL) voor enquiry-mogelijkheden ter beschikking moeten worden gesteld. De data administrator zal hierop door middel van adequate controlemaatregelen moeten inspelen en een effectieve controle mogelijk moeten maken.

5. Organisatorische interne controlemaatregelen

In dit hoofdstuk zal nader worden ingegaan op de betekenis van de ADR-programmatuur voor de organisatie en de organisatorische maatregelen die daarvoor vereist zijn.

Gebruikersorganisatie

In het reeds gememoreerde artikel "Geïntegreerde gegevensverwerking" wordt een aantal keren gesproken over de verbijzonderde functie gegevensbeheer (data administration) in de gebruikersorganisatie. De belangrijkste taken van de DA-functie zijn:

- geven van richtlijnen met betrekking tot het gegevensgebruik, die dan door de database administrator moeten worden uitgevoerd;
- zorgen voor controle op naleving van de voorschriften.

De verbijzonderde functie gegevensbeheer op een hoog niveau in de organisatie is voor de verdere beschrijving als uitgangspunt genomen. Deze functie zal de beveiligingsmaatregelen moeten treffen, die ervoor zorg dragen dat de essentiële functiescheidingen in de gebruikersorganisatie effectief zijn en blijven.

Gegevensbeheer zal primair het conceptuele gegevensmodel moeten definiëren en opstellen (vastlegging in de data dictionary). De vertaling en implementatie van het conceptuele gegevensmodel naar het interne schema en het externe schema door de automatiseringsorganisatie, zal door gegevensbeheer nauwgezet gecontroleerd en bewaakt moeten worden (test-, acceptatie- en overdrachtsprocedures). Informatie uit de data dictionary op basis van status/versie indicatie is hiervoor essentieel. Voor de vertaling en implementatie van het conceptuele gegevensmodel kan niet gebruik worden gemaakt van

het DBMS. De overeenstemming tussen conceptueel, intern en extern schema zal door gegevensbeheer afzonderlijk moeten worden vastgesteld.

Gegevensbeheer zal tevens waarborgen moeten scheppen voor het opstellen en implementeren van uniforme autorisatieprofielen bij gebruik van IDEAL en dataquery. Beide pakketten kennen een eigen wijze van beveiliging inzake de toegang tot data, zodat het raadplegen van het uniforme autorisatieprofiel via aanvullende maatregelen zal moeten worden afgedwongen. Het DBMS bezit hiervoor zelf geen faciliteiten.

Het bewaken van de "referential integrity" van de data en de meta-data is een grote zorg voor de functie gegevensbeheer. ADR biedt hiervoor geen standaardoplossing, zodat gegevensbeheer zelf "edit and validation" routines zal moeten definiëren en vaststellen, die garanderen dat data die in meerdere tabellen zijn opgenomen consistent blijven. Elke aanpassing in het gegevensmodel zal daarbij moeten leiden tot aanpassingen in de "edit and validation" routines.

Tevens zal gegevensbeheer eisen stellen ten aanzien van de beschikbaarheid van data en meta. De DBA zal met gebruikmaking van het DBMS hierin moeten voorzien. Gegevensbeheer zal vervolgens moeten vaststellen dat de geïmplementeerde maatregelen voldoende zijn en regelmatig testen of ze ook juist en volledig worden uitgevoerd.

Automatiseringsorganisatie

De automatiseringsorganisatie heeft als doelstelling het volgens gebruikersnormen uitvoeren van opgedragen taken, hetgeen primair inhoudt:
- uitsluitend verwerking met geautomatiseerde programmatuur en de juiste bestanden;
- het bewaren van gegevens.

De gebruikersorganisatie "definieert" wat geautomatiseerd wordt en met welke randvoorwaarden dat moet worden omgeven (zie onder andere de functie gegevensbeheer). De "vertaling" en "implementatie" van het gedefinieerde naar applicaties en overkoepelende systeem-software zal voor rekening van de automatiseringsorganisatie komen.

In de automatiseringsorganisatie speelt de DBA (Data Base Administrator) een centrale rol bij het vertalen en implementeren van de door gegevensbeheer gedefinieerde eisen, hierbij gebruik makend van de mogelijkheden die de ADR-programmatuur hem hierbij bieden.

De volgende taken zijn onder andere voor de DBA van groot belang:
- vertalen van het conceptueel schema naar het extern en het intern schema (vastleggen in de data dictionary);
- adequate definiëring van de back-up, logging en recovery-parameters in datacom-DB;

- implementeren van de vereiste maatregelen voor exclusive control, alsmede voor het voorkomen en signaleren van deadlock-situaties;
- garanderen dat gebruikers zowel voor IDEAL als voor dataquery van hetzelfde autorisatieprofiel gebruik maken.

Het belang van deze taken is door ADR onderkend en er is een goede "technische" DBA-documentatie beschikbaar om duidelijk te maken welke maatregelen met welke hulpmiddelen "hoe" kunnen worden gerealiseerd. De essentiële beveiligingsmaatregelen worden behandeld, maar zijn slechts op willekeurige plaatsen in de documentatie terug te vinden.

Organisatie van de automatisering

De hoofddoelstelling van de organisatie van de automatisering is het ontwikkelen van efficiënte en betrouwbare informatiesystemen, die moeten voldoen aan de door de gebruikers gestelde normen (geheimhouding, betrouwbaarheid, continuïteit, privacy, controleerbaarheid etc.).

Deze normen kunnen alleen worden gehaald als wordt uitgegaan van een "zuivere" ADR/datacom-omgeving. Hieronder verstaan we dat alle applicaties in IDEAL worden ontwikkeld, het gebruik van dataquery voor ad-hoc-informatiebehoeften wordt toegestaan en dit alles functioneert onder beheer van datacom-DB en datacom-DD. Applicaties niet functionerend onder deze hulpmiddelen mogen niet worden toegestaan.

6. Conclusie

Vatten wij de bevindingen van het onderzoek samen, dan blijkt, dat in opzet de structuur van de interne controle- en beveiligingsmaatregelen een beheersbare gegevensverwerking in een ADR/datacom-omgeving mogelijk maakt. Essentiële voorwaarden hierbij zijn:
- uitgaan van een "zuivere" ADR/datacom-omgeving;
- het realiseren van organisatorische maatregelen, zoals met name in hoofdstuk 5. beschreven.

In figuur 4 is in matrixvorm weergegeven op welke wijze interne controle- en beveiligingsdoelstellingen kunnen worden bereikt, met gebruikmaking van ADR-programmatuur en de daarvoor vereiste organisatorische maatregelen.

Compact is een uitgave van

KPMG-Klynveld EDP Audit Services

Figuur 4.

Interne controle-doelstellingen	Interne controle-maatregelen	ADR-produkten						ORGANISATIE					
								Gebruikers-organisatie			Automatiserings-organisatie		
		Datacom-DB	Datacom-DD	CICS S.F.	Ideal appl.	Dataquery	DA	AA	Gebruiker	DBA	SO	Produktie
1. Bevoegdheid												
- toegangsbeveiliging data		x	x	x	x	x		1		2	2	3
- toegangsbeveiliging meta-data		x	x	x			1			2		3
- geheimhouding data		x	x	x	x	x		1		2	2	3
- geheimhouding meta-data		x	x	x			1			2		3
2. Betrouwbaarheid												
- juistheid data			x		x	x			1		3	3
- juistheid meta-data		x	x				1			2		3
- volledigheid data			x		x	x			1		3	3
- volledigheid meta-data		x	x				1			2		3
- tijdigheid data			x		x	x			1		3	3
- tijdigheid meta-data		x	x				1			2		3
3. Continuïteit												
- back-up		x		x			1	1		2		3
- logging		x		x			1	1		2		3
- recovery en restart		x		x			1	1		2		3
4. Controleerbaarheid												
- meta-data			x				1			2		
- applicaties					x			1			2	
- bevoegdheidsmaatregelen			x				1	1		2	2	
- betrouwbaarheidsmaatregelen					x		1	1		2	2	
- continuïteitsmaatregelen		x					1	1		2	2	
- gegevensverwerking		x	x	x	x	x	1	1		2	2	3

1 = definiërend/controlerend
2 = implementerend/vertalend
3 = uitvoerend

Herfst 1987

BELANGRIJKE FUNCTIES VAN EEN TOEGANGSBEVEILIGINGSPAKKET

door M.C. Duym

Inleiding

Dit artikel behandelt de functionele eisen die aan een toegangsbeveiligingspakket gesteld moeten worden. Na een opsomming en korte toelichting van de eisen wordt eerst ingegaan op de registraties (bestanden) die het pakket voor haar functioneren nodig heeft. De beschrijving van de inhoud van een aantal van deze bestanden dient namelijk als basis voor een verdere uitdieping van het functionele eisenpakket.

Doel van een toegangsbeveiligingspakket

Een toegangsbeveiligingspakket heeft tot doel de toegang tot bestanden alleen te verlenen door middel van aan bepaalde gebruikers verleende toegangsrechten.

Ten aanzien van de toegangsrechten kan een onderscheid worden gemaakt in de rechten die betrekking hebben op het te benaderen bestand (bestandsrechten) en die betrekking hebben op andere bestanden en systeemcomponenten door middel waarvan deze gegevens kunnen worden geraadpleegd (routerechten).

Voor een goed begrip van dit artikel een nadere specificatie van de andere in deze alinea gehanteerde begrippen:
1. bestanden. Het betreft zowel gegevensbestanden, bronprogramma's, objectprogramma's, JCL-procedures en dergelijke;
2. gebruikers. Een toegangsrecht kan alleen aan een gebruiker worden toegekend en niet aan een proces. Een proces kan alleen een van een bepaalde gebruiker afgeleid toegangsrecht verkrijgen;
3. systeemcomponenten. Hieronder vallen fysieke terminals, logische terminals, schijfeenheden, tape units en dergelijke.

Functionele eisen

Ter verwezenlijking van het geformuleerde doel moet een toegangsbeveiligingspakket voldoen aan de volgende eisen:
1. toegangsbeveiliging dient een standaardfunctie te zijn van het besturingssysteem. Indien dit niet het geval is dient het toegangsbeveiligingspakket de integriteit van het besturingssysteem niet aan de tasten. Dit kan worden aangeduid met "goede gast";
2. programmatuur en bestanden van het toegangsbeveiligingspakket kunnen alleen door middel van de daartoe aangewezen personen en hulpmiddelen worden geïnstalleerd en onderhouden. Zelfbescherming;

3. het pakket moet uitgaan van de filosofie: niets mag;
4. toegang tot de bestanden kan alleen worden verkregen door middel van het toegangsbeveiligingspakket. Het alleenrecht;
5. de gebruikersidentificatie moet de kans op misbruik minimaliseren. Legitimatie;
6. het toegangsbeveiligingspakket moet zich ervan vergewissen dat degene die zich heeft gelegitimeerd ook werkelijk van het systeem gebruik maakt en dit ook als enige blijft doen. Surveillance;
7. gebruikers moeten bij de beveiliging worden betrokken. Participatie;
8. integrale en uitzonderingsrapportage ten aanzien van status en gebruik van de bevoegdheden. De verantwoording;
9. gebruikers, bestanden en systeemcomponenten die niet meer bestaan moeten direct worden verwijderd. De bijbehorende toegangsrechten moeten direct worden verwijderd. Realiteit;
10. de toegang van individuele gebruikers dient gecontroleerd te kunnen worden. Doorwerking;
11. koppeling met bibliotheeksysteem waardoor alle bestanden en hun generaties met hun volledige naam, ongeacht het opslagmedium, kunnen worden beveiligd. Bestandsspecificatie.

In het voorgaande is geen eis ten aanzien van de volledigheid van bestanden, systeemcomponenten en gebruikers gesteld. Deze is namelijk impliciet verwoord door de eisen ten aanzien van niets mag (3) en alleenrecht (4).

Naast bovengenoemde criteria, die alle betrekking hebben op de kwaliteit van de beveiliging, zijn er ook nog een aantal eisen te stellen ten aanzien van het gebruiksgemak. Deze zijn essentieel voor acceptatie en gebruik en als zodanig indirect van belang voor de kwaliteit van de beveiliging. Deze zijn:
12. mogelijkheid tot aansluiting aan de organisatiestructuur. Maatwerk;
13. mogelijkheid tot het opdelen van het beheer van toegangsregels en andere door het pakket bijgehouden registraties. Gedistribueerd beheer.

De bestanden van het toegangsbeveiligingspakket

Het toegangsbeveiligingspakket is een samenstel van een aantal logische bestanden. Gegroepeerd naar type zijn dit:
1. programmabestanden:
   a. het toegangsbeveiligingssysteem;
   b. de installatieprogramma's.
2. JCL-bestanden:
   a. installatie JCL;
   b. JCL voor Initial Program Load (IPL).
3. stuurbestanden:
   a. statische. Deze bevatten informatie die alleen tijdens installatie wordt geraadpleegd;

b. dynamische. Deze bevatten informatie die tijdens de verwerking wordt geraadpleegd.

4. gegevensbestanden:
   a. gebruikers;
   b. bestanden;
   c. systeemcomponenten;
   d. toegangsrechten.

Gegevensbestanden

Hieronder worden de genoemde bestanden 4.a. tot en met d. nader uitgediept.

ad a. gebruikers

Gegroepeerd naar het gebruiksdoel, betreft de informatie die over een gebruiker moet worden opgeslagen:

1. identificatie. Een unieke gebruikersidentificatie moet aanwezig zijn. Deze dient zoveel mogelijk de bevoegdhedenstructuur van de organisatie te weerspiegelen waardoor groepering van de toegangsrechten mogelijk wordt. Definitie en beheer worden hierdoor sterk vereenvoudigd;
2. authenticatie. Hiertoe behoort minimaal een wachtwoord, minimale en maximale geldigheid wachtwoord en wachtwoordhistorie;
3. classificatie. Bepaalt welke status de gebruiker heeft ten opzichte van het toegangsbeveiligingspakket. Betreft het een gewone gebruiker, een beveiligingsbeambte, een accountant enz.;
4. communicatie. Telefoonnummer, interne postcode, verantwoordelijke chef en dergelijke;
5. gebruiksgegevens. Gebruikspatroon, tijd en bron laatste toegang, aantal overtredingen, laatste wachtwoordwijziging, datum en tijd laatste overtreding;
6. schonen. Wanneer verlopen de rechten van de gebruiker.

ad b. bestanden

Deze informatie hoeft alleen identificerend te zijn.

ad c. systeemcomponenten

Er zijn veel typen componenten mogelijk; Afhankelijk van het type kunnen vastgelegd worden:

1. fysieke identificatie. Een eventueel hardware-matig aanwezig identificatienummer;
2. logische identificatie. Een door middel van configuratie toegekend nummer;
3. locatie. Plaats waar de component zich bevindt;
4. gebruikstijd. De tijd waarin de component gebruikt mag worden.

ad d. toegangsrechten

De specificatie van een toegangsrecht moet minimaal de mogelijkheid hebben tot het opnemen van de volgende gegevenselementen:

1. identificatie object. De identificatie van het bestand waarvoor het recht geldt;
2. identificatie rechthebbende;
3. route;
4. bevoegdheid. Nader te verdelen in:
   a. type toegang. Een onderscheid moet gemaakt kunnen worden tussen Lezen, Schrijven, Wissen, Kopiëren, Hernoemen, Uitvoeren;
   b. de tijd waarin de gebruiker over het object mag beschikken.

Functionele eisen

Hierna worden de in het begin van dit artikel kort weergegeven functionele eisen nader toegelicht.

1. Goede gast

In geval het toegangsbeveiligingspakket geen onderdeel uitmaakt van het besturingssysteem of in het besturingssysteem geen voorzieningen zijn opgenomen voor integratie met dat pakket, moet het beveiligingspakket zodanig kunnen worden geïntegreerd, dat hierdoor de integriteit van het besturingssysteem gewaarborgd blijft.

In een dergelijke situatie zal uitzonderlijke zorg moeten worden besteed aan de implementatie.

2. Zelfbescherming

De beste bescherming vormt het versleutelen van de gegevens. Minimale eis is, dat de wachtwoorden eenzijdig versleuteld zijn. Een andere maatregel is het niet in het interne geheugen houden van onversleutelde toegangsrechten ten behoeve van snelle validatie. Ervan uitgaande, dat geen enkel beveiligingssysteem 100% waterdicht is, wordt hierdoor voorkomen dat tijdelijk een hogere bevoegdheid wordt verkregen.

3. Niets mag

Als de eis "niets mag" niet wordt gesteld kan eigenlijk om twee redenen niet van een toegangsbeveiligingspakket worden gesproken.

Namelijk omdat:
1. via onbeveiligde bestanden met name van het type programma, door de altijd wel aanwezige zwakke plekken in het besturingssysteem en/of toegangsbeveiligingssysteem, beveiligde bestanden kunnen worden gecompromiteerd;
2. dan via procedures moet worden bewaakt welke bestanden wel en welke niet beveiligd moeten worden. Gezien de hoeveelheid bestanden is de kans groot, dat abusievelijk bestanden buiten de beveiliging blijven.

4. Alleenrecht

Indien het toegangsbeveiligingspakket gebruikt wordt naast andere beveiligingsmechanismen ontstaat geen eenduidige rapportage over status en gebruik van bestanden. Tevens is er een groot gevaar dat ten aanzien van bestanden geen of geen volledige toegangsrechten zijn gedefinieerd.

5. Legitimatie

Het wachtwoordmechanisme moet voldoen aan de volgende eisen:
1. controle op minimum lengte van het wachtwoord benodigd voor voldoende unieke combinaties;
2. controle op afwisselend letter- en/of cijferpatroon van wachtwoord;
3. minimale geldigheidsduur ter voorkoming van direct weer ongedaan maken van door maximale duur verplichte wijziging;
4. maximale geldigheidsduur om het risico van bekend raken te verkleinen;
5. een geheugen voor een aantal voorgaande wachtwoorden om herhaling tegen te gaan of toepassing van een wachtwoordgenerator.

Een wachtwoordmechanisme en de mogelijkheid tot het vastleggen van een verplicht inlogpunt is het minimale waarover een toegangsbeveiligingspakket moet beschikken. Uitbreiding van de authenticatie door middel van badge, stem, iris en dergelijke kan gegeven de bedrijfswaarde van de gegevens wenselijk zijn.

6. Surveillance

In het intermenselijk verkeer kijken wij niet alleen naar de legitimatiepapieren maar ook naar het gedrag. Gedraagt men zich overeenkomstig het patroon van het type persoon waartoe men via de legitimatie kan worden ingedeeld? Een toegangsbeveiligingspakket kan door middel van het vastleggen van het gebruikspatroon van de verschillende toegekende rechten een significante afwijking signaleren en melden aan de beveiligingsverantwoordelijke.

Tevens moet worden voorkomen, dat het systeem niet door anderen kan worden gebruikt, doordat het medium waarmee toegang is verkregen onbewaakt open blijft voor invoer. Uitschakelen na het ontbreken van invoer gedurende een bepaalde tijd is daarom noodzakelijk.
Voor een effectieve surveillance is het noodzakelijk dat de mate waarin meldingen plaatsvinden per gebruiker kan worden ingesteld. Dit geldt met name voor de mogelijkheid tot het registreren of melden van het feit dat een bepaalde gebruiker aanlogt en van bepaalde rechten gebruik maakt.

7. Participatie

Naast de gebruiksvriendelijkheid is participatie van de gebruiker noodzakelijk voor het goede gebruik en werking van het beveiligingssysteem. Het gebruik van het pakket moet worden geëffectueerd door acceptatie ervan in de organisatie. Deze beveiligingsattitude moet binnen de organisatie gekweekt worden.
Mechanismen daarvoor zijn:
1. melding van de laatste log-on met plaats waarvan;
2. overzicht van eigen en verleende toegangsrechten.

8. Verantwoording

De status van het beveiligingssysteem moet altijd kunnen worden geraadpleegd. Inzicht moet kunnen worden gegeven in:
1. de statische en dynamische stuurinformatie;
2. welke bevoegdheden hebben één of meer gebruikers;
3. welke gebruikers hebben toegang tot één of meer bestanden en op welke wijze.

Ten aanzien van het gebruik van bevoegdheden is informatie nodig over:
1. foutieve aanloggingen per periode per gebruiker;
2. gebruikers die ongeautoriseerd hebben geprobeerd toegang te krijgen per periode per bestand;
3. bestanden waartoe ongeautoriseerd is geprobeerd toegang te krijgen per periode per gebruiker.

9. Realiteit

Het systeem moet een afspiegeling blijven van de actuele organisatie, de op het computersysteem aanwezige bestanden en de systeemcomponenten die in gebruik zijn. Organisatorische procedures zijn hierbij onontbeerlijk. Het pakket moet deze echter zoveel mogelijk ondersteunen ter bewaking van de juistheid van de toegangsregels.

Per genoemd object moet het toegangsbeveiligingspakket beschikken over een reeks faciliteiten. Voor wat betreft:

1. gebruikers:
   a. specificatie van een uiterste geldigheidsdatum van de toegangsregels. Doel: vooraf inbrengen vertrekdatum;
   b. rapportage van gebruikers die een aantal dagen geen gebruik van het systeem hebben gemaakt. Doel: ontdekken van uit dienst getreden personeelsleden, vakanties en langdurig zieken.
2. bestanden. Regelmatig doorlopen van de bibliotheken en nagaan welke toegangsrechten gespecificeerd zijn ten aanzien van niet meer aanwezige bestanden. Toegangsregels voor bestanden waarvoor in geen van de toegangsrechten een aanmaakbevoegdheid is gespecificeerd zouden direct voor verwijdering aangemerkt kunnen worden;
3. systeemcomponenten. Regelmatig doorlopen van de systeemtabellen en nagaan in welke toegangsregels systeemcomponenten zijn opgenomen die niet meer aanwezig zijn.

10. Doorwerking

Transactieverwerkende pakketten als CICS en database-pakketten als IMS en IDMS worden door de systeemprogrammatuur als één geheel gezien. De individuele gebruikers zijn hierin door de systeemprogrammatuur niet te herkennen. De aanduiding voor deze systemen is Multiple User Single Address Space Systems. Om toch toegangsbeveiliging op gebruikersniveau te realiseren moet het toegangsbeveiligingspakket met dergelijke MUSASS kunnen samenwerken.

Vanwege het door de systeemprogrammatuur als één geheel zien van een dergelijk pakket is het technisch in vele gevallen onmogelijk een controle uit te voeren op het moment van bestandstoegang. Vandaar dat toegangsbeveiliging moet worden geëffectueerd door het afschermen van de toegang tot andere objecten. Bijvoorbeeld:

1. transacties;
2. transactiewachtrijen;
3. gebruik deelbeschrijving database.

11. Bestandsspecificatie

Diverse opslagmedia bieden onvoldoende ruimte om de volledige bestandsnaam te registreren. Een bekend voorbeeld is de naam op een tapelabel in een IBM MVS-omgeving. In dit label is plaats voor een bestandsnaam van 17 posities. MVS staat echter bestandsnamen toe tot 40 posities.

Voor het organiseren van bestanden wordt door de meeste besturingssystemen een boomstructuur gehanteerd. Een bestandsnaam is daarom veelal opgebouwd uit de namen van takken waaronder het bestand zich bevindt met als laatste

de eigenlijke naam. Beperking van de lengte betekent daarom een automatische groepering van bestanden en daarmee van de toegang daartoe. Dit kan in sommige situaties ongewenst zijn.

Ook uit hoofde van een goede bedrijfsvoering is een op een dergelijke wijze bepaalde naam een crime. Vandaar dat de bibliotheeksystemen die voor een dergelijk besturingssysteem worden aangeboden, veelal de mogelijkheid bieden wel de volledige naam te gebruiken. Een dergelijk bibliotheeksysteem schrijft dan niet in het label de eigenlijke bestandsnaam, maar bijvoorbeeld een nummer en houdt in een eigen registratie de volledige naam bij.

Het zal duidelijk zijn, dat een toegangsbeveiligingssysteem in dergelijke situaties moet voorzien in een koppeling met het bibliotheekpakket om de toegang tot bestanden op dergelijke media te kunnen bewaken.

12. Maatwerk

Organisatiestructuur en bevoegdheden lopen in vele gevallen tot op grote hoogte parallel. Een goed toegangsbeveiligingspakket speelt hierop in, waardoor het aantal te specificeren toegangsregels wordt geminimaliseerd.

Dit gebeurt door het ontkoppelen van de code waarmee de gebruiker zich bij de aanlogprocedure bekend maakt (logon-id) en de code die dient als identificatie ten behoeve van de specificatie van toegangsrechten (user-id). De logon-id die, samen met bijvoorbeeld een wachtwoord moet worden onthouden, is qua lengte beperkt. De user-id hoeft dit niet te zijn. Hierdoor kunnen in de user-id bijvoorbeeld de namen van de divisie, afdeling, bureau en sectie waar de gebruiker werkt worden opgenomen.

Wordt anderzijds in de naamgeving van de bestanden goed de functie waarvoor deze wordt gebruikt opgenomen, dan is eenvoudige specificatie van toegangsrechten mogelijk met behulp van maskers.

13. Gedistribueerd beheer

Ten aanzien van het gebruik van het toegangsbeveiligingspakket is een minimale functiescheiding noodzakelijk om te voorkomen dat iemand zichzelf autoriseert. Scheiding in functies is nodig ten aanzien van:

1. installatie van het pakket;
2. toevoegen, wijzigen en verwijderen van toegangsrechten;
3. toevoegen, wijzigen en verwijderen van bevoegde gebruikers;
4. controle op de werking en afhandelen van de gemaakte overtredingen;
5. controle op de werking van alle bovengenoemde functies.

Naast een scheiding tussen de verschillende taken moet binnen een taak ook een scheiding mogelijk zijn naar inhoud. Bijvoorbeeld voor het onderbrengen van de bevoegdheid tot het toevoegen, wijzigen en verwijderen van gebruikers op hoofdafdelingsniveau. Daar bestaat namelijk inzicht in wie wel en wie niet werkzaam is. Het is wenselijk, dat bepaalde gebruikersbevoegdheden op een lager niveau kunnen worden gemuteerd.

Tot slot

Een groot aantal toegangsbeveiligingspakketten wordt aangeboden op de markt. Bij de keuze van een pakket kunnen de in dit artikel gespecificeerde functionele eisen in de beschouwing worden betrokken. Een adequate toegangsbeveiliging is van niet te onderschatten betekenis voor een beheersbare geautomatiseerde gegevensverwerking.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Herfst 1987

Boeken

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

Unix for superusers
Auteur: Eric Foxley
International computer science series

Het boek beschrijft de aspecten van het UNIX-besturingssysteem die van belang zijn voor de "superuser" (de beheerder) van het systeem, zoals het opstarten en stoppen, het introduceren van nieuwe gebruikers, het verzorgen van de integriteit van het file-systeem en het op peil houden van de performance van het systeem. Het boek veronderstelt een zekere bekendheid met UNIX op het normale gebruikersniveau en is voornamelijk bedoeld om mensen, die al op een UNIX-systeem werken, voldoende kennis bij te brengen om een UNIX-systeem te kunnen beheren.

Na een korte inleiding waarin de schrijver zijn bedoeling met het boekje duidelijk maakt, volgt een hoofdstuk over de achtergrond van bedrijfssystemen in het algemeen. Hierbij komen ook aspecten als multitasking, scheduling, memory management en I/O aan de orde. Helaas is deze behandeling dermate oppervlakkig dat voor de rest van het boek eigenlijk meer ondergrond benodigd is.

Hierna volgt een beschrijving van de standaardindeling van de schijven: waar de systeemprogramma's staan, de utilities, de compilers, tekstverwerkers, etc. De schrijver geeft een uitstekende "road-map" van de UNIX-schijfindeling en ook waarom de programma's en bestanden juist zó zijn verdeeld over het schijfgeheugen.

Vervolgens bespreekt de schrijver de gang van zaken bij het opstarten en stoppen van het systeem. Dit is een van de zaken binnen UNIX-systemen die niet gestandaardiseerd zijn. Daarom is de bespreking die gegeven wordt voor veel systemen niet relevant.

De hoofdstukken 6, 7 en 8 gaan over het in- en uitloggen, de commando interpreter (de shell) en het beheer door de superuser ten aanzien van de gebruikers. Vooral hoofdstuk 8 geeft een goed beeld van de mogelijkheden die de systeembeheerder heeft om de gebruikers niet overal toe te laten in het systeem.

Randapparatuur wordt in UNIX bestuurd door middel van dezelfde hulpmiddelen die ook ter beschikking staan voor het aanmaken van bestanden, omdat rand-

apparaten door het systeem gezien worden als standaardbestanden. Dit maakt het beheren van de randapparatuur een stuk eenvoudiger. In het boek worden er dan ook weinig woorden aan vuil gemaakt.

Wellicht het moeilijkste deel van UNIX is de structuur van het file-systeem. Dit is het systeem dat gebruikt wordt door UNIX om de bestanden, programma's en directories op een geordende hiërarchische manier op schijf te zetten. De belangrijkste taak van de systeembeheerder van een UNIX-systeem is het bewaren van de consistentie en integriteit van het file-systeem. Omdat het systeem zo snel mogelijk de diverse bestanden moet kunnen benaderen, zijn diverse gegevens over de schijven redundant opgeslagen. Door deze redundantie is echter een mogelijke bron van inconsistentie geïntroduceerd. Een goed boek dient uitgebreid in te gaan op de gereedschappen die de systeembeheerder ter beschikking staan om eventuele problemen op te lossen. Helaas blijft het boek "UNIX for superusers" steken bij programma's voor de registratie van het gebruik van disk-ruimte, back-up-programma's en dergelijke. Wat te doen als er problemen zijn wordt niet vermeld (behalve het terugladen van de back-up van vorige week).

UNIX is door de doorzichtige opzet en vele mogelijkheden moeilijk waterdicht te krijgen tegen indringers van binnen uit. Het password-systeem biedt een goede beveiliging tegen indringers van buiten af, maar eenmaal het systeem binnen, kan men relatief eenvoudig zijn gang gaan. Om een UNIX-systeem van binnen goed af te sluiten is veel kennis van UNIX nodig. Er is in de literatuur een grote schat aan al of niet geslaagde "kraakpogingen" en "sluipwegen" bekend. Het is juist daarom zo jammer dat de schrijver slechts een hoofdstuk van enkele pagina's over de beveiliging van UNIX heeft weten samen te stellen. De schrijver die werkzaam is op de universiteit van Nottingham zou toch te maken moeten hebben gehad met "krakende" studenten. Wellicht maken de studenten in Groot Brittanië het de systeembeheerder niet zo lastig als hier in Nederland.

Na deze hoofdstukken volgt een behandeling van verschillende voor de systeembeheerder nuttige programma's alsmede een opsomming van de mogelijkheden van de diverse commando-interpretatoren en een verklarende woordenlijst van programma's en termen die veel binnen UNIX gebruikt worden.

Concluderend kan gezegd worden dat het boek UNIX for superusers minder biedt dan de titel doet vermoeden. Het vereist meer voorkennis dan in de inleiding gesteld wordt, maar biedt minder dan nodig om een UNIX-systeem werkelijk goed te kunnen beheren. Met name wordt (vrijwel) niets gezegd over wat te doen als er met het filesysteem iets mis is. Ook het hoofdstuk over (inbraak)beveiliging is wat karig. Het beheren van machines die opgenomen zijn in het standaard UNIX-netwerk (UUCP) komt vrijwel niet aan bod; een groot gemis. Sommige hoofdstukken geven echter een frisse blik op aspecten van UNIX, zodat het uitstekend als aanvulling op andere literatuur gebruikt kan worden. Ook kan het boek de standaard gebruiker van een UNIX-systeem een idee geven wat de taken van systeembeheerder onder andere inhouden.