KPMG Klynveld EDP Audit Services

88/1
winter 1988

COMPACT

MONSTEREXEMPLAAR NIET MEENEMEN

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 46 **Winter 1987/1988**
ISSN 0920-1645

COMPACT

Winter 1987/1988

VAN DE REDACTIE

Ogenschijnlijk hebben de drie artikelen in deze Compact weinig met elkaar gemeen.

Toch bevatten alle één gemeenschappelijke noemer namelijk de poort naar de toekomst van moderne automatisering en controle-activiteiten.

A. Systeembouw gebaseerd op systemen met ingebouwde deskundigheid maar op gecontroleerde wijze ter vermijding van onbeheersbaarheid.

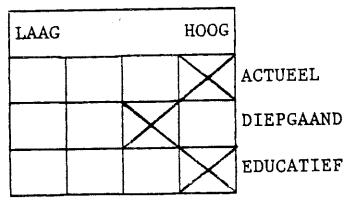
B. Beveiliging bij datatransmissie.

In de rubrieken worden de actualiteiten behandeld, lezing ervan wordt aanbevolen. Onder Tijdschriften komt het artikel voor Electronic Funds Transfer, het elektronisch uitvoeren van betalingen.

Heeft u naar aanleiding van het bovenstaande reacties, opmerkingen of goede oplossingen schrijf ons die dan. Wij staan gaarne ruimte voor u af in Compact.

Hieronder volgt een samenvatting van de inhoud van de hoofdartikelen.

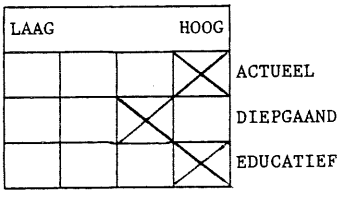
SKE, Structured Knowledge Engineering
door ing. A. van der Vlist



Het werken met "Expert"systemen geeft in de praktijk nogal eens problemen. Bij het n-de prototype ontstaat wel een compleet systeem, maar het blijkt dat het in feite als project en daarmede ook de implementatie ervan onbeheersbaar is geworden.
Met SKE/KADS streeft men naar een beheersbaar project en komt men tot een aantal "milestones", vergelijkbare stappen als in een conventioneel software-ontwikkelingstraject.

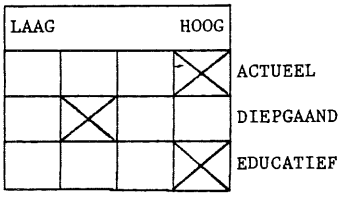
Winter 1987/1988

Beveiliging bij datatransmissie
door ing. H.A.J.M. Spape



Datatransmissie en netwerken scheppen nieuwe mogelijkheden doch leiden tevens tot nieuwe bedreigingen voor de betrouwbaarheid en de continuïteit van de geautomatiseerde informatievoorziening. Als regel zijn maatregelen vereist om deze bedreigingen te beheersen. Hiertoe zal enerzijds gebruik worden gemaakt van technische hulpmiddelen, zoals beveiligingsapparatuur en -programmatuur. Anderzijds zullen organisatorische voorzieningen getroffen moeten worden. Dit artikel geeft een overzicht van de bedreigingen die zich in een situatie met datatransmissie kunnen voordoen en bespreekt een aantal technische en organisatorische voorzieningen die ter beheersing van de bedreigingen kunnen worden getroffen.

Electronic Funds Transfer, het elektronisch uitvoeren van betalingen
door mw. ing. I.M. van Duin



De laatste tijd staat Electronic Funds Transfer, het elektronisch uitvoeren van betalingen, bij veel bedrijven en instellingen in de belangstelling. Hopelijk draagt dit nummer bij tot een vergroting van uw kennis van en interesse in het elektronisch betalen.

Van ieder van de schrijvers van de hoofdartikelen hebben wij een profielschets samengesteld. Het is duidelijk dat het een momentopname betreft van jonge mensen midden in hun ontwikkeling, zie hiervoor de laatste pagina.

COMPACT

Winter 1987/1988

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 Amsterdam
Strawinskylaan 1257
Toren D 11e etage
1077 XX AMSTERDAM
Postadres:
Postbus 72001
1007 TB 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

A. COMPUTERVIRUS ACTUELE BEDREIGING COMPUTERSYSTEMEN

Computervirussen komen meer en meer in de publiciteit. Dit vooral nadat een aantal virussen in grote installaties zijn ontdekt.

Virussen zijn (kleine) programmadelen die in staat zijn zichzelf te implanteren in andere programmatuur. Dit kan zich herhalen, tot op den duur alle programmatuur op een computersysteem geïnfecteerd is. Deze manier van voortplanten lijkt zeer sterk op de manier waarop een biologisch virus van cel tot cel gaat: het dringt een cel binnen, injecteert het genetisch materiaal van het virus in dat van de cel, waarop de cel aangezet wordt tot produktie van meer virussen.

Een computervirus kan daarnaast ook nog een kwaadaardige functie in zich dragen, zoals een "timebomb" die op een bepaalde datum bestanden wist of mutaties uitvoert.

Hieronder een aantal maatregelen die tegen virussen genomen kunnen worden:
- programmavirussen kunnen slechts daar toeslaan waar het virus de mogelijkheid heeft te schrijven in bestaande programma's. Een eerste maatregel tegen virussen kan dan ook bestaan uit het fysiek "onoverschrijfbaar" maken van de programmatuur. Bij PC's bijvoorbeeld door de diskette tegen overschrijven te beschermen met een plakkertje of het no-write-schuifje;
- gebruik uitsluitend officiële programmatuur, gebruik geen "kopie van de buurman";
- alle programmatuur dient direct na ontvangst gekopieerd te worden naar diskettes en/of tapes, waarna de officiële disk en/of tape niet wordt gebruikt, maar bijvoorbeeld in een kluis wordt bewaard. De kopie kan dan gebruikt worden. Mocht zich ooit een besmetting voordoen, kan weer een (onbesmette) kopie getrokken worden van de officiële distributiedisk en/of -tape;
- probeer programmatuur en data zoveel mogelijk gescheiden te houden bij het maken van een back-up, zodat na een virusaanval, de programmatuur van de officiële disk en/of tapes gehaald kan worden. De data (die niet geïnfecteerd kan worden) kan dan zonder gevaar voor nieuwe besmetting van de back-up gehaald worden.

Er wordt (ook binnen KPMG Klynveld EDP Audit Services) momenteel veel onderzoek verricht naar virussen en mogelijke tegenmaatregelen.

In de volgende Compact(r) zal in een artikel uitvoerig op het verschijnsel virussen worden ingegaan.

Ing. J.C. van Winkel

B. SAMENWERKING SOFTWARE-KEURING

Persbericht

Vier Nederlandse organisaties hebben besloten om in onderlinge samenwerking te komen tot keuringen van software-pakketten op financieel-administratief en technisch-wetenschappelijk terrein.
De deelnemers in deze aanpak zijn:
- Van Dien + Co. Computer Audit Services;
- Instituut voor Toegepaste Informatica - TNO Delft;
- N.V. KEMA;
- KPMG Klynveld EDP Audit Services.

Afnemers en gebruikers van standaard-software hebben behoefte aan grotere zekerheid omtrent de kwaliteit van aangeboden programma's.
Anderzijds is voor producenten en leveranciers van software van groot belang dat zij kunnen aantonen dat hun produkten voldoen aan gestelde kwaliteitseisen. Het ligt voor de hand dat een keurings- en certificatiesysteem zal kunnen bijdragen tot een algemene verbetering van de kwaliteit van de aangeboden pakketten.
De genoemde organisaties zijn in de afgelopen jaren al actief geweest in het beoordelen en toetsen van programma's. De vier samenwerkende bedrijven beschikken ieder over hun eigen specifieke expertise en bestrijken samen een breed terrein van het financieel-administratieve en technisch-wetenschappelijke automatiseringstraject. Deskundigheid is dus in ruime mate aanwezig. Doel van de gezamenlijke aanpak is om te komen tot een éénduidig systeem voor keuring met een breed draagvlak.

De keuringsdiensten zijn vooral gericht op toepassingsprogrammatuur voor micro- en minicomputers, die gewoon op de Nederlandse markt wordt aangeboden.
Er wordt naar gestreefd de certificatie te laten plaatsvinden in het kader van ICIT (Instituut Certificatie Informatie Technologie).
De keuringen zullen worden uitgevoerd volgens de eisen die in West-Duitsland zijn opgesteld door de GGS (Gütegemeinschaft Software). De GGS-eisen bevatten onder meer de minimumvoorwaarden voor de produktbeschrijving. Hierin dienen de functionele en technische gegevens van het pakket te zijn beschreven, die voor de koper c.q. gebruiker van belang zijn. Tevens bevatten de GGS-eisen voorwaarden voor de goede werking van het pakket. Bij de in Nederland uit te voeren keuringen zullen aanvullende eisen worden gesteld met betrekking tot de betrouwbaarheid en continuïteit van de verwerking.

Keuringen zullen worden uitgevoerd in opdracht van belanghebbenden. In de meeste gevallen zal dit de producent, de leverancier of de importeur van het programma zijn.
Dat de keuringen vertrouwelijk zullen worden uitgevoerd is gegarandeerd doordat de samenwerkende organisaties vanuit hun beroepsuitoefening gewend zijn hoge eisen te stellen aan de vertrouwelijkheid.

Het streven is de eerste keuringen volgens de geschetste aanpak in het eerste kwartaal van 1988 uit te voeren. Leveranciers die software-pakketten ter keuring willen aanbieden, kunnen zich aanmelden bij elk van de deelnemers.
Het streven is de eerste keuringen volgens de geschetste aanpak in het eerste kwartaal van 1988 uit te voeren. Leveranciers die software-pakketten ter keuring willen aanbieden, kunnen zich aanmelden bij elk van de deelnemers.

Achtergrondartikel

1. Achtergronden

Een automatiseringsprobleem kan men weliswaar met "maatwerk-software" optimaal oplossen, vaak is echter op de markt verkrijgbare "standaard-software" een veruit goedkopere oplossing. De voordelen zijn:

- tijdbesparing — De ontwikkeltijd vervalt en het pakket is (idealiter) direct te gebruiken.
- kostenbesparing — De ontwikkelkosten worden door vele gebruikers gedragen.
- kopen van know how — Een wezenlijk onderdeel van software is de in programmacode besloten oplossing.
- minder risico — Extra kosten van uitlopende projecten, zoals bij eigen ontwikkeling vaak gebeurt, vervallen.
- minder onderhoud — Het onderhoud wordt door de producent van de software gedaan.

Afnemers en gebruikers van software-pakketten worden in hun selectieproces ondersteund en krijgen meer zekerheid bij de aanschaf indien de pakketten door een onafhankelijke instelling op een aantal essentiële aspecten zijn beoordeeld. Leveranciers, producenten en importeurs wordt door middel van deze keuringsdienst de mogelijkheid geboden hun produkt in de markt te profileren als een kwaliteitsprodukt. Het "koren" onder de software-pakketten wordt aldus gelegenheid gegeven zich te onderscheiden van het "kaf". Verwacht kan worden dat een keurings- en certificatiesysteem zal bijdragen tot een algemene verbetering van de kwaliteit van de aangeboden software-pakketten.

2. Gemeenschappelijke aanpak

Vier Nederlandse organisaties hebben gezamenlijk een aanpak ontwikkeld die het uitvoeren van deze keuringsdienst mogelijk maakt. Er wordt naar gestreefd om goedgekeurde pakketten te certificeren in het kader van het ICIT. Aan deze gezamenlijke aanpak werken mee: Van Dien + Co. Computer Audit services, KPMG Klynveld EDP Audit Services, N.V. KEMA en het TNO Instituut voor Toegepaste Informatica (ITI-TNO).
In eerste instantie richt men zich op de uitwerking van een norm voor het keuren van standaardpakketten, waarmee in Duitsland al ervaring is opgedaan, maar de samenwerking zal zich ook gaan uitstrekken tot het uitvoeren van de keuring zelf.

De samenwerkende bedrijven beschikken alle vier over eigen specifieke expertise en bestrijken samen een breed terrein van de financieel-administratieve en technisch-wetenschappelijke automatiseringstoepassingen. Dit omvat onder meer:
- beoordeling van functionaliteit en betrouwbaarheidsaspecten;
- de controle van geautomatiseerde systemen;
- onderzoek en keuzebepaling van hard- en software-produkten.

Doordat bij de uitvoering van de keuringswerkzaamheden zowel experts op het gebied van de informatietechnologie als experts op het gebied van de specifieke applicatie meewerken, wordt een pakket deskundig bekeken. Zo wordt een pakket niet alleen gekeurd op correctheid van de produktbeschrijving en documentatie, maar wordt ook gekeurd op de kwaliteit van de door het pakket geleverde resultaten en of voldaan is aan specifieke overheidsvoorschriften.
Door de samenwerking wordt de deskundigheid optimaal benut en gecoördineerd, zodat kennis en inzicht actueel zijn en er op de meest efficiënte wijze en zeer doelgericht wordt gewerkt.

3. Inhoud van de keuring

Bij het keuren van een pakket kan men verschillende stappen onderscheiden:
- de controle van de produktbeschrijving, waarbij wordt nagegaan of deze voldoet aan de norm, en of beweringen die erin gedaan worden controleerbaar zijn;
- de installatie van het pakket, waarbij de installatieprocedure zoals die door de leverancier is opgegeven wordt uitgevoerd en op juistheid wordt gecontroleerd;
- de controle van de buiten de produktbeschrijving aanwezige documentatie, zoals de gebruikershandleiding, waarbij wordt getoetst op consistentie en volledigheid;
- de eigenlijke programmatest.

Het testplan wordt opgesteld op grond van de documentatie en omvat een test van alle functies. Alle in de documentatie vermelde grenswaarden worden daarbij getest. Tevens is er een test op robuustheid. Van iedere invoerfunctie wordt nagegaan hoe het pakket reageert op het gebruik van niet gedefinieerde toetsen. Ten slotte wordt gecontroleerd of de juiste foutmeldingen worden gegeven in overeenstemming met hetgeen staat vermeld in de documentatie.
Branche-specifieke eisen worden niet bij de keuring betrokken. Voor zover een branche-organisatie het pakket op specifieke eisen heeft beoordeeld, mag dit in de documentatie van het pakket worden vermeld.
Er zal worden gekeurd volgens de eisen die in West-Duitsland zijn opgesteld door de Gütegemeinschaft Software (GGS), aangevuld met betrouwbaarheidseisen op financieel-administratief en technisch-wetenschappelijk gebied.

De GGS-eisen, die zijn vastgesteld in de Duitse norm DIN V-66285 (september 1985), bevatten de minimumvoorwaarden van de produktbeschrijving, waarin de functionele en technische gegevens van het pakket worden beschreven die voor de koper c.q. gebruiker van belang zijn.
Voor ieder onderdeel van de keuring bestaan minimumeisen ten aanzien van hun eigenschappen, kenmerken en functies, waarvan de vervulling door geeigende metingen onderzocht wordt. De criteria zijn zodanig gedefinieerd, dat een objectieve beoordeling door de keuringsinstantie zo goed mogelijk is gewaarborgd.

4. Doelgroepen

De gezamenlijke keuringsaanpak zal zich in hoofdzaak richten op toepassingspakketten voor mini- en microcomputers. Dit betreft pakketten op financieel-administratief alsmede pakketten op technisch-wetenschappelijk en industrieel gebied. In bijzondere gevallen zoals mainframe en process-control-toepassingen kan nader worden overlegd.
De aanpak is gericht op keuring van op de Nederlandse markt aangeboden software-pakketten, waarvoor de leverancier een openbaar certificaat wenst.

5. Werkwijze en aanpak

Een software-pakket kan alleen worden gekeurd indien minimaal de programmatuur, de produktbeschrijving en de gebruikersdocumentatie aanwezig zijn. Evenzeer dient de vereiste apparatuur beschikbaar te zijn. Indien in de produktbeschrijving opleidingen worden voorgesteld, zal dit aspect in de keuring worden betrokken.
Voor het effectueren van de gezamenlijke aanpak van de keuring is voorlopig gekozen voor de volgende uitgangspunten:

- de gezamenlijke aanpak geldt vooralsnog voor de periode tot 1 januari 1989;
- voordat een keuring wordt uitgevoerd, worden in overleg tussen de deelnemende instellingen de keuringseisen vertaald in een testscenario. Daarbij wordt ook bepaald welke deelnemers de verschillende tests zullen uitvoeren;
  De tests gebeuren onder de verantwoordelijkheid van de opdrachtnemer;
- het opstellen van het keuringsrapport gebeurt door de opdrachtnemer. Voordat het keuringsrapport wordt vrijgegeven aan de opdrachtgever vindt overleg plaats van alle deelnemers over de inhoud en vorm van het keuringsrapport en de onderliggende keuringsresultaten;
- omdat er wordt gestreefd naar certificatie van software-pakketten in het kader van het ICIT, worden de ervaringen met het keuren aan het ICIT voorgelegd.

Het overleg zoals beschreven in de bovengenoemde punten is gericht op het uitwisselen van ervaringen met de keuringsvoorschriften, het bereiken van een gemeenschappelijke interpretatie daarvan en het vaststellen van aanvullingen en wijzigingen waar nodig.

6. Vertrouwelijkheid

De samenwerkende organisaties zijn vanuit hun beroepsuitoefening al gewend hoge eisen te stellen aan de vertrouwelijkheid. In deze samenwerking is extra nadruk gelegd op dit punt.
Alle gegevens die in het kader van een keuring ter kennis komen van de deelnemers zullen strikt vertrouwelijk worden behandeld. De deelnemer die de opdracht verwerft, garandeert de geheimhouding naar de opdrachtgever. Over de inschakeling van andere deelnemers bij uitvoering van de keuring vindt overleg plaats met de opdrachtgever.

7. Aanmeldingsprocedure

Leveranciers die software-pakketten willen aanbieden ter keuring, kunnen zich aanmelden bij elk van de deelnemers. De contactpersonen voor de vier organisaties zijn:

Van Dien + Co. Computer Audit Services
Contactpersoon: A. Straatman RA
Churchilllaan 11
3527 GV Utrecht
telefoon 030-939941

Instituut voor Toegepaste Informatica-TNO
Contactpersoon: ir. J.H.A.M. Krabbenborg
Postbus 214
2600 AE Delft
telefoon 015-697097

N.V. KEMA
Contactpersoon: ir F. Rienstra
Utrechtseweg 310
6812 AR Arnhem
telefoon 085-566223

KPMG Klynveld EDP Audit Services
Contactpersoon: A.W. Neisingh RA
WTC
Strawinskylaan 1257
1077 XX Amsterdam
telefoon 020-5469111

Voor nadere informatie en voor het aanvragen van offertes inzake keuringen kan contact worden opgenomen met bovengenoemde personen.
Condities (onder andere de kosten van de keuring) waaronder de opdracht wordt uitgevoerd, is gespreksonderwerp tussen de opdrachtgever en de betreffende deelnemer.

C. GESCHILLENBESLECHTING IN DE AUTOMATISERINGSBRANCHE

Waar mensen zijn, komen geschillen voor. Dat is de stelling van prof. mr. H. Franken bij aanvang van de conferentie over geschillenbeslechting in de automatiseringsbranche die op 28 januari 1988 door het NOVI georganiseerd werd.
Ook in deze branche komen, steeds meer, geschillen voor tussen bijvoorbeeld leverancier en afnemer van software. In veel gevallen lukt het de strijdende partijen niet om zelfstandig tot overeenstemming te komen en zoeken ze hun toevlucht tot een deskundige derde.
In zijn rede gaf prof. Franken een overzicht van de diverse vormen van conflictregulering en -hantering teneinde een antwoord te vinden op de vraag wie de meest geschikte persoon of instantie is om effectief en efficiënt problemen tussen partijen in de automatiseringsbranche uit de wereld te helpen. De vormen die hij daarbij aangaf plaatste hij op een schaal die het stadium aangeeft waarin het conflict zich bevindt; door mij de "schaal van Franken" genoemd:

1. Problem solving onderhandelen:
   a. Procesbegeleiding.
      De derde confronteert de betrokken partijen met hun gedrag en bevordert het inzicht in het samen moeten functioneren.
   b. Onderzoek of enquête.
      De derde spoort de knelpunten op en helpt aan te geven hoe deze barrières kunnen worden beslecht.

   Bij deze twee vormen van conflicthantering heeft de derde deskundige geen beslissingsbevoegdheid. Het is een informele, snelle en goedkope procedure.

2. Mini trial:
   a. Verzoening.
      De derde probeert de partijen tot elkaar te brengen. Hij kan hen geen bindende oplossing voorleggen, maar evalueert oplossingsvoorstellen die tijdens de onderhandelingen worden geformuleerd en waaruit zij een keuze kunnen maken.
   b. Bemiddeling.
      De derde tracht de partijen tot elkaar te brengen door daartoe zelf voorstellen te doen en pressie op een van hen of op beide uit te oefenen.

   Ook voor deze twee vormen geldt dat het een informele, snelle en goedkope procedure is waarbij de derde geen dwang maar wel drang uit kan oefenen.

3. Bindend advies.
   Partijen kunnen overeenkomen een (toekomstig) geschil door een derde te laten beslissen. Deze geeft een oordeel omtrent de wijze waarop de partijen zich ten aanzien van de uitlegging of uitvoering van hun overeenkomst dienen te gedragen. Dit oordeel wordt beschouwd als een onderdeel van die overeenkomst.

De beslissing van de derde leidt echter niet tot een executoriale titel: in geval van onwil tot nakoming van het bindend advies is een procedure bij de rechter nodig. De rechter kan het advies marginaal toetsen op de redelijkheid en billijkheid. Er zijn geen wettelijke waarborgen ten aanzien van de benoeming van de adviseur. De adviseur wordt daarentegen niet gehinderd door een formele rechtsgang en de uitslag wordt niet openbaar gemaakt.

4. Arbitrage.
Bij overeenkomst kunnen partijen hun geschil voorleggen aan een of meerdere arbiters die daaromtrent een beslissing geven die voor de partijen bindend is. Deze beslissing is neergelegd in een executoriaal vonnis. Arbitrage is geregeld in de wet: de artikelen 1020-1076 van het Wetboek van Burgerlijke Rechtsvordering. Hiernaast zijn er nog vele internationale overeenkomsten waarin arbitrage geregeld is.
Partijen zijn vrij in hun keuze van de arbiter(s) op grond van specifieke materiedeskundigheid, er is geen verplichte procesvertegenwoordiging, er zijn geen vaste bewijsregels en de procedure kan een snel verloop hebben. De uitspraak kan uit de publiciteit gehouden worden. Daarentegen dienen de arbiters over een aanzienlijke juridische kennis te bezitten, zijn ze moeilijk te vinden en kan er altijd nog een rechterlijke procedure volgen. Bij het Nederlands Arbitrage Instituut zijn zo'n 400 arbiters opgenomen waarop een beroep gedaan kan worden. De aangesloten arbiters zijn gebonden aan een reglement.

5. Gewone rechtspraak.
Geschillen over burgerlijke rechten en over schuldvorderingen zijn opgedragen aan de rechterlijke macht. Alleen wanneer partijen dat uitdrukkelijk verklaren, kunnen zij hun geschil door anderen dan de overheidsrechter laten afdoen.
Procederen via de rechter, al dan niet in kort geding, is van oudsher omgeven met een groot aantal waarborgen. De rechter is onafhankelijk en hoeft niet door de partijen betaald te worden. Indien de rechter echter een deskundigenbericht nodig acht, dan brengt dit wel hoge kosten met zich mee. De procedure kan soms traag verlopen, alhoewel procederen in kort geding enige snelheid waarborgt. Uitspraken door de rechter zijn altijd openbaar.

De keuze van een bepaalde vorm van conflictregulering hangt van diverse overwegingen af. Voor problem-solving-onderhandelen en mini trial moeten de partijen zelf de uiteindelijke beslissing nemen. Indien het conflict enigermate is geëscaleerd, zal daarom de keuze gaan tussen bindend advies en vooral tussen arbitrage of rechtspraak. Een van de grootste problemen hierbij is het vinden van goede arbiters met voldoende kennis op het gebied van de automatisering.
Is het toeval dat het bestuur van het NIvRA op aandrang van het Nederlands Arbitrage Instituut in het februarinummer van "de Accountant" een oproep heeft gedaan aan accountants om zich bij het NAI aan te melden als arbiter??
R.A. s'Jacob

Winter 1987/1988

SKE, STRUCTURED KNOWLEDGE ENGINEERING

door ing. A. van der Vlist

Inleiding

Het op de markt komen van een grote variëteit aan "expert"systemen heeft ertoe geleid dat men op velerlei gebied onderzoek doet naar de toepasbaarheid van dergelijke systemen.
De meeste "expert"systemen zijn in de vorm van speciale programmeertalen of expert system shells. (Talen: Lisp, Prolog en shells: XI-plus, GoldWorks etc.) Onder een expert system shell wordt een hulpmiddel verstaan om consultatie en probleemoplossende systemen te bouwen. De hieruit ontstane systemen voeren taken uit die normaliter door menselijke experts worden uitgevoerd.
Het werken hiermee in de praktijk geeft echter nogal wat problemen als men deze hulpmiddelen gebruikt voor "Rapid Prototyping". Rapid prototyping is een techniek om in een korte doorlooptijd gestructureerde informatiebehoeften om te zetten in prototypes van informatiesystemen. Op zich is prototypen een goede techniek, mits beheersbaar toegepast. Een aantal redenen voor het toepassen van rapid prototyping zijn:

- deelaspecten van het totaal systemen kunnen worden getest;
- het is voor een "expert" relatief eenvoudig om aanvullingen te bedenken op een draaiend systeem;
- management is gevoelig voor "draaiende" systemen;
- gebrek aan een betere methode om te komen tot een implementatie.

De beschikbare "expert"systemen lenen zich om geautomatiseerde kennissystemen te ontwikkelen met behulp van prototypen. Bijvoorbeeld, een kleine set van "rules" in een expert shell kan al een werkend prototype opleveren. Als de basis voor een compleet geautomatiseerd kennissysteem op deze manier ontstaat dan is de kans groot dat het produkt onbeheersbaar blijkt ten opzichte van bijvoorbeeld planning, modulariteit, consistentie en hiërarchie.

Voor het klassieke ontwikkelen van geautomatiseerde systemen zijn goede uitgekristalliseerde ontwikkelmethoden beschikbaar (bijvoorbeeld SDM, ISAC etc.). Hierin wordt voorzien in projectbeheersing, documentatie en het sturen van het denkproces. Prototypen vindt hierin een "beheerste" plaats.
Wat nieuw is, en wat ook het onderwerp van dit artikel is, is een model van een dergelijke methode maar dan toegespitst op het ontwerpen van geautomatiseerde kennissystemen. Onder de ESPRIT-vlag is aan de UvA') de "Knowledge Acquisition Documentation and Structuring system" (KADS) methode ontwikkeld.

') Universiteit van Amsterdam. Het onderzoek wordt geleid door Breuker en Wielinga.

Deze theoretische benadering is omgewerkt van een in de praktijk hanteerbare methode tot de "Structured Knowledge Engineering" (SKE)') methode.
Met de SKE/KADS-methodiek streeft men naar een beheersbaar project en komt men tot een aantal "milestones", vergelijkbare stappen als in een conventioneel software-ontwikkelingstraject.

Terminologie: In dit artikel zal de term "kennissysteem" gehanteerd worden. Er is nogal een spraakverwarring en ook interpretatieverschil over termen als "knowledge based system", "expert system", "Intelligent Tutoring System" etc.

KADS-aanpak

De gestructureerde aanpak van een project voor een kennissysteem is te vergelijken met de aanpak van een conventioneel software-ontwikkelingsproject in stappen als bijvoorbeeld de SDM-fasering. Dit is als volgt in beeld te brengen:

SDM	KADS
definitiestudie	initiatiefase
functioneel ontwerp	kennisacquisitiefase
technisch ontwerp	architectuurfase
programmeren	implementatiefase
testen en acceptatie	testen en acceptatie
onderhoud	onderhoud

Als er verschillende stappen zijn te onderscheiden in het ontwikkeltraject van een kennissysteem, wordt niet alleen het project beheersbaarder, ook kan er op die manier een exacte afbakening komen op verschillende werkterreinen van de "knowledge engineer". De kennisacquisitiefase kan door een cognitief psycholoog worden uitgevoerd, terwijl de architectuur en implementatiefasen door "programmeurs" worden uitgevoerd. De praktijk tot op heden voor kleine projecten is dat alle fasen door één persoon worden uitgevoerd.
In de volgende paragrafen zullen de fasen van KADS nader uitgewerkt worden. Gestreeft wordt, analoog aan de ontwikkelingen in software-enginee-

') SKE is ontwikkeld bij het Helmondse bedrijf Bolesian Systems Europe B.V. Er is ook een cursus via dit bedrijf beschikbaar, ontwikkeld in opdracht van het NIIO (Nationaal Inhaalprogramma Informatica Opleidingen) instituut. KKC was uitgenodigd om een evaluatiesessie bij te wonen. De cursus wordt gegeven vanaf oktober 1987.

ring-methodieken, om medio 1988 een Knowledge Engineer's Workbench (KEW)') ter beschikking te stellen waarin de fasen van KADS-computer ondersteund doorlopen kunnen worden.

De methode om tot de uiteindelijke implementatie te komen is binnen KADS de modellering van expertise. Er wordt geen gebruik gemaakt van het opbouwen van inferentiestructuren uit beschikbare data. Het modelleren van expertise is goed vergelijkbaar met conventionele informatie-analyse. De methoden om te komen tot een model van de expertise liggen echter meer op het vlak van de cognitieve psychologie.

Initiatiefase

De start van een project wordt vastgelegd in een tweetal onderdelen:
- een kennisdomeinbeschrijving van het "probleem";
- een haalbaarheidsstudie.

Een domeinbeschrijving geeft een indruk om welke specifieke kennis het gaat en inventariseert dit. Dat is weer van belang voor de haalbaarheidsstudie waar het gaat om deze gegevens te interpreteren en daaruit te concluderen of het project uiteindelijk haalbaar is. Als bijvoorbeeld in het kennisdomein veel "common sense knowledge" voorkomt, geeft dit een negatieve indicatie voor de haalbaarheid van het project.
Andere aspecten die naar voren komen in de haalbaarheidsstudie zijn bijvoorbeeld:
- is er één expert te modelleren of een groep en zo ja, is er consensus onderling;
- is er goede documentatie van het kennisdomein;
- is er sprake van expliciete modellen en/of methodologieën;
- is het mogelijk om prototypische gevallen te onderscheiden;
- vormen potentiële gebruikers een homogene groep;

etc.

Een belangrijk aspect is een tijdsschatting van de eigenlijke experttaak. Een "ideale" gemiddelde experttaak moet ongeveer 25 à 40 minuten duren. Duurt bijvoorbeeld een experttaak 2 uur, dan is het domein onbeheersbaar en zijn ook de taakstructuren niet te overzien. Let wel dat deze schattingen afkomstig zijn van redelijk bekende domeinen zoals bijvoorbeeld medische diagnosesystemen. Voor andere kennisdomeinen kan dit uiteraard verschillend zijn.
Het resultaat van deze fase (een milestone) is een oordeel over de haalbaarheid, een globale probleemstelling/domeinbeschrijving, een globale planning en een kostenschatting.

') De KEW is in ontwikkeling bij de Universiteit van Amsterdam (UvA).

Kennisacquisitiefase

De kennisacquisitiefase kan worden onderverdeeld in drie deelfasen, te weten:
- oriëntatie;
- probleemidentificatie;
- probleemanalyse.

Parallel met deze drie fasen wordt een taakanalyse uitgevoerd.
De drie deelfasen zijn sterk verbonden aan een aantal interview-technieken: het gefocusseerde interview, het gestructureerde interview, expertgebruiker dialoog en het hardopdenk-protocol.
Deze technieken worden apart in een daaraan gewijde paragraaf behandeld.

De oriëntatie gaat verder dan een eerste domeinverkenning in de initiatiefase en bevat literatuurstudies en gefocusseerde interviews met de expert. Aan het einde van deze subfase wordt vastgesteld wat de rol van de expert is en wordt een probleemdefinitie of wel de typering van de probleembeschrijving gemaakt. Ook een verklarende woordenlijst wordt toegevoegd van "vakjargon".

De probleemidentificatie heeft als doel een functionele analyse van de expertkennis te maken door middel van een formele beschrijving. Door middel van gestructureerde interviews wordt de gevonden literatuurkennis getoetst aan de expertkennis en wordt een functionele analyse opgesteld. Een aantal neventaken die uitgevoerd dienen te worden tijdens de probleemidentificatie zijn:
- het maken van een decompositie van de gehele experttaak;
- het genereren van structuren van domeinbegrippen;
- verzamelen van probleemgevallen (cases);
- globale gebruikersanalyse.

De domeinbegrippen kunnen worden vastgelegd in (gerichte) grafen, bijvoorbeeld een hiërarchie van "is_een" relaties (hond is een viervoeter, viervoeter is een dier, etc.).

De probleemanalysefase is bedoeld om vanuit de voorgaande fasen te komen tot (samengestelde) interpretatiemodellen van de experttaak. Hiervoor wordt onder meer gebruik gemaakt van "hardopdenk-protocollen" om te komen tot:
- een compleet interpretatiemodel (conceptueel model);
- een gebruikers- en omgevingsanalyse.

Met name het conceptueel model is essentieel. Het vormt de basis voor de architectuurfase en de implementatiefase. Blijkt in die latere fasen dat het kennissysteem de experttaak onvolledig kan uitvoeren dan is dat het directe gevolg van een onvolledig interpretatiemodel.
In een aparte paragraaf zal worden ingegaan op het interpretatiemodel.

De taakanalyse, die over de gehele kennisacquisitiefase heen uitgevoerd wordt, is in wezen een concept-vorming aangaande het interpretatiemodel.

Afhankelijk van ervaring en domeinkennis zal een concept-interpretatiemodel in een zo vroeg mogelijk stadium ontstaan (zie voor interpretatiemodellen de daaraan gewijde paragraaf).

Architectuurfase

In deze fase dient de overstap gemaakt te worden van de functionele beschrijving in de interpretatiemodellen naar de implementatiefase. Hier maakt men de keus voor een ontwikkelomgeving (taal of shell) en deze fase is de "vertaalslag" tussen de interpretatiemodellen enerzijds en de taal of shell anderzijds. De volgende deeltaken en/of vragen worden behandeld:
- keuze van een representatietechniek;
- keuze van een inferentiemechanisme;
- beschrijvingen van scherm-lay-outs, kennisbeveiliging;
- onzekerheidsfactoren;
- beschrijving van implementatie en hardware.

Het interpretatiemodel, dat verschillende beschrijvingsniveaus van kennis heeft, wordt uiteengerafeld en beschreven wordt hoe elk van die niveaus wordt geïmplementeerd in de gekozen taal/shell. Het resultaat van deze fase is een globaal technisch ontwerp van de implementatie en vormt een fundamentele schakel in de documentatie. Als het architectuurmodel onvoldoende wordt beschreven zal de implementatie onbeheersbaar worden. Dit omdat het van belang is om overzicht te hebben waar en hoe de verschillende soorten van kennis (bijvoorbeeld strategische of feitenkennis) terecht komen in de uiteindelijke implementatie.

Implementatiefase

De implementatie is zeer afhankelijk van de keuze die men gemaakt heeft in de architectuurfase aangaande de ontwikkelomgeving of shell. Als men voor een zeer gebruikersvriendelijke shell heeft gekozen dan bevat deze fase niet veel meer dan het invoeren van rules volgens bepaalde formaten. Als men besloten heeft om het kennissysteem in Lisp of Prolog op te zetten dan kan deze fase omvangrijk zijn. De eindprodukten van deze fase zijn:
- de programmatuur;
- de programmadocumentatie;
- een installatiehandleiding;
- een gebruikershandleiding.

Vanuit de architectuurfase is het model van het probleemoplosproces beschikbaar waarin de subtaken, de diverse inputs en outputs beschreven zijn. De programmatuur wordt getransformeerd vanuit deze beschrijving in de volgende stappen:
- het bouwen van een controlestructuur (redeneerstrategieën);
- het maken van de inferentiestructuur (meta-klassen, kennisbronnen);
- het construeren van domeinhiërarchieën (in frames).

Deze top-down-opbouw is eigenlijk een directe weerspiegeling van de verschillende lagen van het interpretatiemodel uit de kennisacquisitiefase. Hier is duidelijk het verschil aan te geven tussen de procedurele code (controle en taakstructuren) en de declaratieve code (meta-klassen, kennisbronnen en domein-frames).

Test en acceptatie

De KADS-methodiek voorziet niet in een uitgewerkte test- en acceptatiefase. Slechts twee belangrijke onderdelen worden aangegeven om te komen tot een oordeel over de implementatie:
- testen op correctheid en volledigheid;
- testen op pathologische condities.

Dit laatste houdt ook in die situaties waarin het geautomatiseerde kennissysteem "geen oplossing"-antwoorden genereert. De expert zelf moet in deze fase "vergeleken" worden met het produkt. Alle cases die opgesteld zijn in de kennisacquisitie moeten worden doorlopen.

Onderhoud

In de KADS-methodiek is een hiërarchie aan te geven van de verschillende soorten kennis. Dat houdt in dat de procedurele kennis (wanneer voer ik welke taak uit) losgemaakt is van de declaratieve kennis (feiten, regels). Hierdoor is het wijzigen van kennis relatief eenvoudig omdat goed aan te geven is waar de te wijzigen kennis is gerepresenteerd en ook hoe de samenhang van kennis is vastgelegd. In het architectuurmodel is gedocumenteerd hoe representaties van kennis en hun onderlinge samenhang zijn gerealiseerd in de implementatie.
Op zich is er nog niet veel ervaring op dit gebied vanwege de relatief kleine hoeveelheid projecten die met behulp van de KADS-methodiek zijn gerealiseerd.

Kenniselicitatietechnieken

De elicitatie') van kennis vormt een zeer belangrijk onderdeel van KADS. Maakt men hier fouten of slaat men delen over, dan breekt dat zeer sterk op in latere fasen. Kenniselicitatie vindt plaats in een vroege fase van KADS, de kennisacquisitiefase.

') Elicitatie komt van het Engelse woord "elicit" wat staat voor "ont-, uitlokken; aan het licht brengen".

Elicitatie van kennis binnen KADS gebeurt door middel van vier technieken die sterk gerelateerd zijn aan de deelfasen van de kennisacquisitie. Deze zijn:
- het gefocusseerd interview;
- het gestructureerd interview;
- hardopdenk-protocollen;
- expertgebruikerdialoog.

De elicitatie van kennis start met een globaal literatuuronderzoek van de knowledge engineer. Aan de hand hiervan wordt een agenda samengesteld die dient voor een gefocusseerd interview. Dat is een sessie waarin de expert in een "normale" conversatie op een breadth-first manier vertelt over de experttaak. De interviewer (de knowledge engineer) houdt de agenda aan en blijft globaal. De opmerkingen van zijn kant beperken zich tot aansporingen, reflecties en zeer beperkte bijsturingen.

Deze vorm van interviewen is duidelijk bedoeld voor het eerste deel van de acquisitiefase, het oriënterend onderzoek. De tweede vorm van elicitatie van kennis is meer specifiek en probeert een depth-first-strategie te volgen. Men spreekt hier van een gestructureerd interview dat samengesteld is uit aandachtsgebieden die naar voren zijn gekomen uit de literatuurstudies en het gefocusseerde interview. De vorm van dit interview is duidelijk strakker en de interviewer zal zeer gestructureerd de agenda aflopen en de diepte ingaan. In het gefocusseerd interview heeft de expert eigenlijk de leiding van het gesprek en de interviewer houdt alleen de agenda aan; in het gestructureerd interview stuurt de interviewer en antwoordt de expert op specifieke vragen. Het gestructureerde interview is bedoeld voor het tweede deel van de acquisitiefase, de probleemdefinitiefase.

De derde vorm, de hardopdenk-protocollen, vinden plaats in de derde fase van de acquisitiefase, de probleemanalysefase. Het principe is eenvoudig, de expert dient al hardopdenkend een voor hem onbekende casus op te lossen. Van belang is het hierbij dat alle denkstappen door de expert genoemd worden. De interviewer stimuleert continu om de expert hardop te laten denken. Het protocol dient "zuiver" te blijven en de expert moet ook vermijden introspectieve en retrospectieve opmerkingen te maken (bijvoorbeeld: ik vind het leuk om ..., daarnet zei ik ook al ...).

De laatste vorm, de expertgebruikerdialoog probeert in de probleemanalysefase een aantal moeilijke aspecten te "meten". Het gaat hier om de communicatiecapaciteiten van het systeem. Denk aan non-verbale communicatie en volgorde van vragen van de expert aan de gebruiker. Een goed hulpmiddel kan zijn om deze sessie te laten verlopen met behulp van twee terminals in gescheiden ruimten. Een andere manier is het vastleggen van een sessie met video-apparatuur of iets dergelijks. Het wel of niet succesvol verloop van een terminal-sessie geeft bovendien een belangrijke indicatie over de haalbaarheid van het uiteindelijke systeem waar tenslotte de gebruiker op dezelfde wijze zijn informatie zal moeten verkrijgen.

Bovengenoemde eerste drie elicitatietechnieken worden in de praktijk met behulp van een bandrecorder vastgelegd en letterlijk uitgetypt. Vooral de hardopdenk-protocoluitwerkingen kunnen met behulp van "templates" leiden tot het herkennen van taakstructuren en interpretatiemodellen van de eigenlijke experttaak.

Kennis representatieformalismen

In het kort zal hier een aantal technieken om kennis te representeren worden genoemd.

1. Produktieregels

   Verreweg de meest gehanteerde vorm. Hebben de volgende algemene vorm: IF (conditie-1 AND conditie-2 ... AND conditie-n) THEN (actie-1, actie-2 ... actie-n).

2. Horn Clauses

   Een "subset" van de produktieregels. De taal PROLOG is, behalve uitbreidingen op het gebied van IO-faciliteiten, een zuivere implementatie van de Horn Clause logica.
   Algemene vorm: B if A1 AND A2 AND ... AND An. De onderdelen Ax en B zijn atomaire formules van de vorm P(t1..tn). P is het predikaatsymbool en tx vormen de termen.

3. Gestructureerde objecten

   Het vormen van prototypische beschrijvingen voor klassen van bepaalde groepen instanties. Een voorbeeld is een "is_een" hiërarchie, die voor de reeks "dier-viervoeter-hond" drie frames geeft, de klasse "dier", de klasse "viervoeter" en de klasse "hond". Op te merken valt dat dit gebruikt kan worden voor inheritance mechanismen. De eigenschappen van een dier gelden voor een viervoeter en de eigenschappen van een viervoeter voor een hond.

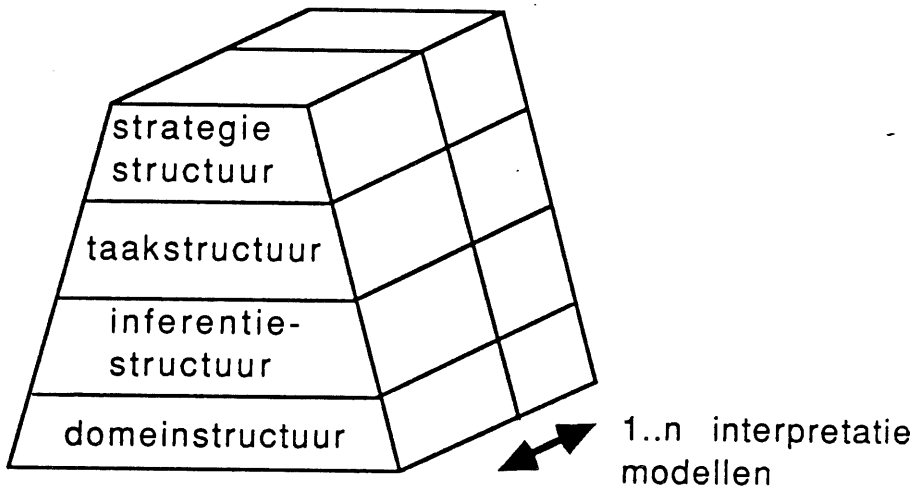
Belangrijke mechanismen die bij produktiesystemen gelden zijn backward en forward reasoning. Als het expertsysteem "aan het werk wordt gezet", dan gaat de interpreter de volgende acties continu ondernemen:
- testen van trigger-gedeelten van produktieregels;
- selecteren van produktieregels;
- uitvoeren van acties.

Bij forward chaining is het conditiegedeelte de trigger van de produktieregel, bij backward chaining juist het actiegedeelte.

Interpretatiemodellen

Bij het uitwerken van het probleemtype (fasen 2 en 3 van de architectuurfase) is het de bedoeling te komen tot een (samengesteld) interpretatiemodel. Een interpretatiemodel is een samenstel van een taakstructuur en van een inferentiemodel. Om deze begrippen te kunnen toelichten is het van belang om eerst de vier kennisbeschrijvingsniveaus te schetsen.

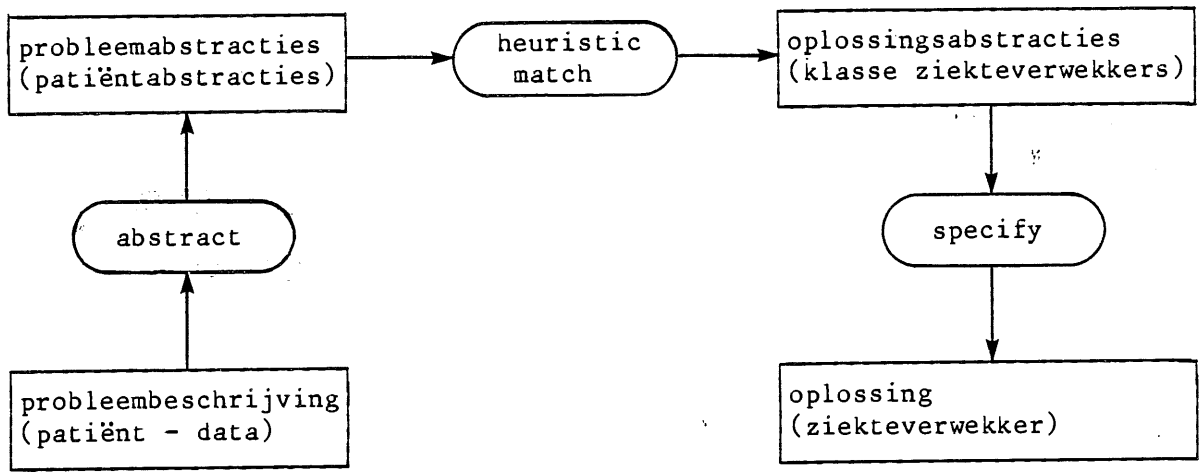
Deze vier niveaus geven de verschillende typen van kennis aan en proberen strikte scheiding tussen die typen aan te brengen. De fundamentele scheiding is de tweedeling in beschrijvende kennis en procedurele kennis.
Het nut hiervan is bijvoorbeeld in de uiteindelijke implementatie groot, feitenkennis wordt losgekoppeld van besturende kennis. De structuur van deze lagen zijn onafhankelijk van kennis representatie formalismen. Het is goed mogelijk om alle niveaus in Prolog te implementeren. Dat houdt in dat één representatiemechanisme gebruikt wordt om alle niveaus te implementeren.



Het domeinniveau bevat beschrijvende kennis, bestaande uit feiten. Van belang is de onderlinge relatie tussen feitenkennis. Denk aan "is een" hiërarchieën. Bij een expert zal blijken dat deze feiten ook op velerlei manieren benaderbaar zijn op verschillende relevante eigenschappen. Het domeinniveau van het expertsysteem zal dus op dezelfde wijze de feitenkennis moeten opslaan en bereikbaar maken.
De twee bovenste lagen geven de procedurele kennis weer.

De inferentiestructuur is de statische beschrijving van de logische samenhang van de experttaak. Er wordt gewerkt met twee soorten bouwstenen, meta-klassen en kennisbronnen.

Inferentiemodel heuristische classificatie



In bovenstaand voorbeeld van een heuristische classificatie zijn abstract, heuristic match en specify de kennisbronnen en de andere "blokjes" vormen de meta-klassen. Meta-klassen zijn eigenlijk een soort velden waar (deel) oplossingen ingevuld worden. Kennisbronnen geven de typen gevolgtrekkingen aan die gemaakt worden uit de feitenkennis (dus via de meta-klassen) uit de domeinstructuur. Het bovenstaande voorbeeld') geeft aan dat het logische denkproces in het vinden van een ziekteverwekker vanuit specifieke patiëntgegevens via een heuristische "match" loopt. Direct waarneembare symptomen van de patiënt worden geabstraheerd tot een globale karakterisering van de patiënt en heuristisch gekoppeld aan ziekteverwekkers of klassen van ziekteverwekkers.
Eén van de dingen die KADS krachtig maken is een modellenbibliotheek van ongeveer 25 inferentiemodellen. Deze modellen blijken bijna alle experttaken te kunnen weergeven. Enkele voorbeelden: simpele_classificatie, heuristische_diagnose, causaal_traceren, lokalisatie, geschiktheidsbeoordeling, bewaking, etc.

De derde laag, de taakstructuur, is een procedurele beschrijving van de acties die plaatsvinden in de inferentiestructuur. Men spreekt hier van doelen en taken. De taken beschrijven de manier waarop kennisbronnen kunnen worden gecombineerd om te komen tot doelen.

') Overgenomen uit het cursusmateriaal van de cursus SKE van Bolesian Systems Europe B.V.

De vierde laag, het strategisch niveau, is eigenlijk een optionele laag. Als de experttaak uit één interpretatiemodel bestaat dan is er geen strategische laag. Als de experttaak uit meerdere interpretatiemodellen bestaat, dan vormt de strategische laag de procedurele beschrijvingen van de gekoppelde interpretatiemodellen. Deze laag is dus eigenlijk een taakstructuur maar dan voor de controle over meerdere interpretatiemodellen.
Een voorbeeld zou kunnen zijn de reeks van taken: bewaking-diagnose-remedie. Elk van deze componenten hebben een eigen inferentiemodel en een eigen taakstructuur. De onderlinge samenhang van deze afzonderlijke taakstructuren is geregeld in de strategische structuur.

Conclusies

KADS is een tot nu toe uniek concept om te komen tot een gestructureerde aanpak van kennissystemen. Het is echter nog dusdanig "vers" van de universiteit dat bepaalde gebieden duidelijk nog niet uitontwikkeld zijn. Het blijkt duidelijk in een behoefte te voorzien. Dit wordt bewezen door het feit dat professionals op het gebied van de knowledge engineering volledig zijn overgeschakeld op deze methode[1]).

Enkele aanvullende opmerkingen:

- KADS is te gebruiken voor kennisformalisatie zonder te komen tot implementatie. Dat houdt in dat men een project kan beëindigen na de kennisacquisitiefase. Het resultaat is dan dat bepaalde expertkennis is geformaliseerd in interpretatiemodellen. Dit kan zeer nuttig zijn voor kennis "continuïteit" binnen een bedrijf of bijvoorbeeld begripsvorming wat nu precies bepaalde expertkennis inhoudt.
  Behalve dat alleen kennisformalisatie wordt gebruikt uit de KADS-methode is het ook goed denkbaar dat in bepaalde gevallen alleen bijvoorbeeld de structuur uit de implementatiefase "geleend" wordt. Bijvoorbeeld in de accountancy-praktijk is het concipiëren door de expert(s) zelf van een discussienota een goed alternatief voor kennisacquisitie.

- De praktijk tot nu toe, analoog met alle andere "expert"systemen, is dat de systemen ontwikkeld met behulp van KADS duidelijk in de eenzijdige hoek van de analytische experttaken zitten. De interpretatiemodellen bibliotheek is wel compleet maar niet uitgewerkt voor de predictieve en synthese modellen.
  Overbekend zijn dan ook taken als diagnose en geschiktheidsbeoordelingen, maar planningen en ontwerpen bijvoorbeeld zijn al duidelijk minder

[1]) Bij de ontwerpers van de SKE-methode, het Helmondse bedrijf Bolesian werkt iedereen met KADS.

triviaal en dus niet volledig uitgewerkt. Dat houdt in dat nog niet vaststaat dat deze techniek altijd en voor alle kennisdomeinen toepasbaar is.

- Wat toch uiteindelijk een nadelig aspect vormt, is dat het nogal lang duurt voordat het uiteindelijke produkt gerealiseerd is. Het project is wel gefaseerd en beheersbaar geworden met KADS maar wat nauwelijks in te schatten is, is het uiteindelijke resultaat. Met andere woorden, prototyping geeft veel sneller een beeld van de mogelijkheden en de uiteindelijke vorm. Het is dus erg moeilijk om van tevoren in te schatten hoe de "baten" zullen zijn als het gaat over experimentele systemen. Tenslotte zullen bij een niet triviaal systeem de ontwikkelkosten waarschijnlijk toch hoog zijn.

- Structured Knowledge Engineering heeft in de initiatiefase een heel pragmatische opsomming van punten waarop gelet moet worden als men een haalbaarheidsstudie samenstelt. Direct uit de praktijk en ook direct toepasbaar in de praktijk.

- Artificial Intelligence is tegenwoordig, vooral in de Verenigde Staten, al weer een beetje "uit". Mogelijke oorzaken moeten toch worden gezocht in het feit dat veel experimentele prototypes bij lange na niet voldeden aan de verwachtingen. Grote investeringen in hard- en software bleken niet de baten op te leveren die men dacht te kunnen behalen. Mogelijk is een ietwat meer gestructureerde aanpak de oplossing. KADS/SKE biedt in ieder geval een breed scala van praktische handvaten.

Literatuur

- Esprit paper P1098.
- Cursusdocumentatie "Structured Knowledge Engineering". Bolesian Systems Europe B.V.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

COMPACT

Winter 1987/1988

EEN INTRODUCTIE TOT BEVEILIGING BIJ DATATRANSMISSIE

door Ing. H.A.J.M. Spape

1. Inleiding

Een organisatie die gebruik maakt van geautomatiseerde gegevensverwerking, hanteert daarbij tegenwoordig nagenoeg altijd datatransmissie als middel voor het transport van gegevens naar en van de computerinstallatie. Een situatie zonder beeldscherm-terminals die via een datatransmissieverbinding op de computer zijn aangesloten is niet meer reëel. Verbindingen tussen computers onderling komen steeds meer voor. Nationale en internationale netwerken bieden mogelijkheden tot datatransmissie met computerinstallaties op vele honderden kilometers afstand.

Datatransmissie en netwerken scheppen nieuwe mogelijkheden doch leiden tevens tot nieuwe bedreigingen voor de betrouwbaarheid en de continuïteit van de geautomatiseerde informatievoorziening. Als regel zijn maatregelen vereist om deze bedreigingen te beheersen. Hiertoe zal enerzijds gebruik worden gemaakt van technische hulpmiddelen, zoals beveiligingsapparatuur en -programmatuur. Anderzijds zullen organisatorische voorzieningen getroffen moeten worden. Dit artikel geeft een overzicht van de bedreigingen die zich in een situatie met datatransmissie kunnen voordoen en bespreekt een aantal technische en organisatorische voorzieningen die ter beheersing van de bedreigingen kunnen worden getroffen.

Opgemerkt moet worden dat de beheersingsproblematiek hier slechts in algemene zin besproken kan worden. Welke bedreigingen in een concrete situatie van toepassing zijn, wat de mogelijke gevolgen daarvan zijn en (daaruit voortvloeiend) welke investeringen in techniek en organisatie verantwoord zijn om de bedreigingen te beheersen, is situatie-afhankelijk. Een goed uitgangspunt om de problematiek in een concrete situatie te onderzoeken is een risico-analyse. Deze dient echter niet voor de datatransmissie alleen te worden uitgevoerd, doch dient deel uit te maken van een analyse van de risico's die van toepassing zijn op de gehele (geautomatiseerde) informatievoorziening. Professionele ondersteuning is hierbij veelal onontbeerlijk.

2. Bedreigingen en risico's

In de inleiding zijn reeds de termen bedreiging en risico gebruikt. Deze termen hebben een verschillende betekenis. Een bedreiging is te definiëren

als een ongewenste gebeurtenis die zich in een bepaalde situatie kan voordoen. Het risico geeft aan welke gevolgen het manifest worden van de bedreiging heeft, zo mogelijk uitgedrukt in geld. Risico is dan de vermenigvuldiging van de kans dat de bedreiging zich voordoet en het financiële verlies dat als gevolg van deze gebeurtenis wordt veroorzaakt. Uit deze definities kan worden afgeleid dat in dit artikel slechts bedreigingen besproken kunnen worden. Risico's zijn immers situatie-afhankelijk. Uiteindelijk gaat het er evenwel om de risico's te beheersen.

In algemene zin kunnen bij datatransmissie de volgende bedreigingen worden onderscheiden:
a. het verloren, verminkt of vertraagd geraken alsmede het toevoegen van gegevens;
b. het onbedoeld bekend geraken van gegevens;
c. het niet beschikbaar zijn van de transmissievoorzieningen waardoor geautomatiseerde gegevensverwerking niet (goed) mogelijk is.

Enkele voorbeelden van directe oorzaken van deze bedreigingen zijn:

Ad a. Verloren of verminkt geraken

- Technische storingen gedurende het gegevenstransport (zoals het niet goed functioneren van transmissie-apparatuur).
- Atmosferische invloeden tijdens het gegevenstransport (onweer, magnetische velden van elektromotoren).
- Opzettelijk beïnvloeden van de gegevens tijdens transport (door het aanbrengen van magnetische velden waarmee gegevens worden veranderd of onderdrukt).
- Opzettelijk wijzigen van gegevens na het (onbevoegd) verkrijgen van toegang tot de computerinstallatie via datatransmissieverbindingen.

Ad b. Onbedoeld bekend geraken

- Het door het netwerk afleveren van informatie op de verkeerde bestemming.
- Het opzettelijk aftappen van transmissieverbindingen.

Ad c. Niet beschikbaar zijn van communicatievoorzieningen

- Het niet functioneren van cruciale componenten in het netwerk.
- Het niet tijdig reageren op storingen.

Voor vele datatransmissieverbindingen worden voorzieningen getroffen om bedreigingen dan wel specifieke oorzaken daarvan te compenseren. Dit kan door middel van preventieve maatregelen (deze voorkomen dat de oorzaak zich kan voordoen) en door repressieve maatregelen (waarbij wordt vastgesteld dat de bedreiging zich heeft voorgedaan en daaropvolgend een herstelactie plaatsvindt). Dergelijke maatregelen, die direct bedreigingen tegengaan of compenseren worden hier beveiligingsmaatregelen genoemd.

Beheersingsmaatregelen dienen hiervan te worden onderscheiden. Deze maatregelen zijn erop gericht een effectieve beveiliging te realiseren en in stand te houden.
Beveiligingsmaatregelen zijn voor het merendeel technisch van aard. Beheersing is primair een organisatorische zaak.

3. Beveiligingsmaatregelen

De techniek biedt een aantal mogelijkheden om tegen de genoemde bedreigingen te beveiligen. Deze mogelijkheden worden hierna besproken. Vooropgesteld dient evenwel te worden dat technische beveiliging niet op zichzelf kan worden beschouwd. Zonder een adequate organisatie ter ondersteuning zijn technische maatregelen van beperkt nut.

Controleberekeningen

Omdat gedurende de transmissie storingen kunnen optreden zijn technieken ontwikkeld waarmee door de ontvanger van een bericht kan worden vastgesteld dat het bericht foutief is geraakt. Deze beveiliging werkt als volgt:
- de zender voert een berekening uit op basis van de inhoud van het te verzenden bericht (voor deze berekening zijn verschillende technieken beschikbaar);
- het resultaat van de berekening wordt met het bericht meegestuurd;
- de ontvanger voert dezelfde berekening uit en vergelijkt het resultaat met het meegezonden resultaat.

Op deze wijze kan de ontvanger vaststellen of een bericht inhoudelijk foutief is geraakt.
Het herstellen van een eventuele fout kan op twee manieren. Het meest toegepast wordt het opnieuw versturen van het bericht, nadat de ontvanger de afzender daarom heeft verzocht. Ook mogelijk is een zodanige controleberekening toe te passen, dat kan worden vastgesteld op welke plaatsen het bericht fouten bevat, waardoor deze door de ontvanger kunnen worden gecorrigeerd.

Hierbij dienen twee opmerkingen te worden gemaakt:
- het aantal fouten dat wordt ontdekt is afhankelijk van de toegepaste controletechniek;
- deze controleberekeningen zijn niet bestand tegen opzettelijke wijzigingen. Het controletotaal kan immers eveneens worden gewijzigd.

Identificatie

Bij gebruik van datatransmissie is de identificatie van de communicerende partijen bijzonder belangrijk. De identiteit van de partijen wordt gebruikt

voor beslissingen inzake het al dan niet verkrijgen van toegangsbevoegdheden op verschillende niveaus (computerinstallatie, groepen programma's, transacties binnen programma's, door middel van transacties bewerkte gegevens).
Onderscheiden kunnen worden:
- locatie-identificatie;
- apparatuuridentificatie;
- eindidentificatie.

Hiervan is eindidentificatie het belangrijkst. Beide andere zijn aanvullend en worden veelal in specifieke situaties toegepast.

Locatie-identificatie

Locatie-identificatie is erop gericht vast te stellen dat gecommuniceerd wordt met een tevoren bekende locatie. Het wordt veelal toegepast wanneer gebruik wordt gemaakt van openbare netwerken zoals het telefoon- en telexnetwerk. De identificatie vindt dan plaats door middel van het kiezen van bekende telefoon-/telexnummers. Dit kan handmatig of geautomatiseerd gebeuren. Een voorbeeld in dit verband is een terugbelautomaat, die op grond van een via een telefoonlijn verstuurde identificatie, deze telefoonverbinding verbreekt en terugbelt naar een bij de identificatie behorend telefoonnummer om de definitieve verbinding tot stand te brengen.

Apparatuuridentificatie

Apparatuuridentificatie vervult als belangrijkste functie het herkennen van een specifiek apparaat, als bevoegde communicerende partij. Deze herkenning kan bijvoorbeeld worden toegepast om aan terminals op bepaalde locaties bepaalde bevoegdheden (niet) toe te kennen, ongeacht of degene die van deze terminals gebruik maakt, deze bevoegdheden heeft.
Apparatuuridentificatie vindt veelal plaats door het gebruik van een in de hardware opgenomen code (adres) dat bij de andere communicerende partij bekend is.

Eindidentificatie

Eindidentificatie is erop gericht de identiteit vast te stellen van de communicerende partijen. Veelal betreft dit een gebruiker en een applicatieprogramma. De gebruiker maakt zich bijvoorbeeld kenbaar door een gebruikerscode en een wachtwoord (password), welke combinatie door of ten behoeve van de applicatie wordt gecontroleerd. Andere technieken zijn het gebruik van een PIN-code (PIN: Personal Identification Number), de herkenning van lijnen van de hand of herkenning van oogpatronen.

Opmerkingen

Hoewel de identificatie betrekking zou moeten hebben op beide communicerende partijen, is in vele gevallen sprake van eenrichtingsverkeer. De computerinstallatie/applicatie waarmee wordt gecommuniceerd identificeert zich veelal niet ten behoeve van de terminal of gebruiker, althans niet op de wijze die van de gebruiker verwacht wordt. Volstaan wordt veelal met een bericht waaruit blijkt dat met computer XYZ verbinding is verkregen.

Identificatie gebeurt door middel van het uitwisselen van berichten via datatransmissie. Zonder aanvullende maatregelen (zoals vercijfering, zie hierna) is deze berichtuitwisseling in principe waarneembaar voor derden (door middel van aftappen van transmissielijnen, of door zogenaamde monitoring van het berichtenverkeer). Tevens kan door berichten te onderscheppen en "na te spelen" de door een gebruiker bedoelde computer worden nagebootst.

Vercijfering

Bij toepassing van vercijfering (encryptie) worden gegevens omgezet naar "geheimtaal". Dit gebeurt door een berekening (volgens het encryptie-algoritme) die wordt uitgevoerd met de gegevens en een sleutel. De ontvanger van het vercijferde bericht voert een omgekeerde bewerking (ontcijfering, decryptie) uit, waardoor het bericht weer in de oorspronkelijke vorm (de "klare tekst") wordt teruggebracht. Encryptietechnieken zijn niet "onkraakbaar". Zij berusten op het principe dat vele jaren rekenen nodig zijn om een vercijferd bericht te achterhalen. Wanneer de computertechniek nieuwe mogelijkheden biedt waardoor aanmerkelijk sneller dan thans gerekend kan worden, zijn de huidige encryptietechnieken mogelijk niet meer effectief.

Het spreekt vanzelf dat de sleutels geheim moeten blijven om te voorkomen dat derde partijen de ontcijfering kunnen uitvoeren. Dit vereist dat sleutels periodiek worden gewijzigd. Zeker in netwerken met veel gebruikers kan dit complex zijn. Wanneer alle gebruikers met elkaar op basis van vercijfering moeten communiceren, vergt dit bij de hiervoor getypeerde techniek een sleutel per gebruikerspaar, waardoor in een netwerk met bijvoorbeeld 50 gebruikers, 1225 sleutels aanwezig zijn die periodiek gewisseld moeten worden. In zo'n situatie is veelal encryptie volgens het "public-key" principe beter. Hierbij heeft elke partij in het netwerk een paar sleutels, waarvan er een publiek bekend wordt gemaakt en de andere geheim blijft. De zendende partij zal met de publieke sleutel van de ontvanger vercijferen. Deze is de enige die over de corresponderende geheime sleutel beschikt en daarmee de ontcijfering kan uitvoeren.

Authenticering

De algoritmen die voor de berekeningen bij encryptie worden gebruikt, vinden tevens toepassing bij authenticering. Doel hiervan is vast te stellen dat een bericht zoals dat ontvangen is, afkomstig is van de partij die beweert het verzonden te hebben. Hierbij behoeft niet het gehele bericht te worden vercijferd. Op basis van de berichtinhoud en de sleutel wordt een code (MAC: Message Authenticator Code) berekend die als soort controlegetal aan het bericht wordt toegevoegd. De ontvanger voert met zijn sleutel dezelfde berekening uit en vergelijkt het resultaat met de toegevoegde MAC. Wanneer deze gelijk zijn, is het bericht gedurende transport niet gewijzigd en is door gebruik van de sleutel de afzender bekend.

End-to-end versus lijngerichte maatregelen

Een netwerk bestaat uit een aantal transmissiekanalen, die eventueel via tussenstations, de eindstations met elkaar verbinden. Bij het toepassen van lijngerichte beveiligingsmaatregelen worden de te onderscheiden transmissieverbindingen tussen stations beveiligd (bijvoorbeeld door controleberekeningen en/of encryptie):

Lijngerichte beveiligingsmaatregelen

```
E --*==========*-- T --*==========*-- T --*==========*-- E
```

E: Eindstation; T: Tussenstation; *: beveiligingspunt; =: beveiligd transmissietraject.

De lijngerichte techniek vereist dat alle tussenstations veilig zijn. Dat wil zeggen dat de berichten daar niet kunnen worden ingezien of gewijzigd, hetzij opzettelijk, hetzij onopzettelijk. Controleberekeningen vinden bijvoorbeeld plaats voor elke verbinding, waarbij aan het eind van de verbinding de controle plaatsvindt. Wordt het bericht in een tussenstation gewijzigd, of gaat het verloren, dan zal de zender reeds een bevestiging van goede ontvangst kunnen hebben gehad en zal hij zich verder op dit gegeven baseren. Dit terwijl het ontvangende eindstation niet het bericht ontvangt dat door de zender is verstuurd.

Bij end-to-end maatregelen worden de beveiligingen aangebracht bij de zender en bij de ontvanger, waardoor de berichten gedurende het gehele transmissietraject beveiligd zijn. Als regel is end-to-end beveiliging een vereiste voor betrouwbare transmissie. De lijngerichte beveiliging is echter veelal eveneens nodig voor technisch betrouwbare en meer efficiënte transmissie.

End-to-end beveiliging

E --*==========T==========T==========*-- E

Continuïteitsgerichte maatregelen

De beveiligingsmaatregelen gericht op de beschikbaarheid van de transmissievoorzieningen zijn qua karakter niet afwijkend van die welke in het algemeen voor de continuïteit van de gegevensverwerking worden getroffen. Gedacht moet worden aan back-up-apparatuur, brandbeveiliging etc. Bij het maken van back-up-kopieën dient tevens de netwerkprogrammatuur en de netwerkstuurinformatie alsmede eventuele bestanden met sleutels etc. betrokken te worden.
Als uitwijkmogelijkheid bij het uitvallen van vaste lijnen tussen twee punten zou het telefoonnetwerk kunnen worden gebruikt. Weinig is te doen tegen het uitvallen van een PTT- of bedrijfstelefooncentrale. Het is echter wel zaak de bedrijfstelefooncentrale in de toegangsbeveiliging en de overige (brand/water)beveiliging te betrekken. Het komt wel voor dat de computerruimte goed beveiligd is, terwijl de centrale, waarlangs soms alle transmissieverbindingen met de computerruimte lopen, over het hoofd is gezien.

4. Beheersingsmaatregelen

Beveiligingsbeleid *)

De basis van een effectieve beveiliging tegen de genoemde bedreigingen is een adequate organisatie om met deze bedreigingen om te gaan. Zonder deze organisatie dreigt het gevaar dat onevenwichtig en daarmee ineffectief en inefficiënt beveiligd wordt. Deze organisatie dient gebaseerd te zijn op een aantal door het hoogste management te formuleren uitgangspunten betreffende beveiliging, waarbij wordt uitgegaan van de doelstellingen die ten aanzien van de organisatie als geheel (dienen te) zijn gesteld. Deze uitgangspunten dienen te zijn verwoord in het beveiligingsbeleid. Hierin worden onder meer verantwoordelijkheden afgebakend en basiseisen ten aanzien van de gegevens van de organisatie geformuleerd. Zo zou bijvoorbeeld kunnen worden gesteld dat een gegevensclassificatie moet worden opgesteld door of namens het gebruikersmanagement en dat door automatisering technische beveiligingen voor de verschillende gegevensklassen dienen te worden getroffen. Hierbij zou in het beleid kunnen zijn verwoord dat deze technische maatregelen op grond van risico-analyse dienen te worden geselecteerd en dat de afweging om bepaalde gegevens al dan niet te beveiligen door de gebruikersorganisatie gedaan wordt.

*) Beveiligingsbeleid en risico-analyse worden meer diepgaand behandeld in het artikel "Beveiligen tegen computermisbruik" in Compact Herfst 1987 (A.W. Neisingh, H. Vossen).

Verantwoordelijkheden

Aangezien het er bij dit onderwerp primair om gaat, de gegevens te beveiligen, dient uitgangspunt bij de beveiligingsorganisatie de verantwoordelijkheid voor de gegevens te zijn. Deze verantwoordelijkheid berust bij de gebruikersorganisatie en niet bij de automatiseringsorganisatie. Een automatiseringsorganisatie dient, conform door de gebruikersorganisatie gestelde eisen ten aanzien van de gegevens (bijvoorbeeld vertrouwelijkheid) technische oplossingen te verzorgen/voor te stellen, die aan deze eisen voldoen. Gezien de aanwezigheid van deskundigen zal de automatiseringsorganisatie de gebruikers bij deze formulering van eisen kunnen ondersteunen (bijvoorbeeld bij het uitvoeren van een risico-analyse). In feite worden taken door de gebruikersorganisatie aan de automatiseringsorganisatie gedelegeerd.

De beheersingsmaatregelen die op grond van de gestelde eisen voor datatransmissie getroffen moeten worden dienen in overeenstemming te zijn met de beveiliging die uit anderen hoofde, doch op basis van dezelfde eisen wordt gerealiseerd. Het nut van vercijfering is beperkt wanneer bijvoorbeeld door automatiseringspersoneel eenvoudig toegang kan worden verkregen tot de voor de vercijfering gebruikte sleutels.

Risico-analyse *)

Een risico-analyse heeft als belangrijkste doelstellingen:
a. het inventariseren van de bedreigingen waaraan de organisatie blootstaat voor wat betreft de automatisering en als deel daarvan de datatransmissie;
b. het vaststellen welke inspanningen uit financieel oogpunt wenselijk en gerechtvaardigd zijn om tegen de bedreigingen te beveiligen.

Een risico-analyse is geen eenmalig proces. Zowel in de eigen automatiseringsinfrastructuur als in de omgeving kunnen zich veranderingen voordoen die een risico-analyse verouderd maken. Het is daarom wenselijk periodiek zo'n risico-analyse uit te voeren.

Change management-organisatie

De technische beveiligingsmaatregelen die getroffen worden zijn als regel gerealiseerd in apparatuur en programmatuur, die veelal gebruik maken van in bestanden of anderszins vastgelegde stuur- of hulpgegevens (bijvoorbeeld gebruikerscodes, passwords, encryptiesleutels; netwerkdefinitie).

*) Beveiligingsbeleid en risico-analyse worden meer diepgaand behandeld in het artikel "Beveiligen tegen computermisbruik" in Compact Herfst 1987 (A.W. Neisingh, H. Vossen).

Deze apparatuur, programmatuur en stuur-/hulpgegevens dienen onderwerp te zijn van een change management-organisatie, die als doelstelling heeft wijzigingen op een beheerste, gecontroleerde wijze door te voeren.
Deze change management-organisatie is fundament van een goede beveiliging. Trefwoorden in dit kader zijn: functiescheiding ontwikkeling/produktie, bevoegdheid aanvraag wijziging, acceptatietest, overdrachtsprocedure, beveiligde acceptatie-omgeving, beveiligde operationele omgeving, controle op overdrachten.
In het algemeen geldt dat wijzigingen in toepassingsprogrammatuur en op de gebruikers betrekking hebbende stuur-/hulpgegevens door de verantwoordelijke gebruikers moeten worden geautoriseerd en geaccepteerd. In het geval een netwerk wordt gebruikt zal een aantal programmafuncties (bijvoorbeeld de controleberekeningen of het vercijferalgoritme) zijn ondergebracht in algemene (i.e. voor alle applicaties gebruikte) programmatuur en apparatuur. Dan zal mede uit hoofde van vereiste technische kennis, het niet goed mogelijk zijn autorisatie/acceptatie door gebruikers te laten uitvoeren. Het is dan de taak van het automatiseringsmanagement om voldoende functiescheiding en procedurele maatregelen in de eigen organisatie aan te brengen opdat (gewijzigde) produkten onafhankelijk van ontwikkeling kunnen worden geaccepteerd. Hierover dient aan de gebruikersorganisatie verantwoording te kunnen worden afgelegd.

Key management-organisatie

Bij het toepassen van encryptie of MAC's is een goede key management-organisatie van belang. Het nut van deze beveiligingstechnieken staat en valt met het sleutelbeheer. Van belang is vast te stellen:
- wie (i.e. welke functie) bepaalt wanneer en met welke frequentie sleutels gewijzigd worden;
- wie bepaalt welke waarde de sleutels krijgen;
- op welke wijze de sleutels worden verspreid;
- door wie de sleutels in de door het encryptie-algoritme gehanteerde tabellen worden ingevoerd;
- hoe controle op het sleutelbeheer kan worden uitgeoefend;
- hoe synchronisatie plaatsvindt tussen de betrokken partijen bij het wisselen van de sleutels.

Er is apparatuur op de markt die een belangrijk deel van de uitvoering van key management overneemt (bijvoorbeeld genereren en verspreiden sleutels).

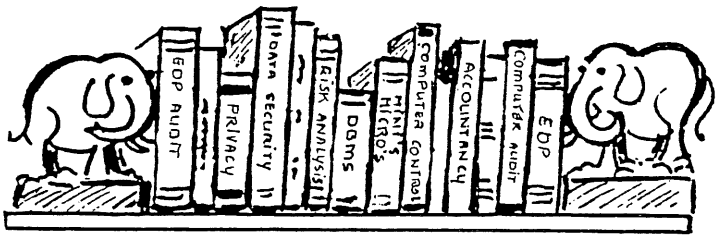
5. Besluit

Besproken is een aantal bedreigingen alsmede technische en organisatorische maatregelen in het kader van beveiliging van datacommunicatie. Benadrukt moet worden dat het gegeven beeld zeker niet volledig is. Zowel op het technische als het organisatorische vlak zijn aanvullende en specifieke

maatregelen denkbaar. Een effectieve beveiliging zal voor elke situatie afzonderlijk moeten worden ontworpen. Dit vergt van degenen die met deze problematiek worden belast inzicht in beide pijlers van de beveiliging, techniek en organisatie. Veelal is de uitwerking van de beveiliging bij de automatiseringsorganisatie ondergebracht. Het organisatorische aspect krijgt dan soms onvoldoende aandacht. Professionele ondersteuning bij het ontwerp van de beveiliging, alsmede een onafhankelijke beoordeling van gerealiseerde maatregelen zijn krachtige hulpmiddelen om tot een effectieve beveiliging te komen.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services



Winter 1987/1988

Boeken

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

Gegevensbescherming
Een praktisch model voor het opzetten en invoeren van een systeem van gegevensbeschermende maatregelen
J.F. Bautz, A. Brouwer en A.J.F. Jongenelen.

door drs. P. Westdijk.

Het boek "Gegevensbescherming" geeft een goede, bruikbare handreiking aan diegenen die belast zijn met het opzetten van een stelsel van gegevensbeschermende maatregelen. Ook als naslagwerk kan het boek een nuttige rol vervullen.

De auteurs zijn uitgegaan van een drietal invalshoeken, die elk op hun beurt weer in 3 aspecten uiteenvallen:
1. Gevolg van de inbreuk:
   - vertrouwelijkheid;
   - betrouwbaarheid;
   - continuïteit.
2. Soort beschermingsmaatregelen:
   - organisatorisch;
   - fysiek;
   - programmeerbaar.
3. Aard van de beschermingsmaatregelen:
   - preventief;
   - repressief;
   - correctief.

Grafisch weergegeven ontstaat dan een kubus van 3x3x3 blokken, die door het boek heen wordt gebruikt als leidraad en plaatsbepaling. Dit lijkt een nuttig hulpmiddel om aan te geven waar een bepaalde maatregel thuishoort in het totaal van beschermende maatregelen.

Na een inleidend hoofdstuk gaan de auteurs in op risico-management, dat als volgt wordt ingedeeld:
1. opstellen risicobeleidsplan;

2. risico-analyse:
   - inventariseren risico's;
   - toekennen waarschijnlijkheden;
   - kwantificeren gevolgen;
   - inventariseren maatregelen;
   - kwantificeren gevolgen van de maatregelen;
   - uitvoeren kosten-/batenanalyse;
3. toetsen en beslissen concept-beschermingsplan;
4. invoeren en evalueren:
   - effectueren beschermingsplan;
   - verrichten metingen;
   - evalueren maatregelen;
   - bijsturen maatregelen.

Het **derde hoofdstuk** geeft een overzicht van de **organisatorische** beschermingsmaatregelen. "Toegang" is hierbij het centrale begrip. De toegang tot ruimtes en gegevens kan worden beheerst door autorisaties, die aansluiten bij verschillen in beveiligingsniveaus (computerzaal vs. kantoren vs. kantine bv.).

Betrouwbaarheid kan worden beheerd door middel van onder andere functiescheidingen, die de integriteit van gegevens moet waarborgen. Op die integriteit kan een specifieke controle plaatsvinden.
Belangrijkste voorstellen voor procedures die de auteurs geven leggen de nadruk op een functionele scheiding tussen gebruikers/ontwikkeling/produktie en het motiveren en opleiden van mensen in de beschermingsgedachte.

Risico-analyse geeft volgens de auteurs aanknopingspunten voor een adequate beveiliging tegen calamiteiten. Naast het voorkomen dient de nodige aandacht te worden besteed aan herstelwerkzaamheden na een calamiteit; reconstructie-archief en uitwijk nemen hier een belangrijke plaats in.

Het **vierde hoofdstuk** gaat in op de **fysieke** beschermingsmaatregelen. Toegangsbeperking, uitval hardware en uitval voorzieningen, zijn van oudsher belangrijke aspecten geweest en zijn dan ook gedetailleerd uitgewerkt in de literatuur door middel van checklists en dergelijke.

Voor de maatregelen rond vertrouwelijkheid wordt de fysieke toegang tot gebouwen/ruimten genoemd. Betrouwbaarheid wordt bevorderd door onderhoud aan en foutregistratie van de hardware, die dubbel kan worden uitgevoerd. Ook de handling van opslagmedia dient in dit kader te worden beheerst. Verder worden noodstroomvoorzieningen, brandmelders en dergelijke genoemd in dit kader.

Het **vijfde hoofdstuk** geeft een aantal aspecten van **programmeerbare** beschermingsmaatregelen. Deze vervangen fysieke maatregelen bij datacommunicatie; access-control-programmatuur vormt hierin de belangrijkste component.

De eigenaar van gegevens kan als enige de inhoudelijke integriteit vaststellen; het rekencentrum kan dat voor de technische integriteit. De auteurs beschrijven een stelsel van controlegetallen op bestanden met data en instructies (bestandsbeheer en programmabeheer). Ook het automatisch dumpen van bestanden op tape na een wijziging wordt in dit licht naar voren gebracht.

In **hoofdstuk 6** wordt een aantal randvoorwaarden besproken:
- functiescheiding in het rekencentrum en gebruikersorganisatie;
- coderingssysteem van bestanden;
- documentatie up-to-date, als noodzaak geaccepteerd door ontwikkelaars;
- gebruik van standaardmethoden en -technieken in ontwikkelingsprojecten, als aanvulling op 2 hiervoor genoemde voorwaarden;
- toetsen en testen van alle mijlpaalprodukten in ontwikkelingsprojecten en goed gecoördineerde en volledige acceptatietests;
- huisregels mogen niet als te zware belemmering worden gezien; procedures en regels dienen echter wel zoveel mogelijk te worden vastgelegd (bijvoorbeeld in functiebeschrijvingen);
- interne controle (zowel beheersing als verantwoording) in het gehele traject van ontwikkeling en produktie.

In **hoofdstuk 7** ten slotte wordt gesproken over de **implementatie** van gegevensbescherming in de organisatie.
Risico-management dient in het informatieplan reeds te zijn opgenomen en daarin geheel door te werken. Het top-management dient zich eveneens hiermee bezig te houden.

Om gegevensbescherming in de bestaande organisatie te implementeren staan de auteurs een aantal afdelingen voor, die zich met deeltaken bezighouden. Deze mogelijkheid is gestoeld op de werkkring van de auteurs.

Verder wordt gepleit voor een projectmatige aanpak: risico-analyse dient in de eerste fasen van het ontwikkelingstraject reeds een element te zijn met een toetsing per fase.

Als laatste komt de acceptatie van beschermingsmaatregelen aan de orde: de medewerkers moeten met de maatregelen kunnen werken zonder "te veel last" daarvan te hebben.

Conclusie

Al met al is er sprake van een goed leesbaar boek, dat een redelijk compleet beeld geeft van de basisproblematiek van de gegevensbescherming in moderne grootschalige automatiseringsorganisaties.

Als leerboek is de gekozen aanpak goed hanteerbaar. Voor andere invalshoeken (bijvoorbeeld naar verantwoordelijkheden in een organisatie) kunnen andere doorsnedes van de kubus worden gebruikt.

Winter 1987/1988

TIJDSCHRIFTEN

onder redactie van mw. D. Jansen Heijtmajer, mw. drs. A. Klaver, J.L.H. Kooijman met medewerking van mw. ing. I.M. van Duin.

In EDP AUDIT INFO - een periodiek ten behoeve van KPMG Klynveld EAS - werd recent aandacht besteed aan Electronic Funds Transfer, het elektronisch uitvoeren van betalingen, dat bij veel bedrijven en instellingen in de belangstelling staat.

Electronic Funds Transfer: door mw. ing. I.M. van Duin.

Inleiding

Het initiatief tot het elektronisch betalen in Nederland werd genomen door diverse benzine- en lease-maatschappijen, door middel van het uitgeven van private label-kaarten. Dit zijn betaalkaarten waarmee binnen het gesloten betalingscircuit van de betreffende maatschappij kan worden betaald. Omdat de introductie van een nationaal systeem van elektronisch betalen op zich liet wachten, gingen steeds meer maatschappijen en winkelconcerns over tot het uitgeven van private label-kaarten.
De ontwikkeling van één nationaal elektronisch betaalsysteem heeft de laatste tijd een impuls gekregen door de toenemende fraude met betaalcheques, het steeds duurder worden van het betalingsverkeer en de achterstand in het elektronisch betalen ten opzichte van het buitenland.

Uit de kranten: Akkoord banken en Postbank

De Nederlandse banken hebben eind vorig jaar een akkoord bereikt over één elektronisch betalingssysteem, waarbij men met de passen van de verschillende banken in één uniform betaalautomaat kan gaan betalen.
Eind 1988 zal dit systeem waarschijnlijk operationeel zijn. Bij de grotere detaillisten in Nederland zal dan een betaalautomaat geplaatst zijn, die geschikt is voor elektronisch betalen door pashouders van alle Nederlandse banken.

Er komt één gemeenschappelijke instelling (switch) die de gegevens van de elektronische betaaltransacties uit de betaalautomaat van de detaillist ophaalt en deze vervolgens doorstuurt naar de computers van de betrokken banken. Deze instelling gaat een deel van de kosten van het elektronisch betalen doorberekenen aan de detaillisten.
In het akkoord is ook vastgelegd dat de banken en de Postbank het elektronisch betalen zullen stimuleren en daarmee op brede schaal een goedkoop, efficiënt, veilig en eenvoudig hanteerbaar alternatief bieden voor de bestaande betaalvormen.
De aanschaf van de betaalautomaat en het onderhoud ervan komen voor rekening van de detaillist, terwijl de banken de kosten zullen dragen die gepaard gaan met de ontwikkeling van de verbinding tussen betaalautomaten en bankcomputers.
Het beleid van de individuele financiële instelling bepaalt of ook de consument moet betalen voor het gemak van het elektronisch betalen. Van de meeste banken is nog niet bekend of zij een gedeelte van de kosten van transacties zullen afwentelen op de consument. De Postbank zegt toe een gratis betaalpakket, inclusief de giromaatpas, te leveren.

Magneetstripkaarten en chip-kaarten

Er zijn twee soorten betaalkaarten: de magneetstripkaart en de chip-kaart of smartcard. Een magneetstripkaart is een plastic kaart die een stripje magnetisch materiaal bevat, waarop de gegevens van de klant zijn vastgelegd. Deze gegevens bevatten een identificatie van de gebruiker.
Vaak moet de gebruiker tevens een Personal Identification Number (PIN) intoetsen. Op grond van de juistheid van deze PIN wordt vastgesteld of de gebruiker de eigenaar van de kaart is. De magneetstripkaart biedt de gegevens op de kaart geen beveiliging. De gegevens kunnen door een willekeurige kaartlezer worden uitgelezen en vervolgens worden verzameld.
De chip-kaart heeft hetzelfde uiterlijk als de magneetstripkaart en werkt voor de gebruiker op dezelfde manier. Het verschil met de magneetstripkaart is dat de kaart een chip bevat waarin gegevens beschermd kunnen worden opgeslagen. Er kan zo bijvoorbeeld gebruik worden gemaakt van een persoonlijke sleutel, waarmee de berichten worden versleuteld bij versturing naar de kaartuitgevende instelling. Op de kaart is een geheugen aangebracht, waarin de sleutels en eventueel het saldo van de klant worden opgeslagen. Het moet onmogelijk zijn om de informatie van de kaart te lezen tijdens routinehandelingen. De chip-kaart is, in tegenstelling tot de magneetstripkaart, niet te kopiëren.
In Nederland wordt de chip-kaart nog niet gebruikt. Redenen hiervoor zijn dat de aanmaakkosten hoog zijn en de banken reeds veel geld in magneetstripkaarten geïnvesteerd hebben.

Betaling door middel van de betaalpas

De betaalpas kan op twee manieren worden gebruikt: via geldautomaten en via afrekensystemen in de winkel (point of sale terminals).
De betaling door middel van een betaalpas bestaat uit twee stappen:
1. Identificatie: de klant maakt zich bekend;
2. Legitimatie: de klant bewijst dat hij de persoon is waarvoor hij zich uitgeeft.

Het identificeren gebeurt door het in de automaat steken van de bankpas. De automaat leest de gegevens, onder andere het rekeningnummer van de klant, van de magneetstrip. Nadat is vastgesteld dat de pas geldig is, moet de gebruiker zich legitimeren door middel van het Personal Identification Number (de PIN-code).
De ingevoerde PIN-code wordt gecontroleerd. Wordt hij juist bevonden, dan is de gebruiker geautoriseerd om transacties te laten plaatsvinden.
De controle van de PIN kan off-line en on-line geschieden. Off-line-autorisatie houdt in dat de PIN in de terminal wordt gecontroleerd. Er wordt geen verbinding gemaakt met de centrale computer, waardoor de autorisatie sneller en goedkoper verloopt. Deze methode is minder veilig dan de on-line-autorisatie, omdat de terminal de cryptografische sleutels bevat. Deze informatie moet fysiek en logisch beveiligd worden tegen fraudeurs.
Voor on-line-autorisatie is een directe verbinding met de centrale computer noodzakelijk. De ingevoerde PIN-code wordt in versleutelde vorm aan de computer doorgegeven, die vervolgens de controle uitvoert. Een voordeel hiervan is dat de sleutel waarmee de autorisatie wordt uitgevoerd, niet in de terminal aanwezig is. Wel moet de verbinding tussen terminal en centrale computer beveiligd worden tegen aftappen en inbreken.

De PIN-code

Het Personal Identification Number (de PIN-code) is een getal waarmee de gebruiker van een bankpas zich kan legitimeren. Omdat de PIN-code gemakkelijk te onthouden maar ook voldoende groot moet zijn, dit om de kans op het raden van de code zo klein mogelijk te houden, wordt een PIN-lengte van vier of zes cijfers aanbevolen.
Een PIN-code kan afhankelijk of onafhankelijk van de persoonlijke informatie worden gekozen. Een afhankelijke code wordt door een cryptografische berekening uit de persoonlijke informatie afgeleid. Het voordeel is dat uitgegeven PIN-codes niet opgeslagen hoeven te worden. Een nadeel is echter dat wanneer de berekening en de sleutelvariabelen aan iemand bekend is, de bij de pas behorende PIN-code kan worden berekend.
De onafhankelijke PIN-code is niet uit de persoonlijke gegevens berekend. Een nadeel van deze methode is dat een bestand met uitgegeven PIN-codes bijgehouden moet worden. Dit bestand moet beveiligd worden tegen ongeautoriseerd gebruik.
De gebruiker van de bankpas moet er voor zorg dragen dat zijn PIN-code niet bekend wordt aan anderen. Dit om ongeautoriseerd gebruik te voorkomen.

Identificatietechnieken

In de huidige toepassingen wordt de PIN-code als identificatiemiddel gebruikt. De bezwaren die hieraan kleven, zijn:
- de gebruiker kan de PIN-code vergeten en moet ervoor zorgen dat anderen zijn PIN-code niet te weten komen;
- de PIN-code is niet strikt persoonlijk (de code kan bekend zijn aan iemand anders dan de gebruiker);
- de PIN-code is niet uniek (er zijn meerdere gebruikers met dezelfde PIN).

Om deze bezwaren te ondervangen, zou men ook de volgende identificatietechnieken kunnen toepassen:
1. handtekeningverificatie;
2. netvliesherkenning;
3. vingerafdrukherkenning.

Handtekeningverificatie

De karakteristieken van iemands handtekening worden vastgelegd met behulp van een elektromagnetische pen en een uiterst gevoelige sensor. Omdat iemands handtekening nooit volledig identiek is aan de voorgaande, wordt de handtekening binnen definieerbare toleranties geaccepteerd.
Het voordeel van deze verificatie is, dat een handtekening een beproefd en vertrouwd identificatiemiddel is. Een handtekening kan niet verloren gaan, gestolen of vergeten worden, en vanwege de vastgelegde karakteristieken, zoals de snelheid van de pen en de druk op het papier, is hij moeilijk na te maken. Het nadeel van deze methode is dat de kosten voor dit systeem hoog zijn en dat iemand zijn handtekening altijd zó moet zetten dat hij binnen de vastgestelde toleranties valt.

Netvliesherkenning

Iedereen heeft een karakteristiek netvliespatroon. Dit patroon wordt met behulp van infrarood licht gemeten en vastgelegd in de computer. Bij verificatie wordt het netvliespatroon van de persoon vergeleken met het opgeslagen patroon.
Deze techniek van verificatie is nog in een experimenteel stadium.

Vingerafdrukherkenning

Vingerafdrukken zijn uniek, vandaar dat de politie ze al jaren gebruikt voor het identificeren van misdadigers. Maar juist deze associatie met de misdaad maakt dat men deze methode niet graag wil invoeren. Bovendien bestaat het risico dat de politie de verificatiebestanden gaat gebruiken bij het opsporen van misdadigers.

Beveiliging

Vanwege de fraudegevoeligheid moet het systeem van elektronisch betalen (EFT) aan een aantal strenge veiligheidseisen voldoen.

Communicatiebeveiliging

De verbinding tussen computer en terminal moet beveiligd worden tegen aftappen, zeker wanneer het telefoonnet wordt gebruikt. Dit kan door middel van authenticatietechnieken. Dit zijn technieken waarmee vastgesteld wordt, dat:

- de gebruiker van het systeem degene is voor wie hij zich uitgeeft;
- de gebruiker de terminal mag gebruiken;
- het bericht niet wordt veranderd tijdens het transport van terminal naar computer.

Computerbeveiliging

De computer moet fysiek en logisch beveiligd worden tegen ongeautoriseerd gebruik van de opgeslagen informatie.

Terminal-beveiliging

Als in de terminal informatie opgeslagen is, dient de terminal fysiek beveiligd te worden tegen inbraak. Zowel de geheime als niet-geheime informatie dient beveiligd te zijn, omdat een ongeautoriseerde persoon zich toegang tot het systeem zou kunnen verschaffen door wijziging van de niet-geheime gegevens.

Bankkaartbeveiliging

Men kan alleen toegang krijgen tot het systeem indien men in het bezit is van een bankkaart en de bijbehorende PIN-code. De magnetische strip is vrij eenvoudig te kopiëren met behulp van een stukje video-tape. Dit kopiëren is niet te beveiligen. Een oplossing voor dit kopiëren biedt de smartcard. De informatie op deze kaart is vastgelegd in een elektronisch circuit (chip) en is niet te lezen zonder gebruik te maken van de PIN-code.

Switch-beveiliging

De switch is de instelling die de schakelfunctie vervult tussen de detaillisten en de banken (de kaartuitgevende instellingen). Het toevoegen van deze schakelfunctie houdt in dat de kaartuitgevende instellingen niet meer in staat zijn om de beveiliging van de gehele transactie te beheersen. Omdat juistheid, volledigheid en geheimhouding van transacties gewaarborgd moeten zijn, wordt er in samenwerking met EDP Audit Services een beveiligingsconcept ontwikkeld.

Beveiliging van de PIN-code

De kaartuitgevende instelling moet door een duidelijk veiligheidsbeleid zijn klanten overtuigen van het belang om voorzichtig te zijn met de geheime PIN-code. Het bekend worden van de PIN kan niet alleen voor de klant maar ook voor de kaartuitgevende instelling nadelige gevolgen hebben (goodwill-verlies, schadeclaims). Uiteraard moet ook de kaartuitgevende instelling ervoor zorgen dat de PIN-codes niet aan anderen, bijvoorbeeld employeés van de instelling, bekend worden.

Het twee-chip-kaartenprincipe

Het twee-chip-kaartenprincipe is een identificatiemethode voor toepassingen met chip-kaarten. Deze methode is gebaseerd op de handshake, die gemaakt wordt door de pas van de winkelier en de pas van de consument.
Op de pas van de consument zijn twee gegevens vastgelegd, de Card Identification (CID) en de Key ten behoeve van de communicatie tussen de consument en de detaillist (Kcd). De Kcd kan worden afgeleid uit de CID met de sleutel Kcd en een algoritme. De beide chip-kaarten dienen aan elkaar te bewijzen in het bezit te zijn van de geheime sleutel Kcd. Hiertoe worden zij in een terminal geplaatst. De consumentenkaart verzendt de CID naar de detaillistenkaart. De detaillistenkaart kan de sleutel Kcd berekenen. Vervolgens genereert de detaillistenkaart een randomgetal en stuurt dit naar de consumentkaart. Beide kaarten berekenen vervolgens met het versleutelingsalgoritme en de sleutel Kcd de vercijferde waarde van dit random-getal. Vervolgens verstuurt de consumentenkaart de versleutelde waarde naar de detaillistenkaart terug. De detaillistenkaart kan nu vaststellen of de door de consumentenkaart berekende waarde overeenkomt met de eigen berekende waarde. Op grond hiervan accepteert of weigert de detaillist de consument.
Andersom wil de consument ook vaststellen dat de detaillist over een goede kaart beschikt en dat het een echte terminal betreft. Hiertoe genereert ook de consumentenkaart een random-getal en verzendt dat naar de detaillistenkaart. Beide kaarten berekenen weer de bijbehorende versleutelde waarde en dit keer zendt de detaillistenkaart de berekende waarde aan de consumentenkaart. De consumentenkaart kan nu vaststellen of de detaillistenkaart de juiste sleutel Kcd heeft berekend. Als deze procedure is uitgevoerd en beide kaarten zijn overtuigd dat de andere kaart correct is, kan vervolgens de transactieverwerking plaatsvinden.

Conclusie

Het elektronisch betalen heeft uiteraard gevolgen voor de controle door de accountant. Omdat de transacties elektronisch vastgelegd worden, zijn er geen eerste aantekeningen in de vorm van boekingsdocumenten meer.

Het stelsel van interne controlemaatregelen van de cliënt zal aangepast moeten worden aan het elektronisch betalen, zodat de juistheid, volledigheid en tijdigheid van de gegevens gewaarborgd zijn, alsmede dat uitsluitend goedgekeurde transacties worden verwerkt. Het geheel zal ook controleerbaar moeten blijven. Het management van het bedrijf en de individuele bankrekeninghouder - indien het om een persoonlijke bankrekening gaat - zijn de eerste verantwoordelijken. Deze verantwoordelijkheid mag noch de EDP auditor noch de accountant overnemen.

Van de controlerend accountant respectievelijk EDP auditor wordt een oordeel gevraagd over het samenstel van controle- en beveiligingsmaatregelen. Hiertoe zal een adequaat controleprogramma vereist zijn waarin de scope alsmede de feitelijk uit te voeren (test)werkzaamheden vermeld staan. Op grond van deze werkzaamheden zal de accountant/EDP auditor tot een oordeel komen hetgeen begrepen zal zijn in de verklaring bij de jaarrekening, indien het onderzoek een onderdeel vormt van de controle van de jaarrekening of wel verwoord in een mededeling in geval van het bijzondere onderzoek. Opmerkingen kunnen eventueel worden weergegeven in de management letter.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

Automatisering
Beveiliging
Controle
NIEUWS

Winter 1987/1988

onder redactie van M.C. Duym, J.F.C. van Epen en drs. J. Kuipers
met medewerking van mw. ing. I.M. van Duin

Automatisering

In Compact 87/2 berichtten wij reeds over problemen in de geautomatiseerde verwerking van het betalingsverkeer van een Australische bank. Als oorzaak werd het hoge transactievolume vermeld. Inmiddels is in EDPACS van december 1987 een artikel verschenen waarin naast het transactievolume nog andere oorzaken staan vermeld. Vandaar, dat wij op deze zaak terugkomen.

Afgelopen zomer is een Australische bank in grote moeilijkheden gekomen door het falen van software.
In één weekend werden een nieuwe versie van IBM's database-systeem (IMS) en een door de bank ontwikkelde module geïnstalleerd. In eerste instantie leek het systeem goed te functioneren, totdat het na enkele uren "plat" ging. Het opnieuw opstarten van het systeem gebeurde - logisch gezien - gebrekkig, terwijl er tegelijkertijd veel transacties van rekeninghouders plaatsvonden. Het gevolg hiervan was dat de controles binnen het systeem niet meer uitgevoerd werden en de rekeninghouders onbeperkt geld konden opnemen. De EDP-staf kwam in actie door de oude versie van de software van vóór de moeilijkheden, te herinstalleren.

De bank en IBM laten niets los over de oorzaak van de moeilijkheden.
Buitenstaanders schrijven de moeilijkheden toe aan:
- de implementatie van de nieuwe software-versie;
- problemen met de door de bank ontwikkelde software;
- de fysieke grootte van het netwerk waarmee de bank werkt;
- een fout in het mainframe;
- de grote hoeveelheid transacties;
- het onvoldoende testen van de nieuwe software;
- de aanwezigheid van 150 bekende, maar niet gecorrigeerde fouten in de nieuwe versie van de software;
- IBM's tactiek om onvoldoende geteste software te installeren op grote systemen.

Bron: EDPACS december 1987.

Beveiliging

Practicum

In de Verenigde Staten zijn negen studenten aangeklaagd voor hun deelname in een omvangrijk fraudecomplot. De aanklacht betreft het onrechtmatig gebruik van computers, het plegen van fraude met credit cards, het ontvangen van gestolen goederen en het "crimineel samenzweren".
Bij het plegen van deze criminele daden werd waarschijnlijk gebruik gemaakt van home-computers om toegang te krijgen tot credit-card-rekeningen in supermarkten en modems om telefoonlijnen af te tappen. Het commentaar van een deskundige was, dat het talentvolle studenten zijn.

Bron: EDPACS december 1987.

Bijna-fraude leidt tot regelmatig overleg justitie en banken

Vorig jaar werden vlak na de kerst drie mannen aangehouden die verdacht werden van een poging tot fraude van 15,1 miljoen dollar. Een van de verdachten, die bij een kleine Amsterdamse bank werkte, heeft geprobeerd de dag voor kerst naar twee banken in Zürich respectievelijk 8,4 en 6,7 miljoen dollar over te maken. De eerste overboeking kon met succes worden uitgevoerd. Bij de tweede overboeking werd echter een fout gemaakt waardoor de computerverbinding werd verbroken. Hierdoor kreeg men argwaan. De desbetreffende bank heeft van de fraudepoging aangifte gedaan omdat de medewerker de bank dreigde met het bekendmaken van bedrijfsgeheimen.

De medewerker was in staat de overboeking geheel zelfstandig uit te voeren omdat hij over alle wachtwoorden, benodigd voor het overboeken, beschikte.

Deze fraudepoging heeft ertoe geleid, dat politie, Openbaar Ministerie en vertegenwoordigers van het bankwezen regelmatig bijeen zullen komen. Doel van deze bijeenkomsten is meer te weten te komen over de werkwijze van fraudeurs.

Commentaar op bovenstaande

Bij belangrijke on-line real-time-transacties wordt altijd aanbevolen een procedure te volgen met bij voorkeur een drietal stappen:
1. invoering;
2. verificatie;
3. autorisatie.

In dit geval is niet bekend of deze procedure bij de desbetreffende bank werd gehanteerd. Minimaal zal een procedure met de stappen invoeren en verifiëren/autoriseren zijn gevolgd. De desbetreffende medewerker heeft dus over drie respectievelijk twee wachtwoorden moeten beschikken. In hoeverre hij deze zelf heeft moeten vergaren of gewoon ter beschikking heeft gekregen, in verband met de geringe bezetting rond de kerstdagen, is onbekend. Overduidelijk is echter aangetoond, dat een strakke wachtwoorddiscipline bij zowel individuele personen als de organisatie geen overbodige luxe is.

Bron: Het Parool 11 januari 1988.

Bunker

American Airlines heeft recentelijk in een super beveiligde ondergrondse bunker een computercentrum geopend. Het centrum is beveiligd tegen aardbevingen, overstromingen, brand, terroristen en elke andere vorm van een ramp of aanslag.
Bij betreding van de bunker vindt er een uitgebreide toegangscontrole plaats. Met behulp van een toegangskaart en na intoetsing van het employeenummer komt men in een cel, waar het aderpatroon van het netvlies van het personeelslid wordt vergeleken met gegevens in de computer. Om "piggybacking" te voorkomen, wordt de persoon gewogen.
In het computercentrum wordt men in de gaten gehouden met behulp van camera's.

Bron: EDPACS december 1987.

Richtlijnen voor Engelse Data Protection Act 1984

In maart jongstleden heeft het Office of The Data Protection Registrar, in het Verenigd Koninkrijk een serie van acht richtlijnen (guidelines) uitgegeven over de Data Protection Act 1984.
Het doel van deze serie richtlijnen is "... to inform individuals of their rights under the Act and to help those who process personal data to understand their obligations".
De richtlijnen hebben de volgende titels:
1. Introduction to the Act;
2. The definitions;
3. The Register and Registration;
4. The Data Protection Principles;
5. Individuals Rights;
6. The Exemptions;
7. Enforcement and Appeals;
8. Summary for Computer Bureaux.

De richtlijnen kunnen worden besteld door de Registrar's Enquiry Service te Wilmslow te bellen 09-44 625 53577. Zij worden dan gratis toegezonden.

Controle

Expertmeningen en risico-analyse

Onder de titel "Het gebruik van expertmeningen in veiligheidsstudies" heeft de TU Delft een rapport uitgebracht over een literatuuronderzoek naar het gebruik van expertmeningen bij risico-analyses.
Een onderdeel van risico-analyses is het berekenen van de kans op schade. De betrouwbaarheid van de berekening van kansen wordt onder andere beperkt door een gebrek aan gegevens over het falen van componenten in systemen. De beperkingen in het bepalen van betrouwbare kansen zijn het grootst als het gaat om catastrofaal falen. Op het gebied van de EDP zou men kunnen denken aan langdurige uitval van een rekencentrum. Als gevolg van het gebrek aan statistisch materiaal is de risico-analist aangewezen op het raadplegen van experts en het verwerken van de verkregen expertmeningen.
Het raadplegen van experts en het kwantificeren van onzekerheid door experts is niet nieuw. Het bekendste voorbeeld daarvan is wel het in probabilistische termen voorspellen van het weer ("de kans op regen morgen bedraagt ...").
Sinds een aantal jaren wordt bij risico-analyses gebruik gemaakt van expertmeningen. Het wordt volgens het onderzoek langzamerhand duidelijk dat hieraan een aantal specifieke problemen verbonden zijn. Deze problemen concentreren zich op: spreiding, elicitatie en combinatie. Ten eerste, kansschattingen door verschillende experts kunnen een enorme spreiding geven, zodat het geven van puntschattingen onvoldoende is en kansverdelingen gewenst zijn. Het tweede probleem is hoe men komt aan de kansverdelingen en hoe de verschillende vormen van vertekening of kleuring (bias), waaraan expertmeningen onderhevig zijn, worden vermeden. De vraag naar de combinatie gaat in op het kiezen van verschillende experts en het combineren van hun individuele uitkomsten.
Bovengenoemde problemen met spreiding, elicitatie en combinatie maken het volgens de onderzoekers gewenst het gebruik van expertmeningen te formaliseren.

De onderzoekers merken op dat de kwaliteit van kansuitspraken van experts niet erg bemoedigend zijn.
Er wordt een aantal onderzoeken aangehaald waaruit blijkt dat er veelal sprake is van zelfoverschatting (overconfidence bias).

Helemaal moeilijk wordt het schatten van "zeldzame gebeurtenissen" (kansen minder dan .01). Er blijkt geen geschikte methode te zijn voor het verkrijgen van kansuitspraken over zeldzame gebeurtenissen.

Uit de literatuurstudie komt onder andere naar voren dat als kansbegrip de subjectieve interpretatie de voorkeur verdient boven een objectieve kansinterpretatie, waarbij de kans bepaald wordt als frequentie van in het verleden opgetreden gebeurtenissen. De subjectieve benadering stelt dat de kans een maat van "geloof" van een subject is met betrekking tot het optreden van een gebeurtenis. De objectieve benadering maakt dus gebruik van statistisch materiaal voor het bepalen van kansen.

Een belangrijke conclusie uit het rapport is dat er voldoende mogelijkheden aanwezig lijken om te komen tot een gestructureerde inbreng van expertmeningen bij veiligheidsstudies. Voor de EDP audit is deze conclusie een uitdaging om na te gaan hoe expertmeningen in, uitgevoerde of uit te voeren, risico-analyses worden verwerkt.

Hulpprogramma voor controle op wijziging load libraries

Door de NMB is, in eerste instantie voor eigen gebruik, programmatuur ontwikkeld waarmee controle kan worden uitgevoerd op het ongeautoriseerd wijzigen van load libraries. De programmatuur is geschikt voor IBM mainframes draaiende onder OS/VS1 en MVS.

Initieel wordt door deze programmatuur per load-module een hash total berekend en opgeslagen. Later in de tijd (op afroep van bijvoorbeeld een IAD) worden deze berekeningen per module herhaald en automatisch vergeleken met de eerder gemaakte berekeningen. Uit de gesignaleerde verschillen die op een overzicht verschijnen, kan worden opgemaakt of de desbetreffende modules inhoudelijk zijn gewijzigd. De wijzigingen dienen te kunnen worden verklaard uit de registratie van programma-overdrachten. Zodoende is een integrale controle mogelijk op de naleving van de overdrachtprocedures. Dit geldt zowel voor applicatie- als systeemprogrammatuur.

Via bemiddeling van KPMG Klynveld EDP Audit Services is deze programmatuur aan enkele van onze cliënten verstrekt. Recent heeft de NMB ons deze programmatuur ter beschikking gesteld en ons gemachtigd deze zelf aan belangstellende cliënten kostenloos te verspreiden onder vermelding van NMB.

Indien u belangstelling voor deze programmatuur en bijbehorende documentatie (of in eerste instantie alleen de documentatie) hebt, kunt u zich in verbinding stellen met KPMG Klynveld EDP Audit Services, sectie Support & Programming, telefoon 020 - 5461908.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

ONDERWIJS

EDP-audit-opleidingen in Nederland

Op 9 februari 1988 organiseerde de sectie EDP auditing van het Nederlands Genootschap voor Informatica een bijeenkomst dat als thema had: "EDP-audit-opleiding: wat is dat eigenlijk".

In het hierna volgende zullen de opleidingen van de opleidingen van de Vrije Universiteit, de Erasmus Universiteit en de Katholieke Universiteit Brabant met elkaar worden vergeleken.
In de inleiding voor deze dag gaf de voorzitter van de sectie EDP auditing (B. Goossens) een referentiekader aan voor de inleiders gericht op het aangeven van de aspecten die en met welke diepgang in de betreffende opleiding voorkomen.

Als uitgangspunt en antwoord op de vraag: "wat is EDP auditing", refereerde hij aan een definitie die reeds vijf jaar geleden door de sectie EDP audit werd gehanteerd en waarin als elementen voorkomen: de onafhankelijke deskundige voor de uitvoering van het onderzoek, de te beoordelen kwaliteitsaspecten betrouwbaarheid (in ruime zin), doeltreffend- en doelmatigheid, en de te beoordelen objecten informatiesystemen (zowel operationeel als in ontwikkeling), organisatie van de gegevensverwerking en de "technische" organisatie of infrastructuur. Tevens stelde hij de vraag op welk type informatiesysteem de EDP audit zich richt. De financiële, personele, logistieke of andere informatiesystemen.
Overigens zal het antwoord op de vraag wat EDP audit eigenlijk is uit de beroepsorganisatie(s) dienen te komen.

Vrije Universiteit (H. de Lange)
De doelstelling van de postdoctorale beroepsopleiding bij de economische faculteit van de VU, is het verzorgen van een opleiding voor het uitvoeren van EDP audits als zelfstandig werkterrein naast financiële en operational audits. Daarbij worden kennis en vaardigheden aangeleerd voor het uitvoeren van audits van informatiesystemen, computercentra en management audits van geautomatiseerde systemen (gericht op doelmatig- en doeltreffendheid).
Gesteld wordt dat alleen ten aanzien van de technisch organisatorische aspecten en infrastructuur slechts een kennisniveau bereikt wordt dat een zinvol contact met betreffende specialisten mogelijk moet maken. Het type auditor dat nu wordt opgeleid kan misschien beter gekarakteriseerd worden als Information Systems Auditor.
Het ligt in het voornemen de opleiding uit te breiden met een richting "technical audit", die voor een deel parallel loopt met de huidige opleiding maar waarbij de kennis over bovengenoemde technische infrastructuur verder wordt uitgediept.

Tijdens een EDP audit krijgt de auditor onder meer te maken met een breed scala van activiteiten in het kader van de automatisering zoals beleidsvorming, planning, ontwikkeling en onderhoud van systemen, wijze van gegevensverwerking en -opslag en gebruik van de resultaten van de verwerking.
De EDP auditor dient kennis te hebben van informatica, beveiligings- en continuïteitsconcepten en de besturingsprocessen in een organisatie. Tevens dient hij de voor een effectieve uitvoering benodigde methoden en technieken te kunnen toepassen.

Gesteld wordt dat ook kennis vereist is ten aanzien van de financieel-economische facetten van de besturingsprocessen, de administratieve organisatie en de algemene grondslagen en methoden en technieken van de accountantscontrole waarmee een sterke nadruk wordt gelegd op het financieel-economische aspect van een EDP audit.
Deze nadruk komt ook naar voren in de toelatingseisen voor het volgen van de tweejarige EDP-audit-opleiding, namelijk het met goed gevolg afgerond hebben van de vakken administratieve organisatie en controleleer voor registeraccountants.

Het eerste jaar van de opleiding is gericht op het bijbrengen van kennis op het gebied van programmerings- en overige automatiseringstechnieken. Hierbij worden tevens strategieën behandeld voor het geven van een oordeel ten aanzien van de betrouwbaarheid, doelmatig- en doeltreffendheid hierbij.
Het eerste jaar bestaat uit de volgende modules:
- basiskennis automatisering;
- besturingssystemen; waarbij wordt ingegaan op auditing van definities, lokale wijzigingen en het onderhoud van systeemprogrammatuur, en het gebruik van systeemprogrammatuur voor de audit zelf;
- datacommunicatie;
- system development methodologieën;
- computercentra audit-/data-gerichte controle; de opgedane kennis dient te worden toegepast op relatief eenvoudige rekencentra. Hetzelfde geldt ten aanzien van het gebruik van audit software en de data-gerichte controle.

In de eerste helft van het tweede jaar wordt het ontwerpen van een informatiesysteem behandeld. De tweede helft is geheel gericht op het verkrijgen van kennis van en vaardigheid in auditing.
De volgende modules worden gegeven:
- gestructureerde informatie-analyse;
- database-omgeving; hierbij wordt onder meer de audit in een database-omgeving behandeld;
- workshop systeemontwerp/database; omvat het ontwerpen en implementeren van een database op ORACLE en een toepassing op de database met behulp van SQL;
- audit van informatiesystemen;
- audit van grote computercentra;

- management audit; gericht op het vormen van een oordeel over de effectiviteit en de efficiëntie van de automatisering in een organisatie.

Behalve in de laatste module wordt aan de aspecten doelmatig- en doeltreffendheid slechts in geringe mate aandacht besteed.

Katholieke Universiteit Brabant (H.B. Moonen)

De in februari 1988 gestarte postdoctorale beroepsopleiding tot EDP auditor wordt verzorgd door het Tilburgs Instituut voor Academische Studies (TIAS) als een van de postdoctorale opleidingen aan de KUB.
De EDP auditor houdt zich bezig met de beoordeling van de kwaliteit van de automatiseringsfuncties en -activiteiten binnen organisaties.
Als onderzoekterrein van de EDP auditor worden genoemd:
- de aanpak van de automatisering;
- de kwaliteit van de automatiseringsorganisatie;
- de adequaatheid van gebruikte of te gebruiken informatiesystemen.

Tot nu toe zijn de deskundigen die zich bezig houden met het geven van oordelen en adviezen voornamelijk afkomstig uit het accountantsberoep. Hierbij krijgt het aspect betrouwbaarheid, inclusief beveiliging en ook continuïteit, de meeste aandacht.
In de opleiding die aan de KUB wordt verzorgd zal echter de nadruk worden gelegd op de aspecten doeltreffend- en doelmatigheid. De opleiding zal bovendien sterk op de praktijk gericht zijn.
De opleiding is gericht op het verwerven van kennis met betrekking tot de beheersing van bovengenoemde kwaliteitsaspecten en de vaardigheden nodig voor beoordeling. Daarnaast zal aandacht worden besteed aan de voor het EDP-audit-onderzoek benodigde methoden en technieken en vaardigheden die behoren tot de beroepsuitoefening inclusief rapportage.
De opleiding is bedoeld voor academici en HBO'ers die over voldoende informaticakennis beschikken en reeds op dit terrein werkzaam zijn. Hierbij wordt ook gedacht aan bedrijfseconomen, bedrijfskundigen en registeraccountants.
De opleiding omvat de volgende vijf modules:

Introductie

Hier wordt ingegaan op het vakgebied EDP audit, en een aantal centrale begrippen zoals de aandachtsgebieden: controllability, dat zich richt op de kwaliteitsaspecten van de beheersinstrumenten en auditability, dat gericht is op de beoordeling van kwaliteitsaspecten en de beheersing van kwaliteit. Beheersbaarheid en controleerbaarheid worden in de volgende modules verder uitgewerkt ten aanzien van:
- de doelstellingen;
- de selectie van audit-technieken en beheersinstrumenten en
- de criteria daarvoor.

In de volgende modules wordt steeds een EDP-audit-opdracht als uitgangspunt genomen. Iedere module bestaat uit onderwerpen die elk een object van EDP audit vertegenwoordigen. Per onderwerp worden één of meer kwaliteitsaspec-

ten bekeken en wordt behandeld welke audit- en control-technieken bij de uitvoering van de opdracht kunnen worden gebruikt.
De modules worden afgesloten met een case-study.

Infrastructuur: informatie-organisatie

Onderwerpen die aan de orde komen zijn: het automatiseringsbeleid, systeemontwikkeling en onderhoud, beveiliging, informatieverwerking en informatieverkrijging en -gebruik in de gebruikersorganisatie.

Infrastructuur: informatiemiddelen

Behandeld worden diverse soorten hardware en besturings-software, database management-systemen en software voor toegangsbeveiliging, systeemontwikkeling en applicaties en de relatie met de informatie-organisatie.

Specifieke toepassingen van de infrastructuur

Als specifieke toepassingen worden electronic banking, CAD/CAM en kantoorautomatisering genoemd.

EDP audits in relatie tot specifieke doelstellingen

Zoals jaarrekeningcontrole, privacy-eisen, keuren van door software-houses ontwikkelde pakketten.
De nadruk op doelmatig- en doeltreffendheid is afhankelijk van de als uitgangspunt gekozen EDP-audit-opdrachten.

Erasmus Universiteit (H.C. Kocks)
De Erasmus Universiteit is in 1984 als eerste in Nederland gestart met een opleiding tot EDP-accountant. Deze opleiding is gericht op het verkrijgen van kennis van enkele deelgebieden in de automatisering voor het beoordelen van geautomatiseerde informatiesystemen en de automatiseringsorganisatie. Tevens wordt inzicht gegeven in de invloed van geïntegreerde gegevensverwerking op de interne en externe controle. De doelstelling van het curriculum is de (aankomend) accountant de voor de controlepraktijk benodigde kennis op het gebied van automatisering bij te brengen en het benodigde inzicht te geven voor het verantwoord inschakelen van EDP-audit-specialisten. De behandelde stof richt zich alleen op het aspect betrouwbaarheid inclusief continuïteit.
Het curriculum bestaat uit de volgende modules:
- scope van het curriculum;
- systeemontwikkeling;
- automatiseringsorganisatie;
- systeembeoordeling;
- geïntegreerde gegevensverwerking;
- gedistribueerde automatisering;
- automatisering in kleinschalige omgeving;
- gebruik van de computer in de controlepraktijk.

Behalve de eerste module worden alle modules afgesloten met een case-study. De gegeven presentatie echter bestond uit een algemene beschouwing over de betekenis en inhoud van EDP audit, waarbij de volgende verschillen tussen een opleiding tot EDP-accountant en een EDP-audit-opleiding werden aangegeven.
De EDP-accountant-opleiding is gericht op een beperkte doelgroep. Daarbij vormen de functies van de accountant met betrekking tot: interne controle, jaarrekeningcontrole sec en adviesfunctie het uitgangspunt. EDP audit wordt hierbij bezien vanuit een beperkte scope, namelijk de administratieve organisatie en de te behandelen kwaliteitsaspecten beperken zich tot het aspect betrouwbaarheid. Doel van de opleiding is het opvullen van leemten in de kennis van automatisering en audit bij de accountant.
EDP audit echter is een eigen vakgebied met relaties naar andere vakgebieden. De gegeven definitie verdeelt het onderzoekterrein van organisatie en automatisering/informatisering in een logische (gebruikersomgeving), ontwikkel- (systeemontwikkeling) en technische (computercentrum) infrastructuur, waarbij de drie aspecten betrouwbaarheid, doelmatigheid en doeltreffendheid van even groot belang zijn.

Behalve bovengenoemde indeling naar infrastructuur wordt nog een onderscheid gemaakt in een strategisch, tactisch en operationeel beschouwingsniveau en daarbinnen in een structuur- en een procescomponent.
Als vakgebieden die aan de logische infrastructuur gerelateerd zijn kunnen Economie en Bestuurlijke Informatiekunde worden genoemd en voor de technische infrastructuur Informatica en Elektrotechniek.
Een opleidingscurriculum is nog niet voorhanden. Gedacht wordt aan een tweejarige opleiding waarin het eerste jaar gericht is op auditing en het tweede jaar op specifieke EDP-audit-specialisaties per infrastructuur.
Voor toelating vormt de aanwezigheid van kennis van de bovengenoemde infrastructuren op de verschillende beschouwingsniveaus een voorwaarde. Getracht wordt om deze nieuwe EDP-audit-opleiding over anderhalf jaar te starten.

Vergelijking van de universitaire opleidingen
Samengevat ontstaat het volgende beeld ten aanzien van omvang en diepgang van het kennisgebied bij de verschillende gepresenteerde universitaire opleidingen, alsmede de richting waarin deze zich ontwikkelt.
De huidige opleiding aan de VU richt zich voornamelijk op het aspect betrouwbaarheid en het audit-object informatiesystemen met een voorkeur voor financiële systemen.
In de KUB-opleiding worden benadrukt de aspecten doelmatig- en doeltreffendheid en als audit-object de technische infrastructuur. Er is geen voorkeur voor een bepaald type informatiesysteem.
De te ontwikkelen EUR-opleiding zal alle drie de genoemde aspecten met gelijke diepgang behandelen en zich per specialisatie richten op een van de audit-objecten informatiesystemen of technische infrastructuur. Er is eveneens geen voorkeur voor een bepaald type informatiesysteem.

EXIN (G. Groenenboom)
De stichting EXIN richt zich op het afnemen van examens op HBO-niveau voor onder meer de AMBI88-modules. De modules zijn deels vrij te kiezen en af te stemmen op een bepaalde functie in de automatisering. AMBI88 kent onder meer de kennisrichtingen: informatiekunde, programmatuur en gegevensstructuur. Een kennisrichting wordt afgesloten met een afstudeeropdracht. Een van de modules binnen de richting informatiekunde betreft: "Betrouwbaarheid en beveiliging van informatiesystemen (EDP auditing)". Voor het volgen van deze module wordt, behalve elementaire kennis van informatica, ook kennis vooronderstelt van organisatie, informatiebeleid en systeemonderzoek.
Volgens de exameneisen dient na het volgen van de module inzicht verkregen te zijn in:

- het beoordelen van geautomatiseerde gegevensverwerking op betrouwbaarheid, doeltreffendheid en doelmatigheid (systems audit). Deze omvat de terreinen: organisatie van de ontwikkeling, programmerings- en besturingssystemen;
- risico-analyse; analyse vindt plaats met betrekking tot het falen van systemen, de maatregelen ter vermindering ervan en de restrisico's;
- het beoordelen van maatregelen:
  - ter beheersing van de betrouwbaarheid van informatie;
  - ter beveiliging tegen onbevoegd gebruik van informatie en verwerkingscapaciteit;
  - tot het beperken van de risico's van het niet beschikbaar zijn van systemen en informatie;
- het gebruik van controlemethoden en -technieken;
- het gebruik van computerassistent audit techniques.

Ten aanzien van de vraag wat is kwaliteit, wordt verwezen naar de verkregen kennis op dit gebied met betrekking tot logistieke systemen.
Kwaliteit is een relatief begrip en onder meer afhankelijk van het ambitieniveau van de gebruiker. Er zijn ten aanzien van het begrip behalve economische en technische aspecten ook sociale aspecten te onderkennen.

Om kwaliteit uit te drukken noemt Starreveld als elementen: relevantie, betrouwbaarheid, doelmatigheid en doeltreffendheid. Maar ook het belang van de doelmatigheid of doeltreffendheid voor de kwaliteit is afhankelijk van het feit of we te maken hebben met functionaliteit, structuur, vormgeving, instrumentatie of verwerking. In het laatste geval zal de doelmatigheid van meer belang zijn dan de doeltreffendheid. Om de kwaliteit van een informatiesysteem te kunnen beoordelen is dus kennis van een veelheid aan kennisgebieden nodig.
De module EDP auditing is bedoeld voor het verkrijgen van basiskennis voor EDP auditing maar behandelt slechts een deel van de benodigde kennisgebieden.

NIvRA (H.A. Kampert)
Het NIvRA verzorgt geen opleiding tot EDP auditor. Binnen het NIvRA zijn er echter stromingen die aan een eigen EDP-audit-opleiding denken. Binnen het NIvRA verricht de Commissie van advies inzake Automatiseringsvraagstukken (CAV) onderzoek op het gebied van de automatisering ten behoeve van de beroepsuitoefening van accountants en rapporteert hierover. De door het CAV gehanteerde definitie van EDP audit komt overeen met die uit de inleiding. EDP audit is ontstaan binnen het accountantsberoep als een specialisatie (AC- en EDP-accountant), gericht op het aspect betrouwbaarheid.
Deze specialisatie verschuift steeds meer naar de technische infrastructuur en de beheersing ervan. De niet gespecialiseerde accountant zal steeds meer zelf de voor hem van belang zijnde informatiesystemen en daarbij behorende organisatie gaan beoordelen.

EDP audit is een vakgebied geworden voor in verschillende richtingen gespecialiseerde EDP auditors (al dan niet RA).
Gedacht wordt hierbij aan de volgende specialisaties:
- organisatie: gericht op systeemontwikkeling en informatiesystemen;
- hardware: gericht op beleid, selectie, architectuur en beheersing;
- software: gericht op besturingssystemen en overige "harde" software.

Voor het functioneren van de accountant wordt onder meer gesteld dat de accountant moet kunnen oordelen en adviseren ten aanzien van:
- interne controle en beveiliging bij automatisering;
- informatie- en automatiseringsbeleid.

Vastgesteld wordt dat de, nu reeds te lange, accountantsopleiding ten aanzien van de bovengenoemde punten achterblijft bij de ontwikkelingen in de informatica. Het verkrijgen van de noodzakelijke automatiseringskennis naderhand verlengt de opleidingsduur nog verder.
Door de structurele schaarste aan automatiseringsdeskundigen en de specifieke eisen ten aanzien van kennis en persoonlijke eigenschappen die aan EDP auditors worden gesteld, zal door de te verwachten schaarste de inschakeling van EDP auditors slechts beperkt mogelijk zijn.
De conclusie wordt dan ook getrokken dat heroriëntatie van de aanpak van de accountantscontrole en de opleiding noodzakelijk is.
Verwacht wordt dat er voorlopig nog behoefte zal blijven bestaan aan een AC-accountant als intermediair tussen accountant en EDP-audit-specialist en eindstation indien verdere specialistische kennis niet nodig is.

Het NIvRA dient geen eigen EDP-audit-opleiding te entameren maar wel een kopopleiding voor EDP auditors te bevorderen bij de bestaande universitaire informatica-opleidingen. Er is hierover echter nog geen overleg geweest tussen NIvRA en de universiteiten.

Het curriculum van een EDP-audit-opleiding dient zorg te dragen voor het verkrijgen van een:
- brede en diepgaande kennis van informaticatechnologie;
- inzicht in het functioneren van bedrijfshuishoudingen;
- inzicht in bedrijfsdoelstellingen ten aanzien van de automatisering;
- inzicht met betrekking tot bestuurlijke informatiesystemen.

Per specifiek toepassingsgebied waarin de EDP auditor gaat functioneren zal een verder toegespitst curriculum moeten worden opgesteld waarin de kennisgebieden variëren van bijvoorbeeld onderdelen van de informatietechnologie tot medische, juridische en accountancy-toepassingsgebieden.
Een curriculum voor EDP auditors die zich willen specialiseren in de samenwerking met accountants zal onder meer de vakken Administratieve Organisatie en Controleleer bevatten. De additioneel benodigde kennis is voornamelijk gericht op de aspecten: betrouwbaarheid, doeltreffendheid en doelmatigheid.
Doelstelling van dit curriculum zal zijn het verkrijgen van kennis van zowel audit- als beheersaspecten. Op dit moment zijn er de verschillende EDP-audit-opleidingen. Hierbij kan worden opgemerkt dat er sprake is van een zekere maatschappelijke verspilling door het ontbreken van coördinatie voor een landelijke opzet van een "brede" EDP-auditor-opleiding met specialisaties en bijbehorende exameneisen.

Certified Information Systems Auditor) P.P. van Besouw)
Binnen de internationale EDP Auditors Association houdt de EDP Auditors Foundation incl. (EDPAF) zich bezig met het verbeteren van de opleidingen van en de communicatie tussen EDPAA-leden, alsmede het ontwikkelen van standaarden en het doen van onderzoek op het gebied van "information systems auditing". De CISA Certification Board is gelieerd aan de EDPAA en de EDPAF en is verantwoordelijk voor zowel het vaststellen van het te volgen beleid, als de uitvoering van het CISA-examen. Voor de toelating tot het examen worden geen eisen gesteld. Om het certificaat te behouden worden eisen gesteld aan ervaring en het bijhouden van de kennis. Tevens dient men zich te houden aan enkele (ethische) gedragdsregels. Op basis van een analyse van het uit te voeren audit-werk zijn multiple-choice-vragen opgesteld, die de kennis en vaardigheid van de kandidaat moeten testen. De vragen betreffen onder meer de volgende onderwerpen:
- het beoordelen van de in operationele applicaties opgenomen controles;
- het beoordelen van de juistheid, volledigheid en consistentie van de opgeslagen gegevens;
- het beoordelen van de bij de applicatie-ontwikkeling en het wijzigen van bestaande applicaties gevolgde procedures;
- het beoordelen van applicaties in ontwikkeling ten aanzien van de opgenomen en nog op te nemen controles;
- beoordelen van het gegevensverwerkingsproces en de daarbij benodigde bedieningsprocedures;

- beoordelen van de beveiliging van de programmatuur, gegevens en de computerinstallaties;
- het vaststellen van de door de Information System Audit functie op zich te nemen verantwoordelijkheid en het zorg dragen voor een doelmatige en doeltreffende functievervulling.

De EDPAF verzorgt geen opleiding tot Information Systems Auditor.

Samenvatting van de paneldiscussie.

Dat binnen hetzelfde algemene kader toch verschillende inleidingen worden gehouden is het gevolg van de verschillende wegen waarlangs de opleiding plaatsvindt. Aan de VU wordt in de tweejarige opleiding (basis)kennis van automatisering en EDP audit bijgebracht, terwijl de EUR en de KUB in hun startende opleidingen twee jaar willen besteden aan EDP audit. Een EDP-audit-opleiding dient zo breed van opzet te zijn dat een volledige diepgang op alle gebieden in de huidige opleidingen niet zal kunnen worden bereikt.

Als dakorganisatie voor EDP audit wordt gedacht aan een forum van verschillende beroepsorganisaties waaronder het NIvRA, NGI sectie EDP auditing en eventuele buitenlandse beroepsorganisaties.
Het is niet duidelijk hoe de internationale buitenwereld zal reageren op de universitaire EDP-audit-opleidingen. Het meenemen van de toetsingseisen voor CISA wordt zinvol geacht. Het opleidingsniveau voor CISA is te vergelijken met AMBI en kan een bijdrage leveren om te komen tot een basisniveau met een internationale herkenbaarheid.
De bewaking van de kwaliteit berust wat de universitaire opleidingen betreft primair bij de betreffende universiteit.
De inbreng vanuit de praktijk en de beroepsorganisaties NIvRA en NGI, wordt geleverd via de samenstelling van programmaraad, curatorium en docententeams.
Het toetsen of aan de doelstellingen van de opleidingen is voldaan geschiedt aan de hand van het examenreglement en overige daarop betrekking hebbende universitaire voorschriften (VU en EUR). Voor de opleiding aan de KUB moeten nog toetsingsnormen worden ontwikkeld.
Voor de EDP-audit-module zijn exameneisen opgesteld en zijn een modelexamen en literatuurlijst beschikbaar.

Over het antwoord op de vraag of EDP auditing een vakgebied is, zoals bijvoorbeeld de economie, of een beroep, waren de meningen verdeeld.
Hopelijk geeft de werkgroep binnen de sectie EDP auditing, die zich bezig gaat houden met standaarden, een antwoord op deze vraag.
Een aparte studierichting EDP audit wordt door de presentators van KUB en EUR wel wenselijk maar in de huidige situatie niet haalbaar geacht.
Volgens het panellid van de VU echter is de benodigde onderbouw een synthese van informatica- en financieel-economische facetten die ook deel uitmaken van de opleiding voor registeraccountant.

Compact is een uitgave van

KPMG Klynveld EDP Audit Services

OVERZICHT VAN DE AUTEURS

Aan dit nummer van Compact werkten de volgende auteurs van KPMG Klynveld EDP Audit Services mee.

Ing. A. van der Vlist, assistent EDP auditor. Hij is in de sectie Software Engineering werkzaam.
Na zijn opleiding dat eindigde met het behalen van het diploma van de HIO, heeft Aart van der Vlist zich in een aantal specifieke vakgebieden verdiept. Genoemd kunnen worden: Expert systemen, optische systemen, 4e generatietalen, simulatietechnieken alsmede gestructureerde ontwikkelingstechnieken.
Hij is actief lid van NGI, NIRIA en ACM.

Ing. H.A.J.M. Spape, EDP auditor.
Reeds geruime tijd voert Henri Spape EDP audits uit.
Tijdens zijn opleiding behaalde hij het diploma van de HTS Informatica, momenteel studeert hij aan de Katholieke Universiteit Brabant, doctoraal Bedrijfseconomie en Accountancy. Een van zijn technische specialismen is datacommunicatie. Hij treedt regelmatig op als spreker op congressen van onder andere het NGI.
Hij is lid van ACM en NGI. Hij is voorzitter van de NGI-werkgroep Beveiliging Datacommunicatie.

Mw. ing. I.M. van Duin, junior EDP auditor.
Na het behalen van HTS Bedrijfskunde heeft Irma een groot deel van de AMBI-studie voltooid.
Na een start in de sectie Support & Programming richt Irma haar capaciteiten nu op het uitvoeren van EDP audit.