COMPACT

TIJDSCHRIFT EDP-AUDITING

REKENCENTRA OF BEREKENDE CENTRA

1976/6

Compact ®
Jaargang 23, nummer 6
Een uitgave van KPMG EDP Auditors NV en Samsom Bedrijfs-Informatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers RE
Drs. R.G.A. Fijneman RE RA
J.C. van Praat RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Prof.dr. J.C. Arnbak
Mr. P. van Dijken
G. van Essen
Prof.mr. H. Franken
Dr. K.J. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Redactiesecretariaat
Mw. I. de Koning, Samsom BedrijfsInformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 746
Fax : 0172 – 466 569
Vormgeving
Bureau Karakter, Delft
Opmaak
Sander Pinkse Boekproduktie, Amsterdam
Abonnementen
f 165,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom BedrijfsInformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax : 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.
Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij het redactiesecretariaat. Prijs per overdruk per artikel (inclusief omslag) f 5,-.

Uitgever
Drs. Th.P.M. Brinkman

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: • beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG, KPMG EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij Samsom BedrijfsInformatie BV, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

REKENCENTRA OF BEREKENDE CENTRA

Rekencentra maken turbulente ontwikkelingen door. Termen als decentralisatie, outsourcing en facility management zijn aan de orde van de dag. De grootschalige mainframe-omgeving is bij sommige organisaties een gepasseerd station, decentralisatie is daarbij aan de orde. Andere organisaties besteden hun IT-activiteiten uit bij aanbieders die hun kracht juist ontlenen aan de massaliteit van verwerking op grootschalige computersystemen. Dit heeft alle kenmerken van een centralisatie van verwerkingsactiviteiten.

De invloed van datacommunicatiefaciliteiten op de positie en inhoud van het rekencentrum is groot. Hierdoor worden mogelijkheden geboden tot het 'openbreken' van de relatief gesloten structuren uit het verleden, kunnen wereldwijde verbindingen worden gerealiseerd, etc. Het rekencentrum wordt met deze ontwikkelingen geconfronteerd, waarbij niet alleen de technologie aandacht verdient, maar ook het vaststellen en beoordelen van beveiligingseisen.

Kortom, ontwikkelingen zijn in diverse richtingen waarneembaar. Dit vormt de aanleiding om in deze Compact uitgebreider bij dit onderwerp stil te staan.

Rekencentra kunnen diverse stadia doorlopen (van interne aanbieder tot externe, professionele service-provider). In deze Compact wordt aan de hand van een model nader ingegaan op deze stadia, waarbij de consequenties voor het management van deze centra worden belicht. Uit de ervaring blijkt dat technologische omschakelingen tussen deze stadia nog wel te doorlopen zijn, echter dat veel aandacht benodigd is voor de organisatorische en sociale managementaspecten. Populair gezegd is het succesvol introduceren van een nieuwe positie van het rekencentrum veelal afhankelijk van hoe het tussen de oren van de medewerkers en de klanten wordt beleefd.

De EDP-auditor wordt bij de uitvoering van zijn opdrachten met deze steeds complexere structuren in rekencentra geconfronteerd. Dit vereist een goede aanpak van het onderzoek, waarbij duidelijke normen, gerelateerd aan de beoordelingsobjecten, van belang zijn. Een gestructureerde aanpak om niet het spoor bijster te raken is daarbij gewenst. Overigens is zo'n aanpak ook voor het management van het rekencentrum een conditio sine qua non. De IT-objecten dienen te worden beheerd vanuit een integrale management control-benadering.

Het rekencentrum tendeert hierdoor naar een berekend centrum. Het management maakt zich niet meer alleen druk over de aangeboden rekenfuncties (verwerkingsfaciliteiten), maar ook over de bedrijfseconomische afwegingen in en rondom het centrum. Daarbij zijn zaken aan de orde als kostprijscalculaties van services, contractafspraken, ISO-certificeringen en service level agreements.

Kortom, het management dient op zijn taak 'berekend' te zijn. Dit geldt idem dito voor de EDP-auditor in zijn adviserende of beoordelende functie.

Drs. R.G.A. Fijneman RE RA

Een beheersbaar verandertraject voor rekencentrummanagers

P. Teeuwen

De Nolan-fasentheorie kan rekencentrummanagers ondersteunen bij het doorvoeren van veranderingen in rekencentra. De EDP-auditor kan bij het doorlichten van rekencentra op verschillende kwaliteitscriteria eveneens zijn voordeel doen met deze Nolan-fasering. Met andere woorden, na identificatie van de fase waarin het rekencentrum verkeert kan worden vastgesteld, in overleg met het management, of de juiste mix van maatregelen wordt ingezet.

INLEIDING

Rekencentrummanagers hebben het zwaar tegenwoordig. Klantgericht werken, het invoeren van ITIL, de introductie van nieuwe technologieën, het maken van service level agreements, invoeren of verbeteren van doorbelasting: het leidt tot een waslijst van projecten die niet meer is te overzien. Bovendien moeten die projecten uitgevoerd worden naast de normale operationele taken: het van dag tot dag in de lucht houden van het rekencentrum. Gevolg is dat medewerkers en managers omkomen in het werk en dat het moeilijk is de zo goed bedoelde projecten op tijd af te ronden.

Maar er is hoop! Bij de analyses van vele rekencentra is Nolan, Norton & Co. (NNC) tot de slotsom gekomen dat één van de sleutels tot een *beheerste* manier van verbeteren ligt in het hanteren van de juiste *volgorde* in de vele verbeteringsacties. Het geheim is: doe het niet allemaal tegelijk en doe het in een bepaalde volgorde.

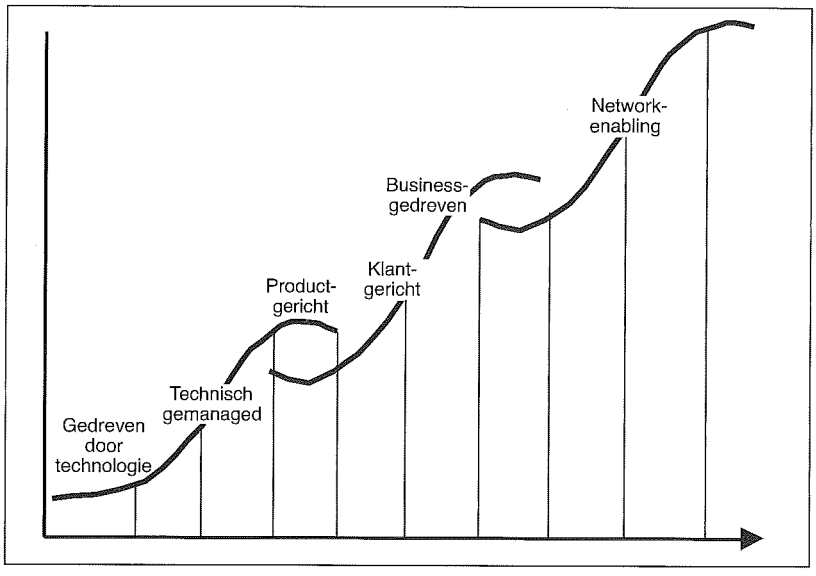
Samenvattend komt het erop neer dat de rekencentrummanager eerst de techniek onder controle moet krijgen en daarna de financiën. Als hij dat voor elkaar heeft, dan is de basis gelegd om op een succesvolle manier klantgericht te kunnen gaan werken. Deze volgorde is ingegeven door de Nolan-fasentheorie en zal in de volgende paragrafen verder worden uitgewerkt[1].

EEN FASENTHEORIE VOOR REKENCENTRA

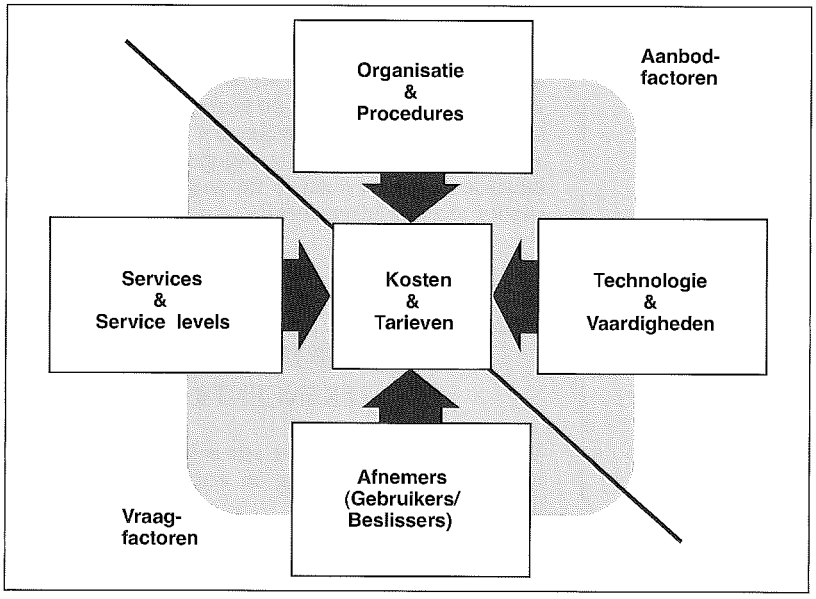
Voor de ontwikkeling die een rekencentrum doormaakt, kan een fasering in zes stappen worden aangehouden:
- technisch gedreven;
- technisch gemanaged;
- productgericht;
- klantgericht;
- business-gedreven;
- network-enabling.

De relatie met groeifasen is in figuur 1 weergegeven.

De Nolan-fasentheorie is een model om organisatie en automatisering op elkaar aan te sluiten. Door het toepassen van deze theorie worden de veranderingsprocessen in de automatisering beheersbaar. Deze beheersbaarheid ontstaat door een viertal groeiprocessen in samenhang te managen. Deze groeiprocessen, hier aangepast voor de situatie in rekencentra, spelen in elke fase een rol (zie figuur 2):
- organisatie en procedures;
- technologie/vaardigheden van het personeel;
- de services en service levels die aangeboden worden;
- de rol die de klanten spelen, te onderscheiden naar gebruikers en beslissers.



Figuur 1. Het rekencentrum in de Nolan-fasen.



Figuur 2. De groeiprocessen voor een rekencentrum.

Financieel vindt een en ander zijn neerslag in het kostenniveau van het rekencentrum en de bijbehorende tarieven. Een analyse van het uitgavenpatroon door benchmarking kan een goede start zijn van een plaatsbepaling van het rekencentrum in de fasen.

De vier bovengenoemde groeiprocessen kunnen worden gesplitst in twee vraagfactoren (services en klanten) en twee aanbodfactoren (organisatie en procedures, respectievelijk technologie/vaardigheden).
Ook voor het rekencentrum geldt dat het pas optimaal wordt gebruikt als er een evenwicht is tussen de vraagfactoren en de aanbodfactoren. Dit betekent bijvoorbeeld dat een goed rekencentrum slechts kan ontstaan indien er een goede klantengroep is.

1. Voor een beschrijving van de Nolan-fasentheorie zie Van der Zee en Koot: IT-Assessment (gepubliceerd in Informatie jaargang 31 nr. 11).

Verderop in het artikel wordt hierop teruggekomen.

Het is de taak van de rekencentrummanager zijn organisatie door de fasen heen te leiden. Om de juiste acties te initiëren, moet hij weten in welke fase hij begint. Dit startpunt kan worden bepaald door de vergelijking van het rekencentrum met 'best practice'-modellen (zoals die bijvoorbeeld in KPMG's World Class IT-methoden beschikbaar zijn); ook een benchmark-vergelijking kan helpen om het rekencentrum te positioneren.

Als de rekencentrummanager zijn verbeteracties start, let hij erop dat de vier groeiprocessen en de financiële aspecten steeds in balans blijven. In de volgende paragrafen zullen wij de fasen beschrijven en daarna focussen op de acties die de rekencentrummanager moet initiëren om zijn organisatie in de volgende fase te brengen.

BESCHRIJVING VAN DE FASEN

Hieronder worden de fasen in meer detail behandeld.

Het technisch gedreven rekencentrum

De eerste fase, die in de meeste rekencentra een tiental jaren achter ons ligt, werd gekenmerkt door de kennismaking met de techniek. De managementstijl was ad hoc en gericht op technische events. Er was geen inbreng van de gebruiker en geen financieel management.
Er werden met name financiële applicaties gedraaid in het rekencentrum; er was echter geen sprake van diensten.

Het technisch gemanaged rekencentrum

In de tweede stap ligt de nadruk op het onder controle krijgen van de techniek. Men herhaalt wat blijkt te werken. Hiertoe worden procedures ingevoerd voor bijvoorbeeld capaciteitsmanagement en change management. Dit zijn vaak informele procedures, die langzaam maar zeker uitdijen tot een bureaucratisch geheel.
Rekencentrumdiensten worden in deze fase de facto als afgeleide beschouwd van systeemontwikkelingstrajecten. Daarbij is er een vrijwel onbeperkte vraag vanuit de klantkant, waarbij van een werkelijke prioriteitstelling geen sprake is. Prioriteiten worden bepaald door wie het hardst schreeuwt. Dit kan ook leiden tot snelle wisselingen in de technologie, wat voor de technisch georiënteerde specialisten in het rekencentrum kansen oplevert, die met beide handen worden aangegrepen.

Het productgerichte rekencentrum

In de derde stap begint het besef door te dringen dat het rekencentrum een product levert. Het be-

langrijkste thema is het definiëren van de producten en deze op een consistente manier aanbieden. Deze wijze van aanbieden wordt vaak service genoemd, maar gaat veelal niet verder dan CPU-seconden en megabytes. Om die consistentie in het productaanbod te krijgen, wordt vaak een matrixorganisatie opgericht met naast een technische verantwoordelijkheid een productverantwoordelijkheid.
Soms slaat dit door naar te veel afstemming en bureaucratie.

Als gevolg van de snelle kostenstijging in de vorige fase zoekt het management naar middelen om de kosten onder controle te krijgen. Voltooiing van budgettering en invoering van doorbelasting zijn hier aan de orde.
Ook financieel georiënteerde benchmarks kunnen hier een belangrijke rol spelen. Indien de resultaten daarvan tegenvallen, kan dat bijdragen tot het gevoel van crisis dat aan het eind van deze fase optreedt.

Door de grote veranderingen in het vraagpatroon van de klanten (ook PC's, netwerken, pakketten, ad hoc-oplossingen), kraakt de oude matrix van techniek en product in zijn voegen. Afbraak van de bureaucratie is nodig om een antwoord aan de klant te kunnen geven.
In deze fase zien we ook de omslag van het traditionele (mainframe-georiënteerde) rekencentrum naar een algemener infrastructuurcentrum. Het rekencentrum ziet kansen in andere producten zoals kantoorautomatisering, PC's, netwerken.

Men begint met SLA's (service level agreements) om de bestaande diensten vast te leggen. Dit zijn vaak standaarddiensten met weinig mogelijkheden voor de klant om variaties te vragen (bijvoorbeeld in openingstijden). Soms verzanden deze SLA's in een bureaucratische exercitie met weinig toegevoegde waarde.

Het klantgerichte rekencentrum

De overgang naar het klantgerichte rekencentrum is te vergelijken met de kanteling van de product/markt-matrix die vele bedrijven in verschillende branches hebben meegemaakt. Doelstelling is zo goed mogelijk aan de verwachtingen van de klant tegemoet te komen. Dat betekent dat er verschillende service levels zijn voor verschillende klanten (in termen van responstijd of openingstijden). Dit leidt tot de noodzaak om tot klantsegmentatie te komen om het leveringsprogramma beheerst te houden.
De klanttevredenheid wordt gemeten als een continu proces. Eén van de essentiële punten om klanten tevreden te maken en te houden is het managen van de verwachting van die klant. Als klanten onrealistische verwachtingen hebben, zullen zij nooit tevreden gesteld kunnen worden. Dit vereist ook volwassenheid aan de klantkant.

In deze fase komt ook een grote cultuurverandering aan de orde, met een nadruk op business skills. Voor het technisch georiënteerde personeel in het rekencentrum betekent dit een minder prominente rol en een vermindering van de invloed van deze medewerkers. Op persoonlijk vlak kan dit tot grote onzekerheden leiden. In het meetsysteem moet daarom duidelijk worden wat van hen wordt verwacht en wat hun bijdrage aan het succes van het rekencentrum is.

Bij de klantgerichte focus hoort dat alle diensten in SLA's zijn vastgelegd met rapportage en doorbelasting in business-termen. Daarnaast is er voor intern gebruik een complete set van performance-indicators waarmee de onderliggende processen worden bewaakt.

SLA's krijgen langzaam maar zeker het karakter van gewone contracten. Dit zullen vaak meerjarige contracten zijn. Om de financiële risico's te beperken zal het rekencentrum in zijn verplichtingen rekening gaan houden met de looptijd van de contracten en proberen de verplichtingen (bijvoorbeeld leases) zo goed mogelijk in overeenstemming te brengen met de contractduur.

Het business-gedreven rekencentrum

In het business-gedreven rekencentrum wordt de belangrijkste opgave het organiseren van de productontwikkeling om die producten te blijven aanbieden die de klanten nodig (zullen) hebben.

In het klantgerichte rekencentrum krijgen de SLA's het karakter van gewone contracten.

De klanten die het rekencentrum op dit niveau benaderen, weten hoe informatietechnologie werkt, zien informatietechnologie als een integraal deel van hun business en maken weinig onderscheid tussen interne of externe dienstverleners. De bijdrage van de IT-leverancier (intern of extern) aan het realiseren van de bedrijfsdoelstellingen van de klant is maatgevend voor de tevredenheid van de klant.

Om toegevoegde waarde te kunnen blijven leveren moet het rekencentrum als leverancier zijn productenpakket up-to-date blijven houden. Voor hobbyisme is echter geen plaats; diensten zullen worden geleverd tegen marktprijzen en niet tegen kostprijzen. Mislukte productontwikkeling gaat dus direct ten koste van het financiële resultaat van het rekencentrum.

Waar in eerdere fasen het rekencentrum vaak ook nog een centrale ('corporate') beleidstaak had, worden het dienstencentrum en de centrale beleidsstaf in deze fase van elkaar gesplitst. Daarnaast zijn er binnen de business units IT-verantwoordelijken. De reden ligt in de verschillende doelen van de twee organisaties. Voor het dienstencentrum is dat het zo effectief mogelijk leveren van diensten; voor de centrale ligt dat in het bewaken van synergie, architectuur, samenhang en dergelijke.

Het network-enabling rekencentrum

In het network-enabling rekencentrum wordt de belangrijkste opgave het ondersteunen van nieuwe organisatievormen zoals team-based organisaties. Hiertoe zal het dienstencentrum computer- en netwerkfaciliteiten aanbieden, maar wellicht ook applicatieve modules voor algemeen gebruik.

Het onderscheid tussen de interne en de externe leverancier verdwijnt geheel. Klanten letten op toegevoegde waarde en de performance en zijn niet werkelijk geïnteresseerd in de juridische status van het rekencentrum.

In het network-enabling rekencentrum verdwijnt het onderscheid tussen de interne en de externe leverancier.

Klanten zijn steeds op zoek naar nieuwe manieren van werken, en verwachten van hun IT-partners (wat het rekencentrum dan moet zijn) steeds nieuwe vormen van IT-ondersteuning.

ACTIES VOOR DE REKENCENTRUMMANAGER

Voor een rekencentrummanager is het belangrijk te weten welke stappen hij moet nemen om van de ene fase naar de volgende te komen. In deze paragraaf zullen de acties worden beschreven die moeten worden uitgevoerd.

De overgang naar het technisch gemanaged rekencentrum

Deze overgang is in de meeste gevallen reeds lang achter de rug: het gaat hier om het invoeren van technische standaarden die in het verleden zijn ontstaan door eenvoudigweg te herhalen wat blijkt te werken.
Tegenwoordig is het ITIL-raamwerk beschikbaar en is de start van een ITIL-implementatie een goede manier om de techniek onder controle te krijgen. Het gaat dan met name om de ITIL-processen Incident, Problem, Change en Operations management.

De overgang naar het productgerichte rekencentrum

Bij de overgang naar het productgerichte rekencentrum komt er naast de lijnorganisatie verantwoordelijk voor de techniek, een lijn met een productverantwoordelijkheid. Een matrix-organisatie is geboren.

In termen van ITIL-implementatie introduceert men Capacity management en Availability management, terwijl een begin wordt gemaakt met Service management.

Deze overgang treedt vaak op in een periode dat er grote kostendruk is op informatietechnologie in het algemeen (eind fase 3 in Nolan-termen).

Gedwongen door het algemeen management moet de rekencentrummanager actie ondernemen op de gebieden van budgettering en invoering van doorbelasting.
Ook financieel georiënteerde benchmarks spelen hier een belangrijke rol. Indien de resultaten daarvan tegenvallen, kan dat bijdragen tot het gevoel van crisis dat aan het eind van deze fase optreedt.
In gevallen waar uit de benchmark-vergelijking blijkt dat het rekencentrum duurder is dan vergelijkbare rekencentra, komt dit meestal doordat het aantal procedures is geëxplodeerd en dat het personeel in het rekencentrum (met de beste bedoelingen) meer elkaar bezighoudt, dan dat het waarde aan het product toevoegt.
Dit gaat dan bovendien nog samen met een weinig klantgerichte opstelling.

Aan het einde van de fase van het productgerichte rekencentrum begint het besef door te dringen dat klanten belangrijk zijn. Er wordt een start gemaakt met service level management en het opstellen van service level agreements. Een risico hierbij is dat indien de mate van bureaucratie nog te hoog is, ook het opstellen van de service level agreements een bureaucratische exercitie wordt met relatief weinig toegevoegde waarde.

De overgang naar het klantgerichte rekencentrum

Het managen van een cultuurverandering is het belangrijkste element voor de rekencentrummanager bij de overgang naar het klantgerichte rekencentrum. Een cultuuromslag van gerichtheid op technisch perfectionisme naar resultaatgericht (waarbij resultaat vanuit de klant gedefinieerd wordt) is daarbij nodig.
Afbraak van de aanwezige bureaucratie is hierbij een noodzakelijke voorwaarde. Alle medewerkers moeten het eisenpakket van de klant voelen; niemand mag door dikke lagen bureaucratie hiervan worden afgeschermd.

Om ieders bijdrage te definiëren en te volgen, krijgt iedere functie een set van performance-indicators. Dit ondersteunt het resultaatgericht werken in hoge mate.
Een bijkomend voordeel is dat dit aan de technici in het rekencentrum duidelijk maakt wat hun bijdrage is. Door het klantgerichte werken vermindert hun invloed, wat frustratie op kan leveren. Het duidelijk definiëren van doelstellingen kan dit voor een deel voorkomen.

In het klantgerichte rekencentrum worden alle diensten door SLA's gedekt. Het voltooien van de SLA's is een belangrijke taak in het begin van deze fase. Later in deze fase wordt gerealiseerd dat rap-

portages en doorbelasting in business-termen gaan geschieden.
Deze SLA's worden in toenemende mate klantspecifiek. Waar in het productgerichte rekencentrum vaak sprake is van standaard-openingstijden, standaard-responstijden en standaard-uitwijkvoorzieningen, is het klantgerichte rekencentrum in staat hier gedifferentieerde diensten aan te bieden.
De vraag van 'volwassen' klanten zal in deze fase het rekencentrum dwingen zijn interne structuur aan te passen, onder andere door het instellen van servicemanagers per klant.

De rekencentrummanager gaat in deze fase bewust kiezen wat hij in zijn eigen organisatie kan doen en welke diensten hij zal inkopen van derden. Door bijvoorbeeld gebrek aan schaalgrootte, of door de mate van specialisme, zal het rekencentrum niet in staat alles zelf tegen concurrerende prijzen te doen.

In deze fase gaat het rekencentrummanagement bewust de verwachtingen van de klant managen. Tevreden klanten kunnen immers alleen bestaan indien het verwachtingsniveau realistisch is.
Als een rekencentrum voorloopt op zijn klant, kunnen op dit punt spanningen ontstaan. Het rekencentrum zal mogelijk zelfs terug moeten vallen op een houding die past bij een eerdere fase.

Aan het eind van deze fase zullen de meeste SLA's de vorm hebben van een meerjarencontract. Het rekencentrummanagement zal, om de financiële risico's te beperken, ervoor moeten zorgen dat de verplichtingen (bijvoorbeeld leases) overeenkomen met de duur van de contracten.

Hierbij past ook een financiële verzelfstandiging tot een profit center met de mogelijkheid om meerjarencontracten af te sluiten, investeringen zelf te bepalen en het financiële resultaat te bestemmen voor eigen investeringen (na een redelijke afdracht aan de aandeelhouders).

De overgang naar het business-gedreven rekencentrum

Het business-gedreven rekencentrum moet zijn bestaansrecht elke keer weer bewijzen door diensten met toegevoegde waarde voor de klant aan te bieden.
De klant beoordeelt zijn leveranciers (en dus ook zijn rekencentrum) op performance, en maakt daarbij geen onderscheid tussen interne en externe leveranciers.

De rekencentrummanager moet zijn organisatie stimuleren steeds nieuwe diensten met toegevoegde waarde aan te bieden aan zijn klanten. Hij kan hierbij niet meer rekenen op 'corporate' richtlijnen en gedwongen winkelnering. Dit betekent dat het rekencentrum voortdurend in staat moet zijn nieuwe producten te definiëren. De rekencentrummanager moet daartoe zijn productontwikkeling organiseren.

In deze fase zullen de verleende diensten afgerekend gaan worden op marktprijzen, en niet meer op kostprijzen, zoals voorheen. Tevergeefse productontwikkeling leidt dan ook direct tot een verlies op de bottom line.

De sterke druk van de gebruikersorganisatie op het business-gedreven rekencentrum als dienstverlener leidt ertoe dat het rekencentrum zich op die rol moet concentreren. Het rekencentrum moet pertinent weigeren de dubbelrol op zich te nemen van dienstverlener én bewaker van de bedrijfsbrede ('corporate') architectuur en infrastructuur. De tweede rol zal namelijk voortdurend in conflict komen met de eerste rol. Bovendien kan die tweede rol niet gefinancierd worden uit de lopende dienstverlening, omdat de druk op de prijzen te groot zal zijn.

Vanuit de nadruk op toegevoegde waarde zal de rekencentrummanager zich ook structureel moeten bezinnen op wat hij zelf doet en wat hij inkoopt (make or buy). Wide Area Netwerken vormen nu reeds een dienst die maar weinig rekencentra zelf kunnen aanbieden. In de toekomst zal de rekencentrummanager gedwongen zijn voortdurend de afweging te maken welke diensten hij van derden moet betrekken en waar de toegevoegde waarde van zijn diensten zit.
Als de rekencentrummanager diensten die elders beter of goedkoper zijn toch zelf uitvoert, ondergraaft hij de economische basis van zijn organisatie.

Het business-gedreven rekencentrum moet voortdurend in staat zijn nieuwe producten te definiëren.

De overgang naar het network-enabling rekencentrum

Langzamerhand worden de contouren duidelijk van wat de netwerkorganisatie zal gaan betekenen voor organisaties[2]. Op dit moment lijkt het erop dat een werkelijk business-gedreven rekencentrum relatief makkelijk de overgang naar een network-enabling rekencentrum kan maken. De druk vanuit de gebruikersorganisatie zal immers zo groot zijn dat het aanbieden van de juiste diensten een 'do or die' zal zijn. Indien het rekencentrum zijn productontwikkeling goed voor elkaar heeft, zal het ook in staat zijn steeds de juiste diensten in de portefeuille te hebben.

TOT SLOT

Het doorlopen van de beschreven ontwikkeling vormt geen gemakkelijke weg. Er zijn rekencentra die een aantal van deze stappen met succes hebben doorlopen en op weg zijn naar de volgende fase. De meest geavanceerde rekencentra zijn op dit mo-

2. *Zie bijvoorbeeld Nolan en Croson: Creatieve Destructie: zes fasen voor bedrijfstransformatie (Uitgeverij Contact 1995/Harvard Business School Press).*

P. Teeuwen
Was ten tijde van het schrijven van dit artikel senior adviseur op het gebied van organisatie van rekencentra bij Nolan, Norton & Co. (NNC). Tegenwoordig is hij verantwoordelijk voor de introductie van doorlichtingsmethoden voor IT-organisaties in verschillende Europese landen in het kader van het KPMG World Class IT-programma. Tevens geeft hij in dat kader opleidingen aan KPMG- en NNC-adviseurs over doorlichtings- en benchmark-methoden.

ment op weg om de stap naar het klantgerichte rekencentrum te volbrengen.

Het vak van rekencentrummanager is een boeiend vak. De reeks van stappen overziend, valt op dat het karakter van de functie verandert van een technisch gerichte functie via een financieel gerichte functie naar een marketinggerichte functie. Dit is in overeenstemming met de veranderingen die vele andere organisaties hebben doorgemaakt. In die zin wordt nog eens duidelijk dat een rekencentrummanager van vandaag een algemeen manager met verstand van techniek moet zijn.

Van rekencentrum naar infocentrum

Dr. ing. H.T.M. van der Zee

Het traditionele rekencentrum (technisch, capaciteitsgeoriënteerd) blijkt onder druk van marktontwikkelingen steeds vaker te veranderen. Dit vraagt om herstructurering van de interne activiteiten. De EDP-auditor kan als sparringpartner voor het management optreden bij deze veranderingsprocessen. Hiervoor dient de EDP-auditor te beschikken over inzicht in de motieven voor de veranderingen. Vanuit een pro-actieve rol kan de EDP-auditor adviserend toegevoegde waarde leveren, echter ook bij het uitvoeren van security audits is kennis van deze veranderingsprocessen van belang.

INLEIDING

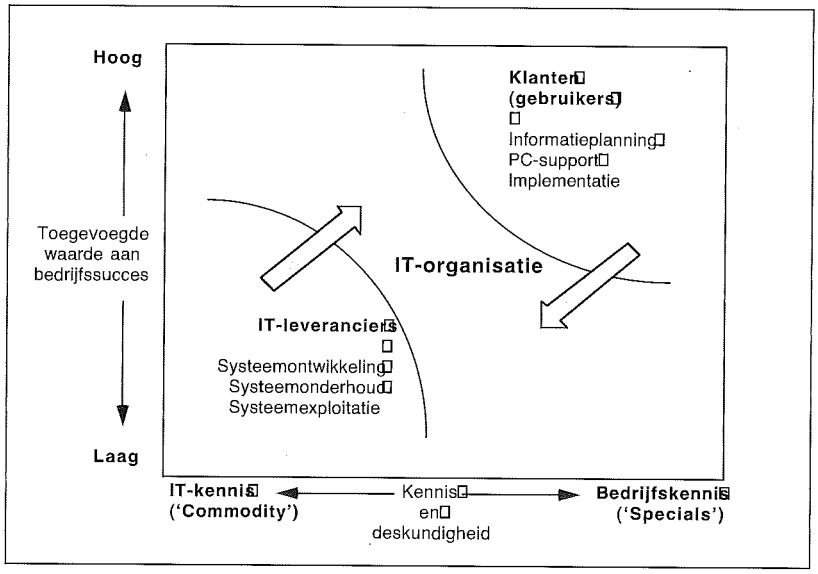
De IT-organisatie in het algemeen, en het rekencentrum in het bijzonder, komt steeds meer onder druk te staan: de concurrentie is hevig. Enerzijds komt deze concurrentie vanuit de richting van commerciële, professionele dienstverleners, die claimen door hun schaalgrootte aanzienlijk goedkoper te zijn. Zij voeren voornamelijk traditionele IT-activiteiten uit, zoals systeemontwikkeling, systeemonderhoud en systeemexploitatie. Daarnaast is er concurrentie vanuit de richting van afnemers die een aantal IT-activiteiten zelf uitvoeren, zoals informatieplanning, ondersteuning van PC-gebruik, implementatie van nieuwe informatie(deel)systemen, etc. De IT-organisatie ziet daarmee een aantal taken die zij traditioneel uitvoerde verdwijnen of aanzienlijk verminderen (zie figuur 1).

Daarmee staat ook het rekencentrum onder druk, en daarom opereert het steeds vaker als een zelfstandige, autonome eenheid, bijvoorbeeld in de vorm van een facilitair bedrijf. Het moet kunnen aantonen dat kwalitatief hoogwaardige producten en diensten worden geleverd die net zo aantrekkelijk zijn geprijsd als de concurrerende producten en diensten van IT-leveranciers. Als gevolg hiervan zal een rekencentrum zich moeten transformeren naar een commercieel denkend bedrijf, met een oriëntatie op markten en producten, in plaats van budgetten en aantallen personeelsleden. De 'marketing-P's' (product, prijs, promotie en plaats) vormen tezamen met de S van service belangrijke drijfveren voor het voortbestaan (zie figuur 2).

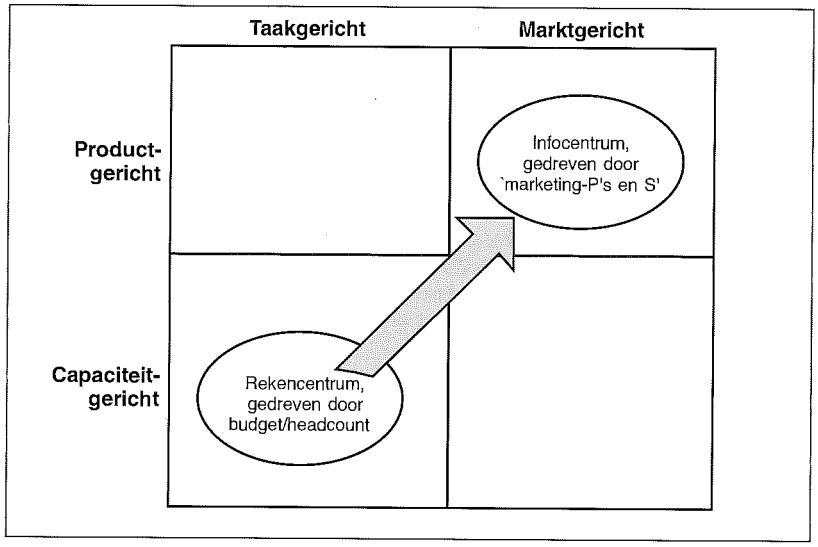
Het uiteindelijke succes kan, net als in andere commerciële organisaties, worden bepaald door de omzet te verminderen met de kosten. Het verschil is de winst – het succes. De winst kan worden verbeterd door de omzet te vergroten, de kosten te verlagen, of beide. De twee zijden van de verlies- en winstrekening vergen daarmee dus de nodige aandacht.

Het verhogen van de omzet kan op verschillende manieren worden gerealiseerd, zoals het verbeteren van de dienstverlening in termen van beschikbaarheid en flexibiliteit, het aanbieden van nieuwe vormen van dienstverlening op het gebied van gedistribueerde gegevensverwerking, het beheer van lokale netwerken, het beheer van werkplekautomatisering en dergelijke. En, als het rekencentrum een zelfstandige eenheid is, kan natuurlijk naar nieuwe klanten worden gezocht buiten de grenzen van de 'eigen' organisatie. Voor de rekencentra die niet als zelfstandige eenheid werken geldt dat aanvullende omzet kan worden gegenereerd met nieuwe producten en diensten, maar omdat het rekencentrum een kostenpost is voor de 'moederorganisatie' zal het niet direct kunnen profiteren van omzet bij derden.

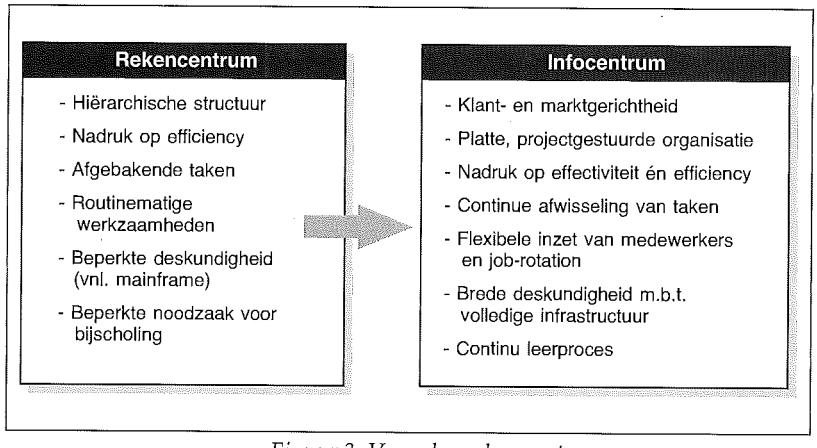
Als kostenpost zal het rekencentrum regelmatig onder de loep worden genomen, en het stelselmatig verlagen van kosten heeft dan de grootste aandacht.



Figuur 1. De IT-organisatie onder druk.



Figuur 2. Verandering van oriëntatie.



Figuur 3. Veranderende aspecten.

Het verlagen van kosten kan op verschillende manieren worden gerealiseerd, zoals het consolideren van meerdere rekencentra, het vergaand automatiseren van handmatige handelingen, het (gedeeltelijk) uitbesteden van rekencentrumactiviteiten, of het aangaan van flexibelere financieringsvormen met hardwareleveranciers.

WAT VERANDERT ER EIGENLIJK?

Verhoging van de omzet en vermindering van kosten moeten worden gezocht in veranderende producten, diensten en soms markten (klanten); de optimalisering van werkprocessen en de organisatie; de inzet van mensen en middelen; en, last but not least, een aangepaste cultuur van het traditionele rekencentrum.

Producten en diensten

Hoe effectief het infocentrum feitelijk is wordt uiteindelijk bepaald door de afnemers van de diensten: de klanten, in het verleden ook wel gebruikers genoemd. Het is dus zaak om pro-actief de (latente en potentiële) behoeften en wensen van klanten te inventariseren en het scala van aan te bieden producten en diensten met deze behoeften in overeenstemming te brengen.

De behoeften van klanten kunnen worden ontleend aan een aantal kenmerken van een moderne organisatie en de invloed daarvan op de beschikbaarheid en betrouwbaarheid van IT-faciliteiten, zoals:

– Sneller werken vanwege de korte doorlooptijden van bedrijfsprocessen vereist korte responstijden van informatiesystemen, realtime-verwerking van transacties en automatisering van werkzaamheden die relatief gezien weinig waarde toevoegen.

– Klantgericht werken vereist de toegankelijkheid en beschikbaarheid van allerlei gegevens die in verschillende databases opgeslagen kunnen zijn, inzicht in het historisch verloop van de klantrelatie en de transacties die in het verleden met de klant zijn aangegaan, etc. en dat alles met een 7 x 24 uur online-beschikbaarheid van dit soort gegevens.

– Proces- en teamgericht werken (in tegenstelling tot de traditionele functionele en afdelingsgewijze inrichting van bedrijfsactiviteiten) vereist procesondersteunende informatietechnologie zoals workflow-tools en teamondersteunende hulpmiddelen zoals groupware, inclusief het beheer, de begeleiding en de ondersteuning van deze beide.

– Autonoom werken als gevolg van vergaande decentralisatie en delegatie van verantwoordelijkheden vereist, naast de toegankelijkheid van een scala van informatiebronnen, de beschikbaarheid van hoogwaardige en gebruikersvriendelijke faciliteiten zoals beslissingsondersteunende systemen, tekstverwerkers, datamanipulatie-tools en ver-

gaande communicatiemogelijkheden (fax, E-mail en dergelijke).

– Het werken op een veelheid van plaatsen (zoals op het werk, thuis, bij de klant en onderweg) vereist naast de beschikbaarheid van informatiebronnen en uitgebreide communicatiefaciliteiten de mogelijkheid om centrale en decentrale databases continu te kunnen up- en downloaden en te kunnen synchroniseren.

De door het infocentrum aangeboden portfolio van producten en diensten wordt dus niet langer uitgedrukt in termen als CPU-capaciteit, opslagcapaciteit, printcapaciteit en vergelijkbare eenheden (zoals het traditionele rekencentrum dat deed in het verleden), maar in termen die de klant aanspreken en die aansluiten bij de 'werkzaamheden nieuwe stijl' van de klant van het infocentrum.

Werkprocessen en organisatie

De inrichting van de bedrijfsprocessen, de organisatie van het infocentrum en de uitvoering van taken dienen afgestemd te zijn op de nieuwe portfolio van producten en diensten en op de relatie met de klant. Processen moeten, net zoals dat in andere organisatie-onderdelen gebeurt, worden ge-'reengineered' om optimale prestaties te bereiken in termen van kosten, doorlooptijd en door de klant gevraagde kwaliteit. Werkprocessen en organisatie worden ingericht om zowel de efficiency als de effectiviteit te maximaliseren (zie figuur 4), waarbij de projectorganisatie als organisatiestructuur domineert daar waar het mogelijk is.

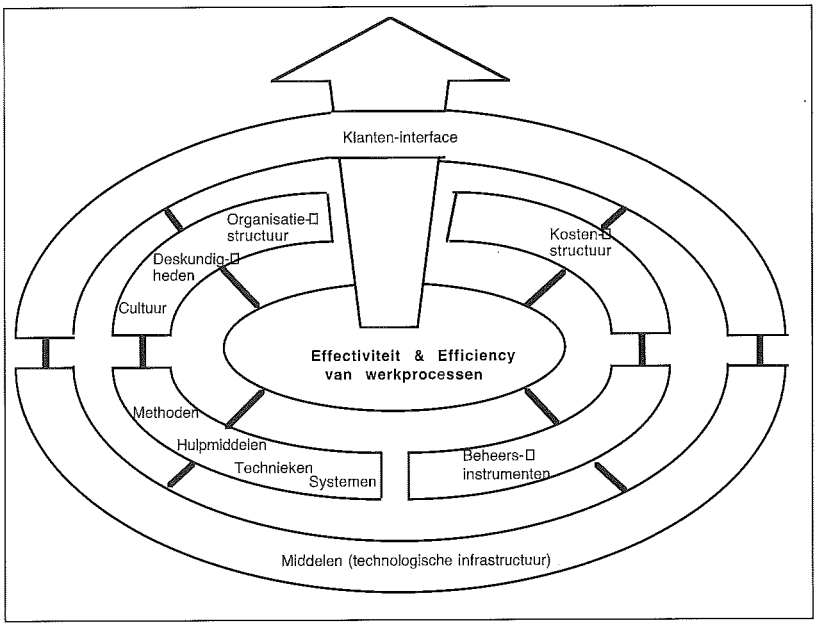
Effectiviteit (doen we wat we moeten doen) heeft dan vooral met de huidige en toekomstige relatie met de klant te maken. Deze externe gerichtheid omvat aspecten als account management, marketing, SLA-management, problem solving, klantenservice en helpdeskdienstverlening. Processen en organisatievorm zijn voor wat betreft de effectiviteit gericht op een optimale tevredenheid van de klant in de verschillende fasen van dienstverlening: vooraf, tijdens, en achteraf.

Efficiency (doen wat we moeten doen tegen de laagst mogelijke kosten) betreft interne aspecten zoals de productiviteit van werkwijzen en de inzet van mensen en middelen. Vergaande automatisering van administratieve en beheerstaken van het infocentrum is mogelijk, zodat enerzijds de totale kosten kunnen worden verlaagd en anderzijds capaciteit kan worden vrijgemaakt voor taken die een hogere waarde toevoegen aan de klanttevredenheid.

Mensen en middelen

In het infocentrum zijn de belangrijkste kostenposten (of positiever geformuleerd: de 'core competencies en resources') de mensen en de technologie die nodig zijn om de producten en diensten te realiseren.

De technologie verandert snel. Niet alleen de mogelijkheden van mainframetechnologie maar ook die van midrange-computers, werkstations, LAN's, netwerkcomputers, openbare netwerken (Internet) en input/output-media vereisen een continue herbezinning over de inzet van deze middelen. Daarbij speelt uiteraard ook de veranderende kostprijs van de verschillende componenten een grote rol. Zo geeft de Nolan, Norton & Co Data Center Baseline Database (die benchmarks omvat van honderden rekencentra/infocentra) een kostendaling aan van maar liefst gemiddeld twintig procent van de technologie-uitgaven door infocentra in de periode 1994–1995. Deze verlaging van kosten werd voornamelijk gerealiseerd door renovatie van hard-, soft- en netware, door alternatieve financieringsovereenkomsten met leveranciers, door verbeterde planning van capaciteitsvereisten en door samenwerking met leveranciers of anderen om samen piek-capaciteitsbehoeften in te dekken of te delen.



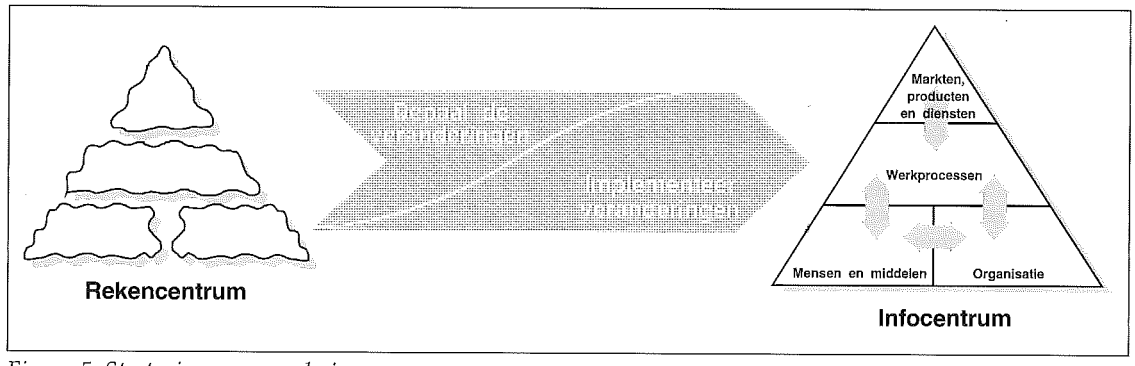
Figuur 4. Effectiviteit en efficiency van werkprocessen.

De inzet van mensen verandert eveneens. De genoemde Nolan, Norton & Co Data Center Baseline Database geeft een daling in het aantal infocentrum-medewerkers aan van gemiddeld twaalf procent per jaar gedurende de periode 1991–1995. Deze daling is vooral te danken aan de verder gaande invoering van geautomatiseerde verwerking van routinematige zaken, minder arbeidsintensieve parametrisering en verbeterde betrouwbaarheid van soft-, hard- en netware. Tegenover de daling in de personeelsbehoeften voor administratieve en beheertaken is echter een verhoging waar te nemen van het benodigde personeel voor de planning en het architectuurontwerp van de gehele infrastructuur, en voor het verlenen van assistentie aan de klant. Deze verhoging past bij de veranderende oriëntatie van rekencentrum naar infocentrum.

Cultuur

De aandacht voor pure efficiency en het leveren van CPU-, disk- en printcapaciteit in het verleden maakt dus plaats voor de aandacht voor effectivi-

Dr. ing. H.T.M. van der Zee
Is directeur van het Nolan, Norton & Co Institute, een Research Organisatie van KPMG te Utrecht.



Figuur 5. Strategie voor verandering.

teit én efficiency, infrastructurele producten en diensten, klantenservice, marketing, innovatie, communicatie en dergelijke. Deze ommezwaai vormt voor velen een grote culturele verandering – en dat moet het ook zijn om als infocentrum succesvol te kunnen opereren. Veranderingen in de cultuur zullen daarom ook moeten worden begeleid door de 'rules of the game' die de informele organisatie ondersteunen: een adequate prestatiemeting van producten, diensten en processen die past bij de nieuwe missie van het infocentrum, de bijbehorende loopbaanbegeleiding en beoordelingssystemen, de beloningsstructuur en dergelijke. Bovenal is een hernieuwde managementstijl onontbeerlijk die past bij de nieuwe waarden, normen en uitdagingen voor het infocentrum.

HOE ZIET EEN SUCCESVOLLE VERANDERINGSSTRATEGIE ERUIT?

Omdat geen enkele situatie hetzelfde is, zal ieder rekencentrum voor zichzelf een strategie moeten ontwikkelen om vanuit de huidige situatie van het rekencentrum de brug te slaan naar de uitdagingen van de toekomst: het infocentrum. Deze strategie is gericht op een optimale configuratie van werkprocessen, organisatie, mensen en middelen, zodanig dat de juiste producten en diensten op effectieve en efficiënte wijze worden aangeboden aan de klanten van het infocentrum, en zodanig dat de gewenste cultuur wordt ondersteund of mogelijk gemaakt (zie figuur 5).

Bij de strategie-ontwikkeling kunnen de volgende richtlijnen behulpzaam zijn:

– Onafhankelijk van de vraag of het infocentrum een zelfstandige, autonome entiteit is of niet: gedraag je als zodanig. Beschouw het infocentrum als een organisatie die concurreert met andere, eveneens commerciële dienstverleners van IT-faciliteiten. Bestudeer de cultuur, het gedrag en de werkwijzen van deze commerciële organisaties en evenaar ze.

– Optimaliseer de reikwijdte en diepgang van de aan te bieden portefeuille van producten en diensten. Wees creatief, en denk vanuit de (latente of potentiële) behoeften van de klant.

– Ga pro-actief marketen en verkopen: word een organisatie die wordt gedreven door de mogelijkheden van de markt, in plaats van de organisatie die wordt beperkt door budgetten en toegestaan aantal personeelsleden.

– Evalueer de processen en de organisatiestructuur van het infocentrum. Optimaliseer processen met behulp van re-engineeringtechnieken en voer een meer project-gerichte organisatiestructuur in, in plaats van de aloude hiërarchische structuur.

– Automatiseer zoveel mogelijk de routinematige administratieve en beheersfuncties.

– Pas de bestaande loopbaanontwikkelingsprogramma's aan om tegemoet te komen aan de benodigde eisen ten aanzien van de kwalitatief en kwantitatief benodigde kennis en kunde, vooral op het gebied van klantrelaties, innovatie en technologieplanning.

– Pas de personeelsbeoordelingssystemen aan om de culturele veranderingen te kunnen ondersteunen en te versterken.

– Ga allianties aan met leveranciers en eis optimale flexibiliteit ten aanzien van capaciteit, inkoopcondities en ondersteuning. Overweeg innovatieve financieringsvormen.

CONCLUSIE

De toekomst van het rekencentrum hangt direct af van de manier waarop de ommezwaai naar een slagvaardig, toekomstgericht, commercieel infocentrum wordt gemaakt. Omdat er vele kapers op de kust zijn zal een uitgekiende strategie noodzakelijk zijn om de concurrentie buiten de deur te houden. De noodzakelijke transformatie van producten, diensten, werkprocessen, organisatie, mensen, middelen en cultuur is primair gericht op optimale klanttevredenheid, innovatie en efficiency, en zou wel eens de levensverzekering voor de toekomst kunnen zijn.

Informatiebeveiliging in outsourcing-trajecten

H.R.D. Janus,
G. Hulst CISA,
ing. A. Shahim en
dr. E. Roos Lindgreen

Zowel aan de vraagzijde als aan de aanbodzijde zal in de outsourcing-markt rekening moeten worden gehouden met beveiligingseisen. Een op de Code voor Informatiebeveiliging/British Standard 7799 gebaseerde cyclische benadering wordt beschreven die de service-provider en diens afnemer in staat stelt duidelijke afspraken te maken over de wederzijdse verantwoordelijkheden op het gebied van informatiebeveiliging. De service-provider en de afnemer stellen hiertoe een formele beveiligingsovereenkomst op die deel uitmaakt van het algemene service level agreement. De overeenkomst wordt afgeleid van een classificatie van de te beheren IT-omgeving; een onafhankelijke derde toetst de naleving van de overeenkomst.

INLEIDING

De moderne informatietechnologie (IT) kent vele zegeningen, maar zowel de kosten als de kwaliteit van de IT-dienstverlening laten in veel organisaties nog te wensen over. Volgens recent onderzoek ([Paan94]) kan het uitbesteden van het beheer van IT-voorzieningen (outsourcing) de kosten verminderen en tegelijkertijd de kwaliteit van de dienstverlening verbeteren. Deze voordelen kunnen met name gaan gelden als de service-provider concurreert met andere IT-dienstverleners. Een groot aantal organisaties is inmiddels tot outsourcing overgegaan.

In een typisch outsourcing-proces maken de service-provider en diens afnemer van tevoren afspraken over de kwaliteit van de dienstverlening. Het weinig tastbare begrip 'kwaliteit' wordt daarbij veelal opgesplitst in een aantal afzonderlijke kwaliteitsaspecten; bekende voorbeelden hiervan zijn responstijden, throughput-tijden en beschikbaarheidsintervallen. Deze en andere kwaliteitseisen worden doorgaans vastgelegd in een service level agreement, dat weer deel uitmaakt van een mantelovereenkomst tussen de service-provider en de afnemer.

Dit artikel richt zich op de kwaliteitseisen die samenhangen met het onderwerp informatiebeveiliging, welk begrip in dit artikel is gedefinieerd als het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatiesystemen tegen opzettelijke en onopzettelijke verstoringen ([Roos96]); deze specifieke kwaliteiteisen worden verder aangeduid als beveiligingseisen.

Ondanks het belang van informatiebeveiliging in outsourcing-trajecten is dit onderwerp in veel service level agreements een summier uitgewerkte paragraaf. In dit artikel wordt een eenvoudige maar structurele benadering voor dit probleem voorgesteld. De inhoud van het artikel is als volgt. Allereerst zal worden betoogd waarom het voor zowel de service-provider als voor diens afnemer lonend is om expliciete, duidelijke afspraken over informatiebeveiliging te maken. Daarna gaan de auteurs in op de basiseisen waaraan een beveiligingsovereenkomst tussen de service-provider en de afnemer dient te voldoen. Daarna wordt een structurele benadering om tot zo'n overeenkomst te komen, beschreven. Ten slotte wordt ingegaan op de praktische toepasbaarheid van deze benadering.

MOTIVATIE

De voordelen van een expliciete beveiligingsovereenkomst kunnen inzichtelijk worden gemaakt door eerst te kijken naar de voordelen vanuit het gezichtspunt van de service-provider. Deze is doorgaans onderworpen aan een contractuele verplichting om een van tevoren overeengekomen serviceniveau te bieden. Wat de afnemer betreft geldt deze verplichting te allen tijde, ook als de service-provider wordt geconfronteerd met opzettelijke of onopzettelijke acties die het naleven van het service level agreement kunnen belemmeren. Voor de service-provider is het treffen van adequate beveiligingsmaatregelen dus een noodzakelijke voorwaarde om het contractueel overeengekomen serviceniveau te kunnen waarborgen. Er is echter een tweede en wellicht belangrijker reden voor de service-provider om adequate beveiligingsmaatregelen te treffen: de afnemer *verwacht* eenvoudigweg dat de service-provider zich als een goed huisvader over de te beheren informatiesystemen ontfermt, aangezien deze systemen veelal bedrijfskritieke functies vervullen. In de outsourcing-markt is betrouwbaarheid inmiddels een kritieke succesfactor geworden – beveiligingsincidenten die moeten worden toegeschreven aan de onzorgvuldigheid van de service-provider zullen slechts weinig nieuwe klanten aantrekken. Informatiebeveiliging is daarmee een essentieel onderdeel van elke outsourcing-dienst.

De effectiviteit van de beveiligingsmaatregelen die de service-provider treft, blijkt echter in hoge mate afhankelijk te zijn van een relatief klein aantal activiteiten die volledig onder verantwoordelijkheid van de afnemer plaatsvinden; deze activiteiten variëren van het kiezen van sterke wachtwoorden tot het tijdig melden van beveiligingsincidenten. Informatiebeveiliging is hiermee een wederzijdse verantwoordelijkheid van de service-provider en de afnemer, hetgeen impliceert dat het maken van duidelijke afspraken op dit gebied noodzakelijk is. Tegelijkertijd biedt een dergelijke beveiligingsovereenkomst een redelijke basis voor het oplossen van verantwoordelijkheids- of zelfs aansprakelijkheidsvraagstukken die kunnen ontstaan nadat zich een beveiligingsincident heeft voorgedaan, in welk geval zowel de afnemer als de service-provider schade kan oplopen.

Informatiebeveiliging is een essentieel onderdeel van elke outsourcing-dienst.

Samenvattend kan derhalve worden gesteld dat een adequate informatiebeveiliging een integraal onderdeel van elke outsourcing-dienst hoort te zijn, zowel uit het oogpunt van risicomanagement als om te kunnen voldoen aan de verwachting van de klant; aangezien het een wederzijdse verantwoordelijkheid betreft, is het maken van duidelijke afspraken een noodzakelijke voorwaarde.

Het impliciete voordeel voor de afnemer is evident: de beveiliging wordt zichtbaar goed geregeld. In een aantal gevallen zullen de normen van de service-provider hoger blijken te liggen dan het oorspronkelijke beveiligingsniveau van de te beheren IT-omgeving vóór outsourcing, zodat outsourcing feitelijk een direct zichtbare verbetering van de beveiliging tot gevolg heeft.

BASISEISEN

De volgende stap is het inventariseren van de eisen waaraan een beveiligingsovereenkomst en de wijze waarop deze tot stand komt, dienen te voldoen. Onderstaande lijst is niet uitputtend.

Eis 1 – Formele specificatie van eisen en wederzijdse verantwoordelijkheden

Boven alles dient de beveiligingsovereenkomst een eenduidige specificatie van beveiligingseisen en wederzijdse verantwoordelijkheden te bevatten. De service-provider en de afnemer dienen eenvoudig uit de overeenkomst te kunnen afleiden welke partij verantwoordelijk is voor welke maatregelen.

Eis 2 – Helderheid

Een beveiligingsovereenkomst – alsmede de wijze waarop deze tot stand komt – dient voldoende helder te zijn om aan de eerste eis te kunnen voldoen. Eén aspect van de gewenste helderheid is het niveau van detail van de overeenkomst. Een overeenkomst die te abstract is, is ook dubbelzinnig, waardoor ruimte ontstaat voor interpretatieverschillen die doorgaans pas aan het licht komen als de naleving van de overeenkomst wordt getoetst. Maar als de overeenkomst te veel details bevat, zal zij snel als star en bureaucratisch terzijde worden geschoven.

Het bereiken van voldoende helderheid is een optimalisatieprobleem dat nog verder wordt gecompliceerd doordat beveiligingseisen van een andere aard zijn dan de kwaliteitseisen die we doorgaans in een service level agreement vinden. Deze kwaliteitseisen zijn in de regel goed te kwantificeren; voorbeelden zijn performance (kloksnelheid), opslagcapaciteit (gigabytes), bandbreedte (kilobits per seconde), responstijden (seconden) en beschikbaarheid (percentage); zulke eisen worden vaak verder uitgewerkt door ze voor specifieke intervallen te definiëren. Beveiligingseisen daarentegen zijn notoir moeilijk te kwantificeren en missen een algemeen geaccepteerd formalisme waarin zij kunnen worden uitgedrukt. Gelukkig kan deze problematiek in de praktijk worden omzeild door beveiligingseisen in operationele zin te specificeren, dat wil zeggen: in termen van te treffen beveiligingsmaatregelen.

Eis 3 – Volledigheid

Als beveiligingseisen niet in doelstellende, maar in operationele zin worden gedefinieerd, blijkt volledigheid een elementaire eis te zijn. Zo zal een beveiligingsovereenkomst niet alleen technische, maar ook organisatorische maatregelen dienen te bevatten, en wel alle organisatorische maatregelen die uit het oogpunt van risicomanagement noodzakelijk zijn. De volledigheidseis is een direct uitvloeisel van het 'negatieve' karakter van informatiebeveiliging; de kleinste omissie kan een informatiesysteem openstellen voor elke potentiële tegenstander. Het is geen geheim dat de vereiste volledigheid op gespannen voet staat met de evenzeer vereiste helderheid; ook hier blijkt dat het opstellen van een beveiligingsovereenkomst een niettriviaal optimalisatieprobleem is.

Eis 4 – Voldoen aan standaarden

De beveiligingsovereenkomst dient zoveel mogelijk te voldoen aan bestaande standaarden. Dit bevordert de doelmatigheid en biedt een steviger basis voor het wederzijds vertrouwen tussen de service-provider en de afnemer. Een standaard die zeker voor dit doel in aanmerking komt, is de Code voor Informatiebeveiliging ([NNI94]). Deze standaard is ontstaan in het Verenigd Koninkrijk en is in 1994 in Nederland uitgegeven door het Nederlands Normalisatie-Instituut, onder auspiciën van het Ministerie van Economische Zaken. De standaard is in het Verenigd Koninkrijk inmiddels uitgeroepen tot British Standard BS 7799 ([BSI95]). De Code definieert technische en organisatorische maatregelen, die zijn onderverdeeld in de volgende onderwerpen:

1. beveiligingsbeleid;
2. beveiligingsorganisatie;
3. classificatie en beheer van bedrijfsmiddelen;
4. beveiligingseisen ten aanzien van personeel;
5. fysieke beveiliging en beveiliging van de omgeving;
6. computer- en netwerkbeheer;
7. toegangsbeveiliging voor systemen;
8. ontwikkeling en onderhoud van systemen;
9. continuïteitsplanning;
10. toezicht.

In Engeland is BS 7799 gelanceerd met een omvangrijk publiciteitsoffensief; de acceptatiegraad blijkt echter per sector te verschillen. Volgens een recent onderzoek van KPMG in het Verenigd Koninkrijk heeft circa twee procent van de ondervraagde organisaties BS 7799 volledig geïmplementeerd en is circa elf procent hiermee bezig ([Baco96]). Ondanks deze volgens sommigen teleurstellende statistieken geldt de Code op dit moment als de breedst geaccepteerde standaard.

Eis 5 – Eenvoud

Een beveiligingsovereenkomst dient niet alleen helder, maar ook eenvoudig van opzet en uitwerking te zijn. De reden hiervoor is dat de overeenkomst zal worden gebruikt door functionarissen van wie geen specifieke beveiligingsdeskundigheid mag worden verwacht; de overeenkomst vormt immers een raakvlak tussen de service-provider en de afnemer en zal derhalve het pad kruisen van directeuren, managers, verkopers, account managers en juristen. Elk van deze partijen dient de essentie van de overeenkomst te kunnen begrijpen zonder zich in het vakgebied informatiebeveiliging te hoeven specialiseren.

Eis 6 – Differentiatie

Omdat verschillende informatiesystemen nu eenmaal verschillende beveiligingseisen kennen, dient elke beveiligingsovereenkomst 'op maat gesneden' te kunnen worden; het is algemeen geaccepteerd dat de bedrijfswaarde van een informatiesysteem de grondslag voor de gewenste differentiatie moet vormen.

De vereiste volledigheid staat op gespannen voet met de evenzeer vereiste helderheid.

Eis 7 – Keuzevrijheid

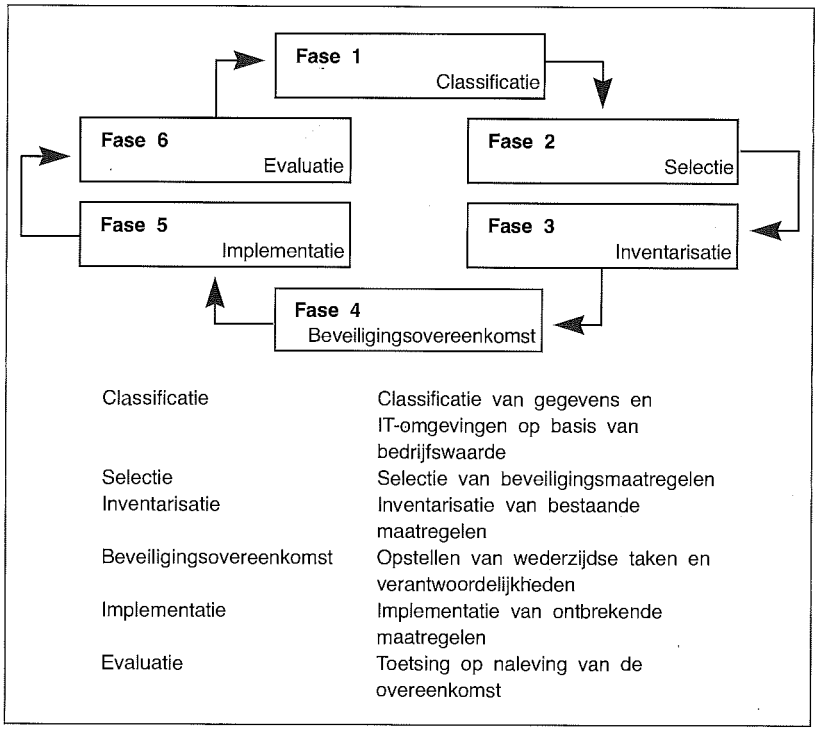
In elk outsourcing-traject moet de afnemer de vrijheid behouden om elke gewenste vorm van dienstverlening te kunnen kiezen. Een service-provider die zijn afnemer strikte eisen en beperkingen oplegt, zal zichzelf al snel uit de markt prijzen. Dit houdt ook in dat de afnemer vrij moet zijn om bepaalde beveiligingsmaatregelen niet te treffen; voorwaarde daarbij is dat deze keuze weer expliciet wordt vastgelegd.

Eis 8 – Flexibiliteit

Informatiebeveiliging wordt beïnvloed door vele externe factoren die voortdurend aan verandering onderhevig zijn. Voorbeelden hiervan zijn informatietechnologie, standaarden, wetgeving en het beveiligingsbeleid van de afnemer. Door de inherente dynamiek van deze factoren dient een beveiligingsovereenkomst regelmatig te worden herzien en voldoende flexibel te zijn, dat wil zeggen: open te staan voor uitbreiding of verandering.

Eis 9 – Onafhankelijke toetsing

Om het wederzijds vertrouwen te bevorderen, dient een onafhankelijke derde te beoordelen in welke mate de service-provider en de afnemer zich aan de afgesloten beveiligingsovereenkomst houden. Aangezien het zwaartepunt van deze toetsing doorgaans bij de naleving van de beveiligingsovereenkomst door de service-provider zal liggen, ligt het voor de hand dat de service-provider een third party review laat uitvoeren en een third party-mededeling laat afgeven inzake de kwaliteit van de



Figuur 1. De information security cycle.

beveiligingsmaatregelen die onder de verantwoordelijkheid van de service-provider vallen; zie ook [Velt95].

DE INFORMATION SECURITY CYCLE

Om aan bovengenoemde eisen te kunnen voldoen, presenteren wij een gestructureerde, eenvoudige cyclische benadering voor de interactie tussen de service-provider en de klant in een outsourcing-traject.

Deze benadering, de information security cycle, bestaat uit zes opeenvolgende stappen (zie figuur 1).

Deze fasen worden opeenvolgend doorlopen, waarbij er een nauwe samenwerking is tussen de service-provider en de afnemer. Omdat de beveiligingsovereenkomst van invloed zal zijn op het contract tussen beide partijen – met inbegrip van commerciële en financiële aspecten – dient de cyclus reeds tijdens het offertetraject te worden geïnitieerd. Als het offertetraject resulteert in een outsourcing-contract, dient de cyclus ten minste jaarlijks te worden doorlopen, of indien één van beide partijen dat noodzakelijk acht.

Navolgend worden de fasen van de information security cycle nader belicht.

Fase 1 – Classificatie

In de classificatiefase beoordeelt de afnemer de gevoeligheid van de te beheren IT-omgeving op grond van de waarde van de IT-omgeving voor de ondersteunde bedrijfsprocessen en de waarde van die processen. Hierbij houdt de afnemer rekening met de aspecten vertrouwelijkheid, integriteit en beschikbaarheid van de IT-omgeving en de applicaties en gegevens binnen die omgeving.

Er bestaan diverse methoden om zo'n classificatie uit te voeren, waarbij kan worden gekozen tussen top down en bottom up. Bij een top down-benadering begint de classificatie met een inventarisatie van bedrijfsprocessen en informatiesystemen. Bij de tegenovergestelde benadering, bottom up, dient de IT-omgeving zelf als basis voor de classificatie. Omdat de te beheren IT-omgeving in de regel redelijk in kaart is gebracht, verdient een bottom up-benadering de voorkeur. Hiertoe worden twee stappen uitgevoerd: allereerst inventariseert een classificatieteam de gegevens en applicaties binnen de IT-omgeving; daarna inventariseert het classificatieteam alle bedrijfsprocessen die de desbetreffende applicaties gebruiken.

Vervolgens wordt het relatieve belang van elk van deze bedrijfsprocessen ingeschat voor elk van de gehanteerde kwaliteitsaspecten (vertrouwelijkheid, integriteit, beschikbaarheid). De resulterende classificatie wordt vastgesteld volgens het 'high water mark'-principe: de belangrijkste gegevens en/of applicaties zijn bepalend voor de classificatie van de IT-omgeving als geheel.

Daarnaast wordt de IT-omgeving geclassificeerd op basis van de gevoeligheid voor negatieve publiciteit in geval van een beveiligingsincident.

Fase 2 – Selectie

In de selectiefase kiest de afnemer een verzameling beveiligingsmaatregelen uit een standaardcatalogus die is gebaseerd op de Code voor Informatiebeveiliging. De catalogus bevat twee categorieën beveiligingsmaatregelen: (a) basismaatregelen die de service-provider noodzakelijk acht om te kunnen voldoen aan de vereiste minimum-zorgplicht; deze maatregelen worden aangeduid als de information security baseline; en (b) aanvullende beveiligingsmaatregelen (information security services).

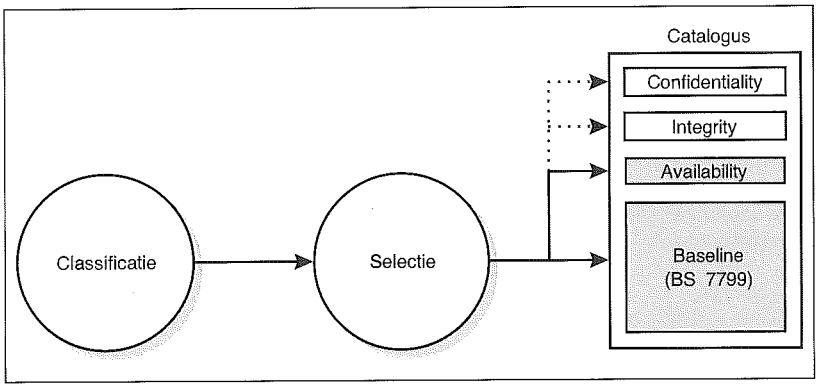
1. Basismaatregelen: de security baseline
In de vorige paragraaf is reeds betoogd dat de beveiligingsmaatregelen zoveel mogelijk dienen te zijn afgeleid van bestaande standaarden, met name de Code voor Informatiebeveiliging. De praktische toepasbaarheid van de Code kan eenvoudig worden verbeterd door de volgende maatregelen uit de Code te verwijderen:
- redundante maatregelen;
- maatregelen die gericht zijn op bijzondere omgevingen, zoals mainframe-omgevingen;
- maatregelen die het begrip 'minimum-zorgplicht' te boven gaan;
- applicatiespecifieke maatregelen;
- onnodige details.

Omwille van de toetsbaarheid dient elke wijziging zorgvuldig te worden gedocumenteerd en gemotiveerd. Het resultaat is een 'opgeschoonde' versie van de Code, waarbij de oorspronkelijke structuur,

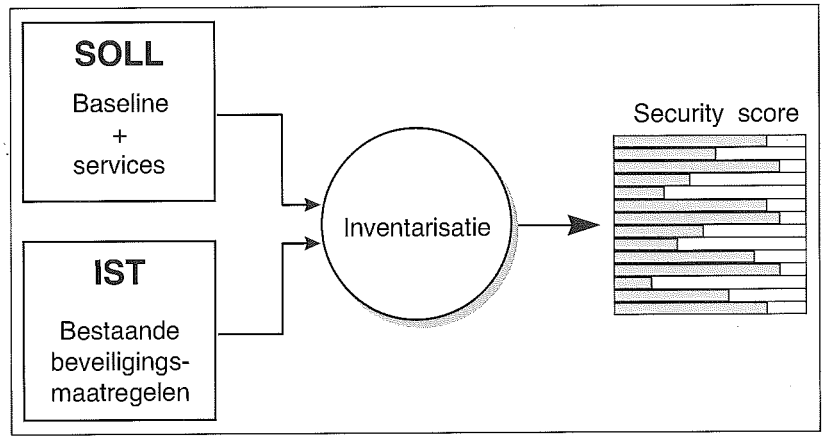
inhoud en geest van de standaard behouden zijn gebleven.
De resulterende baseline is verplicht – waarbij de vereiste keuzevrijheid vanzelfsprekend dient te worden gerespecteerd. Sommige maatregelen in de baseline vallen onder de verantwoordelijkheid van de afnemer (zoals het formuleren van een beveiligingsbeleid, het definiëren van eigenaren van alle informatiesystemen, het toekennen en intrekken van bevoegdheden van medewerkers en het kiezen van sterke wachtwoorden); sommige maatregelen vallen onder de verantwoordelijkheid van de service-provider (zoals het installeren van een centrale eenheid voor het melden van beveiligingsincidenten of het configureren van de logische toegangsbeveiliging tot de te beheren IT-omgevingen); en sommige maatregelen vallen onder beider – ongedeelde – verantwoordelijkheid (zoals het opnemen van beveiligingseisen in contracten met derden en het zorgvuldig omgaan met apparatuur en programmatuur).

2. Additionele beveiligingsdiensten
Vanzelfsprekend kan de afnemer beveiligingseisen stellen die de hierboven beschreven baseline te boven gaan. In dat geval dient de afnemer in staat te worden gesteld zijn maatregelen uit een additionele catalogus te selecteren. Zo een catalogus zou beveiligingsdiensten voor elk van de kwaliteitsaspecten vertrouwelijkheid, integriteit en beschikbaarheid kunnen definiëren; die diensten zouden dan geïmplementeerd kunnen worden door middel van tastbare maatregelen zoals encryptie, uitgebreide toegangsbeveiliging of zelfs TEMPEST-maatregelen.[1]

De selectie van basismaatregelen en aanvullende maatregelen dient plaats te vinden op basis van de classificatiefase (zie figuur 2).



Figuur 2. Van classificatie naar selectie.



Figuur 3. Inventarisatie van bestaande beveiligingsmaatregelen.

Fase 3 – Inventarisatie

Nadat een verzameling basismaatregelen en aanvullende maatregelen is geselecteerd, dienen de service-provider en de afnemer een initiële evaluatie uit te voeren om vast te stellen welke maatregelen reeds getroffen zijn. Deze audit dient binnen korte tijd afgerond te worden en dient een eerste indruk te geven van een eventuele beveiligingsachterstand. Om de doorlooptijd van deze fase te beperken, kan gebruik worden gemaakt van een geautomatiseerd tool.

Fase 4 – Beveiligingsovereenkomst

De service-provider en de afnemer komen formeel overeen welke maatregelen door wie dienen te worden getroffen. De resulterende beveiligingsovereenkomst staat op zichzelf en verwijst naar de corresponderende paragraaf in het algemene service level agreement en vice versa.

Het ligt voor de hand de beveiligingsovereenkomst te modelleren naar de security baseline, zodat voor elk van de maatregelen in de baseline een verantwoordelijke partij is gedefinieerd. Daarnaast maken de service-provider en de afnemer in de beveiligingsovereenkomst afspraken over de realisatie van aanvullende beveiligingsdiensten.

Fase 5 – Implementatie

In de implementatiefase implementeren de service-provider en de afnemer de overeengekomen maatregelen, voorzover die nog niet getroffen zijn. De implementatiefase dient volgens goede beginselen van projectmanagement te worden uitgevoerd; vóór implementatie dienen de service-provider en de afnemer ten minste afspraken te maken over de te implementeren maatregelen, de te volgen procedures en de voorwaarden voor acceptatie.

Fase 6 – Evaluatie

In de laatste fase toetst een onafhankelijke derde in hoeverre de service-provider en de afnemer zich aan de beveiligingsovereenkomst houden. Deze toetsing zal eventuele afwijkingen van de overeenkomst aan het licht brengen, en zo het wederzijds vertrouwen tussen de service-provider en de afnemer bevorderen. De toetsing dient periodiek te worden herhaald.

1. TEMPEST-maatregelen zijn de maatregelen die het afluisteren door meting van de elektromagnetische emissie van apparatuur (het zogenaamde Van Eck-effect) tegengaan.

H.R.D. Janus
Is Business Development Representative bij Communication Solutions Nederland te Leidschendam. Zijn aandachtsgebieden zijn cryptografie, informatiebeveiliging en marketing research.

G. Hulst CISA
Is Security Manager bij Communication Solutions Nederland te Leidschendam. Hij is verantwoordelijk voor de organisatie van informatiebeveiliging bij CSN en ondersteunt cliënten bij het uitvoeren van de Information Security Cycle. Hij is tevens lid van de projectgroep Internet van de afdeling Beveiliging van het NGI.

Ing. A. Shahim
Is consultant bij KPMG Management Consulting en houdt zich bezig met adviseering en projectmanagement op het gebied van informatiebeveiliging, cryptografie en systeemontwikkeling.

Dr. E. Roos Lindgreen
Is EDP-auditor bij KPMG EDP Auditors. Hij is gespecialiseerd in Corporate Information Security en de inrichting en beveiliging van moderne IT-omgevingen.

DISCUSSIE EN CONCLUSIES

De hierboven beschreven benadering is ingevoerd door Communication Solutions Nederland en wordt momenteel in de praktijk toegepast, ondersteund door standaardformulieren, geautomatiseerde tools, modelcontracten en uitgebreide beveiligingscatalogi. De information security cycle blijkt een goed uitgangspunt te zijn om het complexe aandachtsgebied informatiebeveiliging op een beheersbare wijze in de dagelijkse outsourcingpraktijk te kunnen aanpakken. Desondanks kan een aantal kritische opmerkingen worden geplaatst.

De classificatiefase dient met de nodige zorgvuldigheid te worden doorlopen. Omdat de classificatie is gebaseerd op het 'high water mark'-principe is het zeer wel denkbaar dat een relatief grote IT-omgeving als zeer gevoelig wordt geclassificeerd terwijl slechts een klein gedeelte van deze omgeving ook werkelijk zo gevoelig is. In dat geval kan de service-provider voorstellen de IT-omgeving in verschillende compartimenten op te delen; elk compartiment kan dan 'op maat' worden beveiligd. Een tweede risico is dat de classificatiefase tot intensieve en tijdrovende discussies kan leiden over details die ontegenzeggelijk zeer belangrijk zijn, maar in het bestek van de beveiligingsovereenkomst minder relevant zijn. Dit kan op zijn beurt de doorlooptijd van de cyclus weer verlengen, hetgeen de acceptatie ervan zal verlagen. Voor een efficiënte classificatie zijn ervaring en expertise twee noodzakelijke voorwaarden.

Een formele beveiligingsovereenkomst zal door sommige klanten zeer op prijs worden gesteld, maar door andere klanten als onnodig bureaucratisch worden ervaren. De geschetste benadering dient niet tot doel op zich te worden verheven; de service-provider zal zich moeten realiseren dat een goed contact en een open discussie met de afnemer vele malen belangrijker zullen zijn dan welke beveiligingsovereenkomst en third party-mededeling dan ook.

Een laatste punt van kritiek betreft de eenvoud van de geschetste benadering. Hiertegen zijn drie argumenten in te brengen. In de eerste plaats stellen de eisen 2 en 5 een bovengrens aan het detailniveau van een benadering die 'praktische toepasbaarheid' hoog in het vaandel heeft staan. In de tweede plaats is elke afnemer uniek, hetgeen de universele toepasbaarheid van een gedetailleerde benadering in de weg zal staan. In de derde plaats dient de benadering voldoende ruimte te bieden aan de snelle veranderingen in de huidige IT-omgevingen; elke verwijzing naar IT-specifieke maatregelen zal dit streven belemmeren.

Om de benadering goed in de praktijk te laten functioneren, dienen alle betrokken partijen te worden overtuigd van het belang en de toegevoegde waarde ervan. Dit is misschien wel de grootste uitdaging binnen het vakgebied informatiebeveiliging. Het is een algemene ervaring dat het beveiligingsbewustzijn – in het bijzonder op de hogere managementniveaus – wellicht effectiever kan worden gestimuleerd door te benadrukken dat informatiebeveiliging een normaal onderdeel van de bedrijfsvoering vormt én een toegevoegde waarde voor de klant heeft dan door het opdissen van griezelverhalen over hightech hackers en andere informatiecriminelen.

LITERATUUR

[Baco96] M. Bacon et. al., *National Computer Security Survey*, KPMG, 1996.

[BSI95] British Standards Institution, BS 7799 – *Code of practice for information security management*, BSI, 1995.

[NNI94] Nederlands Normalisatie-Instituut, *Code voor Informatiebeveiliging, een leidraad voor beleid en implementatie*, NNI/EZ, 1994.

[Paan94] R. Paans en M.H.E. Gianotten: *Data center management – getting order out of chaos*, The 1994 Report, Giarte Publishing, 1994.

[Roos96] E. Roos Lindgreen, *A Sense of Secureness – Approaches to information security*, Technische Universiteit Delft, Delft 1996.

[Velt95] P. Veltman, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact 95/3.

Methoden en technieken van logische toegangs-beveiliging

Drs.ing. E. Beijer

Logische toegangsbeveiliging kan op basis van kennis, op basis van bezit of op basis van zijn worden geïmplementeerd. Deze categorieën worden uitgelegd en geëvalueerd. Tevens worden de beheeraspecten besproken, die telkens specifieke aandachtspunten met zich meebrengen.

INLEIDING

Logische toegangsbeveiliging[1] is nog altijd een actueel onderwerp en zal dat ook in de toekomst blijven. Dit komt voornamelijk door de nog altijd verder gaande automatisering. Op dit moment worden bijvoorbeeld kredieten en hypotheken bij kredietverlenende instellingen nog afgesloten door contact met de cliënt, maar waarschijnlijk zal dit contact in de toekomst afbrokkelen en zullen krediet- en hypotheekautomaten (en misschien Internet) dit overnemen (rechtstreekse toetsing van de klant bij het BKR en automatisch vervaardigen en versturen van offertes en uiteindelijk op de juiste datum transfereren van het geld naar bijvoorbeeld de notaris). Het is dan goed te weten dat het systeem een zodanige beveiliging heeft dat in het gehele proces geen ongeautoriseerde acties kunnen plaatsvinden.

Vandaar dat in dit artikel de verschillende methoden en technieken zijn samengebracht, met als doel een evaluatie te geven van de technieken, welke resulteert in een uitspraak omtrent welke techniek c.q. technieken op dit moment de beste beveiliging biedt c.q. bieden.

Ook wordt in dit artikel aandacht besteed aan het beheeraspect rondom logische toegangsbeveiliging, omdat een techniek van logische toegangsbeveiliging nooit effectief kan worden ingevoerd als het beheer niet is ingevuld.

BESCHRIJVING

In de beschrijving van de verschillende vormen van logische toegangsbeveiliging wordt eerst een algemene beschrijving van de methode gegeven en vervolgens wordt per methode een aantal technieken uitgewerkt, waarbij wordt ingegaan op de identificatie en de authenticatie van de verschillende technieken (uitgewerkt in de te nemen stappen om te komen tot communicatie tussen het werkstation en de host).

Op basis van een indeling naar authenticatiemethoden komt in de eerste paragraaf de beveiliging aan de orde, waarbij de gebruiker iets moet onthouden om toegang tot een systeem te krijgen (bijvoorbeeld password of PIN-code). In de tweede paragraaf dient de gebruiker iets te bezitten om toegang te krijgen tot een systeem (bijvoorbeeld een token of smartcard) en in de derde en laatste paragraaf van deze beschrijving gebruikt de gebruiker iets persoonlijks om toegang te krijgen tot een systeem (bijvoorbeeld vingerafdruk of handtekening).

BEVEILIGING OP BASIS VAN KENNIS

Onder beveiliging *op basis van kennis* wordt in dit artikel verstaan dat de gebruiker zich dient te authenticeren op basis van onthouden informatie (bijvoorbeeld een password of PIN-code).
In deze paragraaf worden twee technieken van beveiliging *op basis van kennis* besproken, namelijk password en PIN-code.

Password

Bij de toegangsbeveiliging op basis van een password wordt een user-id gebruikt als identificatiemiddel en wordt een password gebruikt om de gebruiker te authenticeren.

De user-id is meestal samengesteld uit een achternaam aangevuld met eventuele voorletters. Ook is het mogelijk de user-id te laten bestaan uit andere gegevens (bijvoorbeeld het personeelsnummer). Het password is een door de gebruiker gekozen code, welke wordt gebruikt om de gebruiker toegang te verschaffen tot het systeem.

Het proces van inloggen van een gebruiker geschiedt, bij de beveiliging op basis van een password, als volgt:

1. bij gebruik van het systeem toetst de gebruiker op het werkstation zijn user-id en password in. Deze worden vervolgens naar de host gezonden alwaar deze gegevens worden gecontroleerd;
2. indien de gegevens juist zijn, logt het systeem de gebruiker in. Indien de gegevens onjuist zijn, zendt de host een afwijzingsbericht naar het werkstation.

De discipline van de gebruiker zal afnemen naarmate hij meer passwords dient te onthouden.

Het grote probleem bij het gebruik van passwords is de discipline van de gebruiker (een password dient niet eenvoudig te raden te zijn en toch gemakkelijk te onthouden, password mag niet verder verteld worden en mag niet opgeschreven worden). Deze discipline zal afnemen naarmate een gebruiker meer passwords dient te onthouden (gebruikers zullen de passwords o.a. gaan opschrijven en synchroniseren).

Om het bovenstaande probleem op te lossen worden in de literatuur vele maatregelen genoemd, zoals:

- passwords dienen frequent te worden gewijzigd;
- beperkt aantal toegangspogingen (meestal drie tot vijf), daarna blokkering van de user-id;
- check op eenvoudig te raden passwords;
- password-cyclus, waardoor men een aantal malen een nieuw password dient te verzinnen;
- password dient te bestaan uit een combinatie van letters en cijfers.

Er wordt echter veelal voorbijgegaan aan het feit dat deze maatregelen alleen de beheerders van het systeem helpen. De gebruikers zijn niet direct gebaat bij een periodieke password-wijziging en een password-cyclus. Het zou voor gebruikers juist makkelijker zijn, en beveiligingstechnisch gezien misschien ook beter, als passwords niet verplicht frequent hoeven te worden gewijzigd, maar bijvoorbeeld 'slechts' eens per jaar of misschien wel helemaal nooit.

Immers, als gebruikers minder frequent een password hoeven te wijzigen bestaat een grotere kans dat gebruikers echt gaan nadenken over hun te kiezen password. Voorwaarde is dan wel dat men gebruikers handvatten geeft om goede passwords te kunnen kiezen. Verder dienen de gebruikers bewust te worden gemaakt van de risico's indien het password bekend raakt en van de verantwoordelijkheden die de gebruiker heeft bij het gebruik van een combinatie van user-id en password.

Ook het gebruik van een password-cyclus lost bovenstaande probleem niet op. Gebruikers die nu minder goede (lees: makkelijk raadbare) passwords gebruiken zullen dat gedrag immers niet veranderen als ze een password frequent dienen te wijzigen. Sterker nog, de kans bestaat dat, indien het systeem een password-cyclus heeft, een groot aantal gebruikers hun password met behulp van een volgnummer uniek houden (bijvoorbeeld linda1, linda2, linda3, etc.).

In bovenstaande beschrijving is alleen uitgegaan van een combinatie van user-id/password, maar in de loop van de tijd zijn allerlei varianten bedacht. Onderstaand volgen enkele van deze varianten.

Combinatie user-id/wiskundige formule
Hierbij is zowel bij de host als bij de gebruiker een 'wiskundige' formule bekend (bijvoorbeeld $z = 5x + 4y + 10$). De computer genereert vervolgens twee getallen (bijvoorbeeld 6 en 4, respectievelijk x en y) en de gebruiker dient de uitkomst (56) als authenticatie in te geven. (Identificatie gebeurt overigens op basis van een user-id.) Zowel door de gebruiker als door de host wordt deze berekening gemaakt. De uitkomst welke de gebruiker intoetst wordt naar de host gezonden, en de host vergelijkt deze uitkomst met de zelf berekende uitkomst. Indien deze overeenkomen logt het systeem de gebruiker in.

Combinatie user-id/persoonlijk gegeven
Hierbij wordt als password een persoonlijk gegeven van de gebruiker gekozen. De gebruiker dient bijvoorbeeld tien persoonlijke gegevens in te voeren (bijvoorbeeld woonplaats, trouwdatum en naam van de kinderen). Telkens bij het inloggen wordt gevraagd om één van deze gegevens in te voeren. Een verdere verfijning is om in plaats van naar het hele gegeven te vragen, te vragen naar een bepaalde letter van een bepaald persoonlijk gegeven (bijvoorbeeld wat is de derde letter van de voornaam van uw echtgenote).

1. Onder logische toegangsbeveiliging wordt verstaan een geprogrammeerde maatregel welke tot doel heeft data, programmatuur en resources te beschermen tegen ongeautoriseerde acties (waarbij onder acties wordt verstaan: raadplegen, muteren en gebruik).

Combinatie user-id/eenmalig password
Hierbij kan worden gedacht aan twee varianten:

1. De gebruiker heeft een lange lijst met passwords. Iedere keer dat hij zich moet authenticeren, gebruikt hij het volgende password van een lijst en streept dit af. Een password wordt dus maar één keer gebruikt. De gebruiker dient de passwords precies in die volgorde te gebruiken als ze op de lijst staan. De telebankiertoepassing Girotel maakt gebruik van deze methode.

2. Voor kritieke toepassingen is een password slechts éénmaal geldig. Bij het inloggen in het systeem dient het password iedere keer te worden gewijzigd.

Voor beide varianten geldt echter dat het voor een gebruiker ondoenlijk is om de passwords te onthouden en er dus een grotere kans bestaat dat de gebruiker de passwords gaat opschrijven. (Bij Girotel wordt een lijst met passwords uitgereikt; hierdoor kan deze techniek ook worden gezien als een vorm van logische toegangsbeveiliging *op basis van bezit*.)

PIN-code

Bij de toegangsbeveiliging op basis van een PIN-code wordt een magneetstripkaart gebruikt als identificatiemiddel en wordt een PIN-code gebruikt om de gebruiker te authenticeren.

De pas bevat meestal de volgende informatie:
- naam van de houder;
- expiratiedatum;
- rekeningnummer;
- pasnummer;
- en een magneetstrip, waarin dezelfde gegevens als op de kaart vermeld staan, zijn opgeslagen.

Een PIN (Persoonlijk Identificatie Nummer) is eigenlijk niets anders dan een soort password; het is een geheim nummer uitgegeven aan een individu. Dit nummer kan gebruikt worden voor authenticatiedoeleinden. PIN's worden algemeen gebruikt door financiële instellingen als een manier om hun cliënten te verifiëren als zij een financiële transactie willen uitvoeren (bij een geld- of betaalautomaat).

Het proces van uitvoeren van een transactie door een gebruiker geschiedt, bij de beveiliging op basis van een PIN-code, als volgt:
1. een cliënt steekt zijn pas in een uitleesapparaat (identificatie) en toetst vervolgens zijn PIN-code in via een PIN-pad (authenticatie);
2. vervolgens verzendt het uitleesapparaat de gegevens (pasgegevens en PIN-code) naar de host;
3. de host verifieert de gegevens; indien deze juist zijn (= juiste PIN-code bij de gelezen pasgegevens) wordt de gebruiker ingelogd;
4. vervolgens kiest de gebruiker het over te boeken c.q. uit te keren bedrag. Daarna stuurt het uitleesapparaat deze gegevens naar de host;
5. de host (die de gegevens controleert op voldoende saldo) stuurt vervolgens een bevestiging (in de vorm van een akkoordbevinding of geld) of afwijzing (in de vorm van een bericht) en zal ten slotte de verbinding verbreken.

BEVEILIGING OP BASIS VAN BEZIT

Onder beveiliging *op basis van bezit* wordt in dit artikel verstaan het in bezit hebben van een of ander apparaatje, dat geheel (of deels[2]) zorgt voor de authenticatie van de gebruiker.

Als wordt gekeken naar de beschikbare technieken van logische toegangsbeveiliging *op basis van bezit*, dan komen twee soorten apparaatjes hiervoor in aanmerking. Dit zijn het token en de smartcard.

In de literatuur wordt een token meestal geassocieerd met een rekenmachine-achtig apparaatje. Dit wordt dan gebruikt bij het authenticatieproces.

Een smartcard is een apparaatje dat een chip bevat waarop allerlei gegevens kunnen zijn opgeslagen. De authenticatiegegevens kunnen onderdeel zijn van deze gegevens.

In deze paragraaf worden twee soorten technieken van beveiliging *op basis van bezit* besproken, namelijk het token en de smartcard.

Token

Een token is meestal een klein, vaak rekenmachine-achtig apparaatje voor toegangsbeheersing. Dit wordt gebruikt voor het berekenen van een respons op een gegenereerde challenge (uitdaging), dan wel wordt het gebruikt als onderdeel voor een te berekenen respons. Het voordeel van het gebruik van een token boven de smartcard (en ook magneetstripkaart) is dat er geen kaartlezer nodig is. Wel krijgt het computersysteem er een stuk software bij en iedere gebruiker zijn eigen persoonlijke token.

Er zijn twee soorten tokencombinaties te onderscheiden, namelijk token/hardware (hierna: hard token) en token/software (hierna: soft token).

Het verschil tussen beide is dat bij het hard token de berekening van de respons in het apparaatje plaatsvindt, terwijl deze bij het soft token door de op het werkstation geïnstalleerde software plaatsvindt.

Beide vormen worden hierna besproken.

Hard token
Bij het gebruik van het hard token dient de gebruiker de challenge, welke door de host wordt gegenereerd, in het token in te voeren. Het token berekent vervolgens de respons die de gebruiker op het werkstation dient in te voeren.

Het 'geheim' op basis waarvan authenticatie plaatsvindt, zit in het token.

2. Deels, omdat het nogal eens voorkomt dat een respons wordt samengesteld op basis van het in het token invoeren van een challenge en een door de gebruiker ingevoerde PIN-code (in het token zelf of in de software op de werkplek). Hierdoor is dus geen sprake meer van een 'zuivere' vorm van beveiliging op basis van bezit, maar is een 'mengvorm' gecreëerd tussen beveiliging op basis van kennis en op basis van bezit.

Het proces van inloggen van een gebruiker geschiedt, bij het hard token, als volgt:

1. op een inlog-verzoek van een gebruiker genereert de host een challenge en stuurt deze naar het beeldscherm van de gebruiker (werkstation);
2. de gebruiker activeert het token door het invoeren van een PIN-code en voert vervolgens de challenge in op het token. Deze genereert de respons;
3. de gebruiker voert deze respons in op het werkstation. Op hetzelfde moment berekent ook de host de verwachte respons;
4. authenticatie vindt plaats doordat beide partijen (werkstation/host) met elkaar kunnen communiceren (de respons wordt gebruikt voor het in stand houden van de verbinding). Dit geschiedt door het versluieren (met de respons) van verschillende over te zenden, bij beide partijen (host en werkstation) bekende, gegevens. Na ontsluiering van de gegevens, door de host, komen er controleerbare gegevens uit. Indien deze gegevens juist zijn, is de verbinding tot stand gebracht en de gebruiker ingelogd.

Het token heeft boven de smartcard het voordeel dat er geen kaartlezer nodig is.

Om het inbrengen van de challenge in het token te vereenvoudigen, zijn er ook tokens die de challenge zelf van het beeldscherm kunnen lezen. Het token is dan voorzien van lichtgevoelige cellen, die de cijfers van het beeldscherm kunnen lezen.

Soft token

In tegenstelling tot bij het hard token hoeft de gebruiker bij het gebruik van een soft token niets op het token in te voeren. Op het moment dat een gebruiker van een dienst gebruik wil maken, geeft het token een code aan. Deze code wordt zowel bij de host als in het token berekend; dit gebeurt op basis van tijdslots (van dertig of zestig seconden).

Het 'geheim' op basis waarvan authenticatie plaatsvindt, zit slechts gedeeltelijk in het token en voornamelijk in de software.

Het proces van inloggen van een gebruiker geschiedt, bij het soft token, als volgt:

1. indien een gebruiker wil inloggen, dient hij zich bekend te maken met zijn user-id en dient hij zijn PIN-code en de code welke het token heeft gegenereerd, in te voeren (PIN-code + tokencode = passcode);
2. vervolgens genereert het werkstation, op basis van de tijd en de ingevoerde passcode een 256 bit code. Alvorens deze verstuurd wordt, wordt deze opgedeeld in vier 64 bit Workstation Passcode (WP) delen;
3. de eerste WP wordt samen met de gebruikersnaam naar de host gezonden;
4. met de gebruikersnaam haalt de host de sleutel (die zich in het token van de gebruiker bevindt), de PIN-code en de statistiek over de klok (stabiliteit of uit de pas lopen) uit de database;
5. de host berekent onder gebruikmaking van de huidige tijd (vastgesteld op basis van de huidige tijd en de uit de database verkregen statistieken) en de sleutel voor het gebruikte token, de verwachte respons van het gebruikte token in het huidige tijdslot (30/60-seconden). Omdat de tijd een belangrijke rol speelt bij het voorspellen van de door het token gegeven respons, worden door de host voor de zekerheid ook de voorgaande en de volgende respons (dus voor het voorgaand en volgend tijdslot) gegenereerd;
6. op basis van bovenstaande genereert de host vervolgens drie 256 bit codes;
7. daarop aansluitend wordt bekeken of het begin (64 bit WP) van één van de drie overeenstemt met de door het werkstation verzonden 64 bit WP. Als dit zo is, stuurt de host een bericht naar het werkstation waarin staat dat de gebruiker is geauthenticeerd. Vervolgens wordt de gebruiker ingelogd. Indien de host via berekening geen overeenkomst met de gestuurde WP kan vinden, wordt een afwijzing naar het werkstation gestuurd.

Er is ook een token beschikbaar dat de respons in het token zelf berekent. Dit betekent dat op het werkstation het algoritme en de sleutel niet meer aanwezig zijn. Het enige wat de gebruiker op het token (dat weer is voorzien van een toetsenbordje) hoeft in te voeren, is de PIN-code. Het token berekent vervolgens op basis van de tijd het tokencode. Met behulp van de PIN-code en de sleutel wordt deze omgevormd tot de af te geven respons.

Smartcard

Een smartcard is een computer met een vast programma op een kaartje, dat even groot is als een magneetstripkaart. Op een smartcard kunnen allerlei gegevens worden bewaard. Omdat het programma van de smartcard alle gegevens op de kaart beschermt, kunnen ook vertrouwelijke gegevens en zelfs geld in elektronische vorm worden opgeslagen.

Identificatie en authenticatie kunnen met behulp van een smartcard plaatsvinden *op basis van bezit*. Het is evenwel mogelijk dat, net als bij de magneetstripkaart, de smartcard ook van een PIN-code is voorzien.

Het gebruik van smartcards vraagt per werkplek een smartcard-lezer en een stukje software. Voor het aanmaken van smartcards, het zogenaamde personaliseren, is speciale apparatuur en software nodig.

Het grote verschil van een smartcard ten opzichte van een magneetstripkaart is dat een smartcard allerlei berekeningen zelfstandig kan uitvoeren en een grote opslagcapaciteit heeft. Hierdoor kan een smartcard voor meerdere toepassingen worden ingezet.

In deze subparagraaf worden twee verschillende smartcards besproken. Dat zijn de semi-anonieme smartcard en de persoonlijke smartcard.

Semi-anonieme smartcard
De semi-anonieme smartcard is een smartcard die, na te zijn gebruikt, door het (financieel) opwaarderen van de kaart opnieuw te gebruiken is. Hierbij is het gebruik anoniem en het opwaarderen persoonlijk.

Indien een gebruiker een semi-anonieme smartcard in bezit heeft, kan hij hiermee de volgende functies uitvoeren:

Opwaarderen
Alvorens de smartcard kan worden gebruikt, dient deze door de gebruiker te worden opgewaardeerd. Daartoe gaat de gebruiker naar een geldautomaat (in de nabije toekomst zal het opwaarderen in de telefooncel en via het telefoontoestel tot de mogelijkheden gaan behoren) en stopt (net als met de magneetstripkaart) de smartcard in het afleesgedeelte van het apparaat. Vervolgens dient de gebruiker de PIN-code in te voeren (waardoor de gebruiker toegang krijgt tot zijn rekeningnummer) en geeft vervolgens het bedrag aan, dat hij op de smartcard wil hebben bijgeschreven. Het systeem maakt daarna een opwaardeerinstructie aan. Deze wordt door de smartcard gecontroleerd en verwerkt. Het systeem zorgt tot slot voor de juiste afhandeling van de opwaardering naar de float (een soort tussenrekening) en afboeking van de rekening van de gebruiker.

Betalen
De betaling (nu alleen nog in de winkel, maar in de (nabije) toekomst multifunctioneel (dan o.a. ook in telefooncellen, parkeermeters en openbaar vervoer (strippenkaarten)) geschiedt conform de werkwijze met de PIN-betaling. Er hoeft echter geen PIN-code te worden ingevoerd. Wel dient de gebruiker het bedrag van een betaling expliciet goed te keuren. De gebruiker krijgt zowel voor als na de betaling het resterende saldo te zien (overigens is 'rood' staan niet mogelijk).

Het doen van een betaling met behulp van een semi-anonieme smartcard resulteert in een logfile met (veel) cijfers. Deze ontstaan doordat elementen van alle drie de betrokken partijen (gebruiker, bank en winkelier) worden 'gemengd' in de vastgelegde transactiegegevens in de terminal. Het aanpassen van de cijfers, toevoegen van cijfers en het nogmaals aanbieden van de transacties leidt tot weigering bij de verwerking. De terminals worden dan ook leeggezogen via een normale telefoonlijn, zonder verdere specifieke maatregelen.

Hier is alleen de betaalfunctie van de semi-anonieme smartcard besproken. In de nabije toekomst zal de semi-anonieme smartcard ook gebruikt gaan worden voor andere doeleinden zoals bijvoorbeeld spaarsystemen (waaronder zegels en kortingen), toegangsbeveiliging tot gebouwen en als identiteitsbewijs.

Persoonlijke smartcard
Het grote verschil van deze kaart vergeleken met de semi-anonieme smartcard is, dat voor het gebruik van deze kaart altijd een PIN-code benodigd is. Dit betekent dat met behulp van deze PIN-code dus de authenticiteit van de gebruiker wel wordt vastgesteld.

Dit soort smartcards wordt gebruikt in omgevingen die extra eisen stellen aan beveiliging (o.a. homebanking en SWIFT).

Een smartcard kan allerlei berekeningen zelfstandig uitvoeren.

Het proces van inloggen van een gebruiker geschiedt, bij de persoonlijke smartcard, als volgt:
1. de gebruiker stopt de smartcard in een uitleesapparaat. Vervolgens dient de gebruiker een PIN-code in te voeren. Deze PIN-code wordt door de smartcard zelf geverifieerd;
2. indien de PIN-code juist is, wordt een connectie met de host opgebouwd. Hierbij stuurt de smartcard de identificatiegegevens over naar de host. De host stuurt vervolgens een challenge naar de smartcard. Deze antwoordt vervolgens met een respons. Deze respons wordt door de host vergeleken en indien deze juist is, wordt de gebruiker ingelogd.

Per sessie wordt (door de smartcard) een unieke sleutel gegenereerd. Deze wordt samen met de identificatiegegevens naar de host gestuurd. Indien de host de smartcard (lees: het werkstation of de gebruiker) authenticeert, wordt deze sleutel de gehele sessie gebruikt om het gegevensverkeer tussen de host en het werkstation te versluieren.

BEVEILIGING OP BASIS VAN ZIJN

Onder beveiliging *op basis van zijn* (biometrische kenmerken) wordt in dit artikel verstaan dat de authenticatie van een gebruiker plaatsvindt op basis van een persoonlijk kenmerk (bijvoorbeeld vingerafdruk of handschrift).

Alhoewel er reeds verschillende leveranciers zijn, die producten aanbieden op het gebied van toegangsbeveiliging *op basis van zijn*, is het momenteel voor de leveranciers nog een uitdaging om een techniek te ontwikkelen die in hoge mate accuraat is én door gebruikers wordt geaccepteerd (bijvoorbeeld retinaherkenning (= iriscopie) is honderd procent accuraat, maar stuit op weerstand bij de gebruikers).

In het navolgende wordt een algemene beschrijving van de techniek van beveiliging *op basis van zijn* gegeven.

Biometrische kenmerken

Identificatie en authenticatie zijn in de dagelijkse omgang tussen mensen nooit een probleem. Je herkent iemand aan zijn stem, zijn gezicht of zijn handschrift. Dat is veel eenvoudiger dan de technieken die hiervoor zijn genoemd, die allemaal fraudegevoelig zijn in de zin dat de gebruiker zijn kaart en geheime code kan verliezen door onachtzaamheid of afpersing.

Er zijn ook methoden voor toegangsbeveiliging, die zich richten op persoonlijke kenmerken. De authenticatie[3] is gebaseerd op 'iets wat men is', de zogenaamde biometrische eigenschappen. Een aantal voorbeelden van biometrische eigenschappen die kunnen worden gebruikt voor authenticatie is:

Vingerafdrukken
De gebruiker plaatst een vingerafdruk op een speciaal oppervlak en deze wordt vergeleken met een opgeslagen versie van de vingerafdruk. Als deze identiek zijn is de gebruiker geauthenticeerd. Een variant op het gebruik van vingerafdrukken is het gebruik van de aders in de hand of een driedimensionale afbeelding van de hele handpalm.

Patroon van het netvlies (retinaherkenning)
Deze vorm werkt identiek aan vingerafdrukken, alleen dient een gebruiker nu in een apparaat te kijken.

Gezichtsherkenning
De gebruiker moet plaatsnemen voor een camera welke een opname maakt van het gezicht en deze vergelijkt met een in het systeem opgeslagen foto.

Dynamische handtekening
De gebruiker moet een handtekening zetten op een speciaal oppervlak waarbij niet alleen de uiteindelijke vorm van de handtekening wordt gecontroleerd, maar ook hoe hard de gebruiker op de pen drukt en hoe snel hij zijn pen beweegt tijdens het zetten van de handtekening.

Stemgeluid
De gebruiker moet een standaardzin uitspreken. Deze wordt vergeleken met een opgeslagen versie van zijn stem.

Patronen van toetsenbordgebruik
De gebruiker wordt gevraagd om een zin te typen en op basis van de tijd tussen verschillende toetsaanslagen wordt hij geauthenticeerd.

Er bestaan ook ideeën om DNA te gebruiken voor toegangsbeheersing. DNA is drager van erfelijke kenmerken in de lichaamscellen. De verwachting is echter dat dit op behoorlijke weerstand bij de gebruikers zal stuiten.

Het voordeel van het gebruik van aan de persoon gebonden kenmerken is duidelijk: de gebruiker heeft geen geheim dat hij kan verliezen (onder de aanname dat vingerafdrukken niet met bijbehorende vinger gestolen worden).

3. In dit artikel is bij iedere techniek gesproken over de scheiding van identificatie en authenticatie. Bij deze techniek is deze scheiding echter niet aanwezig en zijn identificatie en authenticatie verenigd in het authenticatiemiddel.

Zoals blijkt uit bovenstaande voorbeelden is voor het gebruik van biometrische kenmerken speciale invoerapparatuur vereist: een scanner voor de handtekening (eventueel met pendrukmeting), een apparaat om de stem te digitaliseren, of een camera voor het registreren van het gezicht of het registreren van het oogpatroon. Daarnaast is geavanceerde software nodig voor patroonherkenning. Het systeem moet bovendien de gedigitaliseerde persoonlijke kenmerken registreren. Dit maakt deze techniek van logische toegangsbeveiliging duurder dan de andere besproken technieken.

Na digitalisering in het invoerapparaat ontstaat een vaste biometrische code. Deze biometrische code vertegenwoordigt de persoon en is even kwetsbaar voor afluisteren als een password. Een afgeluisterde biometrische code zou wellicht buiten het invoerapparaat om ingevoerd kunnen worden. Waardoor ook authenticatie met biometrische codes beveiliging vereist van de communicatie en de database.

Het proces van inloggen van een gebruiker geschiedt, bij beveiliging op basis van een biometrisch kenmerk, als volgt:
1. indien een gebruiker toegang wenst tot een bepaald systeem, dient hij een leesapparaat te activeren. Vervolgens leest het apparaat het persoonlijke kenmerk en zet dit om in voor de computer leesbare taal (digitaliseren). Deze gegevens worden naar de host gezonden;
2. de host vergelijkt de aangeboden gegevens met de, in de database, aanwezige gegevens. Indien deze overeenkomen wordt de gebruiker ingelogd.

BEHEER

Zoals reeds eerder gezegd kan logische toegangsbeveiliging niet effectief worden ingevoerd als ook niet het beheeraspect wordt ingevuld.

Vandaar dat in de volgende paragrafen een beschrijving wordt gegeven van de verschillende organisatorische maatregelen waaraan aandacht dient te worden besteed om een techniek voor toegangsbeveiliging effectief te maken. Deze beschrijving geschiedt aan de hand van procedures, welke een organisatie in het kader van een techniek van logische toegangsbeveiliging minimaal dient te vervaardigen.

Deze paragrafen geven aan welke procedure waarom dient te worden vervaardigd en sommen tevens de aspecten op die in een bepaalde procedure beschreven dienen te worden.

BEVEILIGING OP BASIS VAN KENNIS

Password en PIN-code zijn uitgangspunten voor de beschrijving van beveiliging op basis van kennis.

Password

De beveiliging van passwords richt zich onder andere op de uitgifte en intrekking van user-id's, de vormvereisten voor en het gebruik van passwords en de registratie van rechten.

Uitgifte user-id's
Om het identificatieproces mogelijk te maken, dienen gebruikers bekend te zijn in het systeem. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- hoe maakt een gebruiker kenbaar dat hij gebruik wil maken van een bepaald systeem (bijvoorbeeld aanvraagformulier);
- welke gegevens dienen op een aanvraagformulier te worden ingevuld, bijvoorbeeld paraaf chef gebruiker (om aan te geven dat de gebruiker uit hoofde van zijn functie inderdaad een user-id nodig heeft) en paraaf security administrator[4] (die zorg draagt dat de gebruiker in het systeem wordt ingevoerd);
- door wie en hoe een user-id in het systeem wordt ingevoerd;
- waar, hoe (bijvoorbeeld alfabetisch) en hoe lang (bijvoorbeeld tot drie maanden na intrekking van de bevoegdheden) deze aanvraagformulieren worden bewaard.

Intrekken van user-id's
Omdat gebruikers de organisatie verlaten of van functie veranderen, dienen gebruikers uit het systeem te worden verwijderd. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- wanneer en hoe wordt een user-id afgemeld (bijvoorbeeld in verband met pensioen, andere werkgever of andere functie binnen hetzelfde bedrijf (waarbij geen gebruik van het systeem behoeft te worden gemaakt));
- wie is verantwoordelijk voor het intrekken van user-id's (bijvoorbeeld chef of security administrator, indien gedurende een langere periode geen gebruik van een user-id wordt gemaakt);
- door wie en hoe wordt een user-id uit het systeem verwijderd;
- waar, hoe en hoe lang dient dit in de administratie te worden vastgelegd (bijvoorbeeld afmeldingsformulier).

Uitgifte passwords
Om het authenticatieproces mogelijk te maken, dient het password bekend te zijn in het systeem. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe wordt het initiële password in het systeem kenbaar gemaakt. Indien het initiële password is gezet, dient het systeem af te dwingen dat, als de gebruiker voor de eerste maal aanlogt, deze direct het initiële password wijzigt. Met andere woorden, het initiële password mag slechts één keer worden gebruikt, namelijk bij de eerste maal aanloggen;
- door wie en hoe wordt het password aan de gebruiker kenbaar gemaakt.

Vergeten/geblokkeerd password
Een password dat door de gebruiker is vergeten of door te veel onjuiste aanlogpogingen is geblokkeerd, dient te worden gereset. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe wordt een verzoek voor het resetten van een password geaccepteerd (bijvoorbeeld een security administrator op grond van een ingevuld (voorzien van juiste handtekeningen) reset-formulier);
- door wie en hoe wordt een reset-verzoek uitgevoerd;
- waar, hoe en hoe lang wordt een reset-verzoek in de administratie vastgelegd.

Het systeem dient af te dwingen dat de gebruiker bij de eerste maal aanloggen direct het initiële password wijzigt.

Password-parameters
Om het gebruik van passwords 'veiliger' te maken, kunnen allerlei parameters worden gezet en onderhouden. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe worden password-parameters gezet;
- waar, hoe en hoe lang wordt een wijziging van een parameter vastgelegd.

Opslag password
Passwords dienen zodanig te worden opgeslagen dat deze voor niemand leesbaar zijn. Dit kan men doen door de rechten op een zodanige wijze te zetten dat niemand de passwords kan lezen of door een versleutelingsmechanisme toe te passen zodat niemand de passwords kan achterhalen.

Uitgifte van rechten
Om het autorisatieproces mogelijk te maken, dienen de rechten van een gebruiker bekend te zijn in het systeem. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- hoe maakt een gebruiker kenbaar welke rechten hij dient te hebben in een bepaald systeem (bijvoorbeeld aanvraagformulier);
- welke gegevens zijn op het aanvraagformulier ingevuld;
- door wie en hoe worden rechten in het systeem ingevoerd;
- waar, hoe (bijvoorbeeld alfabetisch) en hoe lang (bijvoorbeeld tot drie maanden na intrekking van de bevoegdheden) worden deze aanvraagformulieren bewaard.

Mutatie van rechten
Omdat gebruikers binnen een organisatie van functie kunnen veranderen, dienen rechten van gebruikers in het systeem te worden gewijzigd c.q. te worden verwijderd. In een procedure die dit regelt, dient het volgende beschreven te zijn:

4. *In dit artikel wordt een security administrator gedefinieerd als degene die gebruikers en bijbehorende rechten in een bepaald systeem invoert en onderhoudt.*

- wanneer worden rechten van een gebruiker gewijzigd; bijvoorbeeld in verband met andere functie binnen hetzelfde bedrijf;
- door wie en hoe worden mutaties uitgevoerd;
- waar, hoe en hoe lang worden de mutaties in de administratie vastgelegd (bijvoorbeeld afmeldingsformulier).

Intrekken van rechten
Verondersteld wordt dat de rechten van een bepaalde gebruiker uit het systeem verdwijnen als de user-id van een bepaalde gebruiker wordt ingetrokken (zodat hiervoor geen aparte procedure hoeft te worden opgesteld).

Rapportageparameters
Indien het systeem ook nog rapportagemogelijkheden kent, dient hiervoor een procedure te worden vervaardigd. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie, hoe en met welk doel worden de rapportagemogelijkheden (met andere woorden, wat wordt gerapporteerd en waarom) aan- en uitgezet;
- voor wie zijn deze rapportages bestemd;
- hoe, waar en hoe lang worden deze rapportages bewaard.

Toegang database
Daar niet iedereen toegang zal hebben tot de gebruikersdatabase is het raadzaam een procedure op te stellen, die de toegang tot de database regelt. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- welke functionaris (in dit artikel wordt uitgegaan van een security administrator) heeft toegang tot de database;
- welke werkzaamheden worden door deze functionaris uitgevoerd.

Vervanging security administrator
Deze procedure regelt de vervanging indien de security administrator zijn password vergeet of niet aanwezig is. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- wat houdt de backup in;
- waar kan deze worden gevonden;
- wanneer en door wie mag deze worden aangesproken;
- welke werkzaamheden mag de vervanger uitvoeren.

PIN-code

De aanmaak van passen vindt meestal plaats bij een derde. In dit artikel worden de verschillende procedures die op deze techniek betrekking hebben, besproken.

In het geval dat de te bespreken procedures door een derde worden uitgevoerd, dient een organisatie zich ervan te overtuigen, dat de daar gevolgde procedures voldoende waarborgen bieden dat de pas en PIN-code 'veilig' bij de gebruiker aankomen. Er dient onder meer voor gezorgd te worden dat:
- het aanmaken van de passen en het aanmaken van PIN-codes gescheiden wordt uitgevoerd (anders is binnen de organisatie bekend welke PIN-code bij welke pas behoort. Dit mag alleen de gebruiker weten);
- er tussen het versturen van de pas en de PIN-code enkele dagen vertraging zit (in geval van diefstal heeft de dief alleen de pas of alleen de PIN-code);
- dat de passen en PIN-codes op een zodanige wijze verzonden worden dat het niet duidelijk is van welke organisatie deze passen en PIN-codes afkomstig is.

De onderneming die passen en PIN-codes vervaardigt, zal de organisatie op de hoogte dienen te stellen, dat de pas en PIN-code zijn aangemaakt en naar de gebruiker zijn verstuurd.

De procedures die de organisatie dient te vervaardigen, zijn:
- uitgifte van rechten;
- mutatie van rechten;
- password-parameters (wordt in dit verband PIN-code-parameters);
- toegang database;
- vervanging security administrator.

Voor de overzichtelijkheid is ervoor gekozen deze subparagraaf op te splitsen in het beheer van de passen en het beheer van de PIN-codes.

Passen
Het beheer van de passen richt zich op de aanmaak, de uitgifte en de retournering van passen alsmede de afhandeling van verloren of gestolen passen.

Aanmaak van de passen
Om het identificatieproces mogelijk te maken, dienen gebruikers de beschikking te krijgen over een pas. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe worden blanco passen uit het magazijn gehaald;
- het proces van beschrijven van een pas (met andere woorden, wie mag een pas met welke informatie beschrijven);
- wat gebeurt met beschreven passen (en door wie en hoe);
- door wie en hoe geschiedt het vernietigen van passen, als gevolg van uitval (bijvoorbeeld door opmaak van proces-verbaal door twee functionarissen);
- waar, hoe en hoe lang worden eventuele bescheiden, ten aanzien van uitval, bewaard.

Uitgifte van de passen
Er dient voor gezorgd te worden dat een pas 'veilig' bij de gebruiker aankomt. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe worden aangemaakte kaarten naar de gebruikers verstuurd;
- aan wie worden verstuurde kaarten, welke niet kunnen worden bezorgd, geretourneerd;
- wat geschiedt met eventueel niet bezorgde kaarten (en door wie en hoe).

Geretourneerde passen (bij inname vanwege verbruik maximaal aantal pogingen)
Indien de PIN-code na bijvoorbeeld drie keer niet

juist is ingevoerd, dient de pas te worden ingenomen door bijvoorbeeld de balie-employé of de betaalautomaat. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- wanneer en door wie wordt een pas ingenomen;
- wat geschiedt met ingenomen passen (en door wie en hoe).

Indien een cliënt zijn rekening wil opheffen, wordt ervan uitgegaan dat dit gebeurt door het overboeken van het resterende saldo naar een andere rekening en het deactiveren van de rekening (dit betekent dat de gebruiker zijn kaart niet hoeft in te leveren).

Verloren/gestolen passen
Op aangeven van een cliënt dient de uitgegeven pas met onmiddellijke ingang te worden gedeactiveerd. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- wanneer, door wie en hoe wordt een pas geblokkeerd.

Indien een pas wordt ingenomen of geblokkeerd, kan worden besloten om, in verband met de gebruiksvriendelijkheid, automatisch een nieuwe pas voor de gedupeerde cliënt aan te vragen.

PIN-codes
Bij PIN-codes zijn vooral de generatie en de uitgifte en wijziging van belang.

PIN-generatie
Om het authenticatieproces mogelijk te maken, dient voor een bepaalde pas een PIN-code te worden gegenereerd. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- hoe ziet een PIN-code eruit (bijvoorbeeld vier posities gevuld met numerieke tekens);
- door wie en hoe wordt een PIN-code gegenereerd. Er zijn drie mogelijkheden voor PIN-generatie, namelijk: (1) berekende PIN (PIN wordt berekend op basis van een gegeven op de kaart, bijvoorbeeld rekeningnummer); (2) random-PIN (PIN wordt bepaald door een generator); (3) cliënt-PIN (de gebruiker kan de PIN zelf bepalen);
- wat gebeurt met de gegenereerde PIN-code (en door wie en hoe).

PIN-uitgifte/wijziging
Er dient voor te worden gezorgd dat een PIN-code 'veilig' bij de gebruiker aankomt. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe wordt een PIN-code aan een gebruiker bekend gemaakt (in het algemeen worden hier PIN-mailers voor gebruikt. Daar deze geprint worden, zijn de PIN-codes niet herleidbaar tot een bepaalde pas c.q. gebruiker);
- door wie en hoe worden aangemaakte PIN-mailers naar de gebruikers verstuurd;
- aan wie worden verstuurde PIN-mailers, welke niet kunnen worden bezorgd, geretourneerd;
- wat geschiedt met eventueel niet bezorgde PIN-codes (en door wie en hoe);
- indien sprake is van een cliënt-PIN, hoe maakt de cliënt de PIN-code bekend (bijvoorbeeld PIN-mailer of PIN-invoer op een beveiligde terminal (door de gebruiker)) en wie brengt de PIN-code in het systeem in (ook hierbij weer de eis dat een PIN-code niet herleidbaar is tot een pas c.q. een gebruiker).

Als een gebruiker zijn PIN-code vergeet dient een nieuwe pas te worden aangevraagd en de oude te worden vernietigd.

BEVEILIGING OP BASIS VAN BEZIT

De beveiliging op basis van bezit vindt plaats met behulp van tokens of smartcards.

Token

Bij het gebruik van tokens dienen het initialiseren, het versturen en retourneren alsmede het verloren gaan of gestolen worden procedureel te worden opgelost.

Het aanmaken van de passen en van PIN-codes moet gescheiden worden uitgevoerd.

Het initialiseren van tokens
Op het moment van binnenkomst, bij de organisatie, zijn het tokens alleen voorzien van het algoritme en dienen zij, alvorens door een gebruiker te kunnen worden gebruikt, te worden voorzien van een sleutel. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe worden tokens uit het magazijn gehaald;
- door wie en hoe wordt een token van een sleutel voorzien;
- wat geschiedt met de aangemaakte tokens (en door wie en hoe).

Versturen van het token
Er dient voor gezorgd te worden dat een pas 'veilig' bij de gebruiker aankomt. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe worden aangemaakte tokens naar de gebruikers verstuurd.

Bij het gebruik van hard tokens kunnen de gebruikers gedwongen worden een PIN-code in het token in te voeren. Dit kan een vaste (eens ingevoerd geen wijziging) of een variabele (wijziging eens per x weken) PIN-code betreffen. In het geval gekozen wordt om te werken met PIN-codes, dienen er ook procedures te zijn, die het zetten van PIN-code-parameters regelen en die beschrijven hoe dient te worden omgegaan met het resetten van PIN-codes.

Het retourneren van tokens
Indien een gebruiker geen gebruik meer maakt van het token of indien het token defect raakt, dient het

token te worden geretourneerd. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- aan wie en hoe wordt het token geretourneerd;
- wat geschiedt met een geretourneerd token (bijvoorbeeld resetten van de sleutel en daarna terug naar magazijn) (en door wie en hoe).

Verloren/gestolen tokens
Op aangeven van een gebruiker dient de uitgegeven pas met onmiddellijke ingang te worden gedeactiveerd. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- wanneer, door wie en hoe wordt het token geblokkeerd.

Een ander facet is het sleutelbeheer. Het is mogelijk de sleutels van de hard tokens te wijzigen. Dit betekent echter wel, dat zowel de sleutel in de database als in alle tokens dient te worden veranderd. Indien men dit periodiek van plan is, dient hiervoor een procedure te worden vervaardigd, waarin is beschreven wat de frequentie (of criteria) voor wijziging zijn, door wie de sleutel mag worden veranderd en hoe dit dient te gebeuren.

Indien nieuwe software naar de werkplekken dient te worden gezonden, dient er ook een procedure te zijn voor softwaredistributie. Hierin moet beschreven zijn door wie en hoe software naar de werkplekken dient te worden verzonden en hoe ervoor gezorgd dient te worden dat de werkplekken op een bepaald tijdstip met de nieuwe programmatuur werken.

Bij het gebruik van hard tokens kunnen de gebruikers gedwongen worden een PIN-code in het token in te voeren.

Voor deze techniek zijn ook de volgende procedures van belang (deze zijn echter reeds eerder besproken):
- uitgifte van user-id;
- intrekken van user-id;
- uitgifte van rechten;
- mutatie van rechten;
- password-parameters (wordt in dit verband PIN-code-parameters);
- opslag password (wordt in dit verband opslag PIN-code);
- toegang database;
- vervanging security administrator.

Met uitzondering van het initialiseren van het token gelden alle bovenstaande procedures ook voor het soft token. Het soft token kent ten aanzien van de bovenstaande procedures de volgende verschillen:
- indien wordt gekozen voor het periodiek wijzigen van de sleutels dienen bij de soft tokens de database en alle software op de werkstations van nieuwe sleutels te worden voorzien;
- omdat bij deze techniek altijd een PIN-code aan de gebruiker dient te worden verstrekt, is hierbij ook de procedure uitgifte password (zoals in de vorige paragraaf beschreven onder 'Password') van kracht.

Smartcard

De procedures zoals die in de vorige paragraaf zijn beschreven bij het aanmaken van magneetstripkaart en PIN-code gelden ook voor de semi-anonieme en persoonlijke smartcard.

Voor de semi-anonieme en persoonlijke smartcard geldt echter ook de volgende additionele procedure:

Defecte semi-anonieme smartcard
Indien een semi-anonieme smartcard defect raakt, kan het zijn dat de gebruiker nog een tegoed heeft. In een procedure die dit regelt, dient het volgende beschreven te zijn:
- door wie en hoe wordt bepaald hoeveel tegoed een gebruiker nog heeft;
- wat geschiedt met het tegoed (en door wie en hoe).

Tevens kan hier, net zoals bij het token, sleutelbeheer van toepassing zijn. Ook hierbij geldt dat indien men dit periodiek van plan is hiervoor een procedure dient te worden vervaardigd, waarin is beschreven wat de frequentie van wijziging is of wat de criteria voor wijziging zijn, door wie de sleutel mag worden veranderd en hoe dit dient te gebeuren.

BEVEILIGING OP BASIS VAN ZIJN

De procedures zoals die zijn beschreven bij de beveiliging op basis van een password gelden ook voor de beveiliging *op basis van zijn* (biometrische kenmerken). De beveiliging *op basis van zijn* verschilt echter op de volgende punten:

- Bij de uitgifte van een password hoeft de gebruiker niet naar een bepaalde plaats om het password in te voeren (in geval van een initieel password dient hij dit alleen bij de eerste keer aanloggen te wijzigen). Bij de techniek *op basis van zijn* dient de gebruiker wel naar een speciale plaats te gaan alwaar het persoonlijke kenmerk van de gebruiker dient te worden gescand en gedigitaliseerd in een database te worden vastgelegd. In een procedure die dit regelt, dient het volgende beschreven te zijn:
  - door wie en hoe wordt het persoonlijke kenmerk van de gebruiker initieel gescand;
  - wat geschiedt met de gescande gegevens (en door wie en hoe).

- De procedures uitgifte en intrekken user-id gelden niet. Het identificatieproces heeft namelijk tot doel om iedere gebruiker uniek te identificeren. In principe is dit bij beveiliging *op basis van zijn* niet nodig, omdat een gebruiker uniek kan worden geïdentificeerd aan de hand van het authenticatie-

middel (dit is namelijk voor geen twee gebruikers gelijk).

Indien het niet wenselijk wordt geacht dat iedere willekeurige voorbijganger de mogelijkheid krijgt zich te identificeren door simpelweg het uitleesapparaat te activeren, kan gebruik worden gemaakt van een identificatiemiddel (bijvoorbeeld passen). Indien men dit wil, dienen ook de volgende procedures beschreven te worden:
- aanmaak van de kaarten;
- uitgifte van de kaarten.

EVALUATIE

In deze paragraaf wordt een evaluatie gegeven van de in de eerste paragrafen beschreven technieken. Deze evaluatie vindt plaats aan de hand van een vergelijking van de volgende kwaliteitsaspecten:
- betrouwbaarheid;
- onderhoudbaarheid;
- gebruiksvriendelijkheid;
- vertrouwelijkheid;
- kosten.

Allereerst wordt een definitie van de bovengenoemde kwaliteitsaspecten gegeven. Vervolgens worden de besproken technieken aan de hand van deze kwaliteitsaspecten geëvalueerd en wordt een conclusie geformuleerd.

Definitie van de kwaliteitsaspecten

De kwaliteitsaspecten, die in de vergelijking worden betrokken zijn, in het kader van dit artikel, als volgt te definiëren:
- *betrouwbaarheid*: de mate waarin de techniek van toegangsbeveiliging geautoriseerde gebruikers toelaat en ongeautoriseerde gebruikers afwijst;
- *onderhoudbaarheid*: de mate waarin en het gemak waarmee de techniek van toegangsbeveiliging is aan te passen aan veranderde situaties (met andere woorden, hoe beheersbaar is de techniek van toegangsbeveiliging);
- *gebruiksvriendelijkheid*: de mate waarin de techniek van toegangsbeveiliging door eindgebruikers wordt geaccepteerd, rekening houdend met de inspanning die de gebruiker dient te verrichten;
- *vertrouwelijkheid*: de mate waarin derden kennis of bezit kunnen nemen van de voor identificatie en authenticatie benodigde gegevens;
- *kosten*: de mate waarin uitgaven dienen te worden gedaan om het systeem van logische toegangsbeveiliging operationeel te krijgen en te houden.

Overigens bepaalt het samenstel van bovenstaande kwaliteitsaspecten de effectiviteit en efficiency[5] van een bepaalde techniek van logische toegangsbeveiliging. Weliswaar zou men kunnen verdedigen dat een techniek altijd effectief is als deze betrouwbaar is, met andere woorden, als alle ongeautoriseerde aanlog-pogingen worden afgewezen en alle geautoriseerde aanlog-pogingen worden gehonoreerd. Maar indien een bepaalde techniek niet onderhoudbaar is en niet door gebruikers wordt geaccepteerd, zal deze nooit effectief kunnen worden ingevoerd.

Evaluatie van de technieken

In deze subparagraaf worden de in de eerste paragrafen besproken technieken afgezet tegen de in de vorige subparagraaf gedefinieerde kwaliteitsaspecten.

Om de verschillende technieken met elkaar te kunnen vergelijken, wordt per te onderkennen kwaliteitsaspect een waardering gegeven. Deze waardering loopt van 1 tot 5. Hierbij is 1 de laagst en 5 de hoogst mogelijke waardering. Voor betrouwbaarheid betekent dit hoe hoger de betrouwbaarheid des te hoger de waardering; voor de kosten is de waardering net andersom, dus hoe hoger de kosten des te lager de waardering.

Betrouwbaarheid
Ten opzichte van de andere technieken scoren de semi-anonieme smartcard en de beveiliging *op basis van zijn* lager. Dit heeft de volgende oorzaken:

- Bij de semi-anonieme smartcard wordt de gebruiker bij het verrichten van betalingen niet geverifieerd. Dit betekent dat een kaart gestolen kan worden en dat een ongeautoriseerde gebruiker hiermee betaling kan verrichten, zonder zich te authenticeren. Het is echter wel mogelijk om op de smartcard een PIN-code aan te brengen, zodat een gebruiker, voordat hij betalingen kan verrichten met de smartcard, eerst de juiste PIN-code dient in te geven.

- Alhoewel binnen de beveiliging *op basis van zijn* verschillende technieken worden onderschei-

5. In het kader van dit artikel wordt effectiviteit gedefinieerd als de mate waarin een methode van logische toegangsbeveiliging een bepaald systeem beveiligt en efficiëntie als de mate waarin het inlog-proces van de techniek van logische toegangsbeveiliging gebruik maakt van middelen om een zo effectief mogelijk proces van toegangsbeveiliging te verkrijgen.

Tabel 1. Vergelijking technieken van logische toegangsbeveiliging.

	Betrouwbaarheid	Onderhoudbaarheid	Gebruiksvriendelijkheid	Vertrouwelijkheid	Kosten
Password	4	3	4	2	4
PIN-code	4	2	4	3	3
Hard token	4	3	3	4	3
Soft token	4	3	4	3	3
Semi-anonieme smartcard	3	2	4	3	3
Persoonlijke smartcard	4	3	4	4	3
Biometrische kenmerken	2/5*	2	2/5*	5	2

* De aspecten betrouwbaarheid en gebruiksvriendelijkheid lijken een verband met elkaar te hebben. Immers, er zijn technieken beschikbaar welke honderd procent accuraat zijn (DNA en retinaherkenning), maar welke door gebruikers niet geaccepteerd worden. Dus hoge waardering voor betrouwbaarheid (5) en lage waardering voor gebruiksvriendelijkheid (2). Aan de andere kant zijn technieken beschikbaar welke door gebruikers geaccepteerd worden maar (nog) niet voldoende accuraat zijn (zoals stemherkenning en gezichtsherkenning). Dus lage waardering voor betrouwbaarheid (2) en hoge waardering voor gebruiksvriendelijkheid (5). In de toelichting zal hierop verder worden ingegaan.

den, is er op dit moment niet één techniek (die door de gebruiker wordt geaccepteerd), die altijd het onderscheid kan maken tussen een geautoriseerde en een ongeautoriseerde gebruiker (alhoewel er technieken (o.a. gezichtsherkenning) zijn die claimen dat de foutkans kleiner dan 0,1 procent is). Overigens zijn de technieken die door gebruikers niet worden geaccepteerd (DNA en retinaherkenning) wel betrouwbaar. Zelfs betrouwbaarder dan alle overige technieken, omdat bij andere technieken het gevaar van masquerading[6] niet uit te sluiten is.

Onderhoudbaarheid
Ten opzichte van de andere technieken scoren de PIN-code, de semi-anonieme smartcard en de beveiliging *op basis van zijn* lager. Dit heeft de volgende oorzaken:

Er is niet één door gebruikers geaccepteerde techniek die altijd het onderscheid kan maken tussen een geautoriseerde en een ongeautoriseerde gebruiker.

– De PIN-code en semi-anonieme smartcard vragen een strikte organisatie. Dit wordt mede veroorzaakt door het feit dat deze combinatie veelal wordt gebruikt in relatie tot het verrichten van financiële transacties. Eén van de eisen die daarom aan de genoemde technieken wordt gesteld, is dat zowel de kaart als de PIN-code bij de gebruiker aankomt, zonder dat iemand anders de combinatie magneetstripkaart/PIN-code kent of zou kunnen kennen.

– Bij de beveiliging *op basis van zijn* kan weliswaar een aantal procedures (ten opzichte van de beveiliging op basis van een password) vervallen, echter voornamelijk de procedure voor het digitaliseren van het authenticatiemiddel vraagt meer van de organisatie. Indien men dit namelijk gebruiksvriendelijk wil houden, zullen meerdere plaatsen in de buurt van de gebruiker moeten worden aangeboden waar het digitaliseren kan plaatsvinden. Tevens dienen aparte ruimten (bijvoorbeeld binnen een kantoor) te worden gecreëerd waar het digitaliseren kan plaatsvinden (onder andere in verband met privacyredenen).

Gebruiksvriendelijkheid
Ten opzichte van de andere technieken scoort het hard token lager, terwijl de beveiliging *op basis van zijn* hoger scoort. Dit heeft de volgende oorzaken:

– Het toetsenbordje op het hard token wordt door de gebruikers niet als prettig ervaren (te klein en te stroef). Daarom heeft deze techniek een achterstand op het soft token. Verschillende fabrikanten hebben (overigens met succes) getracht om deze achterstand te verkleinen door de gebruiker een token aan te bieden dat de challenge van het beeldscherm afleest.

– De beveiliging *op basis van zijn* scoort hoger, omdat een gebruiker niets meer hoeft te onthouden. De gebruiksvriendelijkheid wordt echter wel enigszins aangetast door het feit dat de gebruiker naar een speciale plaats moet om het authenticatiemiddel te laten digitaliseren. Echter dient wel opgemerkt te worden dat de gebruiksvriendelijkheid (en dus de toe te kennen waardering) afhankelijk is van het soort authenticatiemiddel (het gebruik van een vingerafdruk is gebruiksvriendelijker dan het gebruik van DNA).

Vertrouwelijkheid
Ten opzichte van de andere technieken scoren het password, de PIN-code, het soft token en de semi-anonieme smartcard lager, terwijl de beveiliging *op basis van zijn* hoger scoort. Dit heeft de volgende oorzaken:

– Zowel de identificatie als de authenticatie bij de beveiliging op basis van een password werkt alleen *op basis van kennis*, terwijl dit bij alle andere technieken werkt *op basis van kennis en bezit* of alleen *bezit*.

– Bij de beveiliging op basis van een PIN-code en de semi-anonieme smartcard hoeft de PIN-code nooit te worden gewijzigd. Terwijl dit bij het password wordt gezien als één van de maatregelen om de techniek veiliger te maken. Dus lijken de PIN-code en de semi-anonieme smartcard minder veilig dan de beveiliging op basis van een password. Toch is het maar de vraag of het wenselijk is om voor de genoemde technieken een PIN-code-cyclus in te voeren. De nadelen (kiezen van voor de hand liggende PIN-codes (zoals 1111, 3333, etc.), vaker vergeten van PIN-codes en mogelijk organisatorische consequenties (bijvoorbeeld iedere gebruiker krijgt per een bepaalde datum een nieuwe PIN-code toegewezen)) zouden misschien niet opwegen tegen de voordelen (het minder snel bekend raken van de PIN-code, waarbij de verantwoordelijkheid voor het bekend raken van de PIN-code bovendien ligt bij de gebruiker (met andere woorden, de kaartuitgevende instantie lijdt hierdoor geen schade)).

– Bij het soft token vinden alle berekeningen (om van een bepaalde challenge tot een respons te komen) in het geheugen van het werkstation plaats. Daarom lijkt deze techniek de schijn tegen te hebben. Zoals eerder besproken, is er ook een token dat alle berekeningen in het token zelf uitvoert.

– De beveiliging *op basis van zijn* scoort hoger, omdat een gebruiker, in tegenstelling tot de andere technieken, minder fraudegevoelig is omdat de gebruiker niets heeft dat gestolen kan worden.

Kosten
Ten opzichte van de andere technieken scoort de beveiliging *op basis van zijn* lager, terwijl het password hoger scoort. Dit heeft de volgende oorzaken:

– De beveiliging *op basis van zijn* is momenteel redelijk duur om te implementeren. Hoofdoorzaak hiervan is de specialistische apparatuur welke benodigd is om het authenticatiemiddel te kunnen uitlezen.

– De techniek op basis van een password scoort

6. Masquerading is het uitvoeren van ongeautoriseerde acties doordat iemand zich voordoet als een geautoriseerde gebruiker.

hoger, omdat voor deze techniek in vergelijking met andere technieken, zowel voor de identificatie als voor de authenticatie, geen additionele middelen benodigd zijn.

CONCLUSIE

Als een optelling wordt gemaakt van de in de vorige subparagraaf toegekende waarderingen dan blijkt dat de techniek met de persoonlijke smartcard de beste beveiliging biedt. Reden hiervoor is voornamelijk dat de persoonlijke smartcard vertrouwelijk (berekening van de respons op een challenge vindt plaats in de smartcard en authenticatie vindt plaats *op basis van kennis* en *bezit*) en gebruiksvriendelijk (het enige wat de gebruiker hoeft te doen is de smartcard in een uitleesapparaat te doen en een PIN-code in te voeren) is.

Bij bovenstaande conclusie dient te worden aangetekend dat indien oplossingen worden gevonden voor de nu nog aanwezige 'kinderziekten' voor de beveiliging *op basis van zijn* (de verschillende beschikbare technieken zijn niet altijd even betrouwbaar en/of gebruiksvriendelijk en zijn duur), deze methode (of in ieder geval een of meer technieken) kan uitgroeien tot de beste beveiliging.

Wel dient te worden bedacht dat bovenstaande wijze van bepalen van de beste methode niet geheel objectief is. Ook dient namelijk het te beveiligen belang in deze evaluatie te worden betrokken. Dit kan bijvoorbeeld als volgt worden gedaan.

Men kiest opnieuw een waardering lopend van 1 tot 5 en wijst deze, naar belangrijkheid (waarbij 1 gelijk is aan laag en 5 aan hoog), toe aan de verschillende kwaliteitsaspecten. Hierbij dienen deze waarderingen te worden geïnterpreteerd als wegingsfactoren.

Stel, men dient een intern systeem met relatiegegevens te beveiligen, waarbij de volgende randvoorwaarden zijn gesteld: lage kosten, gemiddelde onderhoudbaarheid en hoge gebruiksvriendelijkheid. Waarbij men, naar aanleidmg van een uitgevoerde risico-analyse, tot de conclusie komt dat de betrouwbaarheid van het systeem van voldoende niveau dient te zijn en de vertrouwelijkheid van minder belang wordt geacht.

Men zou dan aan de verschillende kwaliteitsaspecten de volgende wegingsfactoren kunnen toekennen:

– betrouwbaarheid	3
– onderhoudbaarheid	3
– gebruiksvriendelijkheid	5
– vertrouwelijkheid	2
– kosten	5

Indien men deze nu vermenigvuldigt met de scores van de in de vorige subparagraaf gepresenteerde tabel, dan blijkt de techniek met het password het hoogst te scoren.

Iedere keer als men een systeem bouwt c.q. aanschaft dient men zich allereerst af te vragen welk niveau van beveiliging men nodig acht voor het te beschermen systeem. Voor het bepalen hiervan kan het vervaardigen van een risico-analyse een hulpmiddel zijn.
Dit houdt in dat voor het te beschermen systeem de bedreigingen dienen te worden geanalyseerd, vervolgens wat de kans is dat een bepaalde bedreiging optreedt en wat dan de te verwachten schade is. Op basis van de uitkomst van deze analyse kan men de wegingsfactoren voor de kwaliteitsaspecten betrouwbaarheid en vertrouwelijkheid bepalen (hoe hoger het risico (= kans * schade) hoe hoger de wegingsfactor dient te zijn).

De wegingsfactor voor de kosten zal afhangen van het budget dat men ter beschikking stelt voor het vervaardigen c.q. aanschaffen van een techniek van logische toegangsbeveiliging (hierbij is een laag budget gelijk aan een hoge wegingsfactor).

Onderhoudbaarheid en gebruiksvriendelijkheid kunnen worden gezien als noodzakelijke randvoorwaarden om een systeem effectief te kunnen invoeren (hoe meer belang hieraan wordt gehecht hoe hoger de wegingsfactor dient te zijn).

LITERATUUR

[Duth96] A.W. Duthler e.a. *Module Juridische aspecten van informatietechnologie*, Erasmus Universiteit Rotterdam, Rotterdam 1996.

[Erns93] Ernst & Young, *A practical approach to logical access control*, McGraw-Hill, London 1993.

[Inte93] Intercai telematics consultants, *Chipcards (applications and opportunities)*, Samsom BedrijfsInformatie, Alphen aan den Rijn 1993.

[Kock95] H.C. Kocks, *Collegedictaat inzicht in samenhang*, Erasmus Universiteit Rotterdam, Rotterdam 1995.

[Kooij94] D.J. Kooijman, *Reader overige besturingsprogrammatuur*, Erasmus Universiteit Rotterdam, Rotterdam 1994.

[Moll93] K.IJ. Mollema e.a., *Computercriminaliteit (NIVRA-geschrift 62)*, Kluwer bedrijfswetenschappen/NIVRA, Amsterdam 1993.

[NNI94] Nederlands Normalisatie Instituut, *Code voor informatiebeveiliging*, NNI, Delft 1994.

[Over92] P.L. Overbeek en W.H.M. Sipman, *Informatiebeveiliging (een praktische gids voor de bescherming van uw gegevens)*, Tutein Nolthenius, Amsterdam 1992.

[Praa94] J. van Praat en H. Suerink, *Inleiding EDP-auditing*, Kluwer bedrijfswetenschappen, Deventer 1994.

Drs.ing. E. Beijer
Is sinds 1992 als EDP-auditor werkzaam bij de Interne Accountantsdienst van de GWK Bank. Recentelijk is hij aan de Erasmus Universiteit Rotterdam afgestudeerd op het onderwerp logische toegangsbeveiliging.

[Stro93] L.A.M. Strous (red.), *Standaardisatie van informatiebeveiliging*, Kluwer bedrijfswetenschappen, Deventer 1993.

[Tele94] Telematica research centrum, *Informatiebeveiliging (een blik achter de schermen)*, Samson BedrijfsInformatie, Alphen aan den Rijn 1994.

[Webe88] R. Weber, *EDP-auditing (conceptual foundations and practice)*, McGraw-Hill, United States 1988.

Surfen met de AS/400

Drs. R.Ch.T. Ewals RE

Datacommunicatie speelt een steeds belangrijkere rol in de informatievoorziening. Beschikbare hardware dient idealiter geschikt te worden gemaakt voor integratie met externe netwerkinfrastructuren. Voor de AS/400-computer is hiervoor een aantal mogelijkheden ontwikkeld. Kennis hiervan inclusief de daarbij behorende beveiligingsconsequenties is voor EDP-auditors van belang.

INLEIDING

Surfen op Internet is mode; gebruik maken van Internet behoort dan ook op vele systemen tot de mogelijkheden, zij het dat het net vaak wordt benut als een client en niet als een server. Om te kunnen surfen op Internet worden vaak applicaties toegepast die gebruik maken van het protocol TCP/IP. Een goede ondersteuning van deze protocol-familie was lang niet voorhanden op een AS/400. Met het toenemend belang van datacommunicatie alsmede van intranetten en Internet heeft ook IBM ingezien dat adequate ondersteuning van TCP/IP naast het standaard aanwezige SNA snel in importantie toeneemt. Zeker omdat de AS/400 ook als server in netwerken wordt gepositioneerd.
Tegen de achtergrond van de veranderingen in het toepassen van informatietechnologie heeft IBM ondersteuning van de TCP/IP-protocol-familie opgenomen in de besturingsprogrammatuur van de AS/400, OS/400, sinds versie V3R1 (bij de eerdere versies van OS/400 moest hiervoor een apart programma worden aangeschaft). Daarnaast is het recentelijk mogelijk geworden om de AS/400 als World Wide Web (WWW) server te gebruiken (vanaf versie V3R2). Maar op dezelfde computer draaien vaak ook de bedrijfsapplicaties. Nieuwe mogelijkheden dus, maar ook nieuwe bedreigingen.

In dit artikel wordt ingegaan op de mogelijkheden die de AS/400 biedt om gebruik te maken van Internet-technologie. Hierbij wordt aandacht besteed aan de AS/400 als server en als client. De beveiligingsmogelijkheden zullen nadrukkelijk in de beschouwing worden betrokken. Deze mogelijkheden zullen zich in dit artikel beperken tot maatregelen die op elke AS/400 zijn te nemen. Met behulp van nieuwe (soms nog in ontwikkeling zijnde) programmatuur is het wellicht mogelijk de beveiliging te vergroten, doch over de robuustheid van deze programmatuur kan nog niet in alle gevallen worden geoordeeld.

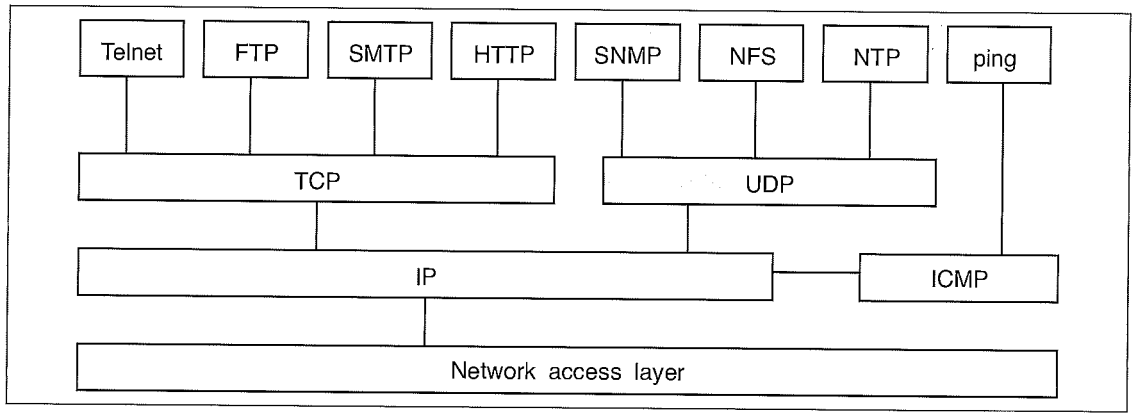
KOPPELINGEN MET INTERNET

De AS/400 biedt diverse mogelijkheden om gebruik te maken van Internet. Voordat hierop nader wordt ingegaan, zullen eerst kort enkele kernbegrippen rondom Internet worden behandeld.

Inleiding Internet

Achtereenvolgens komen applicaties, architectuur en het gebruik van Internet als client en als server aan de orde.

Geschiedenis en applicaties
De oorsprong van het huidige Internet wordt gevonden in het ARPAnet, dat in de jaren zeventig is ontwikkeld in opdracht van het Amerikaanse Department of Defense. Werd dat net in eerste instantie veel gebruikt door universiteiten, in de jaren negentig wordt het Internet 'herontdekt' door het



Figuur 1. Internet-architectuur.

bedrijfsleven en zien velen voordelen in het (commercieel) gebruik ervan.

Binnen het Internet wordt veel gebruik gemaakt van het Transmission Control Protocol en het Internet Protocol (TCP/IP). Door deze protocollen te hanteren kan applicatieprogrammatuur beschikken over een in principe foutvrije sequentiële communicatieverbinding. Tabel 1 bevat een overzicht van enkele min of meer bekende TCP/IP-applicaties tezamen met de protocollen die zij gebruiken inclusief een eventuele verwijzing naar bekende producten ([OTB96]).

Architectuur

Ten behoeve van communicatie tussen applicaties wordt gebruik gemaakt van protocollen op verschillende niveaus. Een bekend voorbeeld van een structuur op dit gebied is het OSI-model, waarin zeven lagen worden onderscheiden. Zonder een directe koppeling te maken met het OSI-model wordt in figuur 1 aangegeven welke lagen kunnen worden onderscheiden van een aantal in tabel 1 opgenomen protocollen ([OTB96]).[1]

Gebruik van Internet als client en server

Van het Internet kan op twee manieren gebruik worden gemaakt: als client en als server. De client vraagt informatie op bij een server en initieert acties. De server biedt informatie aan en voert verzoeken uit van de client. De AS/400 heeft de mogelijkheden om client en server te zijn. Indien meerdere connecties met Internet bestaan kan een AS/400 tegelijkertijd beide vormen uitvoeren.

1. Het Overlegorgaan Technische Beveiligingsstandaarden (OTB) stelt technische beveiligingsrichtlijnen op gebaseerd op het principe van 'goed huisvaderschap'. De richtlijnen zijn een nadere invulling van de in brede kring aanvaarde Code voor Informatiebeveiliging. Inmiddels zijn een OTB-standaard voor UNIX en een OTB-studie Internet-koppelingen verschenen.

Tabel 1. Overzicht enkele bekende TCP/IP-applicaties.

Applicatie	Protocol	Beschrijving	Productnaam
E-mail	SMTP	elektronische post	mail, elm, xmail, Eudora
FTP	FTP	bestandsoverdracht	FTP
TELNET	TELNET	inloggen vanaf een ander computersysteem	Telnet
WWW	HTTP	World Wide Web	Netscape, Mosaic, Internet explorer
SNMP	SNMP	netwerkbeheer en monitoring	
NFS	NFS	toegang files vanaf andere systemen	

In figuur 2 is schematisch een Internet-verbinding tussen een server en een client weergegeven.

De AS/400 als client

Met behulp van TCP/IP kan de AS/400 toegang krijgen tot Internet en kan een aantal applicaties worden gebruikt om acties uit te voeren op het Internet (maar ook om toegang tot andere netwerken te krijgen). Het betreft de volgende protocollen (die soms dezelfde naam hebben als de bijbehorende applicatie):

- SLIP (Serial Line Interface Protocol);
- Telnet;
- FTP (File Transfer Protocol);
- SMTP (Simple Mail Transfer Protocol);
- Post Office Protocol (POP);
- SNMP (Simple Network Management Protocol).

Deze protocollen maken het voor de gebruikers van de AS/400 mogelijk om Internet te benaderen. De AS/400 kan echter ook worden benaderd door derden vanaf een remote locatie. Om ongeautoriseerd gebruik van bestanden en programmatuur te voorkomen is een adequate afscherming noodzakelijk. De beveiligingsmogelijkheden van enkele van de hierboven genoemde protocollen binnen de AS/400-omgeving worden verderop nader uitgewerkt.

De AS/400 als server

In de nieuwste versie van het operating systeem (V3R2 voor de CISC-computers en V3R7 voor de RISC-computers) kan de AS/400 ook als server dienen voor Internet en Intranet. Hiermee wordt het voor ondernemingen mogelijk met behulp van Hypertext Transfer Protocol (HTTP) en Hypertext Markup Language (HTML, een syntax die wordt gebruikt om gegevens te versturen over het Internet en die door verschillende systemen kan worden geïnterpreteerd) Webpagina's te maken en deze aan te bieden op Internet. Deze mogelijkheid heet Internet Connection/400 HTTP Server (IC/400 of HTTP Server). Om op een juiste wijze gebruik te kunnen maken van de verbinding met Internet zijn ook applicaties nodig die in de vorige subparagraaf zijn opgenomen.

Het aanbieden van Webpagina's geschiedt met behulp van het HTTP-protocol en het reageren op een verzoek van een client wordt gedaan door het versturen van de HTML. Voor de acties die van belang zijn voor het aanbieden van de pagina's wordt door de AS/400 het profiel QTMHHTTP gebruikt en voor het versturen van de pagina's die worden verzocht door de client wordt het profiel QTMHHTP1 gebruikt.

De AS/400 kan ook worden benut om verzoeken van clients uit te voeren op de lokale computer. Hiertoe worden door de HTTP-server de zogenaamde Common Gateway Interfaces (CGI) scripts gebruikt. Een CGI is een standaard Webserver-protocol waardoor programma's die zijn gebaseerd op het client/server-principe, interactief kunnen werken met een Webbrowser ([Beck96]). Het resultaat van de uitvoering van de CGI-scripts wordt verzonden naar de client.

Door de mogelijkheid van de AS/400 als een Webserver te functioneren krijgen vele anderen derhalve toegang tot een computer waar in veel gevallen ook bedrijfs(kritieke) applicaties op draaien. Een adequate bescherming is daarom noodzakelijk.

Toekomstige mogelijkheden

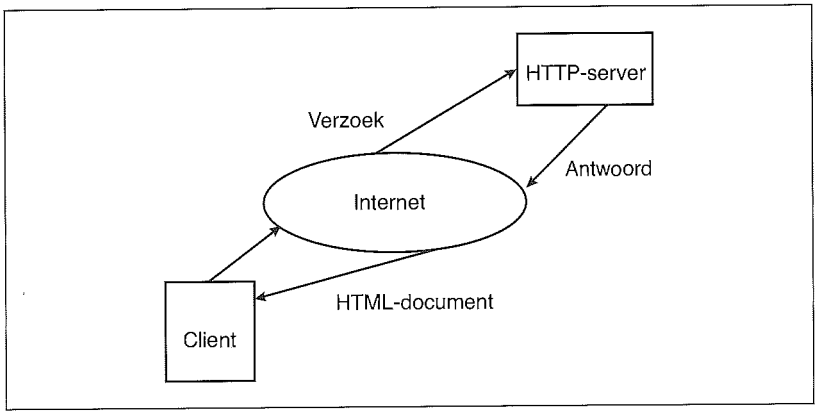
Als een 'Statement of general direction' heeft IBM aangegeven dat services zoals Point-to-Point Protocol (PPP), Domain Name Services (DNS) en Dynamic Host Configuration Protocol (DHCP) onderdeel zullen gaan uitmaken van de TCP/IP-ondersteuning op de AS/400. Ook zal de AS/400 geschikt worden gemaakt om te kunnen dienen als een proxy server ([IBM96a]). Met dit laatste worden de mogelijkheden vergroot om de AS/400 te benutten als server voor zowel Internet- als Intranet-services.

RISICO'S EN MAATREGELEN BIJ GEBRUIK VAN INTERNET

Aan het gebruik van Internet is onlosmakelijk een aantal risico's verbonden. Op deze risico's en te nemen maatregelen wordt hieronder ingegaan.

Risico's

Het allerbelangrijkste risico bij het gebruik van Internet is dat ongewenste personen toegang kunnen krijgen tot de interne netwerken en daar de integriteit van de informatiesystemen of de vertrouwelijkheid van gegevens schenden. Internet wordt mede daarom beschouwd als inherent onveilig. Regelmatig verschijnen in de pers berichten over succesvolle inbraakpogingen via Internet. Elke onderneming die overweegt gebruik te gaan maken van Internet zal zich terdege bewust moeten zijn van de risico's. Deze risico's kunnen worden onderverdeeld in drie categorieën: risico's voor de bedrijfsvoering, voor informatie en voor de IT-omgeving ([OTB96]).



Figuur 2. Relatie tussen server en client.

Bedrijfsvoering
Als de aansluiting op het Internet bedrijfskritiek is, zullen eisen worden gesteld aan de beveiliging van de aansluiting, aan de betrouwbaarheid van de technologie die wordt gebruikt en aan de leverancier van de IP-aansluiting.

Informatie
Voor veel gegevens die worden verzonden via Internet bestaan er risico's voor de vertrouwelijkheid en integriteit. Temeer daar vele gegevens niet geëncrypt worden verstuurd. Ook bestaan risico's aangaande het importeren van gegevens van Internet. Sommige berichten of informatie bevatten uitvoerbare programmatuur (waaronder virussen), die grote schade kunnen toebrengen aan informatie.

IT-omgeving
Een laatste categorie betreft de gevoeligheid van de IT-omgeving. Door de koppeling van Internet met een directe aansluiting op het systeem kan in principe iedereen het netwerk benaderen. Zeker als het interne netwerk ook communiceert met behulp van TCP/IP.

Maatregelen

De belangrijkste technische maatregel tegen computervredebreuk is de plaatsing van een firewall tussen het interne netwerk en het Internet. Een firewall kan een goede bescherming bieden, maar een belangrijke voorwaarde hierbij is wel dat op geen enkel ander punt in het interne netwerk een aansluiting op het Internet bestaat (single point of access). De volgende soorten firewalls worden onderscheiden ([Huls94], [Reid95]):
- enkelvoudig packet filter;
- screened host;
- dual homed host;
- screened subnet.

Voor een diepgaande beschouwing over de effectiviteit van deze soorten firewalls wordt verwezen naar de literatuur.
Naast een adequate installatie van een firewall kan de organisatie aanvullende maatregelen nemen zoals het beperken van inkomend en uitgaand berichtenverkeer of het beperken van file transfer.

BEVEILIGING VAN INTERNET-SERVICES

Beveiliging is noodzakelijk bij gebruik van de AS/400 als Webserver en als client om de integriteit van de programmatuur en bestanden te kunnen blijven waarborgen. Hiervoor kunnen verschillende maatregelen worden genomen.

Niet gebruiken

De beste beveiliging tegen inbreuken op de interne netwerken is het verbieden van elke vorm van toegang tot het Internet. Hiertoe bestaan op de AS/400 mogelijkheden. Belangrijk hierbij is dat de commando's om de verschillende services te activeren adequaat zijn afgeschermd. Dit kan bijvoorbeeld worden uitgevoerd door het commando STRTCP (Start TCP) niet te gebruiken; standaard is de bevoegdheid van *PUBLIC reeds op *EXCLUDE gezet. Initieel kan dit commando worden gebruikt door de standaard-gebruikersprofielen QSECOFR, QSRV, QSRVBAS, QSYSOPR en QPGMR. Daar deze profielen regelmatig worden gebruikt als groepsprofiel is een risico aanwezig dat te veel gebruikers de mogelijkheid hebben om TCP/IP te starten. Het is aan te bevelen de toegangsrechtenlijst van dit commando nader te beperken. Is beperking niet wenselijk, dan kan worden besloten om het gebruik van dit commando te registreren in de audit-logging.

De beste beveiliging tegen inbreuken is het verbieden van elke vorm van toegang tot het Internet.

Beheersen van toegang tot Internet

Indien een verbod op de toegang tot Internet niet realistisch is, zullen maatregelen moeten worden getroffen om de risico's die samenhangen met het gebruik van dit inherent onveilige netwerk zo goed mogelijk te beheersen. Hierbij dienen risico's te worden afgewogen tegen de kosten van de te nemen maatregelen.

Beveiliging TCP/IP-applicaties
De AS/400 bevat verschillende applicaties die gebruik maken van TCP/IP. Met behulp van deze applicaties kunnen gebruikers op de AS/400 toegang zoeken tot Internet. Ook kunnen derden trachten toegang te zoeken tot de AS/400 met behulp van bijvoorbeeld Telnet. Een aantal beveiligingsmaatregelen van de belangrijkste TCP/IP-applicaties wordt hier nader uiteengezet, te weten Telnet en FTP.

Telnet
Telnet kan worden gebruikt om vanuit de AS/400 contact te zoeken met een andere machine alsmede omgekeerd; er wordt contact gezocht met de AS/400 vanaf een andere machine om vervolgens applicaties te gebruiken op de server. Er vindt feitelijk terminal-emulatie plaats. Telnet zal aan een verzoekende gebruiker een sign-on scherm laten zien (beveiligingsniveau moet 20 of hoger zijn), zodat een gebruikersprofiel en een password vereist zijn. De uitwisseling van deze gegevens geschiedt echter niet in geëncrypte vorm.

Ter voorkoming van het automatisch opstarten van de Telnet-server (het commando STRTCPSVR, start TCP-server) als de TCP-server wordt geactiveerd, zijn maatregelen nodig. De default-waarde onder V3R2 ([IBM96b]) is dat deze server niet automatisch opstart. Om het aantal pogingen te beperken die kunnen worden gewaagd om toegang te krijgen tot het systeem verdient het aanbeveling de systeemwaarde QMAXSIGN (die aangeeft hoeveel pogingen kunnen worden gewaagd) op 3 tot 5 te zetten. Daarnaast staat de systeemwaarde QAUTOVRT (deze geeft het aantal virtuele devices aan waarop kan worden aangelogd) bij voorkeur op 0. Indien deze waarde hoger is dan nul wordt het aantal te nemen pogingen vermenigvuldigd met de waarde van QMAXSIGN.

Een belangrijke technische maatregel die kan worden genomen om het gebruik van Telnet te beperken is de poorten via welke de gegevensuitwisselingen geschieden te beperken. Hierbij kan aan een gebruikersprofiel een bepaalde poort worden toegekend. Daarmee worden alle andere gebruikers uitgesloten van het gebruik van deze poort.

Voor het starten van Telnet op de AS/400 dient toegang te bestaan tot het hiervoor benodigde commando (STRTCPTELN). Dit is af te schermen door in de toegangsrechtenlijst voor dit commando bepaalde gebruikers expliciet te autoriseren of anderen juist uit te sluiten. Daarnaast zal *PUBLIC moeten worden uitgesloten.

FTP
Met behulp van FTP kunnen bestanden worden uitgewisseld tussen systemen. De beperking van FTP op de AS/400 bestaat uit de mogelijkheid om alleen gehele bestanden uit te wisselen, terwijl DB2/400 (met behulp van APPN) ook voorziet in het uitwisselen van velden in bestanden. Via FTP levert dit veelal een beschadigd bestand op ([Vill-96]). De oplossing van IBM voor dit probleem is MPTN (Multi Protocol Transport Networking), waarvan de productnaam Anynet is. Ook kan FTP worden gebruikt om commando's te laten uitvoeren op de server. Het gebruik van FTP vereist een gebruikersprofiel en een password. Op de AS/400 bestaat echter ook de variant Anonymous FTP, waarbij geen identificatie en authenticatie is vereist. De uitwisseling van passwords geschiedt niet in geëncrypte vorm.

Voor het starten van FTP op de AS/400 als client dient toegang te bestaan tot het hiervoor benodigde commando (STRTCPFTP). Dit is af te schermen door in de toegangsrechtenlijst voor dit commando bepaalde gebruikers expliciet te autoriseren of anderen juist uit te sluiten. Daarnaast zal *PUBLIC moeten worden uitgesloten. Overigens geldt ook dat gebruik van het commando Start TCP (STRTCP) kan leiden tot het automatisch starten van de FTP-server. Dit is niet het geval als de automatische startfunctie op *NO is gezet.

Voor het beveiligen van FTP gelden dezelfde maatregelen als genoemd onder Telnet, maar het toekennen van een gebruikersprofiel aan een poort sluit in principe weliswaar alle andere gebruikers automatisch uit, doch is niet waterdicht. Een gebruiker die toegang zoekt tot de FTP-server gebruikt voor de toegang tot een poort een standaard AS/400-profiel, dat wel toegang heeft tot de desbetreffende poort. Het systeem schakelt pas over naar het individuele profiel nadat de verbinding tot stand is gebracht.

Zoals hierboven reeds is aangegeven, kent de AS/400 de mogelijkheid om het aantal inlogpogingen te beperken met behulp van een systeemparameter. Deze werkt echter niet voor FTP. Na vijf toegangspogingen wordt de sessie weliswaar verbroken, maar kunnen eenvoudig nieuwe sessies worden opgezet en toegangspogingen worden gedaan. Het verbreken van de verbinding na vijf pogingen wordt wel geregistreerd in de History Log.

Sinds versie V3R2 en V3R6 heeft de AS/400 enkele verbeterde mogelijkheden om het gebruik van FTP en Anonymous FTP te beheersen. Het betreft de volgende exits ([IBM96a]):
- authenticatie is vereist bij toegang tot gespecificeerde bestanden;
- de mogelijkheid tot het aangeven welke commando's kunnen worden gegeven door FTP-gebruikers (met name GET and PUT zijn belangrijk);
- de mogelijkheid tot het definiëren welke gebruikers FTP-servers mogen benaderen;
- de mogelijkheid tot het aangeven welke bestanden mogen worden gebruikt door *PUBLIC voor Anonymous FTP.

Bij gebruik van FTP is het uitermate belangrijk dat de toegangsregels juist zijn gedefinieerd. Zeker omdat alleen leesrechten (*USE) al tot gevolg kunnen hebben dat bestanden worden gekopieerd.

TCP/IP
Naast het afschermen van het gebruik van bepaalde op TCP/IP gebaseerde applicaties moeten ook de bestanden met informatie over de TCP/IP-configuraties worden beveiligd. Deze bestanden zijn opgenomen in de library QUSRSYS ([IBM96b]). Het is aan te bevelen voor al deze bestanden ten minste *PUBLIC uit te sluiten van toegang. Daarnaast moet goed worden afgewogen welke medewerkers uit hoofde van hun functie wel toegang moeten hebben tot deze bestanden.

Beveiliging IC/400
Voordat wordt ingegaan op de beveiliging IC/400 wordt kort aangegeven welke mogelijkheden tot beveiliging de AS/400 als Webserver (nog) niet heeft.

De AS/400 kan niet dienen als een proxy server. Ook kan de AS/400 op dit moment geen onderscheid maken tussen gebruikers die vanaf Internet toegang zoeken tot de machine. Er is geen vorm van identificatie en authenticatie vereist om de Webpagina's van de AS/400 te benaderen. Tevens is het nog niet mogelijk dat de uitwisseling van gegevens tussen de AS/400 en de client plaatsvindt met behulp van encryptie. Dit wordt als een belangrijke beperking van de beveiliging beschouwd.

Na het lezen van bovenstaande ontstaat vrijwel zeker de vraag welke mogelijkheden de AS/400 dan wel biedt en of deze dan als voldoende moeten worden beschouwd. De beveiliging van de AS/400 is integraal onderdeel van het operating systeem, hetgeen betekent dat ruime mogelijkheden bestaan tot beveiliging van de bedrijfsgegevens.

De activiteiten van de HTTP-server worden uitgevoerd onder het profiel QTMHHTTP op de AS/400. Dit profiel heeft geen password zodat er niet mee kan worden ingelogd. Overigens wordt door het gebruik van de AS/400 als Webserver ook de normale sign-on operatie niet uitgevoerd. Om het gebruik van de AS/400 als HTTP-server te beperken kan het profiel worden *DISABLED. Dit weerhoudt de AS/400 van opstarten als een HTTP-server.

Elk verzoek van een client aan de HTTP-server passeert een tweetal controles ([IBM96b]):
- het verzoek moet expliciet zijn gedefinieerd voor de HTTP-server;
- het profiel QTMHHTTP of *PUBLIC moet toegang hebben tot de gevraagde bronnen.

Elk verzoek door de client wordt gedaan met behulp van een Universal Resource Locator (URL) aan de HTTP-server. Of deze verzoeken mogen worden uitgevoerd, zal binnen de AS/400-omgeving zo precies mogelijk moeten worden gedefinieerd. Hiervoor beschikt de AS/400 over de zogenaamde HTTP-directives. Hierin kan worden aangegeven wat moet worden uitgevoerd op basis van welke URL. Hierbij dienen algemene (generic) namen en wildcards zoveel mogelijk te worden vermeden. Ook lijkt het verstandig om een zekere herschrijving uit te voeren van de URL ten opzichte van de feitelijke namen (met behulp van het commando MAP). Hiermee wordt voorkomen dat een hacker te veel informatie verzamelt over kenmerken van een systeem. Ook is het mogelijk bepaalde objecten in een library, die mag worden benaderd met behulp van een URL, expliciet uit te sluiten met behulp van de directives.
Het is derhalve essentieel dat de aan QTMHHTTP en *PUBLIC toegekende bevoegdheden precies zijn gedefinieerd. Een te brede toekenning van rechten zorgt voor gaten in de beveiliging die hadden kunnen worden gedicht. Een aanpak om de rechten te beperken is door het profiel QTMHHTTP expliciet geen bevoegdheden (*EXCLUDE) te geven op alle libraries met uitzondering van de speciaal voor de Webpagina's gecreëerde libraries. Ook de bevoegdheden van *PUBLIC moeten worden geëvalueerd.

Voor het configureren van de IC/400 is de special authority *IOSYSCFG vereist, waardoor de risico's beperkt zijn tot de profielen die over deze special authority beschikken. Als standaard is deze alleen toegekend aan de Security Officer op de AS/400.

De HTTP-server, preciezer QTMHHTTP, is niet in staat direct wijzigingen aan te brengen op de AS/400. Het is wel mogelijk dat een verzoek van een client tot gevolg heeft dat een CGI-script wordt aangeroepen. De AS/400 schakelt dan automatisch

over naar het profiel QTMHHTP1 ([Fink96a]), dat het CGI-script zal uitvoeren. De CGI-scripts zijn wel in staat wijzigingen door te voeren op de AS/400. Met behulp van deze scripts kan zelfs direct toegang worden verkregen tot de database van de AS/400, DB2/400. Het resultaat van de vraag wordt met behulp van HTML verstuurd naar de client. Deze mogelijkheid van de AS/400 geeft duidelijk aan dat de bevoegdheden van QTMHHTP1 zeer nauwkeurig moeten worden vastgesteld en geïmplementeerd. Ook voor het profiel QTMHHTP1 geldt dat aan dit profiel geen password is toegekend, zodat hiermee niet kan worden ingelogd. Verder heeft QTMHHTP1 geen bijzondere bevoegdheden in het profiel zelf (user class is *USER en special authorities zijn niet toegekend). Het is overigens verstandig om, evenals dat bij QTMHHTTP het geval is, QTMHHTP1 uit te sluiten van toegang tot de libraries (behalve de libraries die dit profiel echt nodig heeft).

BEVEILIGING LOKALE AS/400

Wanneer een onderneming besluit om de AS/400 rechtstreeks aan te sluiten op het Internet, is het van groot belang dat de lokale AS/400 en eventueel daaraan gekoppelde systemen adequaat zijn beveiligd. Mocht een ongeautoriseerde persoon zich toch toegang weten te verschaffen, dan zullen de gevolgen hiervan zo gering mogelijk moeten zijn. Voor deze beveiliging biedt de AS/400 een groot aantal mogelijkheden, waarvan de belangrijkste zullen worden behandeld.

Niveaus van de beveiliging

De AS/400 beschikt over een vijftal niveaus van beveiliging, die worden weergegeven als de niveaus 10, 20, 30, 40 en 50. De niveaus 10 en 20 worden als ontoereikend beschouwd voor de classificatie adequate beveiliging. Dit betekent dat ten minste niveau 30 actief moet zijn. Op niveau 30 is de zogenaamde objectbeveiliging van toepassing, waardoor individuele objecten op de AS/400 zijn te beveiligen. Aan niveau 30 kleven echter enkele inherente nadelen die onder niveau 40 niet meer bestaan. Onder niveau 40 is het bijvoorbeeld niet mogelijk dat een CGI-programma AS/400-systeemobjecten benadert zonder gebruik te maken van daarvoor geautoriseerde programma's (zogenaamde API's) die deze systeemobjecten beschermen. Ook biedt niveau 40 bescherming tegen het terugplaatsen van een programma met een paard van Troje ([Fink96b]). De IC/400 van de AS/400 kan overigens ook worden uitgevoerd onder niveau 50, maar dit voegt niet zoveel extra bescherming toe. De voorkeur hebben derhalve de niveaus 40 en 50. IBM heeft overigens aangegeven dat het besturingssysteem vanaf versie V3R7 wordt afgeleverd met beveiligingsniveau 40.

Bevoegdheden gebruikersprofielen

Gebruikersprofielen kunnen op de AS/400 worden onderscheiden in twee categorieën: geprivilegieerde profielen en profielen zonder bijzondere bevoegdheden.

Geprivilegieerde profielen
De AS/400 bevat een aantal bevoegdheden die, mits toegekend aan een gebruikersprofiel, bijzondere rechten geven op het gehele systeem. Deze bijzondere rechten worden 'special authorities' genoemd. De volgende special authorities bestaan:

- *ALLOBJ: geeft toegang tot alle objecten, met uitzondering van de objecten en elementen waarvoor één of meer andere special authorities zijn vereist;
- *SECADM: geeft rechten tot het aanmaken en onderhouden van gebruikersprofielen;
- *SAVSYS: geeft rechten op het gebied van back-up en restore van objecten;
- *AUDIT: geeft rechten met betrekking tot het definiëren en lezen van te loggen informatie;
- *SPLCTL: geeft rechten op spool files;
- *JOBCTL: geeft rechten op het gebied van de processen die lopen op het systeem;
- *IOSYSCFG: geeft rechten op het gebied van communicatie.

Ten behoeve van een adequate beveiliging met Internet wordt bijzondere aandacht gevraagd voor profielen die beschikken over de special authority *IOSYSCFG. Deze profielen zijn in staat communicatielijnen te definiëren, op te bouwen en te onderhouden. Het toekennen van deze bevoegdheid aan gebruikers dient derhalve met grote terughoudendheid te geschieden. *IOSYSCFG is noodzakelijk om de IC/400 HTTP-server van de AS/400 te configureren. Overigens heeft uitsluitend de Security Officer (QSECOFR) deze bevoegdheid bij installatie van het systeem.

Security Officer
De Security Officer heeft op de AS/400 alle special authorities. Het spreekt voor zich dat zeer voorzichtig moet worden omgegaan met het gebruik van dit profiel. Ten behoeve van een adequate beveiliging (tegen gebruik door onbevoegden) zouden aparte regels moeten worden gedefinieerd voor het gebruik van dit profiel. Hierbij kan worden gedacht aan een password dat ten minste acht karakters lang is en een expiratie-interval kent van bijvoorbeeld veertien dagen. Voorts kunnen speciale eisen worden gesteld aan dit password, zoals het verplicht gebruik van een cijfer, het niet naast elkaar mogen gebruiken van dezelfde tekens, een steeds wisselend password of het verbieden van evidente passwords. Daarnaast zou de Security Officer moeten worden beperkt in de locaties vanaf welke hij kan inloggen op het systeem. De meeste van deze elementen kunnen (eenvoudig) worden geïmplementeerd door onder meer het juist instellen van een aantal systeemparameters. Ook zouden alle acties van de Security Officer moeten worden gelogd.

Overigens is de Security Officer (QSECOFR) op de AS/400 in staat alle instellingen te wijzigen. Reden om dit profiel onder alle omstandigheden met terughoudendheid te gebruiken en niet alleen inzake koppelingen met Internet. Met adequate organisatorische procedures en instellingen in het systeem

voor het gebruik van dit profiel kan het risico van ongeautoriseerd gebruik zo laag mogelijk worden gehouden.

Hierboven is speciaal melding gemaakt van het QSECOFR-profiel, maar dezelfde regels kunnen ook van toepassing worden verklaard op alle profielen waarvan de onderneming van mening is dat zij als gevoelig moeten worden beschouwd.

'Gewone' profielen
De 'gewone' gebruikersprofielen op de AS/400 kunnen weliswaar geen communicatielijnen opzetten en activeren op operating systeem-niveau, afhankelijk van de robuustheid van de beveiliging kunnen zij echter wellicht meer dan is gewenst. Dit geldt met name voor gebruikers die gebruik mogen maken van de command line en dus in staat zijn commando's uit te voeren en applicaties aan te roepen. Het gebruik van de command line zal derhalve zoveel mogelijk moeten worden beperkt. Een beproefd middel hiertoe is aan te geven in het gebruikersprofiel dat de 'Limited Capabilities' op 'Yes' dienen te worden gezet. Overigens betekent dit geen honderd procent beveiliging tegen het uitvoeren van commando's, maar in dit artikel wordt hier vanwege de vereiste technische diepgang niet verder op ingegaan. Een ander middel om ongeautoriseerd gebruik van profielen tegen te gaan is het beperken van de tijden waarop het mogelijk is in te loggen op het systeem (mogelijk vanaf versie V3R2).

Afscherming objecten

Naast het beperken van de mogelijkheden van de gebruikersprofielen kunnen objecten (individueel) worden afgeschermd. Hiervoor biedt de AS/400 onder meer de mogelijkheden van library-bescherming en gebruik van *PUBLIC.

In het kader van de beveiliging van de AS/400 die als HTTP-server dient, moeten de libraries die worden gebruikt voor communicatie met Internet worden beschermd. Dit kan geschieden door aan de toegangsrechtenlijst expliciet de profielen QTMHHTTP en QTMHHTP1 toe te voegen. Daarbij kan desgewenst onderscheid worden gemaakt tussen de rechten van deze twee profielen op de desbetreffende libraries.
Libraries op het systeem die geen enkele relatie met Internet hebben, moeten worden beschermd door bijvoorbeeld op de toegangsrechtenlijst van deze libraries aan te geven dat de profielen QTMHHTTP en QTMHHTP1 expliciet zijn uitgesloten (*EXCLUDE) van toegang tot deze libraries. Deze profielen kunnen dan ook geen objecten meer benaderen in deze libraries.

Het onjuist gebruik van *PUBLIC leidt vaak tot onverwacht veel toegangsrechten op objecten (en dat kunnen ook libraries zijn). Een profiel krijgt de toegangsrechten op een object via *PUBLIC indien het desbetreffende profiel op geen andere gedefinieerde wijze toegangsrechten heeft op dit object. Voor de connectie met Internet is derhalve een juiste definitie van de rechten van *PUBLIC belangrijk voor ten minste alle libraries op het systeem. Het is aan te bevelen om de *PUBLIC-bevoegdheid van alle productielibraries op het systeem op *EXCLUDE te zetten, ongeacht het belang van de library. Is dit om een bepaalde reden niet efficiënt, ongewenst of niet mogelijk, dan verdient het sterk de aanbeveling dit wel te doen voor alle kritieke libraries. Daarnaast zal moeten worden geëvalueerd in welke mate zich kritieke objecten bevinden in de libraries die op zichzelf als niet kritiek zijn beoordeeld.

De boodschap moet dan ook, zoals eigenlijk altijd, luiden: beperk de toegangsrechten tot het minimaal noodzakelijke voor zowel *PUBLIC als voor gebruikersprofielen.

Gebruik van de logging

Op de AS/400 bestaan verschillende mogelijkheden om informatie over gebeurtenissen te registreren in een logging. Hiervan worden de audit-logging, Access Log en Error Log achtereenvolgens behandeld.

Audit-logging
Naast de (grote) variëteit van preventieve maatregelen om de AS/400 te beschermen tegen inbreuken van buitenaf bestaan mogelijkheden om achteraf vast te stellen of de integriteit inderdaad is gewaarborgd en om vast te stellen of pogingen zijn gedaan om in te breken. Hierbij kunnen ook succesvolle pogingen worden geregistreerd.

De AS/400 beschikt over audit-logging-faciliteiten op drie niveaus:
- systeemniveau;
- gebruikersprofielen;
- objectniveau.

De registratie van gebeurtenissen vindt plaats in een audit-journal dat alleen kan worden gelezen als een profiel over de special authority *AUDIT beschikt. Mutatie van een audit-journal is niet mogelijk. De door de AS/400 geboden mogelijkheden zorgen ervoor dat bepaalde acties van bepaalde profielen worden geregistreerd in de audit-logging. Welke acties dit zijn kan gedetailleerd worden aangegeven. Ook kan worden geregistreerd welke objecten zijn benaderd en/of welke zijn gewijzigd.

Access Log
Naast het gebruik van de standaard-audit-logging van de AS/400 kan gebruik worden gemaakt van de Access Log van de HTTP-server. De Access Log kan worden gebruikt tezamen met de audit-log. De informatie die in deze logging wordt geregistreerd, is ([IBM96c]):
- het URL-adres van de pagina('s) die werd(en) geraadpleegd;
- het IP-adres of de host-naam van de client;
- de HTTP-server-methode en het toegangspad tot het geraadpleegde document;
- de datum en tijd van het verzoek.

De bruikbaarheid van deze logging is echter beperkt omdat met name van IP-adressen bekend is dat zij eenvoudig kunnen worden gesimuleerd. Hierdoor bestaat feitelijk geen zekerheid over de juistheid van de afkomst van het verzoek.

Drs. R.Ch.T. Ewals RE
Werkt bij KPMG EDP Auditors, momenteel in de functie van EDP Audit Manager. Hij heeft zich gespecialiseerd in de midrange-omgevingen, met als speciaal aandachtsgebied de AS/400.

Error Log
In de Error Log wordt informatie vastgelegd over verzoeken die niet konden worden uitgevoerd. De volgende informatie wordt geregistreerd ([IBM-96c]):
- het URL-adres;
- het error adres;
- de datum en tijd van het verzoek.

Voor zowel de Error Log als de Access Log geldt dat zij een standaardgrootte hebben. Dit betekent dat wanneer het log-bestand vol is, geen informatie meer wordt geregistreerd. Hiervan krijgt de systeem-operator wel een bericht.

DE INTERNET-AUDITOR

De AS/400-wereld wordt snel groter en complexer. Dit komt vooral door de migratie van de AS/400 naar een open systeem, de toevoeging van de TCP/IP-protocollen en de popularisering van Internet. Dit betekent voor de EDP-auditor dat hij niet alleen kennis en inzicht dient te hebben in de aloude beveiligingsmogelijkheden van de AS/400 inclusief APPN en APPC, hij zal nu ook kennis moeten hebben van Internet en TCP/IP. De AS/400-wereld is immers uitgebreid met de Unix-wereld. Het uitvoeren van een EDP-audit in een AS/400-omgeving is derhalve complexer geworden en stelt dan ook hogere eisen aan de kennis van de EDP-auditor. Maar niet alleen aan de EDP-auditor. Ook personen die zich bezighouden met de inrichting van systemen en speciaal de communicatie tussen systemen zullen hun kennis moeten verrijken met de (beveiligings)mogelijkheden van TCP/IP. Een EDP-auditor gespecialiseerd op de terreinen AS/400 en Internet kan hierbij adviezen verlenen.

TOT SLOT

In dit artikel is beknopt een aantal maatregelen beschreven waarmee het mogelijk is de toegang tot Internet te beheersen alsmede de lokale AS/400-computersystemen adequaat af te schermen. Ook blijkt dat veel maatregelen kunnen worden genomen op de lokale computer en met behulp van de standaardvoorzieningen van de AS/400. Het dient echter met nadruk te worden gesteld dat niet alle maatregelen zijn behandeld. Binnen de AS/400-omgeving zijn nog meer (zeer) technische mogelijkheden aanwezig om gebruik van Internet-verbindingen te beschermen. Daarnaast zijn applicaties op de AS/400 te verkrijgen die meer mogelijkheden bieden ter beveiliging dan de op dit moment standaard aanwezige AS/400-functionaliteit voor de Internet-connectie (bijvoorbeeld Webulator). Deze zijn in dit artikel echter niet behandeld. Wanneer een dergelijke applicatie wordt gebruikt ter verhoging van het niveau van de beveiliging zal de effectiviteit ervan moeten worden beoordeeld door de EDP-auditor. Een absolute beveiliging en dus bescherming tegen hackers is echter vooralsnog niet voorhanden. Op geen enkel systeem.

LITERATUUR

[Beck96] M. Beckman, *Internet Connection for AS/400*, NEWS/400, februari 1996.

[Fink96a] J. Finkenaur, *Explore IBM's new AS/400 web server*, NEWS/400, juli 1996.

[Fink96b] J. Finkenaur, *Securing Internet Connection/400 HTTP Server*, NEWS/400, oktober 1996.

[Huls94] H. van Hulst, *Internet? Maar dan wel met een firewall*, Compact 1994/3.

[IBM96a] IBM, *OS/400 V3R2 Announcement and V3R6 Product availability update*, nummer A96-624, juni 1996.

[IBM96b] IBM, *Tips and tools for securing your AS/400*, 1996.

[IBM96c] IBM, *TCP/IP Configuration and Reference*, derde editie, juni 1996.

[OTB96] Overlegorgaan Technische Beveiligingsstandaarden, *OTB-studie Internet-koppelingen*, november 1996.

[Reid95] J. Reid, *Open systems security: traps and pitfalls*, Proc. Compsec 1995, Elsevier Advanced Technology, 1995.

[Vill96] D. Villanueva, *Netwerkbeheer nog problematisch*, Computable, 18 oktober 1996.

Het einde van Halons

G. Doddrell

De continuïteit van rekencentra is van essentieel belang gelet op de toenemende afhankelijkheid van de (geautomatiseerde) informatievoorziening. Detectiemaatregelen voor het onderkennen van calamiteiten zijn uiterst belangrijk. Eén daarvan betreft het installeren van branddetectievoorzieningen en het installeren van een Halon-installatie. Het succesvol implementeren van deze voorzieningen vergt een gedegen aanpak.

INLEIDING

Het is vier uur 's ochtends. De beveiligingsmedewerker heeft zojuist zijn laatste ronde van die nacht afgesloten. Hij noteert 'alles in orde' in zijn logboek en denkt aan ontbijt, een heerlijke dag slaap en de voetbalwedstrijd van zaterdag. Terwijl hij net het bedrijfsterrein afrijdt, begint het waterniveau in de koffieketel in de lunchkamer te dalen, overgaand in stoom doordat het verwarmingselement op hol slaat. Lange jaren trouwe dienst eisen hun tol; de thermische beveiliging moet in werking treden maar doet het niet. In slechts vijftien minuten tijd begint de bovenste laag van de werktafel al te schroeien en vervolgens te smeulen, dan breken er vlammen uit die steeds meer vat krijgen op het houten blad. Een kortgesloten kabel laat de stoppen nog wel springen, maar het is al te laat.

Twintig meter verderop in de gang beëindigt een midrange-computer de laatste backup op tape en wacht op de nieuwe dag – een dag die niet zal aanbreken. Vlammen spelen langs de kasten en bereiken de plafondtegels, die de brand maar even remmen maar dan neerstorten in een regen van vonken. De hitte blaast in de ruimten van de verlaagde plafonds en omdat vuur nu eenmaal vuur is, raast het door de openingen. Nog meer plafonddelen komen in brand te staan en vallen vervolgens op het meubilair en de scheidingswanden. Kabels vatten vlam en verspreiden het vuur als lonten. Bijtende rook vult alle ruimten en de computer staat rustig te wachten. Een vooruitziende blik zal de computer wel redden, er was immers een gasblusinstallatie voor de totale ruimte geïnstalleerd. Maar loopt het ook zo?

Het brandrisico voor de computerruimte was niet goed onderzocht. Het alarm gaat nog wel af en het gas wordt uitgestoten, maar dat lost op in dikke wolken van rook en as. Ten slotte begeven ook de laatste afschermingswanden van de computerruimte het.

Wat ging er mis? Als we dit scenario analyseren, kan een aantal tekortkomingen worden vastgesteld:

- de algemene kantoorruimte had beschermd dienen te worden met behulp van brandmelders en bij voorkeur ook door een brandbestrijdingssysteem;
- de koffieketel had na kantoortijd uitgeschakeld dienen te worden (met een tijdklok) en verkeerde niet in deugdelijke staat;
- alhoewel de computerruimte 'beschermd' was door een gasblusinstallatie bleek deze installatie niet te werken omdat de ruimte zelf niet meer intact was. Deze installaties vereisen tenslotte een minimum aan gasconcentratie voor een effectieve brandbestrijding.

Sceptici kunnen dan wel beweren dat dit scenario niet realistisch is maar een onderzoek in kantoren met computerinstallaties zou genoeg voorbeelden van dergelijke niet-toereikende brandbeveiliging en verspild geld onthullen.

De doelstelling van dit artikel is om gasblusinstal-

laties in perspectief te plaatsen binnen het totale schema van brandbeveiliging, -bestrijding en -beheersing, met het oog op het implementeren van effectieve, geïntegreerde oplossingen voor brandbeveiliging.

GEÏNTEGREERDE BEVEILIGING

Een gasblusinstallatie is een ineffectieve, kostbare verspilling van geld, tenzij zij wordt beschouwd als slechts een onderdeel van de brandbeveiliging van een gebouw.

Geïntegreerde beveiliging vereist actie op een aantal gebieden, bijvoorbeeld:
- brandmelders door het hele gebouw;
- rechtstreekse alarmmelding bij de brandweer;
- beoordelen van het brandrisico van een door een gasblusinstallatie beveiligde ruimte;
- handbrandblussers;
- sprinklers in gedeelten die niet beschermd worden door een gasblusinstallatie;
- indien van toepassing: een gasblusinstallatie in ruimten waar installaties of materialen worden ondergebracht die waardevol of van kritiek belang zijn;
- effectief, continu onderhoud en controles op de installaties.

Opgemerkt dient te worden dat niet alle gebouwen door een sprinklerinstallatie of zelfs maar brandmeldinstallaties beveiligd moeten worden om reeds te voldoen aan de lokale brandweervoorschriften. Dienovereenkomstig besteedt slechts een klein aantal eigenaren van gebouwen op vrijwillige basis geld aan de verbetering van het niveau van brandbeveiliging, tenzij dit door de wet wordt afgedwongen. Wanneer een huurder een gebouw betrekt, is het brandbeveiligingssysteem normaal gesproken al geïnstalleerd en de huurder zou slechts met veel moeite de eigenaar ertoe kunnen brengen alleen voor hem de installaties te verbeteren, tenzij men natuurlijk bereid is hiervan zelf de kosten te dragen.

Hierin ligt het dilemma besloten – de kosten versus de risico's en consequenties van niet-adequate beveiliging. Dit is een gebied waar een op professionele wijze uitgevoerde risicobeoordeling het management behulpzaam kan zijn bij het bouwen of selecteren van een gebouw of op het moment dat het verbeteren van de brandbeveiliging wordt overwogen.

GASBLUSINSTALLATIES, EEN OVERZICHT

Omdat een aantal betrokkenen de technische ontwikkelingen niet zal hebben gevolgd, geeft deze paragraaf in niet-technische termen korte opsommingen van een aantal aspecten van gasblusinstallaties.

Doelstellingen

De doelstellingen van het installeren van een gasblusinstallatie zijn:
- het zo vroeg mogelijk ontdekken van een brand binnen het beveiligd gebied;
- het informeren van het personeel ter plaatse en bij voorkeur ook de brandweer over een brandalarm;
- het personeel in staat stellen het beveiligd gebied te verlaten voordat het gas de ruimte vult;
- het gas op een dusdanige wijze uit laten stromen dat de afdichting van de beveiligde ruimte intact blijft;
- het blussen van de brand;
- het lang genoeg op peil houden van de gasconcentratie om het weer oplaaien van het vuur te voorkomen;
- de storingstijd waarin de beveiligde apparatuur niet gebruikt kan worden, zo kort mogelijk houden.

Overwegingen bij het ontwerp

Er is een aantal factoren die het ontwerp van gasblusinstallaties en het compartiment van het beveiligd gebied beïnvloeden:
- de omvang van het beveiligd gebied;
- het aantal aparte kamers binnen het gebied en afzonderlijke tussenruimten op plaatsen zoals onder verhoogde toegangsvloeren en in plafondruimten;
- het aantal meldpunten en onderbrekingsknoppen;
- de gasdichtheid van een beveiligde ruimte om lekkage te voorkomen;
- geschikte locaties voor het opslaan van de gascylinders;
- beperkingen van de ruimte voor de aanleg van leidingen.

Onderdelen

Een gasblusinstallatie bestaat uit een aantal onderdelen die met elkaar verbonden zijn:
- een controlepaneel met:
  - een energievoorziening met een reservebatterij;
  - elektronische indicatoren voor het ontdekken van rook, controle van de gasuitstoot en de werking van alarmbellen en waarschuwingssystemen voor ontruiming;
  - indicatoren om het personeel over de stand van de blusinstallatie en het brandalarm te informeren;
  - een verbinding met de brandweer;
- rookdetectoren, aangebracht op van tevoren bepaalde plaatsen overeenkomstig het ontwerp (doorgaans in de plafondruimten, onder de plafondplaten en onder de verhoogde vloer);

- tanks waarin het gas (bijvoorbeeld Halon 1301) is opgeslagen;
- elektrisch gestuurde uitstroomventielen, één op iedere gastank;
- leidingen van de voorraadtanks naar de uitstroomopeningen die zijn aangebracht in de plafondruimten, onder de plafondplaten en onder de verhoogde vloer;
- knoppen voor luchtafsluiting met hoorbare 'gasisolatie'-alarms bij iedere uitgang van het beveiligd gebied;
- verlichte 'ontruiming'-borden binnen het beveiligd gebied bij iedere uitgang en verlichte 'niet betreden'-borden bij iedere ingang aan de buitenkant van het beveiligd gebied;
- tweetonig, akoestisch ontruimingsalarm. De eerste toon klinkt wanneer voor het eerst rook wordt waargenomen, de tweede toon tijdens de wachtperiode voorafgaande aan de uitstoot.

Volgorde van gebeurtenissen bij alarm

De specifieke volgorde van acties bij een alarm voor een gasblusinstallatie is:

a. één rookmelder wordt geactiveerd;
- het eerste akoestisch alarm gaat af;
- het controlepaneel geeft aan in welke zone de rook is waargenomen;
- elektronisch gesloten deuren worden ontsloten;
- de airconditioning in het beveiligde gebied wordt uitgezet;
- het personeel kijkt (hopelijk) of het het vuur met handbrandblussers onder controle kan krijgen. Als het niet bijtijds of in het geheel geen actie kan ondernemen, dan volgt fase b.

b. een tweede rookmelder in dezelfde zone wordt geactiveerd;
- het tweede akoestisch alarm gaat af;
- de borden 'ontruiming' en 'niet betreden' worden verlicht;
- de wachttijd (gewoonlijk dertig seconden) voorafgaande aan de uitstoot van gas gaat in;
- een alarmmelding gaat uit naar de brandweer;
- in sommige ruimten wordt de computerhardware uitgezet;
- personeel ter plaatse heeft de keuze om ofwel de gasblusinstallatie af te sluiten, waarmee het aangeeft de brand te kunnen beheersen, ofwel het gebouw vóór de uitstoot te ontruimen;
- het gas wordt verspreid in tien tot zestig seconden;
- de gasconcentratie wordt lang genoeg op peil gehouden om het vuur te doven.

Deze procedure verschilt overigens van gebouw tot gebouw, met name voor wat betreft het tijdstip van het uitschakelen van de airconditioning en computerhardware en de alarmmelding bij de brandweer.

Voordelen

De voordelen van gasblusinstallaties zijn:
- branden kunnen doorgaans geblust worden zonder schade aan de apparatuur aangezien er geen water aan te pas komt;
- de storingstijd waarin de installaties niet gebruikt kunnen worden, blijft tot een minimum beperkt.

Nadelen

De nadelen zijn:
- sommige gassen zijn schadelijk voor het milieu doordat zij de ozonlaag dunner maken en het opwarmen van de aarde bevorderen;
- sommige van de beschikbare gassen produceren toch verbrandingsresten die materialen aantasten of zijn bijzonder giftig;
- sommige gassen veroorzaken overgevoeligheden van het hart bij de concentratie die benodigd is om te blussen;
- de meeste gassen zijn duur en de doorlopende kosten kunnen hoog zijn als vals-alarm-situaties tot uitstoot leiden.

ERVARINGEN IN HET VERLEDEN

De bouw van grote centrale computervoorzieningen vanaf midden jaren zestig tot laat in de jaren tachtig verhoogde het bewustzijn bij bedrijven over de potentiële verliezen als gevolg van brand, en vele van deze ruimten met hoogwaardige technologie werden voorzien van een gasblusinstallatie.

In de begintijd van computervoorzieningen werd vaak gekozen voor kooldioxide, maar de giftige eigenschappen bij de concentratie die benodigd is om te blussen en het afkoelingseffect (thermische schok) waarvan door sommige technici wordt aangenomen dat deze schade toebrengt aan elektronische apparatuur, verminderden de populariteit toen Halons beschikbaar kwamen.

De intrede van Halons en de bouw van computervoorzieningen voor mainframes waarop kritieke toepassingen draaien, resulteerde in het op grote schaal gebruiken van Halon-blusinstallaties. In Australië zijn de hoeveelheden Halon 1301 die gebruikt werden in nieuwe blusinstallaties aanzienlijk geweest, maar in de loop der tijd verminderd, van 220 ton in 1986 naar 38,9 ton in 1992 tot nihil in 1993. (Deze cijfers geven niet de totale hoeveelheid Halons die ook in andere varianten voorkomen in bestaande installaties in Australië.)

Waar deze systemen voor het overgrote deel technisch correct geïnstalleerd waren wat betreft het ontwerp van de leidingen, diameters van de leidingen, plaats van de uitstroomopeningen en gasconcentraties, droegen zaken die buiten de controle vielen van de installateur van het brandbeveiligingssysteem bij aan een verminderde effectiviteit van deze installaties:

- verzuim om het totale brandrisico van de ruimte die door de blusinstallatie wordt beschermd te beoordelen, zoals in het scenario hierboven;
- het wijzigen van het beveiligd gebied zonder overeenkomstige aanpassingen aan de blusinstallatie:
  - het optrekken van tussenmuren en het plaatsen van schotten zonder het aanbrengen van extra uitstroomopeningen en de daarmee verband houdende veranderingen aan het leidingstelsel;
  - het vergroten van het beveiligd gebied waardoor het gasvolume wordt teruggebracht tot onder het niveau dat benodigd is voor het bestrijden van de brand;
  - het aanbrengen van openingen in het beveiligde compartiment zonder adequate brandvertragende of zelfs helemaal geen voeringen;
- niet-toereikend onderhoud van de blusinstallatie zelf en het daarmee verband houdende rookdetectiesysteem;
- verzuim om de flessen na gebruik (meestal na een vals alarm of fout in de testprocedure) opnieuw te vullen vanwege de hoge kosten van het opnieuw vullen;
- de gasblusinstallatie op handbediening houden tegen valse alarms vanwege de hoge kosten van het hervullen of bezorgdheid over de veiligheid van het personeel.

MILIEU-EFFECTEN

Wat zijn de effecten? De milieu-effecten van de thans beschikbare blusinstallaties kunnen gemeten worden ten aanzien van:

- Het ozonverdunningspotentieel (ODP). Ozon in de atmosfeer vermindert het niveau van ultraviolette straling dat het aardoppervlak bereikt. Als de ozonlaag dunner wordt, neemt de ultraviolette straling toe, met een evenredig toegenomen risico op huidkanker, oogziekten, vermindering van sommige immuniteitsreacties en een afname van activiteiten in de landbouw en het leven in zee. Een meer recente methode om de stoffen die de ozonlaag dunner maken te beoordelen, is te bepalen op welke wijze deze bijdragen aan de totale hoeveelheid chloor in de stratosfeer. Bij het classificeren, implementeren en gebruik van gasinstallaties worden deze ozonverdunningspotentieelwaarden nog steeds gebruikt.

- Het potentieel van het opwarmen van de aarde (GWP). Het opwarmen van de aarde kan veranderingen teweegbrengen in de weerpatronen op aarde met mogelijke effecten op de landbouw en het leven in zee en het optreden van meer extreme weersomstandigheden in gebieden waar dit voorheen nauwelijks voorkwam.

- De levensduur (in jaren) in de atmosfeer gedurende welke de bovenstaande effecten blijven bestaan. De atmosferische levensduur voor vele van deze middelen is verrassend lang, variërend van 7 tot 10.000 jaar (theoretisch).

Het Protocol van Montreal uit 1987, dat werd gevolgd door de amendementen van Londen (1990) en Kopenhagen (1992), resulteerde in een internationale overeenkomst over het geleidelijk uit productie nemen van chemische stoffen met ODP- en GWP-potentieel. Onder dergelijke chemische stoffen vallen onder andere CFK's, Halons, tetrachloorkoolstof, methylchloroform en HCFK's (gehalogeneerde koolwaterstof), die alle op zeer uiteenlopende terreinen worden gebruikt, bijvoorbeeld voor koeling, brandbestrijding, productie van schuimrubber, schoonmaak en sterilisatie.

Eén gas dat al jaren wordt gebruikt in computerruimten en andere ruimten waar kritieke apparatuur staat opgesteld, is Halon 1301, met een ODP van 16. Ter vergelijking: dit ODP is iets minder dan zestien keer het ODP van de beter bekende en veel beschreven CFK- en HCFK-chemicaliën die worden gebruikt in spuitbussen en koelingssystemen, waarvan het gebruik thans geleidelijk wordt afgeschaft.

MILIEUVRIENDELIJKE ALTERNATIEVEN

De noodzaak om Halon 1301 af te schaffen voor alle behalve slechts enkele essentiële toepassingen resulteerde in een acuut probleem omdat effectieve en milieuvriendelijke alternatieven niet voorhanden waren. Op dit moment bestaan er nog geen 'kant-en-klare' vervangers die op bevredigende wijze alle eigenschappen van Halon 1301 vervangen. Er is echter een aantal alternatieven ontwikkeld die geschikt zijn voor computervoorzieningen. Deze zijn in tabel 1 opgenomen.

De beschikbaarheid van deze producten varieert per land en u zult dus ter plaatse moeten informeren.

De beschikbaarheid van een milieuvriendelijk 'kant-en-klaar' alternatief zou waarschijnlijk de status 'uitsluitend essentieel gebruik' van Halon overbodig maken, aangezien het vervangend product dezelfde werking zou hebben in uiterst kritieke toepassingen. Bovendien kunnen ook andere producten die een ODP- en GWP-waardering groter dan nul hebben, onderworpen worden aan regulering en afschaffing in de toekomst.

Bij het selecteren van een product voor toepassing in een computerruimte dient met een aantal factoren rekening te worden gehouden:
- beschikbaarheid van de producten;
- kosten van het gas, de installatie, het gebruiksklaar maken, de service en de vervanging van het gas;
- het vrijkomen van giftige of agressieve verbrandingsresten (voorzover van toepassing);
- schadelijke effecten op mensen, zoals hartovergevoeligheden (voorzover van toepassing);
- ODP- en GWP-factoren en de kans dat er in de

Blusmiddel	Formule	Toepassing	ODP	GWP	Atmosferische levensduur (in jaren)
Halon 1301		Ruimtevullend	16	0,8	107
R-595 (NAFG NAFSIII)	HCFC-123 (4,47%) HCFC-22 (82%) HCFC-124 (3,75%) Isopropenyl-l Methylcyclohexaan (3,75%)	Ruimtevullend	0,044	0,1	7
HFC-227 e.a. (Great Lakes FM200)	CF, CHFCF		0	0,6	42
HFC125 (Dupont FE25)	CF, CHF	Ruimtevullend	0	0,84	28
HGC23 (Dupont FE13)	CHF	Ruimtevullend	0	13	400
Kooldioxide (Pyrozene)	CO_2	Ruimtevullend	0	–	–
IG-541 (Tyco Inergen)	Stikstof (52%) Argon (40%) Kooldioxide (8%)		0	0	0
FC-3-1-10 (3M PF410)	C_2F_{12}	Ruimtevullend	0	18,2	2600
Water			0	0	
Schuimpoeder			0	0	

Tabel 1. Halon 1301 en mogelijke alternatieven.

toekomst beperkingen aan het product zullen worden opgelegd;
- de door de fabrikant aanbevolen installatiemethoden en hun compatibiliteit met bestaande apparatuur.

Het valt buiten de reikwijdte van dit artikel om de beschikbare producten op een technisch niveau te vergelijken. Gekwalificeerde consultants op het gebied van brandbeveiliging kunnen deze service echter wel verlenen.

GASBLUSSING – IS HET DE BESTE OPLOSSING?

Het is niet zo dat een gasblusinstallatie altijd de meest geschikte oplossing is, omdat situaties aanzienlijk kunnen verschillen en er andere systemen beschikbaar zijn voor brandmelding, het bestrijden van brand en het weren daarvan.

Een gasblusinstallatie is waarschijnlijk het meest geschikt indien:
- een onderbreking van de bedrijfsactiviteiten, zelfs voor korte tijd, een aanzienlijk negatief effect zou hebben op het bedrijf;
- de tijd die nodig is om de omgeving te herstellen of te zorgen voor een alternatieve omgeving de voor het bedrijf acceptabele periode zou overschrijden;
- er geen belangrijke budgettaire beperkingen zijn;
- er reeds prioriteit is verleend aan:
  - vroegtijdige alarmering door rookdetectiemelding;
  - het in kaart brengen van het brandrisico en isolatie van het te beveiligen gebied;
  - het verwijderen van ontvlambare materialen uit het beveiligd gebied;
- snelle brandbestrijding een kwestie van leven of dood is.

Een gasblusinstallatie is waarschijnlijk minder geschikt indien:
- een onderbreking van de bedrijfsactiviteiten voor korte tijd geen groot negatief effect op het bedrijf zou hebben;
- de tijd die nodig is om de omgeving te herstellen of een alternatieve omgeving te creëren binnen de voor het bedrijf acceptabele periode valt;
- er aanzienlijke budgettaire beperkingen bestaan;
- er nog geen prioriteit is verleend aan:
  - vroegtijdige alarmering door rookdetectiemelding;
  - het in kaart brengen van het brandrisico en isolatie van het te beveiligen gebied;
  - het verwijderen van ontvlambare materialen uit het beveiligd gebied;

Brandbestrijdings-systeem	Ontstekings-mechanisme	Uitwerking op mensen	Uitwerking op apparatuur	Schoonmaakvereisten
Gasblusinstallatie	Rookdetectie – door vroegtijdige waar-schuwings- of plaats-detectoren.	Varieert van giftig na een korte blootstelling tot niet-giftig, zelfs na lang-durige blootstelling.	Sommige gassen genereren corrosieve verbindingen indien bloot-gesteld aan vuur. Thermische schok kan een probleem vormen.	Gas afzuigen. Brandschade kan schoonmaakbeurt vereisen. De isolatie van het compartiment kan be-schadigd zijn, indien niet adequaat ontworpen.
Sprinklerinstallatie	Hitte direct op koppen van de sprinklerinstallatie.	Men wordt nat. Letsel kan optreden als gevolg van de brand.	Als de apparatuur draait, kan grote schade ontstaan door het water. Het vuur zal waarschijnlijk schade veroorzaken.	Meestal aanzienlijk, omdat het vuur doordringt voordat de sprinklerinstallatie in werking treedt, en als gevolg van het water.
'Pre-action' sprinklerinstallatie	Rookdetectie – door vroegtijdige waar-schuwings- of plaats-detectoren, hitte vervol-gens direct op de koppen van de sprinklerinstallatie.	Men wordt nat. Letsel kan optreden als gevolg van de brand.	Als de apparatuur draait, kan grote schade ontstaan door het water. Het vuur zal waarschijnlijk schade veroorzaken.	Meestal aanzienlijk, omdat het vuur doordringt voordat de sprinklerinstallatie in werking treedt, en als gevolg van het water.
Waternevel	Rookdetectie – door vroegtijdige waar-schuwings- of plaats-detectoren.	Men wordt nat.	Als de apparatuur draait, kan schade ontstaan door het water, anderszins minimaal.	Schoonmaakbeurt vereist als gevolg van water en vuur, maar kan minimaal zijn bij vroegtijdige detectie.

Tabel 2. Gas en alternatieve systemen.

- snelle brandbestrijding gewenst is maar geen kwestie is van leven of dood;
- het niet mogelijk is alle punten met een hoge prioriteit in actie om te zetten als gevolg van fysieke beperkingen.

Het blussen met gas versus alternatieve systemen

Soms ontstaat er verwarring met betrekking tot de relatieve voor- en nadelen van gasbrandbestrijdingssystemen versus andere brandbestrijdingsmethoden. Tabel 2 geeft de belangrijkste aspecten van een aantal alternatieven.

HET UIT GEBRUIK NEMEN EN VERNIETIGEN VAN HALON 1301

De schadelijke effecten van Halon 1301 voor het milieu brengen met zich mee dat het in de atmosfeer brengen hiervan in vele landen is verboden, waardoor het noodzakelijk is dat men zich er op een aanvaardbare wijze van ontdoet.

Op dit moment worden daarvoor twee methoden toegepast:

- opslag, totdat er veilige methoden voor verwijdering beschikbaar zijn in de regio;
- vernietigen, waarbij gebruik wordt gemaakt van installaties die met een speciale plasmaboog extreem hoge temperaturen genereren en de chemische stoffen afbreken.

Sommige autoriteiten verkozen Halon over te nemen en gratis op te slaan om vervolgens kosten in rekening te brengen voor opslag of vernietiging nadat voldoende voorraad was opgebouwd. Op het moment van schrijven berekent het Australische Department of Administrative Services bijvoorbeeld 19,5 (Aus)dollar per kilo om Halon 1301 te vernietigen. Dit lijkt goedkoop, totdat men zich realiseert dat de opslag voor een grote computerruimte in totaal gemakkelijk 1000 kg kan bevatten.

CONCLUSIE

Samenvattend kan worden gesteld dat de beslissing welk alternatief het meest geschikt is als vervanger van Halon afhangt van een aantal belangrijke aspecten:

- de opvangcapaciteit van het bedrijf ten aanzien van onderbrekingen;
- de kosten van een totaaloplossing voor beveiliging, inclusief detectie, inschatten van integrale brandrisico's en brandbestrijding;
- fysieke beperkingen;
- het beleid van de organisatie ten aanzien van verantwoordelijkheid voor het milieu en de veiligheid van het personeel.

Men bedenke wel steeds dat een gasblusinstallatie slechts één onderdeel is van een beleid voor brandbeveiliging en dat het niet de juiste oplossing behoeft te zijn. In het meest ongunstige geval kan het pure geldverspilling betekenen.

G. Doddrell
Is senior manager bij de KPMG Information Security Group, Melbourne, Australië. Hij heeft een uitgebreide ervaring met de implementatie van beheersystemen en bedrijfsbrede continuïteitsplanningen. Hij heeft een reeks van publicaties op deze gebieden op zijn naam staan.

COBIT - CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY

Drs. R.G.A. Fijneman RE RA

EDP AUDITORIUM

Inleiding

In het voorjaar van 1996 is het CobiT-framework gepubliceerd door de Information Systems Audit and Control Foundation ([ISAC96]). Dit framework is in ISACA-verband internationaal ontwikkeld. De aanleiding voor deze ontwikkeling vormde de geconstateerde behoefte aan een systeem (structuur) van interne controle voor informatietechnologie (IT). Daarbij wenste ISACA de materie niet puur technisch te benaderen, maar primair vanuit een 'business'-invalshoek de interne controles te definiëren.

De behoefte aan eenduidige normen is ook in de Nederlandse EDP-auditpraktijk waarneembaar. Ook hier tekent de tendens zich af dat EDP-auditors optimaal proberen aan te sluiten bij de wijze waarop het management van een organisatie de informatietechnologie beheert. Deze management control- (of business control-) benadering wordt in toenemende mate tevens in de financial audit door certificerende accountants gevolgd.
Het vaststellen van de door de te beoordelen organisatie gehanteerde normen voor het beheersen van haar processen is hierbij veelal nog een lastig punt. CobiT beoogt voor de informatietechnologie een structuur aan te reiken, die in internationaal verband bruikbaar is. In deze 'business'-organisatienormen zijn ook normen opgenomen ten aanzien van beveiliging. Dit maakt dat het model in principe ook benut kan worden bij door EDP-auditors uit te voeren beveiligingsonderzoeken (bijvoorbeeld in het kader van een third party-onderzoek). Hierna wordt nader ingegaan op de inhoud van CobiT en op de relatie tussen CobiT en andere normenstelsels, en volgen enkele afsluitende conclusies. In het IS Audit & Control Journal van ISACA ([ISCJ96]) wordt uitgebreider op deze materie ingegaan.

Inhoud CobiT

De primaire invalshoek binnen CobiT is de business-oriëntatie. Het doelstellingenmodel is bedoeld als een hulpmiddel voor de proceseigenaren binnen organisaties bij het realiseren van de beheersing van informatietechnologie. Het uitgangspunt daarbij is dat IT-resources beheerd dienen te worden door IT-processen, die logischerwijs zijn gegroepeerd om kwalitatief afdoende informatie te genereren. De onderkende IT-resources zijn: mensen, applicaties, hardware en systeemsoftware, faciliteiten en gegevens. De IT-processen zijn in vier groepen ingedeeld:
- planning en organisatie;
- acquisitie en implementatie;
- levering en support;
- monitoring.

In totaal zijn 32 processen ondergebracht in bovenstaande vier groepen, waarvoor algemene beheersdoelstellingen zijn vastgesteld. Een IT-beheersdoelstelling is daarbij gedefinieerd als een omschrijving van het gewenste resultaat, dat bereikt kan worden door het implementeren van procedures in de IT-processen en -activiteiten. De beheersing is gericht op alle kwaliteitscriteria en beperkt zich niet tot beveiliging alleen.
De beheersdoelstellingen zijn gebaseerd op bestaande standaarden of ontleend aan 'best practices'. Tijdens het onderzoek zijn diverse bronnen geraadpleegd; voorbeelden daarvan zijn de Code of Conduct (in Nederland beter bekend als de Code voor Informatiebeveiliging), COSO report, ISO 9000-standaarden, etc.
Recentelijk zijn aansluitend op de 32 onderkende processen de audit guidelines vastgesteld. Daarbij zijn de uit te voeren auditwerkzaamheden (o.a. interviews, verificatie, e.d.) niet per beheersdoelstelling uitgewerkt, aangezien daarbij te veel redundantie zou optreden. Indien relevante doelstellingen worden geselecteerd, dienen de audit guidelines nader te worden uitgewerkt.

Relatie CobiT en andere beheersmodellen

Het CobiT-model valt te positioneren tussen de 'business control'-modellen (zoals COSO) en de meer gespecialiseerde modellen voor informatietechnologie (technologische standaarden). Er wordt met andere woorden een brugfunctie opgezet. Tabel 1 bevat een overzicht van een aantal bestaande 'control'-modellen.

In het IS Audit & Control Journal ([ISCJ96]) is een meer uitgebreide vergelijking opgenomen tussen CobiT, SAC94, COSO92 en SAS 55/78. Indien CobiT wordt gerelateerd aan de Code voor Informatiebeveiliging valt direct op dat CobiT het gehele kwaliteitsspectrum in en rondom de IT-processen beoogt af te dekken. De Code voor Informatiebeveiliging richt zich daarentegen primair op kwaliteitscriteria als integriteit, exclusiviteit en controleerbaarheid.

Conclusies

De eerste gedachte bij CobiT kan zijn dat het meer van hetzelfde is. Wederom een checklist, wellicht iets anders ingedeeld, maar toch. De EDP-auditor kent daarvan al diverse voorbeelden. Bij een nadere bestudering van CobiT is echter een aantal voordelen te onderkennen:
- *de internationale toepasbaarheid.* Gezien de toenemende internationalisatie van organisaties

Tabel 1. Comparison of Control Concepts. Bron: A comparison of Internal Controls: CobiT, SAC, COSO and SAS 55/78 (IS Audit & Control Journal, volume IV, 1996).

	CobiT	SAC	COSO	SASs 55/78
Primary Audience	Management, users, information system auditors	Internal Auditors	Management	External Auditors
IC viewed as a	Set of processes including policies, procedures, practices, and organizational structures	Set of processes, subsystems, and people	Process	Process
IC Objectives	Effective & efficient operations. Confidentiality, Integrity and Availability of information. Reliable financial reporting. Compliance with laws & regulations.	Effective & efficient operations. Reliable financial reporting. Compliance with laws & regulations.	Effective & efficient operations. Reliable financial reporting. Compliance with laws & regulations.	Reliable financial reporting. Effective & efficient operations. Compliance with laws & regulations.
Components of Domains	Domains: Planning and organization. Acquisition and implementation. Delivery and support. Monitoring.	Components: Control Environment. Manual & Automated Systems Control Procedures.	Components: Control Environment. Risk Management Control Activities. Information & Communication. Monitoring.	Components: Control Environment. Risk Assessment Control Activities. Information & Communication. Monitoring.
Focus	Information Technology	Information Technology	Overall Entity	Financial Statement
IC Effectiveness	For a period of time	For a period of time	At a point in time	For a period of time
Responsibility for IC System	Management	Management	Management	Management
Size	187 pages in four documents	1193 pages in twelve modules	353 pages in four volumes	63 pages in two documents

en de inzet van informatietechnologie is het van belang om internationaal bruikbare normen en kaders beschikbaar te hebben.
- *een bedrijfsmatige benadering*. Het gedefinieerde model volgt de business-benadering van informatietechnologie. De auditor kan aansluiting bij deze benadering zoeken.
- *de brede benadering van kwaliteit*. Niet alleen beveiliging wordt uitgewerkt als kwaliteitscriterium, maar alle relevante kwaliteitscriteria.

Indien het management van een organisatie voor de beheersing van de informatietechnologie het CobiT-model hanteert, kan de EDP-auditor hierbij optimaal aansluiten. Zo is het denkbaar dat in het kader van bijvoorbeeld een third party review-onderzoek het CobiT-model als normstelling wordt gehanteerd door de EDP-auditor. De auditor dient dan de relevante doelstellingen uit het model te selecteren. Aanvullend zal de auditor, afhankelijk van de aangetroffen verwerkingsomgeving (mainframe, PC-netwerk, minisystemen), de in CobiT algemeen geformuleerde doelstellingen specifiek moeten maken.

De mate waarin het CobiT-model operationeel wordt ingezet door organisaties voor het beheer van informatietechnologie zal in de komende jaren moeten blijken. De EDP-auditor kan daarbij een stimulerende rol vervullen.

Literatuur

[ISAC96] Information Systems Audit and Control Foundation, CobiT executive summary, 1996; CobiT framework, 1996; CobiT control objectives, 1996; CobiT audit guidelines, 1996.

[ISCJ96] IS Audit & Control Journal, *A comparison of Internal Controls: CobiT, SAC, COSO, and SAS 55/78*, volume IV, 1996.

[SAC94] Institute of Internal Auditors Research Foundation, *Systems Auditability and Control*, 1994.

[COSO92] Committee of Sponsoring Organisations of the Treadway Commission, *Internal Control – Integrated Framework*, AICPA, Jersey City 1992.

[SAS88] SAS, *Consideration of the Internal Control Structure in a Financial Statement Audit*, SAS 55, Institute of CPAs, en *Consideration of Internal Control in a Financial Statement audit: An amendment to SAS 55*, SAS 78, Institute of CPAs, 1988.

KPMG EDP Auditors
Samsom BedrijfsInformatie