ECONSTOR
Make Your Publications Visible.

A Service of
ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Bruwer, P. J.S.

Article

'n Strategiese bestuursbenadering tot sekuriteit en beheer binne 'n komplekse gerekenariseerde inligtingstelselomgewing

South African Journal of Business Management

Provided in Cooperation with:
University of Stellenbosch Business School (USB), Bellville, South Africa

Suggested Citation: Bruwer, P. J.S. (1991) : 'n Strategiese bestuursbenadering tot sekuriteit en beheer binne 'n komplekse gerekenariseerde inligtingstelselomgewing, South African Journal of Business Management, ISSN 2078-5976, African Online Scientific Information Systems (AOSIS), Cape Town, Vol. 22, Iss. 1/2, pp. 16-21,
https://doi.org/10.4102/sajbm.v22i1/2.894

This Version is available at:
https://hdl.handle.net/10419/218064

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

https://creativecommons.org/licenses/by/4.0/

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

'n Strategiese bestuursbenadering tot sekuriteit en beheer binne 'n komplekse gerekenariseerde inligtingstelselomgewing

P.J.S. Bruwer
Nagraadse Skool vir Bestuurswese, PU vir CHO, Potchefstroom 2520, Republiek van Suid-Afrika

Ontvang 1 Februarie 1990; aanvaar 20 April 1990

Rekenaarsekuriteit en -beheer word oor die algemeen erken as 'n noodsaaklikheid, maar min word werklik gedoen om rekenaarsekuriteit en -beheer ten uitvoer te bring. Gewoonlik word daar eers opgetree en hulpbronne geallokeer nadat insidente soos bedrog, diefstal en skade plaasgevind het. Situasies wat ook voorkom, is dat daar wel gedokumenteerde beplanning, stelsels, prosedures en beleid bestaan, maar nie toegepas word nie of dat min of geen amptelike beleid bestaan nie, maar dat daar wel 'n mate van instinktiewe beheer toegepas word. Binne die huidige Suid-Afrikaanse milieu is die volgende elemente teenwoordig: Bedrog en diefstal; terrorisme en sabotasie; sanksies en boikotte; disinvestering en isolasie; bankrotskappe en likwidasie; oproer en stakings. Bestuur is reeds vir 'n geruime tyd afhanklik van, en sal in 'n toenemende mate ten volle afhanklik raak van gerekenariseerde inligting en inligtingstelsels vir vinnige, betroubare en akkurate besluitneming. Daar bestaan dus 'n noodsaaklike behoefte na en verantwoordelikheid om die bron en die basis vir voortbestaan te beskerm en te beheer. Die oogmerk van hierdie navorsingsprojek was om die onderliggende probleme met betrekking tot rekenaarsekuriteit en -beheer te ondersoek en faktore wat tot die huidige bedeling aanleiding gee, te ontleed. Verder is daar gepoog om 'n bestuursbenadering voor te stel wat aandui hoe daar te werk gegaan kan word om essensiële maatreëls daar te stel deur middel van 'n strategiese/funksionele proses.

A strategical management approach towards security and control within a complex computerized information system environment In a dinamic technological computer environment it is essential for management to establish a logical and systematic process to protect, secure and safeguard the management information resources and assets in such a manner to minimize risks, threats and exposures to a satisfactory and acceptable level. To achieve the objectives of total security implementation it is essential to identify the problems and factors (for example risks, threats and exposures) that might have an impact on computer security and control. It is necessary to define and understand computer security and control and important to assess the current situation to provide an implementation methodology to cover and enhance areas for improvement. In this research project a strategic management process approach is suggested to enable management to formulate and implement a strategy for security and control in a complex computerized information system environment.

Inleiding

Probleme met betrekking tot rekenaarsekuriteit

Probleme met betrekking tot rekenaarsekuriteit kan in drie areas verdeel word, naamlik:
— Tegnologie-vordering
— Agterstand van belangrike ondersteunende hulpfunksies
— Opsetlik veroorsaakte verliese

Parker verwys na die probleme as

> 'technology advances, development of important supportive functions that protect the technology from intentional losses in lagging behind. One reason is that the human capability to development of complex systems of today is being taxed to its limits. Computer security is another supportive function that is not keeping up with the advancement of technology. A fundamental problem with cases of intentionally caused losses is the transition in forms of negotiable assets needing "protection"' (1983: 9).

Vraag na gevorderde rekenaarsekuriteit

Konsentrasie van groter en meer komplekse toepassingsverwerkingstelsels

Fine beweer dat

> 'probably the main reason for greater computer risk is the increasing number of computer applications and the consequent concentration of information and processing' (1986: 3).

'n Toenemende neiging na groter en meer komplekse stelsels wat van intydse verwerking gebruik maak en gewoonlik uit groot en gesofistikeerde databasisse bestaan, is verdere komplikasies. Die kompleksiteit van toepassings neem ook toe met groter gesofistikeerde, toegedeelde en ingeskakelde netwerke.

Aangewesenheid op sleutelpersoneel

Die aangewesenheid op sekere sleutelpersoneel plaas die organisasie in die hande van 'n relatief beperkte aantal individue. Hierdie spesialisgroep het dikwels unieke en ongedokumenteerde kennis van wysigings aan, of die bedryf van programmatuur. Kontrole oor hul werk is uiters moeilik.

Verdwyning van tradisionele kontroles

Die meeste van die nuwe toepassingstelsels maak nie vir die tradisionele ouditspoor of hardekopie-kontroles voorsiening nie. Die nuwe toepassingstelsels bevat outomatiese kontroles om sodoende die integriteit van data wat verwerk word, te verseker.

Rekenaarbedrog, -misdaad en -misbruik

Volgens Parker (1983: 210) word rekenaarbedrog gepleeg wanneer 'n persoon ongemagtigde toegang het, veranderings aan enige rekenaar, rekenaarstelsel, rekenaarnetwerk of enige deel van 'n rekenaar aanbring, skade of vernietigingsaksies laat geskied by wyse van valse voorwendsels of voorstellings met die voorneme om bates of dienste te beheer.

Met die toenemende rol wat die gebruik en belangrikheid van rekenaars in ons samelewing speel, sal rekenaarbedrog

en -misdaad toenemend 'n invloed en impak op 'n organisasie hê. 'n Groeiende tendens in rekenaarbedrog en rekenaarmisdaad is reeds bespeur in die Verenigde State van Amerika, die Verenigde Koninkryk en selfs in die Republiek van Suid-Afrika.

Navorsing deur die Business Computer Information Systems College of Business Administration, North Texas State University onder leiding van Richards (1986: 15–24) het tot interessante bevindings in die Verenigde State van Amerika gelei.

Die studie toon individuele jaarlikse verliesreekse wat strek vanaf $145 tot $730 miljoen en is op inligting gebaseer wat deur 72 firmas van die American Bar Association verskaf is.

— Altesaam 16% van die 119 gevalle van bedrog wat deur die Instituut van Gesertifiseerde Rekenmeesters en Ouditeure (AICPA) geïdentifiseer is, oorskry $100 000.
— 22% van die 67 gevalle van bedrog wat deur die Inspekteur van plaaslike Besture ondersoek is, oorskry $100 000.
— 12% van die 65 gevalle van bedrog wat deur die Inspekteur-Generaal ondersoek is, oorskry $100 000.
— Kredietkaartbedrog het in dollarwaarde van $5,5 miljoen tot $29,2 miljoen oor die twaalf maande van 1981 tot 1982 toegeneem. Dit is 'n toename van 430% in hierdie tipe bedrog.

Rekenaarmisdaad vir rekenaargebaseerde ondernemings in Suid-Afrika word op R140 miljoen geraam gedurende 1986 (Anon. 1986: 27). Rekenaarkonsultante wat die misdaadtendens monitor, is van mening dat die misbruik van die rekenaar aan die toeneem is. 'n Waarskuwing word gerig dat die situasie sal vererger en dat verliese sal groei tensy daar aan basiese beginsels van rekenaarsekuriteit en -beheer voldoen word en ondernemings effektiewe teenmaatreëls implementeer.

Navorsingsmetodiek

Die navorsingsmetodiek wat gebruik is, behels die volgende:

— 'n Literatuurstudie van gesaghebbende partye op die gebied van rekenaarsekuriteit en -beheer, asook 'n wye spektrum van aktuele artikels, geskrifte en publikasies.
— Ontleding en vertolking van onlangse bevindinge van navorsers met betrekking tot die huidige situasie van rekenaarsekuriteit binne Suid-Afrika, die Verenigde State van Amerika en die Verenigde Koninkryk.
— Kontak en gespreksvoeringe met kundiges van die volgende instellings:
  * Rekenaarvereniging van SA (CSSA)
  * Instituut van Geoktrooieerde Rekenmeesters (SA)
  * Instituut van Interne Ouditeure (SA)

'n Strategiese bestuursbenadering

Met inagneming van die dinamies-veranderende gerekenariseerde inligtingstelselomgewing, die bedreigings, blootstellings en risiko's asook bevindinge ten opsigte van die huidige situasie van rekenaarsekuriteit en -beheer, word daar vervolgens 'n bestuursbenadering voorgestel wat aandui hoe daar te werk gegaan kan word om essensiële maatreëls daar te stel deur middel van 'n strategiese/funksionele proses.

Die strategiese en funksionele of operasionele bestuursprosesse kan egter nie los van mekaar gesien word nie. 'n Strategiese bestuursproses is gerig op die langtermynoorlewing en groei van 'n onderneming en die funksionele proses is gerig op korttermynoorlewing.

Die strategiese proses is dus 'n hulpmiddel vir organisasies en departemente om langtermynoogmerke te stel en die middele te bepaal hoe daardie oogmerke bereik kan word. Die organisasie bepaal dus wat die oogmerke nou is, waar hulle dit wil hê en hoe om dit te bereik.

Rekenaarsekuriteit-strategie-formuleringsproses

Binne 'n dinamiese gerekenariseerde inligtingstelselomgewing is dit uiters noodsaaklik vir 'n organisasie om wel oor 'n rekenaarinligtingstelselstrategie te beskik, wat ook rekenaarsekuriteit en -beheer as integrale deel van die strategie insluit.

Strategiese formuleringsmodelle verskil in die literatuur hoofsaaklik vanweë die graad van eksplisietheid, detail en kompleksiteit. Daar is verskillende outeurs wat verskillende sieninge het, maar die meeste sluit die basiese elemente en stappe in.

Die strategiese formuleringsproses word volgens Hofer en Schendel (1978: 46,47) gesien as 'n spesiale soort probleemoplossingsproses vir die definiëring van 'n organisasie se strategie. 'n Hersiening van die belangrikste voorskrywende strategieformuleringsmodelle sluit óf eksplisiet óf implisiet die volgende sewe stappe in:

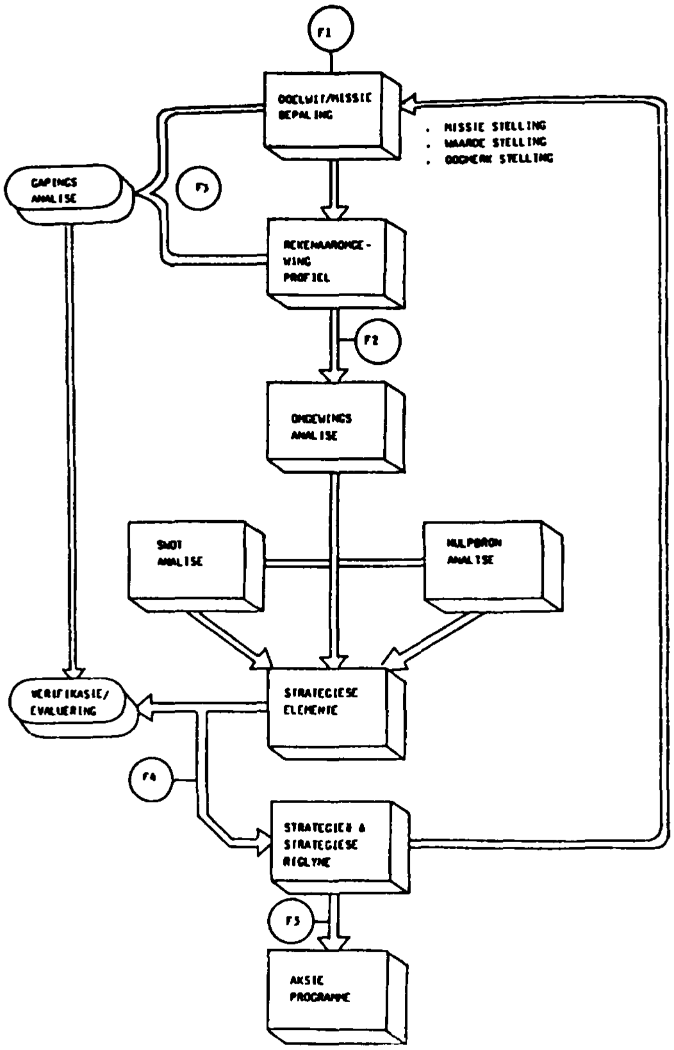
— Strategie-identifisering is die bepaling van die organisasie se huidige strategie en strategiese komponente.
— Fase 2 (F2) behels die ontleding van die rekenaaromgewing aan die hand van die rekenaaromgewingsprofiel, die sterk en swak punte en geleenthede/bedreigings (SWOT-analise) en die hulpbronne wat beskikbaar is om die geleenthede en bedreigings die hoof te bied. Die eindresultaat van die verskillende analise word vervat in strategiese elemente.
— Fase 3 (F3) is 'n proses waardeur die huidige strategie (in fase 1) vergelyk word met die strategiese elemente wat in fase 2 geïdentifiseer is.
— Fase 4 (F4) sluit eerstens die identifisering van alternatiewe strategiese elemente in. Tweedens word die strategiese opsies vir implementering geëvalueer en geselekteer. Laastens en baie belangrik word die doelwit/missie van die onderneming aangepas by die strategiese oogmerke.
— Fase 5 (F5) behels die formulering van aksieplanne/programme waarin uitgespel word hoe, wanneer en deur wie die strategie geïmplementeer en in bedryf gestel word.

Hierdie fases word skematies in Figuur 1 aangetoon.

Doelstellingbepaling

Daar word tans algemeen aanvaar dat daar 'n hiërargie van doelwitte in 'n onderneming bestaan, net soos daar 'n hiërargie van bestuurders bestaan.

Aangesien bestuurders in verskeie vlakke van die onderneming met verskillende vlakke van die omgewing in wisselwerking is, kan aanvaar word dat die aard van die



Figuur 1 'n Strategiese formuleringsprosesmodel (Bezuidenhout 1988:99)

doelwitte in die verskillende vlakke van die onderneming sal verskil. Soos wat daar vertikaal in die hiërargie van die onderneming beweeg word, word die doelwitte meer algemeen en omvat dit 'n groter persentasie van die totale doelwitte van die onderneming. Die doelwitte wat vervat is in die topstruktuur van die onderneming staan bekend as korporatiewe doelwitte.

Doelstellingbepaling bestaan uit drie fisiese komponente:

— Missiestelling is langtermyngerig en word oorkoepelend geformuleer.
— Waardestelling is 'n verbintenis en konsensus deur alle belanghebbende partye waarbinne die toekomstige klimaat geskep word.
— Oogmerkstelling is die bepaling van realistiese, bereikbare en meetbare oogmerke.

Aangesien doelwitte en oogmerke somtyds as sinonieme deur die bestuursliteratuur gebruik word, is dit belangrik om 'n onderskeid tussen die twee terme te tref. Hofer en Schendel onderskei soos volg:

> 'goals are the ultimate, long-run, open-ended attributes or ends a person or organization seeks, while objectives are the intermediate-term targets that are necessary but not sufficient for the satisfaction of goals' (1978: 20).

Missiestelling

Die missiestelling is 'n uitgebreide standpunt of stelling van wat die onderneming/departemente oor die lang termyn wil bereik met betrekking tot rekenaarsekuriteit en -beheer deur die daarstelling van mikpunte of langtermyndoelwitte oorkoepelend te formuleer.

Waardestelling

Die waardestelling verskaf 'n basiese begrip en aanvaarding wat deur konsensus en verbondenheid deur die betrokke partye vanuit die missiestelling lei. Die waardestelling bevat verder ook waardes waaroor daar beskik moet word in die inligtingstelseldepartement asook 'n omvattende definisie van wat rekenaarsekuriteit en -beheer behels en wat dit beteken.

Die omgewingsklimaat dui aan waarin en waarheen rekenaarsekuriteit en -beheer beweeg.

Voortspruitend uit die missiestelling en waardestelling volg die oogmerkstelling.

Oogmerkstelling

Oogmerke word deur Gleuck en Jauch (1984: 73) gedefinieer as: 'Objectives are those ends which the organization seeks to achieve through its existence and operations'. Oogmerke is basiese mylpale in 'n nimmereindigende navolging van doelwitte.

Oogmerkstelling vir rekenaarsekuriteit en -beheer kan algemeen en spesifiek gerig wees.

Algemene oogmerke bevat aspekte soos rekenaarbedrog, -misdaad en -misbruik. Verder behoort oogmerkstellings ook daarop gerig te wees om rekenaaromgewingsrisiko's, -blootstellings en -bedreigings te minimaliseer en selfs uit te skakel.

Die EDP Auditors Foundation (1983: 5) onderskei vyf hoofkontrole-areas wat elk ingedeel is in spesifieke kontrole-oogmerke.

Die hoofoogmerkareas is:

— Bestuurskontroles
— Algemene inligtingstelselkontroles: stelselontwerp-, ontwikkeling- en instandhoudingkontroles
— Algemene inligtingstelselkontroles: bedryf
— Toepassingstelselkontroles
— Tegnologiese kontroles, waaronder databasisondersteunde stelsels, verspreide verwerking en netwerkbedryf, mikro-rekenaars en rekenaartyddeling

Rekenaaromgewingsprofiel

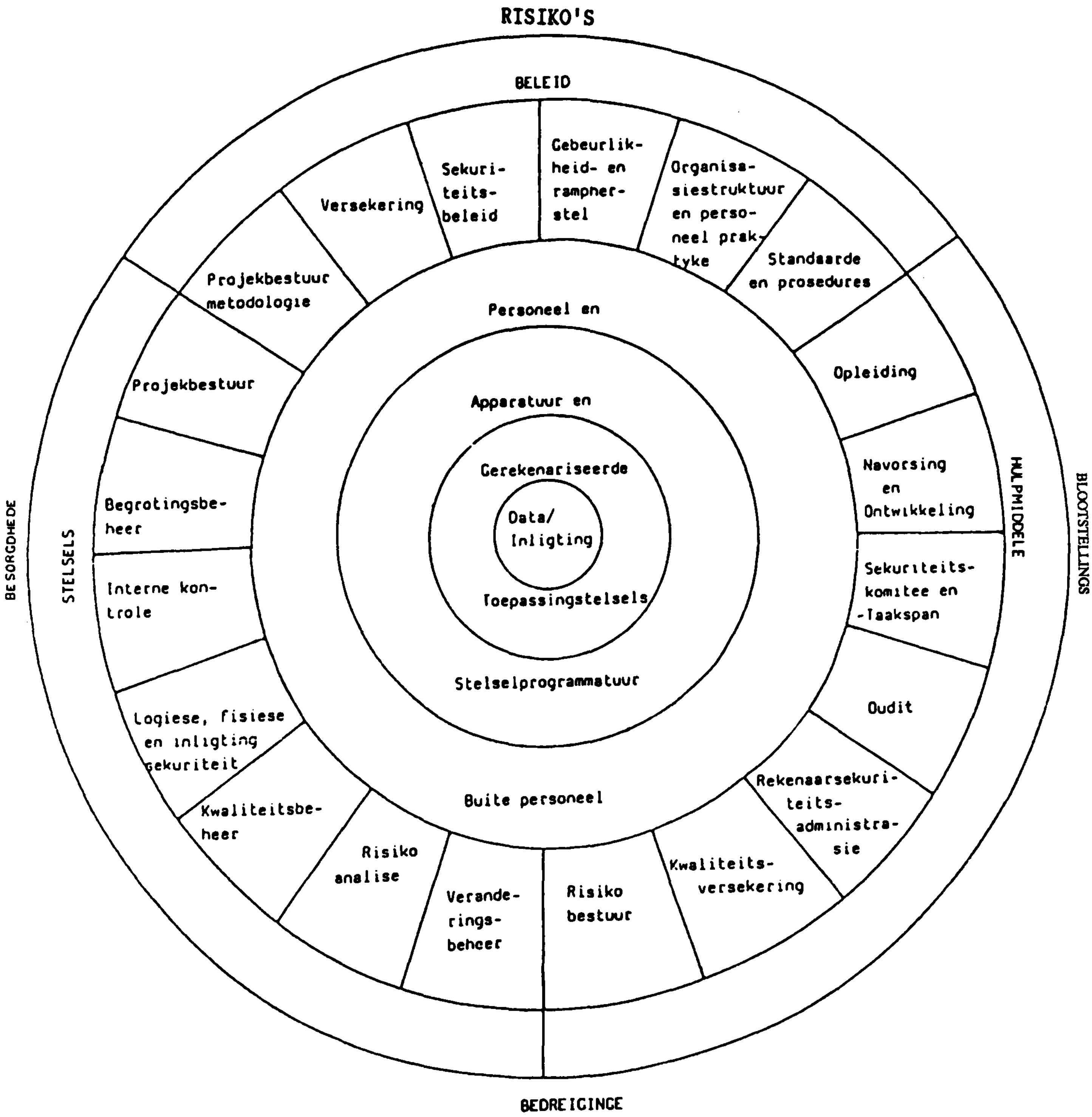
Die rekenaaromgewingsprofiel is uniek tot elke organisasie en word saamgestel uit verskeie kombinasies van rekenaaromgewingskomponente.

Die oogmerk van hierdie aksie is om die rekenaaromgewingskomponente te identifiseer en te definieer.

Fitzgerald (1984: 101–157) verwys na 'n verskeidenheid rekenaaromgewingskomponente, waarvan die volgende die belangrikste is:

— Bedryfsprosesdures oor data-invoere en -afvoere
— Data-invoertoerusting en intydse terminale
— Modems en multipleksors/konsentreerders/skakelaars
— Kommunikasielyne en kommunikasiebeheereenhede

— Stelselprogramme, beheer oor databasis en datakommunikasie
— Databasis, databasisadministrasie, -bedryfstandaarde en 'n datawoordeboek
— Afvoerintegriteit van toepassingsprogramme en afvoertoerusting
— Rekenaarapparatuur-beheermeganismes
— Persooneelpraktyke en maatreëls met betrekking tot die databasis
— Rekenaarsentrum, datakommunikasie, -invoere, intydse terminale, data-afvoere en stelselprogramme
— Rekenaarsekuriteitadministrasie
— Beheerbeleid
— Rekenaarsentrumkomponente waaronder lugversorging, gebeurlikheidsbeplanning, elektrisiteitgenerators, fasiliteite, versekering, bestuursbeleid en opleidingsprogramme
— Fisiese sekuriteit
— Stelselprogrammatuur en gebruikerdokumentasie
— Stelsel- en programlêers.



Figuur 2 Geïntergreerde rekenaarsekuriteit- en -beheerraamwerk binne 'n komplekse gerekenariseerde inligtingstelselomgewing (Bezuidenhout, 1988:109)

Omgewingsanalise

Gleuck en Jauch (1984: 122) reken 'n belangrike taak van topbestuur is om die omstandighede te skets vir effektiewe ontleding en diagnose van die omgewing. Die bestuur moet bepaal wat die mees kritiese faktore in die omgewing is. Dié kritiese faktore sal op hul beurt bepaal watter inligting ingewin moet word en waar, en deur wie in die onderneming dit ontleed en gediagnoseer moet word. Die onderneming sluit faktore van sektore buite die organisasie, wat kan lei tot geleenthede of bedreigings, in.

Die oogmerk met die omgewingsanalise is om vanuit die rekenaaromgewingsprofiel die omgewing te ontleed en aan die hand van scenario's die toekomstige tendens van die omgewing te bepaal.

Hulpbronanalise

Die oogmerk met die hulpbronanalise is hoofsaaklik om die hulpbronne wat beskikbaar is en beskikbaar mag wees, te identifiseer en te ontleed.

Die hulpbronne is die interne komponente wat tot die beskikking van 'n organisasie mag wees en wat aangewend kan word om die verwagte tendense in die rekenaaromgewing en eksterne omgewing te akkomodeer.

Hulpbronne kan geïdentifiseer word aan die hand van Figuur 2 met betrekking tot beleid, stelsels en hulpmiddele.

Sterkpunte/swakpunte en geleenthede/bedreigings: (SWOT)-analise

Die oogmerk is om die sterkpunte en swakpunte te identifiseer en te omskryf met betrekking tot effektiwiteit, doeltreffendheid en volledigheid van rekenaarsekuriteit en kontroleareas, asook toekomstige areas wat geïdentifiseer is. Die verwagte sterk- en swakpunte moet ook beskryf word aan die hand van omgewingsontledings en scenario's.

Die bedreigings, blootstellings en risiko's, asook enige ander toepaslike bedreigings of toekomstige bedreigings moet geïdentifiseer, omskryf en ontleed word.

Strategiese elemente

Die strategiese elemente is die eindresultaat van die kritiese omgewingsveranderlikes (vanuit die omgewingsanalise), die kritiese sterkpunte/swakpunte en geleenthede/bedreigings (vanuit die SWOT-analise) en die kritiese hulpbronne (vanuit die hulpbronanalise).

Strategiese elemente kan geïdentifiseer word as aspekte wat, indien dit voldoende aangespreek sou word, die onderneming/departement sou neem van waar dit tans is tot waar dit wil wees.

Die strategiese elemente is daardie elemente wat die geantisipeerde gaping tussen die huidige strategie en scenario's wat geskep is, sal vernou.

Voortspruitend uit die evaluasie- en verifikasieproses ontstaan 'n gapingsanalise wat prakties toegepas kan word met behulp van 'n strategie en strategiese riglyne.

Rekenaarstrategie en strategiese riglyne

'n Onderskeid moet getref word tussen korporatiewe, besigheids- en funksionele strategieë. 'n Korporatiewe strategie is hoofsaaklik strategies, 'n besigheidstrategie takties en 'n funksionele strategie operasioneel gerig.

Daar moet egter gewaak word teen die volgende misvattings en algemene slaggate in die definiëring van 'n strategie:

- Verwarring van doelwitte en oogmerke met 'n strategie;
- Om slegs melding te maak van die wyse waarop 'n strategie in die toekoms sal verander in plaas van duidelike strategieformulering en definiëring;
- Onvoldoende beskrywing van die strategiese komponente;
- Nalatigheid om sinergie waar te neem by beide die korporatiewe en besigheidsvlakstrategieë; en
- Om slegs te konsentreer op eksplisiete stellings en nie die korrekte strategie-afleiding te maak uit aksies wat in die verlede geneem is nie.

Die rekenaarstrategie en strategiese riglynformulering behels die identifisering van strategiese alternatiewe en die ontleding van daardie kritiese strategiese elemente. Die strategiese alternatiewe word vervolgens geëvalueer aan die hand van vooraf bepaalde kriteria en dan geselekteer vir implementering.

Strategiese elemente wat geselekteer word, word omskryf deur middel van doelwitte en oogmerke wat spesifiek gestel moet word en wat tot gevolg het dat die huidige rekenaarsekuriteit en -beheerstrategie aangepas moet word met behulp van daardie geïdentifiseerde elemente/aspekte.

Aksieplan

Die daarstelling van aksieprogramme is die finale resultaat van die strategiese formuleringsproses.

Aksieplanne behels 'n reeks stappe wat uitgevoer moet word om 'n gewenste resultaat te behaal en word opgestel aan die hand van doelwitte, oogmerke en strategiese elemente.

Die vereistes en voorwaardes waaraan aksieplanne moet voldoen, is:

- Die planne moet duidelik wees.
- Die planne moet realisties wees.
- Die planne moet bereikbaar wees.
- Take moet deeglik uitgespel wees.
- Verantwoordelikhede moet toegeken wees.
- Tydperk en keerdatums moet gekoppel wees aan aksies.
- 'n Bestuursborg moet geïdentifiseer word en betrokke wees.
- Konsensus en verbintenis moet deur alle partye onderneem word.

Aksieplanne is dus die padkaart waarvolgens 'n strategie geïmplementeer kan word.

Instandhouding en koördinering van rekenaarsekuriteit en -beheer

Die instandhouding van rekenaarsekuriteit is die funksie van elke betrokke party en word geïmplementeer deur die rekenaarsekuriteitstaakspan en gekoördineer deur die rekenaarsekuriteitskomitee.

Daar moet 'n formele kanaal en stelsel wees vir enige wysigings of verbeterings aan rekenaarsekuriteit en -beheer en behoort in 'n logiese volgorde geïdentifiseer, geëvalueer en aanbeveel te word, en deur bestuur goedgekeur te word na behoorlike regverdiging.

Toekomsperspektiewe en samevatting

Rekenaarsekuriteit en -beheer sal toenemende tegnies en meer gekompliseerd raak, namate die rekenaaromgewing ontwikkel en bedreigings en risiko's toeneem.

Rekenaarsekuriteit sal veral in aanvraag wees in areas soos rekenaarnetwerke, elektroniese fondsoorplasingstelsels, komplekse databasisse, persoonlike rekenaars, en by personeel en gebruikers van rekenaars.

'n Groter verantwoordelikheid sal op bestuur rus om die inligtingshulpbronne en bates te beveilig namate meer kapitaal geïnvesteer word in rekenaars en inligtingstelselontwikkeling.

Rekenaarsekuriteit is egter nie gratis nie, en bestuur sal besef dat deur 'n doeltreffende strategie/funksionele formuleringsproses en implementeringsbenadering daar te stel, rekenaarsekuriteit en -beheer nie noodwendig duur is nie, maar wel koste-effektief kan wees.

Elke rekenaargebaseerde inligtingstelselorganisasie word genoodsaak en is verantwoordelik om faktore wat rekenaarsekuriteit mag beinvloed, te identifiseer en te ontleed, die huidige situasie in oënskou te neem en sistematies en logies daardie elemente wat afwesig mag wees, te implementeer en instand te hou.

Verwysings

Anon. 1986. The invincible rip-off. *Computer Mail*, 25 Julie.

Bezuidenhout, R.J. 1988. *'n Strategie tot rekenaarsekuriteit en beheer*. Ongepubliseerde MBA-Skripsie, PU vir CHO, Potchefstroom.

EDP Auditors Foundation. 1983. Control objectives: Controls in a computer environment: objectives, guidelines and audit procedures. *Carol Stream*, No Ill; p.144.

Fritzgerald, J. 1984. *Designing controls in computerized systems*. Redwood City, California: Fitzgerald.

Glueck, W.F. & Jauch, L.R. 1984. *Business policy and strategic management*. Auckland: McGraw-Hill.

Hofer, C.W. & Schendel, D. 1979. *Strategy formulation: Analytical concepts*. New York: West.

Parker, D.B. 1983. *Fighting computer crime*. New York: Scribners.

Richards, T.C. 1986. A historical prospective of computer related fraud. *Security, Audit and Control Review*, No.4,(3): 27 February.

S.A. Instituut van Geoktroieerde Rekenmeesters. 1986. *Rekenkundige stelsels en interne beheermaatreëls*. Johannesburg. (Standpunt OU230).